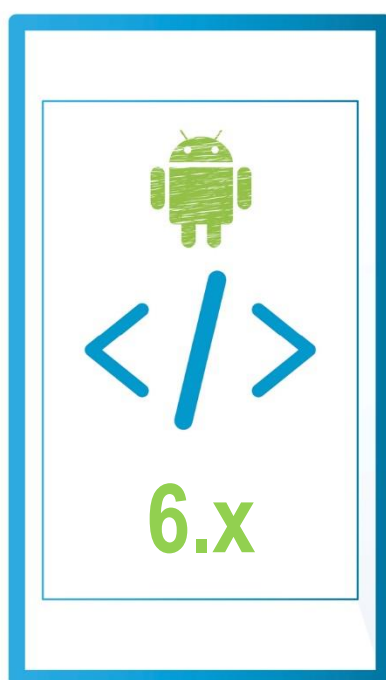


Guía de Seguridad de las TIC

CCN-STIC 453D

SEGURIDAD DE DISPOSITIVOS MÓVILES: ANDROID 6.x



Mayo 2018

Edita:



CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=52800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRYPTOLOGICO NACIONAL, c=ES
2018.06.05 12:38:31 +02'00'

© Centro Criptológico Nacional, 2018

NIPO: 785-18-033-5

Fecha de Edición: mayo de 2018

Raúl Siles y Mónica Salas (DinoSec) han participado en la realización y modificación del presente documento y sus anexos.

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

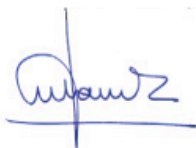
Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, modificado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Mayo de 2018



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN.....	8
2. OBJETO	8
3. HISTORIA DE ANDROID: VERSIONES Y CARACTERÍSTICAS.....	9
4. ALCANCE	11
4.1. ANDROID 2.X	11
4.2. ANDROID 3.X	12
4.3. ANDROID 4.0	12
4.4. ANDROID 4.1	13
4.5. ANDROID 4.2	13
4.6. ANDROID 4.3	15
4.7. ANDROID 4.4	16
4.8. ANDROID 5.X	18
4.9. ANDROID 6.X	20
4.10. DIFERENCIAS ENTRE LAS MÚLTIPLES VERSIONES DE ANDROID	24
5. ENTORNO DE APLICACIÓN DE ESTA GUÍA.....	25
6. ACTUALIZACIÓN DEL SISTEMA OPERATIVO ANDROID	29
6.1. ACTUALIZACIÓN AUTOMÁTICA DEL SISTEMA OPERATIVO ANDROID	29
6.2. SERVICIOS DE GOOGLE PLAY	38
6.3. ACTUALIZACIÓN MANUAL COMPLETA DE ANDROID.....	40
6.4. ACTUALIZACIÓN MANUAL PARCIAL DE ANDROID	46
7. MODELO Y ARQUITECTURA DE SEGURIDAD DE ANDROID	50
7.1. MODELO DE PERMISOS DE ANDROID	51
7.1.1. MODELO DE PERMISOS EN TIEMPO DE INSTALACIÓN	51
7.1.2. MODELO DE PERMISOS EN TIEMPO DE EJECUCIÓN	55
7.1.3. PERMISOS NORMALES Y PELIGROSOS	59
7.1.4. PERMISOS SIMPLIFICADOS Y GRUPOS DE PERMISOS DE GOOGLE PLAY	59
7.1.5. APP OPS	63
7.2. SANDBOX DE EJECUCIÓN DE LAS APPS	64
7.3. DIRECT SHARE.....	66
7.4. ART (ANDROID RUNTIME)	68
7.5. INSTALACIÓN DE APPS (DE ORÍGENES DESCONOCIDOS) EN ANDROID.....	69
7.6. FIRMA DIGITAL DE APPS EN ANDROID	71
7.7. SELINUX EN ANDROID	73
7.8. PROCESO DE ARRANQUE SEGURO: VERIFIED BOOT	74
7.9. MODO DE ARRANQUE SEGURO: SAFE MODE	76
7.10. CONFIGURACIÓN POR DEFECTO DEL DISPOSITIVO MÓVIL.....	77
8. GESTIÓN EMPRESARIAL DE DISPOSITIVOS MÓVILES BASADOS EN ANDROID	79
8.1. GESTIÓN REMOTA DE DISPOSITIVOS ANDROID POR PARTE DEL USUARIO.....	81
8.2. ANDROID FOR WORK	96
9. ACCESO FÍSICO AL DISPOSITIVO MÓVIL.....	99
9.1. PIN DE LA TARJETA SIM	100
9.2. CÓDIGO DE ACCESO AL DISPOSITIVO MÓVIL.....	102
9.3. HUELLA DACTILAR DIGITAL (<i>FINGERPRINT</i>)	112
9.4. BLOQUEO Y DESBLOQUEO DE PANTALLA	117
9.5. DESBLOQUEO MEDIANTE SMART LOCK.....	120
9.6. PANTALLA DE DESBLOQUEO: PREVISUALIZACIÓN DE DATOS	131

9.7. INTERRUPCIONES	133
9.8. NOTIFICACIONES	136
9.9. AHORRO DE BATERÍA	142
9.10. CONFIGURADOR DE IU DEL SISTEMA	145
9.11. PANTALLA DE DESBLOQUEO: APAGAR EL DISPOSITIVO MÓVIL	150
9.12. MENÚ DE AJUSTES RÁPIDOS Y BARRA DE NOTIFICACIONES	151
9.13. PANTALLA DE DESBLOQUEO: WIDGETS Y CARPETAS	156
9.14. PANTALLA DE DESBLOQUEO: CÁMARA.....	159
9.15. PANTALLA DE DESBLOQUEO: INFORMACIÓN DEL PROPIETARIO	160
9.16. PRECAUCIONES Y RECOMENDACIONES ADICIONALES	162
9.17. DESBLOQUEO MEDIANTE LA CUENTA DE USUARIO DE GOOGLE	163
9.18. RESTAURACIÓN DEL CÓDIGO DE ACCESO	163
9.19. MÚLTIPLES PERFILES DE USUARIO	165
10. CIFRADO DE DATOS EN ANDROID	173
10.1. CIFRADO DEL DISPOSITIVO MÓVIL.....	173
10.2. ALMACENAMIENTO ADOPTABLE	180
10.2.1. ALMACENAMIENTO ADOPTABLE EXTERNO	181
10.2.2. ALMACENAMIENTO ADOPTABLE INTERNO.....	183
10.3. DISPOSITIVOS DE ALMACENAMIENTO OTG (ON-THE-GO)	189
10.4. ELIMINACIÓN DE DATOS DEL DISPOSITIVO MÓVIL.....	191
11. GESTIÓN DE CERTIFICADOS DIGITALES Y CREDENCIALES	193
11.1. ANDROID KEYSTORE SYSTEM: ALMACENAMIENTO DE CREDENCIALES	193
11.2. CERTIFICADOS DIGITALES DE SISTEMA Y DE USUARIO	196
11.3. GESTIÓN DE CERTIFICADOS DIGITALES	202
11.3.1. GESTIÓN DE CERTIFICADOS DIGITALES DE AUTORIDADES CERTIFICADORAS	202
11.3.2. GESTIÓN DE CERTIFICADOS DIGITALES SERVIDOR.....	207
11.3.3. GESTIÓN DE CERTIFICADOS DIGITALES CLIENTE	207
12. LOCALIZACIÓN (O UBICACIÓN) GEOGRÁFICA	212
12.1. SERVICIOS DE UBICACIÓN DE GOOGLE	216
12.2. GOOGLE MAPS	217
12.3. A-GPS.....	225
12.4. GPSONEXTRA.....	226
12.5. HISTORIAL DE UBICACIONES	227
12.6. OTRAS APPS QUE HACEN USO DE LA LOCALIZACIÓN	231
12.6.1. GOOGLE MAPS: NAVEGACIÓN	231
12.6.2. NOTICIAS Y EL TIEMPO	232
12.6.3. BUSCADOR DE GOOGLE.....	232
12.6.4. REDES SOCIALES	234
12.6.5. NAVEGADOR WEB	234
12.7. INFORMACIÓN GEOGRÁFICA EN FOTOGRAFÍAS.....	236
13. COMUNICACIONES USB.....	239
13.1. ALMACENAMIENTO USB	240
13.2. CONEXIÓN DE RED COMPARTIDA POR USB (TETHERING).....	243
13.3. OPCIONES DE DESARROLLO Y DEPURACIÓN USB	246
13.4. RELACIONES DE CONFIANZA A TRAVÉS DE USB.....	249
14. COMUNICACIONES NFC.....	251
14.1. UTILIZACIÓN DE LAS COMUNICACIONES NFC.....	251
14.2. CONFIGURACIÓN DE NFC	252

14.3. PAGOS (Y OTROS SERVICIOS) MEDIANTE NFC	254
15. COMUNICACIONES BLUETOOTH.....	258
15.1. UTILIZACIÓN DE LAS COMUNICACIONES BLUETOOTH	258
15.2. CONFIGURACIÓN GENERAL DE BLUETOOTH	262
15.3. DISPOSITIVOS BLUETOOTH EMPAREJADOS	265
15.4. CONFIGURACIÓN AVANZADA DE BLUETOOTH	270
15.5. OBEX PUSH	271
15.6. MANOS LIBRES BLUETOOTH	273
15.7. CONEXIÓN DE RED COMPARTIDA POR BLUETOOTH	275
15.8. BLUETOOTH LOW ENERGY (BLE).....	276
16. COMUNICACIONES WI-FI.....	279
16.1. UTILIZACIÓN Y CONFIGURACIÓN DE LAS COMUNICACIONES WI-FI.....	279
16.2. SELECCIÓN DE LA RED DE DATOS EN ANDROID.....	284
16.3. RECOMENDACIONES DE SEGURIDAD PARA LA CONEXIÓN A REDES WI-FI	288
16.4. LISTA DE REDES PREFERIDAS (PNL)	297
16.5. CONEXIÓN AUTOMÁTICA A REDES WI-FI: OCULTAS O VISIBLES Y RESTRICCIÓN DE CONEXIÓN	300
16.6. PUNTO DE ACCESO O ZONA WI-FI.....	305
16.7. WI-FI DIRECT (“P2P”).....	309
17. COMUNICACIONES MÓVILES: MENSAJES DE TEXTO (SMS)	312
18. COMUNICACIONES MÓVILES: VOZ Y DATOS.....	316
18.1. DESACTIVACIÓN DE LAS COMUNICACIONES DE VOZ Y DATOS MÓVILES.....	316
18.2. CONFIGURACIÓN Y SELECCIÓN DE LA RED (VOZ) DE TELEFONÍA MÓVIL	320
18.3. CONFIGURACIÓN DE LA RED DE DATOS MÓVILES	327
18.4. SELECCIÓN DE LA RED DE DATOS MÓVILES	328
19. COMUNICACIONES TCP/IP	331
19.1. ADAPTADORES DE RED.....	331
19.2. SEGURIDAD EN TCP/IP.....	335
19.3. ESCANEADO DE PUERTOS TCP Y UDP	336
19.4. HTTPS: SSL/TLS	337
19.5. IPV6.....	340
19.6. REDES VPN.....	341
20. CUENTA DE USUARIO DE GOOGLE.....	347
20.1. ASIGNACIÓN DE UNA CUENTA DE USUARIO DE GOOGLE AL DISPOSITIVO MÓVIL....	349
20.2. SINGLE SIGN-ON: AUTENTICACIÓN DE USUARIOS DE DISPOSITIVOS MÓVILES EN SERVICIOS Y APPS	353
20.3. INICIO DE SESIÓN Y SEGURIDAD: VERIFICACIÓN EN DOS PASOS.....	355
20.3.1. GOOGLE AUTHENTICATOR	364
20.4. INFORMACIÓN PERSONAL Y PRIVACIDAD.....	366
20.4.1. “TU INFORMACIÓN PERSONAL”	366
20.4.2. ADMINISTRAR TU ACTIVIDAD DE GOOGLE	368
20.4.3. ANUNCIOS	370
20.4.4. CONTROLA TU CONTENIDO.....	372
20.5. PREFERENCIAS DE LA CUENTA	377
20.6. GESTIÓN DE LAS CREDENCIALES DE LAS CUENTAS DE USUARIO DE GOOGLE.....	379
20.7. INICIO DE SESIÓN Y SEGURIDAD	384
20.8. OTROS AJUSTES DE GOOGLE	387

21. COPIAS DE SEGURIDAD	388
21.1. COPIA DE SEGURIDAD LOCAL	388
21.2. COPIA DE SEGURIDAD EN LOS SERVIDORES DE GOOGLE	391
21.3. COPIA DE SEGURIDAD DE FOTOS Y VÍDEOS	394
21.4. COPIA DE SEGURIDAD AUTOMÁTICA DE LOS DATOS DE LAS APPS	401
22. APP GOOGLE: ASISTENTE DE GOOGLE, MI TABLÓN Y SERVICIOS DE BÚSQUEDA DE GOOGLE	403
22.1. GOOGLE “NOW ON TAP”	409
22.2. CUENTAS Y PRIVACIDAD	411
22.3. ASISTENTE PERSONAL Y “OK GOOGLE”	416
23. APLICACIONES MÓVILES (APPS) EN ANDROID	423
23.1. NAVEGACIÓN WEB: NAVEGADOR CHROME	424
23.1.1. CONTENIDOS ADOBE FLASH	437
23.1.2. CONTENIDOS ADOBE PDF	437
23.1.3. HISTORIAL DE ACTIVIDAD WEB Y DE APLICACIONES	438
23.1.4. CERTIFICATE PINNING Y CERTIFICATE BLACKLISTING	444
23.1.5. ANDROID WEBVIEWS	445
23.2. CORREO ELECTRÓNICO (E-MAIL) Y GMAIL	448
23.3. REDES SOCIALES	451
23.4. APPS DE TERCEROS: GOOGLE PLAY	451
23.5. SCREEN PINNING	456
23.6. ESTADÍSTICAS DETALLADAS DE USO DE LAS APPS	458
23.7. SAFETYNET	459
23.8. VERIFICACIÓN DE SEGURIDAD DE LAS APPS: GOOGLE PLAY PROTECT	462
23.9. GESTIÓN DE APPS EN ANDROID	467
23.9.1. ACTUALIZACIÓN DE APPS EN ANDROID	467
23.9.2. ACTUALIZACIÓN AUTOMÁTICA DE APPS	474
23.9.3. INSTALACIÓN REMOTA DE APPS	476
23.9.4. ELIMINACIÓN REMOTA DE APPS	477
23.9.5. CONEXIÓN GTALKSERVICE	478
23.10. ACCESO Y ALMACENAMIENTO DE DATOS DESDE APPS	479
23.11. ALMACENAMIENTO DE CREDENCIALES E INFORMACIÓN SENSIBLE EN APPS	480
23.12. ENLACES Y REFERENCIAS WEB DESDE LAS APPS	481
23.13. INSTANT APPS	483
23.14. SERVICIO DE CONTRASEÑAS DE GOOGLE SMART LOCK	484
24. APÉNDICE A: PROCESO DE INSTALACIÓN Y CONFIGURACIÓN INICIAL	487
25. APÉNDICE B: CAPTURA DE LA PANTALLA EN ANDROID	506
26. REFERENCIAS	507

1. INTRODUCCIÓN

1. El desarrollo de los dispositivos y comunicaciones móviles, y de las tecnologías inalámbricas, en los últimos años ha revolucionado la forma de trabajar y comunicarse. El uso creciente de estas tecnologías sitúa a los dispositivos móviles como uno de los objetivos principales de las ciberamenazas.
2. La proliferación de dispositivos móviles en los últimos años, junto al aumento de las capacidades, prestaciones y posibilidades de utilización de los mismos, hace necesario evaluar en profundidad la seguridad ofrecida por este tipo de dispositivos respecto a la información que gestionan, profundizando en los mecanismos de protección que ofrecen, dentro de los entornos de Tecnologías de la Información y las Comunicaciones (TIC).
3. Se considera dispositivo móvil aquél dispositivo electrónico de uso personal o profesional de reducido tamaño que permite la gestión de información (almacenamiento, intercambio y procesamiento de información) y el acceso a redes de comunicaciones y servicios remotos, tanto de voz como de datos, y que habitualmente dispone de capacidades de telefonía, como por ejemplo teléfonos móviles, *smartphones* (teléfonos móviles avanzados o inteligentes), *tablets* (o tabletas) y agendas electrónicas (PDAs, Personal Digital Assistants), independientemente de si disponen de teclado físico o pantalla táctil.
4. Pese a que los dispositivos móviles se utilizan para establecer comunicaciones personales y profesionales, privadas y relevantes, y para el almacenamiento e intercambio de información sensible, el nivel de percepción de la amenaza de seguridad real existente no ha tenido la suficiente trascendencia en los usuarios finales y las organizaciones.
5. La concienciación, el sentido común y las buenas prácticas en la configuración y el uso de los dispositivos móviles constituyen una de las mejores defensas para prevenir y detectar este tipo de incidentes y amenazas [Ref.- 404].
6. El presente documento realiza un análisis detallado de los mecanismos y la configuración de seguridad recomendados para uno de los principales sistemas operativos de dispositivos móviles utilizados en la actualidad, Android 6.x, en concreto hasta la versión 6.0.1, con el objetivo de reducir su superficie de exposición frente a ataques de seguridad.

2. OBJETO

7. El propósito del presente documento es definir una lista de recomendaciones de seguridad para la configuración de dispositivos móviles basados en el sistema operativo Android versión 6.0.1 (en adelante Android) [Ref.- 1], cuyo objetivo es proteger el propio dispositivo móvil, sus comunicaciones y la información y datos que gestiona y almacena.
8. La presente guía proporciona los detalles específicos de aplicación e implementación de las recomendaciones de seguridad generales descritas en la guía inicial de esta misma serie [Ref.- 400], que presenta la información necesaria para la evaluación y análisis de los riesgos, amenazas, y vulnerabilidades de seguridad a las que están expuestos los dispositivos móviles en la actualidad.

9. La serie CCN-STIC-450, “Seguridad de dispositivos móviles”, se ha estructurado en dos niveles: una guía genérica inicial centrada en el análisis de seguridad de dispositivos móviles (CCN-STIC-450) [Ref.- 400], complementada por guías específicas para los principales sistemas operativos empleados por los dispositivos móviles hoy en día (o en el pasado). Por este motivo, antes de la lectura y aplicación de la presente guía, asociada a un sistema operativo (y versión concreta del mismo), se recomienda la lectura de la guía general de seguridad, CCN-STIC-450.
10. La presente guía está basada en la versión previa de la misma guía “*Seguridad de dispositivos móviles: Android 5.x*”, centrada en la versión 5.1.1 de Android y publicada en el año 2017 [Ref.- 405].
11. Adicionalmente, se recomienda la lectura de las guías de esta misma serie asociadas a otros sistemas operativos y versiones de plataformas móviles, en caso de ser necesaria su aplicación en otros terminales, y a la gestión empresarial de dispositivos móviles (MDM):
 - CCN-STIC-450 - Seguridad de dispositivos móviles [Ref.- 400]
 - CCN-STIC-451 - Seguridad de dispositivos móviles: Windows Mobile 6.1
 - CCN-STIC-452 - Seguridad de dispositivos móviles: Windows Mobile 6.5
 - CCN-STIC-453(A) - Seguridad de dispositivos móviles: Android 2.x [Ref.- 401]
 - CCN-STIC-453B - Seguridad de dispositivos móviles: Android 4.x [Ref.- 402]
 - CCN-STIC-453C - Seguridad de dispositivos móviles: Android 5.x [Ref.- 405]
 - CCN-STIC-454(A) - Seguridad de dispositivos móviles: iPad (iOS 7.x)
 - CCN-STIC-455(A) - Seguridad de dispositivos móviles: iPhone (iOS 7.x)
 - CCN-STIC-457 - Gestión de dispositivos móviles: MDM (*Mobile Device Management*) [Ref.- 403]

Nota: Esta serie de guías están diseñadas considerando como requisito la necesidad de encontrar un equilibrio entre seguridad y usabilidad en relación a las capacidades y funcionalidad disponibles en los dispositivos móviles a proteger, con el objetivo de poder hacer uso de la mayoría de características disponibles en los mismos de forma segura.

3. HISTORIA DE ANDROID: VERSIONES Y CARACTERÍSTICAS

12. Android es un sistema operativo diseñado para dispositivos móviles, que emplea software de código abierto (*open-source*) basado en Linux (originalmente en el kernel 2.6.x) y que incluye el sistema operativo y el kernel, una capa de abstracción hardware (HAL, *Hardware Abstraction Layer*), un conjunto de librerías (o APIs, *Application Programming Interface*), el entorno de ejecución (Dalvik y ART, *Android RunTime*) y el entorno de desarrollo para las aplicaciones móviles (de aquí en adelante referenciadas como apps, indistintamente, y por abreviar), tanto las desarrolladas por terceros como el conjunto de aplicaciones móviles (o apps) disponibles por defecto [Ref.- 11] (ver siguiente imagen¹).

¹ Imagen: http://www.techotopia.com/index.php/Image:Android_architecture2.png

13. Inicialmente desarrollado por Android Inc., fue adquirido por Google en el año 2005, colaborando en su desarrollo la Open Handset Alliance (OHA), y encargándose de su mantenimiento el Android Open Source Project (AOSP) [Ref.- 84]. La primera versión comercial, Android 1.0, fue publicada en septiembre de 2008 [Ref.- 130].
14. La evolución de las versiones posteriores de Android (desde las versiones 2.x a la versión 4.x) ha conllevado notables modificaciones sobre el kernel de Linux estándar, y pese a seguir empleándose versiones y referencias al kernel de Linux 3.x, en los años 2010 y 2011 cada vez el entorno Android distaba más de un entorno Linux tradicional. Sin embargo, ambos proyectos, Android y Linux, volvieron a reunificarse en la versión 3.3 del kernel².



15. Las versiones de Android (desde la versión 1.5) emplean nombres en clave correspondientes a nombres de postres y dulces en inglés, ordenados alfabéticamente. A continuación se muestra el listado de versiones de Android conocidas en el momento de elaboración de la presente guía:

- *Alpha* (1.0)
- *Beta* (1.1)
- *Cupcake* (1.5)
- *Donut* (1.6)
- *Eclair* (2.0-2.1)
- *Froyo* (2.2-2.2.3)
- *Gingerbread* (2.3-2.3.7)

² <http://www.zdnet.com/article/android-and-linux-re-merge-into-one-operating-system/>

- Honeycomb (3.0-3.2.6)
 - Ice Cream Sandwich (4.0-4.0.4)
 - Jelly Bean (4.1-4.3.1)
 - KitKat (4.4-4.4.4)
 - Lollipop (5.0)
 - Marshmallow (6.0)
16. Google mantiene una web en la que proporciona recomendaciones generales sobre buenas prácticas de seguridad para desarrolladores, que se puede consultar para obtener una visión global de qué elementos resultan clave dentro de la plataforma Android para garantizar la seguridad del dispositivo móvil y las apps que en él se instalen [Ref.- 184].

4. ALCANCE

17. Las Autoridades responsables de la aplicación de la Política de Seguridad de las TIC (STIC) determinarán su análisis y aplicación a los dispositivos móviles ya existentes o futuros bajo su responsabilidad.

4.1. ANDROID 2.X

18. El primer dispositivo móvil Google Nexus, basado en Android 2.1, fue el *smartphone* Nexus One (dispositivo empleado en la versión previa de la presente guía [Ref.- 401], con una pantalla de 3,7", y desarrollado por Google y HTC), que se empezó a comercializar en enero de 2010. Posteriormente, en mayo de 2010, fue actualizado a la versión Android 2.2 y comercializado como el primer dispositivo móvil con esta nueva versión de Android.
19. Android versión 2.2 (con nombre en clave "Froyo") fue la versión por defecto incluida en numerosos dispositivos móviles disponibles en el mercado durante los años 2010 y 2011, complementando versiones previas, como la versión 2.0/2.1 de Android ("Eclair"), 1.6 ("Donut") y 1.5 ("Cupcake") [Ref.- 130].
20. La versión 2.2 (analizada en la versión previa de la presente guía) añadió, entre otras, mejoras de rendimiento, la versión v8 del motor de JavaScript de Chrome, la posibilidad de actuar como hotspot Wi-Fi para compartir la conexión de datos de telefonía móvil con otros dispositivos, y soporte para Adobe Flash en el navegador web.
21. Android anunció una actualización en diciembre de 2010 asociada a la versión 2.3 ("Gingerbread") [Ref.- 9], que añadía mejoras en el interfaz de usuario, el teclado táctil y las capacidades de copiar y pegar datos, así como soporte para SIP (voz sobre IP, VoIP) y NFC (*Near Field Communication*), con capacidades NFC extras añadidas en la versión 2.3.3 [Ref.- 10]. El primer dispositivo móvil basado en Android 2.3 fue el *smartphone* Nexus S (desarrollado por Google y Samsung), comercializado en la misma fecha de lanzamiento que Android 2.3.

4.2. ANDROID 3.X

22. La versión 3.0 de Android (“Honeycomb”) fue diseñada para dispositivos en formato tableta (o *tablets*), con pantalla de mayor tamaño y mayor capacidad de procesamiento (tanto del procesador principal como gráfico). Esta versión añadió la posibilidad de aplicar un cifrado completo a los datos almacenados en el dispositivo móvil [Ref.- 85]. El primer dispositivo móvil basado en Android 3.0, la tableta Motorola Xoom, se empezó a comercializar en el mercado en febrero de 2011.
23. Posteriormente se publicaron las versiones 3.1 y 3.2 en mayo y julio de 2011 respectivamente. La versión 3.1 añadió soporte para más dispositivos de entrada y conexión USB para la transferencia de ficheros, mientras que la versión 3.2 añadió soporte para tarjetas de memoria SD y mejoras en la gestión de la pantalla y de distintas resoluciones gráficas.

4.3. ANDROID 4.0

24. La versión 4.0 de Android (“Ice Cream Sandwich”, ICS), basada en el kernel 3.0.1 de Linux, fue anunciada en octubre de 2011 y proporcionó gran parte de la funcionalidad existente en “Honeycomb” (Android 3.x) a los *smartphones* (no únicamente a *tablets*), añadiendo un gran número de funcionalidades y cambios en el interfaz de usuario, como por ejemplo mejoras en las capacidades multitarea, nuevas funcionalidades en la pantalla de desbloqueo (como el acceso directo a la cámara o el acceso al centro de notificaciones), control de acceso mediante reconocimiento facial utilizando la cámara frontal, control y monitorización del tráfico de red y datos (redes móviles y/o Wi-Fi), la posibilidad de compartir información mediante NFC (y Android Beam), soporte para Wi-Fi Direct (o Wi-Fi Peer-to-Peer, “P2P”), soporte para el perfil Bluetooth HDP (*Health Device Profile*) y para la conexión a sensores y dispositivos médicos y de salud inalámbricos, y nuevas capacidades de gestión y almacenamiento de credenciales y certificados digitales (keychain API [Ref.- 188]), entre otros. El primer dispositivo móvil basado en Android 4.0, el *smartphone* Galaxy Nexus (desarrollado por Google y Samsung), se empezó a comercializar en noviembre de 2011, y fue el primer Nexus con soporte para LTE (4G).
25. Android 4.0 implementó ASLR (*Address Space Layout Randomization*) para proteger tanto los componentes del sistema como las aplicaciones móviles (apps) de terceros frente a la explotación de vulnerabilidades debidas a una incorrecta gestión de la memoria. Adicionalmente, Android 4.0 incorporó el *Android VPN Framework* (AVF, o VPN API), que añade por defecto un cliente VPN con soporte para L2TP e IPSec. En versiones previas de Android el uso de software de conexión a redes VPN, en algunos escenarios, requería disponer de un dispositivo móvil Android *rooteado* (o con el proceso de *root* aplicado).
26. Desde el punto de vista de la gestión, se añadieron controles para poder deshabilitar remotamente la(s) cámara(s) del dispositivo móvil mediante las soluciones de gestión empresarial de dispositivos móviles o MDM (*Mobile Device Management*) y mediante el uso de la app de gestión de Google asociada (de tipo *Device Policy Manager*) en Android.

4.4. ANDROID 4.1

27. La versión 4.1 de Android (“Jelly Bean”, JB) fue anunciada en la conferencia Google I/O en junio de 2012, centrada en mejorar la funcionalidad y rendimiento del interfaz de usuario, y con nuevas capacidades como las transferencias de datos mediante Bluetooth vía Android Beam (adicionalmente a las basadas en NFC), el descubrimiento de servicios a través de Wi-Fi Direct (o Wi-Fi “P2P”), o el descubrimiento de servicios a través de *multicast* DNS en redes Wi-Fi (Wi-Fi NDS, *Network Service Discovery*). El primer dispositivo móvil basado en Android 4.1, la tableta o *tablet* Nexus 7 (desarrollada por Google y Asus), se empezó a comercializar en julio de 2012.
28. Adicionalmente la versión 4.1 de Android añadió soporte para GCM (*Google Cloud Messaging*) [Ref.- 143], un servicio que permite el envío de mensajes y notificaciones *push* a los usuarios de apps específicas por parte de sus desarrolladores desde sus servidores a través de Google. Estas capacidades pueden ser también empleadas, por ejemplo, por las soluciones empresariales de gestión de dispositivos móviles (MDM).
29. Asimismo, Android 4.1 añadió múltiples capacidades a Google Play, como funcionalidad para proteger las apps de pago y sus contenidos mediante cifrado, empleando una contraseña específica para cada dispositivo móvil, antes de ser distribuidas y almacenadas desde la tienda o mercado oficial de apps de Google. Los nuevos servicios de Google Play también permiten integrar las capacidades de autenticación asociadas a la cuenta de usuario de Google en las apps de Android, así como integrarlas con Google+. Con el objetivo de mejorar y optimizar la distribución de nuevas actualizaciones de las apps, las actualizaciones de apps inteligentes (*Smart App Updates*) permiten enviar a los dispositivos móviles Android únicamente los elementos de la app que han sido actualizados, en lugar del paquete de Android (o APK) completo de la app.

4.5. ANDROID 4.2

30. La versión 4.2 de Android (también denominada “Jelly Bean”), basada en el kernel 3.4.0 de Linux, fue anunciada en octubre de 2012³, e introducía nuevas capacidades en la pantalla de desbloqueo (como el soporte para complementos, *widjets*), soporte para múltiples cuentas o perfiles de usuario (sólo para tabletas), la reimplementación de la pila NFC y de la pila Bluetooth (pasando de BlueZ a BlueDroid, esta última desarrollada por Google y Broadcom), soporte para pantallas externas (incluso a través de Wi-Fi, mediante *Wi-Fi Display*), la ocultación de las opciones de desarrollo por defecto, debiendo activarse éstas manualmente, y optimizaciones en el entorno de ejecución Dalvik. Los primeros dispositivos móviles basados en Android 4.2 fueron el Nexus 4 (*smartphone* desarrollado por Google y LG) y la Nexus 10 (tableta desarrollada por Google y Samsung), ambos comercializados en noviembre de 2012.
31. La versión 4.2 añadió notables mejoras de seguridad [Ref.- 140], destacando:
 - *Always-on VPN*, para permitir que las apps únicamente generen tráfico de red si existe una conexión VPN activa y proteger así el envío de datos no cifrados a través de otras redes que podrían acceder a la información transmitida (ej. directamente a través de Internet); ver apartado “19.6. Redes VPN”.

³ Android 4.2 fue simplemente anunciada a través de una nota de prensa debido al huracán Sandy.

- Generación de notificaciones, y confirmación por parte del usuario, antes de realizar el envío de mensajes SMS *premium* (con coste adicional).
 - Verificación de apps, funcionalidad que permite analizar las aplicaciones móviles (apps) antes de su instalación para detectar si disponen de código o funcionalidades dañinas conocidas (*malware*); ver apartado “23.8. Verificación de seguridad de las apps: Google Play Protect”.
 - La librería principal con soporte para SSL/TLS añadió soporte para *certificate pinning* [Ref.- 79], permitiendo disponer de un mayor control sobre el certificado digital empleado por una app o un dominio concreto, y evitando problemas de seguridad asociados a las autoridades certificadoras (CAs, *Certificate Authorities*).
 - Organización de los permisos de las apps en grupos, lo que simplifica su aprobación por parte del usuario estándar, pero limita la granularidad en su análisis y en la autorización por parte de usuarios avanzados.
 - El demonio *install* encargado de la instalación de apps no ejecuta con permisos de root (o superusuario), limitando así la explotación de potenciales vulnerabilidades sobre este componente.
 - Los scripts de arranque (*init scripts*) aplican la semántica basada en la directiva O_NOFOLLOW para prevenir ataques mediante enlaces (o *links*) simbólicos.
 - Por defecto, las apps que hacen uso de la API 17 o superior no exportan sus proveedores de contenidos (ContentProviders), reduciendo así su exposición frente a posibles ataques.
 - Por defecto, las apps que hacen uso de la API 17 o superior y que utilizan WebViews no permiten el acceso directo al método “*addJavaScriptInterface()*”, limitando la ejecución remota de código en la interacción entre JavaScript y Java, y reduciendo así su exposición frente a posibles ataques.
 - Mejoras en la implementación por defecto para la generación de números aleatorios (SecureRandom) y RSA pasa a hacer uso de OpenSSL (1.0.1), con soporte para TLS v1.1 y v1.2.
 - Múltiples actualizaciones de seguridad de librerías, como por ejemplo WebKit, libpng, OpenSSL, y LibXML.
32. Adicionalmente, la versión Android 4.2 proporcionó una nueva funcionalidad para establecer conexiones USB seguras con un ordenador (concretamente desde la versión Android 4.2.2 y posteriores), autenticando las conexiones ADB mediante un par de claves RSA, y solucionó la vulnerabilidad Master Key (teóricamente desde Android 4.2.2, aunque la versión concreta depende del fabricante del dispositivo móvil).

4.6. ANDROID 4.3

33. La versión 4.3 de Android (también denominada “Jelly Bean”), fue liberada en julio de 2013, con soporte para Bluetooth Smart (o BLE, *Bluetooth Low Energy*, disponible inicialmente en los modelos Nexus 4 y Nexus 7 2013), acceso restringido para nuevos perfiles de usuario, la disponibilidad temporal de “App Ops” (un sistema granular de control de permisos para las aplicaciones móviles, oculto por defecto⁴), optimizaciones en el cálculo de la localización vía hardware en lugar de software (*hardware geofencing*) y soporte para la obtención de información de redes Wi-Fi cercanas para los servicios de localización, incluso cuando el interfaz Wi-Fi está apagado. La mayoría de dispositivos móviles Nexus obtuvieron la actualización 4.3 a la semana de su publicación, y el primer dispositivo móvil en ser comercializado directamente con Android 4.3 fue la segunda generación de la *tablet* Nexus 7, conocida como Nexus 7 2013 (también desarrollada por Google y Asus), en julio de 2013.
34. La versión 4.3 añadió notables mejoras de seguridad [Ref.- 140], destacando:
- Las apps pueden configurar las credenciales de redes Wi-Fi WPA(2)-Empresariales que necesiten, pudiendo emplear múltiples métodos de autenticación basados en el estándar EAP (*Extensible Authentication Protocol*).
 - La API de keychain dispone de nuevas capacidades para establecer que un conjunto de credenciales no puede ser exportado fuera del dispositivo móvil, es decir, se vinculan al hardware o dispositivo móvil concreto. Asimismo, las apps disponen de capacidades para almacenar credenciales en un Keystore privado que no esté accesible a otras apps, y estas credenciales pueden ser añadidas sin interacción del usuario, siendo posible definir que tampoco puedan ser exportadas.
 - La partición de sistema (“/system”) en Android 4.3 es montada con restricciones mediante el parámetro o flag *nosuid*, y los procesos derivados de zygote no disponen de capacidades para ejecutar programas SUID, limitando por tanto la ejecución de programas con *setuid* o *setgid* por parte de las apps (por ejemplo, con privilegios de root o superusuario), y evitando así la explotación de ciertas vulnerabilidades previamente conocidas. Adicionalmente se eliminaron numerosos programas *setuid* o *setgid*.
 - Tanto zygote como ADB reducen sus capacidades antes de ejecutar apps, evitando así que las apps ejecutadas tanto desde el propio Android como desde una *shell* (a través de ADB) no dispongan de capacidades privilegiadas. Adicionalmente zygote evita que se añadan nuevas capacidades antes de ejecutar código por parte de las apps, evitando la elevación de privilegios vía “execve”.
 - Utilización de las capacidades FORTIFY_SOURCE por parte de las librerías y aplicaciones del sistema para prevenir la explotación de vulnerabilidades de *strings* no terminados adecuadamente o de corrupción de memoria, junto a

⁴ Este sistema granular de control de permisos para las aplicaciones móviles fue eliminado en una versión posterior de Android por Google, concretamente en la versión 4.4.2. El mismo actuó como el precursor del modelo de permisos en tiempo de ejecución introducido en Android 6.x.

otras protecciones en la reubicación de código (*relocation*) para binarios enlazados estáticamente y en el propio código de Android.

- Soporte para MAC (*Mandatory Access Control*, frente a *Discretionary Access Control*, DAC) en Android a través de SELinux (Security-Enhanced Linux) [Ref.-142] y la definición asociada de políticas de seguridad. En Android 4.3 se hace uso de SELinux en modo permisivo o *permissive mode*, donde únicamente las acciones no legítimas son registradas por el kernel, pero no bloqueadas [Ref.-141].
- Las capacidades MAC (*Mandatory Access Control*) de SELinux en Android se pueden emplear en todos los procesos, tanto los asociados a las apps como los procesos de sistema que ejecutan como root o system (aplicando el modelo de permisos basado en *Linux capabilities*), dependiendo de la versión de Android.

4.7. ANDROID 4.4

35. La versión 4.4 de Android (“KitKat”, KK [Ref.- 148]) fue anunciada en septiembre de 2013, optimizada específicamente para ejecutar en dispositivos más básicos con capacidades reducidas, incluso con tan sólo 512 MB de memoria RAM (o incluso menos⁵; *Project Svelte*⁶). Adicionalmente, esta versión añadió capacidades de impresión inalámbricas, un nuevo proveedor de SMS para la gestión de mensajes (SMS/MMS), soporte para emulación de *host* en NFC (HCE, *Host Card Emulation*), permitiendo que las apps de un dispositivo móvil lean y emulen *smartcards* NFC (como las empleadas como medio de pago en las tarjetas EMV), incorporó nuevos perfiles Bluetooth (*Bluetooth HID over GATT* (HOGP), MAP (*Message Access Profile*) y extensiones para AVRCP), soporte para *Wi-Fi Tunneled Direct Link Setup* (TDLS), añadió una implementación nueva de WebView basada en Chromium, añadió también la certificación *Wi-Fi Display Specification* haciendo compatibles con Miracast a los dispositivos móviles Android 4.4 (como por ejemplo el modelo Nexus 5), e introdujo el nuevo entorno de ejecución ART (*Android RunTime*) como futuro sustituto de Dalvik, pero todavía de manera experimental y no habilitado por defecto. El primer dispositivo móvil basado en Android 4.4 fue el *smartphone* Nexus 5 (desarrollado por Google y LG), comercializado en octubre de 2013. Posteriormente, la actualización de Android 4.4 (KitKat) se extendió a otros dispositivos móviles de Google, como el Nexus 4, Nexus 7 o Nexus 10, y de otros fabricantes.

⁵ El valor mínimo de RAM necesario para ejecutar Android 4.4.x se supone que es de 340MB.

⁶ <http://android-developers.blogspot.com.es/2013/10/android-44-kitkat-and-updated-developer.html>

Nota: Android 4.4 (KitKat) introdujo soporte nativo para (Google) Cloud Print⁷, un servicio que permite imprimir desde cualquier dispositivo móvil Android (y otros dispositivos y ordenadores), y desde cualquier lugar, en cualquier impresora conectada a Cloud Print, y cuya configuración está disponible bajo el menú “Ajustes [Sistema] - Impresión”. Las versiones previas de Android pueden utilizar la app Cloud Print⁸, disponible en Google Play, para hacer uso de este servicio. Se recomienda deshabilitar las capacidades de impresión de Android si no se está haciendo uso de ellas (habilitadas por defecto). El análisis de seguridad de Cloud Print queda fuera del alcance de la presente guía.

Igualmente, Android dispone de capacidades para extender la funcionalidad del teclado existente por defecto mediante la instalación de apps de teclado de terceros (IME, *Input Method Editor*). Debido a que el teclado gestiona la mayoría de la entrada de datos del usuario, incluyendo contraseñas, un teclado malicioso podría registrar todo lo que teclea el usuario en un fichero local, e incluso enviarlo a un servidor remoto a través de Internet. Por este motivo, debe prestarse especial atención a los teclados actualmente instalados, disponibles desde el menú “Ajustes [Personal] - Idioma e introducción de texto [Teclado y métodos de introducción]”, eliminando aquellos en los que no se confíe, y tomar precauciones a la hora de instalar nuevos teclados. El análisis de seguridad de teclados adicionales en Android queda fuera del alcance de la presente guía.

36. Las subversiones de la versión 4.4 añadieron capacidades destacables, como una mejor compatibilidad con las aplicaciones móviles para ART en 4.4.1, la eliminación del sistema de control de permisos “App Ops” en 4.4.2 (añadido en Android 4.3) o cambios para solucionar la vulnerabilidad de Heartbleed de OpenSSL en 4.4.3.

37. La versión 4.4 añadió notables mejoras de seguridad [Ref.- 86][Ref.- 140], destacando:

- Granularidad para configurar redes VPN por usuario en dispositivos multi-usuario, permitiendo a un usuario redirigir todo su tráfico a través de una red VPN sin afectar a otros usuarios.
- Soporte para las capacidades FORTIFY_SOURCE de nivel 2, y su aplicación a todo el código fuente de Android, que ha sido compilado con estas protecciones.
- Soporte para dos nuevos algoritmos criptográficos: *Elliptic Curve Digital Signature Algorithm* (ECDSA y DSA) para el almacenamiento de credenciales en los proveedores de la Keystore y la utilización de firmas digitales, y soporte para la función de derivación de claves con scrypt a la hora de proteger las claves empleadas en el cifrado completo del dispositivo móvil.
- Notificaciones de seguridad avisando al usuario cuando se añaden certificados digitales al repositorio del dispositivo móvil.
- Capacidades de protección adicionales empleando *certificate pinning* para detectar y prevenir el uso de certificados fraudulentos en comunicaciones SSL/TLS asociadas a los servicios de Google.
- Mejoras para eliminar las vulnerabilidades PileUp o Fake ID (existente desde Android 2.1).

⁷ <http://www.google.com/cloudprint/learn/index.html>

⁸ <https://play.google.com/store/apps/details?id=com.google.android.apps.cloudprint&hl=es>

- En Android 4.4 se hace uso de SELinux en modo obligatorio o *enforcing mode* parcialmente, es decir, sólo para un conjunto crítico de procesos o dominios de sistema (installd, netd, vold y zygote), en el que todas las acciones no legítimas son bloqueadas y registradas por el kernel [Ref.- 141] [Ref.- 142]. Para el resto de procesos o dominios, SELinux en Android 4.4 sigue actuando en modo permisivo, como en el caso de Android 4.3.
38. La versión 4.4.4 de Android soluciona específicamente una vulnerabilidad de seguridad asociada a OpenSSL que permitía la realización de ataques MitM (Man-in-the-Middle) tanto sobre clientes como sobre servidores, con el identificador CVE-2014-0224⁹, y que permite forzar el uso de una clave maestra débil (vacía) en ciertos escenarios de comunicación entre versiones de OpenSSL, conocida como la vulnerabilidad de “inyección CCS (ChangeCipherSpec)” [Ref.- 139] [Ref.- 140]¹⁰.
39. Posteriormente, en julio de 2014, y asociada a la API 20 (en lugar de la API 19 de la versión 4.4 de Android estándar) se anunció la versión 4.4W (o 4.4WE) de Android, con extensiones para dispositivos personales (WE, *Wearable Extensions*) [Ref.- 136].

Nota: El resumen previo de las diferentes versiones de Android no hace referencia específica a las subversiones, como por ejemplo las versiones 4.0.4, 4.3.1 o 4.4.4, salvo que se haya considerado relevante destacar alguna funcionalidad concreta de alguna subversión.

Como referencia, se han incluido referencias a los dispositivos móviles de la gama Google Nexus¹¹ asociados a cada versión principal de Android.

4.8. ANDROID 5.X

40. La versión 5.0 de Android (“Lollipop”, L) fue liberada en octubre de 2014 (tras su anuncio inicial o *preview* en junio de 2014, durante la conferencia Google I/O), con notables mejoras incluyendo el nuevo interfaz gráfico de usuario basado en *Material Design*, haciendo uso de ART (*Android RunTime*) por defecto (y sus mejoras de rendimiento asociadas), con soporte para arquitecturas y CPUs de 64 bits, mejoras en el ahorro de batería con el proyecto Volta¹², nuevas capacidades asociadas a la pantalla de desbloqueo y al centro y capacidades de notificaciones, mejoras en Bluetooth Low Energy (BLE) y NFC para realizar operaciones concurrentes en Bluetooth (escaneos y anuncios¹³) y que las apps registren su identificador de app NFC (AID) dinámicamente, estadísticas de uso de las apps, un nuevo espacio denominado “Overview” (previamente denominado “Recientes”) para la gestión de las tareas y apps en ejecución, mejoras en los gráficos (con soporte para OpenGL ES 3.1), las capacidades multimedia, el audio y la cámara (con soporte más granular para la captura de fotos y el procesamiento de imágenes), la posibilidad por parte del usuario de evitar interrupciones externas durante un periodo de tiempo definido, disponibilidad de un nuevo sensor de inclinación para detectar la actividad del usuario y un sensor del ritmo cardíaco, etc. [Ref.- 500]

⁹ <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224>

¹⁰ Esta vulnerabilidad se solucionó adicionalmente a través de los servicios de Google Play (GPS, *Google Play Services*) para otras versiones de Android previas.

¹¹ http://en.wikipedia.org/wiki/Google_Nexus y <http://www.google.es/nexus/>.

¹² Herramientas: “dumpsys batterystats” y Battery Historian (<https://github.com/google/battery-historian>).

¹³ Escaneos (modo central) y anuncios (modo periférico).

41. Las apps en Android 5.0 disponen de la capacidad (tras obtener autorización del usuario) de capturar la pantalla del dispositivo y compartirla a través de la red.
42. Android 5.x facilita el cambio del idioma, en concreto del IME (*Input Method Editor*), por parte del usuario desde el icono con forma de globo terráqueo del teclado.
43. Asimismo, Android 5.x introduce capacidades para que una app pueda acceder a los contenidos multimedia de otra app, que previamente debe haber exportado los mismos a través de un servicio (*MediaBrowserService*) [Ref.- 502].
44. El acceso a las capacidades de almacenamiento también se extiende en Android 5.x, permitiéndose la selección por parte de las apps de un directorio y de todos sus contenidos, y subdirectorios, en una sola operación, en lugar de individualmente.
45. El soporte para arquitecturas de 64 bits de Android 5.x, aun manteniendo el soporte completo de 32 bits, incluye un mayor espacio de direccionamiento, mejoras de rendimiento generales, en particular para las operaciones criptográficas de OpenSSL, junto a las capacidades asociadas del NDK (*Native Development Kit*), revisión 10c [Ref.- 503] [Ref.- 504].
46. Android 5.x tiene como objetivo ofrecer un mayor tiempo de uso mediante la optimización de la batería y un menor tiempo de carga. Se introduce una función de ahorro de energía, que puede alargar la duración de la batería restante hasta 90 minutos. Asimismo, Android 5.x permite consultar el tiempo estimado que queda para que se agote la batería y el tiempo estimado restante para que finalice la carga de la batería durante el proceso de carga.
47. En versiones previas de Android, la pantalla de “Recientes” o lista de tareas en ejecución sólo mostraba una tarea por cada app ejecutada recientemente, mientras que la nueva pantalla de visualización general de tareas en ejecución de Android 5.x permite disponer de más de una tarea por app, facilitando la multitarea y la interacción con actividades y documentos de diferentes apps de manera consistente [Ref.- 502], como por ejemplo, mostrando distintas tareas para las diferentes pestañas abiertas del navegador web.
48. En Android 5.0 se hace uso de SELinux en modo obligatorio o *enforcing mode* globalmente o completo (*full enforcement*), es decir, tanto para el conjunto crítico de procesos de sistema (ya protegidos en Android 4.4), como para el resto de procesos (con más de 60 dominios) [Ref.- 141][Ref.- 142].
49. Los primeros dispositivos móviles basados en Android 5.x fueron el *smartphone* Nexus 6, con una pantalla de 6” (desarrollado por Google y Motorola) y la *tablet* Nexus 9 (desarrollada por Google y HTC), comercializados en octubre/noviembre de 2014, junto al Nexus Player. Posteriormente, en noviembre de 2014 la actualización de Android 5.x (Lollipop) se extendió a otros dispositivos móviles de Google, como el Nexus 4, 5, 7 y 10, y a dispositivos móviles de otros fabricantes.
50. Posteriormente, en diciembre de 2014 se liberaron las versiones 5.0.1 y 5.0.2 de Android, con mejoras de funcionalidad y errores. Asimismo, en marzo de 2015 se liberó la versión 5.1, que permitía conectarse a redes Wi-Fi y/o emparejarse con otros dispositivos Bluetooth directamente desde los ajustes de configuración rápidos de Android, incluía soporte oficial para múltiples tarjetas SIM [Ref.- 509] y capacidades para aprovisionar los ajustes de los operadores móviles de telecomunicaciones. La versión 5.1 habilitaba por defecto “Factory Reset Protection”, un mecanismo de seguridad para evitar que un dispositivo móvil Android que haya sido robado pueda ser

reutilizado, ya que para su activación, incluso tras restaurar el mismo a los ajustes por defecto de fábrica, es necesario disponer de las credenciales del usuario de Google de su último propietario. La versión 5.1.1 liberada en abril de 2015 ofrecía de nuevo corrección de errores.

51. En concreto, Android 5.1 añade soporte para hacer uso de múltiples tarjetas SIM simultáneamente (en aquellos dispositivos móviles que disponen de varias ranuras), elimina el soporte para componentes antiguos del SDK empleados en las comunicaciones HTTP, dando prioridad a URLConnection, y proporciona soporte para que los proveedores de telecomunicaciones puedan desarrollar apps que puedan modificar los ajustes de configuración del operador móvil y llevar a cabo otras tareas de aprovisionamiento. Este tipo de apps deben de estar firmadas por un certificado de desarrollador que coincida con el certificado UICC (Universal Integrated Circuit Card) del dispositivo móvil [Ref.- 511].
52. Una mejora sustancial de la versión 5.1 fue la resolución del “*memory leak*” que introdujo Android 5.0 y que provocaba que la memoria del dispositivo se llenara, causando fallos en las aplicaciones que ejecutan en segundo plano y en la propia pantalla de inicio. Aunque no afectó a todos los terminales, sí fue un problema muy extendido, especialmente entre aquellos dispositivos con memoria RAM inferior a 2 GB [Ref.- 510].
53. Android 5.1 deja de intentar conectarse automáticamente a aquellas redes Wi-Fi que no proporcionan acceso a Internet. Si una red Wi-Fi que había sido guardada en el dispositivo móvil deja de proporcionar acceso a Internet, aparecerá un mensaje justo debajo del nombre de la red Wi-Fi informando de esa circunstancia.

4.9. ANDROID 6.X

54. La versión 6.x de Android (“Marshmallow”, M) fue liberada en octubre de 2015 (tras su anuncio inicial o *preview* en mayo de 2015, durante la conferencia Google I/O), con soporte para los dispositivos móviles Nexus 5, 6, 7 (sólo para la versión de 2013) y 9. Esta versión incluía mejoras adicionales para el ahorro de batería a través del proyecto Doze, capacidades “Direct Share” para la compartición de datos directamente entre apps¹⁴, optimizaciones de contenido para el “Asistente”¹⁵, soporte para los nuevos conectores USB de tipo C (con capacidad de carga ultrarrápida), capacidades automáticas para la realización de copias de seguridad (o backups) automáticas de los datos de las apps (y su recuperación; ver apartado “21.4. Copia de seguridad automática de los datos de las apps”), *verified boot* (ver apartado “7.8. Proceso de arranque seguro: Verified Boot”), compatibilidad con dispositivos MIDI, la introducción del concepto de dispositivos de almacenamiento flexibles o adoptables [Ref.- 603] (ver apartado “10.3. Dispositivos de almacenamiento”), capacidades que facilitan la transferencia de datos, cuentas y apps durante el proceso de migración a un nuevo dispositivo móvil, funcionalidad para añadir una cuenta de e-mail adicional (personal o corporativa) durante el proceso de instalación y configuración inicial, soporte para el estándar Wi-Fi Hotspot 2.0¹⁶ y para la creación de zonas Wi-Fi en las bandas de frecuencia de 5 GHz,

¹⁴ <https://developer.android.com/about/versions/marshmallow/android-6.0.html#direct-share> [Ref.- 603]

¹⁵ <https://developer.android.com/training/articles/assistant.html>

¹⁶ Soporte para la especificación Hotspot 2.0 Release 1 en dispositivos Nexus 6 y Nexus 9 [Ref.- 603].

soporte para el perfil SAP (*SIM Access Profile*) de Bluetooth que permite hacer llamadas de teléfono desde un vehículo empleando la tarjeta SIM del dispositivo móvil, numerosas nuevas capacidades en Android for Work (ver apartado “8.2. Android for Work”), etc.

55. Android 6.x introduce de forma oficial el “Administrador de permisos”, una funcionalidad que permite al usuario gestionar a nivel de aplicación los permisos de calendario, contactos, cámara, micrófono, SMS, sensores, teléfono y ubicación (ver apartado “7.1. Modelo de permisos de Android”).
56. Android 6.x introduce la función “Now on tap”, cuyo propósito es proporcionar al usuario información contextualizada sobre lo que muestra la aplicación que se encuentra en primer plano cuando se invoca “Now on tap” (ver apartado “22. App Google: Asistente de Google, Mi Tablón y Servicios de Búsqueda de Google”).
57. En relación con el punto anterior, Android 6.x proporciona una integración más directa con el servicio denominado *feed* (cuyo precursor es Google Now), de forma que, manteniendo pulsado el botón de inicio, ofrece más capacidades a la hora de interactuar con el dispositivo móvil y sus servicios asociados a través de la voz [Ref.- 600].
58. En concreto, Android 6.x facilita a las aplicaciones móviles nuevas capacidades para interactuar y llevar a cabo acciones por parte del usuario mediante la voz [Ref.- 603], así como facilitar la interacción con las apps a través del Asistente de Google, pudiendo éste disponer del contexto asociado a cada app. El “Asistente” es activado mediante una pulsación prolongada del botón de inicio (o *Home*).
59. Android 6.x introdujo soporte oficial para los sensores de huellas dactilares digitales (*fingerprint*), junto a las capacidades para hacer uso de estos durante el proceso de autenticación del usuario (o desbloqueo del dispositivo móvil) y su integración para la realización de pagos dentro de las aplicaciones móviles (ver apartado “9.3. Huella dactilar digital (*fingerprint*)”).
60. Android 6.x añade soporte completo para memorias microSD y USB, de forma que es posible conectar mediante USB (haciendo uso de un cable USB OTG, *On-The-Go*) un dispositivo de almacenamiento externo para acceder y ver archivos multimedia o para usarlo como medio de almacenamiento externo (ver apartado “10.2. Almacenamiento adoptable”).
61. Android 6.x introduce un nuevo control de audio, de forma que, al pulsar sobre el botón de volumen, se desplegará un control de sonido que permite regular los controles de volumen del tono, multimedia y de las alarmas, incluso con el dispositivo bloqueado.
62. Android 6.x introduce el denominado “Configurador de IU (interfaz de usuario) del sistema”, una opción experimental que habilita determinadas funcionalidades para personalizar el dispositivo móvil desde el centro de control, disponible en la parte superior, desde los ajustes de configuración rápidos (ver apartado “9.10. Configurador de IU del sistema”).
63. Por otro lado, las optimizaciones de la batería incluyen la función de “Aplicaciones en Espera” (o apps inactivas, limitando el consumo por parte de apps que apenas se utilizan) y un modo “Descanso” (estado suspendido) para que el consumo sea mínimo cuando no se hace uso del dispositivo móvil y que, por ejemplo, pueda permanecer toda la noche encendido para hacer sonar una alarma a la mañana siguiente.

64. El modo “No molestar” (ver apartados “9.7. Interrupciones” y “9.8. Notificaciones”) puede ser gestionado fácilmente desde los ajustes de configuración rápidos, y configurado para que una llamada de un mismo remitente en un periodo de 15 minutos suene de manera estándar. Este modo puede ser activado automáticamente para ciertos periodos de tiempo o para ciertos eventos del calendario.
65. La funcionalidad de realización de copias de seguridad (backups), y restauración, de Android 6.x incluye nuevos ajustes de configuración del sistema, como por ejemplo los ajustes de sincronización, las apps preferidas, la configuración del modo “No molestar”, los ajustes de accesibilidad y los métodos de introducción de texto previamente habilitados.
66. Los nuevos ajustes simplificados, disponibles desde “Ajustes - [Dispositivo] Aplicaciones”, permiten gestionar todas las características y configuraciones de las apps desde una misma ubicación, incluyendo el consumo de batería o memoria, sus permisos y/o notificaciones.
67. En Android 6.x, se cambió de nuevo el comportamiento de la pantalla de “Recientes” para el navegador web nativo (Chrome), de forma que, en lugar de mostrarse cada página web abierta en el navegador de forma independiente (como una tarea separada), sólo se muestra una única tarea, siendo necesario abrir la app del navegador web y pulsar sobre el icono que representa el número de pestañas abiertas para acceder a la lista completa de las mismas.
68. Android 6.x introdujo el mecanismo “Direct Share”, a través del cual una aplicación móvil puede exponer parte de su información y datos a otras aplicaciones para que éstas la utilicen (ver apartado “7.3. Direct Share”).
69. Android 6.x introdujo el denominado “Doze”, un sistema de ahorro de batería similar al modo hibernación de los ordenadores personales (ver apartado “9.9. Ahorro de batería”).
70. Android 6.x elimina el soporte para el cliente HTTP de Apache, promoviendo el uso de `URLConnection` en su lugar para apps con un nivel de API igual o superior a 9 (Android 2.3). Esta clase hace un uso más eficiente de las conexiones HTTP(S) a través de mecanismos de compresión, transparentes para el usuario, y de caché [Ref.- 602].
71. Android está dejando a un lado el uso de OpenSSL como librería criptográfica, y haciendo uso en su lugar de BoringSSL [Ref.- 605]. En el caso de hacer uso del NDK, no se deben referenciar directamente librerías que no pertenezcan a la API del NDK, como por ejemplo “`libcrypto.so`” y “`libssl.so`” (librerías no públicas que pueden cambiar sin previo aviso), y en su lugar, se debería hacer uso de las APIs criptográficas de Java a través de JNI, *Java Native Interface* [Ref.- 602].
72. Android 6.x bloquea el acceso directo a los identificadores hardware del dispositivo móvil, como, por ejemplo, las direcciones MAC asociadas a las APIs de Wi-Fi y Bluetooth [Ref.- 602].
73. Por otro lado, en Android 6.x o superior, para que una app pueda acceder a las direcciones MAC de otros dispositivos externos cercanos a través de escaneos Bluetooth y Wi-Fi, debe solicitar los permisos `ACCESS_FINE_LOCATION` o `ACCESS_COARSE_LOCATION` [Ref.- 602].

74. Los escaneos en background o de fondo (Wi-Fi y Bluetooth) se llevan a cabo empleando una dirección MAC origen aleatoria, por lo que los dispositivos externos no pueden identificar de manera directa la dirección MAC real del dispositivo móvil hasta que establezcan una conexión con él.
75. En Android 6.x las apps no disponen de acceso global a la lista de webs favoritas (o *bookmarks*) del usuario, habiéndose eliminado los permisos existentes previamente para este acceso, `READ_HISTORY_BOOKMARKS` y `WRITE_HISTORY_BOOKMARKS`. En su lugar, las apps con un nivel de API objetivo igual o superior a 23 deben de gestionar internamente su propia lista de web favoritas [Ref.- 602].
76. La implementación de Keystore de Android 6.x no soporta DSA, debiéndose emplear ECDSA (Elliptic Curve DSA) en su lugar [Ref.- 602].
77. Las claves que no requieren ser almacenadas en formato cifrado, no serán eliminadas cuando se deshabilita el uso de un código de acceso en la pantalla de desbloqueo, por parte del usuario o de una app administradora del dispositivo. Las que sí solicitan su almacenamiento cifrado sí serán eliminadas en ese escenario.
78. El entorno de ejecución de Android 6.x no permite a las apps realizar la carga de librerías dinámicas o compartidas con capacidad de reubicar sus secciones de texto (*text relocations*) [Ref.- 602], con el objetivo de disponer de código independiente de su posición en memoria (PIC, *Position Independent Code* o PIE, *Position Independent Executable*) y poder así hacer uso de ASLR. En versiones previas de Android, al llamar a la función “`dlopen()`” con este tipo de librerías se generaba un aviso, pero sí se permitía la carga de la librería.
79. En Android 6.x se lleva a cabo una verificación más estricta de los ficheros APK a la hora de instalar una app, considerándose que el fichero APK está corrupto si un fichero declarado en el fichero *manifest* no está presente dentro del fichero APK. Por tanto, en caso de que cualquier contenido sea eliminado del fichero APK, será necesario firmar de nuevo dicho fichero [Ref.- 602].
80. Android 6.x proporciona nuevos modos de conexión a través del puerto USB del dispositivo móvil, obligando a que la transferencia de datos por USB sea iniciada a través de la notificación que se muestra cuando se conecta otro dispositivo y no desde el menú de “Ajustes [Dispositivo] - Almacenamiento & USB - [...] - Conexión USB a ordenador”, tal como ocurría en versiones previas de Android (ver apartado “13. Comunicaciones USB”).
81. Los primeros dispositivos móviles basados en Android 6.x fueron los *smartphones* Nexus 5X y 6P (desarrollados por Google junto a LG y Huawei, respectivamente), y comercializados en octubre de 2015, ambos con sensor de huella dactilar digital en su parte posterior y con el nuevo conector USB de tipo C.
82. Desde el punto de vista de seguridad, cabe destacar, tal y como se ha mencionado anteriormente, la introducción en Android 6.x de un *framework* o entorno (estándar en dispositivos móviles compatibles y con un lector de huella o *fingerprint*) para llevar a cabo la autenticación mediante huella dactilar digital, que, no sólo permite el desbloqueo del dispositivo móvil (ver apartado “9.3. Huella dactilar digital (*fingerprint*)”), sino también la autenticación desde las apps mediante huella (o incluso con otras credenciales de la plataforma móvil mediante la API `Confirm Credential`), y la realización

de compras mediante Android Pay y de compras en Google Play, junto al inicio de sesión en esta última plataforma.

83. Por otro lado, también desde el punto de vista de seguridad es necesario destacar que Android 6.x introdujo un nuevo modelo de permisos en tiempo de ejecución para las apps, donde ya no es necesario que el usuario otorgue a la app todos los permisos solicitados en el momento de su instalación, sino que estos pueden ser otorgados posteriormente y de manera granular y selectiva (ver apartado “7.1.2. Modelo de Permisos en tiempo de ejecución”). Asimismo, Android 6.x proporciona controles para gestionar (activar y desactivar) individualmente los permisos de cada app, o de las apps que tienen acceso a un grupo concreto de permisos.
84. En diciembre de 2015 se liberó la versión 6.0.1 de Android, con pequeñas mejoras de funcionalidad [Ref.- 86].

4.10. DIFERENCIAS ENTRE LAS MÚLTIPLES VERSIONES DE ANDROID

85. Las principales diferencias y novedades para los usuarios de cada una de las versiones de Android están disponibles en la página web oficial de Android, incluyendo la información histórica para las diferentes versiones [Ref.- 202]: 2.2, 2.3, 3.0, 4.0 (Ice Cream Sandwich, ICS), 4.1, 4.2 y 4.3 (Jelly Bean, JB), 4.4 (KitKat, KK), 5.0 (Lollipop, L), 6.0 (Marshmallow, M) y 7.0 (Nougat, N). En la misma destacan las novedades de las versiones más recientes:
- 4.3 (Jelly Bean): <https://www.android.com/versions/jelly-bean-4-3/>
 - 4.4 (KitKat): <https://www.android.com/versions/kit-kat-4-4/> [Ref.- 148]
 - 5.0 (Lollipop): <https://www.android.com/versions/lollipop-5-0/> [Ref.- 500]
 - 6.0 (Marshmallow): <https://www.android.com/versions/marshmallow-6-0/> [Ref.- 600]
86. Las principales diferencias y novedades técnicas de cada una de las versiones de la plataforma Android están disponibles en la página web para desarrolladores de Android (Developers) [Ref.- 86]. La documentación para las versiones más recientes, con subapartados para las subversiones principales (como por ejemplo Android 5.1), junto a los detalles para los desarrolladores de las APIs o librerías de programación, los cambios más relevantes, y ejemplos de código, están disponibles en:
- 4.4 (KitKat): [Ref.- 86]
 - <https://developer.android.com/about/versions/kitkat.html>
 - 5.0 (Lollipop): [Ref.- 501]
 - <https://developer.android.com/about/versions/lollipop.html>
 - 6.0 (Marshmallow): [Ref.- 601]
 - <https://developer.android.com/about/versions/marshmallow/index.html>

87. Las principales características de seguridad y mecanismos de protección existentes en Android, especialmente para las últimas versiones, están disponibles en la página oficial de seguridad de Android para los usuarios finales [Ref.- 132], y en la página oficial de seguridad de Android para usuarios técnicos [Ref.- 133]. Asimismo, las mejoras de seguridad introducidas por cada una de las versiones de Android están resumidas en la página oficial de mejoras de seguridad de Android, también clasificadas por versiones [Ref.- 140].
88. Por otro lado, las principales características y mejores prácticas asociadas a la privacidad y seguridad de la plataforma Android están disponibles para los desarrolladores de apps en una página web dedicada [Ref.- 57], entre las que se encuentran el uso de HTTPS y TLS, el uso de configuraciones de seguridad de red, la actualización del proveedor de seguridad para evitar la explotación de vulnerabilidades de SSL/TLS, la integración con SafetyNet, la comprobación de URLs mediante la API de navegación segura (*Safe Browsing*), la gestión de claves mediante una Keystore hardware, la mejora de la seguridad mediante el uso de políticas de gestión de los dispositivos móviles, o soporte para arranque directo, entre otros (todas ellas descritas en los apartados correspondientes de la presente guía).
89. En resumen, los recursos de Android oficiales principales se engloban en:
- Las características de Android para usuarios finales [Ref.- 203]:
 - 4.4 ([Ref.- 148]), 5.x ([Ref.- 500]) y 6.x ([Ref.- 600]).
 - Las características de seguridad de Android para usuarios finales [Ref.- 132].
 - Las características de seguridad de Android para usuarios técnicos [Ref.- 133].
 - Las mejoras de seguridad de Android para cada una de las versiones [Ref.- 140].
 - Las características técnicas de Android para desarrolladores para cada una de las versiones [Ref.- 86].
 - Las mejores prácticas de privacidad y seguridad de Android para desarrolladores [Ref.- 57].

5. ENTORNO DE APLICACIÓN DE ESTA GUÍA

90. Los contenidos de esta guía aplican a dispositivos móviles basados en Android en castellano: “Español (España)”. El idioma puede ser seleccionado desde el menú “Ajustes [Personal] - Idioma e introducción de texto - Idioma”.

Nota: El menú “Ajustes” empleado y referenciado en numerosas tareas de configuración del dispositivo móvil Android está disponible desde el menú de ajustes de configuración rápidos, o ajustes rápidos por abreviar (situado en la barra superior de estado) del dispositivo móvil, o desde el icono del *Launcher* (icono con una matriz de puntos situado en la parte inferior central de la pantalla principal o *Home* de Android).

91. La guía ha sido probada y verificada con la versión 5.1.1 del sistema operativo Android.

92. La guía ha sido probada y verificada con la versión 6.0.1 del sistema operativo Android, si bien algunos apartados pueden corresponder con la versión 6.0, especialmente los relacionados con la actualización del sistema operativo o la instalación inicial del dispositivo móvil.

Nota: La información general del dispositivo móvil está disponible bajo la opción “Ajustes [Sistema] - Información del teléfono”, y en concreto, la información de la versión del sistema operativo se encuentra bajo la sección “Versión de Android”.

Nota: La información general del dispositivo móvil está disponible bajo la opción “Ajustes [Sistema] - Acerca del dispositivo”, y en concreto, la información de la versión del sistema operativo se encuentra bajo la sección “Versión de Android”. Es importante reseñar que, en la versión 6.0 de Android, el menú “Ajustes” recibió la denominación “Configuración”.

93. Las operaciones que requieren del uso de un ordenador han sido llevadas a cabo mediante Windows 10 Home Premium 64-bits en inglés.

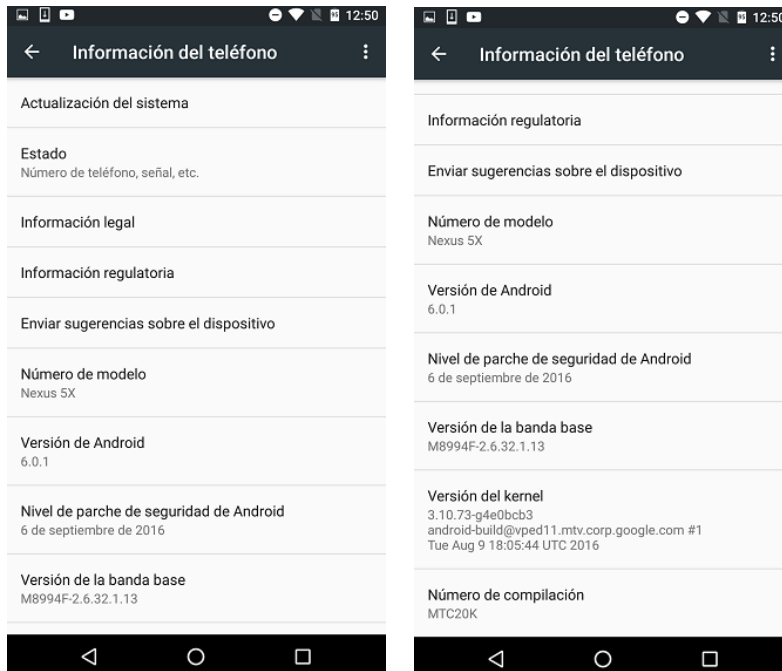
Nota: Para la elaboración de la presente guía se ha empleado una versión de Windows en inglés en el ordenador utilizado para la conexión y sincronización con el dispositivo móvil, con el objetivo de ejemplificar la compatibilidad de idiomas entre el terminal y el ordenador. La simplicidad de las funciones realizadas a través del ordenador, pese a utilizarse otro idioma, no debería dificultar la comprensión de la presente guía.

Nota: La presente guía emplea el término “ordenador” para referenciar al equipo portátil o de sobremesa (o escritorio) empleado para la sincronización, gestión y tareas de administración, depuración y desarrollo sobre el dispositivo móvil.

94. El hardware sobre el que se ha verificado la presente guía tiene las siguientes características:

- Dispositivo móvil Google Nexus 5X (fabricado por LG, modelo LG-H791) [Ref.- 3]:
 - Versión de Android: 6.0.1. Es importante reseñar que el dispositivo móvil dispone de fábrica de la versión Android 6.0 precargada, por lo que algunos aspectos de configuración tras la instalación inicial (incluida la actualización a la versión 6.0.1) pueden estar basados en la versión 6.0.
 - Versión de banda base: (ver imagen inferior): M8994F-2.6.32.1.13
 - Versión de kernel: (ver imagen inferior): 3.10.73-g4e0bcb3 ... Agosto ... 2016
 - Número de compilación: MTC20K

Nota: El dispositivo móvil empleado es un terminal libre, es decir, no asociado a ningún operador de telefonía móvil, con el objetivo de analizar las características y valores por defecto de Android sin verse afectadas por las posibles modificaciones y personalizaciones llevadas a cabo por los operadores de telefonía.



Nota: La guía ha sido diseñada (y aplicada) para dispositivos móviles estándar basados en Android en los que no se ha llevado a cabo el proceso de *rooting* o root. Este proceso permite al usuario disponer de control completo del dispositivo móvil y acceder al mismo como root, superusuario, o usuario privilegiado, y en concreto, al subsistema Linux subyacente en Android, eliminando así los controles y/o restricciones establecidos por la plataforma Android estándar, los fabricantes y/o los operadores de telefonía móvil asociados al dispositivo móvil.

Las apps disponibles para los dispositivos móviles Android, por defecto, no disponen de permisos de escritura en ciertas zonas del sistema de ficheros, no pudiendo reemplazar el sistema operativo, ni de privilegios para hacer uso de capacidades específicas, como reiniciar el dispositivo móvil, modificar el uso de los LEDs hardware, capturar la pantalla del dispositivo móvil o eliminar aplicaciones móviles instaladas por algunos operadores de telefonía móvil. El proceso de *rooting* es utilizado por usuarios avanzados para acceder a estas funcionalidades de bajo nivel.

Los dispositivos móviles Android *rooteados* (o *rooted*) ignoran el modelo de seguridad descrito a lo largo de la presente guía, ya que todas las aplicaciones que sean instaladas podrán disponer de los máximos privilegios en el dispositivo (root), exponiendo potencialmente a los usuarios a código dañino que podría tomar control completo del terminal. Android no requiere llevar a cabo el proceso de *rooting* para permitir la instalación de apps de terceros no oficiales, es decir, no distribuidas a través de Google Play, tal como sucede en otras plataformas de dispositivos móviles, como iOS, donde es necesario realizar el proceso de *jailbreak* (equivalente a *rooting*) para poder instalar ese tipo de apps no oficiales.

Las particularidades del proceso de actualización en Android (ver apartado “6. Actualización del sistema operativo Android”), con largos periodos de tiempo hasta que una nueva actualización está disponible para algunos usuarios, es uno de los motivos que incentiva a los usuarios a realizar el proceso de *rooting* para así poder instalar la última versión de Android en su dispositivo móvil empleando otros proyectos como LineageOS (CyanogenMod).

Nota: Debe tenerse en cuenta que se pueden presentar diferencias en la apariencia de las capturas de pantalla utilizadas a lo largo de la presente guía y la pantalla de otros dispositivos móviles basados en la misma versión de Android, debido al modelo, fabricante o versión concreta del SO.

Asimismo, algunas de las funcionalidades disponibles en Android pudieran ser propias de un fabricante de dispositivos móviles determinado, por lo que las recomendaciones de seguridad asociadas no aplicarían a otros dispositivos móviles basados en Android. Se recomienda llevar a cabo un análisis de seguridad similar al mostrado para estas funcionalidades adicionales añadidas por los fabricantes con el objetivo de determinar las recomendaciones a aplicar en dispositivos móviles de otros fabricantes y en sus aplicaciones propietarias.

95. La versión 6.0.1 de Android para el dispositivo móvil empleado para la elaboración de la presente guía (Nexus 5X) estuvo disponible como actualización parcial OTA (Over-the-Air) partiendo de la versión 6.0 de Android, y complementariamente a la imagen de fábrica completa de esta versión de sistema operativo¹⁷, desde diciembre de 2015 (ver apartado “6. Actualización del sistema operativo Android”).
96. Se recomienda siempre recabar e inventariar la información de versiones, tanto hardware como software, de los dispositivos móviles a proteger, con el objetivo de disponer de toda la información necesaria a la hora de tomar decisiones relativas a la aplicación de nuevas actualizaciones y medidas de seguridad.
97. Debe prestarse atención al contrato de telefonía, y en concreto de datos móviles, asociado a la tarjeta SIM (*Subscriber Identity Module*) empleada en el dispositivo móvil Android. La ausencia de capacidades de comunicación de datos es notificada al usuario en función de las apps que requieren disponer de las mismas.
98. Igualmente, debe prestarse especial atención al tipo de dispositivo móvil (marca y modelo) al que se desea aplicar la guía, ya que la relación de los elementos descritos o referenciados en ella (interfaz de usuario, capacidades hardware, aplicaciones, etc.) puede diferir ligeramente en función de la personalización del sistema operativo realizada por el fabricante del terminal (u operador de telefonía móvil).
99. Antes de aplicar esta guía en un entorno de producción debe confirmarse su adecuación a la organización objetivo, siendo probada previamente en un entorno aislado y controlado donde se puedan realizar las pruebas necesarias y aplicar cambios en la configuración para que los mismos se ajusten a los criterios y requisitos específicos de cada organización.

Nota: El alcance de la presente guía no contempla la realización de un análisis de seguridad detallado de los protocolos de comunicaciones basados en HTTPS (o SSL/TLS) y empleados por los dispositivos móviles Android, las aplicaciones móviles disponibles por defecto (o de terceros) y los diferentes servicios de Google (o de terceros).

¹⁷ <https://developers.google.com/android/nexus/images>

6. ACTUALIZACIÓN DEL SISTEMA OPERATIVO ANDROID

6.1. ACTUALIZACIÓN AUTOMÁTICA DEL SISTEMA OPERATIVO ANDROID

100. Los dispositivos móviles Android, una vez disponen de conectividad de datos hacia Internet a través de las redes de telefonía móvil (2/3/4G) o de redes Wi-Fi, pueden verificar automáticamente si existe una nueva versión o actualización del sistema operativo.
101. Para ello, se establecen conexiones tanto cifradas mediante HTTPS (TCP/443) con los servidores “http[s]://android.clients.google.com” y “https://www.googleapis.com”.
102. Para realizar las comprobaciones de versión llevadas a cabo por Android se utiliza una petición al recurso “/checkin”, de tipo POST, que emplea como parámetros datos en formato ProtoBuffer (“application/x-protobuf”; comprimidos mediante GZIP¹⁸), es decir, empleando el formato binario de intercambio de datos utilizado por muchos servicios de Google y conocido como Google Protocol Buffers¹⁹. Como respuesta, los servidores de Google envían también datos en formato ProtoBuffer, entre los que se incluye la versión más reciente de Android que se puede descargar a partir de la versión actual del terminal.
103. En el caso de Android 6.0, la versión que se ofrece como actualización OTA para el Nexus 5X a fecha de redacción de la presente guía es la 7.1.1, por lo que, si se desea actualizar a la última versión de Android 6.x (la versión 6.0.1 en el momento de elaboración de la presente guía), será necesario descargar la imagen completa correspondiente de la web oficial de Google y realizar una actualización manual (ver apartado “6.3. Actualización manual completa de Android”). Es de reseñar que, aunque la versión 7.1.2 está disponible en el momento de elaboración de la presente guía, la actualización OTA no lleva a ella de forma directa.
104. Dado que la presente guía tiene por objeto analizar la versión 6.x del sistema operativo Android, la actualización automática a la versión 7.1.1 de Android no se contempla.
105. La notificación de disponibilidad y descarga de la actualización automática permite al usuario posponer la descarga (mediante la opción “Más tarde”) o proceder a realizarla (mediante la opción “Descargar”). Si se selecciona la opción “Descargar”, se muestra una pantalla de confirmación que describe el contenido de la actualización y su tamaño, y que, de nuevo, requiere pulsar en la opción “Descargar” para que se inicie el proceso de descarga. No obstante, dado que la versión 7.x de Android queda fuera del alcance de la presente guía, no se documentarán las acciones posteriores asociadas a Android 7.x.
106. El agente de usuario (User-Agent) empleado para la comunicación HTTP/HTTPS en Android 6.0 es:

```
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0; Nexus 5X Build/MDB08L)
```

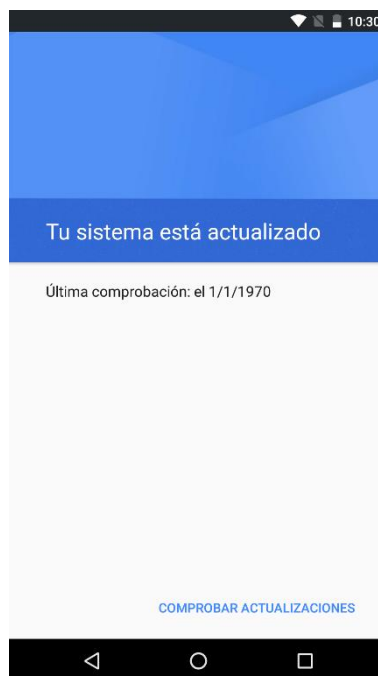
107. Como respuesta a la petición de comprobación de actualizaciones, el servidor “android.clients.google.com” envía otro ProtoBuffer proporcionando multitud de

¹⁸ Dependiendo de la versión de las apps Google Services Framework (GSF) y Google Play Services (GPS).

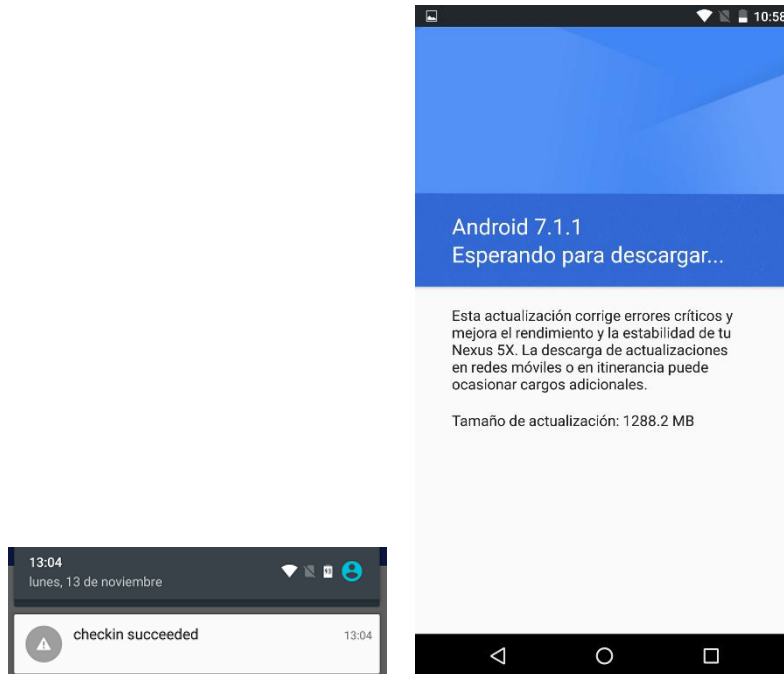
¹⁹ <https://github.com/google/protobuf/>

parámetros, incluida la versión a la que se actualizará “update_title Android 7.1.1” (recordar que no se ofrece la actualización de Android 6.0.1 vía OTA) y un “update_token” que el dispositivo utilizará en el momento de la descarga a través de la cabecera “Authorization”.

108. La descarga efectiva del fichero se realiza mediante una petición HTTPS al servidor “android.googleapis.com”, usando el método GET al recurso “/packages/ota/google_bullhead_bullhead/<valor SHA1 del fichero ZIP de la actualización>.zip”, y en el que se pasa en la cabecera “Authorization” el token recibido como respuesta al recurso “/checkin” previo. Por ejemplo, para la versión 6.0.0 de Android, el valor SHA1 del fichero ZIP de actualización a Android 7.1.1, es 787c9918530955c104f7e093b90de60c20edc565, por lo que el recurso concreto que se solicita es (“bullhead” corresponde al dispositivo móvil Nexus 5X) “/packages/ota/google_bullhead_bullhead/787c9918530955c104f7e093b90de60c20edc56” y que a su vez lleva asociada la descarga del fichero “https://ota.googlezip.net/packages/ota/google_bullhead_bullhead/787c9918530955c104f7e093b90de60c20edc565.zip”.
109. Esta opción es empleada frecuentemente para la distribución de actualizaciones de Android basada en mensajes OTA (Over-The-Air), y complementa la opción por parte del usuario de descargar manualmente el fichero correspondiente a la actualización completa directamente de los servidores oficiales de Google (analizada en el apartado “6.3. Actualización manual completa de Android”).
110. Es posible llevar a cabo esta operación de verificación de disponibilidad de actualizaciones en cualquier momento a través del menú “Ajustes - Información del teléfono - Actualizaciones del sistema - Comprobar actualizaciones”.



- 111.Sin embargo, sigue vigente la utilización del código USSD “*##*checkin#*##*” (o “*##*2432546#*##*”) desde el teclado del teléfono en Android para forzar una búsqueda inmediata de actualizaciones y parches. Cuando se emplea esta opción, se mostrará una notificación que indica si fue posible (*checkin succeeded*) realizar la comprobación de actualizaciones.



- 112.La integridad de las actualizaciones de las nuevas versiones de Android se verifica a través de una firma digital asociada al fichero de actualización (.zip) descargado, en concreto, mediante los certificados digitales (x.509) de sistema disponibles por defecto en “/system/etc/security/otacerts.zip”²⁰ (si no se especifica un conjunto de certificados distinto), que identifican quién puede distribuir y firmar actualizaciones OTA [Ref.- 44] [Ref.- 159].
- 113.La ausencia de cifrado al hacer uso de HTTP podría permitir la manipulación de este intercambio de datos, por ejemplo, mediante la sustitución del fichero ZIP asociado a la actualización OTA por otro fichero asociado a otra versión, también correspondiente a una actualización válida firmada digitalmente.
- 114.Por otro lado, la utilización de un canal no cifrado HTTP permite a un atacante conocer la versión y compilación actual (y potencialmente futura) del dispositivo móvil víctima, pudiendo explotar vulnerabilidades conocidas sobre dichas versiones.
- 115.El fichero con la actualización OTA es almacenado en la partición “/cache” (partición únicamente accesible como root o superusuario), en concreto, en un fichero “.zip” cuyo nombre contiene el valor SHA1 del fichero ZIP de la actualización.
- 116.En base a la documentación y referencias oficiales (incluido el propio mensaje de anuncio inicial), las notificaciones y actualizaciones de seguridad de Android deberían estar disponibles en el grupo o lista de distribución “Android Security Announcements”, creada en 2008. Sin embargo, esta lista únicamente contiene una entrada sobre el anuncio inicial del equipo de seguridad de Android de agosto de 2008 [Ref.- 66].

²⁰ <http://developer.android.com/reference/android/os/RecoverySystem.html>

- 117.Sin embargo, sí permanece activa la lista mencionada en el anuncio inicial (y descrita posteriormente), “Android Security Discussions” [Ref.- 67], no así la lista de preguntas frecuentes de seguridad de Android [Ref.- 68], reemplazada por las mejores prácticas de seguridad.
- 118.Google publica mensualmente a través del grupo “Android Security Updates” [Ref.- 69] el boletín de seguridad correspondiente a las actualizaciones del nivel de parche de seguridad. El proceso de actualizaciones mensuales lleva asociado una imagen OTA que contiene los parches de seguridad de ese mes para cada versión de Android bajo soporte.
- 119.Desafortunadamente no se dispone de un repositorio oficial de notificaciones con el listado de vulnerabilidades que han afectado a Android, y/o que han sido solucionadas, y en consecuencia, no existe un listado de actualizaciones disponibles para resolver esas vulnerabilidades (con la excepción descrita posteriormente para los dispositivos móviles Google Nexus y/o Pixel desde agosto del año 2015).
- 120.Existe otro grupo o lista de distribución para la discusión de temas relacionados con seguridad en Android, denominado “Android Security Discussions” [Ref.- 67]. La problemática actual respecto al modelo de actualizaciones de seguridad de Android (reflejado posteriormente) ha sido analizada y discutida en numerosas ocasiones en dicho grupo.
- 121.Desde un punto de vista no oficial, existe un proyecto de la comunidad, denominado “Android Vulnerabilities” [Ref.- 64] que actúa como repositorio de las diferentes vulnerabilidades de seguridad que han afectado a las múltiples versiones de Android (al menos hasta que Google decidió oficialmente publicar los boletines de seguridad mensuales). El proyecto recibió contribuciones de la comunidad sobre nuevas vulnerabilidades, y permitía clasificarlas por fabricante, año, versión de Android y contribuyente.
- 122.Oficialmente, las actualizaciones de Android, al tratarse de un sistema operativo de código abierto basado en Linux y con modificaciones particulares según los modelos de terminal, deben ser proporcionadas por los diferentes fabricantes de los dispositivos móviles [Ref.- 68] u operadores de telefonía móvil, en base a las modificaciones y ajustes realizados sobre las actualizaciones proporcionadas por el proyecto Android. Google, como líder del proyecto Android, no proporciona directamente actualizaciones para los dispositivos móviles Android (salvo para sus propios modelos de la familia Google Nexus y/o Pixel). Concretamente, empleando como ejemplo el fabricante del dispositivo móvil empleado en esta guía, LG dispone de una página web referente a boletines de seguridad para otros modelos de dispositivos móviles [Ref.- 70].

Nota: Debido a que el dispositivo móvil Android empleado para la elaboración de la presente guía es distribuido por Google directamente (actuando como fabricante del mismo, aunque en realidad pueda ser fabricado por otra compañía con la que Google ha llegado a un acuerdo para cada modelo concreto), los procesos de actualización descritos en este documento afectan únicamente a los dispositivos móviles comercializados por Google, dentro de la familia Google Nexus [Ref.- 75], también conocidos como *Google Experience Devices* [Ref.- 72] o *Pure Android, 100% Google*. Los dispositivos Google Nexus están (o han estado) disponibles desde Google Play directamente (también referidos en el pasado como *Google Play Devices* [Ref.- 71]).

Adicionalmente, existieron en el mercado dispositivos móviles conocidos como *Google Play Edition Devices*, es decir, comercializados por Google desde Google Play [Ref.- 71] pero creados por otros fabricantes, fuera de la familia Google Nexus. Estos dispositivos móviles también utilizan una versión no personalizada de Android, y por tanto, las actualizaciones para los mismos eran parejas en el tiempo a las proporcionadas por Google para la familia Google Nexus. Ejemplos de dispositivos móviles de este tipo han sido las ediciones especiales para Google Play del Samsung Galaxy S4, del HTC One o del Motorola Moto G, referenciados normalmente por su nombre seguidos del calificativo “edición Google Play”. El programa de los *Google Play Edition Devices* parece haber finalizado en enero de 2015, con la retirada del último modelo disponible, el HTC One M8²¹.

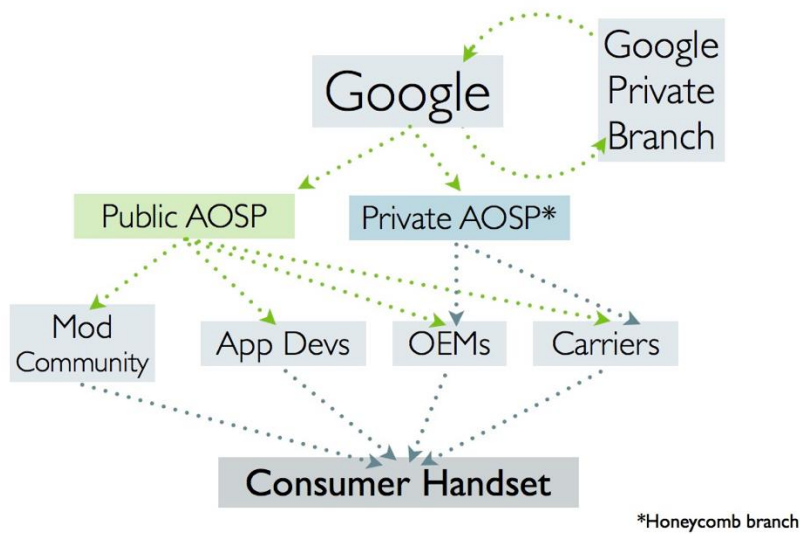
- 123.No existe ningún estándar ni modelo definido para la distribución de las actualizaciones de seguridad de Android, ni ninguna periodicidad definida para su publicación (salvo para los dispositivos Google Nexus y/o Pixel), por lo que Google y otros fabricantes (miembros o no de la *Open Handset Alliance*) pueden seguir procedimientos de actualización diferentes.
- 124.Finalmente, Google comenzó a publicar con periodicidad mensual la lista oficial de vulnerabilidades de Android para los dispositivos móviles Google Nexus en agosto de 2015, tras la vulnerabilidad conocida como Stagefright. Los boletines de seguridad de Android (“Android Security Bulletins”) también se publican en el grupo o foro oficial “Android Security Updates” [Ref.- 69].
- 125.Adicionalmente, Google dispone de información complementaria relativa a seguridad de Android y de las vulnerabilidades que pueden afectar a esta plataforma móvil, incluyendo los detalles del proceso recomendado que debe seguirse para su notificación [Ref.- 204].
- 126.Desde agosto de 2015, tras la vulnerabilidad conocida como Stagefright, Google también inició un programa de publicación y despliegue mensual de actualizaciones de seguridad del sistema operativo Android para sus dispositivos móviles [Ref.- 203], por lo que cada mes se publica una versión nueva de Android, ofreciendo la imagen de fábrica completa (*factory image*) [Ref.- 73] y la versión completa OTA de actualización (*full OTA image*) [Ref.- 199], para los dispositivos móviles bajo soporte.
- 127.De manera similar, Samsung, otro fabricante de referencia en el ecosistema Android, desde octubre de 2015 ha comenzado a publicar y distribuir boletines de seguridad correspondientes a sus dispositivos móviles Android, también con periodicidad mensual [Ref.- 198].
- 128.En el caso de los dispositivos móviles Google Nexus, las diferentes versiones del sistema operativo Android son proporcionadas mediante una imagen completa del sistema operativo (o plataforma móvil) Android (ver apartado “6.3. Actualización manual completa de Android”), o como una imagen parcial, normalmente obtenida como actualización OTA (*Over The Air*) (ver apartado “6.4. Actualización manual parcial de Android”).
- 129.Si la imagen es parcial, todos los datos y configuración del usuario son conservados, mientras que si la imagen es completa, se eliminarán todos los datos y configuración del usuario, fijando los valores de configuración de fábrica durante el proceso. Una imagen

²¹ https://play.google.com/store/devices/details?id=htc_m8 (enlace inactivo a fecha 11/09/2016).

completa instala una nueva versión de Android en el dispositivo móvil como si se tratase de un dispositivo recién comprado u obtenido de fábrica.

130. Debe tenerse en cuenta que antes de realizar una actualización del sistema operativo del dispositivo móvil se recomienda realizar una copia de seguridad de los datos del usuario.
131. Pese a que existen foros en Internet donde se distribuyen imágenes de ROM o *firmware* para múltiples sistemas operativos y fabricantes de terminales (como XDA Developers - <http://forum.xda-developers.com>), desde el punto de vista empresarial, en ningún caso se recomienda la instalación del sistema operativo desde una fuente no oficial.
132. En el mundo Android, las actualizaciones individuales adicionales a las actualizaciones de la versión completa del sistema operativo son muy limitadas, en contraposición a las actualizaciones para otros sistemas operativos de sobremesa cliente o servidor. Esta situación afecta tanto a las actualizaciones generales sobre los distintos componentes del sistema operativo, como a las actualizaciones específicas de seguridad.
133. El modelo de soporte actual de los dispositivos móviles comercializados por Google garantiza que los dispositivos Nexus y Pixel recibirán actualizaciones de seguridad durante al menos 3 años desde que el dispositivo empezó a ser comercializado en la Google Store, o al menos durante 18 meses desde su fecha de fin de comercialización (se toma la fecha más avanzada de las dos), y Google no se compromete a que haya actualizaciones con posterioridad a esa fecha [Ref.- 74].
134. Es importante reseñar que el compromiso de actualizaciones de Google afecta a versiones concretas de Android según el modelo del dispositivo móvil, y no se extiende indefinidamente a la versión original de Android con el que éste se suministró de fábrica (por ejemplo, Android 6.x para el Nexus 5X).
135. Es decir, Google no se compromete a actualizar con los parches de seguridad mensuales todas y cada una de las versiones de Android que han estado disponibles para un dispositivo móvil concreto (Android 6, 7 y 8), sino que actualizará mensualmente únicamente la última versión de Android disponible para los dispositivos Nexus y Pixel aún cubiertos por el soporte de Google. Por ejemplo, la última actualización de seguridad de Android 6.x para el Nexus 5X fue la de septiembre de 2016, ya que los dispositivos Nexus 5X a partir de dicha fecha también disponen de soporte para la versión de Android 7.x.
136. Para el modelo Nexus 5X analizado en la presente guía, la última fecha de compromiso de actualizaciones de seguridad es septiembre de 2018.
137. Desde octubre de 2016, Google añadió la fecha de publicación para cada nueva versión de Android a la nomenclatura empleada en las referencias a los ficheros con las imágenes de fábrica (*factory image*) correspondientes a las actualizaciones de seguridad mensuales. Hasta ese momento, las referencias estaban sólo compuestas por el número de compilación de la versión de Android asociada. El nuevo modelo permite identificar el mes al que corresponde la actualización y, por tanto, el nivel de parche de seguridad de cada fichero.

138. Pese a que en varias ocasiones, e incluso públicamente, los fabricantes de dispositivos móviles de la *Open Handset Alliance* (OHA) han intentado llegar a un acuerdo y comprometerse a proporcionar actualizaciones durante al menos 18 meses (periodo mínimo de soporte) desde la comercialización inicial de cada modelo de terminal, el tiempo y la historia han confirmado que no han sido capaces de mantener y ratificar ni siquiera estos compromisos públicos.
139. El fabricante del dispositivo móvil o el operador de telefonía es el que publicará actualizaciones para el terminal. Como norma general, y salvo que exista un motivo que desaconseje su instalación, se recomienda aplicar sobre el dispositivo móvil todas las actualizaciones facilitadas por el fabricante, ya que pese a que las mismas no reflejen explícitamente que se trata de actualizaciones de seguridad, pueden solucionar vulnerabilidades de seguridad públicamente conocidas.
140. Para abordar la comercialización de dispositivos móviles en mercados emergentes, como por ejemplo en la India, asociados con recursos económicos más bajos, Google anunció en el año 2014 la creación de una plataforma denominada Android One, que, en origen, pretendía llegar a acuerdos con fabricantes de dispositivos móviles de forma que dichos fabricantes desarrollarían terminales de especificaciones y precio reducidos que recibirían soporte directamente por parte de Google. Es decir, en lugar de que el fabricante fuese el encargado de implementar y distribuir las actualizaciones del sistema operativo, Google liberaría las correspondientes imágenes OTA empleando un modelo similar al empleado para los dispositivos Nexus [Ref.- 246].
141. Android One comenzó a estar disponible con Android 4.4.4 (KitKat).
142. Para garantizar las actualizaciones, el programa Android One establece que los dispositivos que se acojan a él deberán incluir únicamente aplicaciones que se puedan gestionar desde Google Play, es decir, sin la capa de aplicaciones propietarias que acompañan comúnmente al hardware de los fabricantes, así como incorporar el servicio Google Play Protect y el asistente de Google (Google Assistant) (consultar apartado “22. App Google: Asistente de Google, Mi Tablón y Servicios de Búsqueda de Google”).
143. Con la incorporación al mercado Android One de la compañía Xiaomi y su terminal Mi A1 [Ref.- 247], que, además de un hardware más potente que el que correspondería a los dispositivos móviles objeto del programa inicial, incluye una aplicación de cámara necesaria para aprovechar las capacidades de la cámara dual, Google, en lugar de proporcionar directamente las actualizaciones de sistema operativo a los dispositivos Android One, se encargará de marcar las pautas en relación a las actualizaciones, pero dejará en manos del fabricante el desarrollo y distribución de las mismas de acuerdo a los términos pactados.
144. Google ha desarrollado un modelo para la resolución de problemas de seguridad y la distribución de actualizaciones en Android a través de CTS (*Compatibility Test Suite*) [Ref.- 89], actividad integrada en el *Android Open Source Project* (AOSP), encargada de asegurar la compatibilidad entre dispositivos Android [Ref.- 84]:



145. Sin embargo, toda la complejidad asociada a las actualizaciones de Android y los diferentes factores y entidades involucradas en el proceso, como las múltiples personalizaciones del sistema operativo realizadas por los fabricantes, dan lugar a retrasos significativos desde que las soluciones a problemas de seguridad son añadidas al repositorio del *Android Open Source Project* (AOSP²²) hasta que están disponibles para los usuarios, dejando los dispositivos móviles desprotegidos durante todo ese tiempo (varios meses habitualmente, en el mejor de los casos).

146. La siguiente imagen refleja algunas de las vulnerabilidades más significativas en Android durante el periodo entre los años 2010 y 2011, varias de las cuales han sido aprovechadas por código dañino públicamente distribuido, como DroidKungFu y DroidDream²³:

Known Android Vulnerabilities 2010-2011		
Year	Vulnerability	Malware that Exploited Vuln
2010	Exploid	DroidDream, zHash, DroidKungFu (Legacy)
2010	CVE-2010-1807 WebKit NaN	
2010	RageAgainstTheCage/Zimperlich	DroidDream, BaseBridge, DroidKungFu (Legacy)
2011	Psneuter/KillingInTheNameOf	
2011	Gingerbreak/Honeybomb	

147. Mediante la realización de una búsqueda por el término “Android” en la US CERT NVD (National Vulnerability Database: http://web.nvd.nist.gov/view/vuln/search-results?query=android&search_type=all&cves=on) o en el proyecto CVE (*Common Vulnerabilities and Exposures*) de MITRE (<http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=android>) es posible obtener un listado de las vulnerabilidades de seguridad conocidas públicamente que han afectado a diferentes versiones del

²² <https://source.android.com>

²³ Las referencias que inicialmente publicó Google para informar sobre este ataque, que tuvo enorme repercusión, han sido eliminadas de sus sitios web [Ref.- 88].

sistema operativo Android en los últimos años, así como a aplicaciones de terceros desarrolladas para Android.

148. Adicionalmente, las soluciones (parches o *fixes*) publicadas para corregir vulnerabilidades de seguridad conocidas suelen estar disponibles únicamente para las últimas versiones de Android, no existiendo un mecanismo establecido encargado de proporcionar dichas soluciones para versiones previas de Android, también vulnerables.
149. Por otro lado, numerosos fabricantes y operadores de telefonía móvil no proporcionan actualizaciones para modelos de dispositivos móviles previos, por ejemplo, basados en las versiones previas de Android, como 2.x ó 4.x, por lo que estos serán siempre vulnerables.
150. Este hecho se ve agravado por la velocidad de consumo de las nuevas tecnologías, que afecta a cuándo los dispositivos móviles son considerados obsoletos, donde, en la actualidad, un dispositivo con dos o más años difícilmente estará soportado e incluido en el ciclo de actualizaciones de software.
151. Por ejemplo, para el dispositivo móvil analizado en la presente guía (Google Nexus 5X), que se empezó a comercializar en septiembre de 2015, Google sólo se compromete a garantizar las actualizaciones del sistema operativo hasta septiembre de 2017, y las actualizaciones de parches de seguridad hasta septiembre de 2018.
152. Esta evolución de las versiones de Android asociada a la finalización del periodo de soporte para modelos de dispositivos móviles previos se ha seguido repitiendo a lo largo de los años. Por ejemplo, los dispositivos móviles Nexus 4 y Nexus 10 dejaron de estar soportados cuando se publicó la versión 6.x de Android (“Marshmallow”) en octubre de 2015, siendo Android 5.x (“Lollipop”) la última versión oficialmente soportada para estos modelos.
153. Asimismo, en agosto de 2016, Google publicó la versión oficial de Android 7.x (“Nougat”), con soporte únicamente para los dispositivos Google Nexus 6, 9, 5X y 6P (junto al Nexus Player, Pixel C y el General Mobile 4G), no soportando dispositivos móviles previos muy extendidos como, por ejemplo, el Nexus 5 y el Nexus 7.
154. La importancia, por un lado, de actualizar la versión de Android en el dispositivo móvil a la última versión disponible, y por otro, de verificar si la actualización corrige vulnerabilidades previas públicamente conocidas, se refleja tanto en vulnerabilidades antiguas relevantes y muy generalizadas como la de TapJacking [Ref.- 116], como en vulnerabilidades críticas más recientes que han afectado a Android, como por ejemplo “Android Master Key” [Ref.- 117], “Android browser SOP bypass” (o Universal XSS, UXSS, en Android < 4.4) [Ref.- 118] (CVE-2014-6041) o sus variantes [Ref.- 100], vulnerabilidades en Android WebView (en Android < 4.4) [Ref.- 119], “Android Fake ID” [Ref.- 101], y otras vulnerabilidades y exploits publicados para Android 4.x y versiones previas hasta el año 2015 [Ref.- 61].
155. Complementariamente, a partir del año 2015, en concreto del mes de agosto, se dispone de la lista oficial de vulnerabilidades que afectan a Android, para sus diferentes versiones a partir de Android 5.x, publicada por Google [Ref.- 69], algunas de ellas de criticidad elevada, como la que originó la publicación mensual de parches de seguridad para Android: Stagefright.
156. En el caso de disponer de un dispositivo móvil Android para el que sí dispone de una actualización a una versión superior de Android, por ejemplo 6.0.1 para un terminal

basado en Android 6.0, se recomienda aplicar la actualización sobre el dispositivo con el objetivo de instalar la última versión disponible y protegerlo de vulnerabilidades conocidas.

157. Con el objetivo de mantener el dispositivo móvil actualizado, se recomienda comprobar periódicamente desde el propio dispositivo la disponibilidad de actualizaciones desde el menú “Ajustes - Información del teléfono - Actualizaciones del sistema”.
158. Desde el punto de vista de seguridad es necesario actualizar igualmente todas las aplicaciones móviles (o apps) instaladas sobre el sistema operativo (ver apartado “23.9.1. Actualización de apps en Android”) y, en particular, la app asociada a los Servicios de Google Play (GPS, *Google Play Services*) debido a las capacidades de actualización que ésta dispone en la propia plataforma móvil Android (ver apartado “6.2. Servicios de Google Play”).

6.2. SERVICIOS DE GOOGLE PLAY

159. En los últimos años Google ha adoptado un modelo de actualizaciones diferente y desconocido en muchas ocasiones, complementario y previo a las actualizaciones mensuales del nivel de parche de seguridad disponibles desde agosto de 2015, y de aplicación no sólo para los dispositivos móviles Nexus y/o Pixel, sino para un gran número de dispositivos Android. A través de Google Play, y de sus servicios asociados, en concreto los Servicios de Google Play (GPS, *Google Play Services*), la plataforma móvil Android recibe numerosas actualizaciones que no sólo afectan a Google Play y al mercado de apps, sino también a otros componentes (o apps) críticas del sistema operativo y existentes por defecto [Ref.- 59].
160. Por tanto, el concepto de actualización en Android ha cambiado. Muchos componentes de la arquitectura de Android se han independizado del núcleo de la plataforma móvil, pudiendo ser actualizados independientemente y con mayor frecuencia. En lugar de tener que actualizar el sistema operativo a una nueva versión para poder disponer de funcionalidades o mecanismos de seguridad previamente ausentes, la actualización individual de la app Servicios de Google Play²⁴ [Ref.- 150] puede proporcionar nuevas actualizaciones para ciertos elementos de la plataforma móvil Android.
161. Otro ejemplo de esta independencia entre los componentes de la plataforma móvil y la versión concreta de Android es la propia aplicación “Google”, que controla todos los ajustes relativos a los servicios de Google, incluyendo el asistente personal (Google Assistant) y los servicios conocidos como “feed”.
162. Adicionalmente, es posible disponer de actualizaciones parciales para múltiples apps a través de la app de Google Play (denominada “Play Store”; el mercado oficial de apps de Android se llama actualmente Google Play, pero la app para acceder a éste desde el dispositivo móvil sigue manteniendo el nombre antiguo del mercado oficial, “Play Store”), como por ejemplo, los teclados del sistema, el navegador web (Chrome), la app de correo electrónico (Gmail) y de mensajería (Hangouts) o la app de calendario pueden ser actualizadas independientemente como cualquier otra app de terceros.
163. La app asociada a Google Play se actualiza de forma automática sin intervención del usuario ni posibilidad sencilla de controlar o detener dichas actualizaciones.

²⁴ <https://play.google.com/store/apps/details?id=com.google.android.gms&hl=es>

164. La app de los ajustes de configuración (Google Settings o “Ajustes de Google”), que existía de forma independiente con la versión 6.0 de Android instalada por defecto, se integra como parte de la app de Google al actualizar dicha app a una versión reciente (lo cual también se lleva a cabo a través de la app “Play Store”). Además, buena parte de esos ajustes se puede controlar desde el menú general de Ajustes, y concretamente, desde el apartado “[Personal] Google”.
165. Las actualizaciones parciales proporcionadas por los Servicios de Google Play son distribuidas incluso para dispositivos móviles que disponen de versiones antiguas de Android (desde Android 2.3, “Gingerbread”) y para las que no se dispone de nuevas actualizaciones o versiones de sistema operativo.
166. Originalmente, las capacidades de *Google Play Services* versión 1.0, disponible desde septiembre de 2012, eran muy limitadas, añadiendo soporte para OAuth 2.0 y algunas APIs de Google+. A lo largo de los años, éstas se han extendido notablemente.
167. Una de las capacidades y/o ajustes de configuración existentes en Android que se actualizaban anteriormente vía Play Store pero que se eliminaron como componente autónomo del dispositivo son las asociadas al administrador de dispositivos de Android, responsable de la gestión remota del terminal (existente desde Android 2.2, e instalado por defecto desde Android 4.4). Este administrador ha pasado a integrarse como parte de los servicios asociados a la cuenta de Google del usuario y a independizarse del dispositivo físico o sistema operativo (ver apartado “8.1. Gestión remota de dispositivos Android por parte del usuario”).
168. A través de Google Play se controlan asimismo las capacidades de escaneo o verificación de apps (ver apartado “23.8. Verificación de seguridad de las apps”).
169. Una de las vulnerabilidades que fue resuelta a través de las capacidades de actualización de los Servicios de Google Play es la asociada (originalmente) a la versión 4.4.4 de Android, y específicamente a la vulnerabilidad de OpenSSL que permitía la realización de ataques MitM (Man-in-the-Middle), con CVE-2014-0224 y conocida como la vulnerabilidad de “inyección CCS (ChangeCipherSpec)” [Ref.- 138][Ref.- 139].
170. El proveedor de seguridad que proporciona las capacidades de comunicaciones de red seguras de Android fue actualizado con la versión 5.0 de los Servicios de Google Play (publicada en julio de 2014 [Ref.- 150]) para mitigar específicamente esta vulnerabilidad de “inyección CSS” [Ref.- 152].
171. Complementariamente, se recomienda que las apps hagan uso de los métodos y APIs asociados a los Servicios de Google Play, por un lado, para confirmar que se dispone de la última versión del proveedor de seguridad, y por otro, para asegurarse de que ejecutan en un dispositivo móvil que hace uso de dicho proveedor de seguridad, que éste está actualizado, y que mitiga ataques basados en vulnerabilidades y *exploits* conocidos.

6.3. ACTUALIZACIÓN MANUAL COMPLETA DE ANDROID

172. Alternativamente a la actualización automática realizada por Android (ver apartado “6.1. Actualización automática del sistema operativo Android”), o cuando esta opción no está disponible para ciertos fabricantes u operadores de telefonía móvil, es posible realizar la actualización del sistema operativo de Android de forma manual mediante la descarga de los ficheros de actualización oficiales desde la web de Google [Ref.- 73] (o del fabricante).
173. La actualización manual requiere conectar un ordenador mediante USB al dispositivo móvil.
174. En el caso de ciertos fabricantes u operadores de telefonía móvil, en la mayoría de ocasiones estos ficheros no son publicados oficialmente, aunque su ubicación puede estar disponible de manera no oficial desde numerosas fuentes en Internet.
175. Para versiones previas de Android, como por ejemplo 2.x, existía una lista no oficial (incompleta) con los ficheros de actualización proporcionados por Google y por los diferentes fabricantes de dispositivos móviles basados en Android (ver versión previa de la presente guía para Android 2.x [Ref.- 401]).
176. Desde el punto de vista de seguridad, las descargas de actualizaciones siempre deben realizarse desde enlaces que referencien a la web oficial de Google (o del fabricante), y es recomendable actualizar siempre a la última versión de Android disponible.
177. En el caso de los dispositivos móviles comercializados por Google, desde hace unos años Google proporciona de manera oficial acceso a las imágenes completas de fábrica (*factory images*) para las actualizaciones y nuevas versiones de Android, en concreto, para los dispositivos móviles de la familia Google Nexus y/o Pixels, *Factory Images for Nexus and Pixel Devices* [Ref.- 73].
178. De manera complementaria, Google también proporciona oficialmente acceso a las imágenes OTA (Over-the-Air) de fábrica (*full OTA images*) para las actualizaciones y nuevas versiones de Android, en concreto, para los dispositivos móviles de la familia Google Nexus y/o Pixel, *Full OTA Images for Nexus and Pixel Devices* [Ref.- 199]. Es importante reseñar que estas imágenes (ver apartado “6.4. Actualización manual parcial de Android”) no son equivalentes a las imágenes parciales que el dispositivo se descarga vía OTA durante una actualización automática (ver apartado “6.1. Actualización automática del sistema operativo Android”).
179. En el caso de las actualizaciones automáticas parciales, el dispositivo se descarga un fichero de tamaño más reducido, que sólo incluye los componentes que han cambiado desde la versión de Android instalada actualmente, de la que se parte para la actualización. En el caso de los ficheros o imágenes OTA disponibles a través de Google, el contenido del fichero es casi similar en tamaño al fichero de la imagen completa (descrita en el presente apartado), pues, a diferencia de lo que ocurría en versiones Android 4.x y anteriores (en las que las actualizaciones a una versión requerían partir de otra versión concreta), Google proporciona un único fichero de actualización OTA denominado “Full OTA Image” sea cual sea la versión de Android de partida.
180. La página web oficial de Google [Ref.- 73] con las imágenes completas de fábrica para los dispositivos móviles Google Nexus y/o Pixel se va actualizando periódicamente según se van publicando nuevas versiones de Android (incluyendo los nuevos niveles de parches

de seguridad mensuales), pudiendo desaparecer las referencias e imágenes de versiones o subversiones previas de Android.

181. Debe tenerse en cuenta que el proceso de actualización del dispositivo móvil a partir de una imagen de *firmware* completa (*factory image*) eliminará todos los datos del terminal, por lo que se recomienda realizar una copia de seguridad antes de llevar a cabo este proceso.
182. La actualización a partir de una imagen OTA (automática, o manual, *full OTA image*), sin embargo, no borra los datos del usuario, aunque se sigue recomendando realizar una copia de seguridad previa a la actualización.
183. Si la imagen de Android es completa, se dispone de los enlaces a las imágenes oficiales directamente desde Google para los distintos modelos de dispositivos móviles Nexus y/o Pixel, descargables desde “<https://dl.google.com/dl/android/aosp/>*”. El nombre del fichero ZIP correspondiente a estas imágenes sigue el siguiente patrón: *nombre clave del tipo de dispositivo móvil + número de compilación + indicativo de que se trata de la imagen completa o de fábrica (“factory”) + 8 primeros caracteres hexadecimales del hash SHA256 del fichero “.zip” o “.tgz”*.

Nota: Hasta la versión 4.x de Android, para los ficheros de imagen completos, en lugar de utilizarse el hash SHA256 se usaba el hash SHA1.

Nota: Para los ficheros de actualización automática (OTA), en lugar del SHA256 Google sigue utilizando internamente el SHA1 en su nomenclatura.

184. Por ejemplo, el fichero de la imagen de fábrica completa correspondiente a la versión Android 6.0.1 (MTC20K) empleada para la elaboración de la presente guía en un terminal Nexus 5X (bullhead), cuyo valor SHA256 es 4a950470af6c1e0111cfa8efbd77422928b88d01800dd2fadc6f8eeae1b97a9, sería:

```
https://dl.google.com/dl/android/aosp/bullhead-mtc20k-factory-4a950470.zip
```

185. Por otro lado, el fichero de la imagen OTA parcial correspondiente a la versión Android 6.0.1 (MTC20K) empleada para la elaboración de la presente guía en un terminal Nexus 5X (“bullhead”), cuyo valor SHA256 es 531d55c028291eb84dc217584d4f7c098490603875458e46f2634683354a6a76, sería:

```
https://dl.google.com/dl/android/aosp/bullhead-ota-mtc20k-531d55c0.zip
```

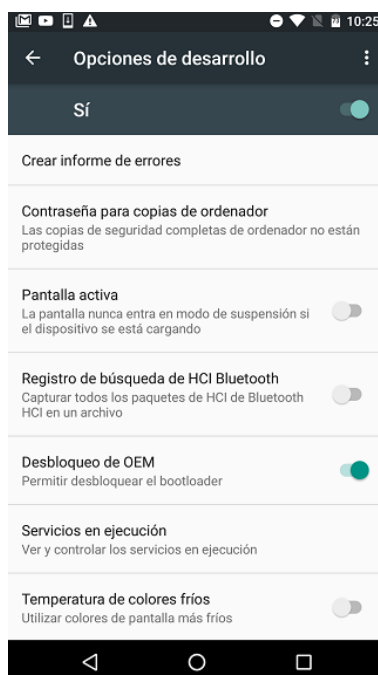
186. Antes de iniciar el proceso de actualización del dispositivo móvil, es necesario verificar que el nivel de batería del dispositivo es suficiente (es decir, superior al 50%).
187. También es necesario hacer uso de la herramienta “fastboot”, disponible como parte del Android SDK, y también de forma independiente²⁵. Las “platform tools” de Android incluyen además la herramienta “adb”, que permite acceso vía USB al dispositivo móvil

²⁵ <https://developer.android.com/studio/releases/platform-tools.html>

como desarrollador mediante el protocolo ADB²⁶ (*Android Debug Bridge*); ver apartado “13.3. Opciones de desarrollo y depuración USB” [Ref.- 110].

188. Para llevar a cabo el proceso de actualización completa desde una imagen de fábrica (*factory image*), desde Windows, Linux o macOS, es necesario desbloquear el gestor de arranque (o *bootloader*) del dispositivo móvil Android, si aún no ha sido desbloqueado previamente.

189. A partir de Android 6.x, para desbloquear el gestor de arranque, es necesario adicionalmente habilitar la opción “Ajustes - Opciones de desarrollo - Desbloqueo de OEM”, que no existía en versiones iguales o previas a Android 5.x. Esta operación requiere que el usuario introduzca el código de acceso (PIN, patrón o contraseña) actualmente empleado como método de protección de acceso al dispositivo móvil. Para poder activar esta opción, es preciso previamente habilitar las opciones de desarrollo (ver apartado “13.3. Opciones de desarrollo y depuración USB”).



190. Si el gestor de arranque se hubiese desbloqueado previamente, desde el menú “Ajustes - Opciones de desarrollo”, se mostrará el valor “Desbloqueo OEM - el gestor de arranque ya está desbloqueado”. Una vez seleccionada la opción “Ajustes - Opciones de desarrollo - Desbloqueo de OEM”, es posible proceder a desbloquear el *bootloader* mediante dos métodos diferentes equivalentes:

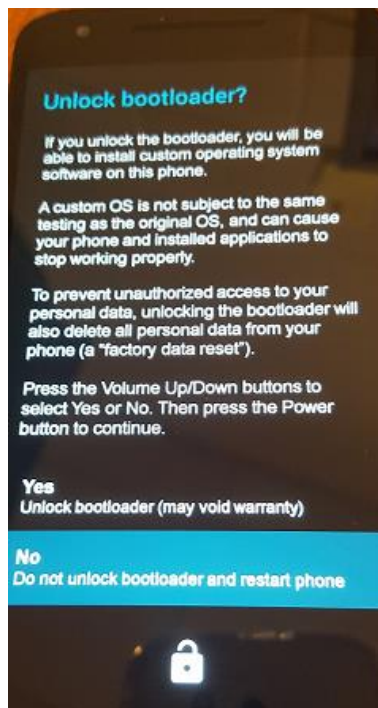
- Apagando el dispositivo móvil y reanunciando el mismo con el botón de bajar el volumen y el botón de encendido pulsados simultáneamente hasta que aparezca la pantalla del *bootloader*. Si el valor de “Device state” del dispositivo aparece como “locked”, indica que el gestor de arranque está bloqueado. Para desbloquearlo, desde el ordenador conectado por USB al dispositivo móvil se deberá ejecutar el comando “*fastboot flashing unlock*” (hasta Android 5.x incluido, el comando era “*fastboot oem unlock*”, que sigue vigente en Android 6.x y 7.x).

²⁶ Para utilizar el protocolo ADB con el objetivo de interactuar con el dispositivo móvil y proceder a actualizar la versión de Android, es necesario descargar la última versión de las “*platform tools*” del Android SDK (la versión mínima necesaria es la 25.0.5, ya que, en versiones anteriores, el demonio de “adb” abortaba su ejecución para ficheros de gran tamaño; consultar “<https://issuetracker.google.com/issues/37139736>” para más detalles).

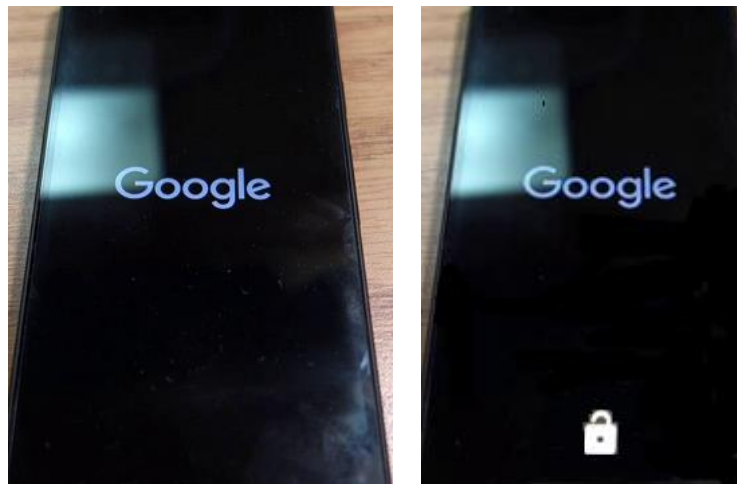
pero cuyo uso se desaconseja frente al nuevo comando). En el dispositivo móvil, se mostrará una pantalla informando de que esta operación eliminará todos los datos del dispositivo, y solicitará confirmación por parte del usuario para continuar.

- Utilizando el protocolo ADB, y la herramienta asociada “adb”, desde el ordenador conectado por USB al dispositivo móvil. Previamente, habrá que habilitar las opciones de desarrollo mediante “Ajustes - Información del teléfono”, pulsando 7 veces sobre el “Número de compilación”. Esta operación hará que aparezca un nuevo menú “Ajustes - Opciones de desarrollo” y, dentro de éste, la opción “Depuración por USB”. Una vez activada esta opción, quedará habilitado el acceso USB al dispositivo móvil como desarrollador mediante el protocolo ADB (*Android Debug Bridge*) [Ref.- 110] (ver apartado “13.3. Opciones de desarrollo y depuración USB”). Estas capacidades permiten que se pueda ejecutar el comando “adb reboot bootloader” para arrancar desde el *bootloader*, acceder al gestor de arranque y, una vez en él, poder ejecutar el comando “fastboot flashing unlock” para desbloquear el gestor de arranque en caso de estar bloqueado.

191. Tras recibir la confirmación del usuario (utilizando el botón de subir volumen y presionando el botón de encendido) a través de la pantalla del dispositivo móvil, se eliminarán todos los datos existentes en el dispositivo móvil y se desbloqueará el *bootloader*.



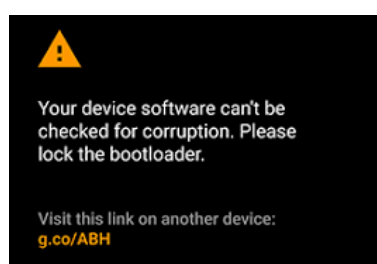
192. Cuando el *bootloader* está bloqueado, en el arranque del terminal no se muestra ningún tipo de candado, a diferencia de lo que sucedía en versiones anteriores a Android 6.x. Si se desbloquea el bootloader, en la pantalla de arranque se mostrará un candado abierto en la parte inferior central del dispositivo móvil:



193. Cuando el *bootloader* está desbloqueado, la pantalla del gestor de arranque o modo *fastboot* muestra el valor “Device State - unlocked” (en versiones anteriores de Android, se mostraba “Lock State - unlocked”).



194. El desbloquear el *bootloader*, cuando se reinicia el dispositivo móvil se mostrará el siguiente mensaje:



195. Esto es debido al mecanismo “Verified boot” (consultar apartado “7.8. Proceso de arranque seguro: Verified Boot”), responsable de examinar el código del sistema operativo al encender un dispositivo Android para verificar su integridad y confirmar que no ha sido modificado y que se puede utilizar de forma segura.
196. Una vez desbloqueado el *bootloader*, el dispositivo móvil permanecerá en este estado aunque se borre la partición de sistema o de datos, por ejemplo, tras llevar a cabo una restauración a fábrica.

197. Seguidamente, se ha de conectar el dispositivo móvil a través de USB y acceder al gestor de arranque (o *bootloader*), también conocido como modo *fastboot* (para dispositivos móviles Nexus y/o Pixel). De nuevo, en caso de haber empleado el método de desbloqueo del gestor de arranque descrito previamente que hacía uso del protocolo ADB, se puede emplear el comando “*adb reboot bootloader*” (a través de USB), o el propio dispositivo móvil (apagando el dispositivo y encendiéndolo mientras se mantienen pulsados simultáneamente el botón de encendido y el botón de bajar el volumen, para el caso concreto del dispositivo móvil empleado para la elaboración de la presente guía).
198. Una vez descargada la imagen completa del *firmware* de la versión de Android a instalar, debe descomprimirse el fichero ZIP, y acceder al directorio asociado recién creado:

```
C:\Android\bullhead-6_0_0_mdb08m> dir
Directory: C:\Android\bullhead-6_0_0_mdb08m
Mode                LastWriteTime         Length Name
----                -
--- 26/10/2015      20:30         4487344 bootloader-bullhead-bhz10i.img
--- 26/10/2015      20:30           968 flash-all.bat
--- 26/10/2015      20:30           839 flash-all.sh
--- 26/10/2015      20:30           794 flash-base.sh
--- 26/10/2015      20:30      933329144 image-bullhead-mdb08m.zip
--- 26/10/2015      20:30      57973248 radio-bullhead-m8994f-2.6.28.0.65.img
```

199. Mediante la ejecución del script “flash-all” (“*.bat*” o “*.sh*”, según se haga uso de un ordenador basado en Windows o en Linux) se llevará a cabo la instalación de la versión de Android correspondiente, incluyendo la instalación de la imagen del gestor de arranque (*bootloader*), del *firmware* del procesador de banda base (*baseband*) o radio, y del sistema operativo Android o partición de sistema (“*/system*”).
200. Si el *bootloader* no está desbloqueado, aunque se ejecute el script “*flash-all*” y aparentemente se estén realizando las acciones contempladas en el mismo, el script terminará fallando con el error “*Failed (remote: device is locked. Cannot flash images)*”.
201. Una vez el dispositivo móvil ha sido actualizado (tras ejecutar el script y pasados unos minutos), se reiniciará y arrancará la nueva versión de Android aplicada. El dispositivo móvil arrancará en su estado original de fábrica, por lo que será necesario completar el proceso de instalación y configuración inicial (ver apartado “24. Apéndice A: Proceso de instalación y configuración inicial”).

Nota: El proceso de actualización desde una imagen completa de Android mediante el script “*flash-all*” también elimina por defecto todos los datos de usuario del dispositivo móvil. Esta es la opción de actualización recomendada con el objetivo de evitar problemas de compatibilidad entre diferentes versiones de Android debido a la existencia de contenidos y datos previamente existentes. Sin embargo, existe la posibilidad de modificar el script “*flash-all*” y en concreto la directiva “*fastboot -w update ...*”, eliminando la opción “*-w*” (*wipe*), para que los datos de usuario no sean borrados durante el proceso de actualización.

202. Desde el punto de vista de seguridad se recomienda bloquear de nuevo el gestor de arranque (*bootloader*) nada más completar el proceso de actualización. Para ello, basta con apagar el dispositivo móvil tras el primer reinicio después de la actualización, arrancar de nuevo en modo *fastboot* mediante ADB a través de USB o desde el propio dispositivo móvil con la combinación de botones descrita previamente, y conectar el dispositivo móvil a un ordenador mediante el puerto USB. Desde el mismo, es posible

ejecutar el comando “*fastboot flashing lock*” para volver a bloquear inmediatamente el gestor de arranque. El estado es indicado en la pantalla del propio gestor de arranque mediante el mensaje (“Device State - locked”):



203. A partir de Android 6.x, si se hubiese llevado a cabo alguna personalización antes de volver a bloquear el *bootloader*, sería necesario realizar una copia de seguridad del dispositivo móvil (ver apartado “21. Copias de seguridad”), ya que el proceso conlleva una restauración a fábrica con la consecuente eliminación de todos los datos de usuario. Este no era el comportamiento de las versiones de Android 5.x o anteriores, en las que el proceso de bloqueo del gestor de arranque no eliminaba ningún dato del dispositivo.
204. Por tanto, una vez bloqueado de nuevo el gestor de arranque (o *bootloader*), será necesario completar el proceso de instalación y configuración inicial.
205. De esta forma, una vez el *bootloader* está bloqueado, no será posible actualizar el dispositivo móvil mediante una actualización completa, ni interactuar con las diferentes particiones existentes en el dispositivo, sin tener que eliminar previamente todos los datos del usuario.

6.4. ACTUALIZACIÓN MANUAL PARCIAL DE ANDROID

206. En el caso de los dispositivos móviles Google Nexus y/o Pixel, las diferentes versiones del sistema operativo Android son proporcionadas mediante una imagen completa del sistema operativo (o plataforma móvil) Android (ver apartado “6.3. Actualización manual completa de Android”), o como una actualización parcial, normalmente obtenida como actualización OTA (*Over-the-Air*) automáticamente por parte de Android (ver apartado “6.1. Actualización automática del sistema operativo Android”).
207. Alternativamente a la actualización automática realizada directamente por Android vía OTA (ver apartado “6.1. Actualización automática del sistema operativo Android”), o al proceso de instalación o actualización manual desde una imagen completa de *firmware*, *factory image* (ver apartado “6.3. Actualización manual completa de Android”), a partir de Android 6.x es posible realizar la actualización del sistema operativo de Android de forma manual mediante la descarga de los ficheros de actualización OTA completos, o

imágenes OTA completas (*full OTA images*), oficiales desde la web de Google (o del fabricante).

208. Estos ficheros no son los mismos que se descarga el dispositivo móvil mediante el mecanismo OTA durante una actualización automática, pues las actualizaciones automáticas detectan la versión de partida del dispositivo móvil y le envían únicamente un fichero que contiene los cambios correspondientes a la versión de Android a la que se actualizará.
209. La principal diferencia entre una actualización manual completa y una actualización manual parcial a través de una imagen OTA es que ésta última mantiene los datos de usuario.
210. En versiones de Android 5.x y anteriores, las actualizaciones parciales solo eran distribuidas a través de OTA de forma automática con conexión a Internet, y no se disponía de los enlaces a las imágenes OTA completas oficiales directamente desde Google para los distintos modelos de dispositivo móvil. Actualmente, se dispone de las imágenes OTA completas para versiones iguales o superiores a Android 6.0.1. Las imágenes completas (no OTA) sí están disponibles para versiones de Android desde la versión 2.x.
211. Adicionalmente, por un lado, existen repositorios no oficiales con referencias, en concreto para los dispositivos móviles de la familia Google Nexus (de interés y aplicación en la presente guía) o Google Experience Devices, que permiten identificar los diferentes ficheros correspondientes a las actualizaciones parciales disponibles, al igual que obtener las referencias a los enlaces OTA oficiales de Google utilizados de manera automática por Android, desde foros como XDA Developers²⁷.
212. Por otro lado, mediante el análisis de los registros o logs de logcat, o del tráfico de red del proceso de actualización de Android, es posible obtener los enlaces a los ficheros de descarga de las actualizaciones OTA, que están disponibles desde el servidor "ota.googlezip.net/packages/ota-api/*". Es importante reseñar que estos ficheros no están disponibles para su descarga oficial desde los servidores de Google, por lo que no se recomienda su aplicación.

Nota: En el caso de Android 6.0 no se muestra un ejemplo de la URL del fichero OTA de actualización, ya que la actualización OTA para el Nexus 5X lleva directamente a la versión 7.1.1 de Android, en lugar de a la versión 6.0.1.

213. Estos ficheros resultan de menor tamaño que las imágenes OTA completas (*full OTA images*) que se pueden descargar manualmente desde el sitio web oficial de Google, ya que contienen sólo los cambios a aplicar entre la versión actual y la versión de Android destino tras aplicarse la actualización.
214. El nombre del directorio incluye el término "google_", seguido del nombre en clave del tipo de dispositivo móvil, en este caso "bullhead" (por duplicado) asociado al Nexus 5X. El nombre del fichero en este caso no corresponde al valor (o parte del valor) del hash SHA256 del fichero ZIP de la actualización, como ocurre con las versiones de las *full OTA images* o de las actualizaciones completas (*factory images*), sino al valor del hash SHA1 de dicho fichero ZIP. Este formato basado en el valor del hash SHA1 ya se utilizaba en la nomenclatura de las actualizaciones parciales en versiones de Android 4.x y anteriores.

²⁷ <https://forum.xda-developers.com>

- 215.El proceso de actualización manual parcial (desde Windows, Linux o macOS) requiere disponer del fichero oficial de actualización OTA completo descargado desde la web de Google, y es también necesario disponer del SDK de Android y habilitar el acceso por USB al dispositivo móvil como desarrollador, en concreto, mediante ADB, al igual que para realizar una actualización manual completa. Se recomienda verificar el hash del fichero de la imagen para asegurarse de que es correcto, comparando los 8 primeros caracteres hexadecimales del valor SHA256 (en el caso de imágenes *full OTA image* descargadas desde la página oficial de Google) o SHA1 (para imágenes OTA parciales que se han descargado mediante el análisis del tráfico o logs) con los disponibles en el nombre del fichero.
- 216.En el caso de Android 5.x, este método permite únicamente la actualización de la versión de Android disponible en el dispositivo móvil mediante una imagen OTA parcial no oficial.
- 217.A partir de Android 6.x, este método también permite la actualización de la versión de Android disponible en el dispositivo móvil mediante una imagen OTA completa oficial (*full OTA image*).
- 218.Una vez el dispositivo móvil se ha conectado al ordenador mediante el puerto USB, es necesario reiniciarlo desde la partición de recuperación (o *recovery*). Para ello se puede utilizar el comando “adb” desde el ordenador vía USB, el gestor de arranque (accesible mediante la combinación adecuada de botones en el dispositivo móvil para acceder al *bootloader*, tal como se ha descrito anteriormente) o acceder directamente mediante una nueva combinación de botones.
- 219.Para acceder a la imagen de recuperación (o *recovery*) mediante el comando “adb” es necesario disponer de acceso como desarrollador mediante USB, y emplear el comando “adb reboot recovery”, que mostrará la pantalla de la imagen de recuperación con un androide y un icono de peligro (descrita posteriormente).
- 220.Para acceder a la imagen de recuperación a través del gestor de arranque o *bootloader*, ya que éste dispone de una opción de menú de recuperación específica (en el dispositivo móvil empleado para la elaboración de la presente guía), puede emplearse el comando “adb reboot bootloader” desde el ordenador mediante USB o se puede acceder al *bootloader* desde el propio dispositivo móvil²⁸, mediante la combinación de botones correspondiente (tal y como se describió en el apartado “6.3. Actualización manual completa de Android”). Una vez en el gestor de arranque, es posible arrancar desde la imagen de recuperación desplazándose hasta la opción “Recovery mode” mediante el botón de bajar volumen y seleccionándola mediante el botón de encendido.
- 221.Para acceder directamente a la imagen de recuperación (o *recovery*) desde el propio dispositivo móvil, se dispone de una combinación de botones específica. Se debe apagar el dispositivo móvil y encenderlo (en el caso del dispositivo móvil empleado para la elaboración de la presente guía) manteniendo pulsados los botones de bajar y subir el volumen simultáneamente. El dispositivo móvil se reiniciará y mostrará una pantalla de recuperación que contiene un androide y un icono de peligro, con una admiración dentro de un triángulo (!) de color rojo. A continuación, debe mantenerse pulsado el botón de encendido y posteriormente pulsar el botón de subir el volumen simultáneamente hasta que aparezca el mensaje “Recovery mode” en la pantalla.

²⁸ <https://source.android.com/source/building-devices.html#booting-into-fastboot-mode>

- 222.El modo de recuperación es mostrado en la pantalla con el texto “Android Recovery” en color amarillo en la parte superior del dispositivo móvil y, debajo, la línea “Google/bullhead/bullhead”, seguida de otra línea que incluye la versión actual de Android disponible en el dispositivo y el número de compilación de dicha versión. Con el botón de bajar volumen es posible desplazarse a la opción “Apply update from ADB”, debiendo usar el botón de encendido para seleccionar la opción deseada.



- 223.Cuando el dispositivo se encuentra ejecutando la imagen de recuperación, y se habilitan las capacidades de comunicación mediante ADB, el estado del dispositivo es diferente al empleado en el acceso ADB estándar, y está identificado por el término “sideload”. Así, al ejecutar el comando “adb devices” en el ordenador, se verá el número de serie asociado al dispositivo móvil seguido del texto “sideload”.
- 224.Para llevar a cabo una actualización manual parcial en el dispositivo móvil, tal como ocurre con las actualizaciones automáticas OTA, o una actualización manual mediante una imagen OTA completa, no es necesario desbloquear el gestor de arranque (o *bootloader*).
- 225.A continuación, es necesario ejecutar desde el ordenador el comando que lleva a cabo la carga del fichero de actualización parcial a través del puerto USB: “adb sideload <nombre_de_fichero>.zip”, donde “<nombre_de_fichero>.zip” corresponde al nombre del fichero ZIP con la actualización parcial a aplicar. Este comando debe ejecutarse directamente desde el directorio donde se descargó dicho fichero.
- 226.Desde Android 6.x este procedimiento sirve tanto para aplicar una imagen OTA parcial no oficial, como una imagen OTA completa oficial (*full OTA image*), mostrada a continuación:

```
C:\> adb devices
List of devices attached
* daemon not running. starting it now at tcp:5037 *
* daemon started successfully *
0111fb177f012345      sideload

C:\> adb sideload 6.0.1_bullhead-ota-mtc20k-531d55c0.zip
opening '6.0.1_bullhead-ota-mtc20k-531d55c0.zip'
connecting...
serving: '6.0.1_bullhead-ota-mtc20k-531d55c0.zip'
Total xfer: 2.00x
```

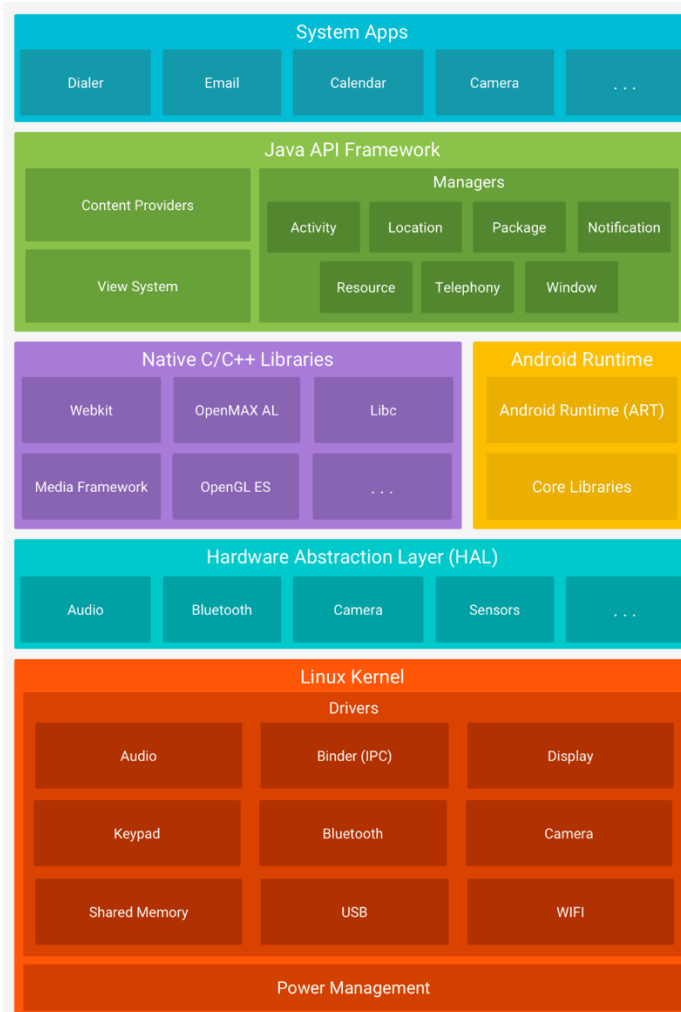
Nota: En algunos casos (dependiendo de las modificaciones realizadas por la actualización y de la versión exacta previa y la versión final de Android) puede ser recomendable adicionalmente, una vez se ha completado la misma, y desde la imagen de recuperación, limpiar la caché del dispositivo móvil a través de la opción del modo de recuperación del gestor de arranque *“wipe cache partition”*.

227. Una vez se ha completado la instalación de la actualización, estado identificado por el mensaje *“Install from ADB complete.”*, se debe seleccionar la opción *“reboot system now”* para reiniciar el dispositivo móvil con la nueva actualización aplicada, proceso que puede llevar algún tiempo.

228. Cuando el dispositivo móvil ha sido actualizado, tras reiniciarlo, ejecutará la nueva versión de Android, conservando los datos de usuario existentes previamente, tal como ocurriría con una actualización automática recibida mediante OTA (vía Wi-Fi o 2/3/4G).

7. MODELO Y ARQUITECTURA DE SEGURIDAD DE ANDROID

229. El modelo o arquitectura de seguridad de Android está basado en el sistema operativo Linux y proporciona adicionalmente numerosas librerías y entornos de ejecución para las aplicaciones móviles [Ref.- 11]:



230. Android intenta aplicar el principio de mínimos privilegios por defecto, donde cada aplicación móvil (o app) únicamente dispone de acceso a sus propios componentes, incrementando así la seguridad general de la plataforma, y limitando las acciones que una app puede realizar sobre otras apps, en el sistema o en su interacción con el usuario.

7.1. MODELO DE PERMISOS DE ANDROID

231. La seguridad más granular de la plataforma Android se basa en un mecanismo de permisos que impone restricciones en las operaciones que un proceso (o app) puede llevar a cabo, incluyendo también restricciones en el acceso a datos (en función de su identificador o URI, *Uniform Resource Identifier*) para los proveedores de contenidos (descritos posteriormente).

232. Se distinguen dos modelos de permisos: en tiempo de instalación y en tiempo de ejecución, que se detallan a continuación.

7.1.1. MODELO DE PERMISOS EN TIEMPO DE INSTALACIÓN

233. El presente apartado describe el modelo de permisos de versiones previas de Android (hasta Android 5.x inclusive), y de aquellas apps que no tienen como versión objetivo Android 6.x o el nivel de API 23. Es decir, las apps que se han sido desarrolladas con el modelo de permisos existente hasta Android 5.x, independientemente de la versión de Android sobre la que ejecuten, harán uso de este modelo.

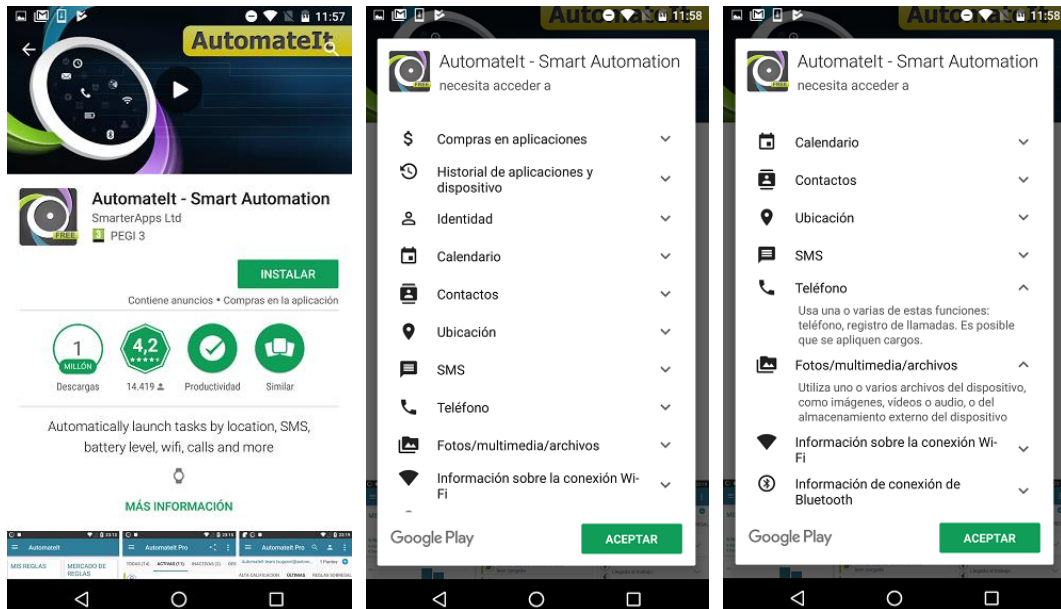
234. Las apps por tanto deben definir y solicitar permiso para acceder a los recursos y datos compartidos en los que están interesadas. El sistema notifica al usuario estos permisos en el momento de la instalación de la app. Una vez el usuario autoriza a una app a disponer de dichos permisos, ésta será instalada y podrá hacer uso de los mismos en cualquier momento durante su ejecución (presente y futuras). En ningún caso se solicitará autorización al usuario durante la ejecución de la app, sino únicamente en el momento de su instalación.

235. Android no proporciona granularidad suficiente para seleccionar únicamente un subconjunto de todos los permisos solicitados por una app y restringir así su funcionalidad. Si se instala una app, ésta dispondrá de acceso a todos los permisos solicitados. Si el usuario no está interesado en proporcionar ciertos permisos a una app, la única opción disponible es no instalar dicha app.

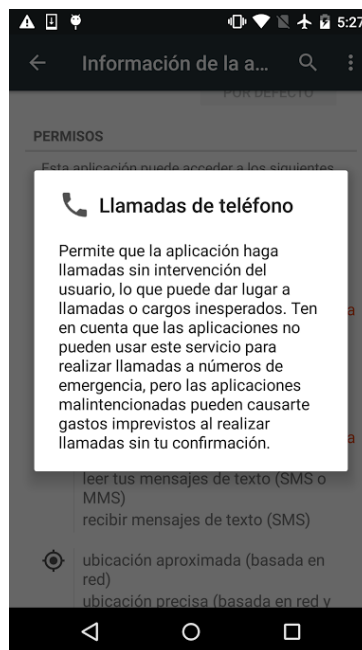
236. Adicionalmente, para ciertos permisos, como el de acceso a Internet, sería deseable disponer de suficiente granularidad en Android para poder autorizar a una app a conectarse a Internet sólo a ciertos sitios web, y no a cualquier destino. Esta funcionalidad no está disponible en el modelo de permisos actual de Android, y las apps con el permiso de acceso a Internet pueden conectarse a cualquier dominio o dirección IP.

237. La única excepción al modelo de permisos general descrito es la asociada a ciertos permisos disponibles para los desarrolladores (como por ejemplo "READ_LOGS", "WRITE_SECURE_SETTINGS", etc.), introducidos en Android 4.2 y que si podían ser habilitados o deshabilitados bajo demanda en cualquier momento y de manera dinámica, mediante el comando "pm grant/revoke", *Package Manager*.

238.El siguiente ejemplo²⁹ muestra los diferentes permisos solicitados durante el proceso de instalación por una app Android concreta, que, aunque ejecutará en la versión 6.0.1 del sistema operativo, no ha sido desarrollada para el nivel 23 de la API. En la aplicación móvil para la descarga de apps de Android, “Play Store”, tras pulsar el botón de instalación en la página de descripción de la app, se solicita la aceptación por parte del usuario de los permisos demandados por la app [Ref.- 623]:

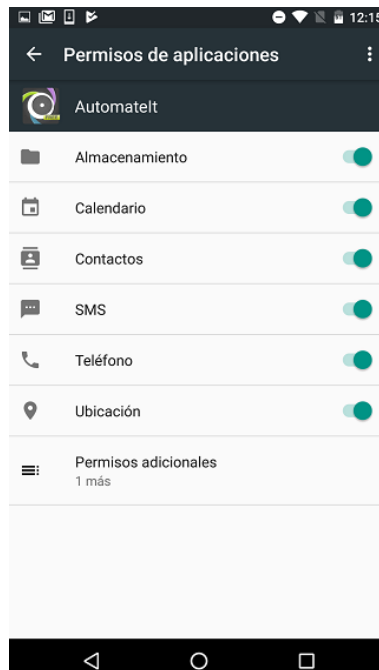


239.En versiones más antiguas de la app “Play Store” que la utilizada en la elaboración de la presente sección de esta guía (9.0.15), al seleccionar de cualquiera de los permisos era posible obtener una descripción breve sobre su propósito (la imagen inferior ilustra la asociada al permiso de acceso al teléfono). Esta información adicional ya no está disponible en versiones más recientes (la captura pertenece a la versión de la app “Play Store” de Android 5.1.1):



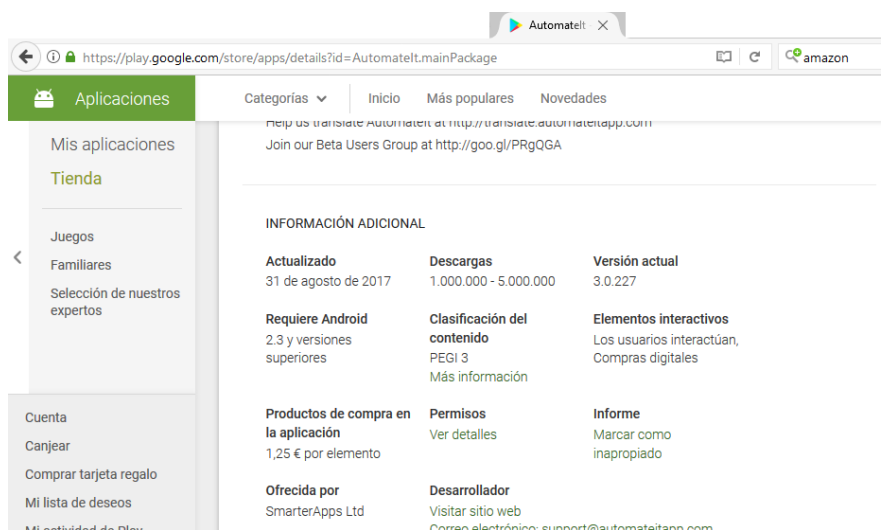
²⁹ Se ha empleado la app "Automatelt" como ejemplo debido al elevado número de permisos que solicita al usuario.

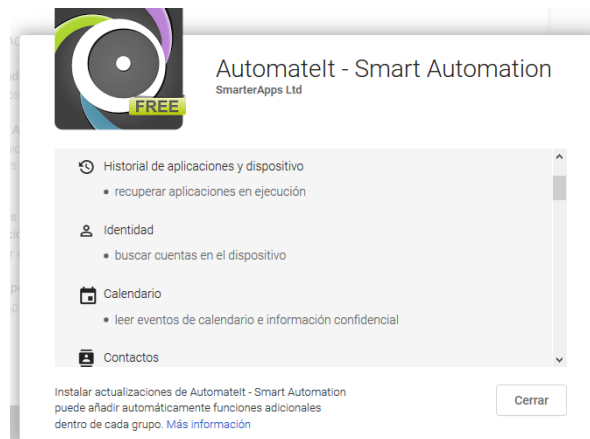
240. Una vez la app ha sido instalada, es posible ver los permisos de los que hace uso desde el menú “Ajustes [Dispositivo] - Aplicaciones”. En Android 6.x desaparecen las listas “Descargadas, En Ejecución, o Todas” existentes en versiones anteriores y se muestra una única lista de aplicaciones. Al seleccionar una aplicación, se abre la ventana “Información de la aplicación” que incluye el campo “Permisos”. Si se selecciona ese campo, se listarán todos los permisos en forma de interruptores que se pueden habilitar/deshabilitar individualmente:



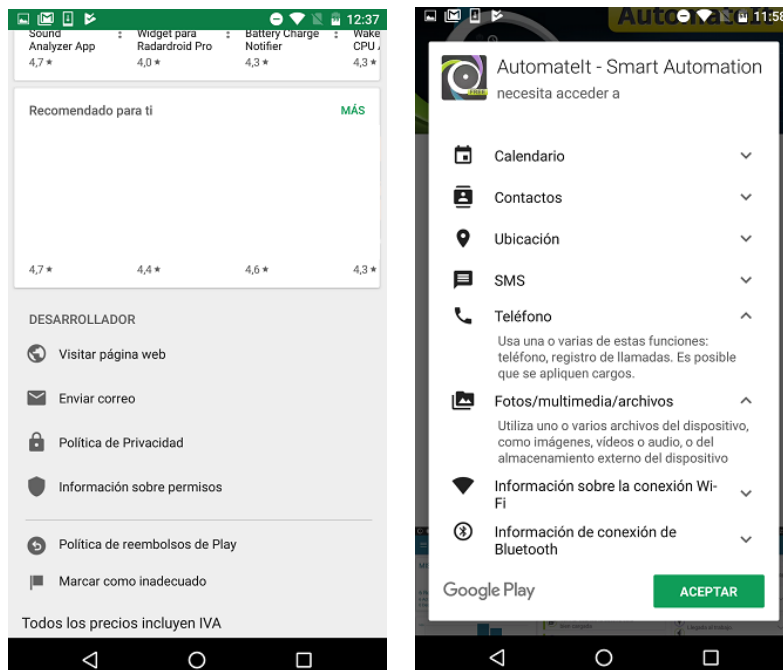
241. Por defecto, las apps no disponen de ningún permiso. Si durante la instalación una app no solicita ningún permiso no quiere decir que (debido a vulnerabilidades en Android) no pueda llevar a cabo acciones que afecten a la privacidad del usuario [Ref.- 55], por ejemplo mediante el envío de mensajes (denominados *intents* en Android) a otras apps, por lo que el usuario debe evaluar minuciosamente la instalación de nuevas apps incluso cuando éstas parecen no requerir ningún permiso.

242. Los permisos requeridos por una app también están disponibles a través de la página web de Google Play, junto a su descripción, que puede ser consultada antes de su instalación. Para ello, es necesario deslizar la barra de desplazamiento hasta la parte inferior y consultar el apartado “Permisos - Ver detalles”:





243. También la app “(Google) Play Store” ofrece la posibilidad de consultar los permisos de la app bajando hasta el apartado “Desarrollador” y pulsando en la opción “Información sobre permisos”:



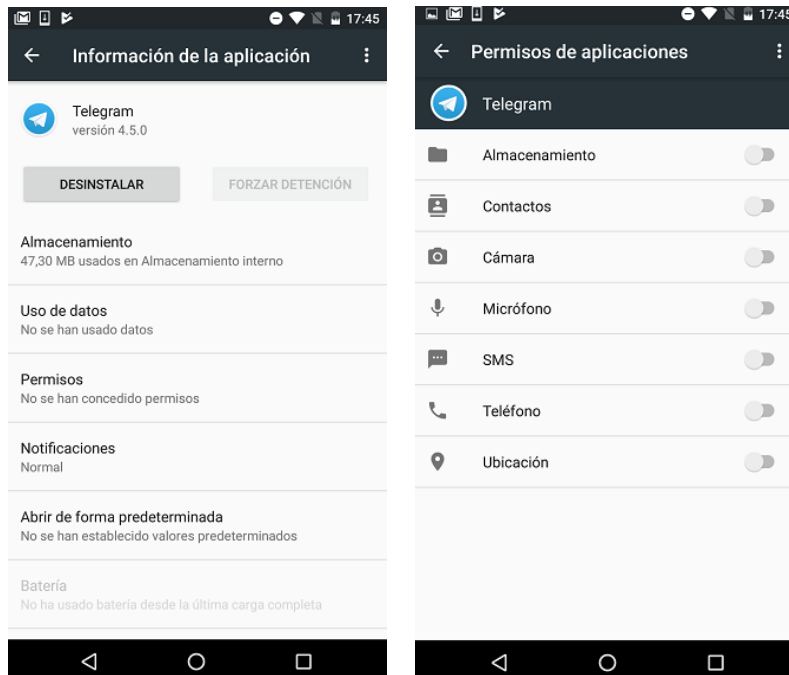
244. Un elevado porcentaje del código dañino (o malware) para Android se distribuye utilizando el código de otras aplicaciones móviles legítimas, que son modificadas y publicadas de nuevo en el mercado oficial de aplicaciones, Google Play, o en mercados de terceros.

245. En otros casos, la app fraudulenta no incorpora ningún código dañino durante la instalación, y éste es añadido al dispositivo móvil posteriormente, en uno de los habituales procesos de actualización de las apps. Este proceso puede hacer uso de vulnerabilidades en Android que no requieren de aprobación por parte del usuario para la instalación de la nueva funcionalidad del código descargado, tal como ya demostró Jon Oberheide con “RootStrap” en el 2010 [Ref.- 225], ejecutando código nativo ARM fuera de la máquina virtual Dalvik.

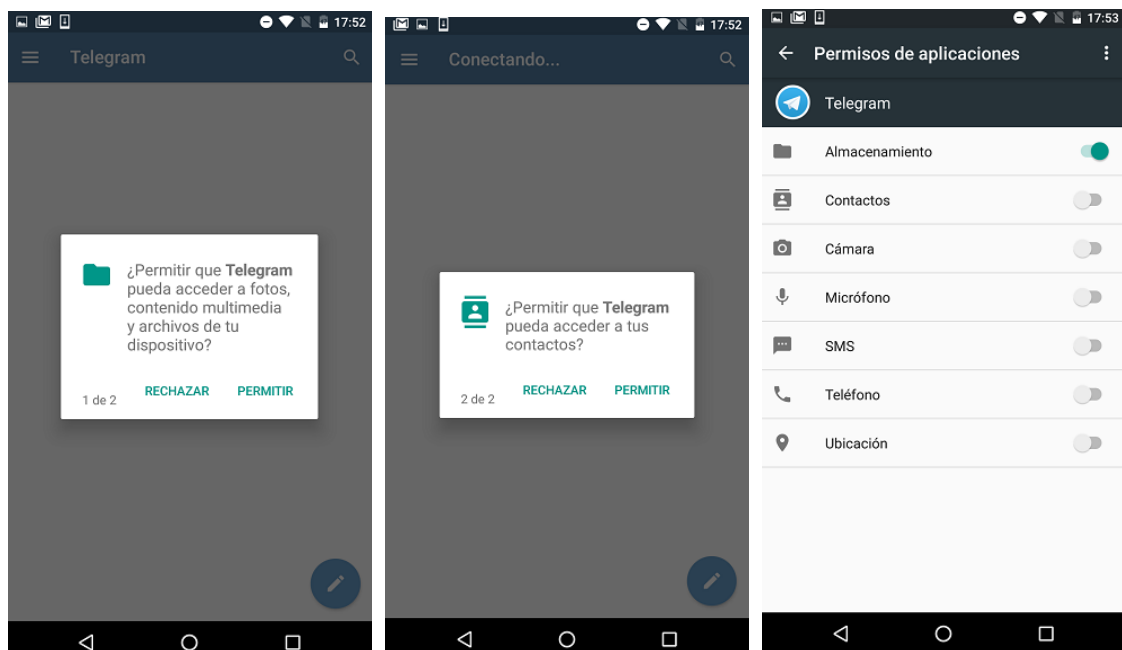
246. Mediante técnicas de ingeniería social es también posible instar al usuario a realizar la actualización de una app maliciosa [Ref.- 126]. Se recomienda por tanto ser muy precavido y evaluar la reputación y los permisos requeridos por el software antes de proceder a instalar cualquier app en el dispositivo móvil.
247. Por otro lado, debe tenerse en cuenta que si una actualización asociada a una app ya instalada requiere disponer de nuevos permisos no solicitados y aprobados por el usuario durante la instalación inicial de la app (o en versiones previas), el usuario será consultado de nuevo para aprobar los nuevos permisos requeridos por la actualización (ver apartado “23.9. Gestión de apps en Android”).
248. Android 5.x estableció un nuevo requisito especificando y asegurando que sólo una app puede definir un permiso personalizado, a menos que esté firmada con el mismo certificado de desarrollador que la app que ya haya definido dicho permiso.
249. Cada app tiene la capacidad de definir cualesquiera permisos personalizados necesite. A partir de Android 5.x, si dos apps definen el mismo permiso personalizado, empleando el mismo nombre, o hacen uso de una librería que define dicho permiso, la instalación de la segunda app con el permiso duplicado se bloqueará. En versiones anteriores de Android, el sistema permitía la instalación de múltiples apps en estas condiciones, y otorgaba el nivel de protección asignado por la primera app que era instalada y que había definido el permiso personalizado.

7.1.2. MODELO DE PERMISOS EN TIEMPO DE EJECUCIÓN

250. Android 6.x, vinculado a la API 23, introduce un nuevo modelo de permisos para las apps, donde los usuarios disponen de la capacidad de gestionar los permisos en tiempo de ejecución de las apps (*runtime permissions*) en lugar de en el momento de instalación de las apps, tal como ocurría en versiones previas de Android [Ref.- 617].
251. Este modelo proporciona un mayor control, visibilidad y granularidad por parte del usuario a la hora de conceder o denegar a las apps acceso a información y servicios. Los permisos pueden ser gestionados individualmente para cada una de las apps instaladas en el dispositivo móvil, y en cualquier momento.
252. Este nuevo modelo de permisos también proporciona al usuario un mejor contexto para comprender el propósito por el que una app solicita un permiso concreto.
253. Las apps que tienen una versión objetivo con un nivel de API igual (o superior) a 23 deben verificar si disponen del permiso antes de hacer uso del mismo, y en caso contrario, solicitarlo al usuario. Es decir, las apps que implementan la API 23 se instalan sin solicitar ningún permiso. Cuando se ejecutan por primera vez y requieren acceder a un recurso controlado por un permiso del sistema, solicitarán al usuario el permiso correspondiente. En este escenario, el usuario puede aceptar o denegar el permiso.
254. Tras la instalación de una app, la misma aparecerá sin ningún permiso de los considerados como “peligrosos” (ver apartado “7.1.3. Permisos normales y peligrosos”) concedido:

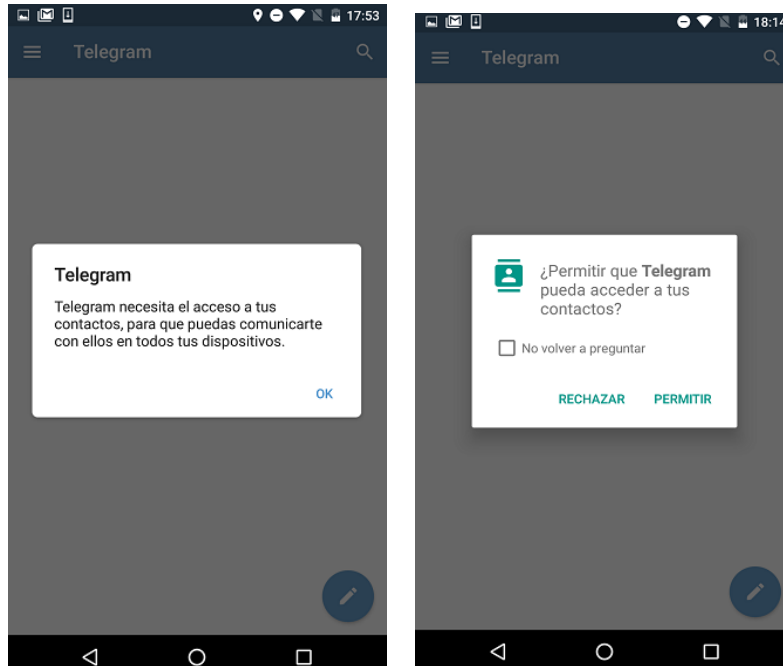


255. Una vez se inicia por primera vez, la app solicitará uno a uno los permisos necesarios cuando se haga uso de ellos en base a su funcionalidad. El usuario puede decidir cuáles quiere otorgar y/o denegar (en el ejemplo que se ilustra a continuación se concede el permiso al almacenamiento compartido, tarjeta SD, pero se rechaza el acceso a los contactos). Esta circunstancia se refleja en los permisos mostrados en los ajustes):



256. A diferencia de lo que ocurre en versiones anteriores de Android, o con aplicaciones que ejecutan en Android 6.x pero implementan una API más antigua que la 23, si una app ve denegado su acceso a un permiso por parte del usuario, su ejecución no terminará, sino que proseguirá, aun sin poder proporcionar la funcionalidad requerida, mostrando un mensaje informativo de la necesidad de otorgar el permiso para poder hacer uso de la funcionalidad en cuestión.

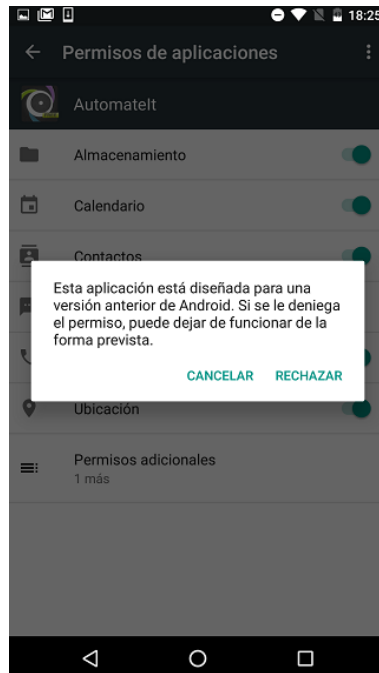
257. Tras reconocerse dicho mensaje pulsando OK, la app solicitará de nuevo el permiso correspondiente. Esta vez incluirá además una opción “No volver a preguntar” que, si se marca, provocará que no se solicite nuevamente el permiso aunque resultase necesario.



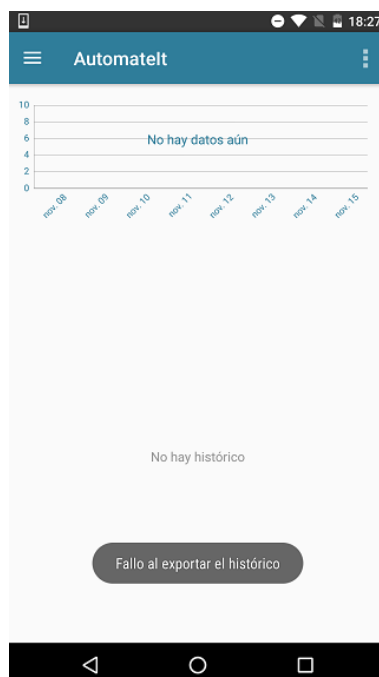
258. Si el usuario desea conceder un permiso ante una circunstancia especial pero no quiere que la app disponga de él permanentemente (por ejemplo, una aplicación de mensajería solicita acceso a la ubicación porque el usuario ha invocado una funcionalidad que la requiere puntualmente), ha de entrar en “Ajustes - [Dispositivo] Aplicaciones - [Nombre de la app] Permisos” y desmarcar los permisos que ya no se desea otorgar a la app.

259. Para las apps que, instalándose sobre Android 6.x, no implementan la API 23, el sistema solicitará al usuario los permisos para la app en tiempo de instalación, siguiendo el modelo antiguo de permisos, y los mostrará en “Ajustes - [Dispositivo] Aplicaciones - [Nombre de la app] Permisos”.

260. Desde dicho menú, el usuario podrá revocar los permisos que considere oportuno. El sistema mostrará un mensaje informando de las posibles consecuencias de esta acción al emplearse el antiguo modelo de permisos:



261. Si una app diseñada para APIs inferiores a la 23 solicita acceso a un recurso controlado por un permiso que el usuario ha revocado, el resultado será un fallo indeterminado o, incluso, una terminación anómala del proceso asociado a la app:



262. Por tanto, ante fallos de una app, se recomienda verificar si los permisos disponibles para ella son los requeridos y, en caso de que falte alguno, habilitarlo y ver si el problema se soluciona.

263. No obstante, no es infrecuente que algunas apps soliciten permisos que no precisan. Por tanto, en aras de la privacidad y la seguridad, se recomienda sopesar la necesidad de habilitar cada permiso y su implicación para el funcionamiento normal de la app.

264. Dentro de las mejores prácticas para los desarrolladores de apps, se recomienda consultar la documentación oficial de Google en relación a los permisos de sistema [Ref.- 618].

7.1.3. PERMISOS NORMALES Y PELIGROSOS

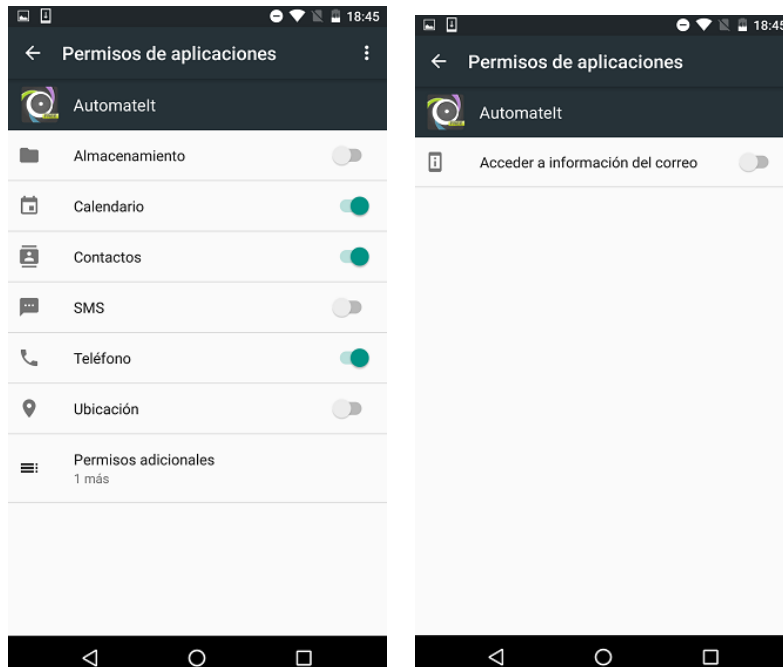
265. Adicionalmente, junto al nuevo modelo de permisos en tiempo de ejecución de Android 6.x, Google introdujo dos categorías de permisos: los permisos peligrosos (*dangerous permissions*) y los permisos estándar (*normal permissions*) [Ref.- 627].
266. Se considera un permiso estándar por parte de Google aquel que, aunque requiera acceso a recursos ajenos al sandbox de la app, no compromete la privacidad del usuario (según Google). El sistema concederá ese permiso de forma automática si la aplicación lo declara en su fichero *manifest* y no consultará al usuario sobre ellos ni se los mostrará en la sección de permisos de la app. Un ejemplo de los permisos que Google cataloga como estándar es el acceso a Internet; otro es BLUETOOTH_ADMIN, que posibilita gestionar el interfaz Bluetooth.
267. Se considera un permiso peligroso (según Google) aquel que concede a la aplicación acceso a datos confidenciales del usuario, o que puede afectar al funcionamiento de otras apps. Los permisos así declarados en el fichero *manifest* de la app deben aprobarse explícitamente por el usuario. Un ejemplo es el acceso a los contactos.
268. Los permisos considerados peligrosos son: almacenamiento, calendario, contactos, SMS, teléfono, ubicación, micrófono y sensores.
269. Puesto que el usuario puede revocar los permisos de una app en cualquier momento, las apps deben chequear si disponen de ellos cada vez que intentan acceder a recursos protegidos por permisos.

7.1.4. PERMISOS SIMPLIFICADOS Y GRUPOS DE PERMISOS DE GOOGLE PLAY

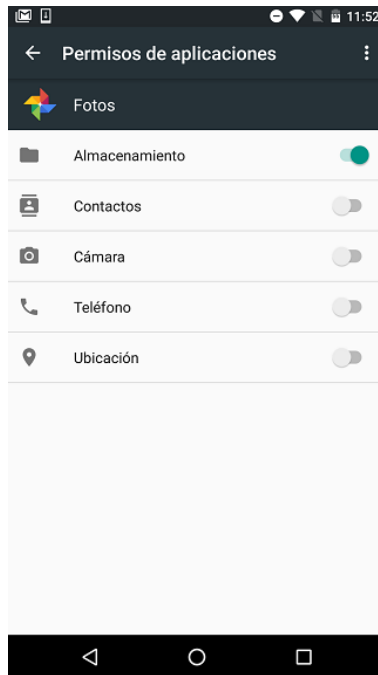
270. En relación al modelo de permisos de Android, Google introdujo una actualización mediante los Servicios de Google Play y la app “Play Store” en junio de 2014, en concreto en la versión 4.8.19³⁰ de “Play Store” (o “Google Play Store”), creando los permisos simplificados (o grupos de permisos) de Android.
271. Este cambio en el modelo de permisos de Android es de aplicación para todas las versiones de Android, desde la versión 4.4 de Android (por la fecha en la que fue introducido), afectando también a las nuevas versiones de Android.
272. Los permisos individuales solicitados por cada app, en lugar de mostrarse a través de Google Play como en versiones previas, se han simplificado y agrupado en función de las capacidades o funciones específicas a las que está asociado cada uno de los permisos, añadiéndose un icono descriptivo asociado, y creándose grupos de permisos relacionados entre sí.
273. El objetivo de esta modificación fue simplificar el interfaz gráfico de usuario (GUI, *Graphical User Interface*) asociado al modelo de permisos de Android, de forma que los usuarios puedan entender más fácilmente qué tipo de capacidades son requeridas por una app en el momento de su instalación. Aproximadamente se han agrupado unos 150 permisos individuales en una docena de categorías o grupos de permisos.
274. Los grupos de permisos, a su vez, son ordenados según los criterios de Google por su criticidad o relevancia, mostrándose en la parte superior los más relevantes y

³⁰ <http://www.androidpolice.com/2014/07/15/google-rolling-out-play-store-v4-8-19-with-paypal-support-simplified-app-permissions-bigger-buttons-and-more-apk-download/#simplified-permission-lists>

disponiéndose de una categoría “Permisos adicionales” en la parte inferior, que engloba el resto de permisos solicitados y no agrupados previamente en los permisos principales [Ref.- 160]. Sin embargo, esta categoría adicional puede incluir también permisos relevantes desde el punto de vista de seguridad, como el acceso a los interfaces Bluetooth y NFC, el acceso al correo, o la capacidad de poder escribir en el historial y en los marcadores o favoritos web:



275. Asimismo, en el caso de las apps de terceros que definen sus propios permisos personalizados, estos también son englobados dentro de la categoría “Permisos adicionales”.
276. Desde el interfaz de usuario, para las apps que no implementen la API 23 de Android 6.x, durante el proceso de instalación de la app, es posible seleccionar los distintos grupos de permisos para ver los permisos individuales solicitados por la app.
277. Igualmente, se pueden consultar los permisos individuales antes de la instalación de una app, desde la app “Play Store” o desde la página web de Google Play, a través de la sección de “Desarrollador”, seleccionando la opción “Información sobre permisos” disponible al final de la página de la app.
278. Asimismo, una vez se ha instalado una app, desde el menú “Ajustes [Dispositivo] - Aplicaciones” es también posible seleccionar la app y en la parte inferior, consultar los permisos individuales solicitados por la misma desde la sección “Permisos”:

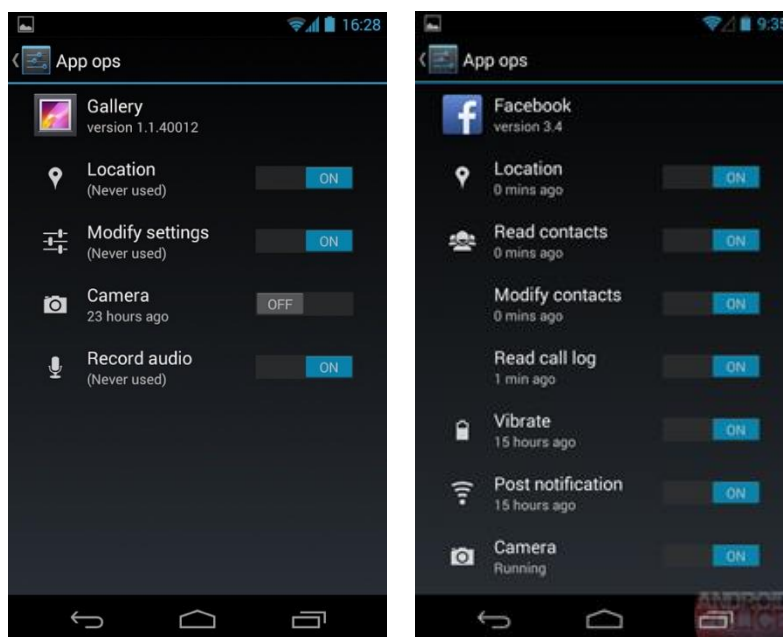


- 279.El problema radica en que la implementación de este nuevo modelo de permisos simplificados introduce nuevas vulnerabilidades de seguridad previamente inexistentes [Ref.- 161].
- 280.Por ejemplo, una app que requiera disponer del permiso para leer SMS, antes solicitaba únicamente el permiso “READ_SMS”, pero en las últimas versiones, aunque solicitará el mismo permiso, se le otorgará el grupo de permisos “SMS”. Al ser instalada, la app obtiene permisos para acceder a todas las capacidades relacionadas con los SMS, incluyendo todos los permisos englobados en dicho grupo, como (potencialmente) el de envío de SMS, aunque el usuario no ha sido consultado sobre (y, por tanto, no ha aprobado) este permiso específicamente [Ref.- 162].
- 281.Por un lado, las apps que ya han sido instaladas y disponen de ciertos permisos, al recibir la siguiente actualización de la app, si ésta requiere de nuevos permisos, obtendrán automáticamente acceso al grupo completo de permisos asociados a cada uno de los permisos individuales de los que ya disponían. Como resultado, obtendrán automáticamente acceso a muchos más permisos de los que solicitaron inicialmente durante su instalación.
- 282.Por otro lado, los grupos de permisos contienen tanto permisos menos relevantes desde el punto de vista de seguridad, como permisos más críticos que son habitualmente utilizados por software malicioso. Por ejemplo, apps que solicitan el permiso de los servicios de localización o ubicación, podrán situar la posición del dispositivo móvil tanto de forma aproximada como más precisa a través del módulo GPS; apps que sólo requerían consultar el listado o registro de llamadas podrán realizar llamadas (incluso sin la intervención del usuario); y apps que solicitaban poder leer contenidos de la tarjeta SD podrán escribir también en ella o incluso formatearla.
- 283.Asimismo, por ejemplo, una app con funcionalidad de linterna (*flashlight*), que previamente requería del permiso para activar el *flash* (o led) de la cámara, al estar este permiso englobado dentro del grupo “Cámara”, ahora también dispondrá de permisos para hacer fotografías, o grabar vídeo y audio.

284. Por último, esta actualización del modelo de permisos de Android otorga por defecto el permiso (existente previamente) de acceso completo a Internet a cualquier app. Es decir, el permiso de acceso a Internet ha sido eliminado de manera efectiva, ya que aunque los desarrolladores de apps tienen que seguir declarando en el fichero *manifest* que la app requiere dicho permiso, los usuarios no verán la solicitud de este permiso durante el proceso de instalación de la app (se puede mostrar en las vistas detalladas de permisos englobado dentro de la categoría “Otros”). Asimismo, las apps que no disponían de este permiso anteriormente, lo pueden obtener automáticamente y sin la aprobación del usuario en la siguiente actualización de la app.
285. Se recomienda por tanto analizar minuciosamente cada uno de los permisos individuales solicitados por las apps antes del proceso de instalación, durante el mismo, y al concluir éste, ignorando la simplificación en grupos de permisos realizada por Google.
286. Si una app solicita en su fichero *manifest* un permiso “peligroso” y no tiene aún ningún permiso perteneciente a ese grupo, el sistema pedirá al usuario confirmación para conceder acceso al grupo, no al permiso particular. Por ejemplo, si una app solicita el permiso `READ_CONTACTS`, el permiso solicitará acceso a los contactos.
287. Si una app solicita en su fichero *manifest* un permiso “peligroso” y ya dispone de algún permiso perteneciente a ese grupo, el sistema le otorgará el permiso automáticamente sin solicitar autorización al usuario. En el caso anterior, si una app obtuvo el permiso `READ_CONTACTS` y posteriormente requiere el permiso `WRITE_CONTACTS`, Android se lo concederá automáticamente.
288. Esta falta de granularidad supone un riesgo para la privacidad del usuario y la seguridad del dispositivo, pues una app que, en principio, solo requeriría acceso de lectura de la tarjeta SD, podría llegar a formatear la misma sin que el usuario pudiera evitarlo.
289. Adicionalmente, se recomienda llevar a cabo este mismo análisis minucioso para cada una de las actualizaciones recibidas para las apps ya instaladas en el dispositivo móvil, habiendo deshabilitado previamente las actualizaciones automáticas de las apps (ver apartado “23.9.2. Actualización automática de apps”), con el objetivo de evitar que una actualización de cualquier app adquiera nuevos permisos sin solicitárselos al usuario.
290. Por último, se debe asumir que actualmente cualquier app de Android dispone de capacidades plenas para conectarse y acceder a Internet.
291. Debe tenerse en cuenta que la simplificación del interfaz de usuario para la aprobación de los permisos requeridos por una app sólo afecta a las apps instaladas desde Google Play. La instalación de apps directamente mediante su fichero APK asociado todavía mostrará la lista individualizada de permisos, qué deberá ser aprobada por el usuario.
292. Se dispone de más información sobre los grupos de permisos, así como de los permisos individuales englobados en cada grupo, su propósito y capacidades, en la documentación oficial de Google [Ref.- 23].

7.1.5. APP OPS

293. “App Ops” es un sistema granular de control o gestión de los permisos de las apps en Android, oculto por defecto, y que fue introducido por Google en Android 4.3 [Ref.- 127], hasta la versión 4.4.2 [Ref.- 161].
294. La principal ventaja de “App Ops” es que podía ser usado para gestionar los permisos tras la instalación de cualquier app, en lugar de tener que aceptar o denegar los permisos en el momento de la instalación de la app, tal y como ocurre por defecto en el modelo de permisos original de Android. Esta funcionalidad permitía revocar permisos individualmente y para cada app.
295. Sin embargo, sólo es posible configurar cada permiso una vez que éste ha sido utilizado, en lugar de proporcionarse desde el inicio la lista completa de permisos de la app, por ejemplo, obtenida de su fichero “AndroidManifest.xml”. Por otro lado, no se genera ninguna notificación hacia el usuario cuando un permiso solicitado por una app es denegado, por ejemplo, explicando el motivo de porqué no es posible hacer uso de dicho permiso.
296. Para poder hacer uso de “App Ops” era necesario crear un acceso directo personalizado que apuntase a la actividad asociada a “Ajustes - App Ops”. La creación de este acceso directo se puede llevar a cabo a través de otra app creada específicamente para este propósito, como por ejemplo la app llamada “AppOps” [Ref.- 131] (entre otras³¹).
297. “App Ops” proporcionaba controles granulares para permisos clasificados en diferentes categorías, como los servicios de localización, permisos personales, de mensajería o del dispositivo. Por ejemplo, permitía habilitar y deshabilitar la modificación de los ajustes, la cámara, la posibilidad de grabar audio del micrófono del dispositivo móvil, notificaciones, vibraciones del teléfono, lectura y modificación de los contactos, lectura del registro de llamadas, etc (imágenes correspondientes a Android 4.4.x):



³¹ <https://play.google.com/store/apps/details?id=com.pixelmonster.AppOps&hl=en>

298. “App Ops” permitía también ver la última vez que cada permiso había sido utilizado.
299. Posteriormente, en Android 4.4, “App Ops” seguía disponible y añadía capacidades para gestionar más permisos (como por ejemplo la capacidad de una app de despertar al dispositivo móvil, “keep awake”) y una nueva categoría asociada a contenidos multimedia [Ref.- 128].
300. Sin embargo, finalmente “App Ops” fue eliminada por Google en la versión 4.4.2 de Android [Ref.- 161], confirmando su carácter experimental y el riesgo de que algunas apps dejaran de funcionar correctamente (ya que las apps esperaban disponer de los permisos solicitados una vez han sido instaladas y aprobadas por el usuario, en base al modelo inicial de permisos de Android).
301. Actualmente, sólo puede hacerse uso de “App Ops” en dispositivos móviles Android *rooteados* (por ejemplo, mediante un módulo Xposed denominado AppOpsXposed³²).
302. En resumen, “App Ops” fue el precursor en Android 4.x del nuevo modelo de permisos en tiempo de ejecución que fue finalmente incorporado en Android 6.x (ver apartado “7.1.2. Modelo de Permisos en tiempo de ejecución”).

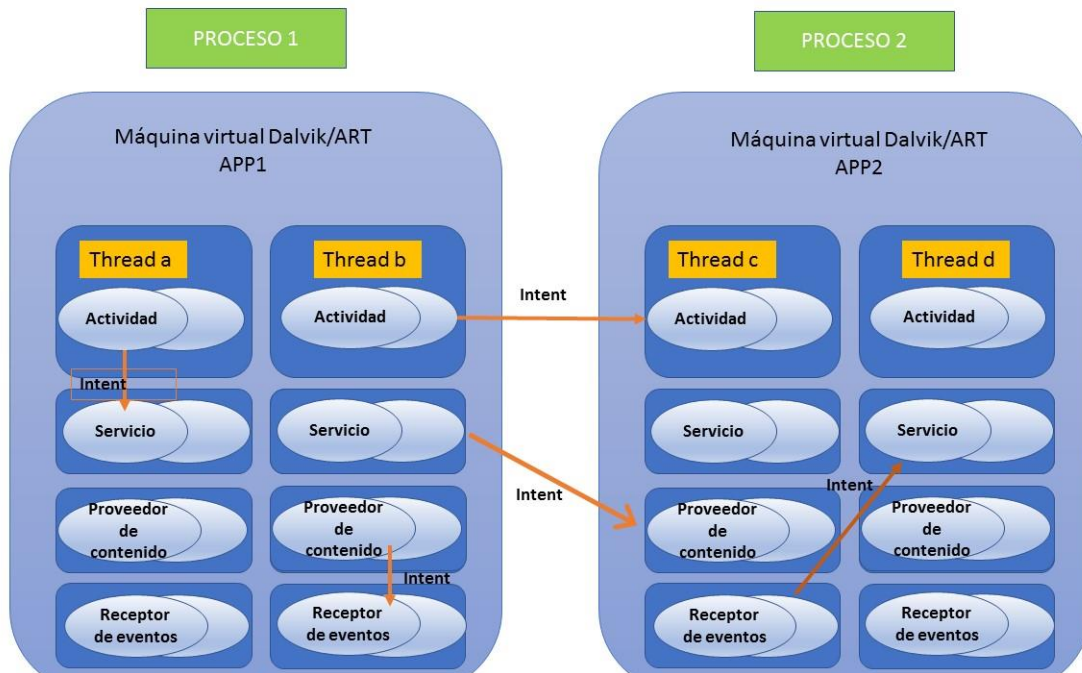
7.2. SANDBOX DE EJECUCIÓN DE LAS APPS

303. Las apps en Android ejecutan de forma independiente en su propio entorno de ejecución o *sandbox*³³ [Ref.- 16]. Cada aplicación móvil (o app) está asociada a un usuario diferente del sistema operativo Linux.
304. En el momento de su instalación, Android asigna a cada app un identificador de usuario único (UID/GID, User ID y Group ID; ID en adelante) a nivel de sistema operativo, y asigna todos los ficheros de la app a dicho ID. De esta forma, sólo la app tendrá acceso a sus ficheros asociados.
305. El ID es asignado y gestionado por Android y las apps no tienen conocimiento del mismo.
306. Excepcionalmente una app puede crear datos (directorios y ficheros) y asignarles permisos de lectura y/o escritura globales, de forma que cualquier otra app pueda acceder a ellos.
307. Cada app ejecutada es un proceso (Linux) independiente a nivel de sistema operativo. El proceso es iniciado cuando cualquiera de los componentes de la app necesita ejecutarse, y es finalizado al no utilizarse más la app o durante las tareas específicas de gestión (y liberación) de memoria del sistema operativo.
308. Cada proceso tiene asignada su propia máquina virtual (VM, *Virtual Machine*) Dalvik, por lo que el código de cada app ejecuta de manera aislada al resto de apps.
309. Las apps pueden compartir datos con otras apps a través de la compartición de un mismo ID (si han sido creadas por el mismo desarrollador), y acceder a servicios del sistema operativo mediante la solicitud de permisos para interactuar con otros componentes y datos del sistema, como la lista de contactos del usuario, los mensajes SMS, la tarjeta de memoria externa, la cámara, el interfaz Bluetooth, disponer de acceso a Internet, el interfaz Wi-Fi, poder realizar llamadas de voz, etc.

³² <http://www.howtogeek.com/177915/how-to-restore-access-to-app-ops-in-android-4.4.2/>

³³ <https://source.android.com/devices/tech/security/index.html>

310. La lista de permisos disponibles en Android está disponible en la definición del fichero *manifest* (o manifiesto, descrito posteriormente) donde se especifican todos los permisos requeridos [Ref.- 23].
311. Las apps que comparten un mismo ID tienen acceso a los mismos ficheros, pueden incluso ejecutar en el mismo proceso y compartir la misma máquina virtual Dalvik. Para ello deben haber sido firmadas con el mismo certificado digital, asociado a su desarrollador, y desde el punto de vista de seguridad, podrían considerarse la misma app.
312. Las apps de Android pueden estar constituidas por diferentes componentes, que permiten la interacción de la app con el sistema y con el usuario, existiendo cuatro tipos de componentes: actividades (*activities*), servicios (*services*), proveedores de contenidos (*content providers*) y receptores de anuncios o eventos (*broadcast receivers*) [Ref.- 16].
313. Los mensajes asíncronos de notificación o solicitud de peticiones entre componentes (dentro de la misma o entre distintas apps) para que se lleve a cabo una acción se denominan *intents*.

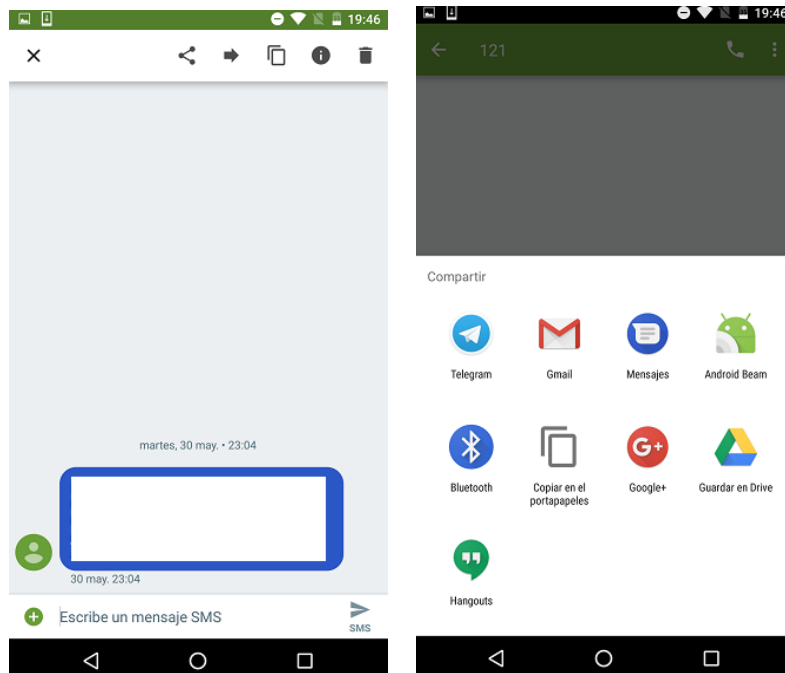


314. Cada app de Android dispone de un fichero de definición, o *manifest* ("AndroidManifest.xml") [Ref.- 105][Ref.- 18], que contiene información sobre los diferentes componentes que constituyen la app. Adicionalmente, el *manifest* incluye los permisos que requiere la app (por ejemplo, acceso a Internet, acceso a la lista de contactos, etc.), las librerías (o APIs, *Application Programming Interface*) empleadas por la app, tanto de sistema como externas (por ejemplo, la librería de Google Maps), o los elementos o capacidades hardware y software empleados por la app (ej. cámara, interfaz Bluetooth, pantalla táctil, etc.).
315. Estos requisitos hardware y software pueden ser empleados para decidir en qué dispositivos móviles puede instalarse y ejecutar una app en función de sus necesidades, principalmente desde Google Play. Los requisitos pueden ser definidos como necesarios o requeridos, u opcionales, en cuyo caso la app podrá ser instalada pero no hará uso de la funcionalidad asociada al requisito no disponible, como por ejemplo, la cámara.

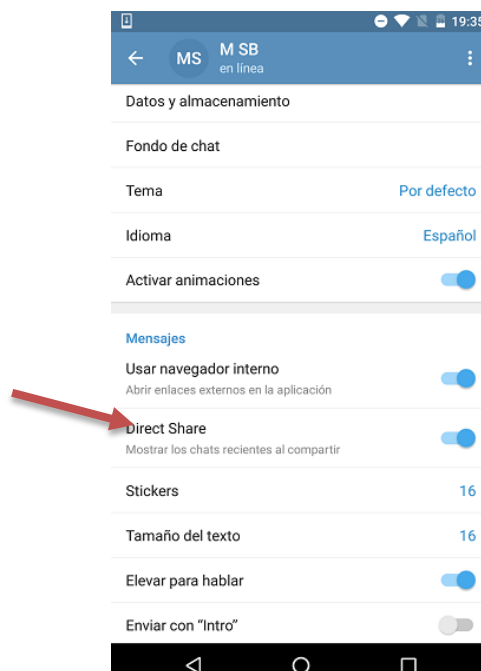
316. Adicionalmente a los permisos estándar [Ref.- 23], existen una serie de permisos que requieren disponer de un nivel de protección elevado (*protectionLevel*) y que están disponibles únicamente para las apps existentes en la imagen de sistema de Android o que han sido firmadas con los mismos certificados que éstas. [Ref.- 105].
317. Las librerías de sistema, denominadas nivel de API (o API level) [Ref.- 19], e identificadas por su número o versión, están asociadas a la versión de Android. Por ejemplo, el nivel de API 23 corresponde a la versión 6.0 de Android (“Marshmallow”).
318. Adicionalmente al código, las apps disponen de recursos (definidos mediante ficheros XML) asociados principalmente a la parte visual o interfaz gráfico de la app, es decir, imágenes, ficheros de audio, contenidos en diferentes idiomas, etc.
319. Con el objetivo de incrementar el modelo y los mecanismos de seguridad disponibles en Android por defecto, la NSA publicó en enero de 2012 una versión de Android restringida, denominada SE Android, y equivalente en filosofía y funcionalidad a SELinux para las plataformas Linux estándar [Ref.- 106].
320. Security Enhanced Android, o SE Android, mejora la seguridad de Android limitando el daño que puede infringir un código dañino, o una potencial vulnerabilidad de seguridad, que afecte al dispositivo móvil, así como añadiendo capacidades para aislar las apps, ficheros y otros componentes entre sí.
321. Posteriormente, las capacidades de SE Android fueron integradas en la plataforma móvil estándar, tal como se describe en el apartado “7.7. SELinux en Android”.

7.3. DIRECT SHARE

322. A través de “Direct Share” las apps pueden publicar sus capacidades para recibir datos de otras apps, que son expuestas al resto del sistema (y al usuario) a través del menú de compartición (o Share). Esta funcionalidad permite que otras apps puedan interactuar con los componentes de la app objetivo (o *target*) que publica sus capacidades, por ejemplo, lanzando una actividad y enviándole datos.
323. La app que quiere ser un objetivo con el que otras apps puedan compartir datos debe declarar el servicio de compartición asociado en su fichero *manifest*, solicitar el permiso `BIND_CHOOSER_TARGET_SERVICE` y crear un “<intent-filter>” con la acción `SERVICE_INTERFACE` [Ref.- 603].
324. Para hacer uso de la compartición de datos vía “Direct Share”, al seleccionar un elemento susceptible de ser compartido, se mostrará la opción marcada con un grafo de tres puntos, el cual, al ser seleccionado, desplegará un menú con los iconos de las aplicaciones (o del contacto concreto dentro de esa aplicación) capaces de recibir ese elemento (o datos):



325. En Android 6.x no existe la posibilidad de deshabilitar la funcionalidad “Direct Share” de forma global. Queda a discreción de la aplicación si desea añadir en sus ajustes propios este servicio, como ilustra la siguiente imagen:



326. Existen múltiples aplicaciones que implementan la posibilidad de configurar (incluyendo deshabilitar por completo) la función “Direct Share”, pero todas ellas son apps de orígenes desconocidos, por lo que no se aconseja su instalación. También es posible controlar el comportamiento de la función “Direct Share” a través de un dispositivo móvil rooteado, lo cual, además de no estar soportado, está totalmente desaconsejado desde el punto de vista de seguridad.

327. De forma temporal, una opción para eliminar del menú “Direct Share” determinados contactos o aplicaciones es eliminar el permiso de acceso a “contactos” de la app en cuestión.

328. Se dispone de un ejemplo de implementación de una app que emplea la característica “Direct Share” en la documentación oficial de Google para desarrolladores [Ref.- 17].

7.4. ART (ANDROID RUNTIME)

329. En versiones anteriores a Android 5.x (Lollipop), las apps para Android, que están desarrolladas en el lenguaje de programación Java, ejecutaban sobre una máquina virtual (VM, *Virtual Machine*) Java ligera denominada Dalvik [Ref.- 16].

330. La máquina virtual Dalvik se optimizó para su utilización en dispositivos móviles, con un consumo eficiente de memoria y de recursos. Dalvik ejecuta ficheros en formato Dalvik Executable (.dex), o DEX, por lo que en el proceso de desarrollo el código fuente Java (ficheros “.java”, asociado habitualmente a ficheros “.class”, Java *bytecode*) de las apps de Android es convertido al formato DEX, Dalvik *bytecode* (mediante la herramienta “dx”).

331. Android 4.4 (KitKat) introdujo el nuevo entorno de ejecución ART (*Android RunTime*) como sustituto de Dalvik [Ref.- 168], pero todavía de manera experimental y no habilitado por defecto. En Android 5.x, ART se convierte en el entorno de ejecución por defecto, sustituyendo a Dalvik.

332. ART no es compatible con binarios en el formato DEX original, y utiliza dos formatos de fichero: “.oat” y “.art” [Ref.- 196].

333. Algunas de las principales ventajas de ART frente a Dalvik es que hace uso de una técnica conocida como compilación AOT (*Ahead of Time*), que mejora el rendimiento de la ejecución de las apps, incorpora un proceso de recolección de memoria mejorado (GC, *Garbage Collector*), y otras mejoras de depuración [Ref.- 503].

334. La técnica AOT, además de aplicar optimizaciones en el uso del procesador (o CPU) y en la limpieza de procesos en memoria, precompila las aplicaciones para evitar que deba realizarse la traducción del *bytecode* DEX al ensamblador correspondiente al procesador del dispositivo móvil (ARM, Intel x86 o x64, etc.) en tiempo de ejecución. De ahí que los dispositivos móviles con Android 5.x requieran disponer de más espacio de almacenamiento asignado a los binarios optimizados de las apps, disponiendo por tanto de algo menos de espacio libre para los datos de usuario. Este proceso de precompilación de apps tiene lugar durante el primer arranque tras instalar o actualizar el sistema operativo (o posteriormente durante la instalación individual de las aplicaciones), y es por ello que se muestra el mensaje de optimización de aplicaciones cuando se actualiza la versión de Android.

335. Las herramientas de desarrollo de software de Android (Android SDK, *Software Development Kit*, o Android SDK Tools, y Android Studio³⁴ [Ref.- 22]) generan las apps para Android, o paquetes Android, en un único archivo o contenedor con extensión “.apk” (*Android PackAge*).

336. Adicionalmente al código Java, Android permite el desarrollo de aplicaciones nativas (ARM) usando C/C++, mediante el Android NDK (*Native Development Kit*), o híbridas, es decir, aquellas que contienen tanto código Java como código nativo (y hacen uso del JNI, *Java Native Interface*).

³⁴ <http://developer.android.com/sdk/index.html>

337. La mayoría de apps que ejecutaban anteriormente en Dalvik podrán ejecutar directamente en ART, salvo aquellas que hacen uso del JNI para ejecutar código nativo C/C++ (o ensamblador), hacen uso de técnicas de ofuscación, u otras técnicas de bajo nivel de limpieza de la memoria³⁵.

7.5. INSTALACIÓN DE APPS (DE ORÍGENES DESCONOCIDOS) EN ANDROID

338. Se denomina aplicación móvil de “orígenes desconocidos” a una app que se instala en el dispositivo móvil empleando un canal diferente al oficial, es decir, al asociado a Google Play. Entre ellas, se incluyen las apps que se instalan a través de un fichero APK descargado directamente desde una página web o mensaje, que se cargan en el dispositivo a través de ADB(mediante comandos como “adb sideload” o “adb install”), o que se instalan a través de un mercado de apps de Android distinto al oficial.

339. Todas las apps para Android deben ser firmadas digitalmente por su desarrollador mediante un certificado digital, siendo por tanto posible identificar (teóricamente) al desarrollador de cualquier app oficial (ver apartado “7.6. Firma digital de apps en Android”).

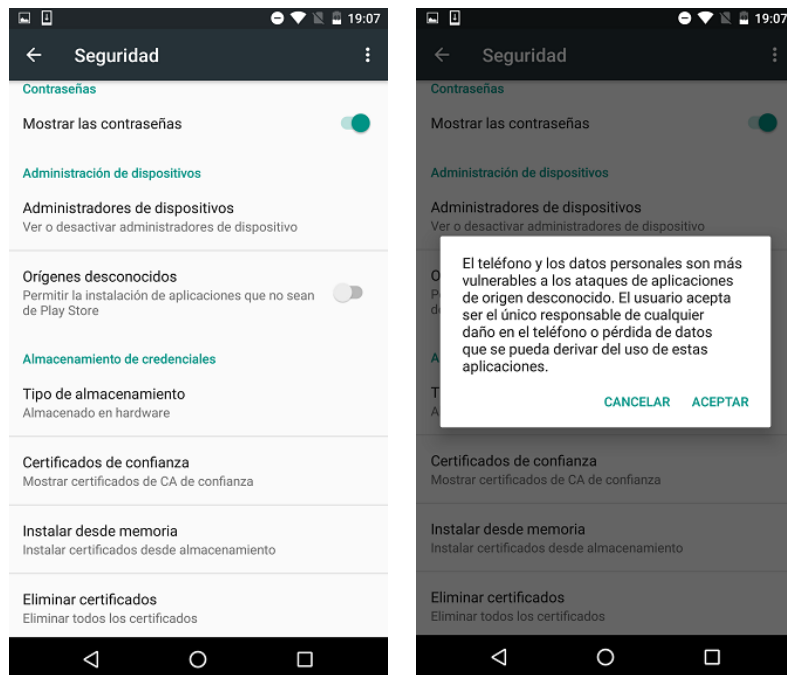
340. La firma de las apps es empleada adicionalmente por Android para establecer permisos de operaciones entre apps y distintos niveles de protección [Ref.- 105] (según el fichero *manifest*), y para permitir a las apps compartir su ID (si han sido programadas y firmadas por el mismo desarrollador).

341. El módulo estándar de instalación de apps de Android (install y Package Manager) verifica mediante certificados digitales que las apps oficiales, es decir, que provienen de Google Play, han sido firmadas convenientemente por su desarrollador.

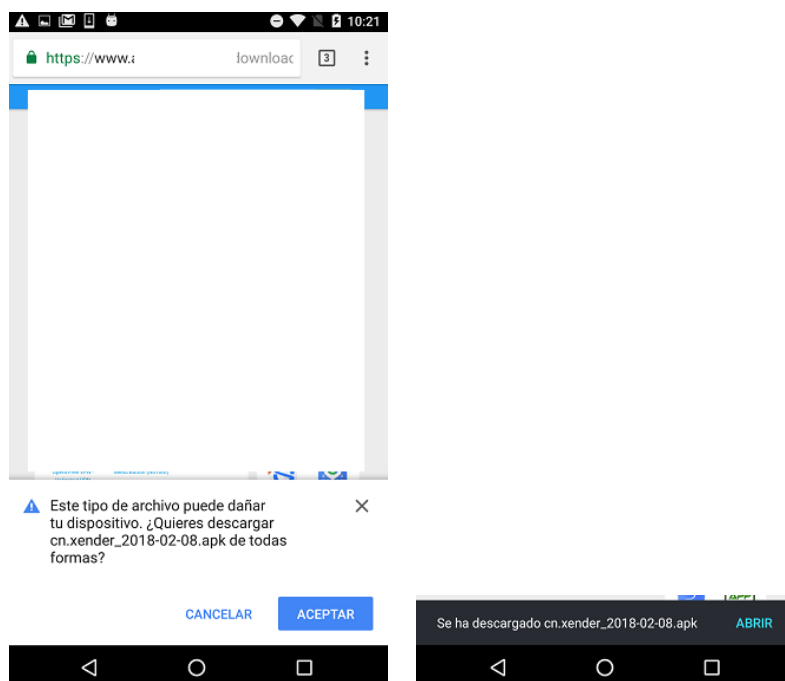
342. Adicionalmente, es posible configurar el dispositivo móvil para permitir la instalación de apps no oficiales (no provenientes de Google Play) sin para ello ser necesario realizar el proceso de *rooting* sobre el dispositivo móvil.

343. Para permitir la instalación de cualquier app, incluso proveniente de fuentes que no son de confianza, simplemente es necesario eliminar las comprobaciones de seguridad asociadas en Android mediante la opción del menú “Ajustes [Personal] - Seguridad [Administración de dispositivos] - Orígenes desconocidos”:

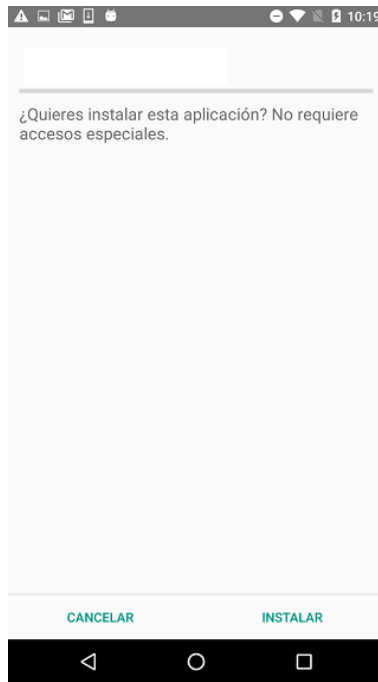
³⁵ <https://developer.android.com/guide/practices/verifying-apps-art.html>



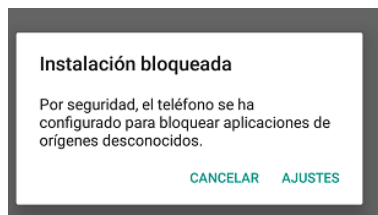
344. En ese estado, cuando se intenta descargar una app directamente desde una página web, Android mostrará un mensaje de advertencia al usuario:



345. Si la opción “Orígenes desconocidos” está activada, cuando se seleccione el nombre del fichero descargado (o se pulse en “Abrir”) se mostrará un mensaje solicitando confirmación al usuario para instalar la app:



346. En caso de que la opción “Orígenes desconocidos” no esté habilitada en el dispositivo móvil, se bloqueará su instalación:



347. Desde el punto de vista de seguridad y con el objetivo de evitar la instalación de apps de fuentes u orígenes desconocidos, o que no son de confianza, se recomienda no habilitar esta opción, tal como advierte el mensaje mostrado por Android.

7.6. FIRMA DIGITAL DE APPS EN ANDROID

348. Para que una app sea considerada válida y pueda ser distribuida oficialmente a través de Google Play debe haber sido firmada digitalmente por su desarrollador [Ref.- 28].

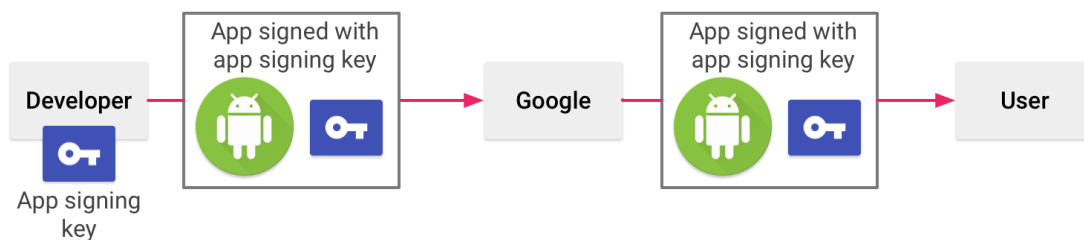
349. Sin embargo, Android no realiza ninguna verificación adicional sobre la seguridad de la app o la firma digital (adicionalmente a las especificadas en el apartado “23.8. Verificación de seguridad de las apps: Google Play Protect”), salvo comprobar la fecha de expiración del certificado asociado a la firma en el momento de la instalación de la app³⁶, permitiéndose certificados auto-firmados y no generados o validados por ninguna autoridad certificadora (o CA).

350. Por tanto, la firma digital de las apps en Android no evita que las mismas contengan vulnerabilidades de seguridad o código malicioso. La firma únicamente permite vincular (teóricamente) la app a su desarrollador, asegura su integridad frente a modificaciones, se emplea para las actualizaciones de la app, verificando que el nuevo código proviene del mismo desarrollador (ha sido firmado por el mismo certificado digital), permite definir permisos especiales basados en la firma de la app (*signature permissions*), y en

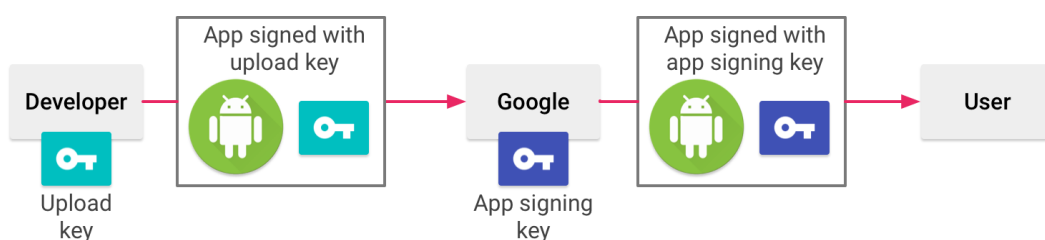
³⁶ Existen referencias confirmando la posibilidad de instalar apps incluso con certificados expirados [Ref.- 26].

algunos escenarios como la compartición del ID entre apps, define el nivel de privilegios de ejecución de la app con respecto a otras apps, permitiéndolas compartir datos entre sí, es decir, estableciendo relaciones de confianza entre apps (del mismo desarrollador).

351. La vinculación entre la app y el desarrollador no ofrece fiabilidad desde el punto de vista de seguridad, ya que al permitirse emplear certificados auto-firmados, los mismos pueden contener información que no está asociada al desarrollador real de la app. Es decir, la firma de una app no permite necesariamente identificar a su desarrollador real.
352. Las apps de Android se distribuyen a través de ficheros APK (*Android PackAge*), una extensión del formato de paquetes Java JAR (*Java ARchive*). Por tanto, las apps hacen uso de capacidades similares a las existentes para firmar ficheros JAR para la firma de los paquetes o ficheros APK [Ref.- 44] [Ref.- 200].
353. La firma de apps no es empleada (como sí puede ser el caso en aplicaciones Java) para la verificación de la integridad (es decir, la firma) de segmentos o porciones de código durante la ejecución de la app. Los controles en tiempo de ejecución de Android se basan en los UIDs/GIDs de los procesos de Linux asociados a la app [Ref.- 26].
354. La firma de las apps es también empleada para permitir la instalación de actualizaciones de las apps, confirmándose que provienen del mismo desarrollador.



355. La imagen superior muestra el modelo tradicional dónde la firma de apps se lleva a cabo mediante un keystore propio al desarrollador de la misma.
356. Existe una variante para el manejo de la firma de aplicaciones consistente en delegar la gestión y custodia de la clave (o certificado) a Google [Ref.- 248]. Esta opción, que emplea la herramienta Play Encrypt Private Key proporcionada por Google Play, está desaconsejada desde el punto de vista de seguridad, pues implica que el desarrollador pierde parte del control sobre su clave (o certificado) de firma.
357. Si se emplea el método de gestión de claves de Google, se requerirá, además de la clave (o certificado) de firma de la app, una clave que se conoce como “de subida” (o *upload*), la cual debe ser registrada en Google con anterioridad a la inclusión de la app en Google Play. Durante el proceso de subida o publicación de la app en Google Play, se utilizará la clave de subida para verificar la identidad del desarrollador de la app. La protección de esta clave de subida es responsabilidad del desarrollador, por lo que, si se ve comprometida, éste debe contactar con Google para revocarla.
358. La imagen inferior muestra el nuevo modelo dónde la firma de apps se lleva a cabo mediante un keystore gestionado por Google.



359. Las apps de sistema han sido firmadas empleando un conjunto de claves asociadas a la plataforma o sistema, pertenecientes a Google (en el caso de las apps por defecto de Android y de los dispositivos móviles Nexus o Pixel) o a los fabricantes de dispositivos móviles u operadores de telefonía móvil (en el caso de los dispositivos móviles con una versión modificada de Android, incluyendo las apps propietarias que estos han incluido).

7.7. SELINUX EN ANDROID

360. El modelo de seguridad de Android se basa parcialmente en la utilización de contenedores (o *sandboxes*) para cada aplicación móvil (o app). La implementación previa a la versión 4.3 de Android empleaba un identificador de usuario (UID/GID) único de Linux, generado en el momento de la instalación de la app, para restringir el entorno de ejecución de cada app (ver apartado “7.2. Sandbox de ejecución de las apps”). Sin embargo, a partir de la versión 4.3 de Android, se emplea también SELinux (Security-Enhanced Linux) para restringir los límites y capacidades asociadas a una app y a su contenedor [Ref.- 106].

361. SELinux proporciona soporte en Android para un modelo de seguridad conocido como MAC (*Mandatory Access Control*), frente al modelo de seguridad estándar y tradicional de Unix/Linux, conocido como DAC (*Discretionary Access Control*), junto a la definición asociada de políticas de seguridad.

362. Como ya se mencionó brevemente en el apartado “4.6. Android 4.3”, las capacidades MAC de SELinux en Android se pueden emplear en todos los procesos, tanto los asociados a las apps como los procesos de sistema que ejecutan como root, pero su implementación es dependiente de la versión de Android.

363. SELinux establece una serie de requisitos de seguridad que controlan los recursos accesibles por un proceso. Cada recurso (fichero, directorio, puerto, proceso, etc.) lleva asociada una etiqueta (o *label*), que también se denomina *contexto* en SELinux.

364. En Android 4.3 se hace uso de SELinux en modo permisivo o *permissive mode*, donde únicamente las acciones no legítimas son registradas por el kernel, pero no bloqueadas.

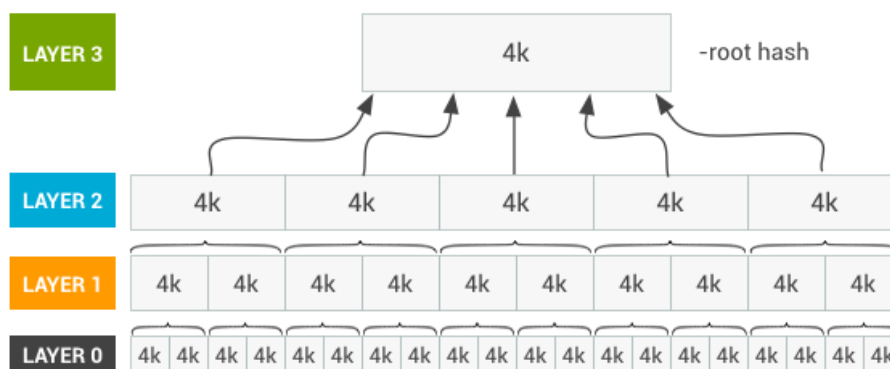
365. En Android 4.4 se hace uso de SELinux en modo obligatorio o *enforcing mode* parcialmente, es decir, sólo para un conjunto crítico de procesos o dominios de sistema (installd, netd, vold y zygote), en el que todas las acciones no legítimas son bloqueadas y registradas por el kernel. Para el resto de procesos o dominios, SELinux en Android 4.4 sigue actuando en modo permisivo, como en el caso de Android 4.3.

366. En Android 5.0 se hace uso de SELinux en modo obligatorio o *enforcing mode* globalmente o completo (*full enforcement*), es decir, tanto para el conjunto crítico de procesos de sistema (ya protegidos en Android 4.4), como para el resto de procesos (con más de 60 dominios) [Ref.- 249].

367. En modo obligatorio, las acciones no legítimas son bloqueadas y registradas por el kernel en dmesg y logcat. Las entradas del subsistema de log de Android (logcat) pueden consultarse a través del comando “adb shell logcat”. Las entradas que el kernel escribe directamente en sus logs pueden analizarse con el comando “adb shell dmesg” o mediante el comando “adb shell su -c 'cat /proc/last_kmsg'”.

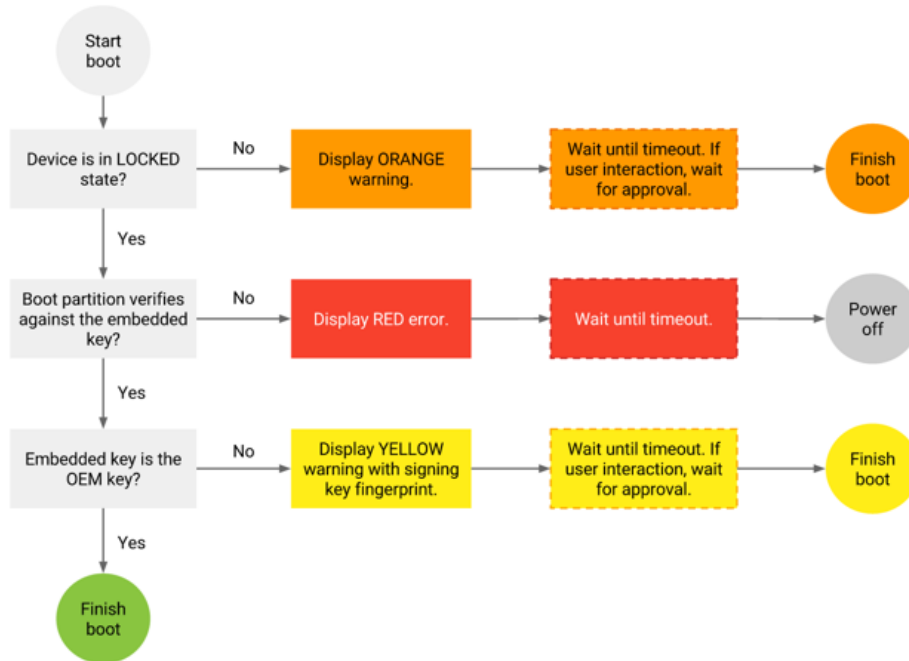
7.8. PROCESO DE ARRANQUE SEGURO: VERIFIED BOOT

- 368.Verified Boot fue introducido en Android 4.4 (“KitKat”) a través de las capacidades del kernel asociadas a device-mapper-verity (*dm-verity*) en dispositivos de almacenamiento de bloques (virtuales), con el objetivo de poder llevar a cabo verificaciones de integridad del proceso de arranque de Android, y evitar así su modificación, por ejemplo, por parte de software malicioso (malware) sin el conocimiento del usuario [Ref.- 34].
- 369.Verified Boot permite al usuario confirmar que el dispositivo móvil se encuentra en un estado conocido, con la partición de sistema protegida y sin modificar.
- 370.Para ello, Android construye un árbol de hashes criptográficos (SHA256) asociados a los bloques (de 4 KB) de almacenamiento de la partición de sistema (“/system”), obteniéndose un hash raíz (*root hash*) que el fabricante del dispositivo móvil utiliza, junto a una clave de verificación propia (*verity_key*), empleada para verificar la integridad de todo el árbol (y de todos sus bloques asociados) y, por tanto, de toda la partición de sistema [Ref.- 512].
- 371.La clave de verificación se almacena en la partición de arranque (o “/boot”), cuya integridad a su vez también debería ser verificada por el código del gestor de arranque o *bootloader* (dependiente del fabricante del dispositivo móvil).
- 372.La modificación de un único bloque de la partición de sistema invalidaría el hash criptográfico raíz, y la tabla (o árbol) de hashes de integridad asociada, y permitiría detectar modificaciones en la integridad de dicha partición.



- 373.La detección de la integridad se realiza de manera automática por el kernel al leer datos de la partición de sistema, y verificar su contenido con la tabla de hashes de integridad. Cualquier modificación de la partición de sistema daría lugar a errores de entrada/salida (I/O, input/output), como si ese bloque de datos no fuese legible.
- 374.Android 6.x añadió nuevas capacidades en Verified Boot para notificar al usuario durante el proceso de arranque acerca del estado e integridad del sistema [Ref.- 619].
- 375.Tras iniciar el dispositivo móvil, se comprueba el sistema operativo con el objeto de detectar modificaciones, confirmándose en caso de verificarse la integridad que el código a ejecutar viene de una fuente fiable (la versión oficial del sistema operativo).
- 376.Si no es posible verificar el sistema durante el proceso de arranque se pueden obtener tres mensajes de aviso³⁷:

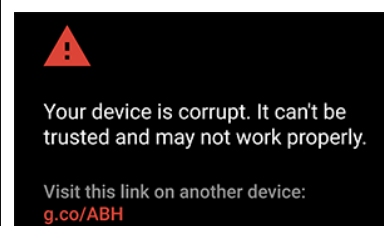
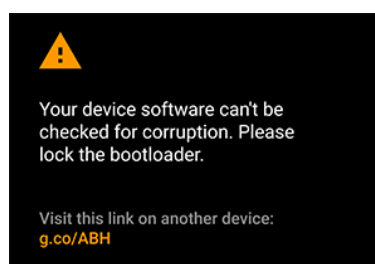
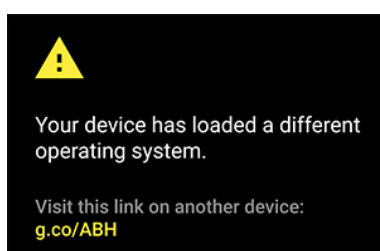
³⁷ <http://www.xda-developers.com/pixel-phones-not-yet-rootable-with-current-methods/>



377. “Your device has loaded a different operating system.”, mostrado en color amarillo durante 10 segundos, indicando que se está arrancando desde un sistema operativo diferente al que venía de fábrica en el dispositivo móvil.

378. “Your device software can't be checked for corruption. Please lock the bootloader.”, mostrado en color naranja durante 10 segundos, indicando que es gestor de arranque está desbloqueado, por lo que el dispositivo móvil permitiría arrancar desde imágenes de arranque (*bootloader*) o recuperación (*recovery*) diferentes y, como consecuencia, no es posible verificar la integridad del sistema operativo.

379. “Your device is corrupt. It can't be trusted and may not work properly.” mostrado en color rojo durante 10 segundos, indicando que el sistema operativo ha sido modificado y no es seguro hacer uso del mismo.



380. En el caso de haber desbloqueado el gestor de arranque intencionadamente, tras completar los cambios deseados, se recomienda volver a bloquear el gestor de arranque para evitar futuras modificaciones por parte de un tercero sin autorización (eliminando así el mensaje de aviso de color naranja).

381. Si el usuario identifica cualquiera de estos mensajes durante el proceso de arranque del dispositivo móvil, y no es consciente de haber llevado a cabo ninguna modificación de bajo nivel sobre el sistema intencionadamente, debería sospechar que el dispositivo móvil haya podido ser manipulado y/o comprometido.

7.9. MODO DE ARRANQUE SEGURO: SAFE MODE

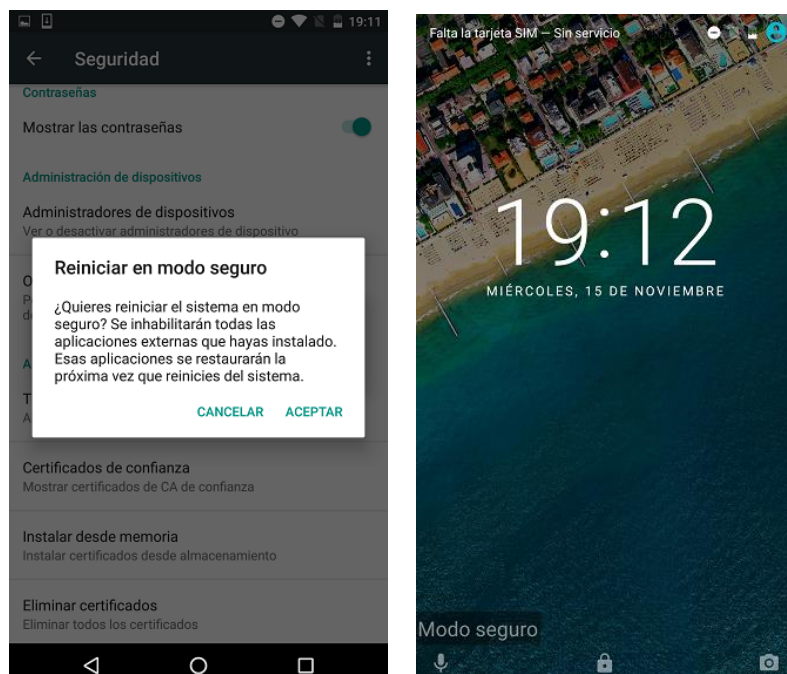
382. Además del modo “Verified Boot” descrito previamente (ver apartado “7.8. Proceso de arranque seguro: Verified Boot”), Android dispone de un modo especial de arranque que el usuario puede utilizar voluntariamente si detecta que el sistema presenta alguna inestabilidad, muestra un comportamiento extraño (como que se agote la batería rápidamente, que el dispositivo móvil se caliente en exceso, se quede sin memoria RAM disponible, lleve a cabo la ejecución de apps de manera ralentizada, etc.), o se sospecha que se ha podido instalar alguna app no fiable o inestable.

383. Se recomienda arrancar desde este modo de arranque si se sospecha que el dispositivo móvil se ha podido ver infectado con algún software o app móvil maliciosa (malware) [Ref.- 513].

384. Al arrancar en modo seguro o Safe Mode, Android ejecutará únicamente las aplicaciones preinstaladas, propias del sistema (es decir, disponibles en la partición de sistema o “/system”) y los servicios básicos necesarios para el buen funcionamiento del sistema operativo Android.

385. El procedimiento para arrancar en modo seguro si el dispositivo móvil está encendido es el siguiente:

- Pulsar el botón de encendido (o apagado) hasta que aparezca el menú de apagado del dispositivo móvil.
- Seleccionar la opción “Apagar” y mantenerla pulsada hasta que el dispositivo informe al usuario de que va a reiniciarse en modo seguro.
- Confirmar la operación mediante el botón “Aceptar”.



386. También es posible arrancar en modo seguro, cuando el dispositivo móvil está apagado, manteniendo pulsado el botón de bajar el volumen una vez aparece el logotipo de Google y se inicia su animación en la pantalla de arranque o inicio [Ref.- 513].

387. Cuando el sistema re arranque, mostrará en la pantalla de inicio el mensaje “Modo seguro” en el margen inferior izquierdo.

388. Todas las aplicaciones que no sean de sistema se mostrarán con sus iconos sombreados, siendo imposible ejecutarlas, pero sí desinstalarlas si se sospecha que alguna de ellas pueda estar ocasionando problemas en el dispositivo móvil.
389. Para salir del modo seguro, simplemente hay que apagar el dispositivo móvil (siendo en ocasiones necesario, según el modelo de dispositivo móvil, mantener el botón de apagado pulsado durante 30 segundos) y volverlo a arrancar con el botón de encendido de manera estándar.

Nota: Este procedimiento para arrancar en modo seguro (Safe Mode) es válido para dispositivos móviles Nexus, como el empleado en la elaboración de la presente guía. Para otros fabricantes, la combinación de teclas podría ser diferente.

7.10. CONFIGURACIÓN POR DEFECTO DEL DISPOSITIVO MÓVIL

390. El dispositivo móvil está configurado por defecto con valores fijados por el fabricante del sistema operativo, el fabricante del *hardware* o el operador de telefonía móvil, que pueden desvelar detalles del terminal o de su propietario.
391. Para evitar la revelación de información sensible, se recomienda modificar esos valores existentes por defecto por valores elegidos por su propietario.
392. El proceso inicial de instalación y configuración del dispositivo móvil (ver apartado “24. Apéndice A: Proceso de instalación y configuración inicial”) tiene una influencia muy limitada sobre los valores existentes por defecto y utilizados en diferentes servicios y tecnologías.
393. El nombre del dispositivo móvil Android, o *hostname* al tratarse de un dispositivo Linux, no puede ser fijado a través de los menús de los ajustes de configuración. Su valor por defecto (desde Android 2.2) es “android-<código>”, donde “<código>” es un valor de 16 caracteres hexadecimales (ver el análisis de la propiedad “net.hostname” posteriormente; por ejemplo “android-9f6edb6be8c72475”).
394. El código corresponde al identificador de Android (ANDROID_ID), un valor de 64 bits (16 caracteres hexadecimales) generado aleatoriamente en el primer arranque del dispositivo móvil y que permanece constante durante toda la vida del dispositivo [Ref.- 46], es decir, hasta que se reinstale o se restablezcan los valores de fábrica.
395. Originalmente en versiones previas de Android, y desafortunadamente, el nombre del dispositivo móvil, que también es empleado como nombre para el servicio DNS (*Domain Name System*), hacía uso del carácter de subrayado (“_”, *underscore*), que no es un carácter válido según el estándar del protocolo DNS y los servicios de resolución de nombres [Ref.- 92]. A partir de Android 4.0 ya se hace uso del carácter guión (“-”) en su lugar.
396. Únicamente los dispositivos móviles Android en los que se ha realizado el proceso de *root* permiten la modificación del nombre del dispositivo móvil (por ejemplo, mediante el comando “hostname” de Linux, o equivalente, y la modificación de los scripts de

arranque³⁸) [Ref.- 92], pese a tratarse de una característica solicitada a Google desde enero de 2010.

397. Las acciones de consulta también pueden ser llevadas a cabo a través del modo de depuración de Android y de la herramienta “adb”, mediante la ejecución del siguiente comando, por ejemplo, desde Windows:

```
C:\> adb.exe shell getprop net.hostname
android-55d5bb2fca9933e3
```

398. La operación de modificación del nombre no se puede llevar a cabo con “adb”, al ser necesario disponer de permisos de administración como el usuario root. “adb” no puede ejecutar como root en versiones del sistema operativo Android de producción (con un tipo de “build” igual a “user”), es decir, en dispositivos móviles reales y no emuladores, salvo en dispositivos Android *rooteados*:

```
$ getprop ro.build.type
user
```

399. En algunas versiones no oficiales de Android, como la versión *rootada* de LineageOS³⁹ (previamente denominada CyanogenMod), es posible modificar de forma permanente el nombre del dispositivo móvil.

400. Las referencias internas a nombres empleadas por el dispositivo móvil Android por defecto pueden ser obtenidas a través de la utilidad “adb” y de sus capacidades de depuración para acceder a las propiedades del dispositivo móvil (“adb shell getprop”):

```
C:\> adb shell getprop |findstr name
[net.bt.name]: [Android]
[net.hostname]: [android-55d5bb2eaa9933e3]
[persist.radio.use_cc_names]: [true]
[ro.build.version.all_codenames]: [REL]
[ro.build.version.codename]: [REL]
[ro.frp.pst]: [/dev/block/platform/soc.0/f9824900.sdhci/by-name/persistent]
[ro.product.name]: [bullhead]
```

401. En caso de desvelarse el nombre del dispositivo móvil en sus comunicaciones, como por ejemplo en el tráfico DHCP (donde se desvela el valor de la propiedad “net.hostname”; ver apartado “19.2. Seguridad en TCP/IP”), éste podría revelar detalles tanto del fabricante del dispositivo móvil, como por ejemplo el modelo del terminal, como del propietario. Estos datos serían muy útiles para un potencial atacante interesado en explotar vulnerabilidades en ese tipo concreto de dispositivo móvil o interesado en realizar ataques dirigidos hacia una persona u organización concreta.

402. Adicionalmente, Android puede emplear otros nombres para el dispositivo móvil al hacer uso de otros servicios y tecnologías, como por ejemplo Bluetooth (ver apartado “15. Comunicaciones Bluetooth”) o el punto de acceso Wi-Fi (ver apartado “16.6. Punto de acceso o zona Wi-Fi”), por lo que la configuración de los ajustes de Bluetooth o del punto de acceso Wi-Fi permiten modificar su valor.

Nota: El valor de la propiedad denominada “net.bt.name”, con el valor “Android” por defecto, no está relacionada con el nombre Bluetooth del dispositivo móvil.

³⁸ <https://play.google.com/store/apps/details?id=nk.bla.android.autostart>

³⁹ <https://lineageos.org>

403. De ser posible en versiones futuras de Android, sería recomendable disponer de ajustes de configuración que permitan modificar el nombre del dispositivo móvil por uno que no desvele detalles ni del dispositivo móvil (fabricante o modelo) ni del propietario (evitando tanto referencias al nombre de la persona como de la organización asociada al mismo), como por ejemplo “dm0001” (“dispositivo móvil 0001”).

8. GESTIÓN EMPRESARIAL DE DISPOSITIVOS MÓVILES BASADOS EN ANDROID

404. Las estrategias y soluciones empresariales de gestión de dispositivos móviles, conocidas como MDM en inglés (*Mobile Device Management*), constituyen un elemento fundamental para gestionar el nivel de riesgo y los mecanismos de seguridad en todas las organizaciones y compañías que pretendan integrar el uso de estos dispositivos en sus actividades diarias.

405. Se dispone de información detallada sobre las soluciones de gestión empresarial de dispositivos móviles o MDM en la guía “CCN-STIC-457 - Gestión de dispositivos móviles: MDM (*Mobile Device Management*)” [Ref.- 403].

406. En 2006, Google comenzó a proporcionar capacidades empresariales para la gestión de dispositivos móviles basados en Android a través de la plataforma Google Apps o Google Apps for Your Domain [Ref.- 13], accesibles desde un navegador web y que no requerían del despliegue de servidores dedicados para este propósito, al emplearse los servicios de Google “en la nube” asociados a un dominio propio.

407. En septiembre de 2016, Google publicó la evolución de Google Apps, posteriormente denominado Google Apps for Work, y finalmente denominado G Suite [Ref.- 205].

408. G Suite es un conjunto (o *suite*) de herramientas colaborativas (en tiempo real) y de productividad, asociadas a los servicios y productos de Google “en la nube”, que no sólo proporciona capacidades empresariales de gestión de los dispositivos móviles, sino acceso a servicios como Gmail, Hangouts, Calendar, Google+ para las comunicaciones entre usuarios, Google Drive para el almacenamiento “en la nube”, Google Docs, Sheets, Slides, Forms, y Sites para mejorar la productividad, etc.

409. Para poder implantar estas políticas de seguridad es necesario que el dispositivo móvil disponga de la app “Google Apps Device Policy”, disponible de forma gratuita en Google Play [Ref.- 13].

410. Desde la versión 2.2 de Android los administradores de un dominio Google Apps (ediciones *Premier* o *Business*, *Government* o *Education*) o G Suite disponen de capacidades para gestionar políticas de seguridad sobre los dispositivos móviles (que van siendo ampliadas a través de las diferentes versiones de la plataforma), incluyendo [Ref.- 91]:

- Borrado remoto de los datos del dispositivo móvil (*wipe*), en caso de haber sido perdido o robado (ver apartado “10.4. Eliminación de datos del dispositivo móvil”).

Nota: Este proceso es equivalente a la opción “Restablecer datos de fábrica” disponible desde el menú “Ajustes - Copia de seguridad [Datos Personales]”.

- Definir el número de intentos de acceso fallidos antes de borrar los contenidos del dispositivo móvil (*wipe*).

- Definir un número de días tras el que si el dispositivo móvil no se ha sincronizado con G Suite, será borrado (*wipe*).
- Forzar la solicitud de un código de acceso en el dispositivo móvil.
- Definir la longitud mínima del código de acceso.
- Definir la fortaleza del código de acceso mediante la utilización de letras y números.
- Definir la política del código de acceso, incluyendo los días de validez antes de que el código expire, bloquear un número concreto de códigos expirados,
- Definir el temporizador de bloqueo del dispositivo móvil tras un periodo de inactividad, cuya duración puede ser también definida en la política de seguridad.
- Auditoría de aplicaciones.
- Definir los requisitos de versión de la app “Google Apps Device Policy”.
- Eliminación remota de una cuenta de usuario de un dispositivo móvil.
- Bloquear los dispositivos móviles cuya seguridad ha sido comprometida.

411.El administrador también puede configurar redes Wi-Fi y gestionar los certificados digitales de acceso a la red Wi-Fi a través de la app de gestión.

412.Adicionalmente, los usuarios de los dispositivos móviles pueden de forma remota restaurar (o resetear) el código de acceso (ver apartado “9.18. Restauración del código de acceso”), hacer que suene el dispositivo móvil, bloquear el mismo, localizar su ubicación y llevar a cabo el borrado remoto de los datos (*wipe*; si esta opción ha sido habilitada por el administrador).

413.Para poder localizar el dispositivo móvil es necesario disponer del permiso de localización asignado a la app de gestión, que es activado automáticamente sólo para dispositivos con un perfil de trabajo o propiedad de la organización (no en dispositivos personales) [Ref.- 91]. La información de localización no se comparte con el administrador.

414.La versión 2.0 (o superior) de la app “Google Apps Device Policy” permite adicionalmente a los administradores definidos en Google Apps incluir como requisito de la política de seguridad el cifrado de los datos de las *tablets* basados en Android 3.0 o los *smartphones* en la versión 4.0 (ver apartado “10.1. Cifrado del dispositivo móvil”), opción disponible desde el panel de control asociado en Google Apps [Ref.- 97].

415.En el caso de que el dispositivo móvil esté configurado con múltiples cuentas de G Suite, cada una haciendo uso de una política de seguridad diferente, será aplicada la política de seguridad más restrictiva. Por ejemplo, si la política de seguridad de un dominio (o cuenta) requiere códigos de acceso de 6 caracteres, y la de otro de 8 caracteres, será necesario disponer de un código de acceso de 8 caracteres [Ref.- 91].

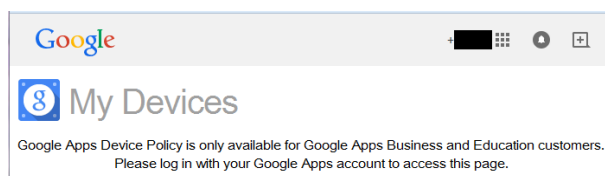
416.El acceso a la gestión de dispositivos móviles y de las políticas de seguridad para los usuarios empresariales de G Suite (*Business, Government y Education*) por parte del administrador está disponible desde el panel de control de G Suite, o desde un dispositivo móvil mediante la app “Google Admin” [Ref.- 213].

417. Las políticas establecidas por el administrador también están disponibles para el usuario empresarial desde el propio dispositivo móvil empleando la pantalla “Policies” de la app “Google Apps Device Policy” [Ref.- 91].

Nota: Las capacidades de gestión de dispositivos móviles Android a través de G Suite quedan fuera del alcance de la presente guía. Los administradores de G Suite disponen de documentación oficial para la gestión de los dispositivos móviles⁴⁰.

418. Una vez se establecen las políticas de seguridad a nivel empresarial y se dispone de la app instalada en los dispositivos móviles a gestionar, un usuario podría desinstalar la app. Sin embargo, el administrador puede configurar el entorno de gestión para que en ese escenario no sea posible sincronizar ningún dato entre el dispositivo móvil y el entorno corporativo (e-mails, contactos, eventos de calendario o fotografías) desde el momento en que se lleve a cabo la desinstalación de la app.

419. Sin embargo, el acceso a “My Devices”⁴¹ por parte de un usuario no asociado a un dominio de Google Apps o G Suite no está permitido, obteniéndose el siguiente mensaje informativo:



420. Microsoft, a través de Microsoft Exchange ActiveSync, también proporciona capacidades de gestión empresarial de dispositivos móviles Android [Ref.- 38], siendo posible la aplicación de numerosas políticas de seguridad [Ref.- 36].

421. Las capacidades disponibles en la política de seguridad dependen de la versión de Android existente en los dispositivos móviles, y de la versión de Microsoft Exchange empleada por la organización (2003, 2007, 2010, 2013..., y la versión de Service Pack (SP) concreta).

Nota: La gestión empresarial detallada de dispositivos móviles Android mediante Microsoft Exchange y ActiveSync (2003 SP2, 2007 o superior), Microsoft Exchange Online (<https://www.microsoft.com/online/exchange-online.aspx>) o System Center Configuration Manager (SCCM) 2012, incluyendo su implementación, configuración, e integración con las soluciones Microsoft Exchange está fuera del alcance de la presente guía [Ref.- 36][Ref.- 37].

8.1. GESTIÓN REMOTA DE DISPOSITIVOS ANDROID POR PARTE DEL USUARIO

422. El soporte para aplicaciones empresariales fue introducido por Android 2.2 a través de la API “Android Device Administration” [Ref.- 268] [Ref.- 272]. Esta API proporciona capacidades de administración a nivel de sistema, como permitir establecer políticas de contraseñas, añadir capacidades de borrado remoto y servicios de gestión del dispositivo móvil y de sus aplicaciones.

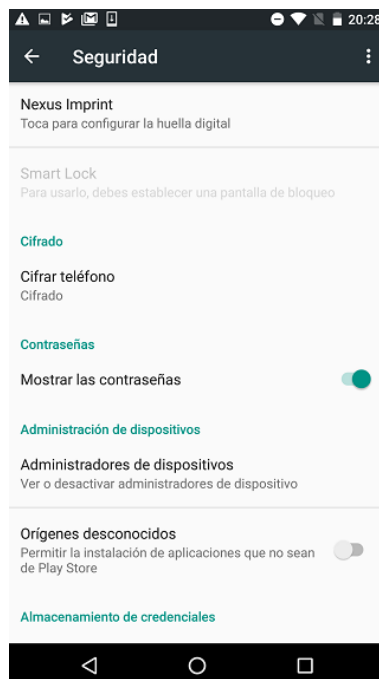
423. Las políticas de administración de dispositivos pueden estar programadas dentro de la app de gestión o solicitarse dinámicamente desde un servidor corporativo. La app de

⁴⁰ <https://support.google.com/a/answer/1056433>

⁴¹ <https://www.google.com/apps/mydevices>

gestión se puede instalar en el dispositivo móvil del usuario final a través de Google Play, de un mercado de apps conocido y de confianza (por ejemplo, privado a la organización), o a través de un servidor web.

424. Cuando se instala la app de gestión, el sistema solicitará al usuario el permiso de “administración de dispositivos”. Si se le concede, la app impondrá sus políticas, y tendrá la capacidad de tomar las acciones definidas si éstas no se cumplen. Así por ejemplo, si la app define una política de longitud mínima de contraseña y el usuario no la cumple, podría denegarle el acceso a un determinado servicio.
425. Adicionalmente, la administración de dispositivos móviles puede establecer políticas que actúen ante la instalación o borrado de determinadas apps, bien sea lanzando un mensaje de aviso o bloqueando por completo la acción.
426. La API de administración de dispositivos no permite cumplimientos parciales de las políticas, es decir, sólo aquellos dispositivos que cumplan todas las restricciones se considerarán aptos.
427. Si un dispositivo contiene varias apps con el permiso de administración del dispositivo, se impondrá la que defina la política más restrictiva, ya que no existe ningún mecanismo para seleccionar una app de administración para diferentes escenarios.
428. Es posible consultar qué aplicaciones tienen el permiso de administración de dispositivos a través de “Ajustes [Personal] - Seguridad [Administración de Dispositivos] - Administradores de dispositivos”:



429. El permiso de administración de dispositivos, al permitir la gestión remota del mismo, incluyendo su borrado, nunca debe ser concedido salvo en escenarios de plena confianza, ya que una app maliciosa podría solicitarlo y hacer uso de estas capacidades avanzadas.
430. El acceso a la gestión remota del dispositivo móvil por parte de los usuarios particulares, no asociados a un dominio de Google Apps o G Suite, se puede llevar a cabo a través del recurso “Encontrar mi dispositivo”, disponible en la URL

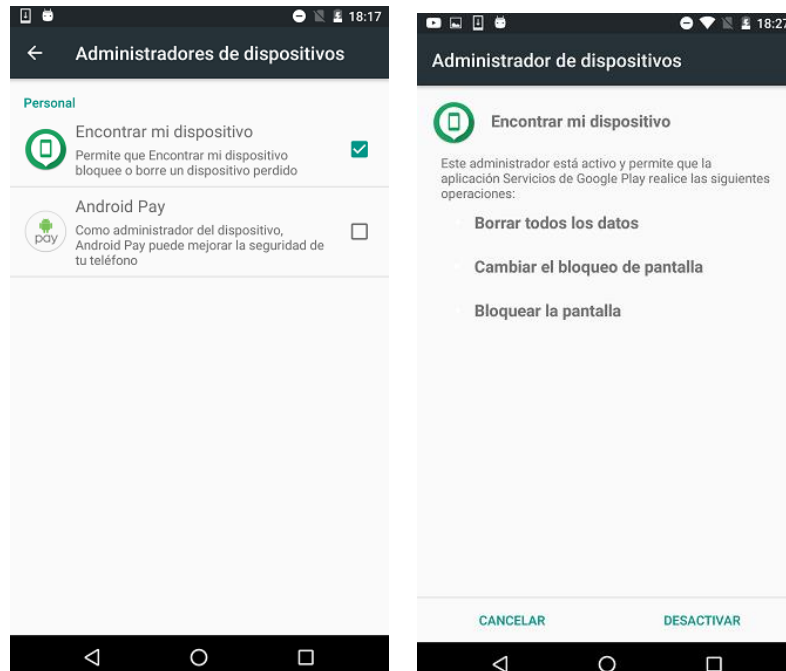
"<https://www.google.com/android/find>", o desde la app disponible en Google Play⁴², también denominada "Encontrar mi dispositivo".

431. Este recurso y app han sustituido a los utilizados en versiones previas de Android, ambos denominados "*Android Device Manager*"⁴³.
432. El servicio "Encontrar mi dispositivo" (Find my device), que hasta Android 4.4 se ofrecía como una app disponible en Google Play (antiguamente denominado Play Store), pasó a formar parte del servicio "Google Play Protect" (ver apartado "23.8. Verificación de seguridad de las apps: Google Play Protect"), de modo que en Android 6.x se ofrece como un componente con permisos de "Administración de dispositivos" [Ref.- 226], y, entre otras cosas, permite al usuario desde un terminal Android encontrar otros dispositivos móviles Android, tanto *smartphones* como *tablets*.
433. Es muy importante reseñar que, tanto la funcionalidad del portal de gestión remota como los mensajes que se muestran en respuesta a las diferentes acciones solicitadas a través de él, son dependientes de Google (y de sus servicios asociados) y pueden variar a lo largo del tiempo. Las opciones y mensajes descritos en la presente guía corresponden a noviembre de 2017.
434. Los requisitos para hacer uso de la funcionalidad de gestión remota son [Ref.- 60]:
- Disponer de una conexión de datos: para poder hacer uso de las capacidades de gestión remota es necesario que el dispositivo móvil disponga de una conexión a una red Wi-Fi o de datos móviles (2/3/4G), a fin de poder comunicarse con los servidores de Google y responder a las acciones solicitadas por estos.
 - Si el dispositivo móvil no dispone de una conexión de datos, el administrador de dispositivos Android no podrá bloquear la pantalla, modificar el código de acceso (referido por Google como la contraseña de bloqueo de la pantalla), hacer sonar el dispositivo móvil, o borrar sus datos remotamente hasta que se establezca una conexión a través de una red Wi-Fi o de la red de datos móviles. Al seleccionar una acción en el administrador de dispositivos Android, ésta se llevará a cabo la próxima vez que el dispositivo móvil vuelva a estar conectado. Lógicamente, el administrador de dispositivos Android no funciona para dispositivos móviles que estén apagados o con el modo avión activado.
 - Disponer del administrador de dispositivos Android activo: desde el menú "Ajustes [Personal] - Seguridad [Administración de Dispositivos] - Administradores de dispositivos [Personal] Encontrar mi dispositivo" es posible activar esta funcionalidad, y la pantalla de confirmación informará de las capacidades de gestión asociadas. Las capacidades de gestión remota que se obtienen al activar el administrador de dispositivos Android son: *bloquear la pantalla* (equivale a bloquear remotamente un dispositivo móvil perdido o robado), *cambiar el bloqueo de pantalla* (en caso de que no se hubiese configurado un código de acceso en el dispositivo móvil, desde el interfaz web de gestión remota se puede configurar uno; si ya hubiese uno vigente, la

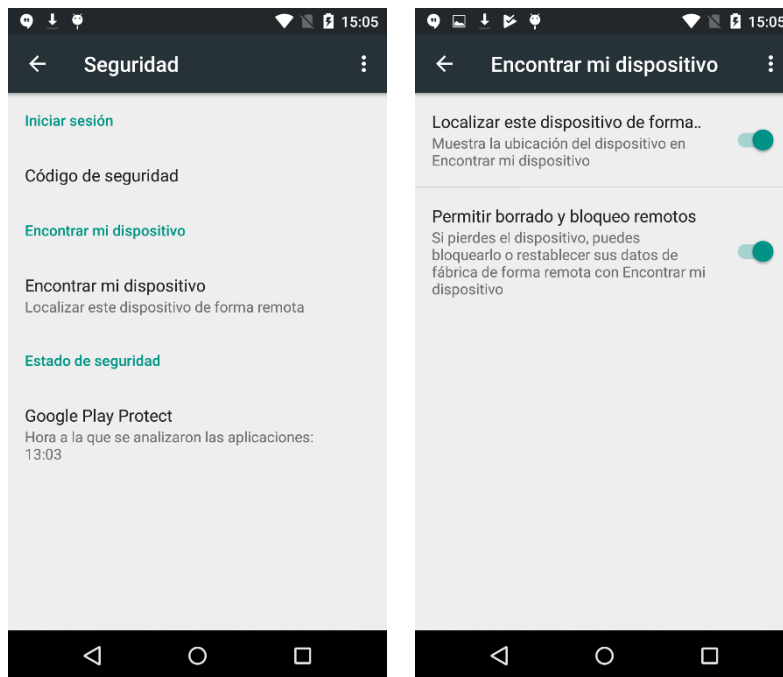
⁴² <https://play.google.com/store/apps/details?id=com.google.android.apps.adm>

⁴³ La URL del recurso "Android Device Manager" era: "<https://www.android.com/devicemanager>". En el momento de elaboración de la presente guía, este enlace redirige al nuevo recurso "Encontrar mi dispositivo": "<https://www.google.com/android/find>".

configuración de un nuevo código de acceso no modificará el código actual) y *borrar todos los datos* (equivale a una restauración a fábrica remota, o *wipe*).

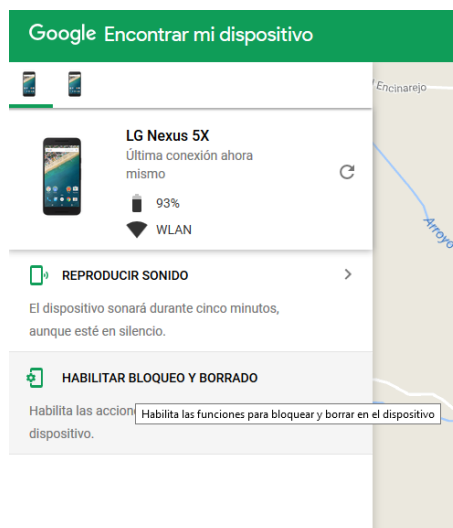


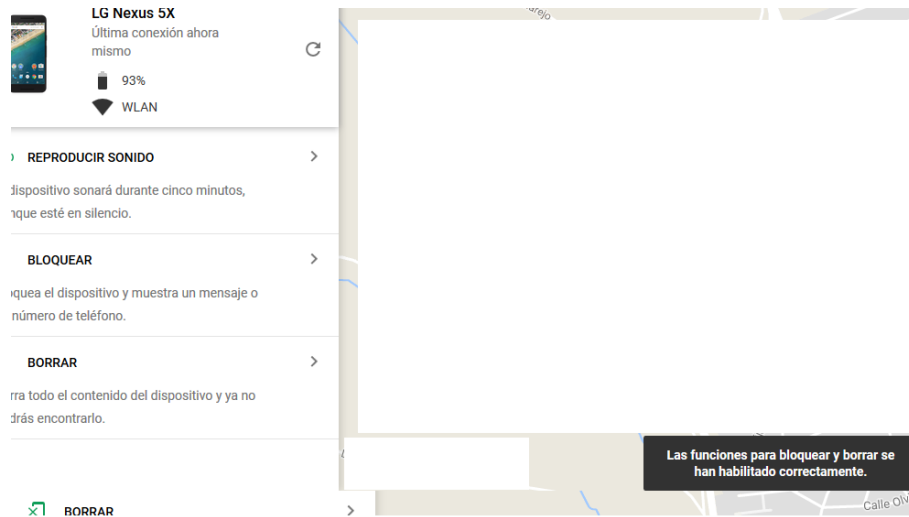
- Disponer de una sesión iniciada con la cuenta de Google del usuario desde el dispositivo móvil, disponible automáticamente en caso de haber sido configurada dicha cuenta.
- El dispositivo móvil debe estar visible en Google Play: el dispositivo se puede hacer visible desde la sección “Visibilidad” de Google Play (“<https://play.google.com/settings>”). Si un dispositivo móvil está oculto en Google Play, no aparecerá en la funcionalidad de “Encontrar mi dispositivo”.
- Tener el servicio de ubicación (o localización) activo: desde la app “Ajustes de Google”, mediante el menú “[Servicios] Ubicación”, es posible habilitar la opción “Ubicación” (servicios de localización) mediante el botón “Sí”.
 - Este acceso es equivalente al acceso estándar correspondiente a los servicios de localización, disponible desde “Ajustes - [Personal] Ubicación”.
- En la versión de Android 5.x, la app “Google” existente por defecto permitía modificar las capacidades y configuración del administrador de dispositivos Android a través de la opción “[Servicios] Seguridad - [Administrador de dispositivos] Administrador de dispositivos”. Las opciones de configuración posibles, que se podían habilitar y deshabilitar individualmente, y que se muestran en las imágenes inferiores, eran “Localizar este dispositivo de forma remota” y “Permitir borrado y bloqueo remotos”:



435.Sin embargo, esta capacidad de permitir sólo la opción deseada no es configurable en la versión de Android 6.x, y las dos opciones son aceptadas implícitamente si se habilita el administrador de dispositivos “Encontrar mi dispositivo”.

436.Sin embargo, aunque la opción “Ajustes [Servicios] - Seguridad - [Administrador de dispositivos] Administradores de dispositivos - Encontrar mi dispositivo” esté deshabilitada en el dispositivo móvil, el interfaz web de gestión remota permite habilitar estas capacidades de forma remota. Si se selecciona esta opción remotamente desde el interfaz web, se activará de nuevo el interruptor “Encontrar mi dispositivo” en el dispositivo móvil. En el interfaz web se mostrará el mensaje *“Las funciones para bloquear y borrar se han habilitado correctamente”*. Es decir, estas capacidades son gestionadas remotamente desde el interfaz web y no desde el propio dispositivo móvil:





437. La información sobre los dispositivos asociados a una cuenta de Google está disponible en el menú “Controles de la actividad de tu cuenta - Información de los dispositivos”, y, pese a que podría pensarse que esta información se limitaría a datos ligados solo al terminal, en realidad incluye datos que no son propios del dispositivo móvil, como los contactos o el calendario de la cuenta de Google vinculada a él [Ref.- 235].

438. Si se desea acceder a las capacidades de gestión remota ante la pérdida o robo del dispositivo móvil, se dispone de dos opciones con funcionalidad similar, ambas descritas en detalle a continuación:

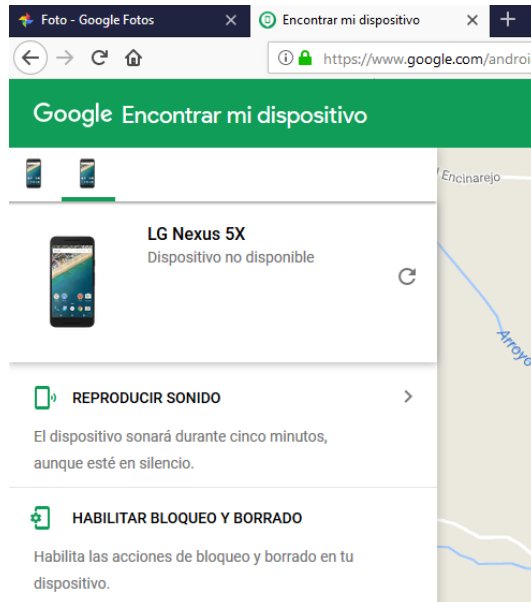
- Utilizar el recurso “Encontrar mi dispositivo” (opción 1), disponible en “<https://www.google.com/android/find>” (o “<https://android.com/find/>”).
- Acceder a la cuenta de Google del usuario del dispositivo móvil desde “<https://myaccount.google.com>” y seleccionar la opción “Encontrar tu móvil” (opción 2), que mostrará la lista de dispositivos móviles que están (o han estado) vinculados a esa cuenta, pudiéndose seleccionar el dispositivo deseado.

439. Si se hace uso del recurso “Encontrar mi dispositivo” (opción 1) [Ref.- 201] para acceder a las capacidades de gestión remota, tras introducir las credenciales de la cuenta de Google del usuario, se mostrarán las siguientes opciones (ver la imagen inmediatamente anterior):

- Reproducir sonido: esta opción hace que el dispositivo móvil emita un sonido con el máximo volumen para poder localizar su ubicación, incluso si se encontraba en silencio. El sonido se reproducirá durante 5 minutos o hasta que se interactúe físicamente con el dispositivo, a través de los botones físicos o de la pantalla.
- Bloquear: esta opción bloquea la pantalla del dispositivo móvil (en caso de estar desbloqueada), y adicionalmente permite que se muestre un mensaje y/o número de teléfono para contactar con su propietario.
- Borrar: esta opción permite eliminar remotamente todos los datos del dispositivo móvil, siendo equivalente a una restauración a fábrica (*wipe*).

440. Si la opción de localización remota está activa, al seleccionar la flecha circular disponible a la derecha de los datos del dispositivo móvil, se refrescará la información de ubicación del mismo. La ubicación, mostrada en Google Maps, reflejará en el mapa dónde se encuentra el dispositivo actualmente (“Última conexión ahora mismo”).

441. A fecha de elaboración de la presente guía, en caso de que el dispositivo no esté localizable cuando se solicita su ubicación, se mostrará un mensaje indicando que no está disponible. En el pasado, al intentar localizar un dispositivo que no estaba disponible, se mostraba la fecha y hora de la última vez que se recibió información de su ubicación y dónde se encontraba el dispositivo móvil en ese momento.



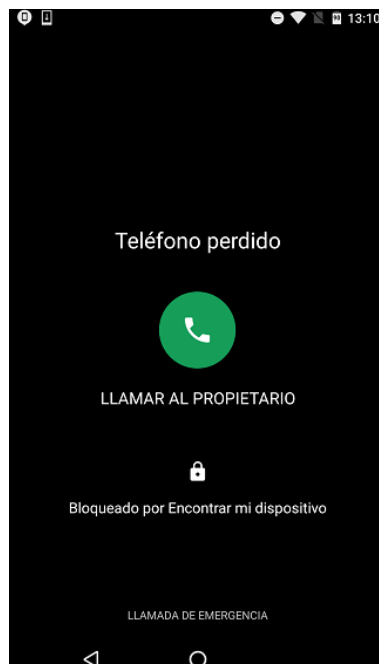
442. La opción “Bloquear” mostrará un menú que permite introducir un código de acceso (o contraseña) y proporcionar un mensaje que se mostrará en la pantalla de bloqueo del dispositivo móvil. La primera vez que se pulse esta opción, se muestra un mensaje indicando que el dispositivo no tiene ningún bloqueo de pantalla. Este mensaje puede resultar confuso, pues no implica que el dispositivo móvil realmente no tenga configurado un código de acceso actualmente, sino que no se ha añadido aún ninguno a través del interfaz web de gestión remota.

443. Por otro lado, aunque se introduzca un código de acceso distinto al que ya estuviese vigente en el dispositivo móvil, el código de acceso actual no se reemplazará y seguirá siendo válido para desbloquear el terminal. Por tanto, esta opción únicamente tiene validez cuando el dispositivo móvil no dispone de un código de acceso configurado, opción no recomendada desde el punto de vista de seguridad.

444. Al confirmar la recepción de la operación, se mostrará el mensaje “*Bloqueo solicitado*”. Cuando el dispositivo móvil vuelva a disponer de conectividad de datos, recibirá la petición, y ejecutará la acción.

445. El interfaz web mostrará un mensaje que indicará si la operación tuvo éxito (se mostrará el mensaje “*Bloqueado*”) o no; sin embargo, en el momento de elaboración de la presente guía, en múltiples ocasiones se ha recibido el mensaje “*No se ha podido bloquear el dispositivo*” aunque la operación haya concluido con éxito (por lo que no se debe confiar en la fiabilidad actual a la hora de confirmar el éxito de las operaciones).

446.Como resultado, si la acción de bloqueo ha tenido éxito, el dispositivo móvil mostrará una nueva pantalla de desbloqueo, con el mensaje especificado previamente (cada vez que se apague la pantalla). Para proceder a desbloquearlo, hay que pulsar en el botón de retroceder a la pantalla previa (o flecha hacia la izquierda situada en la parte inferior de la pantalla) que permitirá acceder a la pantalla principal de desbloqueo.



447.Si el dispositivo móvil no tenía un código de acceso configurado y se solicitó habilitarlo remotamente, será necesario introducir el nuevo código de acceso, y, si ya disponía de él, habrá que introducir el código ya existente.

448.La opción “Borrar” eliminará todos los datos de usuario del dispositivo móvil y restaurará a fábrica el terminal, dejando la versión del sistema operativo Android disponible en el momento de llevar a cabo esta acción. El proceso de eliminación de los datos es equivalente a un *hard reset*, es decir, al restablecimiento del dispositivo móvil a

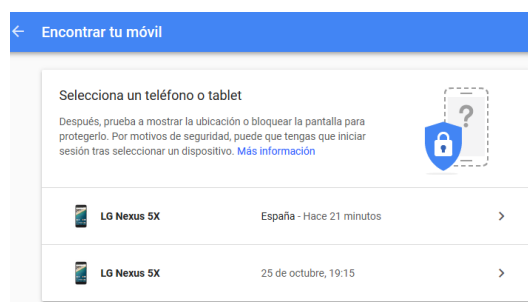
la configuración de fábrica. Durante el proceso, por tanto, se eliminarán las apps instaladas, junto a todos los datos y configuraciones realizadas por el usuario.



449. Las peticiones de bloqueo y borrado remotas se encolan en los servidores de Google, por lo que, si el dispositivo móvil se encuentra apagado o sin conexión de datos (Wi-Fi o móviles) cuando se envía la petición, la misma será reenviada cuando el dispositivo disponga de una conexión de datos.

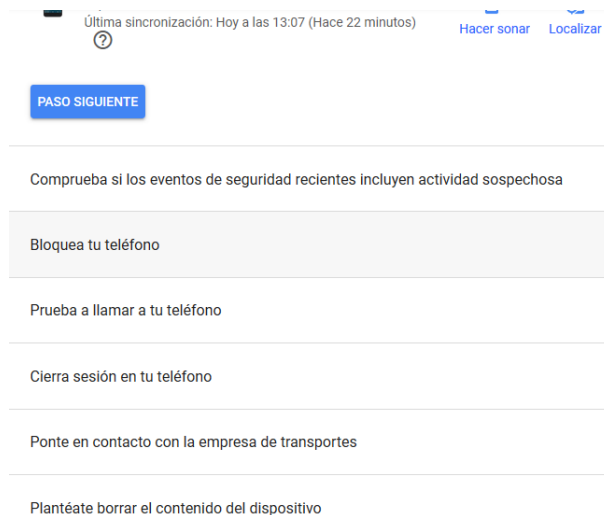
450. Es importante tener en cuenta que puede existir una demora entre que se ordena una determinada acción desde el interfaz web de gestión remota y su ejecución efectiva en el dispositivo móvil. Aunque normalmente se debería recibir un mensaje que confirme el éxito o fracaso de la operación, desafortunadamente se ha constatado que, en determinadas ocasiones, los mensajes de confirmación de la operación en la interfaz web de gestión remota no siempre son coherentes con la acción realizada, no se muestran o tienen un contenido erróneo. Sin embargo, la tasa de coherencia en Android 6.x es significativamente superior a la observada en Android 5.x.

451. Si se utiliza la cuenta de Google del usuario vinculada al dispositivo móvil, mediante la opción de gestión remota “Encontrar tu móvil” (opción 2), y tras introducir las credenciales de la cuenta de Google del usuario, se mostrará un menú con las opciones recomendadas para localizarlo una vez seleccionado el dispositivo móvil:



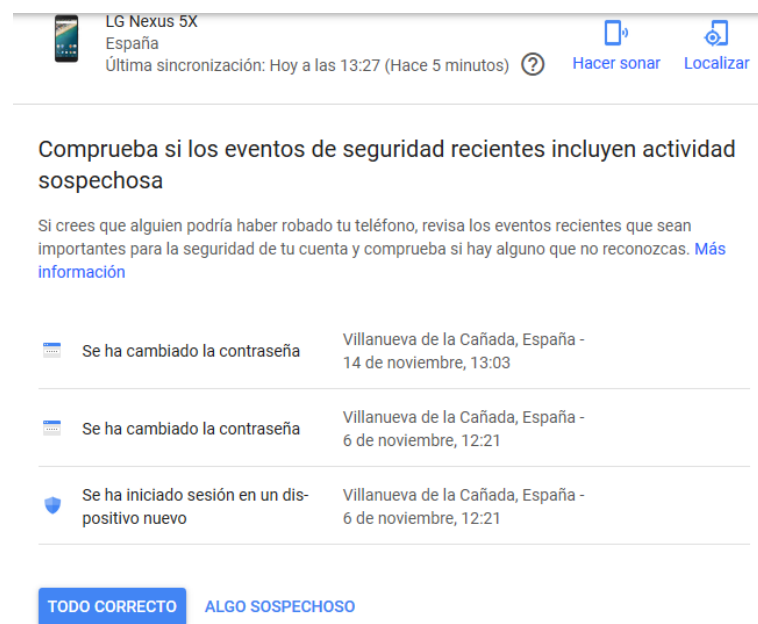
452. Se recomienda por defecto seguir las múltiples opciones disponibles en el orden en el que son presentadas, pues se parte de la premisa de que el dispositivo móvil podría estar aún próximo al usuario.

453. Sin embargo, la política de seguridad para dispositivos móviles de la organización debería definir una secuencia de actuación diferente para este tipo de escenarios en función de los requisitos de seguridad de los dispositivos móviles y de la criticidad de los datos que gestionan.

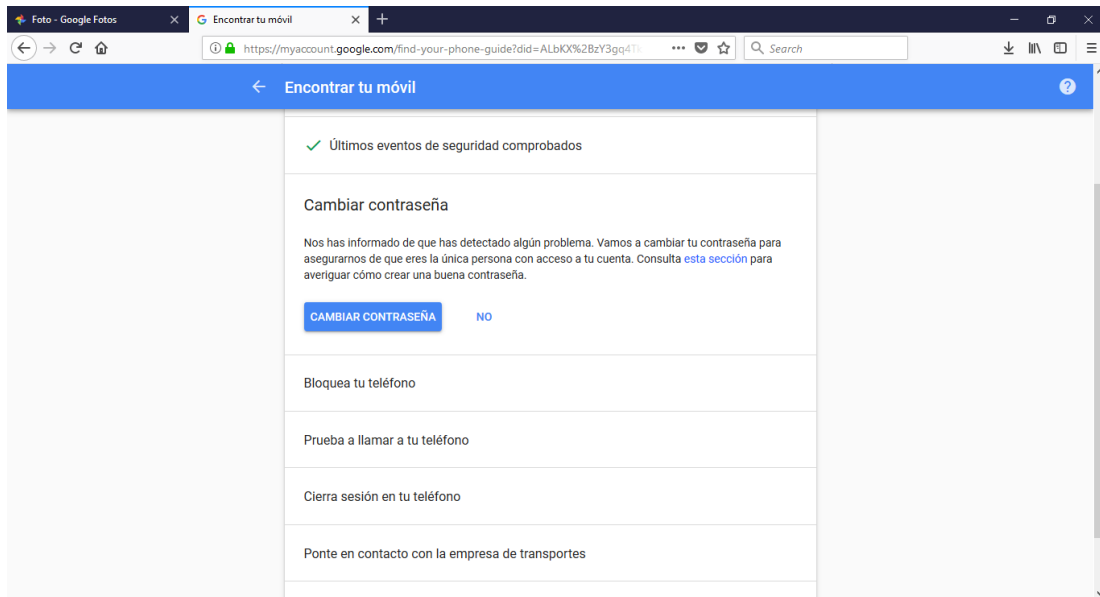


454. Si desde este interfaz web de gestión se selecciona la opción “Localizar”, se abrirá el enlace “<https://www.google.com/android/find>” (equivalente al recurso “Encontrar mi dispositivo” correspondiente a la opción 1 descrita previamente).

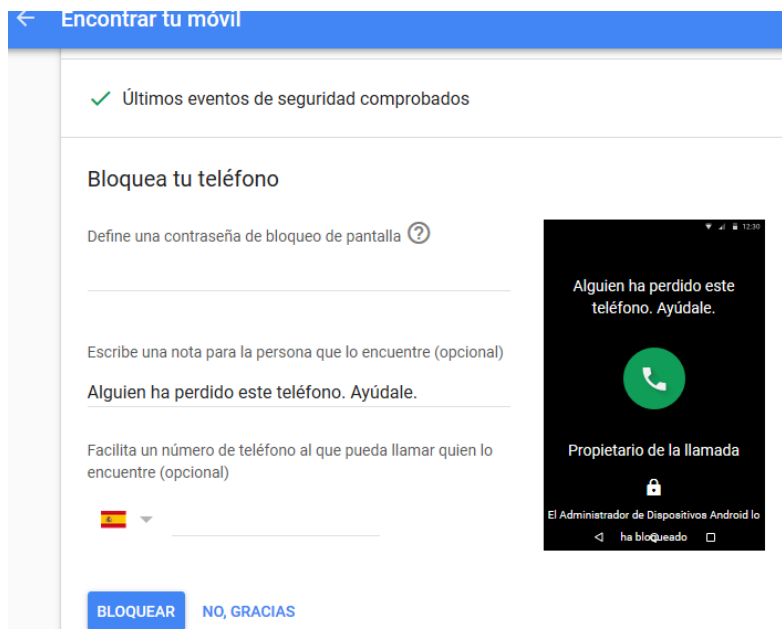
455. Si se selecciona la opción “Paso siguiente”, se desplegará un menú que muestra los últimos eventos de seguridad registrados en la cuenta de Google del usuario, como por ejemplo un cambio de contraseña o un inicio de sesión en un nuevo dispositivo, desde el que no se había efectuado un inicio de sesión nunca.



456. Si el usuario indica que hay algo sospechoso, se propondrá un cambio de contraseña de la cuenta de Google para evitar comprometerla:



457. Si, por el contrario, no se identifica ninguna actividad extraña, se desplegará la opción “Bloquea tu teléfono” (equivalente a la opción “*Bloquea tu teléfono*” del listado de múltiples opciones disponibles), que permite bloquear remotamente el dispositivo móvil. Además, si el dispositivo móvil no disponía de un código de acceso previamente establecido (escenario desaconsejado desde el punto de vista de seguridad), se configurará un código de acceso para el bloqueo del dispositivo con el valor especificado en este menú; si el dispositivo ya disponía de un código de acceso establecido, tal como se ha descrito previamente para la opción 1, se mantendrá el código actualmente configurado en el dispositivo, tal como muestra el mensaje que se obtiene mediante la ayuda (icono con el símbolo “?”):



458. El hecho de que no se lleve a cabo la modificación del código de acceso (o contraseña) actual en el dispositivo móvil supone una diferencia notable respecto al comportamiento del servicio y app *Android Device Manager* empleado en versiones previas de Android, en la que el código de acceso sí se cambiaba por el nuevo valor, tal como muestra la siguiente imagen:

459. Una vez ejecutada la acción, si ésta ha tenido éxito, se recibe confirmación de la operación en el interfaz web de gestión remota. Si no ha sido posible contactar con el dispositivo móvil, se informa de que se ha enviado la solicitud mediante el mensaje *“Hemos enviado una solicitud de bloqueo a tu dispositivo correctamente”*. Cuando el dispositivo móvil vuelva a disponer de conectividad de datos, recibirá la petición, y ejecutará la acción. Como se ha descrito previamente, esto implica que los servidores de Google encolan las peticiones destinadas al dispositivo, y las envían cuando detectan que el dispositivo móvil está de nuevo disponible. En ese momento se mostrará el mensaje de confirmación⁴⁴:

El teléfono está bloqueado. Como ya tienes un bloqueo de pantalla configurado, no se utilizará la contraseña que acabas de configurar.

460. Como resultado, si la acción de bloqueo ha tenido éxito, el dispositivo móvil mostrará una nueva pantalla de desbloqueo, con el mensaje especificado previamente (cada vez que se apague la pantalla). En dicha pantalla se mostrará una nota que indica *“Bloqueado por el ‘Encontrar mi dispositivo’”*.

461. La opción *“Prueba a llamar a tu teléfono”* no realiza acciones directas sobre el dispositivo móvil, sino que propone al usuario alternativas para localizar el dispositivo, diferentes a las que se pueden utilizar desde la página web de gestión. Igualmente ocurre con la opción *“Ponte en contacto con la empresa de transportes”* (referida a *“ponerse en contacto con el operador de telefonía móvil”*).

462. La opción *“Cierra sesión en tu teléfono”* provoca que se cierre la sesión asociada a la cuenta de Google del usuario en el dispositivo móvil. De ese modo se impedirá que, en caso de poderse desbloquear el dispositivo por parte de un tercero no autorizado, éste tenga acceso a los datos de la cuenta. En el dispositivo móvil se mostrará la notificación *“Acción necesaria en cuenta”* y, al desbloquearse el dispositivo y abrir la notificación, se indicará *“Has cerrado sesión en tu cuenta de Google”*. Al seleccionar el botón *“Siguiente”*, se solicitará al usuario la contraseña de la cuenta de Google que estaba activa antes de cerrarse la sesión (aunque haya varias configuradas en el dispositivo móvil).

⁴⁴ Desafortunadamente, no se ha identificado la existencia de ningún registro (o *log*) que refleje las diferentes acciones llevadas a cabo mediante los mecanismos de gestión remota, junto a las confirmaciones del dispositivo móvil, incluyendo una referencia temporal.

Cierra sesión en tu teléfono

Cierra la sesión de tu cuenta de Google @gmail.com en tu teléfono perdido para que nadie pueda acceder a ella. Podrás hacer sonar, localizar y bloquear tu teléfono, así como borrar su contenido.

CERRAR SESIÓN

NO, GRACIAS

463. Por último, la funcionalidad “*Plantéate borrar el contenido del dispositivo*” ofrece al usuario la posibilidad de eliminar todos los datos del terminal remotamente desde el interfaz web de gestión. Una vez ejecutada la acción, mediante el botón “Sí, Borrar”, si el dispositivo móvil disponía de conectividad de datos, se restaurará su configuración de fábrica:

Plantéate borrar el contenido del dispositivo



Al borrar tu dispositivo, se impedirá que otras personas vean tu contenido. Si decides hacerlo, ten en cuenta lo siguiente:

- Es posible que no podamos borrar por completo todas las tarjetas de memoria de tu dispositivo.
- La función Encontrar tu móvil y el Administrador de Dispositivos Android ya no podrán localizar, hacer sonar ni bloquear tu teléfono.
- Perderás de forma permanente el acceso a toda la información del dispositivo de la que no se haya hecho ninguna copia de seguridad en Google.

El contenido del teléfono se borrará la próxima vez que se conecte a Internet. Si no lo hace, no se borrará.

SÍ, BORRAR

NO, GRACIAS

¿Quieres borrar todos los datos?

Mediante esta acción, se restablece la configuración original de fábrica en tu dispositivo. Tus aplicaciones, fotos, música y configuración se eliminarán. Tras borrar el dispositivo, el Administrador de Dispositivos Android dejará de funcionar. Esta acción no se puede deshacer. Es posible que no podamos borrar el contenido de la tarjeta SD del dispositivo.

Si tu dispositivo no está conectado a Internet, restableceremos la configuración original de fábrica cuando se conecte.

CANCELAR

SÍ, BORRAR

464. Tras confirmar la operación de borrado, se intentará contactar con el dispositivo:

Intentando conectar con tu dispositivo para borrar su contenido...

465. Tan pronto se tenga de nuevo conexión de datos desde el dispositivo móvil, se enviará la orden de borrado y se informará al usuario con el mensaje “Se ha borrado el dispositivo”. En la pantalla del terminal, se mostrará un mensaje “Restableciendo datos de fábrica” y el terminal se apagará y reiniciará mostrando el menú de configuración inicial.

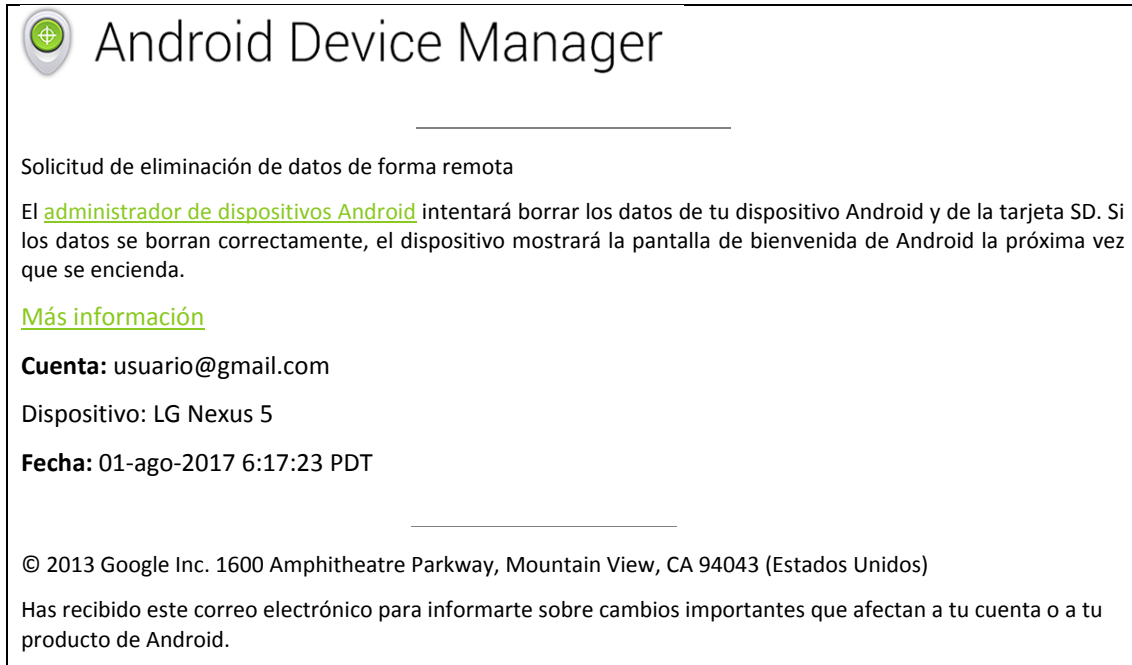
✓ Prueba a llamar a tu teléfono

❓ Cierra sesión en tu teléfono

✓ Ponte en contacto con la empresa de transportes

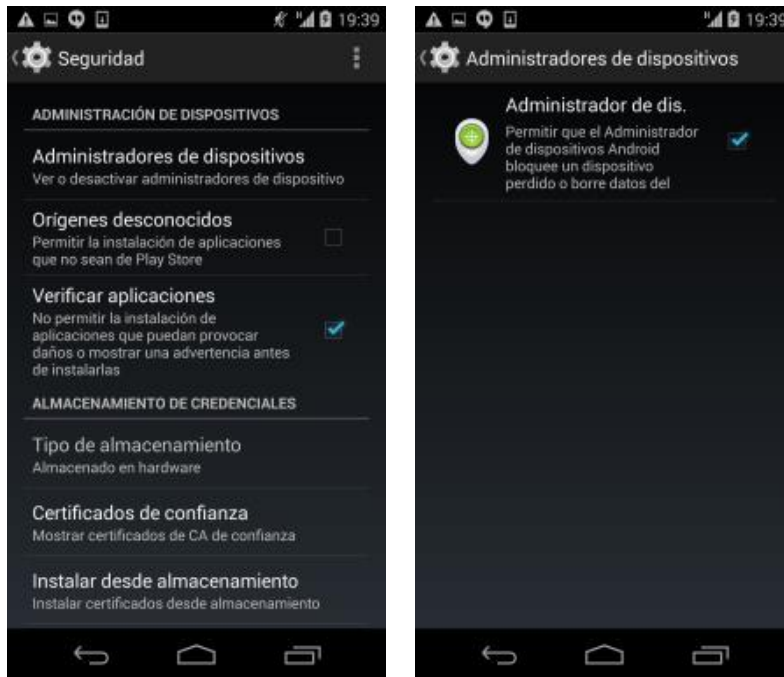
✓ Se ha borrado el dispositivo

466. En el pasado, tras lanzarse la acción de borrado del dispositivo móvil, el administrador de dispositivos enviaba un mail a la cuenta de Google del usuario del dispositivo informando de que se la solicitud de borrado de datos había sido enviada y que el administrador de dispositivos Android intentaría borrar los datos del dispositivo y de la tarjeta SD (el contenido de ese mensaje se ilustra a continuación). A fecha de elaboración de la presente guía, dicho mensaje no es enviado:

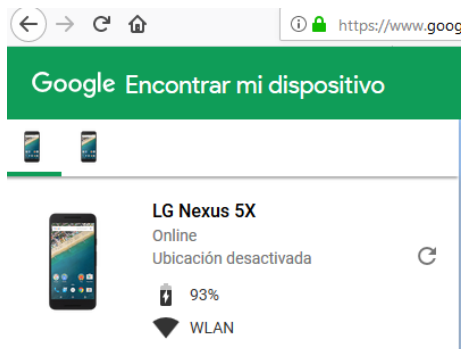


467. Otros dispositivos móviles con versiones de Android más antiguas, anteriores a la versión Android 5.x, también pueden disponer del administrador de dispositivos Android (aunque pudiera no estar habilitado por defecto), ya que el mismo fue introducido por Google en una de las actualizaciones del componente (y app) asociado a los Servicios de Google Play⁴⁵ (sin ser necesario realizar una actualización de la versión del sistema operativo):

⁴⁵ <http://www.howtogeek.com/179638/not-getting-android-os-updates-heres-how-google-is-updating-your-device-anyway/>

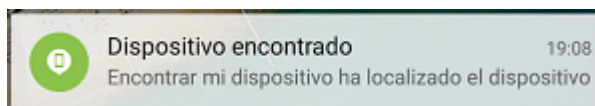


468. Desde Android 5.x, el administrador de dispositivos Android está habilitado por defecto.
469. En el caso de dispositivos móviles con varios usuarios, únicamente el usuario administrador podrá habilitar o deshabilitar el administrador de dispositivos “Encontrar mi dispositivo”.
470. Si el servicio de ubicación del dispositivo móvil estuviese desactivado en “Ajustes - [Personal] Ubicación”, la opción “Localizar (este dispositivo de forma remota)” se mostraría inhabilitada y el interfaz web de gestión remota informaría de este hecho mediante el mensaje “Ubicación desactivada”:



471. En versiones anteriores de Android, como la 5.1.1, al realizarse un cambio en la configuración de las opciones de ubicación remota desde el propio dispositivo móvil, el interfaz web de gestión podía no reflejar el cambio inmediatamente y seguir mostrando el mensaje de “Ubicación desactivada”. En este caso, será necesario salir de la interfaz web de gestión y volver a entrar para refrescar la información del estado del dispositivo móvil.

472. Las acciones realizadas desde el interfaz web generan notificaciones en el centro de notificaciones del dispositivo móvil. Por ejemplo, cuando se accede a la opción de localización y se solicita encontrar el dispositivo, en el terminal se mostrará una notificación “Dispositivo encontrado - Encontrar mi dispositivo ha encontrado ...”. Si se ha solicitado el bloqueo del dispositivo, también se mostrará una notificación en el terminal con el contenido del mensaje de bloqueo. Estas notificaciones podrían desvelar a un usuario no autorizado las tareas de gestión realizadas.



473. Recientemente, Google incorporó a su interfaz de administración de la cuenta de usuario de Google (concretamente, en el apartado “Inicio de sesión y seguridad”), el apartado “Actividad de los dispositivos y eventos de seguridad”, en el cual se pueden ver y gestionar eventos que, en caso de haberse extraviado el dispositivo móvil, permiten detectar si se está realizando algún acceso desde él en la cuenta de Google del usuario. Para obtener más detalles sobre este servicio, se recomienda consultar el capítulo “20.7. Inicio de sesión y seguridad”.

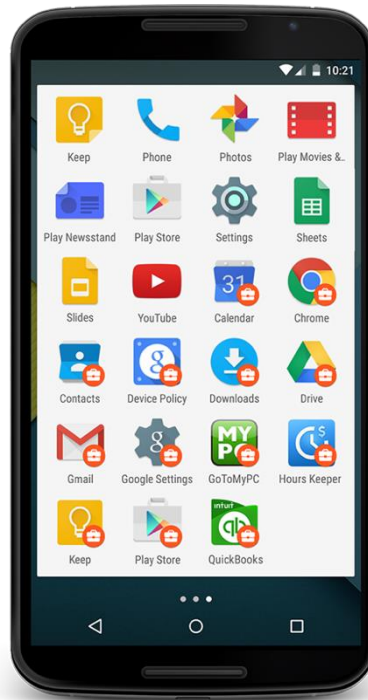
8.2. ANDROID FOR WORK

474. Android for Work [Ref.- 197] es un entorno centrado en que los usuarios puedan aumentar su productividad laboral o profesional, permitiéndoles utilizar en el entorno de trabajo sus dispositivos móviles Android, incluyendo las mismas herramientas que usan en su vida móvil personal.
475. El término Android for Work pasó a denominarse simplemente Android en diciembre de 2016 [Ref.- 514], al considerar Google que la funcionalidad de Android for Work ya estaba disponible en la mayoría de dispositivos móviles Android, pudiéndose emplear todos ellos en entornos de trabajo de manera estándar. Igualmente Play for Work pasó a denominarse simplemente Google Play.
476. Las APIs y la funcionalidad de Android for Work, disponibles en Android y en Google Play para gestionar de manera consistente y uniforme los dispositivos móviles Android, fueron integradas en el sistema operativo Android y en las APIs estándar de esta plataforma móvil a partir de esa fecha.
477. Desde Android 5.x Google ha extendido significativamente el soporte empresarial de Android, protegiendo los datos empresariales y los contenidos privados haciendo uso de zonas de almacenamiento separado para los datos de trabajo y personales.
478. Android 5.x se introduce en el entorno de trabajo (o *workplace*), con un nuevo entorno que permite la gestión de tareas de aprovisionamiento [Ref.- 505], iniciadas por una app de administración del dispositivo (*Device Administrator*). Este administrador de dispositivo puede crear un perfil gestionado o de trabajo (*managed* o *work profile*), que se añade de forma complementaria al perfil personal del usuario del dispositivo (si éste creó uno previamente), habilitando el uso de BYOD (*Bring Your Own Device*) en entornos corporativos.
479. Las notificaciones tanto del perfil personal como de trabajo, así como las tareas o apps recientes en ejecución, se muestran en una vista unificada, aunque los datos

gestionados por cada perfil se mantienen aislados del otro perfil, incluso aunque una misma app esté disponible en ambos perfiles.

480. En el caso de los dispositivos móviles propiedad de la organización pero que pueden también ser utilizados en el plano personal (COPE, *Corporately-Owned Personally-Enabled*), el administrador de la organización puede instalar una app propietaria del dispositivo (*Device Owner*) en los nuevos terminales, y distribuirlos preinstalados con ésta [Ref.- 505].
481. Esta app es una versión especializada de una app de administración del dispositivo (*Device Administrator*) que tiene capacidades especiales para añadir o eliminar usuarios adicionales, y para gestionar los ajustes globales de configuración. Solo puede existir una instancia de este tipo de app por dispositivo móvil.
482. La app (o en su caso una app administradora del dispositivo) se encargará de instalar un perfil gestionado o de trabajo (*managed* o *work profile*) en el dispositivo móvil, qué coexistirá con la cuenta personal del usuario.
483. Un perfil de trabajo permite a la organización definir y administrar los datos y apps corporativas a nivel empresarial, coexistiendo con el resto de datos personales del usuario en el mismo dispositivo móvil [Ref.- 516].
484. Mediante los perfiles de trabajo, los administradores de la organización pueden gestionar de forma más segura el entorno de trabajo, independientemente del entorno personal, y sin restringir la utilización de otros datos y apps personales por parte de los usuarios.
485. Para poder definir, configurar y aplicar un perfil de trabajo en Android 5.x, o versiones posteriores de Android, es necesario disponer de una solución empresarial de gestión de dispositivos móviles (o MDM, *Mobile Device Management*), junto a una app asociada instalada en el dispositivo móvil (que actuará como controlador de las políticas de los dispositivos móviles empresariales). El perfil de trabajo permite definir múltiples opciones en la política de seguridad empresarial, similares a las descritas previamente para las soluciones MDM (ver apartado “8. Gestión empresarial de dispositivos móviles basados en Android”).
486. Es posible verificar si un dispositivo móvil dispone de un perfil de trabajo instalado desde el menú “Ajustes - Cuentas”. En el caso de disponer de un perfil administrado, éste se mostrará en la sección de trabajo [Ref.- 516].
487. Android for Work permite separar las apps de trabajo de las apps personales, con el objetivo de separar ambos mundos, el personal y el de trabajo, no sólo a nivel de los datos sino también de la funcionalidad.
488. En el caso de disponer de apps que son gestionadas dentro del perfil de trabajo por el administrador de la organización, denominadas apps gestionadas, los iconos asociados se muestran en el Launcher con un indicador de trabajo⁴⁶ (icono naranja con un maletín blanco):

⁴⁶ <https://developer.android.com/about/versions/lollipop.html#Work>



489. El administrador del dispositivo puede restringir el acceso a apps del sistema desde el perfil gestionado o de trabajo, como por ejemplo el acceso a la cámara.
490. Cada perfil dispone de su propio espacio de almacenamiento, por lo que no se recomienda que las apps compartan ficheros a través de mensajes (o *intents*), ya que la referencia a un fichero que es válida en una app no tiene porqué serlo en otra (si está asociada a otro perfil).
491. En su lugar, se deben emplear referencias a contenidos (no a ficheros). Así, por ejemplo, el administrador de dispositivo puede establecer que la captura de imágenes sea gestionada por la app de Cámara en el perfil personal, y la referencia a contenido especificará dónde se puede almacenar la foto. Ésta corresponderá a una ubicación donde podrá escribir la app Cámara y desde dónde podrá leer la app que inició la captura de la imagen (mediante un *intent*) [Ref.- 503].
492. Adicionalmente, Android 6.x añade soporte para múltiples capacidades de Android for Work (algunos de ellos detallados a continuación), como controles para dispositivos mono-usuario propiedad de una organización, instalación y desinstalación silenciosa de apps y certificados digitales, aceptación automática de actualizaciones de sistema operativo, o notificaciones del estado del entorno de trabajo, para que el usuario pueda identificar fácilmente que está trabajando dentro de una app gestionada (o de trabajo) o que hay tareas de apps pertenecientes al perfil gestionado (o de trabajo) ejecutando de fondo.
493. Android 6.x incorpora nuevos cambios en Android for Work, como la posibilidad de ver las llamadas asociadas a contactos de trabajo en el histórico de llamadas de la app de “Teléfono”, incluso desde el contexto personal, o todo un conjunto de cambios en el comportamiento asociado a las APIs disponibles para los gestores de la política de seguridad del dispositivo móvil, por ejemplo, por parte de una app administradora del dispositivo [Ref.- 602].
494. Asimismo, Android 6.x incorpora controles avanzados para la app propietaria del dispositivo en dispositivos móviles empleados en entornos COSU (*Corporate-Owned*,

Single-Use), pudiendo deshabilitar (o habilitar de nuevo) el keyguard, la barra de estado, el arranque seguro (safe boot), etc [Ref.- 603].

495. Por otro lado, se permite la instalación y desinstalación silenciosa de apps por parte de la app propietaria del dispositivo, sin la intervención del usuario, junto a la selección silenciosa por parte de la app propietaria del dispositivo de certificados digitales empresariales cuando una app solicita que se seleccione un certificado, sin que el usuario sea preguntado al respecto. Esta app también puede delegar en otra app la gestión de certificados digitales.
496. Las capacidades empresariales permiten obtener remotamente datos de uso de Android. La app propietaria del perfil puede consultar los datos del perfil que gestiona, mientras que la app propietaria del dispositivo puede acceder a los datos de uso del usuario principal gestionado.
497. Adicionalmente, la política de seguridad definida por la app propietaria del dispositivo puede establecer que se instalen automáticamente las actualizaciones de sistema operativo, o postponer su aceptación (incluso por parte del usuario), hasta un periodo de 30 días. Es posible también definir la ventana de tiempo diaria en la que se deberían aplicar las actualizaciones, por ejemplo, cuando el dispositivo móvil (si es utilizado en un kiosko) no está siendo utilizado.
498. Tanto la app propietaria del perfil como la app propietaria del dispositivo pueden establecer una política de permisos para gestionar todos los permisos en tiempo de ejecución de Android 6.x solicitados por las apps instaladas en el dispositivo móvil. El perfil se encargará de permitir y/o denegar las solicitudes de permisos silenciosamente, o de preguntar al usuario. Si el perfil se encarga de la gestión de ciertos permisos, el usuario no podrá posteriormente modificar la elección realizada por el perfil para dichos permisos desde “Ajustes”.
499. Los ajustes de las redes VPN en Android 6.x son visibles desde “Ajustes [Conexiones Inalámbricas y Redes] - Más... - VPN”, y las notificaciones asociadas dependen de la configuración de la red VPN. Para la app propietaria del perfil las notificaciones dependen de si el perfil ha sido configurado como gestionado, personal o ambos, y para la app propietaria del dispositivo las notificaciones dependen de si la VPN se ha configurado para todo el dispositivo móvil.
500. Por otro lado, los perfiles de configuración Wi-Fi que han sido añadidos por una app propietaria de un perfil son eliminados si se borra dicho perfil del dispositivo móvil.
501. Asimismo, se dispone de la posibilidad de bloquear las configuraciones Wi-Fi añadidas por una app propietaria del dispositivo, de manera que el usuario no podrá borrarlas ni modificarlas. El usuario, sin embargo, sí podrá añadir o modificar las configuraciones de otras redes Wi-Fi. Por otro lado, la app propietaria del dispositivo tiene el privilegio para poder borrar o modificar cualquier configuración Wi-Fi, incluso las que no han sido creadas por ella.

9. ACCESO FÍSICO AL DISPOSITIVO MÓVIL

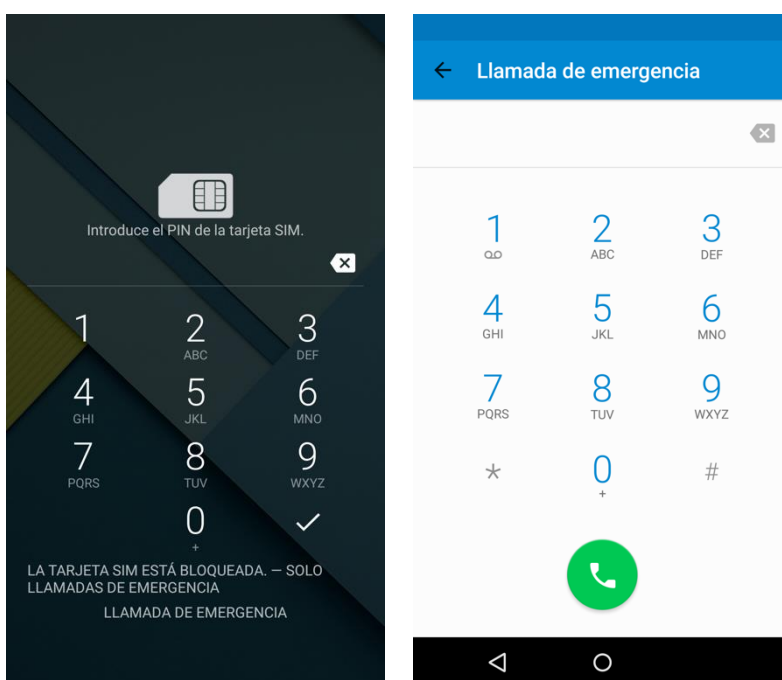
502. La posibilidad de disponer de acceso físico al dispositivo móvil, incluso sólo temporalmente, permitiría a un potencial atacante acceder a los contenidos del mismo o hacer uso de los servicios de telefonía móvil, o cualquier otra funcionalidad o servicio, disponibles.

503. Para evitar ambos tipos de acceso es posible fijar un método de acceso tanto en la tarjeta SIM (mediante un PIN, *Personal Identification Number*) como en el propio dispositivo móvil.

9.1. PIN DE LA TARJETA SIM

504. El PIN de la tarjeta SIM (*Subscriber Identity Module*) bloquea el acceso no autorizado a los servicios y capacidades de telefonía móvil asociados a la propia tarjeta SIM. Si la tarjeta SIM está bloqueada (se desconoce el código PIN), únicamente se permite la realización de llamadas de emergencia (mediante el número de teléfono 112).

505. Sin embargo, si sólo se establece el PIN en la tarjeta SIM y no en el dispositivo móvil (ver apartado “9.2. Código de acceso al dispositivo móvil”), aún es posible para un potencial atacante acceder al terminal directamente, incluyendo sus datos y apps, tras extraer físicamente la tarjeta SIM del dispositivo móvil:



506. Si se ha establecido un PIN en la tarjeta SIM, al arrancar el dispositivo móvil no es posible acceder al mismo mediante ningún botón, ya que Android continúa solicitando el PIN de la tarjeta SIM para permitir el acceso al terminal, siendo necesario extraer la tarjeta SIM previamente para disponer de acceso al terminal sin introducir el PIN de ésta.

507. La disponibilidad de un PIN por defecto asociado a la tarjeta SIM depende del operador de telefonía móvil, siendo muy habitual que las tarjetas SIM tengan fijado un valor por defecto que es proporcionado en la documentación del contrato del operador de telefonía móvil facilitada al usuario al solicitar sus servicios.

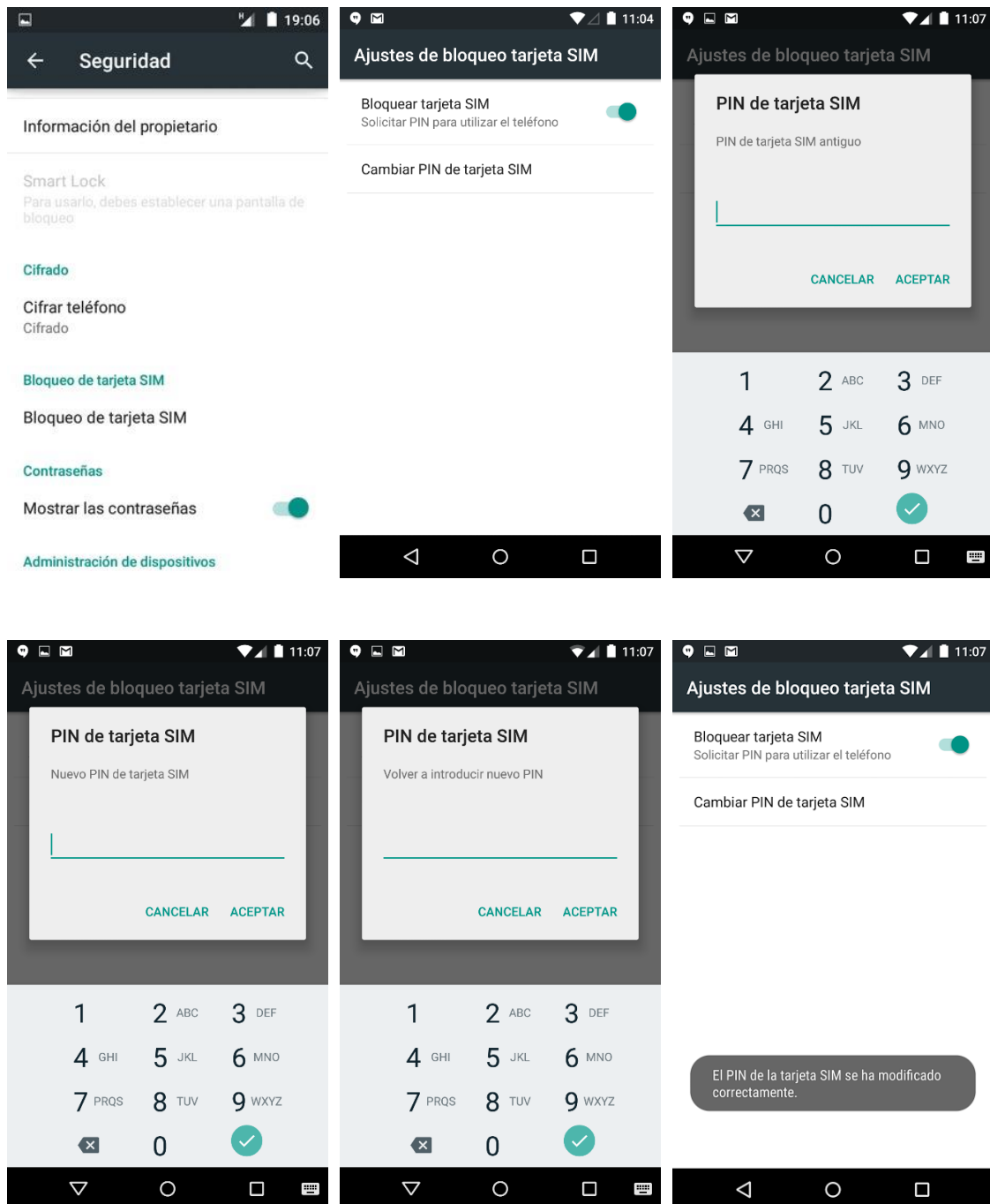
508. El estándar de la industria empleado en la actualidad define un código de 4 dígitos (0-9) como PIN o código de acceso para proteger la tarjeta SIM, sin embargo, se recomienda hacer uso de un PIN de mayor longitud, en concreto, de 8 dígitos (longitud máxima permitida).

509. Android permite emplear un PIN de la tarjeta SIM con un valor de entre 4 y 8 dígitos.

510. Pese a la debilidad de un PIN de 4 dígitos frente a ataques de adivinación o fuerza bruta, los operadores de telefonía móvil y fabricantes de dispositivos móviles implementan

otros mecanismos para evitar este tipo de ataques, como el bloqueo de la tarjeta SIM tras tres intentos de acceso fallidos. En ese caso, para poder desbloquear la tarjeta SIM es necesario emplear una segunda clave de acceso denominada PUK (*PIN Unlock Key*).

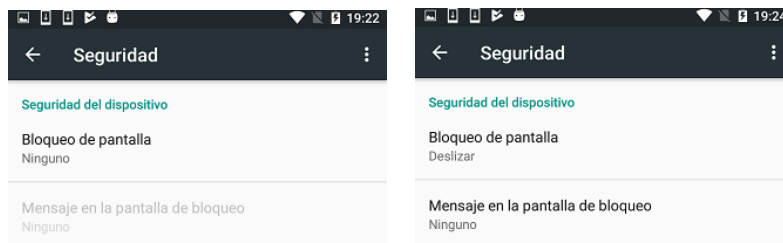
511. Los dispositivos móviles Android 6.x, y posteriores, permiten forzar la utilización de un PIN para la tarjeta SIM (opción “Bloquear tarjeta SIM”), así como fijar o modificar el PIN asociado a la tarjeta SIM (opción “Cambiar PIN de tarjeta SIM”), a través del menú “Ajustes [Personal] - Seguridad [Bloqueo de tarjeta SIM] - Configurar bloqueo de tarjeta SIM”:



512. Se recomienda por tanto fijar en la tarjeta SIM la restricción que requiere introducir un PIN para hacer uso de ésta, y modificar el valor por defecto del PIN, fijando el PIN de la tarjeta SIM con un valor o secuencia de números que no sea fácilmente adivinable, es decir, excluyendo valores típicos como 0000, 1111 ó 1234.
513. Debe tenerse en cuenta que cada vez que el dispositivo móvil sale del “Modo avión” (es decir, cuando este modo es desactivado; menú “Ajustes [Conexiones Inalámbricas y Redes] - Más... - Modo avión”), no se solicitará el PIN de la tarjeta SIM al usuario (tal y como ocurría en versiones previas de Android), al activarse de nuevo los servicios de telefonía móvil. El valor del PIN ha sido almacenado en memoria (o cacheado) para poder disponer de nuevo de acceso a la tarjeta SIM sin que sea necesario introducir el PIN.

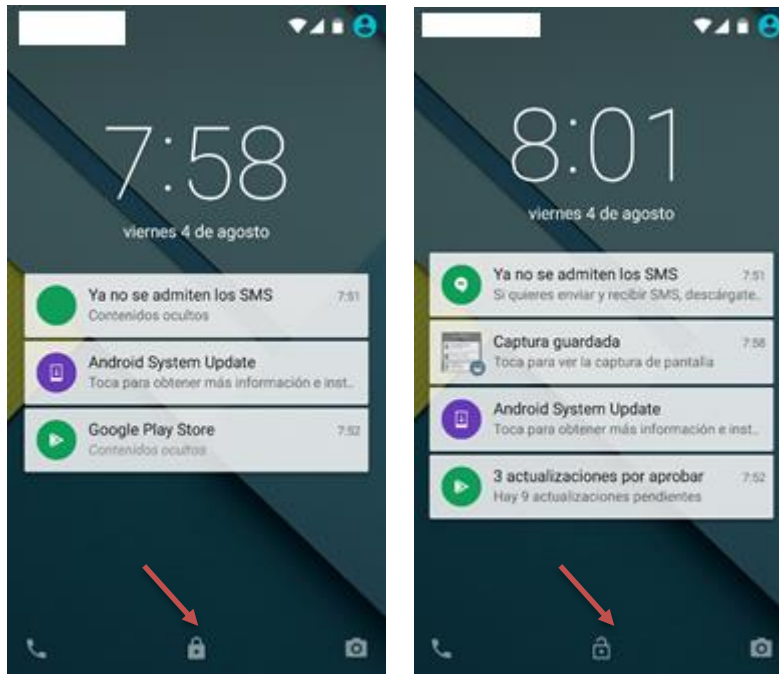
9.2. CÓDIGO DE ACCESO AL DISPOSITIVO MÓVIL

514. El código de acceso (PIN, contraseña, patrón de acceso, etc.) del dispositivo móvil bloquea el acceso no autorizado al terminal, incluyendo sus datos, capacidades de comunicación y aplicaciones móviles (o apps).
515. El patrón (o gesto) fue empleado como método original de desbloqueo en Android, y la posibilidad de usar un PIN o contraseña se añadió en Android 2.2.
516. Una vez el dispositivo móvil está bloqueado, únicamente se permite la realización de llamadas de emergencia (112) sin el código de acceso del terminal. Para ello es necesario marcar el número de teléfono de emergencias tras pulsar el texto “Llamada de emergencia” (situado en la parte inferior de la pantalla).
517. Sin embargo, si únicamente se establece el código de acceso en el dispositivo móvil y no un PIN en la tarjeta SIM (ver apartado “9.1. PIN de la tarjeta SIM”), aún sería posible para un potencial atacante acceder físicamente al terminal, extraer la tarjeta SIM y hacer uso de la misma en otro terminal, incluidos sus servicios y capacidades de telefonía móvil asociados.
518. Por defecto, los dispositivos móviles basados en Android no disponen de un código de acceso para evitar accesos no autorizados al terminal.
519. Se recomienda por tanto establecer un código de acceso al dispositivo móvil a través del menú “Ajustes [Personal] - Seguridad [Seguridad del dispositivo] - Bloqueo de pantalla”:

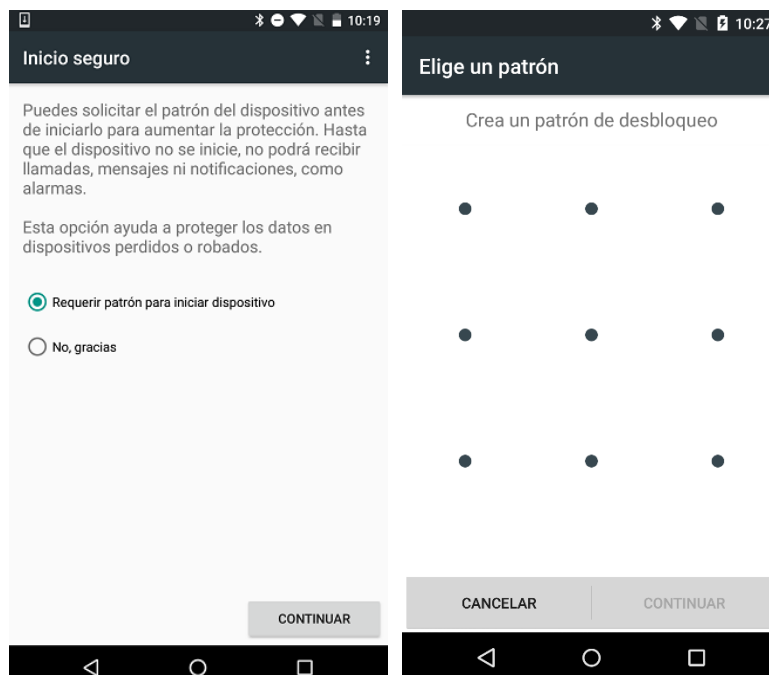


520. Android permite establecer múltiples tipos de códigos de acceso en la pantalla de desbloqueo, también conocida como *keyguard* en Android. El método que se encuentre activo en un momento concreto es el que aparece bajo “Ajustes [Personal] - Seguridad - Seguridad de la pantalla - Bloqueo de pantalla” y, para cambiarlo, el dispositivo solicitará confirmación del código de acceso actual.
521. “Sin seguridad” (o “Ninguno”): deshabilita por completo la pantalla de desbloqueo, pudiéndose acceder directamente a toda la funcionalidad del dispositivo móvil.

522. “Deslizar”: no establece ningún código de acceso, siendo necesario únicamente deslizar el icono con un candado abierto situado en la parte inferior de la pantalla de desbloqueo hacia arriba (hacia la parte superior de la pantalla). Este icono de candado abierto informa además de que el teléfono no tiene establecida pantalla de bloqueo, lo cual podría favorecer que alguien lo sustrajese.



523. “Patrón”: permite establecer un patrón (o gesto) de desbloqueo de pantalla, mediante el establecimiento de un patrón o secuencia de movimientos (en una matriz de 3x3 puntos ubicada en la pantalla del dispositivo) que permitirá desbloquear el dispositivo móvil. El patrón debe comprender un mínimo de 4 puntos y un máximo de 9, aplicándose una serie de reglas (como, por ejemplo, no siendo posible pasar por encima de un punto y que éste no forme parte del patrón).

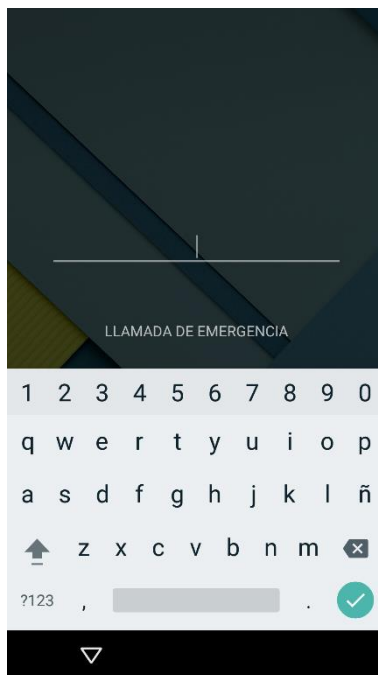


524. Android almacena bajo “/data/system” un hash SHA-1 sin semilla del patrón de acceso configurado (concretamente, en el fichero “gesture.key” para dispositivos con solo un usuario y bajo “/data/system/users/<user_id>/gesture.key” para dispositivos multi-usuario). Al no tener semilla, es factible calcular todas las posibles combinaciones de patrón, por lo que disponer del fichero “gesture.key” (para acceder al cual es necesario disponer de acceso al dispositivo móvil como root) valdría para que un potencial atacante pudiera adivinar u obtener el patrón.
525. “PIN”: Permite establecer un PIN o código numérico tradicional, compuesto por al menos cuatro dígitos (0-9), no desvelándose en la pantalla de desbloqueo la longitud del mismo. Actualmente existe una limitación máxima de 16 dígitos para el PIN (si se excede, el terminal mostrará un mensaje que informa de que el PIN debe tener menos de 17 dígitos).



526. El método de PIN también hace uso de un hash almacenado, pero, a diferencia del del patrón, se emplea una semilla aleatoria de 64 bits, que se almacena en la base de datos *locksettings.db*.
527. “Contraseña”: permite establecer una contraseña alfanumérica, compuesta por un mínimo de cuatro y un máximo de 16⁴⁷ caracteres alfanuméricos (incluyendo, si se desea, letras minúsculas, mayúsculas, dígitos y símbolos de puntuación) y por tanto, constituyéndose como la opción más segura y recomendada desde el punto de vista de seguridad. Si se excede la longitud máxima de la contraseña, de nuevo al igual que con el PIN, el terminal mostrará un mensaje indicando que el número de caracteres de la contraseña ha de ser inferior a 17.

⁴⁷ <https://android.stackexchange.com/questions/154588/why-and-how-to-increase-16-character-lockscreen-password-limit>

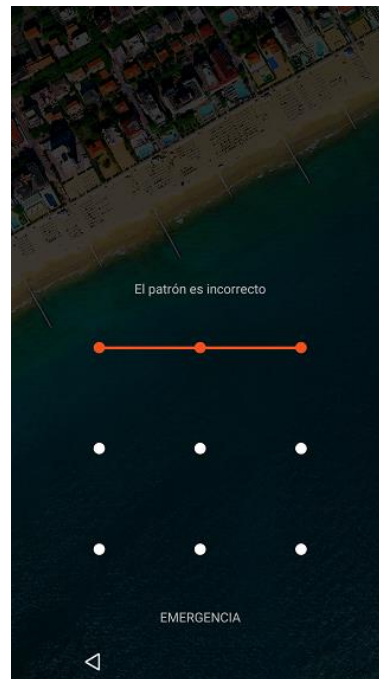
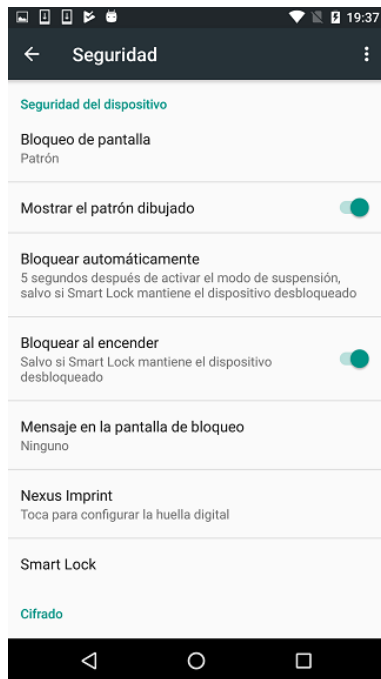


528. Adicionalmente, desde Android 4.0 (*Ice Cream Sandwich*) se dispone de la opción de “Desbloqueo facial” (denominado *Face Unlock*). Este método de desbloqueo ha dejado de ser una opción por sí misma (dentro del apartado “Seguridad” de los “Ajustes” de Android) y se ha integrado como parte de *Smart Lock* desde Android 5.x (siendo renombrado a *Trusted Face*, o cara de confianza). Este método permite emplear biometría para desbloquear el dispositivo móvil mediante reconocimiento facial (ver apartado “9.5. Desbloqueo mediante Smart Lock”).
529. Al emplearse el “Desbloqueo facial”, en el caso en que no se pueda reconocer al usuario, debe fijarse un método de desbloqueo alternativo, pudiéndose elegir entre “Patrón”, “PIN” o “Contraseña”.
530. “Huella dactilar digital” (o *Nexus Imprint*): Adicionalmente, desde Android 6.x es posible desbloquear el dispositivo móvil mediante la huella dactilar digital del usuario (ver apartado “9.3. Huella dactilar digital (*fingerprint*)”).
531. Si se activa el cifrado completo del dispositivo móvil (ver apartado “10. Cifrado de datos en Android”), en Android 6.x incluso algunas de las opciones más sencillas e inseguras para el desbloqueo del dispositivo móvil, como “Sin seguridad” o “Deslizar”, también estarán disponibles (a diferencia de cómo ocurría en versiones previas de Android, como 4.x).
532. Las opciones “Sin seguridad” o “Deslizar” están completamente desaconsejadas desde el punto de vista de seguridad, ya que exponen el dispositivo móvil a accesos no autorizados si un potencial atacante obtiene acceso físico al mismo, incluso temporalmente.
533. Asimismo, la utilización de la opción de “Desbloqueo facial” está desaconsejada desde el punto de vista de seguridad, ya que es posible desbloquear el dispositivo móvil empleando una fotografía o imagen del usuario.

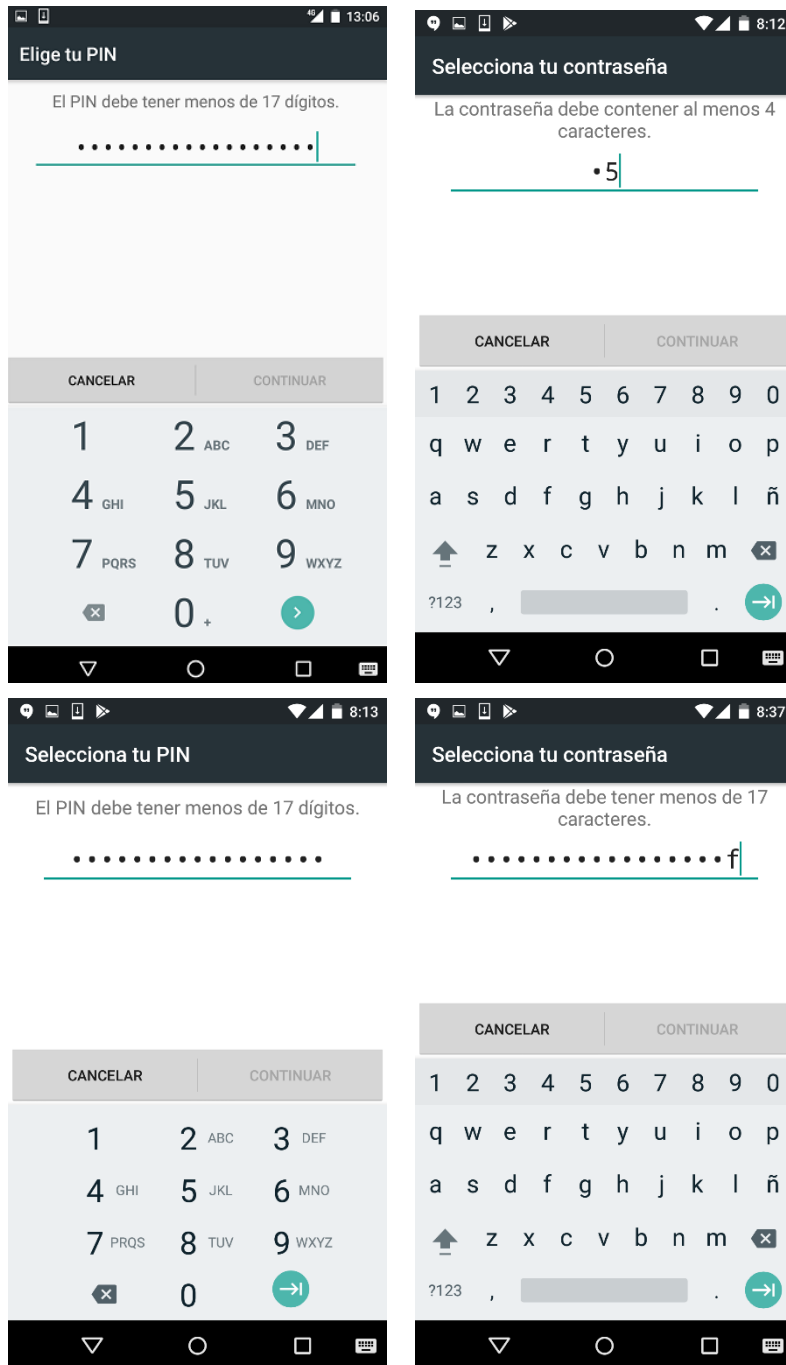
534. Por este motivo, versiones previas de Android (en concreto, disponible desde Android 4.1, *Jelly Bean*), han añadido opciones como por ejemplo “Reconocimiento facial (Solicitar parpadeo al desbloquear)”, para verificar que no se está empleando una fotografía estática. Sin embargo, esta verificación también puede ser potencialmente evitada empleando imágenes animadas o vídeos. En Android 6.x esta opción no se incluye.
535. Adicionalmente, Android 4.1 también introdujo la opción “Mejorar el reconocimiento facial”, que permite capturar la cara del usuario en distintos escenarios (distintas iluminaciones, con o sin gafas, afeitado y sin afeitado, etc), con el objetivo de obtener los rasgos principales de la misma.
536. En el caso de Android 6.x, la opción equivalente sigue estando disponible a través de Smart Lock desde el menú “Ajustes - [Personal] Seguridad - [Seguridad del dispositivo] Smart Lock - [Reconocimiento facial] - Mejorar el reconocimiento facial”.
537. Al seleccionar la opción “Patrón”, Android proporciona la ayuda necesaria para que el usuario aprenda a crear un patrón de desbloqueo, siendo necesario que el patrón incluya al menos cuatro puntos de los nueve (matriz de 3x3 puntos) en los que se divide la pantalla del dispositivo móvil.
538. El número máximo de puntos posibles en el patrón de desbloqueo es de nueve, ya que no es posible repetir la selección de un mismo punto de la matriz de 3x3.
539. Con las anteriores restricciones, el número máximo de combinaciones posibles para los patrones de desbloqueo de Android es de 389.112 [Ref.- 208].
540. Por tanto, se recomienda emplear patrones de desbloqueo complejos, que hagan uso de un mayor número de puntos, como por ejemplo, un mínimo de 6 a 9 puntos (y en ningún caso del número mínimo de tan sólo 4 puntos).



541. Asimismo, se recomienda emplear patrones que no correspondan con iniciales del nombre de usuario o letras comunes del abecedario, como por ejemplo C, L, M, N, O, P, etc.
542. En caso de seleccionar un patrón de desbloqueo, es posible definir si el patrón es o no visible en la pantalla durante el proceso de desbloqueo del dispositivo móvil mediante la opción “Mostrar el patrón dibujado” (habilitada por defecto).



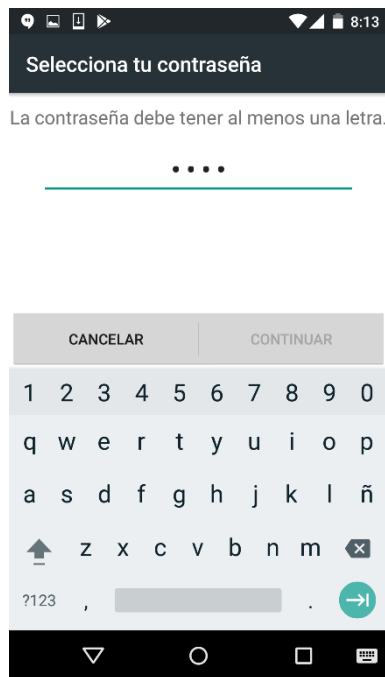
543. Aunque se deshabilite la opción de mostrar el patrón dibujado, en Android 6.x, al igual que ocurría en Android 5.x, se proporcionará una respuesta táctil durante la introducción del patrón mediante una pequeña vibración al seleccionar cada punto de la matriz de 3x3 puntos, lo que permite al usuario confirmar que está introduciendo el patrón correcto.
544. Desde el punto de vista de seguridad se recomienda no habilitar el uso de un patrón visible (que dibujaría las líneas de unión entre los puntos que conforman el patrón), para evitar que alguien con acceso visual temporal sobre la pantalla del dispositivo móvil durante el proceso de desbloqueo pueda obtener el patrón empleado.
545. El tamaño mínimo tanto del PIN como de la contraseña alfanumérica en Android es de 4 dígitos o caracteres. El tamaño máximo de ambos es de 16 dígitos o caracteres respectivamente:



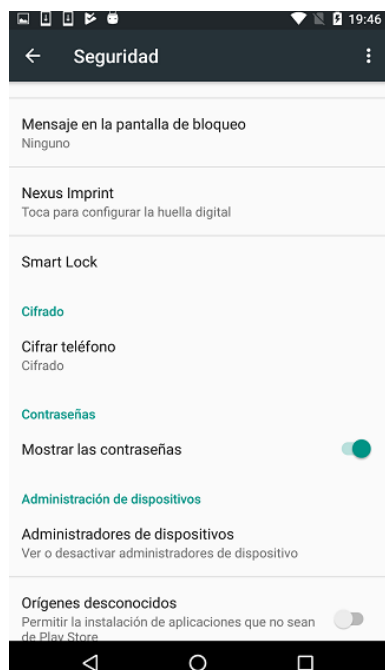
546. Android no realiza ninguna verificación de seguridad sobre el valor del PIN o contraseña elegidos, permitiendo el uso de secuencias simples de dígitos o caracteres, como por ejemplo secuencias conocidas, que se repiten o que siguen un patrón entre sus dígitos o letras, como 1111, 1234, aaaa, abcd, etc.

547. Adicionalmente, en el caso de emplear una contraseña alfanumérica (opción recomendada), por defecto Android no aplica restricciones complejas sobre su contenido, no obligando a que contenga valores en diferentes categorías de las cuatro siguientes: letras minúsculas, letras mayúsculas, números (o dígitos) y símbolos de puntuación.

548. La única restricción de las contraseñas es que contengan al menos una letra, para diferenciarlas de los PIN, basados únicamente en dígitos:

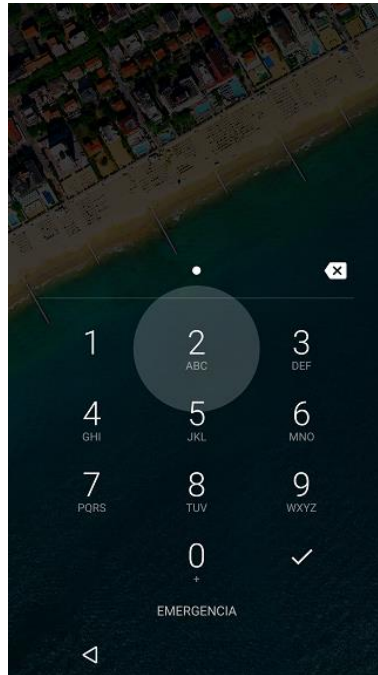


549. Al emplear una contraseña de acceso, Android permite definir si se muestran o no los valores de los caracteres introducidos (en concreto, únicamente el último dígito o carácter pulsado) mientras se escribe en la pantalla de desbloqueo, a través de la opción “[Contraseñas] Mostrar las contraseñas” (habilitada por defecto) y disponible desde el menú “Ajustes [Personal] - Seguridad [Seguridad del dispositivo]”.



550. Desde el punto de vista de seguridad se recomienda no habilitar el uso de contraseñas visibles, para evitar que alguien con acceso visual temporal a la pantalla del dispositivo móvil durante el proceso de desbloqueo pueda obtener la contraseña empleada.

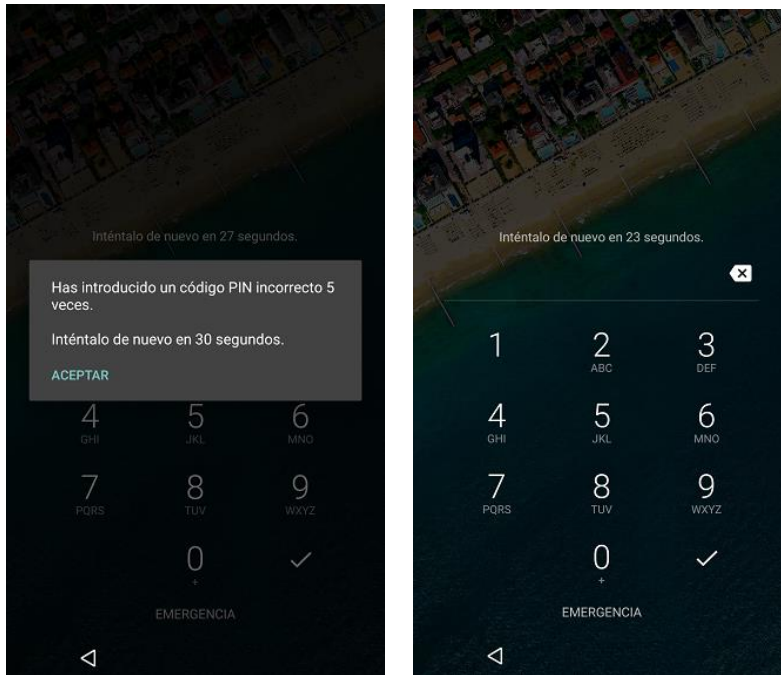
551. En el caso de utilizar un PIN, esta configuración sólo aplicaría durante el proceso de configuración y selección del PIN, ya que la pantalla de desbloqueo siempre muestra (mediante la iluminación de la tecla empleada y la representación numérica correspondiente) el dígito pulsado por el usuario, aunque éste no se muestre en el campo de introducción del PIN. Por este motivo, entre otros, se debe prestar especial atención a quién dispone de acceso visual a la pantalla del dispositivo móvil durante el proceso de desbloqueo.



552. Pese a la debilidad asociada al uso de un PIN de 4 dígitos frente a ataques de adivinación o fuerza bruta, Android implementa un mecanismo que hace que sólo sea posible introducir cinco códigos de acceso (PIN, contraseñas o patrones) incorrectos cada periodo de (al menos) 30 segundos, independientemente de si el valor introducido es siempre el mismo.

553. Tras introducir cinco veces un código de acceso incorrecto el dispositivo móvil bloquea la posibilidad de acceso durante 30 segundos, notificando al usuario este hecho y mostrando un contador de cuenta atrás que indica los segundos restantes hasta poder volver a intentar acceder al dispositivo móvil.

554. Si, transcurrido el plazo para poder volver a introducir el código de acceso, volviesen a superarse los 5 intentos fallidos, se mostrará un mensaje que indicará el total de intentos fallidos de introducción del código desde la última vez que el dispositivo se desbloqueó con éxito.



555. Este mecanismo sólo permite la realización de ataques de adivinación o fuerza bruta del código de acceso con un máximo de 600 intentos por hora. Este cálculo considera el caso ideal para el atacante, con un máximo de cinco intentos cada 30 segundos, despreciando el tiempo empleado para realizar los propios intentos de acceso.
556. Como regla general, es recomendable actualizar a la última versión del sistema operativo que esté disponible, pues a lo largo de la historia de Android ha habido vulnerabilidades que han afectado al método de desbloqueo y al código de acceso al dispositivo [Ref.- 145].
557. Para proceder a modificar el código de acceso del dispositivo móvil, en caso de disponer de un valor ya fijado, es necesario introducir el código de acceso (PIN, contraseña o patrón) actual. Este mecanismo de seguridad evita que un tercero con acceso temporal no autorizado al dispositivo móvil, en caso de encontrarse el dispositivo móvil desbloqueado, pueda modificar el código de acceso existente actualmente sin conocerlo.
558. La pantalla de desbloqueo, o *keyguard*, de Android ha permanecido sin novedades prácticamente desde Android 2.x hasta la versión 5.x, salvo por las capacidades multi-usuario añadidas en Android 4.x (tabletas) y 5.x (*smartphones*).
559. Sin embargo, mientras que en versiones anteriores a Android 4.x, las aplicaciones de terceros podían mostrar ventanas en la capa *keyguard*, por ejemplo para interceptar el botón Home en apps de tipo kiosko, desde Android 4.x la incorporación de ventanas a esta capa sólo está permitida para aplicaciones de sistema (a través de un permiso de tipo *signature*) [Ref.- 159].
560. Desde Android 6.x, con el objetivo de habilitar las capacidades de auditoría de los códigos de acceso o contraseñas, el fichero “*device_policies.xml*” (disponible bajo “/data/system/” y solo accesible por root) almacena los detalles del formato establecido según la política de seguridad del dispositivo móvil para el código de acceso actual.

561.El formato del fichero es el siguiente, y desvela detalles como la longitud o el tipo de categorías permitidas para los caracteres que deben conformar la contraseña (letras mayúsculas o minúsculas, números, símbolos, etc.) [Ref.- 209]:

```
<policies setup-complete="true">
...
<active-password length="6" letters="0" lowercase="0" nonletter="6"
               numeric="6" quality="196608" symbols="0" uppercase="0">
</active-password>
</policies>
```

562.Los detalles de este fichero podrían facilitar a un potencial atacante (que haya obtenido acceso como root en el dispositivo móvil) la realización de ataques de diccionario o fuerza bruta sobre el código de acceso o contraseña, al dar pistas a un potencial atacante que le permitan reducir el conjunto total de posibles combinaciones según la política de seguridad establecida.

563.Android 6.x introduce nuevas modificaciones para permitir la autenticación o desbloqueo del dispositivo móvil mediante una huella dactilar digital, que también afectan al almacenamiento del código de acceso y de otras contraseñas [Ref.- 620].

564.El *gatekeeper* es un demonio de Android 6.x encargado de la gestión (registro y verificación) de los códigos de acceso del usuario. El código de acceso del usuario es convertido en una representación binaria del mismo (denominada *password handle*), y almacenado en forma de firma criptográfica, cuyo formato depende de la implementación del HAL (*Hardware Abstraction Layer*) del fabricante del dispositivo móvil, por ejemplo, haciéndose uso del TEE (*Trusted Execution Environment*) en el caso de la versión AOSP de Android mediante *scrypt* (como algoritmo de derivación de claves) con una semilla (o *salt*), y un identificador asociado a cada usuario [Ref.- 620].

565. El objetivo del *gatekeeper* es almacenar de manera más robusta los diferentes códigos de acceso en Android, y con un nivel de seguridad similar, de manera que no sea más sencillo lanzar ataques de *cracking* (diccionario o fuerza bruta) sobre el patrón de desbloqueo (al no emplearse una semilla) que sobre un PIN o contraseña (tal como ocurría en la implementación de versiones previas de Android).

9.3. HUELLA DACTILAR DIGITAL (*FINGERPRINT*)

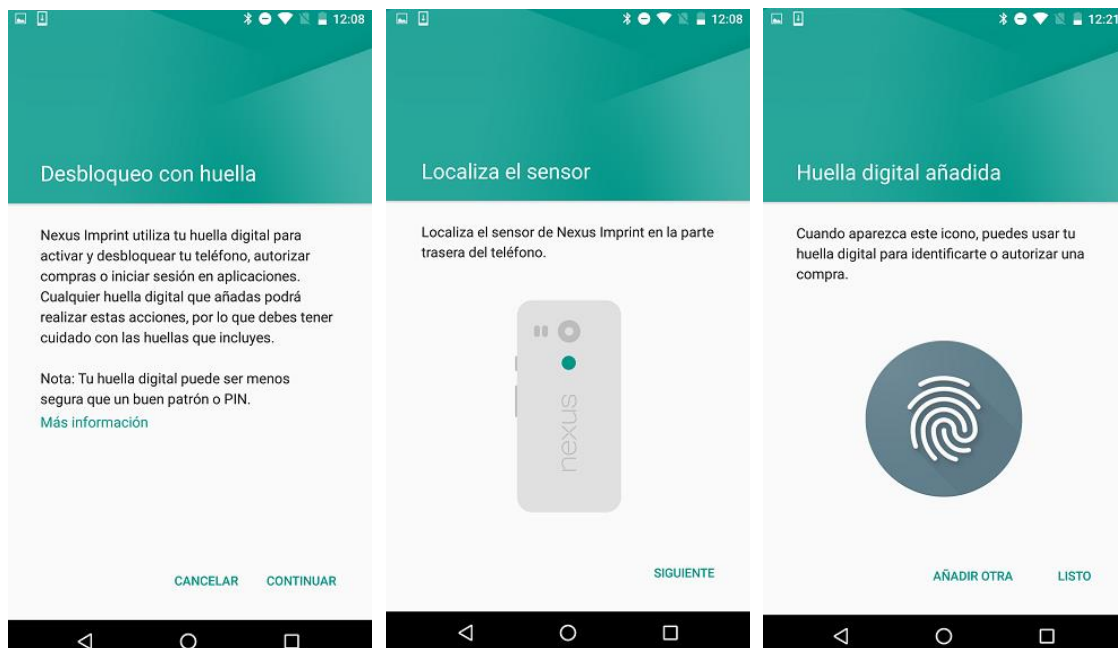
566.Desde Android 6.x se ofrece soporte nativo para llevar a cabo el desbloqueo de la pantalla a través de autenticación mediante una huella dactilar digital (o *fingerprint*). Estas capacidades únicamente están disponibles en aquellos dispositivos móviles que cuentan con un sensor de huella, como por ejemplo el Nexus 5X o 6P.

567.Existen en el mercado múltiples dispositivos móviles (*smartphones*) basados en Android 4.x y 5.x con sensor de huella dactilar digital, pero que no disponían de soporte nativo por parte de Android para su utilización (ni de APIs asociadas), por lo que hacían uso de una implementación propietaria de cada fabricante, dando lugar a debilidades de seguridad [Ref.- 610].

568.Algunos fabricantes de dispositivos móviles Android han diseñado implementaciones inseguras del sensor de huella dactilar digital, permitiendo tanto la interacción directa del kernel de Android (Linux) con el sensor hardware (y las librerías y servicios asociados), o incluso almacenando la representación de la huella dactilar digital del usuario en el sistema de ficheros sin cifrar [Ref.- 611]. Como resultado, una vez se

dispone de acceso como root al dispositivo móvil, es posible tener acceso completo a la representación de la huella dactilar digital del usuario.

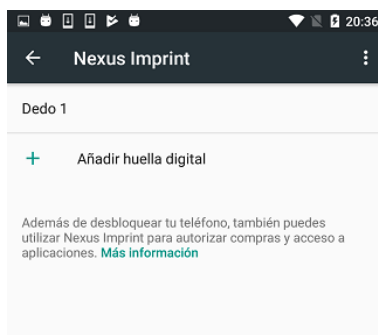
- 569.El sistema de autenticación por huella dactilar digital de los dispositivos móviles Nexus (y Pixel) se conoce como (Nexus) Imprint. La implementación de Imprint en los dispositivos móviles Nexus (y Pixel) obliga al almacenamiento y reconocimiento de la huella dactilar digital en el TEE (*Trusted Execution Environment*), con acceso hardware limitado y protegido por una política de SELinux.
- 570.El mecanismo de autenticación mediante huella dactilar digital puede ser más inseguro que el uso de un patrón, PIN y (especialmente) contraseña robustos, debido a que el usuario desvela (o distribuye) a lo largo del día y en numerosos lugares (incluyendo el propio dispositivo móvil) una copia o representación de su huella dactilar.
- 571.Por tanto, el mecanismo de autenticación mediante huella dactilar digital pretende ofrecer un equilibrio razonable entre la protección de la pantalla de desbloqueo del dispositivo móvil y la usabilidad, conveniencia y facilidad a la hora de tener que introducir el código de acceso decenas o centenares de veces al día por parte del usuario.
- 572.Como mecanismo de protección adicional, a la hora de configurar una huella dactilar digital es necesario seleccionar un mecanismo de autenticación de respaldo (patrón, PIN o contraseña), que será solicitado al usuario cada vez que se reinicia el dispositivo móvil, si no es posible reconocer su huella dactilar digital después de 5 intentos de acceso fallidos, al cambiar de usuario en el dispositivo móvil (en escenarios multi-usuario), y después de 48 horas sin haber desbloqueado el dispositivo móvil con el método de respaldo, añadiendo así múltiples factores de autenticación [Ref.- 609].
- 573.Es posible configurar una huella dactilar digital a través del menú “Ajustes - [Personal] Seguridad - [Seguridad del dispositivo] Nexus Imprint”. Al acceder a este menú es necesario introducir el código de acceso configurado actualmente en el dispositivo móvil.



- 574.Desde dicho menú se muestra la pantalla de Nexus Imprint que indica dónde se localiza el sensor de huella dactilar digital (ubicado en la parte posterior del dispositivo móvil

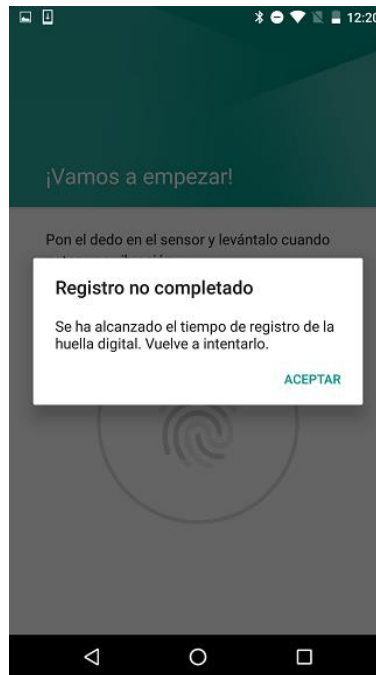
empleado para la elaboración de la presente guía). Una vez localizada su ubicación, el botón “Siguiente” permite comenzar el proceso de reconocimiento de la huella dactilar del usuario, que muestra a través de un tutorial los pasos a seguir. Será necesario colocar y levantar el dedo en múltiples ocasiones (no menos de 6) sobre el sensor hasta que el dispositivo móvil confirme que dispone de los datos de representación de la huella y que esta se ha añadido como método de desbloqueo.

575. Es posible registrar hasta un máximo de 5 huellas dactilares digitales para desbloquear el dispositivo móvil, disponiendo de la posibilidad de renombrar cada una de ellas para su fácil identificación.
576. Como resultado, aparecerá una nueva entrada en la pantalla de Nexus Imprint, denominada por defecto “Dedo 1” (o “Finger 1”). Seleccionando la misma es posible cambiar el nombre que identifica a la representación de dicha huella, por ejemplo, para poder saber a qué usuario y dedo corresponde, o eliminar dicha huella dactilar digital del dispositivo.



577. Una vez registrada la primera huella dactilar digital, durante el proceso de registro inicial (o de una nueva huella posteriormente), se pueden añadir más huellas mediante el botón “Añadir otra”. Una vez registradas todas las huellas dactilares deseadas durante un mismo proceso de registro, se puede finalizar la configuración mediante el botón “Listo”.
578. Debido a que desde la pantalla de Nexus Imprint se pueden añadir, mediante la opción “Añadir huella digital”, hasta un máximo de 5 huellas en total por dispositivo móvil, a la hora de registrar una nueva huella dactilar digital es necesario que se establezca una cadena de confianza mediante la autenticación del usuario, empleando el código de acceso de respaldo. Si transcurre un tiempo entre la introducción del código de acceso y la obtención de la pantalla de Nexus Imprint, y el momento de inicio del proceso de registro y configuración de una nueva huella, se volverá a solicitar al usuario iniciar el proceso de registro y deberá introducir el código de acceso actual de nuevo.
579. En concreto, si transcurren más de 10 minutos entre el inicio del proceso para añadir una huella y la siguiente, o si se tarda ese tiempo desde que se accede al menú de configuración de Nexus Imprint y se inicia el proceso de registro y escaneo de una nueva huella, se interrumpirá el proceso y se mostrará un mensaje de error con el título “Registro no completado”. En este caso, será necesario iniciar el proceso de registro de nuevo, accediendo a la pantalla de Nexus Imprint y debiendo introducir de nuevo el código de acceso (PIN, patrón o contraseña) que esté activo como mecanismo de desbloqueo actualmente. Dicho código de acceso es empleado como mecanismo de respaldo al método de desbloqueo mediante huella dactilar digital, en caso de que no fuera posible autenticarse con la huella dactilar (por ejemplo, porque el usuario haya

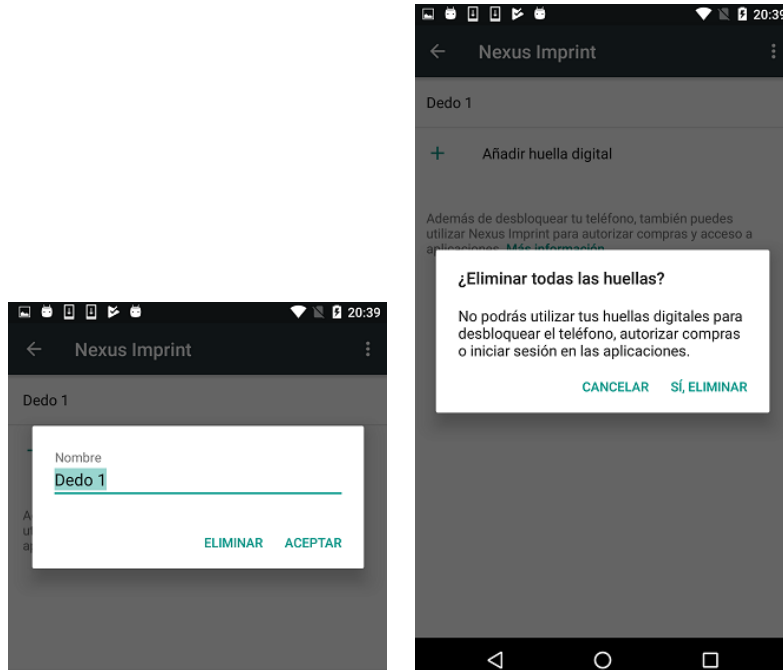
tenido un accidente con el dedo empleado para la autenticación y su huella dactilar se haya visto afectada).



580. Este mecanismo de seguridad evita que un tercero con acceso temporal no autorizado al dispositivo móvil, en caso de encontrarse el dispositivo móvil desbloqueado, pueda registrar una nueva huella dactilar digital sin conocer el código de acceso existente actualmente.
581. El objetivo de proteger la representación (o imagen) de la huella dactilar digital por hardware, tal como ocurre en la implementación utilizada por el dispositivo móvil empleado para la elaboración de la presente guía, es evitar que pueda ser extraída del dispositivo móvil. Asimismo, tampoco esta representación es incluida en las copias de seguridad del dispositivo móvil, o compartida con los servidores de Google.
582. En caso de almacenarse esta representación en el sistema de ficheros (protección por software y opción posible en la implementación de otros modelos de dispositivo móvil Android), debe de hacerse en formato cifrado, adicionalmente al cifrado nativo de la memoria del dispositivo móvil. La representación también debe ser firmada criptográficamente empleando una clave privada específica del dispositivo móvil (y otros valores criptográficos asociados), con el objetivo de que no pueda ser reutilizada en otro dispositivo móvil o entre usuarios del mismo dispositivo móvil [Ref.- 608].
583. La disponibilidad por defecto de las capacidades de huella dactilar digital en Android 6.x ha permitido estandarizar la arquitectura e implementación (incluyendo la guía de buenas prácticas) asociada al uso de este tipo de sensores en Android, mediante una Fingerprint Hardware Abstraction Layer (HAL) que enlaza el sensor hardware y la librería específica proporcionada por el fabricante, con las capacidades disponibles en Android [Ref.- 615].
584. El documento de definición de las reglas de compatibilidad de Google para Android 6.x ("Marshmallow"), "Android (Marshmallow) Compatibility Definition Document (CDD)", define ciertos prerequisites, como que deben limitarse los intentos de acceso al dispositivo móvil al menos durante 30 segundos tras 5 intentos fallidos de autenticación con la huella dactilar digital, que la representación de la huella dactilar

- digital del usuario debe protegerse en una Keystore implementada por hardware, que las verificaciones de la huella deben realizarse en el TEE (o un chip hardware dedicado) y que los datos asociados deben estar cifrados y firmados criptográficamente para que no puedan ser usados fuera del TEE, entre otros [Ref.- 606].
585. Cuando el método de acceso o desbloqueo por huella está activo, en lugar de un candado cerrado, la pantalla de bloqueo mostrará un icono de una huella dactilar en su parte central inferior.
586. La huella dactilar digital puede ser utilizada para desbloquear el dispositivo móvil, pero también se puede emplear para autorizar compras y pagos (mediante Android Pay y Google Play), o para autenticarse dentro de las apps. Cuando tal acción sea posible, el dispositivo móvil mostrará un mensaje solicitando la lectura de la huella dactilar, que en ningún caso se comparte con la aplicación. En ningún momento las apps disponen de acceso a la representación de la huella dactilar digital del usuario, sino que reciben una notificación de confirmación (o rechazo) de la validez de la huella dactilar digital introducida por el usuario.
587. Para ello, Android 6.x añade para los desarrolladores de apps nuevas APIs (FingerprintManager API) para que las apps puedan interactuar con el hardware asociado al sensor de huella dactilar digital. Estas deben de ser utilizadas e integradas conjuntamente con la Keystore de Android (ver apartado “11.1. Android Keystore System: Almacenamiento de credenciales”), junto a un nuevo permiso que debe ser declarado por las apps: `USE_FINGERPRINT`. Las apps pueden integrar las capacidades de autenticación mediante huella dactilar digital con otras nuevas funcionalidades de Android 6.x, como las APIs de pagos móviles (Payment APIs) [Ref.- 603].
588. Adicionalmente, las nuevas APIs de confirmación de credenciales (Confirm Device Credential APIs) permiten a las apps gestionar claves o tokens criptográficos (pudiendo hacer uso de una implementación mediante clave pública o secreta), protegidos por hardware en la Keystore, asociarlos a la pantalla de desbloqueo, y definir políticas de acceso a los mimos (por ejemplo, si el usuario se ha autenticado en el dispositivo móvil en los últimos 5 minutos) [Ref.- 607].
589. De esta forma la app puede autenticar al usuario mediante la autenticación o el desbloqueo del propio dispositivo móvil (en lugar de disponer de un mecanismo de autenticación adicional propio), o conocer si este ha sido desbloqueado recientemente, pudiendo emplear referencias de tiempo de cuándo fue la última vez que se desbloqueó el mismo [Ref.- 603].
590. Esta funcionalidad evita que el usuario tenga que recordar una contraseña adicional para el acceso a la propia app, y elimina posibles errores a la hora de que las apps implementen su propio mecanismo de autenticación y el interfaz de usuario asociado.
591. Si en los ajustes de configuración de la huella dactilar digital se muestra el mensaje “*Screen lock option disabled*”, indica que el administrador del dispositivo móvil ha establecido una política de seguridad que no permite el uso de una huella dactilar digital, obligando al usuario a utilizar un patrón, PIN o contraseña (por ejemplo, en la cuenta de trabajo de Android for Work; ver apartado “8.2. Android for Work”). Con esta configuración, todavía es posible hacer uso de una huella dactilar digital para autorizar compras o autenticarse en apps.

592. Si después de configurar este método de acceso se desea dejar de hacer uso del desbloqueo con huella, es necesario acceder a “Ajustes - [Personal] Seguridad - [Seguridad del dispositivo] Nexus Imprint” y seleccionar una por una las huellas añadidas, pulsando sobre su alias y en la opción “Eliminar”. Con la última huella eliminada se mostrará un mensaje que informa de que no se podrá seguir haciendo uso de las huellas como método de desbloqueo, pago o inicio de sesión en aplicaciones.



9.4. BLOQUEO Y DESBLOQUEO DE PANTALLA

593. El término bloqueo de pantalla refleja el escenario en el que un dispositivo móvil activa la protección de la pantalla mediante un código de acceso.

594. El término desbloqueo de pantalla refleja el escenario en el que un dispositivo móvil requiere que el usuario haga uso del código de acceso definido actualmente en el dispositivo móvil para poder acceder al mismo, a sus datos y aplicaciones. A lo largo de la historia de Android han existido diversas vulnerabilidades asociadas a la pantalla de bloqueo [Ref.- 77]. Dado que el mecanismo de bloqueo es la llave de acceso al dispositivo, se recomienda prestar especial atención a todos los elementos que afectan al mismo.

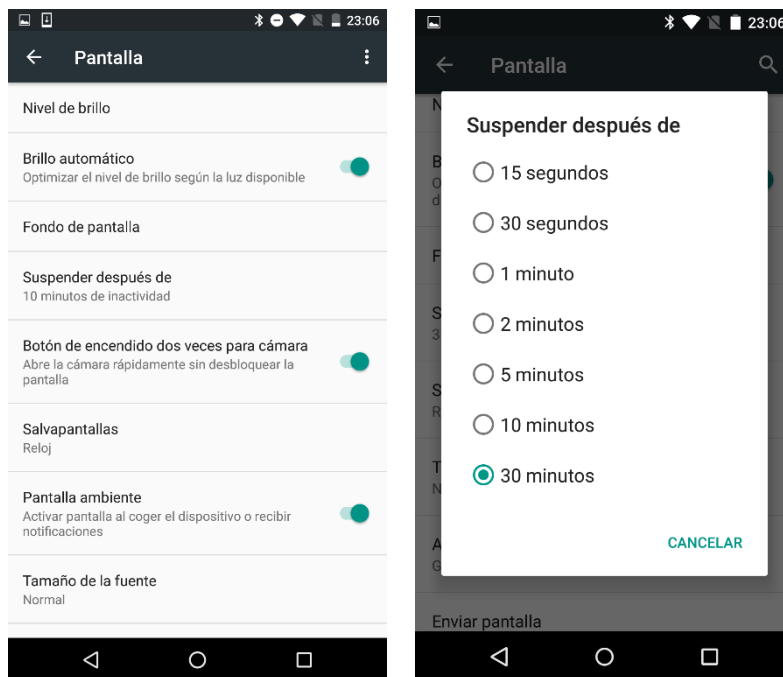
595. El bloqueo de la pantalla del dispositivo móvil puede ser manual o automático. El bloqueo manual tiene lugar cuando el usuario pulsa el botón de encendido (no de manera prolongada, para evitar apagarlo). El bloqueo de pantalla es inmediato tras pulsar este botón. El bloqueo automático se produce al presentarse las condiciones de bloqueo establecidas a través de los diversos ajustes de configuración del dispositivo móvil.

596. Adicionalmente, la pantalla estará bloqueada inicialmente al arrancar el dispositivo móvil.

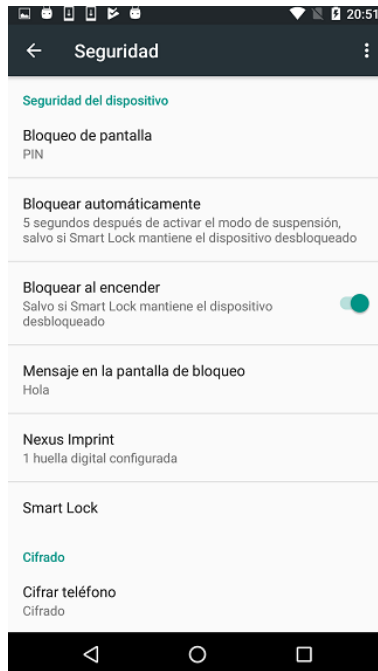
597. Para desbloquear la pantalla activamente, el usuario ha de pulsar en el botón de encendido y emplear el código de acceso definido actualmente en el menú “Ajustes - [Personal] Seguridad - [Seguridad del dispositivo] Bloqueo de pantalla” (ver apartado “9.2. Código de acceso al dispositivo móvil”). A partir de Android 6.x, en caso de haber

registrado una huella dactilar digital a través de la pantalla de configuración de Nexus Imprint, este método también permitirá desbloquear la pantalla (ver apartado “9.3. Huella dactilar digital (*fingerprint*)”).

- 598.El bloqueo automático de pantalla tras un periodo de inactividad está definido por dos factores o parámetros de configuración (analizados en detalle a continuación): por un lado, el temporizador definido para suspender la pantalla tras un periodo de inactividad y, por otro, el temporizador definido para bloquear la pantalla después de haber sido suspendida.
- 599.Se recomienda por tanto establecer el bloqueo del dispositivo móvil tras un tiempo de inactividad, mediante el ajuste de la configuración de ambos parámetros, por ejemplo a 1 minuto. El rango razonable, buscando el equilibrio entre seguridad y usabilidad, debería estar entre 1 y 2 minutos, pero debe ser definido por la política de seguridad de la organización propietaria del dispositivo móvil.
- 600.El temporizador de suspensión de la pantalla por inactividad establece qué tiempo ha de transcurrir desde que el usuario llevó a cabo la última interacción con el dispositivo móvil hasta que la pantalla entre en modo de ahorro de energía y se apague. Este parámetro se define a través del menú “Ajustes [Dispositivo] - Pantalla - Suspender después de”:



- 601.Android proporciona un rango de valores temporales para suspender la pantalla de entre 15 segundos y 30 minutos, siendo el valor por defecto de 30 segundos.
- 602.Como se puede ver, Android no dispone de una opción que permita que la pantalla permanezca indefinidamente activa y que no se suspenda en ningún momento, independientemente del periodo de inactividad, con el objetivo de gestionar el consumo de batería del dispositivo móvil, siendo el periodo máximo de 30 minutos.
- 603.Por otro lado, el temporizador de bloqueo de la pantalla una vez ésta se ha suspendido por inactividad se establece a través del menú “Ajustes [Personal] - Seguridad [Seguridad del dispositivo] - Bloquear automáticamente” (este menú no se muestra si, el método de desbloqueo es “Ninguno” o “Deslizar”, es decir, si no se ha definido un código de acceso).



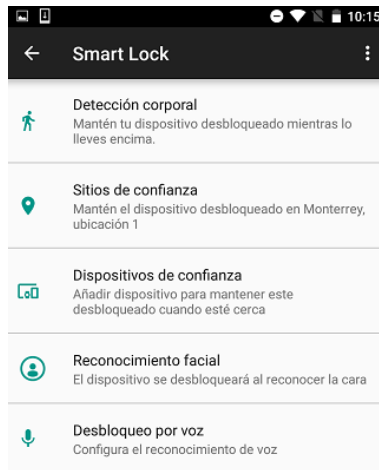
604. Android proporciona un rango de valores temporales para bloquear la pantalla tras suspender el dispositivo móvil de entre 5 segundos y un máximo de 30 minutos, con la posibilidad de bloquear la pantalla inmediatamente (opción más segura), siendo el valor por defecto (una vez fijado un código de acceso) de 5 segundos.
605. Este bloqueo automático no se aplicará si se cumplen algunas de las condiciones asociadas a la funcionalidad Smart Lock (ver apartado “9.5. Desbloqueo mediante Smart Lock”), lo que mantendrá el dispositivo móvil desbloqueado (por ejemplo, al estar en un sitio de confianza, o identificar un dispositivo de confianza).
606. Como se puede ver, Android no dispone de una opción que permita que la pantalla quede sin bloquear indefinidamente tras un periodo de inactividad, opción desaconsejada desde el punto de vista de seguridad en el caso de que existiera, siendo el periodo máximo de 30 minutos.
607. En resumen, se recomienda encontrar el equilibrio entre ambos parámetros de configuración para que se lleve a cabo la activación de la pantalla de desbloqueo tras un periodo de inactividad, por ejemplo, fijando el valor de “Suspender después de” a 1 minuto y el de “Bloquear automáticamente” a 30 segundos, lo que implicaría que pasarían menos de 2 minutos antes del bloqueo automático.
608. Adicionalmente, la configuración asociada al bloqueo de la pantalla del dispositivo móvil tras un periodo de inactividad se complementa con el siguiente parámetro de configuración, que determina si la pantalla debe ser bloqueada cuando la pantalla del dispositivo móvil es apagada manualmente por el usuario mediante el botón de encendido (pero únicamente la pantalla, sin apagar por completo el dispositivo móvil).
609. La opción “Bloquear al encender”, disponible desde el menú “Ajustes [Personal] - Seguridad [Seguridad del dispositivo]”, cuando está activa, implica que el evento de apagar la pantalla manualmente por parte del usuario (mediante el botón de encendido) forzará un bloqueo de la pantalla. Al encenderla de nuevo será necesario siempre introducir el código de acceso para desbloquearla.
610. Sin embargo, si esta opción no es activada, el evento de apagar la pantalla manualmente por parte del usuario es equivalente a que el dispositivo móvil se

suspenda tras un periodo de inactividad. Dependiendo del valor del parámetro “Bloquear automáticamente” (descrito previamente) se bloqueará la pantalla tras el tiempo especificado.

611. Tal como informa el mensaje descriptivo de la opción “Bloquear al encender”, el bloqueo al encender no se aplicará si se cumple alguna condición de la funcionalidad Smart Lock (ver apartado “9.5. Desbloqueo mediante Smart Lock”), lo que, de nuevo, mantendrá el dispositivo móvil desbloqueado.

9.5. DESBLOQUEO MEDIANTE SMART LOCK

612. Smart Lock de Google es una de las principales novedades introducidas en Android 5.x (“Lollipop”). Se trata de una funcionalidad que permite que el dispositivo móvil se mantenga desbloqueado en determinadas circunstancias (por ejemplo, si el dispositivo móvil está en una ubicación configurada por el usuario, o si está conectado a un dispositivo Bluetooth considerando de confianza), a pesar de que se cumplan otras condiciones de bloqueo, por ejemplo, por tiempo de inactividad. Además, Smart Lock permite también el desbloqueo “automático” del dispositivo móvil, omitiendo el resto de mecanismos de seguridad existentes, como el código de acceso, huella dactilar digital, etc., bajo ciertas circunstancias como, por ejemplo, si detecta la cara o la voz registradas por el usuario (en concreto, por el usuario considerado por Android el propietario del dispositivo, en dispositivos multi-usuario).
613. Smart Lock se basa en un concepto denominado “agentes de confianza” (*Trust Agents*) que se introdujo en Android 5.x. Un agente de confianza es un servicio que, de acuerdo a la documentación del *framework* de Smart Lock, notifica al sistema sobre si considera que el entorno del dispositivo móvil es “de confianza” según sus propios criterios de evaluación. En caso de encontrarse en un entorno “de confianza”, el sistema decide cómo relajar la seguridad del dispositivo, por ejemplo, no bloqueando la pantalla [Ref.-206].
614. Para poder utilizar la funcionalidad de Smart Lock, es necesario acceder al menú “Ajustes - [Personal] Seguridad - [Ajustes avanzados] Agentes de confianza - Smart Lock (Google)”.
615. Al activar Smart Lock como agente de confianza, se activará el menú “Ajustes - [Personal] Seguridad - [Seguridad del dispositivo] Smart Lock”, y bajo él se encuentran todas las opciones de configuración de Smart Lock y los distintos métodos de evaluación disponibles. En adelante, este acceso a través de los ajustes será abreviado como menú “Smart Lock”.



616. Al pulsar sobre Smart Lock, siempre se solicitará al usuario el código de acceso al dispositivo móvil. Si no se ha definido ninguno hasta el momento, el dispositivo solicitará que se configure uno antes de poder acceder al menú Smart Lock.

617. Si el dispositivo no se utiliza durante 4 horas o es reiniciado, será necesario desbloquearlo manualmente con el código de acceso establecido actualmente para que las opciones de Smart Lock vuelvan a estar disponibles y operativas.

618. Las opciones de desbloqueo asociadas a Smart Lock, cada una de ellas configurable individualmente, son: [Ref.- 206]

- Detección corporal.
- Sitios de confianza.
- Dispositivos de confianza.
- Reconocimiento facial.
- Desbloqueo por voz.

619. Es importante reseñar que, si se da una situación temporal en las que se requiera que el mecanismo de bloqueo clásico de Android siga activo aunque se cumpla alguna de las condiciones asociadas a Smart Lock, no es necesario acceder al menú Smart Lock, bastará con pulsar momentáneamente el candado de desbloqueo, con lo que se mostrará el mensaje “El dispositivo permanecerá bloqueado hasta que se desbloquee manualmente”.

620. “Detección corporal”: permite mantener el dispositivo móvil desbloqueado cuando el usuario lo lleva encima. Este método está disponible para dispositivos móviles que cuentan con un acelerómetro integrado, de forma que el terminal se mantiene desbloqueado mientras el acelerómetro detecta que aún está en movimiento. En algunos dispositivos móviles, la detección corporal reconoce incluso el patrón que el propietario del dispositivo utiliza (o genera) al caminar. Si el acelerómetro detecta un patrón de desplazamiento que es significativamente diferente al almacenado, es posible que el dispositivo se bloquee. Es importante reseñar que la detección corporal no puede detectar quién tiene el dispositivo móvil encima, por lo que, si un tercero no autorizado dispusiese de acceso al dispositivo móvil mientras éste está desbloqueado, podría conseguir que permaneciese desbloqueado debido a esta función.

621. Adicionalmente, existen otros escenarios de riesgo, como cuando el usuario deja el dispositivo móvil sin bloquear en algún sitio, por ejemplo sobre una mesa, si el mismo

está configurado para bloquearse tras un tiempo (mediante el vencimiento del temporizador de bloqueo automático). Durante ese tiempo el dispositivo móvil aún estará expuesto a ser accedido por un potencial atacante, que podrá mantenerlo desbloqueado mediante la detección corporal.

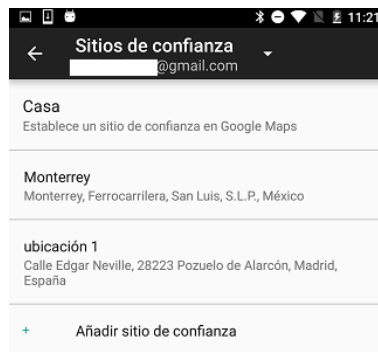
622. Por este, y muchos otros motivos y escenarios detallados posteriormente, los métodos de Smart Lock, como por ejemplo la detección corporal, es significativamente menos segura que un código de acceso (PIN, patrón o contraseña), por lo que se desaconseja su utilización.
623. Otro problema inherente a la detección corporal es el comportamiento del acelerómetro en los medios de transporte. Al utilizar un coche, un autobús, un tren u otro vehículo, el dispositivo móvil puede tardar entre cinco y diez minutos en bloquearse, al seguir detectando movimiento. El desplazamiento en avión o en barco puede provocar que el dispositivo no se bloquee automáticamente en ningún momento. Ambos factores han de tenerse en cuenta por si se considera oportuno bloquear el dispositivo móvil manualmente si fuese necesario.
624. Los datos del acelerómetro sobre el patrón de desplazamiento del usuario se almacenan en el dispositivo móvil, pero se eliminan cuando la función de detección corporal de Smart Lock es desactivada.
625. Para activar la función de Smart Lock de detección corporal, seleccionar el menú Smart Lock, se solicitará el código de acceso al dispositivo, y la opción “Detección corporal”, cambiando el interruptor “No” a la posición de activado o “Sí”.



626. “Sitios de confianza”: permite mantener el dispositivo móvil desbloqueado cuando el dispositivo detecta que se encuentra en una ubicación considerada de confianza, que ha debido ser previamente configurada, como por ejemplo, el domicilio o el lugar de trabajo del usuario. Este método está disponible únicamente para dispositivos móviles que cuentan con un módulo GPS integrado. Hay que reseñar que el dispositivo no se desbloqueará al entrar en el radio de cercanía del sitio de confianza, sino que únicamente se mantendrá desbloqueado si ya se encontraba en una ubicación de confianza, y permanece dentro de ésta.
627. Dado que el servicio de ubicación no es cien por cien preciso, la función sitios de confianza puede mantener el dispositivo desbloqueado en un radio de hasta 80 metros. Por esta razón, desde el punto de vista de seguridad, se desaconseja hacer uso de esta

funcionalidad especialmente en lugares públicos, como el centro de trabajo, cafetería, restaurante, biblioteca, gimnasio, etc., pues el dispositivo móvil podría quedar accesible para un tercero no autorizado.

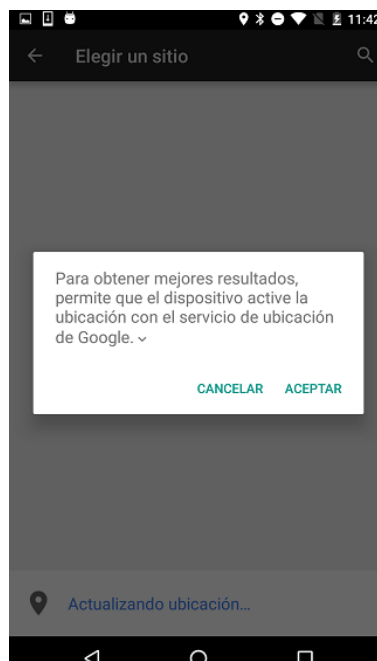
628. Otro aspecto importante a tener en cuenta desde el punto de vista de seguridad es que las señales de ubicación o localización se pueden copiar y/o manipular, por lo que un hipotético atacante podría utilizar equipos especializados para desbloquear el dispositivo móvil en lugares que no son de confianza mediante la falsificación o suplantación de la señal GPS, como si realmente lo fueran.
629. Para configurar los sitios de confianza en Smart Lock, hay que acceder al menú Smart Lock, , se solicitará el código de acceso al dispositivo, y la opción “Sitios de confianza - Añadir un sitio de confianza”.



630. Para activar esta funcionalidad el dispositivo informa al usuario de que es requisito indispensable disponer de conexión a Internet, ya que a la hora de añadir un sitio de confianza, requiere descargar la información de mapas para identificar el sitio a añadir.
631. Si el servicio de ubicación no está activo, el dispositivo móvil también informa al usuario de que es necesario activarlo mediante un mensaje Toast: “Activa el GPS para acceder a sitios de confianza”) para hacer uso de la funcionalidad de sitios de confianza. No obstante, no es necesario activarlo para registrar un nuevo sitio de confianza, por lo que se podría postponer su activación y activar los servicios de ubicación más adelante, a la hora de hacer uso de la funcionalidad de sitios de confianza.
632. Si el servicio de ubicación no está activo, el usuario puede buscar la dirección de interés desplazándose manualmente por el mapa mostrado, o introduciendo los detalles de la dirección en el campo de búsqueda de la parte superior.



633. En el caso de Android 6.x, si el servicio de ubicación no está activo, la barra superior del dispositivo muestra el símbolo de ubicación activa, que permanece así unos segundos mientras se muestra el mensaje solicitando permiso para que el dispositivo active el servicio de ubicación.

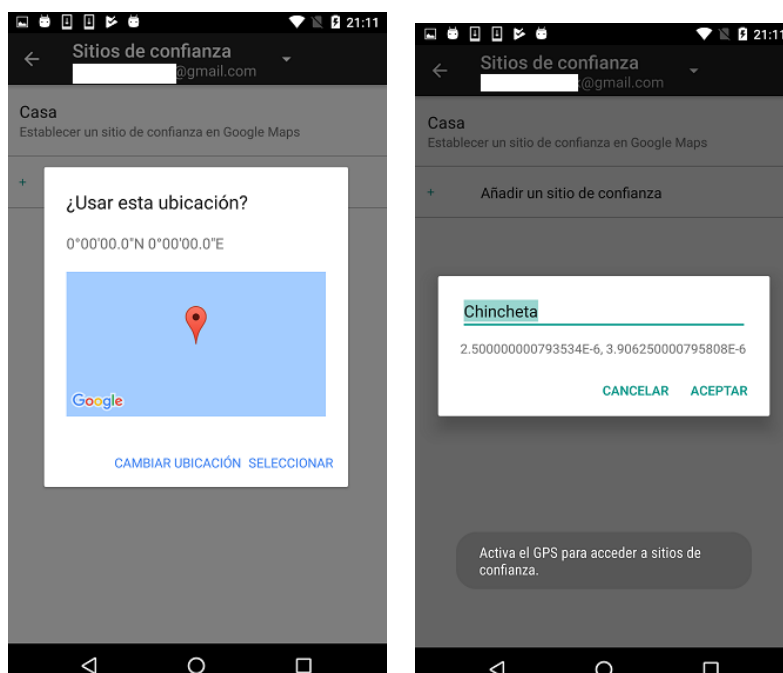


634. Tras disponer de los requisitos necesarios, aparece el menú “Elegir un sitio”, que muestra un mapa de “Google Maps”, con la ubicación actual si el servicio de ubicación está activo (y sobre el Ecuador si no lo está).

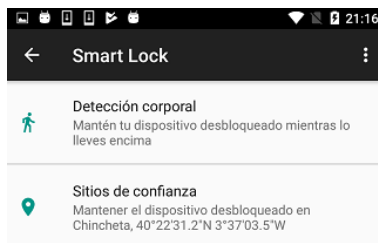


635. Si se desea utilizar la ubicación que se muestra en el mapa como sitio de confianza (que lógicamente requiere que el servicio de ubicación esté activo), se podrá pulsar la opción “Seleccionar esta ubicación”. Si no, se puede pulsar en la lupa que aparece en la esquina superior izquierda del dispositivo móvil, asociada al campo de búsqueda disponible sobre el mapa, para llevar a cabo la búsqueda del sitio de confianza deseado en base a su nombre y/o dirección. La búsqueda puede realizarse mediante el nombre de una dirección o mediante coordenadas GPS (latitud y longitud). También es posible desplazarse tocando sobre el mapa hasta llegar a la ubicación deseada.

636. Tras pulsar en “Seleccionar esta ubicación”, aparecerá una ventana de confirmación “¿Usar esta ubicación?”, que permite “Seleccionar” o “Cambiar ubicación”. Si se pulsa en “Seleccionar”, aparecerá una ventana que permitirá dar nombre a la ubicación (por defecto, muestra las coordenadas de la misma):



637. Al pulsar sobre el lugar elegido, aparecerá la ventana que permite confirmar la ubicación seleccionada, y tras confirmar su registro, se muestra la ventana de edición del sitio de confianza, que permite establecer un nombre para el marcador asociado (por defecto el nombre puede incluir las coordenadas del lugar: latitud y longitud). Ésta será la referencia que aparecerá en el listado de sitios asociado al menú Smart Lock dentro de la opción “Sitios de confianza - <marcador>”.



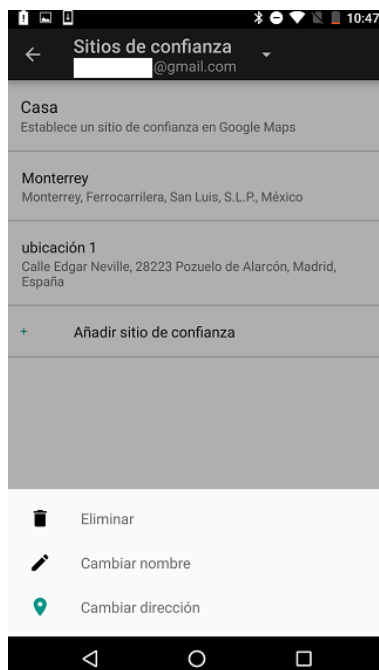
638. La configuración y detalles de los sitios de confianza se almacena en la cuenta de Google del usuario que esté realizando la configuración del sitio de confianza en Smart Lock, y que es mostrada en la parte superior de la pantalla de configuración de “Sitios de confianza”.

639. Por defecto, el menú sitios de confianza presenta un marcador llamado “Casa” que, al pulsarse, permite escribir la dirección particular o acceder a ella a través del mapa. La selección del sitio mediante el mapa hace uso de “Google Maps”. Es importante reseñar, tal como informa el mensaje que se muestra en la parte inferior del dispositivo, que la dirección particular se actualizará en todos los demás productos de Google que la utilicen (por ejemplo, Google Now, Búsqueda de Google y el propio Google Maps).

640. Opcionalmente, en algunas versiones previas de Android (por ejemplo, 5.0.x), también aparecía por defecto el marcador para definir la ubicación del “Trabajo” (además de “Casa”).

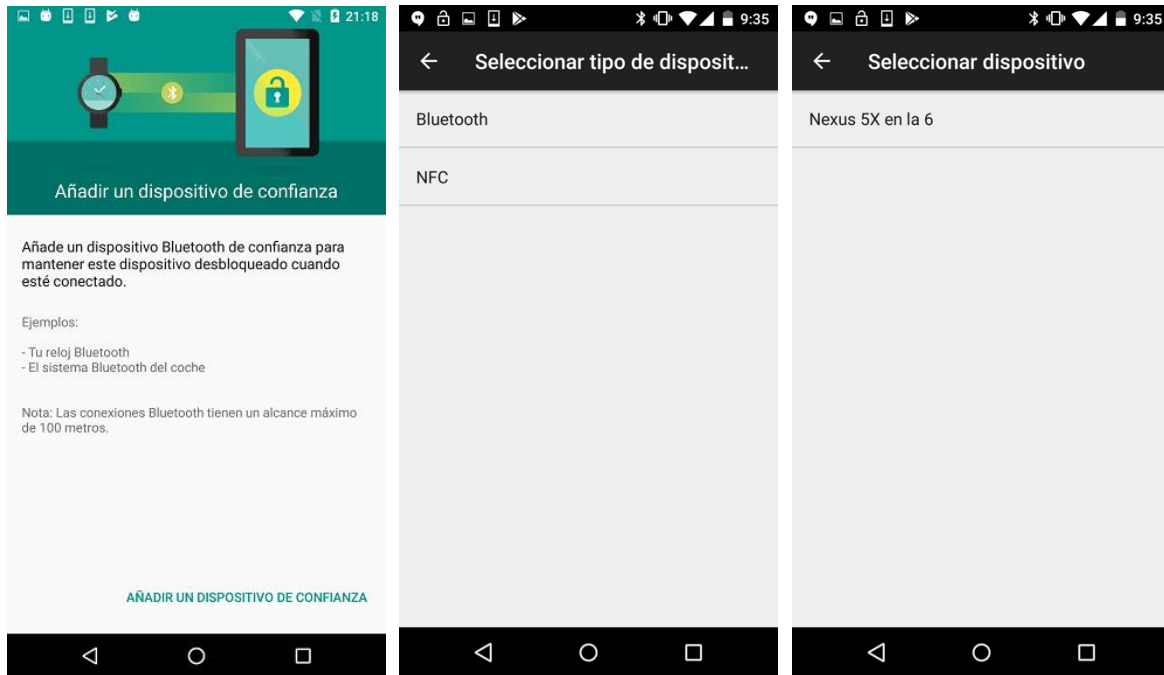
641. Los marcadores existentes por defecto, “Casa” (y opcionalmente “Trabajo”) aparecerán sombreados si no se ha definido en el dispositivo una cuenta de Google.

642. Para eliminar un sitio de confianza, se ha de pulsar brevemente sobre el marcador del sitio que se muestra en el listado del menú “Smart Lock - Sitios de confianza”. Como resultado aparecerá un menú en la parte inferior de la pantalla con varias opciones, como cambiar el nombre, editar la dirección o eliminar el sitio.



643. “Dispositivos de confianza”: mediante esta función, es posible que el dispositivo móvil Android se mantenga desbloqueado cuando esté conectado con otro dispositivo (de confianza) mediante Bluetooth o a través de NFC. Hay que reseñar que el dispositivo móvil no se desbloqueará cuando detecte un dispositivo de confianza, únicamente se mantendrá desbloqueado en presencia de dicho dispositivo si ya se encontraba en ese estado. No se recomienda en ningún caso utilizar como dispositivos de confianza elementos que siempre acompañen al dispositivo móvil, como por ejemplo las fundas o teclados Bluetooth. Tampoco se recomienda confiar en dispositivos que puedan ser sustraídos a la vez que el dispositivo móvil, como, por ejemplo, altavoces Bluetooth portátiles que se transporten en un mismo maletín. Desde un punto de vista de seguridad, tampoco se recomienda establecer esta relación de confianza con un reloj Bluetooth (o cualquier otro dispositivo de tipo *wearable*), ya que ambos podrían ser sustraídos simultáneamente al propietario (por la fuerza o por un descuido), sin que éste dispusiera de margen para bloquearlos.
644. Para configurar un dispositivo de confianza Bluetooth, hay que activar el interfaz Bluetooth en los ajustes del dispositivo móvil y, en primer lugar, establecer un emparejamiento con el dispositivo en el que se va a confiar. Este requisito, y su correcta verificación a la hora de establecerse una conexión Bluetooth entre ambos dispositivos, constituyen una mejora introducida en Android 5.1 (junto a Google Play Services, en abril de 2015), dado que en versiones previas de Android 5.x con Smart Lock, un atacante podía simplemente suplantar la dirección Bluetooth del dispositivo de confianza y, mediante una conexión Bluetooth no cifrada, conseguir que el dispositivo móvil permaneciese desbloqueado [Ref.- 517].
645. Una vez emparejado por Bluetooth el dispositivo de confianza, es necesario acceder al menú “Smart Lock (se solicitará el código de acceso al dispositivo) - Dispositivos de confianza - Añadir un dispositivo de confianza - Bluetooth” (debiendo estar el interfaz Bluetooth activo; ver apartado “15. Comunicaciones Bluetooth”).

646. Como resultado aparecerá la lista de dispositivos Bluetooth emparejados actualmente, de entre los cuales se podrá seleccionar el deseado. Finalmente, se mostrará una pantalla informativa para añadir el dispositivo de confianza seleccionado y se solicitará confirmación por parte del usuario mediante la opción “Sí, añadir”, o “Cancelar”.



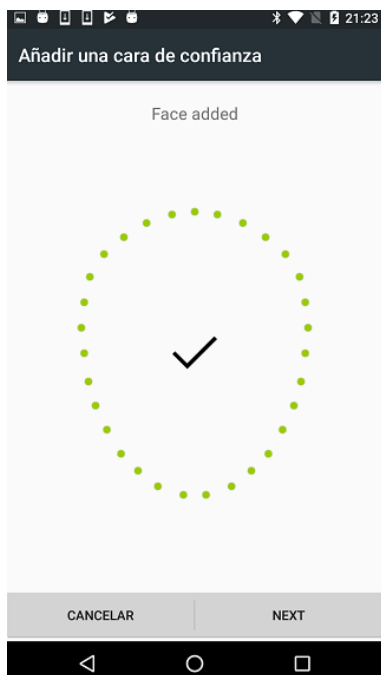
647. Cuando se realiza un emparejamiento con un dispositivo Bluetooth, Smart Lock generará una notificación invitando al usuario a configurar dicho dispositivo como dispositivo de confianza. Si se abre la notificación, se mostrará el menú que permite añadir dicho dispositivo a Smart Lock.

648. Para configurar un dispositivo de confianza NFC, es necesario acceder al menú “Smart Lock (se solicitará el código de acceso al dispositivo) - Dispositivos de confianza - Añadir dispositivo de confianza - NFC” (no siendo necesario que esté el interfaz NFC activo; ver apartado “14. Comunicaciones NFC”). El dispositivo mostrará un mensaje solicitando la activación del interfaz NFC, si estaba apagado, y requerirá acercar (o poner en contacto) el dispositivo móvil con una etiqueta o un dispositivo NFC.

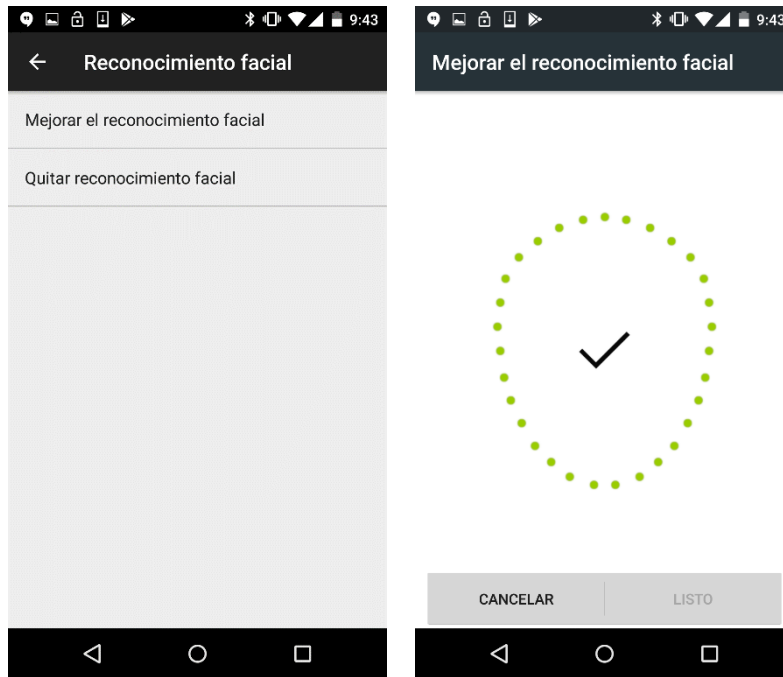
649. “Reconocimiento facial”: este método se introdujo en Android 4.0 (*Ice Cream Sandwich*) bajo el término “Desbloqueo facial” (*Face Unlock*), y dejó de ser una opción por sí misma en los ajustes de configuración para integrarse como parte de *Smart Lock* desde Android 5.x (siendo renombrado a *Trusted face*, o cara de confianza). Este método permite emplear biometría, y en concreto, los rasgos de la cara del usuario para desbloquear el dispositivo móvil mediante reconocimiento facial, tomando previamente, durante el proceso de configuración, una imagen de la cara del usuario.

650. Tras configurar una cara de confianza, desde el menú “Ajustes - [Personal] Seguridad - [Seguridad del dispositivo] Smart Lock - Reconocimiento facial”, el dispositivo móvil intentará identificar la misma cara del usuario cada vez que se intente desbloquear el dispositivo, procediendo a su desbloqueo si la cara es reconocida con éxito a través de la cámara frontal del dispositivo móvil, e indicándolo sutilmente con un icono con un candado abierto situado en la parte inferior de la pantalla de desbloqueo.

651. Uno de los principales inconvenientes de este método es que alguien con rasgos parecidos al usuario podría desbloquear el teléfono, o incluso emplear una fotografía o imagen animada del propietario del terminal para desbloquearlo.
652. Smart Lock no almacena fotos del usuario, sino datos biométricos para reconocer su cara que solo se almacenan en el dispositivo móvil, sin permitir que otras aplicaciones puedan acceder a ellos ni realizar copias de seguridad de los mismos en los servidores de Google [Ref.- 518].
653. Si la cara de confianza está activada, durante el proceso de reconocimiento de la cara, el candado de bloqueo de la parte inferior se transformará en símbolo de cara en lugar de como un candado. Cuando haya conseguido reconocerla, mostrará un candado parpadeante y, al deslizar el dedo hacia arriba, activará la pantalla. Esto puede permitir que un atacante aprenda que esta función está disponible.
654. Para añadir una cara de confianza, hay que entrar en “Ajustes - [Personal] Seguridad - [Seguridad del dispositivo] Smart Lock” (se solicitará el código de acceso al dispositivo) - Reconocimiento facial - Configurar”. Si esta opción está activa, en la pantalla de bloqueo aparecerá brevemente un icono con un símbolo de cara durante el tiempo en el que el terminal esté tratando de reconocer el rostro configurado. Si se consigue reconocerlo, el icono cambiará a un candado abierto que parpadea; en caso contrario, se mostrará un candado cerrado parpadeante.



655. Cuando se esté en condiciones adecuadas para registrar la cara del usuario, según las indicaciones del menú de Smart Lock, pulsar en “Siguiete” para iniciar el proceso de registro. Una vez completado, se puede optar por el menú “Mejorar reconocimiento facial” para registrar otras vistas de la cara y su aspecto en diferentes situaciones.



656. A partir de Android 5.1, se mejoró el proceso de desbloqueo del dispositivo móvil mediante la cara del usuario (Trusted Face), con un nuevo sistema de reconocimiento de caras, menos sensible a condiciones externas de luz, variaciones en la cara (con/sin gafas, con barba o afeitado, etc.), o a la posición del dispositivo móvil.

657. “Desbloqueo por voz”: esta función de Smart Lock, aunque pudiera parecer inicialmente que no desbloquea el acceso a todo el dispositivo móvil, sino únicamente a las capacidades asociadas al servicio “Ok Google”, no es así. El servicio “Ok Google” permite iniciar búsquedas mediante la voz desde la aplicación de Google (o desde cualquier pantalla de inicio de Google Now Launcher), siendo necesario que este servicio esté configurado (ver apartado “22.3. Asistente personal y “Ok Google””).

658. En la integración de “OK Google” (o de desbloqueo por voz) con Smart Lock, y aunque al desbloquearse el dispositivo móvil mediante la voz se muestre en primer lugar la funcionalidad de “Ok Google”, es posible seleccionar el botón para desplazarse a la pantalla previa, o el botón de acceso a la pantalla de inicio, para disponer de acceso completo al dispositivo móvil. Únicamente si se bloquea temporalmente, y de forma manual, el acceso mediante Smart Lock pulsando sobre el candado abierto disponible en la parte inferior de la pantalla de bloqueo, será necesario hacer uso del código de acceso en lugar de la voz para desbloquear de nuevo el dispositivo móvil.

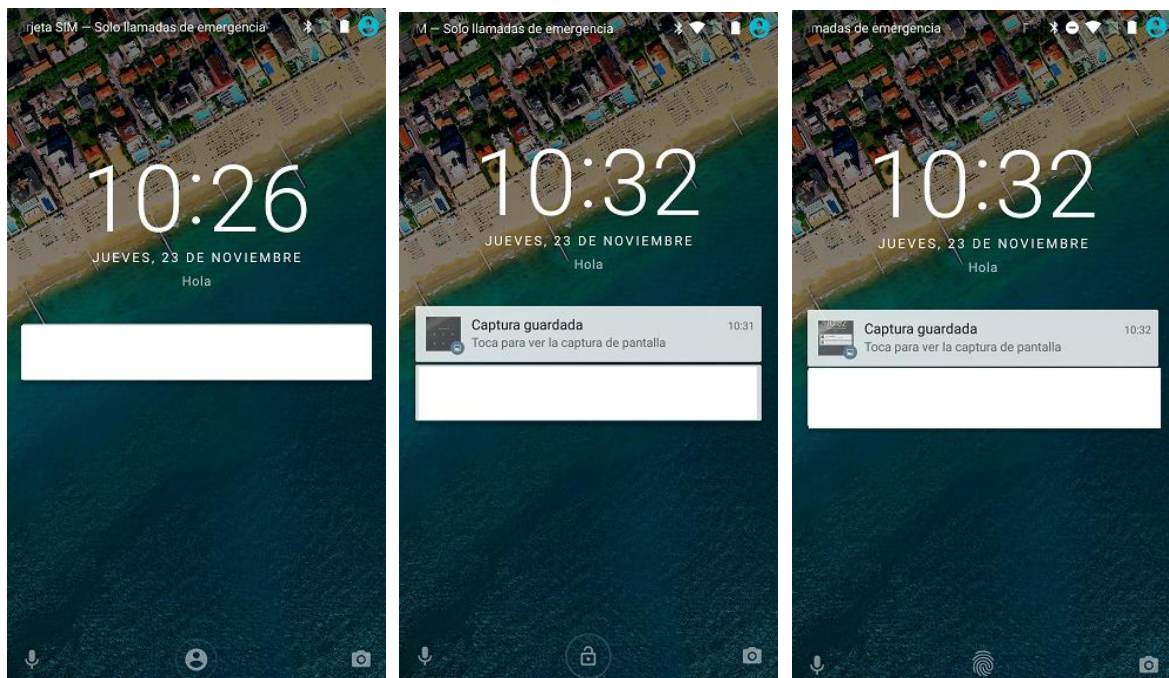
659. El menú de desbloqueo por voz ha evolucionado actualmente, desde Android 5.x, de modo que, además de la opción “En la aplicación Google”, presenta las siguientes opciones (ver apartado “22.3. Asistente personal y “Ok Google””):

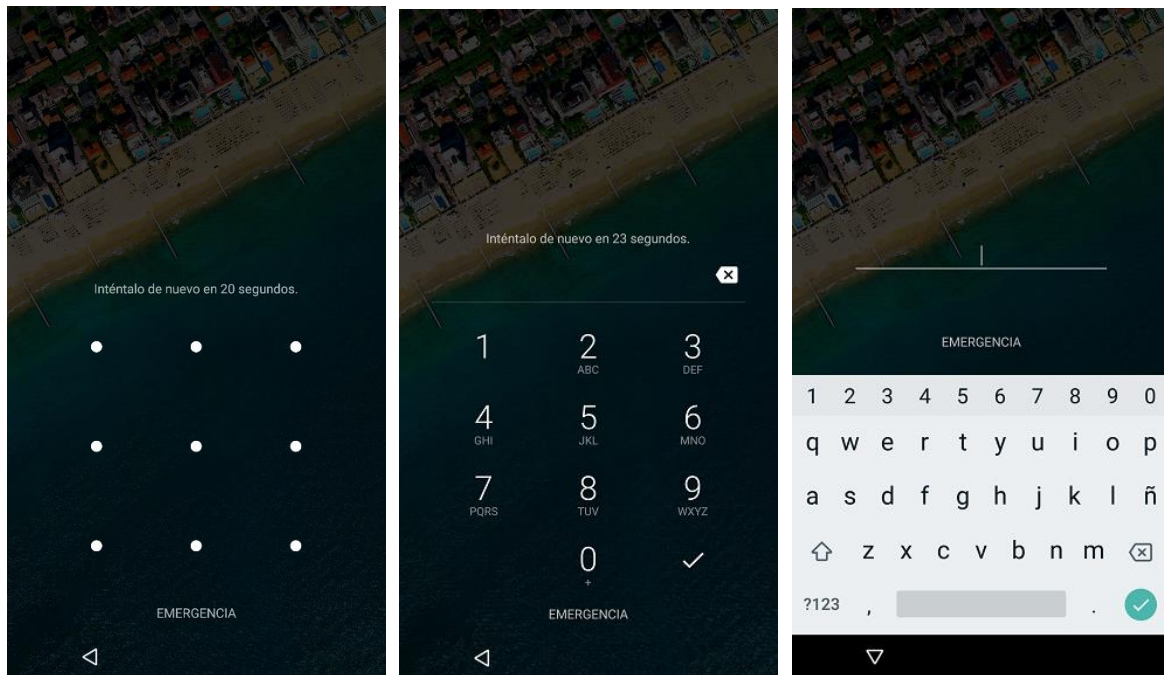
- Desbloqueo por voz: al decir “Ok Google”, el dispositivo se desbloqueará cuando reconozca el modelo de voz del usuario.
- Durante la conducción: para habilitar esta funcionalidad dentro de la app “Google Maps”.
- Modelo de voz de “Ok Google”: permite volver a configurar el modelo de voz del usuario o eliminar el existente.

660. En resumen, pese a la conveniencia que proporciona Smart Lock en la facilidad de uso del dispositivo móvil, esta funcionalidad no justifica los riesgos de seguridad asociados al acceso no autorizado al dispositivo por parte de un tercero en múltiples escenarios, por lo que se recomienda no activar Smart Lock y hacer únicamente uso de un código de acceso y, en todo caso, de autenticación mediante una huella dactilar digital, en caso de que la política de seguridad de la organización también contemple este método de acceso.
661. Adicionalmente, se han detectado vulnerabilidades en la propia funcionalidad de Smart Lock, por ejemplo, la descrita en el CVE-2016-6769 [Ref.- 207], que permitía a un potencial atacante con acceso físico al dispositivo móvil, acceder a la configuración de Smart Lock sin tener que introducir el código de acceso, concretamente en el caso en el que el usuario hubiera accedido al menú de Smart Lock como último ajuste de configuración.

9.6. PANTALLA DE DESBLOQUEO: PREVISUALIZACIÓN DE DATOS

662. En primer lugar, como se puede apreciar en las siguientes imágenes, la pantalla de desbloqueo de Android permite diferenciar visualmente entre las diferentes configuraciones de desbloqueo del dispositivo móvil: ninguno - no se muestra ningún símbolo; deslizar - se muestra únicamente un candado; Smart Lock - se muestra un candado dentro de un círculo que parpadea; Smart Lock con desbloqueo facial - se muestra un icono de cara que parpadea; huella dactilar - se muestra una huella digital que parpadea; patrón, PIN, o contraseña - se muestra un candado dentro de un círculo (además, en este caso, la pantalla de introducción del código de acceso también revelará cuál de los tres métodos está activo, pues se muestran los puntos de la matriz del patrón, un teclado numérico, o un teclado alfanumérico). Estos símbolos pueden facilitar a un potencial atacante una primera aproximación al nivel de seguridad existente en el dispositivo móvil:





663. La pantalla de desbloqueo del dispositivo móvil (*lock screen*) en Android permite, sin necesidad de introducir el código de acceso y, por tanto, sin necesidad de desbloquear el terminal, la previsualización del nombre del operador de telecomunicaciones a la izquierda de la barra superior de estado, que incluye además los iconos de conectividad (Wi-Fi y 2/3/4G y bluetooth), el nivel de batería y el usuario actual. En la zona central también se muestra, por defecto, la hora y la fecha, y el panel de notificaciones.

664. La pantalla de desbloqueo (a partir de Android 4.x) minimizó la posibilidad de desvelar información potencialmente confidencial y sensible a un potencial atacante. Por ejemplo, en el caso de recibirse un mensaje SMS, se indicaba mediante un aviso sonoro, una vibración y un icono de mensaje (por defecto), pero no se mostraba el contenido del mensaje ni en la pantalla de desbloqueo ni en la barra superior de estado.

665. Sin embargo, con el sistema de notificaciones (ver apartado “9.8. Notificaciones”), el usuario puede establecer que la pantalla de bloqueo muestre distintos grados de la información asociada a las aplicaciones (mostrar todo, ocultar todo, o mostrar sólo la información no sensible). Por ejemplo, con la opción “mostrar contenido de notificaciones”, en la pantalla de bloqueo un SMS recibido se mostraría completo, incluyendo el número de teléfono del remitente. Con la opción “ocultar notificaciones sensibles”, ante la recepción de un SMS sólo se mostraría el nombre de la app que gestiona los SMS y el texto “Contenidos ocultos”:



666. Es por ello muy importante revisar la política de notificaciones para evitar que la pantalla de bloqueo pueda proporcionar información sensible que el usuario desearía ocultar.

667. Adicionalmente, la información desvelada en la pantalla de bloqueo puede extenderse mediante la utilización de *widgets* (ver apartado “9.13. Pantalla de desbloqueo: Widgets”).

668. Asimismo, sigue siendo posible hacer fotografías y grabar vídeos sin desbloquear el dispositivo móvil (y sin conocer el código de acceso) deslizando hacia la izquierda el

icono correspondiente a la cámara de fotos, situado en la esquina inferior derecha de la pantalla de bloqueo.

669. Con la incorporación del servicio “Asistente de Google” y, en particular, de “Ok Google” (ver apartado “22.3. Asistente personal y “Ok Google””), la pantalla de bloqueo añade un micrófono en la parte inferior izquierda que permite invocar comandos de voz que serán enviados al asistente de Google. Dado que estos comandos pueden realizar operaciones sensibles, se recomienda aplicar las recomendaciones mostradas en el correspondiente apartado para evitar comprometer la seguridad y la privacidad del usuario.

9.7. INTERRUPCIONES

670. Una interrupción es un evento que una aplicación decide enviar para informar al usuario de un hecho o situación relevante desde el punto de vista de la aplicación. El carácter de la interrupción es definido por la propia aplicación.

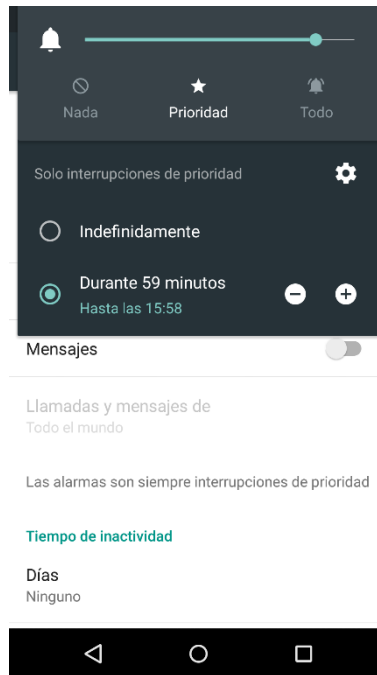
671. Una de las funciones que se incorporaron a partir de Android 5.x (Lollipop) son las interrupciones y notificaciones prioritarias, que permiten a los usuarios configurar el comportamiento del dispositivo móvil en función del calendario y de la importancia de la notificación para evitar interrupciones externas no deseadas.

672. En versiones previas de Android (4.x y anteriores), el modo “silencio” implicaba que el dispositivo móvil no emitía ningún sonido, ni vibraciones, pero sí admitía que las notificaciones visuales se mostrasen normalmente. Con la nueva funcionalidad añadida en Android 5.0, el modo silencio (“None” o “Ninguno”), no sólo silenciaba los sonidos y las vibraciones, sino que impedía por completo la llegada de alarmas y notificaciones, lo que limitaba mucho la usabilidad del dispositivo.

673. Android 5.1 resolvió el problema incluyendo dos modos de funcionamiento (además del modo “Todo”, que no impone ninguna restricción): “Prioridad” y “Nada”, así como su tiempo de duración. Para configurar el dispositivo en uno de estos modos manualmente, hay que pulsar el botón de volumen del dispositivo y se presentarán tres opciones:

- *Todo*: hasta nueva orden, o en el momento en que no cumplan las condiciones definidas, como por ejemplo el “Tiempo de inactividad”, se permitirán todas las alarmas y notificaciones.
- *Nada*: en este modo se suprimirán todas las interrupciones. Se permite seleccionar “Indefinidamente” (y sólo será posible salir del modo silencio manualmente) o “Durante X horas” (por defecto 1 hora, pero ampliable a las horas que especifique el usuario con los botones de + y -). Cuando se está en este modo, en la barra de estado (parte superior derecha de la pantalla) aparecerá un símbolo de prohibición.
- *Prioridad*: al igual que en el modo anterior, se puede especificar un tiempo indefinido o una duración en horas. Además, en la parte superior del menú, aparece el menú de ajustes de las interrupciones de prioridad, que equivale a entrar en el menú “Ajustes - [Dispositivo] Sonido y notificaciones - [Sonido] Interrupciones”. Cuando el dispositivo se encuentra en este modo, en la barra de estado (parte superior derecha de la pantalla) aparecerá una estrella. El propósito de este modo es filtrar las notificaciones menos importantes en los períodos de

tiempo definidos. Las alarmas siempre se consideran interrupciones prioritarias (o de prioridad).



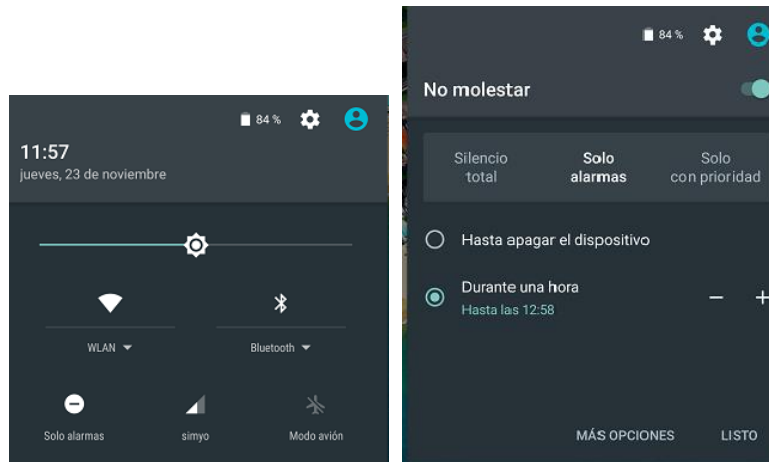
674. Android 5.1 introdujo el concepto de “interrupciones de prioridad”, que son aquellas que pueden disparar acciones en un dispositivo móvil que ha entrado en el modo “prioridad”; a nivel de aplicación, una interrupción de prioridad puede enviar notificaciones; a nivel de contacto, un contacto de prioridad podrá enviar mensajes o cursar llamadas. El resto de notificaciones y llamadas quedarán silenciadas.

675. Android 6.x complementó el modelo de prioridades que surgió con Android 5.1 introduciendo el concepto de modo “No molestar” e independizando las alarmas de las demás interrupciones consideradas “de prioridad”. Si Android 5.1 incluyó los modos “Prioridad” y “Nada” (además del modo “Todo”, que no impone ninguna restricción), Android 6.x introdujo los modos “Silencio total” (equivalente a “Nada” en Android 5.1), “Solo alarmas” (para que únicamente las alarmas interrumpen al usuario) y “Solo con prioridad” (equivalente al modo “Prioridad” de Android 5.1).

676. Para configurar el dispositivo móvil en modo “No molestar”, es necesario deslizar el dedo desde la parte superior de la pantalla hasta que aparezca el panel de ajustes de configuración rápidos. Seleccionando el icono “No molestar”, se activa esa opción y se presenta un menú que da a elegir entre los diferentes modos disponibles. Por defecto, la opción activa es “Solo alarmas”:

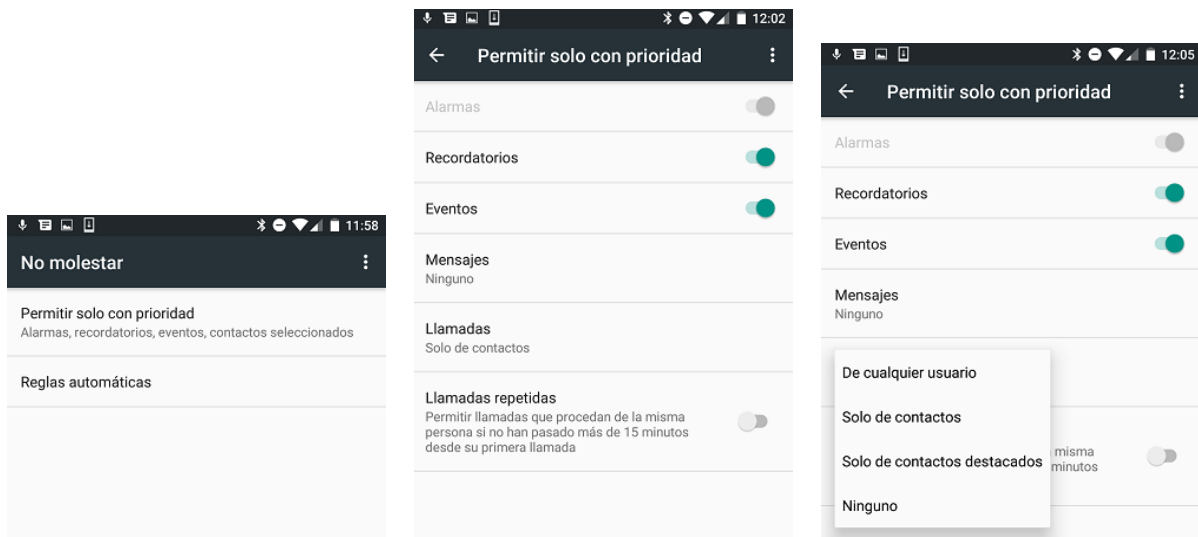
- “Silencio total”: en este modo se suprimirán todas las interrupciones, bloqueándose cualquier sonido o vibración del dispositivo móvil. Se permite seleccionar “Hasta apagar el dispositivo” (y sólo será posible salir del modo silencio manualmente) o “Durante X horas” (por defecto 1 hora, pero ampliable a las horas que especifique el usuario con los botones de + y -). Cuando se está en este modo, en la barra de estado (parte superior derecha de la pantalla) aparecerá un símbolo de prohibición.
- “Solo alarmas”: se dispone de las mismas opciones que en el modo “silencio total”, pero se permiten las notificaciones o interrupciones de las alarmas.

- “Solo con prioridad”: la primera vez que se selecciona este modo, el dispositivo mostrará un mensaje informativo y ofrecerá la opción “Personalizar”. En veces sucesivas, se mostrarán las mismas opciones que para el resto de los modos.

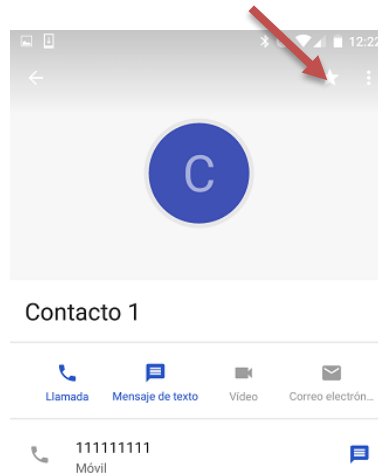


677. Si, en cualquiera de los modos se pulsa sobre “Más Opciones”, se abrirá el menú “Ajustes - [Dispositivo] Sonido y notificaciones - [Sonido] No molestar” (descrito posteriormente). Se solicitará el código de acceso al dispositivo si el mismo se encontraba en la pantalla de bloqueo.

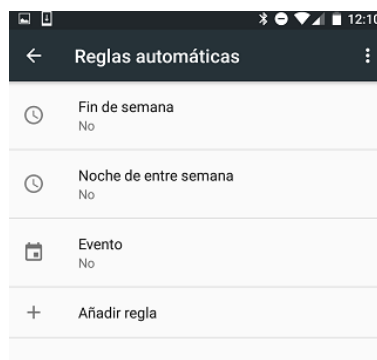
678. En Android 6.x las acciones para configurar las interrupciones han cambiado de formato respecto a Android 5.1. Es posible configurar las reglas de las interrupciones desde el menú “Ajustes - [Dispositivo] Sonido y notificaciones - [Sonido] No molestar”. Al seleccionar el menú aparecen las siguientes opciones:



- “Permitir solo con prioridad”: seleccionando este parámetro se desplegará un menú con las condiciones a cumplir por parte de una interrupción para que se la considere de prioridad (las alarmas, aunque se listan como opción, siempre son consideradas de prioridad y su botón de activación está sombreado):
 - Recordatorios.
 - Eventos.
 - Mensajes: ninguno, solo de contactos, solo de contactos destacados, de cualquier usuario. Para destacar un contacto, es necesario marcar el símbolo “estrella” en los detalles del contacto:



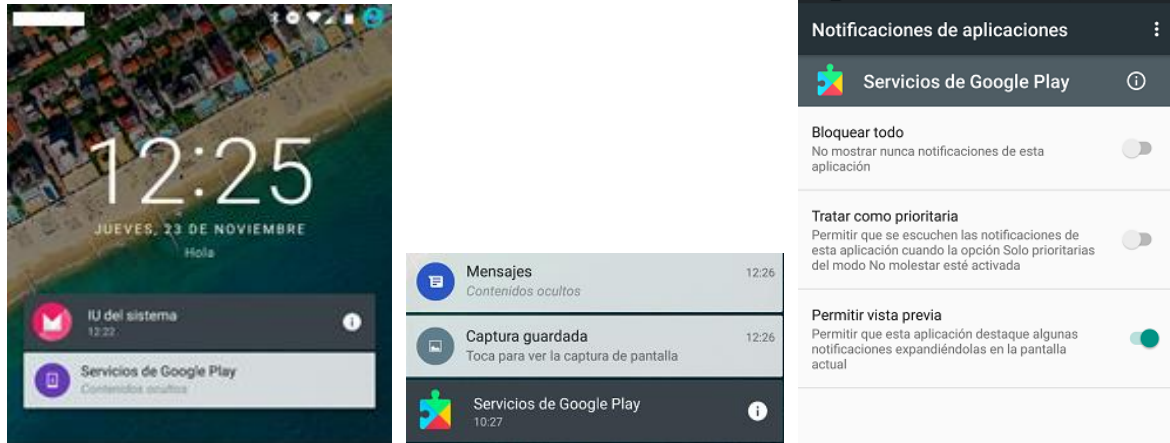
- Llamadas: las opciones son iguales que para “mensajes”.
- Llamadas repetidas: esta opción es nueva en la versión 6.x de Android, y permite que se cursen llamadas que se repiten en un margen inferior a 15 minutos, aunque no cumplan la condición establecida en el campo “Llamadas”.
- “Reglas automáticas”: permite definir reglas temporales por las que el dispositivo entrará en el modo de interrupción definido por la regla. Se presentan tres reglas por defecto (inactivas): “fin de semana”, “noche de entre semana” y “evento”. Además, se muestra la opción “Añadir regla”, que permite al usuario crear sus propias reglas de tipo “evento” o “de hora”. Las reglas de hora, incluidas las de “fin de semana” y “noche de entre semana”, presentan las siguientes opciones:
 - Nombre de la regla.
 - Días en los que la regla se activará.
 - Hora de inicio de la regla.
 - Hora de finalización de la regla.
 - No molestar: a elegir entre “solo prioritarias”, “solo alarmas” o “silencio total”.



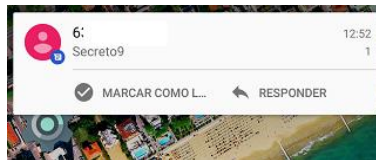
9.8. NOTIFICACIONES

679. Una notificación es un mensaje que una aplicación puede mostrar al usuario fuera del interfaz gráfico propio de la aplicación móvil, para informarle de un evento que se considera relevante desde el punto de vista de la aplicación.

680. Las notificaciones se envían al sistema para que las procese de acuerdo a la configuración definida por el usuario en relación a la política de interrupciones que se encuentre activa en el dispositivo móvil en el momento de recibirse la notificación, a la aplicación que envía la notificación, y a la prioridad de la propia notificación.
681. Android 5.0 (Lollipop) introdujo un cambio en el paradigma de las notificaciones [Ref.-508], entre ellas la capacidad para que una notificación aparezca en la pantalla de bloqueo del dispositivo o que aparezca como una pequeña ventana flotante (*heads-up notification*) cuando el dispositivo móvil está desbloqueado. Además, las notificaciones flotantes pueden mostrar botones de acción que permiten al usuario manejar la notificación sin salir de la aplicación que está activa, o simplemente descartar la notificación.
682. Las notificaciones flotantes surgen cuando la aplicación activa está en modo de pantalla completa y cuando la notificación tiene carácter prioritario y utiliza tonos o vibraciones.
683. Sin embargo, con Android 5.0 surgía el problema de que, cuando llegaba una notificación, no sólo se mostraba en primer plano independientemente de lo que el usuario estuviese haciendo, sino que, además, las únicas opciones para actuar ante ella eran: esperar a que desapareciera transcurridos 10 segundos, procesarla inmediatamente, o descartarla deslizando hacia los lados (derecha o izquierda) de la pantalla.
684. En Android 5.0, el comportamiento de las notificaciones es lo que se denomina “emergente”, es decir, la notificación se presenta en la pantalla activa interrumpiendo al usuario.
685. Con la llegada de Android 5.1, y todavía vigente en Android 6.x, las *heads-up notifications* se empezaron a mostrar, con el dispositivo móvil desbloqueado, en la barra de notificaciones en lugar de en mitad de la pantalla. Con el dispositivo bloqueado, se muestran en mitad de la pantalla. Al igual que en versiones previas, se permite descartar la notificación (deslizando hacia cualquiera de los lados), pero, adicionalmente, se puede minimizar deslizando el dedo desde la notificación hacia arriba, lo que la desplaza al panel o barra de notificaciones (situado en la parte superior) sin perder su contenido, hasta que el usuario decida procesarla.
686. Realizando una pulsación prolongada sobre una notificación, tanto con la pantalla bloqueada como desbloqueada, se mostrará qué componente o app ha generado la notificación. El icono de (i) (información), al pulsarse, abrirá el menú de configuración de las notificaciones de la aplicación concreta, permitiendo al usuario elegir cómo tratar las notificaciones de esa aplicación:



687. Con la pantalla desbloqueada, la app puede ofrecer adicionalmente acciones como respuesta a la notificación:



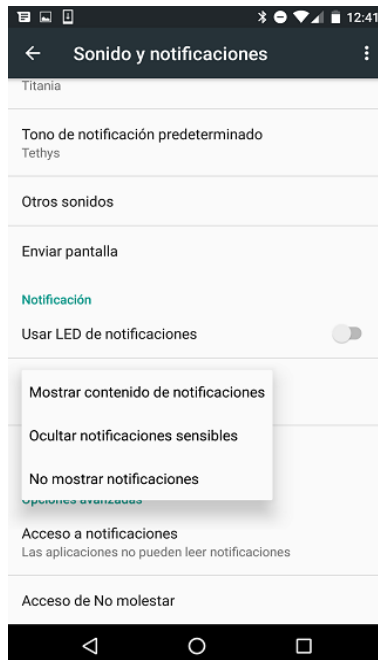
688. El servicio de notificaciones está afectado directamente por la configuración de las interrupciones (ver apartado “9.7. Interrupciones”).

689. La presentación de notificaciones se puede configurar a varios niveles:

- Tratamiento de la notificación: se ve afectado por el estado del dispositivo móvil (bloqueado frente a desbloqueado) y por el nivel de interrupción que esté activo (ver apartado “9.7. Interrupciones”).
- Sensibilidad de la notificación (se define a nivel de la aplicación móvil).
- Definición de la prioridad de la notificación de cada aplicación (carácter de la notificación).

690. El tratamiento de una notificación “Con dispositivo bloqueado” se configura a través del menú “Ajustes [Dispositivo] - Sonido y notificaciones - [Notificación] Con dispositivo bloqueado”. Por un lado, muestra el modo en que se gestionan las notificaciones según la configuración actual y, al pulsar sobre ella, permite definir cómo se gestionarán las notificaciones en la pantalla de desbloqueo, desplegando un menú cuyas opciones son:

- “Mostrar contenido de notificaciones”: visibilidad pública del contenido de la notificación.
- “Ocultar notificaciones sensibles”: sólo se mostrará parte de los contenidos; visibilidad privada.
- “No mostrar notificaciones”: si no se desea que se muestren, ni siquiera el icono o mensaje de la notificación; visibilidad secreta.



691. Con el dispositivo bloqueado, las notificaciones que cumplan la condición para ser visualizadas según el modo de interrupción activo actualmente se mostrarán en el área de notificaciones, que se muestra en primer plano en la pantalla de desbloqueo. Se mostrarán un total de cuatro notificaciones, y, en caso de haberse recibido más, el resto se englobarán en una sola entrada que va precedida con el símbolo “+número”, siendo “número” el número de notificaciones activas que no se están visualizando actualmente.



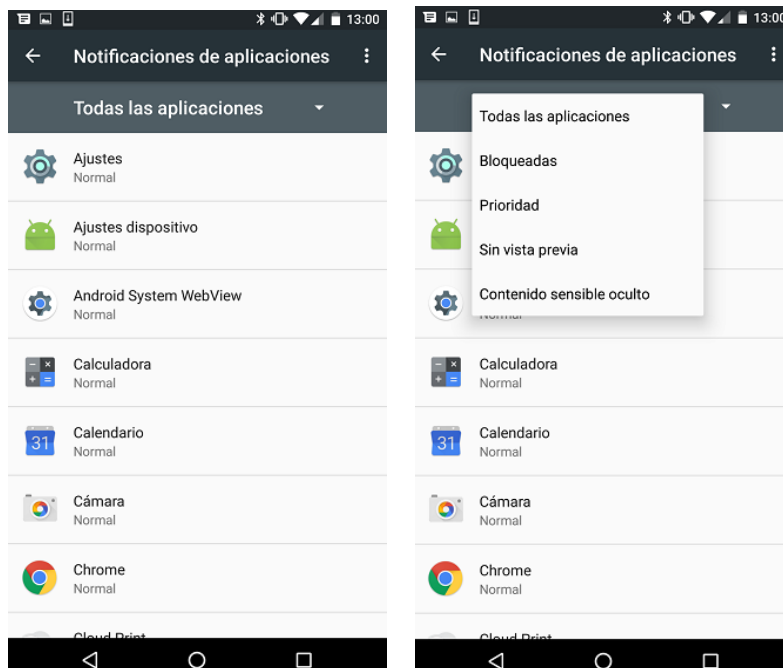
692. Con el dispositivo desbloqueado, las notificaciones se mostrarán en el panel de notificaciones (*notification drawer*) situado en el margen superior izquierdo del dispositivo móvil y, para ver el detalle de la notificación, el usuario ha de desplegar el panel deslizando el dedo desde la parte superior hacia abajo. Tanto el área de notificaciones (de la pantalla de desbloqueo), como el panel de notificaciones, son áreas controladas por el sistema que el usuario puede ver en todo momento, por lo que su contenido debe controlarse para evitar problemas de seguridad y privacidad (por

ejemplo, algunos servicios, como pasarelas de pago, envían al usuario un SMS con el código que han de introducir en la aplicación para validar el pago o completar la operación (segundo factor de autenticación). Un potencial atacante podría explotar una vulnerabilidad que permita el secuestro de la sesión del usuario en dicho servicio y, teniendo acceso visual a su dispositivo móvil, podría obtener y validar el código recibido y, por tanto, realizar la operación deseada.

693. Android 6.x (Marshmallow) refinó el tratamiento de las notificaciones en relación a su antecesor, Android 5.1 (Lollipop) permitiendo mayor control sobre las notificaciones tanto a nivel de cómo se muestran en pantalla al ser recibidas, como a nivel de su configuración por aplicación.

694. De manera global, el comportamiento del sistema ante una notificación de una aplicación se define en el menú “Ajustes [Dispositivo] - Sonido y notificaciones - [Notificación] Notificaciones de aplicaciones”.

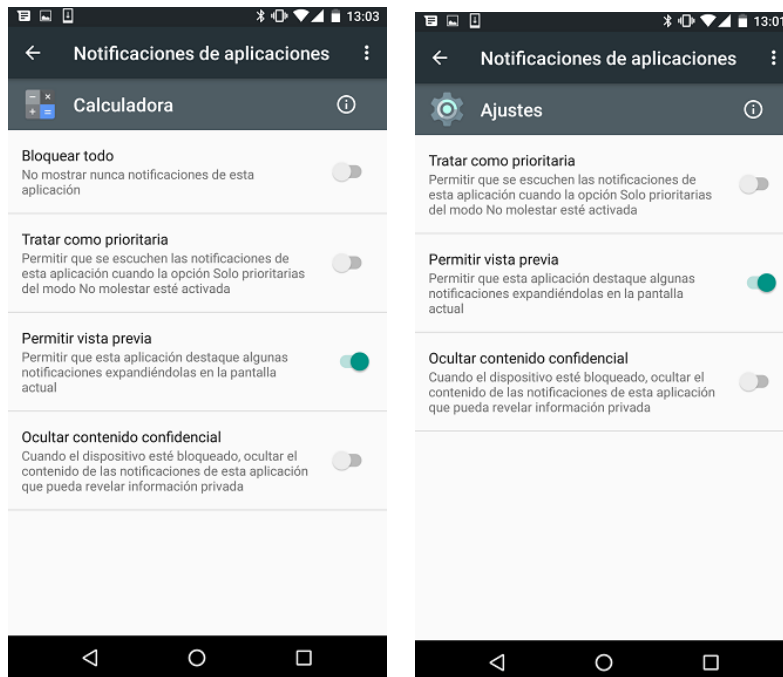
695. Al pulsar sobre “Notificaciones de aplicaciones”, se despliega un menú que ordena las aplicaciones alfabéticamente por nombre de aplicación. Por defecto, se muestran todas las aplicaciones, pero es posible filtrar en base al comportamiento definido por el usuario para cada una de ellas:



696. Para definir la acción que se tomará con respecto a las notificaciones de una aplicación concreta, se debe pulsar sobre el nombre de la aplicación, y aparecerá un menú con las siguientes opciones:

- Icono de información (i) junto al nombre de la aplicación: abre los ajustes de la aplicación de igual modo que el menú “Ajustes - [Dispositivo] Aplicaciones - <nombre de la aplicación>”. Uno de los ajustes del citado menú es “Notificaciones”, que, al ser seleccionado, mostrará las opciones de tratamiento de las notificaciones de esta aplicación por parte del sistema, enumeradas justo a continuación.
- Bloquear todo: no se mostrarán notificaciones de esta aplicación. Esta opción no está disponible para ciertas aplicaciones de sistema como, por ejemplo, la aplicación “Ajustes”.

- Tratar como prioritaria: cuando el dispositivo móvil esté configurado para aceptar sólo interrupciones prioritarias, únicamente las notificaciones que tengan este carácter se aceptarán cuando el modo “No molestar” lo permita (ver apartado “9.7. Interrupciones”).
- Permitir vista previa: la aplicación así catalogada está autorizada para destacar y expandir notificaciones en la pantalla del dispositivo móvil.
- Ocultar contenido confidencial: con el dispositivo móvil bloqueado, se ocultará el contenido que la aplicación marque como privado o sensible.



697. Es importante destacar que en Android 6.x la sensibilidad de las notificaciones (y, por tanto, su presentación en la pantalla de bloqueo) la define la app que genera la notificación a través del método “setVisibility()” del intent asociado a la notificación [Ref.- 628]. Los posibles valores son *public* (el contenido de la notificación se mostrará en su totalidad incluso en la pantalla de bloqueo), *secret* (el contenido se ocultará en la pantalla de bloqueo, aunque el desarrollador puede elegir reemplazar el contenido por otra información no sensible) y *private* (la notificación mostrará información básica, como un título o un icono, pero no su contenido completo).

698. Al hilo de lo anterior, Android 6.x no proporciona ninguna opción que permita al usuario alterar la sensibilidad de las notificaciones de una aplicación concreta. Por ejemplo, no se puede especificar que se desea que las notificaciones de la app que gestiona los SMS sean siempre tratadas como privadas. Únicamente se puede elegir si se oculta el contenido de las notificaciones que la app marque como privadas o secretas, o si se bloquearán por completo.

699. Android 4.4 (KitKat) introdujo un permiso denominado “Acceso a notificaciones”, que una app puede solicitar al usuario al lanzarse su ejecución. El usuario deberá otorgar el permiso de forma explícita, y ninguna app lo tiene concedido de forma automática. Es importante vigilar qué aplicaciones lo solicitan y a cuáles se les concede, ya que activarlo pone en riesgo la privacidad del usuario. Puesto que las aplicaciones con acceso a las notificaciones pueden acceder a todas las notificaciones sin distinción, podrían también acceder a notificaciones especialmente sensibles, como un mensaje confidencial o

crítico. Podría darse el caso de que una aplicación maliciosa capturase las notificaciones y las utilizase con propósitos maliciosos, dañinos o deshonestos, por ejemplo, capturar un SMS enviado por una app de banca on-line cuyo contenido incluya el código de autorización de una transacción.

700. Para identificar qué apps han obtenido el permiso de “Acceso a notificaciones”, se debe entrar en esa opción a través de “Ajustes - [Dispositivo] Sonido y notificaciones - [Opciones avanzadas]”.

701. Google recomienda a los desarrolladores de apps manejar las notificaciones de forma inteligente: por ejemplo, en lugar de reiterar una notificación para un mismo tipo de evento, se aconseja actualizar las notificaciones previas (*stacking notifications*). Un escenario típico de *stacking* sería, para aplicaciones de correo, si llega un nuevo mensaje, cambiar la notificación anterior para que incremente el número de mensajes pendientes sin leer, en lugar de mostrar una nueva notificación adicional indicando que ha llegado otro correo [Ref.- 507].

9.9. AHORRO DE BATERÍA

702. Las nuevas capacidades del proyecto Doze de Android 6.x permiten que las apps presenten diferentes comportamientos de consumo de batería o energía al estar el dispositivo móvil conectado a la corriente, usando únicamente la batería, o cuando el mismo no está siendo utilizado por el usuario, especialmente durante largos periodos de tiempo [Ref.- 616].

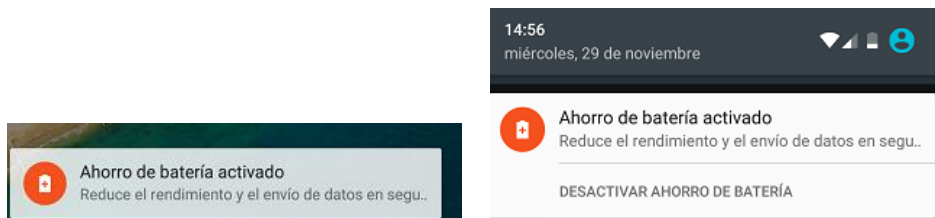
703. Si el usuario deja el dispositivo móvil sin alimentación de corriente, con la pantalla apagada, y sin moverlo (inmóvil), durante un periodo de tiempo determinado, éste entrará en un estado de ahorro de energía conocido como modo Doze.

704. En este estado el dispositivo permanece dormido o suspendido, y resume periódicamente su ejecución durante breves periodos de tiempo para que el sistema pueda completar operaciones pendientes y que las apps puedan sincronizar datos.

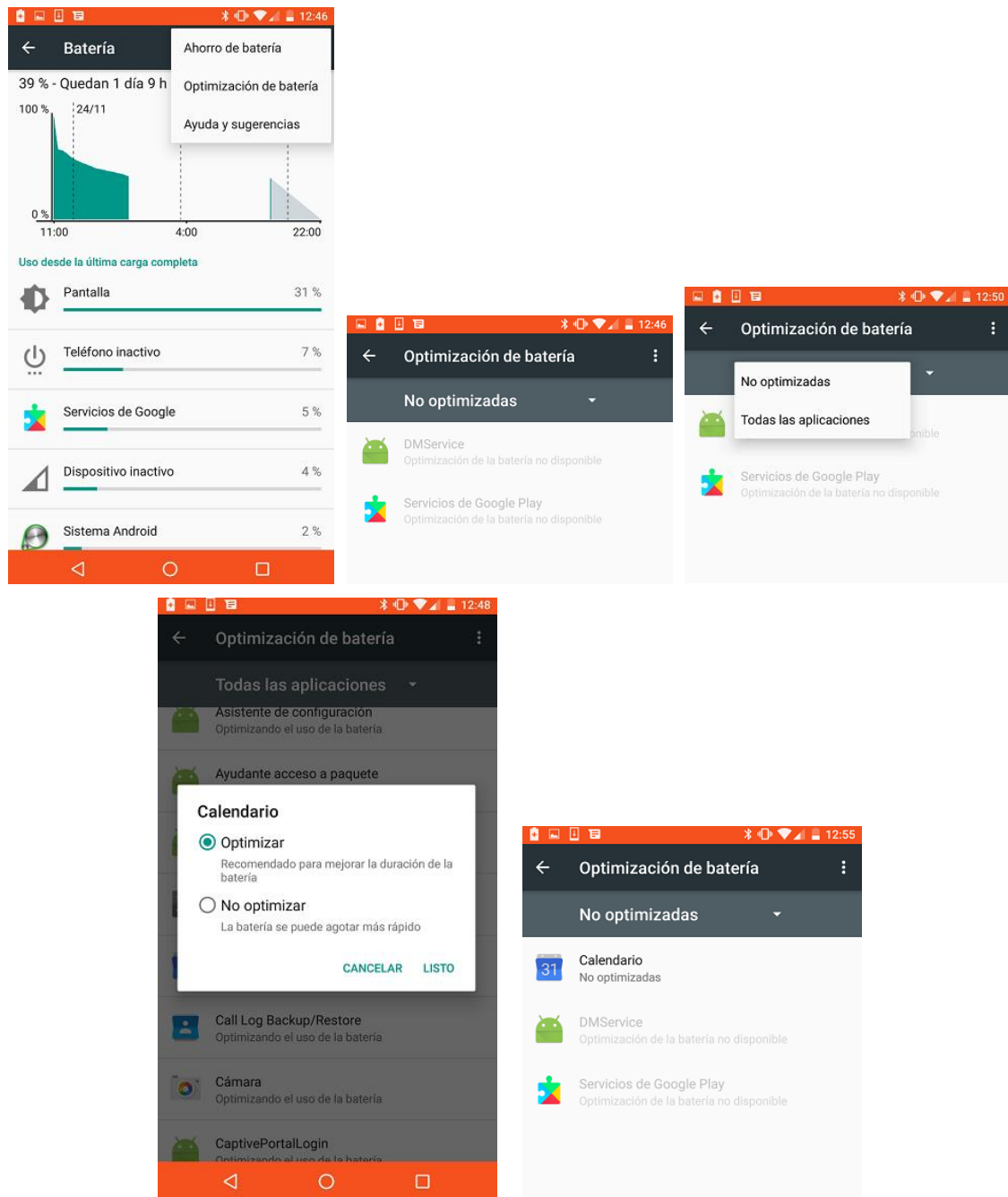
705. Se introducen por tanto dos modos de ahorro de energía:

- Modo descanso (*Doze*): cuando el dispositivo permanece inmóvil y con la pantalla apagada durante un periodo de tiempo determinado, el sistema operativo restringirá el acceso de las apps a la red (incluyendo los escaneos GPS y Wi-Fi) y a otros recursos del dispositivo móvil. También aplaza las tareas, sincronizaciones y alarmas estándares de las apps.
- Modo suspendido (*App Standby*): en este modo, la actividad de red para las apps que no han sido utilizadas recientemente por el usuario se postpone. Se considera que una aplicación no se ha utilizado recientemente cuando el usuario no ha pulsado sobre la pantalla de la app y no se cumple ninguna de las siguientes condiciones:
 - la app no tiene ningún proceso en primer plano en el momento actual (por ejemplo, una app que permite escuchar música de fondo aunque el reproductor no esté en primer plano).
 - la app ha lanzado una notificación que está activa.
 - el dispositivo móvil está conectado a la corriente.

706. Asimismo, y de manera más granular, el sistema puede determinar que una app concreta está ociosa cuando el usuario no la está utilizando activamente. Si el dispositivo móvil no tiene alimentación de corriente, el sistema suspende el acceso a la red, las sincronizaciones y la ejecución de tareas para dicha app.
707. Una aplicación de tipo administrador de dispositivos nunca entra en modo suspendido.
708. Para activar el modo de ahorro de batería, el usuario debe mover el botón “Ajustes - [Batería] ... - Ahorro de batería - No” a la posición “Sí”.
709. Adicionalmente, puede seleccionarse la activación de este modo de ahorro de batería de manera automática cuando se alcance un porcentaje de un 5% o un 15% de carga de la batería si no se dispone de conexión a la corriente.
710. Si se activa este modo de ahorro por parte del usuario, se mostrará una notificación que permanecerá activa en la barra de notificaciones con un símbolo de batería y el signo “+”. Esta notificación no se puede descartar, pero sí admite como respuesta la opción “Desactivar ahorro de batería” y, al pulsarla, se accede al menú de ahorro de batería.



711. El dispositivo, con la pantalla activa, presentará unas bandas rojas en la barra de notificaciones y en los botones táctiles de la pantalla.
712. Se establece una lista de exclusión (o *whitelist*) que permite al usuario definir qué apps pueden saltarse parcialmente las políticas de los modos Doze y App Standby. Para ello, el usuario puede acceder a “Ajustes - [Batería] ... - Optimización de batería”. Por defecto, se mostrará la pantalla de “No optimizadas”, que engloba las apps que están en la *whitelist*.
713. Si se desea añadir una app a esta lista, se desplegará el menú “No optimizadas” y se elegirá la opción “Todas las aplicaciones”. Con ello se mostrarán todas las apps instaladas. Una vez seleccionada la app a incluir en la lista de exclusión, se marcará “No optimizar”.

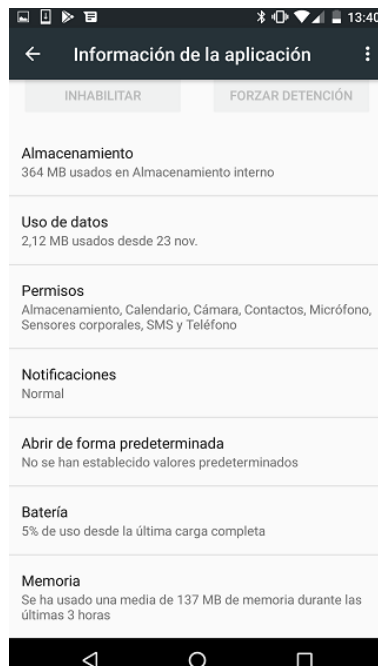


714. Una app no puede saltarse el mecanismo de ahorro de batería si éste está activo. No obstante, Android establece una serie de usos aceptables ante los cuales la app podrá:

- Lanzar un `ACTION_IGNORE_BATTERY_OPTIMIZATIONS_SETTINGS`: este intent abrirá para el usuario el menú de optimización de batería descrito previamente, posibilitando que se pueda añadir dicha app.
- Solicitar el permiso `REQUEST_IGNORE_BATTERY_OPTIMIZATIONS` para permitir al usuario añadir la app a la lista de exclusión directamente, sin pasar por el intent anterior.

715. Ninguno de los dos elementos anteriores provocará que la app sea añadida por el sistema a la lista de exclusión sin intervención del usuario. Además, los usos aceptables de ambos mecanismos están descritos oficialmente en la sección “Acceptable Use Cases for Whitelisting” del documento “Optimizing for Doze and App Standby” [Ref.- 616].

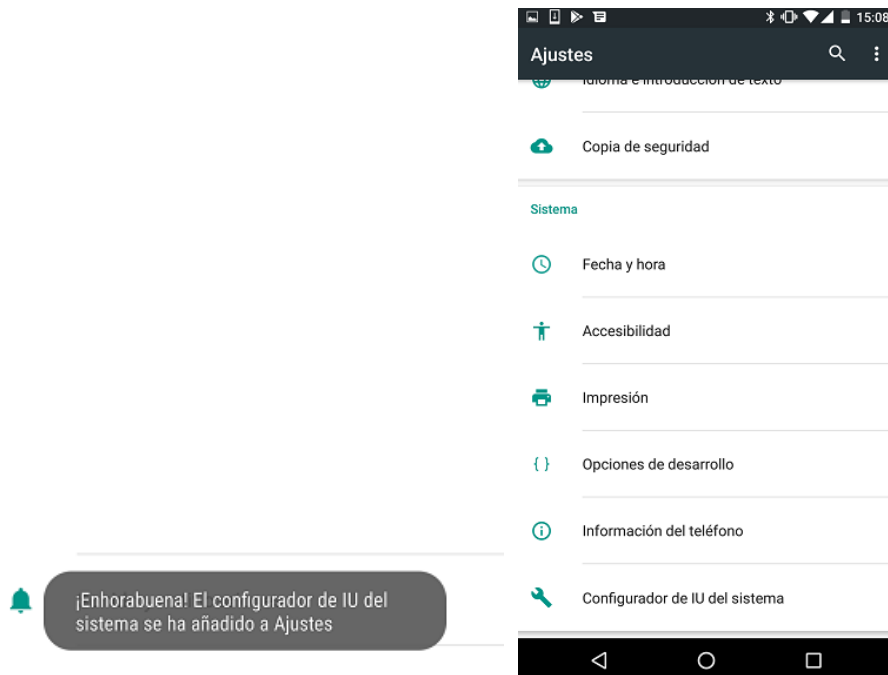
716. Es posible saber cuál es el consumo de batería de una aplicación a través del campo “Batería” de la sección “Ajustes - [Dispositivo] Aplicaciones - [Nombre de la app] Información de la aplicación”. Esta información es muy útil de cara a identificar problemas de consumo irregular de batería.



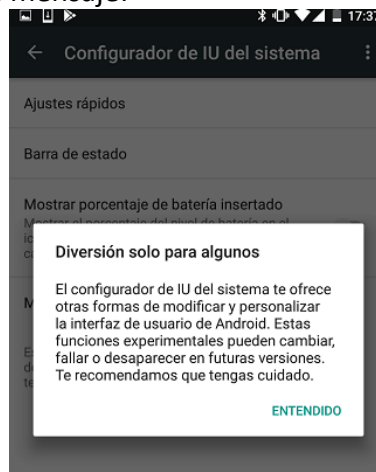
717. Desde el punto de vista de la seguridad del dispositivo móvil, se recomienda mantener un nivel de batería aceptable que no impida, en caso de pérdida, localizar el dispositivo, bien a través de los servicios de localización remota (ver apartado “8.1. Gestión remota de dispositivos Android por parte del usuario”), bien por medios más básicos como llamar al número de teléfono. En este sentido, el uso de las capacidades de ahorro de batería resulta beneficioso para el usuario y para el hardware del dispositivo móvil.

9.10. CONFIGURADOR DE IU DEL SISTEMA

718. El “Configurador de IU del sistema” es una característica introducida en Android 6.x (Marshmallow) que da acceso a funcionalidades “ocultas” que permiten personalizar ciertos elementos del interfaz de usuario de Android, en particular, la barra de estado y el menú de ajustes rápidos (disponible en la parte superior del interfaz gráfico).
719. Hay que reseñar que algunas de estas funcionalidades no están soportadas oficialmente por Google y pueden variar entre versiones. En caso de detectarse un empeoramiento en el rendimiento o en la estabilidad del sistema, se debe proceder a deshabilitarlas.
720. Para activar el configurador de IU (Interfaz de Usuario), hay que habilitar el modo “desarrollador” en el dispositivo móvil (consultar apartado “13.3. Opciones de desarrollo y depuración USB” para más información sobre este modo). Una vez habilitado, es necesario desplegar la barra de ajustes de configuración rápidos y realizar una pulsación prolongada de más de tres segundos en el icono del engranaje correspondiente a los ajustes (hasta que se vea que empieza a girar). Se mostrará el mensaje que ilustra la siguiente imagen y se añadirá un símbolo de llave inglesa al símbolo de ajustes. Además, aparecerá la opción “Configurador de IU del sistema” bajo el menú “Ajustes - Sistema”.

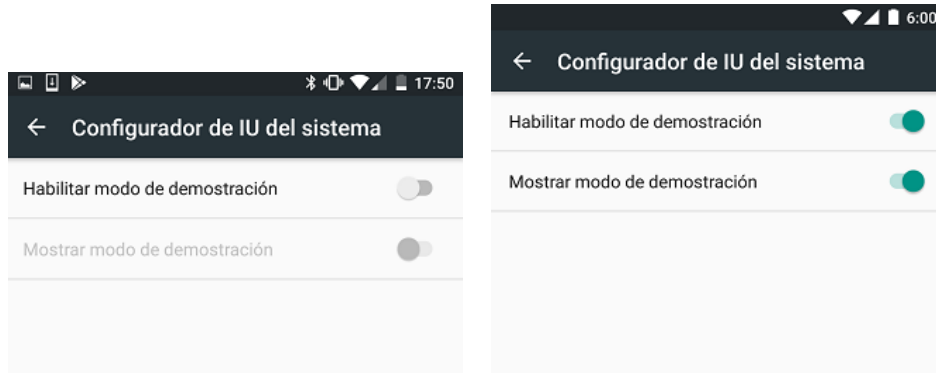


721. Una vez activo, el menú “Configurador de IU del sistema” permite personalizar el interfaz de usuario (IU). Pese a ello, no se recomienda hacer uso de su funcionalidad a menos que se esté seguro de lo que se persigue con ello, de lo cual se advierte al usuario a través del siguiente mensaje:

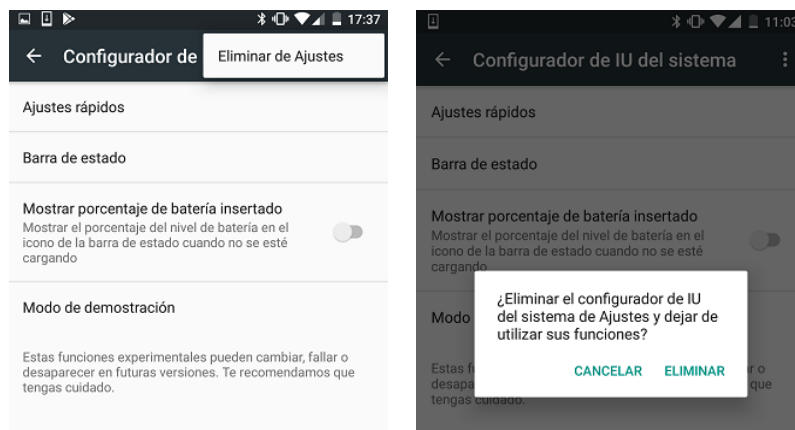


722. La opción “Ajustes rápidos” (ver apartado “9.12. Menú de ajustes rápidos y barra de notificaciones”) permite añadir o eliminar los mosaicos que se presentarán al expandir el menú de ajustes rápidos deslizando los dedos desde la parte superior del dispositivo móvil hacia abajo. Es muy importante tener claro qué opciones se desean añadir a este menú, porque algunos de los ajustes podrán ser accedidos desde la pantalla de bloqueo sin necesidad de autenticación por parte del usuario.
723. La opción “Barra de estado” permite configurar los iconos correspondientes a las opciones que se sitúan en la esquina superior derecha de la pantalla.
724. La opción “Mostrar porcentaje de batería insertado” hará que en el icono de batería de la barra de estado aparezca un número representativo del porcentaje de carga actual, aún con el dispositivo móvil sin conectar a una fuente de carga.
725. La opción “Modo de demostración” reemplaza temporalmente la barra de estado por una totalmente limpia de notificaciones, mostrando únicamente los iconos de Wi-Fi, cobertura y batería al 100%, junto a las 6:00 como la hora actual, en clara referencia a

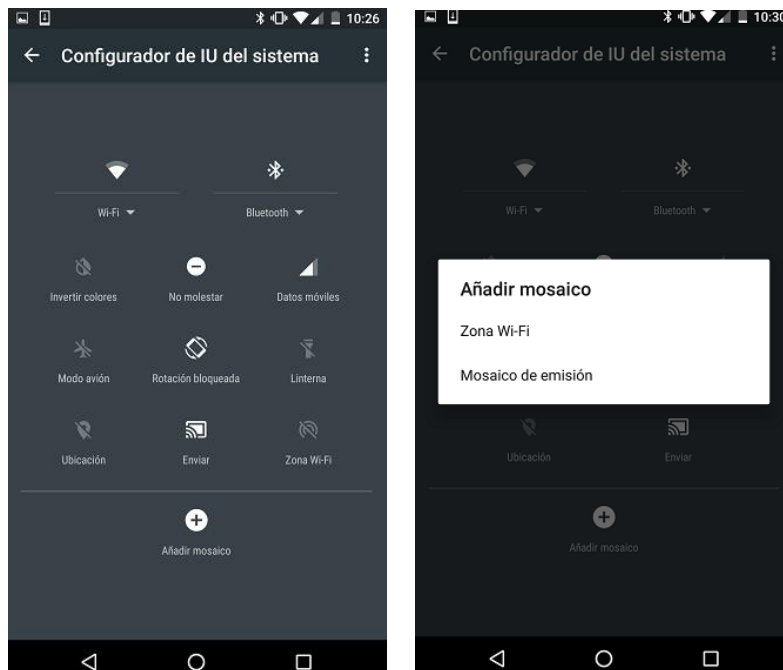
Android 6.0 (Marshmallow). Para pasar a este modo, es preciso seleccionar “Habilitar modo de demostración”. Para mostrarlo temporalmente en un momento concreto en pantalla, hay que marcar “Mostrar modo de demostración”.



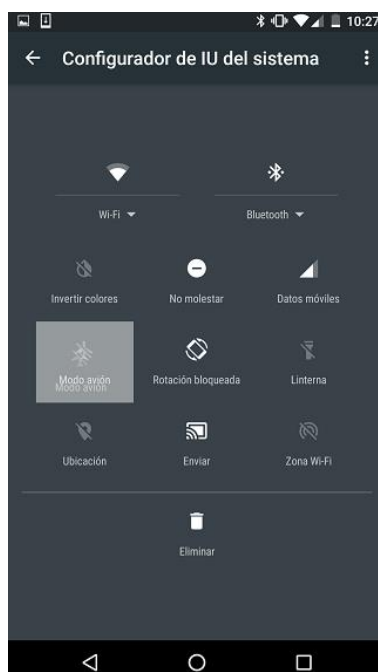
726. Para deshabilitar el configurador de IU de sistema, se puede ir a “Ajustes - Sistema - Configurador de IU del sistema”, seleccionar los 3 puntitos de la derecha y “Eliminar de ajustes”. También existe la opción de pulsar varios segundos en el icono del engranaje de la barra superior de estado correspondiente a los ajustes rápidos, hasta que aparezca el mensaje que solicita confirmación para eliminarlo del menú de ajustes:



727. Para añadir un elemento al menú de ajustes rápidos, se debe seleccionar “Ajustes - Sistema - Configurador de IU del sistema - Ajustes rápidos”. Esta acción desplegará un menú en el que se presentan los elementos disponibles en el menú de ajustes rápidos en el momento actual, y, en la parte inferior, el botón “Añadir mosaico”. Una pulsación sobre dicho botón desplegará los elementos que no forman parte actualmente del menú de ajustes rápidos pero que están disponibles para ser añadidos a él:

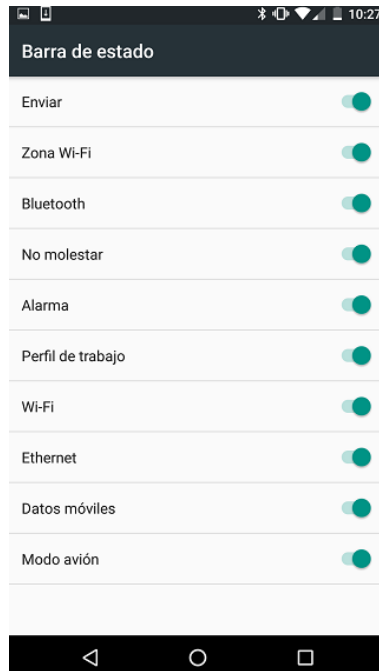


728. Para eliminar un elemento de esta barra de ajustes rápidos, se debe seleccionar el elemento y arrastrarlo hasta el icono “Eliminar” que aparecerá en el margen inferior de la pantalla.



729. Adicionalmente, se permite reordenar los iconos sin más que seleccionarlos y arrastrarlos manteniendo la pulsación sobre ellos hasta la posición a la que se quiera desplazarlos.

730. Para añadir elementos a la barra superior de estado, se debe acceder a “Ajustes - Sistema - Configurador de IU del sistema - Barra de estado” y desplazar los diferentes interruptores a la posición activado/desactivado según lo que se desee mostrar.

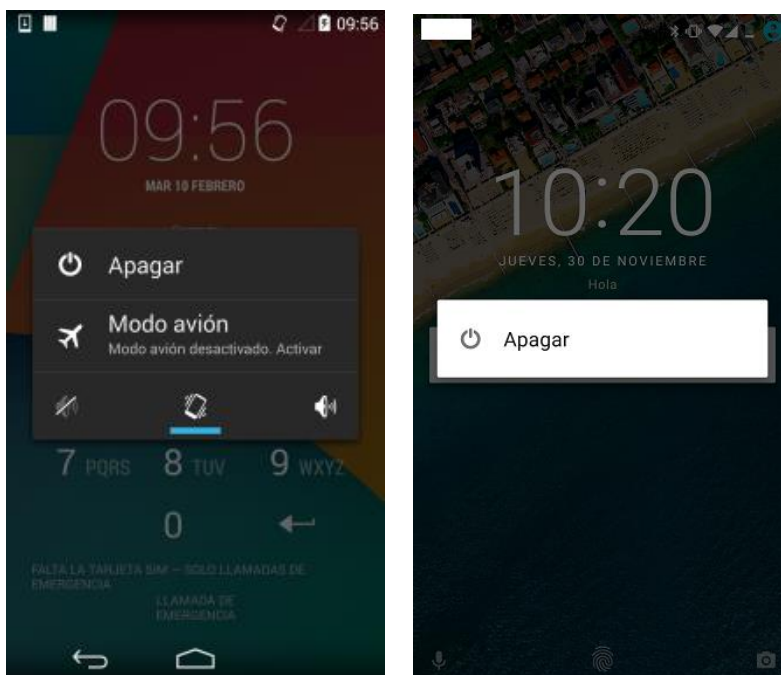


731. Desde el punto de vista de seguridad, el configurador de IU de sistema permite realizar configuraciones interesantes de cara a la seguridad del dispositivo. Por ejemplo, se recomienda eliminar del menú de ajustes rápidos los elementos “Wi-Fi”, “Modo avión”, “Datos móviles” y “Bluetooth”, porque tienen la potestad de activar/desactivar funcionalidades sin requerir la introducción del código de acceso en el dispositivo móvil. Así, por ejemplo, un tercero con acceso físico al dispositivo podría desactivar los datos móviles y/o la conexión Wi-Fi, impidiendo al propietario hacer uso de las capacidades remotas de gestión del mismo (ver apartado “8.1. Gestión remota de dispositivos Android por parte del usuario”), concretamente, en escenarios donde se ha perdido el dispositivo móvil o éste ha sido robado.
732. De igual forma, un tercero malintencionado podría desactivar el componente “Bluetooth” impidiendo que el dispositivo pudiera ser localizado a través de, por ejemplo, un Smart Watch actualmente emparejado con él.
733. No obstante, y dado que se trata de un componente con elementos experimentales, se recomienda hacer uso de la funcionalidad del configurador de IU de sistema sólo en caso de tener buen conocimiento de lo que se pretende conseguir con él.
734. Aunque sería deseable poder activarlo para realizar las personalizaciones necesarias y desactivarlo después para evitar los potenciales riesgos de estabilidad que puede entrañar usarlo, resulta que su desactivación conlleva la pérdida de cualquier personalización realizada previamente.

9.11. PANTALLA DE DESBLOQUEO: APAGAR EL DISPOSITIVO MÓVIL

735. Desde la pantalla de desbloqueo de Android, y sin conocer el código de acceso pero disponiendo de acceso físico temporal al dispositivo móvil, es posible mantener pulsado el botón de encendido y apagado, para proceder a apagar el terminal.

736. Android 4.x ofrecía a través del botón de encendido, además de la opción “Apagar”, un menú que permitía gestionar el sonido, indicando si el dispositivo móvil está en silencio, en modo vibración, o con el volumen activo. También incluía la opción de “Modo avión”. Todos estos controles desaparecieron de este menú en Android 5.x, quedando únicamente la opción “Apagar” también para Android 6.x.



Menú de apagado en Android 4.x - Menú de apagado en Android 6.x

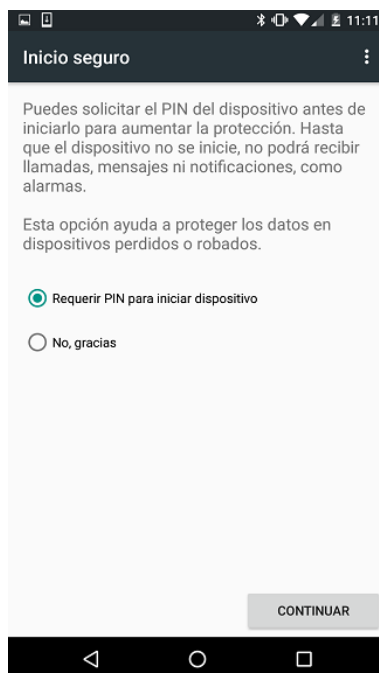
En Android 4.x, el botón de apagar ofrecía adicionalmente activar el modo avión (o modo vuelo, botón “Modo avión”), lo que suponía un riesgo desde el punto de vista de seguridad ya que, si una persona no autorizada obtiene acceso físico al dispositivo móvil y activa el modo avión, no será posible disponer de conectividad de datos desde el dispositivo móvil para poder hacer uso de las capacidades remotas de gestión del mismo (ver apartado “8.1. Gestión remota de dispositivos Android por parte del usuario”), por ejemplo, en escenarios donde se ha perdido el dispositivo móvil, o éste ha sido robado⁴⁸.

Android 5.x no resuelve este problema, porque, si bien la opción para activar/desactivar el modo avión desaparece del botón de encendido, se incorpora irreversiblemente al menú de ajustes de configuración rápidos, que son accesibles como interruptores sin necesidad de autenticación.

737. Android 6.x (Marshmallow) resuelve el problema del modo avión permitiendo suprimir del menú de ajustes rápidos el icono “Modo avión”. Mediante el menú “Ajustes - Sistema - Configurador de IU del sistema - Ajustes rápidos”, una vez localizado el icono del modo avión, es posible pulsar sobre él y arrastrarlo hasta el icono inferior “Eliminar” (ver apartado “9.10. Configurador de IU del sistema”).

⁴⁸ En este escenario el dispositivo móvil está encendido, y por ejemplo, su memoria ya ha sido descifrada.

738. En Android 5.x no existía ninguna opción para forzar a que se solicite el código de acceso al iniciar el dispositivo, salvo si éste está cifrado, pero sí presenta el botón “Ajustes - [Personal] Seguridad - [Seguridad de la pantalla] - Bloquear al encender”, que hará que el dispositivo móvil entre en la pantalla de bloqueo al reiniciarse. Esta opción no impide que se puedan recibir llamadas, mensajes, o notificaciones, lo que podría permitir a un potencial atacante acceder a información desde la pantalla de desbloqueo que podría ser sensible.
739. Android 6.x introdujo una opción denominada “Inicio seguro” bajo el menú “Ajustes - [Personal] Seguridad - [Seguridad del dispositivo] Bloqueo de pantalla - [Tipo de bloqueo] - Inicio seguro”. Si se activa esta opción, se forzará al usuario a introducir el código de acceso (PIN, patrón o contraseña) definido como mecanismo de bloqueo antes de iniciar el dispositivo móvil, de modo que, si no se introduce, no será posible recibir llamadas, mensajes o notificaciones, protegiendo así la información sensible del usuario. Se recomienda activar esta opción para evitar la exposición de la información sensible en caso de pérdida o robo del dispositivo. Esta opción es independiente del estado de cifrado del dispositivo, por lo que se puede utilizar tanto con él cifrado como sin cifrar.



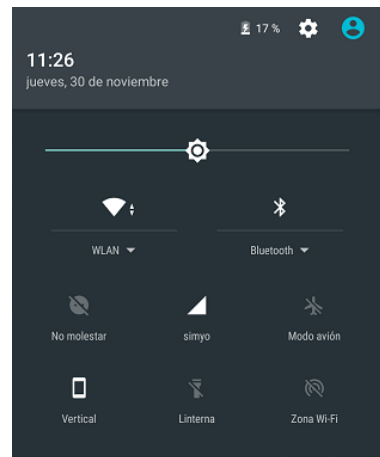
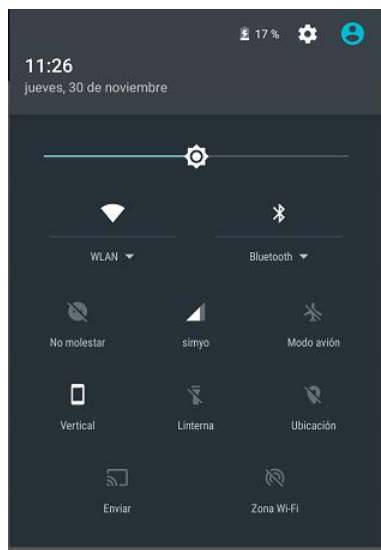
9.12. MENÚ DE AJUSTES RÁPIDOS Y BARRA DE NOTIFICACIONES

740. El menú de ajustes de configuración rápidos, o ajustes rápidos por abreviar, es un menú que permite realizar determinadas configuraciones desde la pantalla actual sin tener que pasar por el menú de “Ajustes” tradicional, seguido del conjunto de menús necesario para llegar hasta la opción de configuración deseada, de forma similar a un acceso directo.
741. Si el dispositivo móvil tiene la pantalla bloqueada, este menú se mostrará al deslizar uno o dos dedos desde la parte superior de la pantalla hacia abajo.
742. Si el dispositivo móvil tiene la pantalla desbloqueada, al deslizar con un dedo se mostrarán las notificaciones activas, siendo necesario deslizar con dos dedos desde la parte superior de la pantalla hacia abajo para acceder directamente al menú de ajustes

rápidos completo. También se puede desplegar el menú deslizando con un dedo en dos ocasiones (o en dos veces), accediendo en primer lugar a las notificaciones y posteriormente al menú de ajustes rápidos.

743. En Android 6.x, el menú de ajustes rápidos mostrará diferentes opciones según si se invoca desde la pantalla de bloqueo o desde la pantalla con el dispositivo móvil desbloqueado. Con la pantalla bloqueada, no se mostrarán el botón “Ubicación”, ni tampoco “Enviar” (opción que permite compartir la pantalla actual con otro dispositivo a través de Wi-Fi Direct).

744. Los ajustes se muestran en color blanco si están activados y atenuados (o en color gris) si están desactivados. Las siguientes imágenes muestran el menú de ajustes rápidos con la pantalla desbloqueada y el menú de ajustes rápidos con la pantalla bloqueada, respectivamente.



745. Los ajustes rápidos existentes en el menú de Android 6.x son los siguientes:

- Fecha y hora.
- Wi-Fi, red móvil y Bluetooth: además del nombre de la conexión o red empleada, se representa el estado de la transmisión de datos:
 - Una flecha hacia arriba indica que el dispositivo está transmitiendo datos hacia Internet.
 - Una flecha hacia abajo muestra que se están transmitiendo datos desde Internet hacia el dispositivo.
 - Un signo de exclamación indica que hay un problema con la conexión.
- Batería: permite consultar el estado actual de carga de la batería.
- No molestar: activa un modo en el que ninguna aplicación emitirá sonidos o vibraciones.
- Linterna: encenderá el flash de la cámara del dispositivo móvil para ser usado como linterna.
- Girar automáticamente: permite habilitar la autorrotación de la pantalla del dispositivo según su orientación (si se fija a un valor *horizontal* o *vertical*, se mostrará dicho valor).

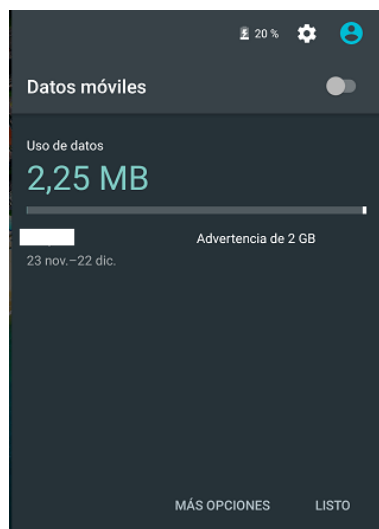
- Modo avión: habilita/deshabilita todas las conexiones inalámbricas del dispositivo.
- Ubicación: permite activar los servicios de localización geográfica (sólo se mostrará si el dispositivo está desbloqueado).
- Enviar: permite compartir la pantalla actual con otro dispositivo a través de Wi-Fi Direct (por ejemplo, con un dispositivo ChromeCast). Sólo se mostrará con la pantalla desbloqueada.
- Invertir colores: permite invertir los tonos negros y blancos de la pantalla. Para que aparezca, requiere que la opción “Ajustes - [Sistema] Accesibilidad - [Pantalla] Invertir colores” haya sido habilitada previamente.
- Zona Wi-Fi: sólo se mostrará si se ha configurado una zona Wi-Fi para compartir la conexión del dispositivo móvil con otros dispositivos a través del menú “Ajustes [Conexiones Inalámbricas y Redes] - Más... - Anclaje a red y zona Wi-Fi”.

746. Hasta Android 6.x no era posible personalizar qué ajustes se incluían como parte del menú de ajustes rápidos, y tampoco se permitía deshabilitarlos de forma que no aparecieran en la pantalla de bloqueo, por lo que no había forma de evitar que un potencial atacante pudiera acceder a ellos, un comportamiento muy relevante desde el punto de vista de seguridad.

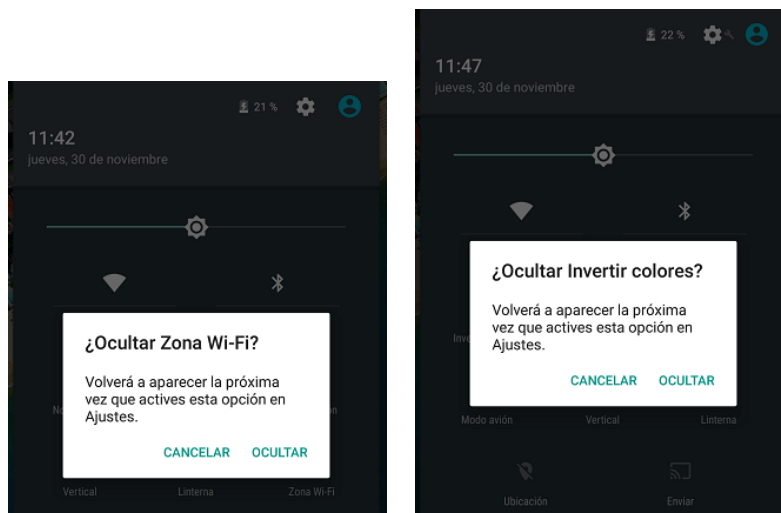
747. Android 6.x introdujo como una de sus novedades el menú “Configurador de IU del sistema” (ver apartado “9.10. Configurador de IU del sistema”), el cual permite realizar personalizaciones sobre la barra de estado y el menú de ajustes rápidos. No obstante, no se puede controlar, ni tan siquiera a través de este menú, qué elementos estarán disponibles únicamente en el menú de ajustes rápidos con la pantalla bloqueada.

748. Con la pantalla bloqueada, además de los ajustes ya existentes en Android 4.x (Wi-Fi, Bluetooth, y girar automáticamente), en Android 5.x se añadió una opción de “Linterna” que persiste en Android 6.x y que permite utilizar el flash de la cámara del dispositivo móvil como si fuera una linterna.

749. Adicionalmente, se muestra también un icono con el nombre del proveedor de servicios de la red de datos móviles que permite consultar el consumo actual de datos para el período mostrado y si hay alguna advertencia sobre el consumo, previamente configurada en el menú “Ajustes - [Conexiones inalámbricas y redes] Uso de datos”.

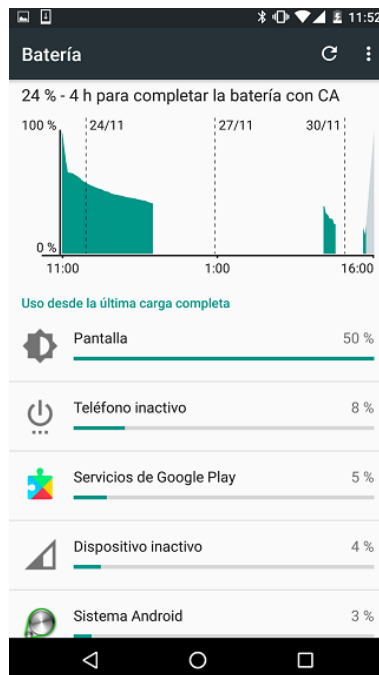


750. Con la pantalla desbloqueada, desde Android 5.x en adelante, se incorpora además la opción “Ubicación” (para activar o desactivar el servicio de ubicación, de forma equivalente al menú “Ajustes - [Personal] Ubicación”) y la opción “Enviar” para compartir la pantalla (opción que permite compartir la pantalla actual con otro dispositivo a través de Wi-Fi Direct, tal como se ha descrito previamente).
751. Android 6.x, a través del icono de ajustes rápidos del interfaz Wi-Fi, permite, además de activar o desactivar el interfaz Wi-Fi del dispositivo móvil, elegir mediante una sola pulsación la red Wi-Fi a la que conectarse. Si bien el modo de activación funciona con la pantalla bloqueada, la opción de cambiar de red Wi-Fi solicitará autenticación al usuario, a menos que las credenciales de conexión a la red Wi-Fi que se seleccione hayan sido guardadas previamente. Este mismo comportamiento se exhibe con el ajuste rápido del interfaz Bluetooth.
752. La novedad que introdujo Android 5.1 para eliminar fácilmente de la barra de ajustes rápidos las opciones dinámicas “Zona Wi-Fi” e “Invertir colores”⁴⁹ (que solo se mostraban al activar esas opciones de configuración concretas), se mantiene en Android 6.x, siendo posible eliminar manualmente esas opciones sin más que realizar una pulsación prolongada sobre los iconos correspondientes y seleccionar “Ocultar” en el menú emergente.

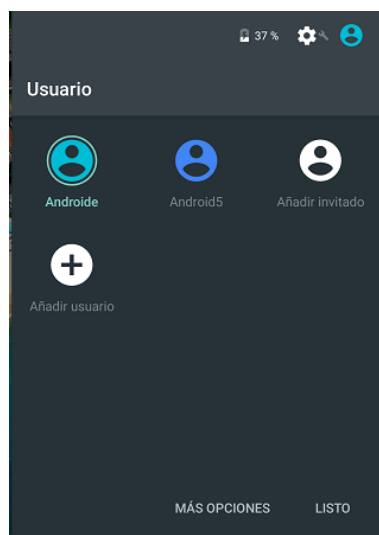


753. Adicionalmente, en la parte superior del menú de ajustes rápidos (en el área que ocupa la barra de estado) se incluye el acceso directo al menú “Ajustes - Batería” y un acceso al menú principal de “Ajustes” que, al seleccionarlo, abre dicho menú (en caso de que el dispositivo móvil esté bloqueado, se solicitará el código de acceso para abrir el menú completo).

⁴⁹ La opción “Invertir colores” se activa desde “Ajustes - [Sistema] Accesibilidad - [Pantalla] Invertir colores”.



754. También en la parte superior del menú de ajustes rápidos (en el área que ocupa la barra de estado) se muestra un acceso al perfil de usuario activo actualmente en el dispositivo móvil, y, seleccionándolo, se presenta la ventana con los usuarios existentes en el dispositivo, permitiéndose poder cambiar a cualquiera de ellos (sin solicitarse ningún tipo de código de acceso para realizar el cambio; sin embargo, sí se solicitará el código de acceso si el usuario al que se cambia ha definido un código de acceso propio). Para más información sobre el perfil multi-usuario, consultar el apartado “9.19. Múltiples perfiles de usuario”.

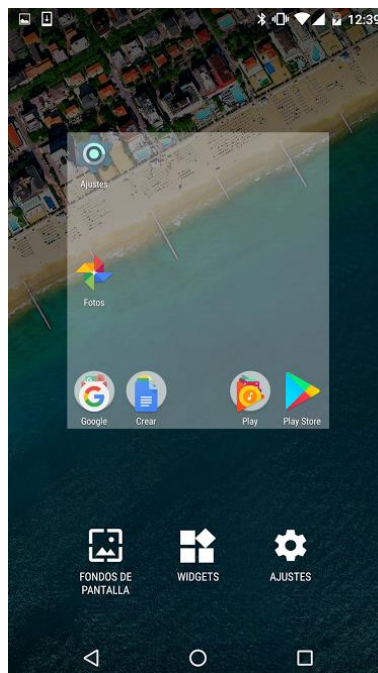


755. Para añadir o quitar elementos del menú de ajustes rápidos, hay que acceder al menú “Ajustes - [Sistema] Configurador de IU del sistema - Ajustes rápidos”. Esta acción desplegará las opciones disponibles del panel de ajustes rápidos. Para eliminar un ajuste rápido, se ha de pulsar en la opción correspondiente y arrastrarla al icono inferior “Eliminar”. Si se pulsa en “Añadir mosaico”, se mostrarán todos los elementos que Android permite integrar como ajuste rápido y que ahora se encuentran inactivos.

756. Para restablecer el menú de ajustes rápidos a las opciones (o elementos) por defecto, es necesario seleccionar el menú “Ajustes - [Sistema] Configurador de IU del sistema - Ajustes rápidos - [Configurador de ajustes rápidos] ... (a la derecha) - Restablecer”.
757. Se recomienda eliminar el “modo avión” del menú de ajustes rápidos para evitar que el dispositivo móvil no pueda ser gestionado remotamente en caso de pérdida o robo.
758. Es importante entender que algunos ajustes rápidos permiten activar y desactivar controles críticos del dispositivo móvil sin necesidad de autenticación. Por este motivo, se recomienda minimizar el número de controles disponibles desde la pantalla de bloqueo como, por ejemplo, el acceso al modo avión.

9.13. PANTALLA DE DESBLOQUEO: WIDGETS Y CARPETAS

759. Android, desde la versión 4.2⁵⁰, permite añadir *widgets* (o complementos) que facilitan mostrar información y contenidos en la pantalla de desbloqueo, especialmente cuando ésta se encuentra bloqueada.
760. A diferencia de Android 4.x (o versiones previas), en el que la configuración de los *widgets* se encontraba dentro del menú “Ajustes [Personal] - Seguridad [Seguridad de la Pantalla] - Habilitar widgets”, a partir de Android 5.x (Lollipop) el acceso a la configuración de *widgets* se realiza con una pulsación mantenida en la pantalla de inicio:



761. Adicionalmente, a partir de Android 5.x los *widgets* no pueden ser añadidos a la pantalla de desbloqueo, reduciendo notablemente el riesgo de seguridad asociado a la revelación de información sensible a través de dicha pantalla. En Android 5.x y versiones posteriores, los *widgets* permiten disponer de accesos directos y de información en la(s) pantalla(s) principal(es) o de inicio de Android, una vez el dispositivo ha sido desbloqueado conociendo el código de acceso [Ref.- 164].
762. Los *widgets* representan normalmente versiones reducidas de ciertas apps, y permiten mostrar la información más relevante de las mismas, como por ejemplo, mensajes de e-

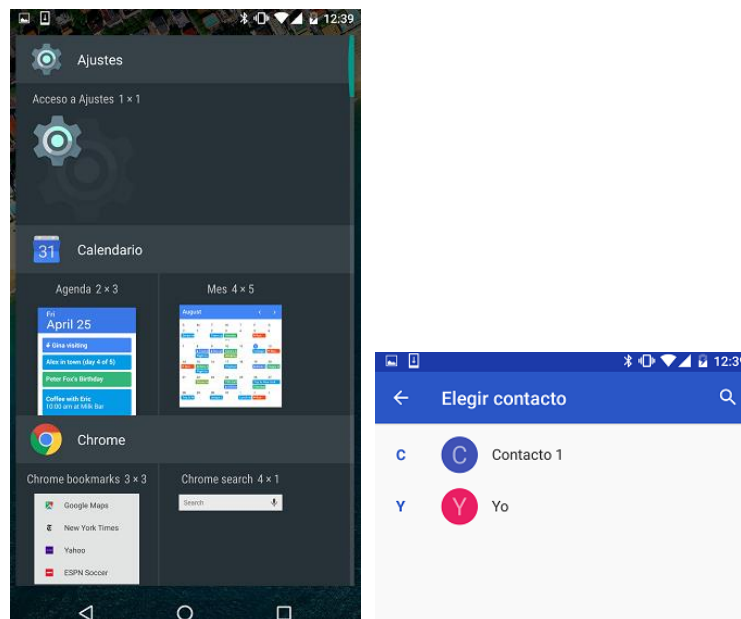
⁵⁰ <http://developer.android.com/about/versions/android-4.2.html#Lockscreen>

mail, citas de calendario o información meteorológica. Se dispone también de *widgets* personalizados de apps de terceros [Ref.- 210].

763. Por defecto en la pantalla de desbloqueo de Android 6.x se muestra únicamente el *widget* asociado al reloj digital.

764. En Android 6.x es posible añadir nuevos *widgets* a la(s) pantalla(s) de inicio mediante el siguiente procedimiento:

- Pulsar un espacio vacío en la pantalla de inicio (o en cualquiera de las pantallas de inicio, en caso de disponer de varias) durante 2 segundos y marcar la opción inferior denominada “Widgets”. Con ello se desplegarán todos los *widgets* disponibles.
- Mantener pulsado el *widget* seleccionado. El dispositivo móvil pasará a mostrar la(s) pantalla(s) de inicio de Android.
- Deslizar el *widget* a la ubicación deseada y soltar el *widget* levantando el dedo. Si el *widget* admite alguna personalización, como por ejemplo gestionar una llamada directa, al soltarlo en la pantalla de inicio que corresponda se abrirá el menú de opciones. En el caso de un acceso directo a una llamada, se mostrará un menú para elegir el contacto.



765. Para cambiar el tamaño de un *widget*, se ha de mantener pulsado el *widget* y levantar el dedo. Si se puede ajustar el tamaño, aparecerá un contorno con puntos en los laterales, y, arrastrando los puntos, se actualizará el tamaño del *widget*. Para terminar, basta con seleccionar cualquier espacio fuera del *widget*.



766. Los *widgets* pueden ser eliminados de la pantalla de inicio mediante una pulsación prolongada sobre el *widget*, y arrastrándolo hacia el texto “X Quitar” existente en la parte superior de la pantalla.
767. Desde la(s) pantalla(s) principal(es) o de inicio, es posible organizar los diferentes iconos y elementos mediante una pulsación larga sobre el icono en cuestión, lo cual permite arrastrarlo y desplazarlo a otra ubicación (incluyendo otro escritorio) y crear grupos de iconos (en Android, se denominan “carpetas”). Por defecto, Android 6.x ya organiza determinadas aplicaciones en carpetas, como “Play” (que contiene todas las apps de “Play”, o “Google”, que engloba las principales apps y servicios de Google, como Gmail, Maps y Fotos).
768. Para crear una carpeta, se pulsará de forma mantenida sobre un icono y se arrastrará el mismo, desplazándolo, hasta superponerlo sobre el icono o carpeta ya existente al que se desea añadirlo. Una carpeta se representa mediante un círculo que tiene destacado al icono inicial sobre el que se comenzaron a añadir los restantes.
769. Para desplegar una carpeta y seleccionar una de las aplicaciones contenidas en ella, se seleccionará brevemente el icono de la carpeta, con lo que se mostrarán todas las aplicaciones que lo integran.



770. Por defecto, una carpeta creada por el usuario no recibe nombre. Si se desea referenciarla de alguna forma, se realizará una pulsación corta sobre la carpeta y se pondrá el dedo sobre el campo “Carpeta sin nombre”, con lo cual aparecerá el teclado y se podrá seleccionar el nombre deseado. Este procedimiento también es válido para cambiar el nombre previamente dado a una carpeta. Por motivos de seguridad y privacidad, se recomienda no dar a las carpetas que contengan aplicaciones sensibles nombres demasiado explícitos, como “Bancos”, “Médicos”, “Contraseñas”..., que podrían dar idea a un potencial atacante con acceso visual a la pantalla sobre el tipo de aplicaciones instaladas.
771. Desde el punto de vista de seguridad, en el caso de querer hacer uso de *widgets*, desde Android 5.x (y vigente en Android 6.x) no existe la posibilidad de seleccionar qué *widgets* se incluirán en la pantalla de desbloqueo, y qué tipo de información, potencialmente sensible, es mostrada por estos (como sí ocurría en versiones previas de Android). En su lugar, la información disponible por defecto (y que puede ser personalizada) en la pantalla de desbloqueo se detalla en el apartado “9.6. Pantalla de desbloqueo: Previsualización de datos”.

9.14. PANTALLA DE DESBLOQUEO: CÁMARA

772. Android, desde la versión 4.0 (*Ice Cream Sandwich*), permite hacer uso de la cámara (para hacer fotografías o grabar vídeos) desde la pantalla de desbloqueo sin necesidad de desbloquearla mediante el código de acceso.
773. El acceso a la cámara desde la pantalla de desbloqueo no está disponible en las tabletas basadas en Android, únicamente en los *smartphones*.
774. El icono de acceso directo a la cámara desde la pantalla de desbloqueo está disponible en la parte inferior derecha, mediante un icono de una cámara. Si se desplaza dicho icono (o la propia pantalla de desbloqueo) hacia la izquierda, se accede a la cámara, disponiendo de control completo sobre la misma y sus opciones de configuración:



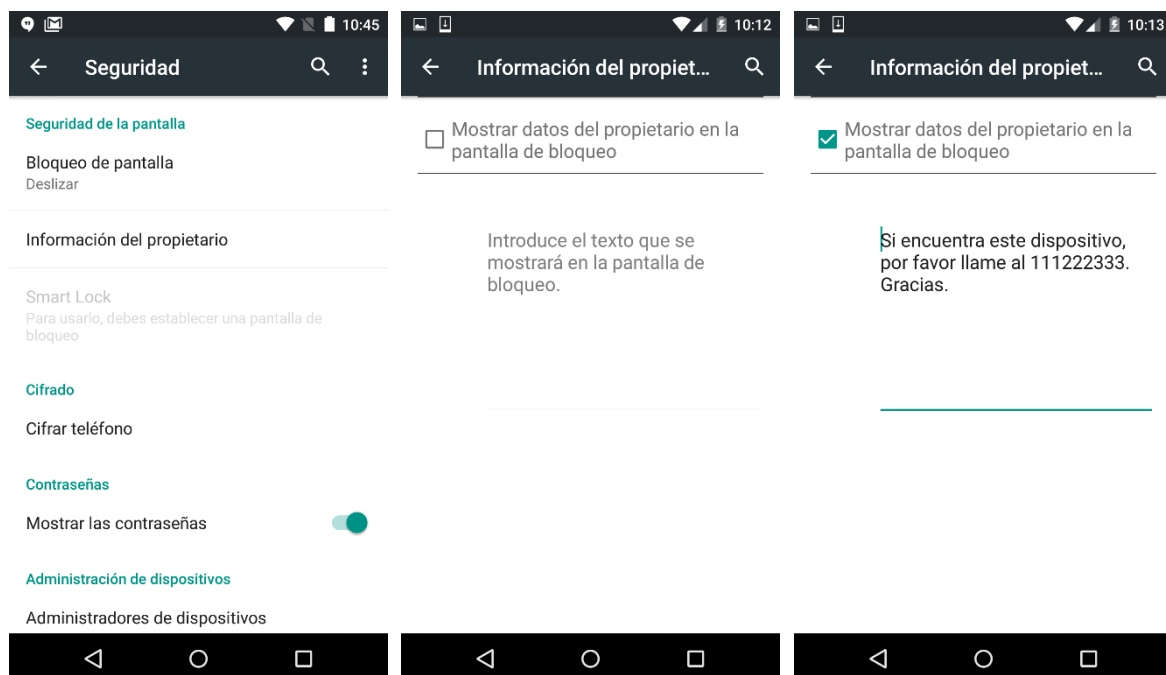
775. Esta funcionalidad tiene implicaciones relevantes desde el punto de vista de seguridad, ya que alguien sin autorización que obtenga acceso físico temporalmente al dispositivo

móvil puede hacer fotografías o vídeos, como si estos hubieran sido realizados por el usuario del terminal.

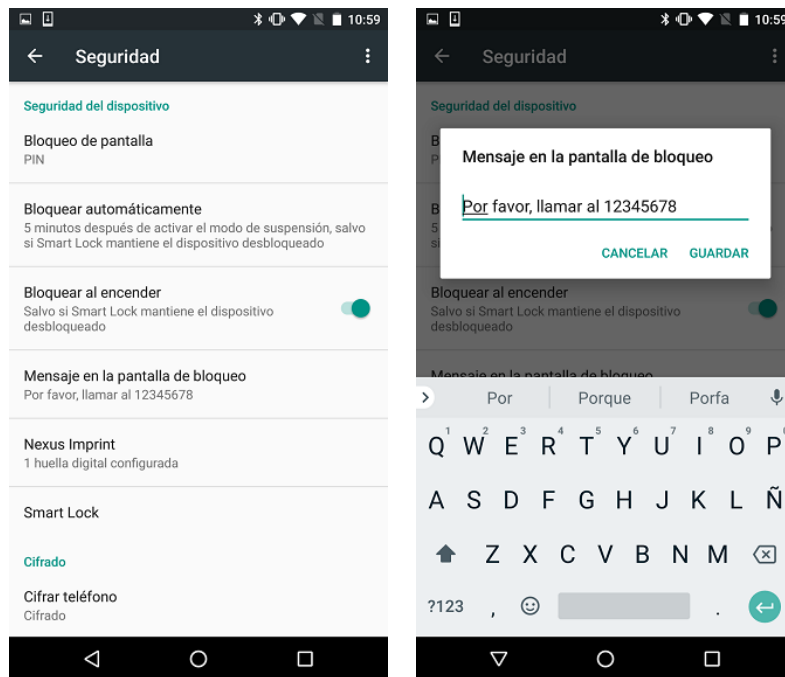
776. De hecho, se han identificado vulnerabilidades importantes que permitían que, a través del acceso a la cámara, se pudiese desbloquear la pantalla sin necesidad de introducir el código de acceso [Ref.- 163].
777. La cámara no puede ser eliminada de la pantalla de bloqueo, ya que Android no dispone de ningún ajuste de configuración con este propósito.
778. Debe tenerse en cuenta que desde la pantalla de bloqueo, respecto a la funcionalidad de la cámara, y sin conocer el código de acceso, sólo se dispone de acceso a las fotografías y vídeos que han sido realizados en la sesión actual (desplazando la pantalla de la cámara hacia la izquierda), no pudiendo visualizarse el resto de fotografías y vídeos. Ello impide que un tercero que tenga acceso físico a un dispositivo Android 6.x bloqueado pueda ver las fotografías o vídeos tomadas previamente por su propietario.

9.15. PANTALLA DE DESBLOQUEO: INFORMACIÓN DEL PROPIETARIO

779. Android permite establecer un mensaje de texto en la pantalla de desbloqueo, característica que es especialmente útil cuando la pantalla se encuentra bloqueada y se extravía el dispositivo móvil.
780. Si alguien con buenas intenciones se encuentra el dispositivo móvil, puede visualizar dicho mensaje y llevar a cabo acciones en función del mismo como, por ejemplo, contactar con su propietario.
781. Hasta Android 5.x incluido, el mensaje con información del propietario está deshabilitado, y se habilitaba a través del menú “Ajustes [Personal] - Seguridad [Seguridad de la Pantalla]” y la opción “Información del propietario”:



782. Desde Android 6.x, el mensaje que se desee mostrar en la pantalla de bloques se configura a través del menú “Ajustes [Personal] - Seguridad [Seguridad del dispositivo]” y la opción “Mensaje en la pantalla de bloqueo”:

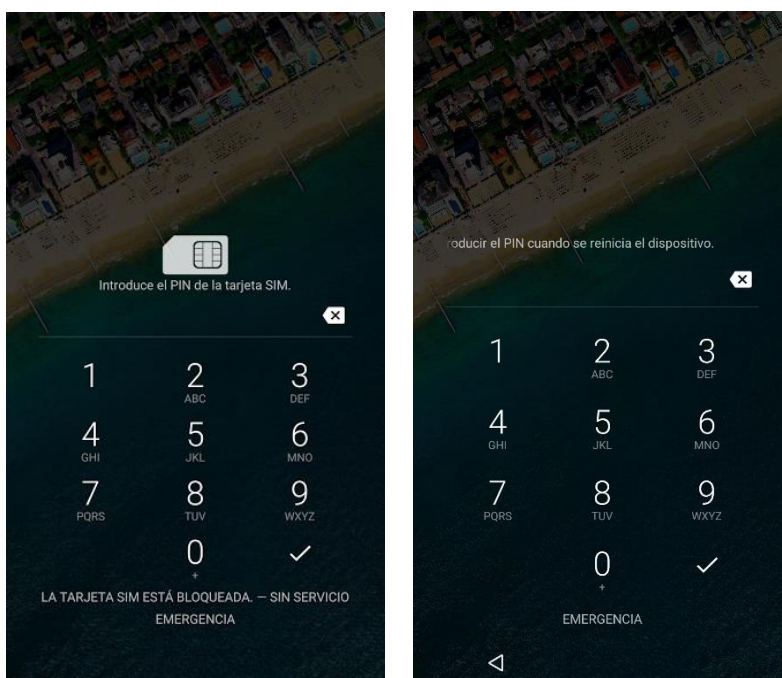


783. Se recomienda proporcionar un mensaje descriptivo que, sin desvelar información sensible, crítica, o que pueda ayudar a identificar detalles innecesarios del propietario, ayude, por ejemplo, a la recuperación del dispositivo móvil. Por ejemplo, se recomienda fijar un mensaje similar al siguiente: “Si encuentra este teléfono, por favor, llame al número +34 123456789. Muchas gracias”. Si el mensaje tiene un número de caracteres que excede el tamaño del área reservada para él en la pantalla de bloqueo, se mostrará como un mensaje que se desliza hacia la izquierda, permitiendo su lectura completa.



9.16. PRECAUCIONES Y RECOMENDACIONES ADICIONALES

784. Adicionalmente a todas las opciones de configuración e implicaciones asociadas detalladas previamente, es posible establecer éstos y otros parámetros de configuración asociados al proceso de desbloqueo del dispositivo móvil a través de las políticas de seguridad de Google G-Suite, sustituto de Google Apps desde finales de 2016 (ver apartado “8. Gestión empresarial de dispositivos móviles basados en Android”).
785. Cuando se establece un código de acceso al dispositivo móvil, si el modo de depuración está habilitado (ver apartado “13.3. Opciones de desarrollo y depuración USB”) es posible acceder al terminal mediante el interfaz USB, por ejemplo para capturar su pantalla, intercambiar datos, gestionar sus ficheros, instalar apps y leer datos del registro de actividades, sin necesidad de desbloquear el dispositivo móvil. Un atacante, mediante acceso físico al terminal, podría potencialmente realizar múltiples tareas de administración del dispositivo móvil sin conocer la contraseña de acceso. El impacto de las acciones que pueden ser llevadas a cabo sin conocer el código de acceso está mitigado por algunas capacidades de seguridad disponibles desde Android 4.4.2 (ver apartado “13.4. Relaciones de confianza a través de USB”).
786. Se recomienda por tanto desde el punto de vista de seguridad deshabilitar el modo de depuración mediante el menú “Ajustes [Sistema] - Opciones de desarrollo”, desactivando la opción “Depuración USB”, y habilitarlo puntualmente cuando se requiera utilizar alguna funcionalidad de este menú.
787. Una vez fijados tanto el PIN en la tarjeta SIM como el código de acceso en el dispositivo móvil, al encender el terminal, el dispositivo móvil solicitará primero el PIN de la tarjeta SIM y después el del terminal, en este orden:



788. Pese a que la obligatoriedad de introducir dos PIN (o códigos de acceso) diferentes puede suponer una molestia para el usuario, desde el punto de vista de seguridad se recomienda que ambos sean distintos, siendo necesario establecer los dos niveles de seguridad para que tanto la tarjeta SIM y sus servicios asociados como el dispositivo móvil y sus datos asociados estén protegidos.

789. Adicionalmente, y con el objetivo de mejorar globalmente la seguridad de los servicios asociados al dispositivo móvil, se recomienda modificar a la mayor brevedad posible el PIN de acceso al buzón de voz proporcionado por el operador de telefonía móvil al activar este servicio. Su valor debe ser diferente al valor del código de acceso del dispositivo móvil y del PIN de la tarjeta SIM.

9.17. DESBLOQUEO MEDIANTE LA CUENTA DE USUARIO DE GOOGLE

790. En versiones de Android 4.x y anteriores, existía la posibilidad de restablecer el código de acceso con la cuenta de usuario de Google o a través del administrador de dispositivos Android (ver apartado 8.1. “Gestión remota de dispositivos Android por parte del usuario”).

791. Esta opción desapareció con Android 5.x (Lollipop), por lo que no se ilustra en la presente guía; si se desea conocer las características de esta funcionalidad, puede consultarse la “Guía CCN-STIC-453B - Seguridad de dispositivos móviles: Android 4.x”. CCN-CERT ([Ref.- 402]).

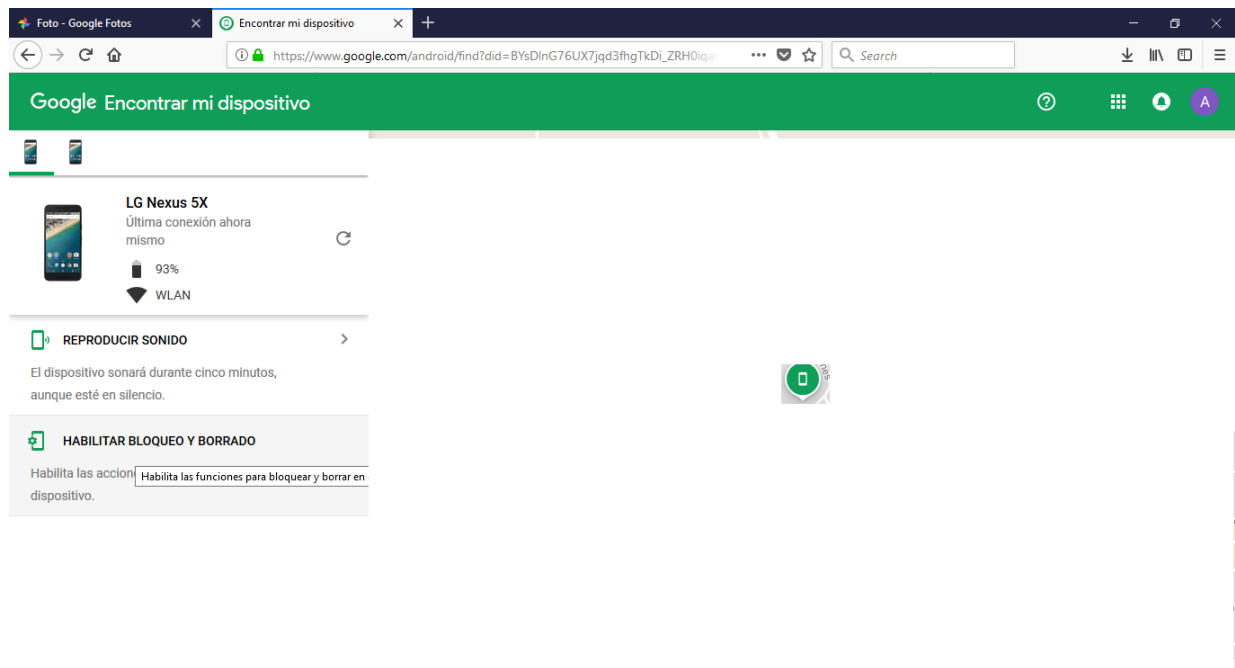
9.18. RESTAURACIÓN DEL CÓDIGO DE ACCESO

792. A través de las capacidades empresariales para la gestión de dispositivos móviles basados en Android proporcionadas por Google, y específicamente a través de la plataforma Google Apps (ver apartado 8.1. “Gestión remota de dispositivos Android por parte del usuario”), es posible llevar a cabo de forma remota la restauración (restablecimiento o reseteo) del código de acceso y desbloqueo del dispositivo móvil desde la versión 2.2 de Android, disponiendo de la app “Google Apps Device Policy”⁵¹ instalada [Ref.- 13].

793. Esta funcionalidad sólo está disponible para los clientes de Google Apps en la categoría de Negocios (Business) que utilizan G Suite (ver apartado “8. Gestión empresarial de dispositivos móviles basados en Android”).

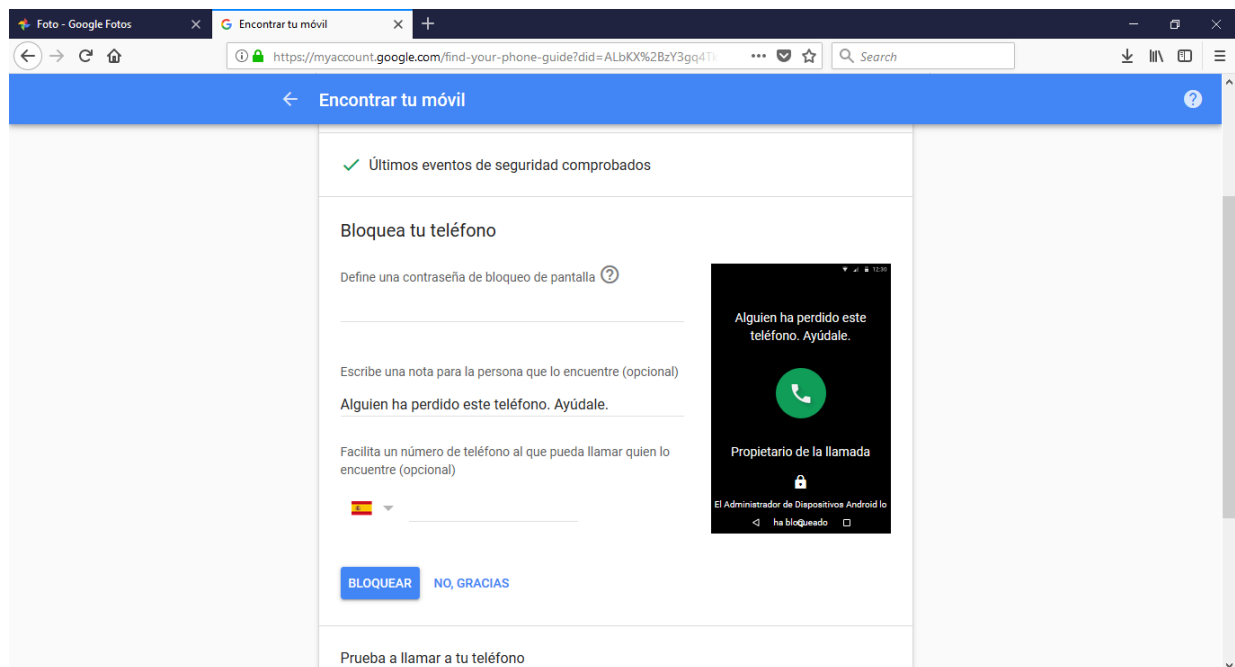
794. El resto de usuarios que disponen de una cuenta de usuario de Google individual pueden hacer uso de la funcionalidad “Encontrar mi dispositivo” (ver apartado “8.1. Gestión remota de dispositivos Android por parte del usuario”), con funcionalidad similar pero que no dispone de las capacidades para restaurar el código de acceso del dispositivo móvil, sino únicamente de “Reproducir sonido” (si se piensa que el dispositivo está en una ubicación donde la emisión de sonido pueda ayudar a localizarlo), “Habilitar bloqueo y borrado” (bloquea la pantalla y permite que se añada un mensaje personalizado) y “Borrar” (equivalente a realizar un reseteo remoto a fábrica) [Ref.- 60].

⁵¹ <https://play.google.com/store/apps/details?id=com.google.android.apps.enterprise.dmagent>



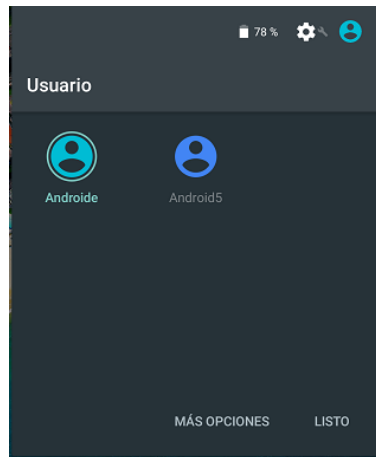
795.El servicio “Encontrar mi dispositivo”, dependiendo de la versión de Android y de los servicios de Google empleada, puede aparecer como “Encontrar tu móvil”, aunque se permite también localizar tabletas.

796.La opción de “Bloquear” permite, en caso de que no se hubiese configurado en el dispositivo un código de acceso previamente (escenario totalmente desaconsejado desde el punto de vista de seguridad), añadir un PIN o una contraseña al mismo.

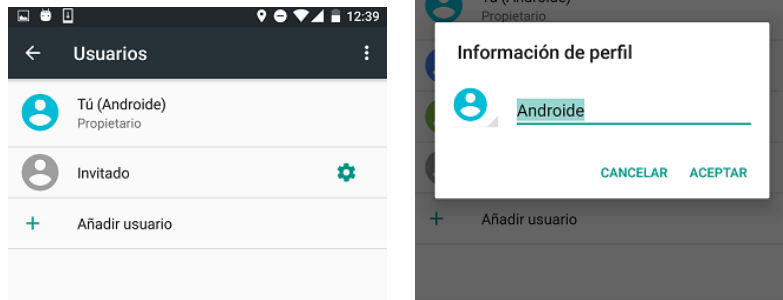


9.19. MÚLTIPLES PERFILES DE USUARIO

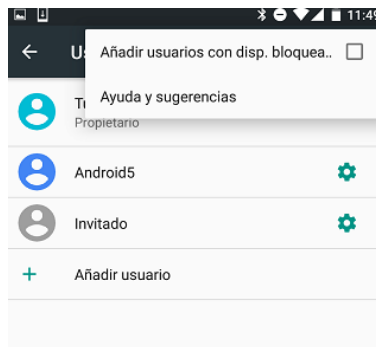
797. La versión 4.2 de Android introdujo para los dispositivos de tipo tableta la posibilidad de disponer de múltiples cuentas o perfiles de usuario, pudiendo cada usuario personalizar la pantalla de desbloqueo, el fondo de pantalla del escritorio, los complementos (*widgets*), las aplicaciones móviles (*apps*) y carpetas, ficheros, cuentas, y ajustes de configuración. Cada usuario dispone de un entorno separado, incluyendo almacenamiento separado en la tarjeta de almacenamiento externa (o tarjeta SD, en caso de existir), mediante emulación. Para más detalles al respecto de la gestión de perfiles en Android 4.x, consultar la “Guía CCN-STIC-453B - Seguridad de dispositivos móviles: Android 4.x” [Ref.- 402].
798. En Android 4.3 se introdujeron los denominados “perfiles restringidos” para los dispositivos de tipo tableta, cuyo objeto es limitar las capacidades de los distintos usuarios definidos en el dispositivo móvil [Ref.- 137].
799. Las capacidades multi-usuario en *smartphones* basados en Android 4.x sólo están disponibles si se lleva a cabo el proceso de *rooting* del dispositivo móvil, pero no oficialmente. Esta limitación se ha establecido en Android definiendo que el número máximo de usuarios en los *smartphones* es igual a uno.
800. Android 5.0 extendió la funcionalidad multi-usuario ya disponible desde Android 4.2 para tabletas a los teléfonos (no todos los teléfonos soportaban esta funcionalidad, aunque sí está disponible en los dispositivos móviles Nexus).
801. Android 5.x también mejora esta funcionalidad en tabletas, como el dispositivo Nexus 9. A diferencia de los teléfonos, las tabletas tienen la opción de crear un perfil. Los perfiles permiten limitar (o habilitar) las apps y servicios que el usuario de ese perfil puede usar. Por ejemplo, es posible limitar la búsqueda de Google, Chrome o la utilización de la cámara [Ref.- 212]. Esta funcionalidad se mantiene en Android 6.x.
802. Como conclusión fundamental de este apartado, y por las razones que se expondrán a continuación, se debe indicar que se desaconseja, desde el punto de vista de seguridad, utilizar la funcionalidad de múltiples perfiles de usuario de Android.
803. La gestión de usuarios y perfiles restringidos está disponible a través del menú “Ajustes [Dispositivo] - Usuarios”, y también desde la barra de ajustes rápidos mediante el icono circular con una silueta seguida del texto “Más opciones”.
804. Para ver los usuarios disponibles en un dispositivo móvil, se accederá a la barra de ajustes rápidos y se pulsará sobre el icono circular del margen superior derecho que representa un humano. Es importante reseñar que esta opción está disponible con el terminal bloqueado, por lo que cualquier persona con acceso físico al dispositivo puede ver qué usuarios existen en el mismo. Si alguno de esos usuarios no hubiese configurado su espacio, o no hubiese definido un método o código de acceso, un intruso podría tomar control de ese usuario y tener acceso a determinadas funcionalidades del dispositivo.



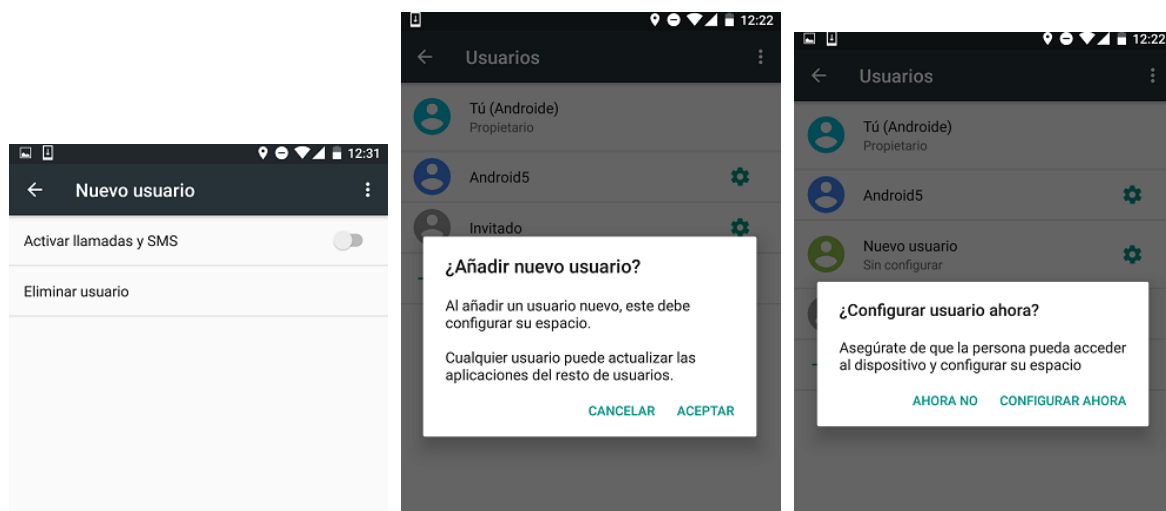
805. El propietario es el usuario que tiene control completo del dispositivo móvil y puede borrar cualquier cuenta (o perfil). El resto de usuarios pueden sólo borrar su propia información y no la de los otros usuarios (incluido, obviamente, el usuario propietario).
806. Para el usuario “invitado” cualquier personalización se almacena solo de forma temporal: cada vez que se selecciona el modo “invitado”, el sistema preguntará si se desea continuar con la última sesión o volver a empezar. El objetivo del perfil de invitado es dar acceso temporal al terminal durante un muy breve periodo de tiempo.
807. Un usuario invitado no debe realizar ningún proceso de configuración inicial, cosa que sí ocurre para el resto de usuarios.
808. Al igual que ocurre con los usuarios, el perfil de invitado tiene su propio espacio en el dispositivo móvil, pero éste puede ser borrado cuando el invitado ha terminado de utilizarlo. Un invitado puede borrarse a sí mismo (y hacer así que desaparezcan los datos que se hayan podido generar durante el periodo de utilización del dispositivo móvil) desde la barra de ajustes rápidos, mediante el icono circular con una silueta seguido del texto “Eliminar invitado”.
809. Por defecto, existen dos usuarios: el propietario o administrador del dispositivo (identificado como “Owner”) y el Invitado. El perfil de invitado aparece directamente en la pantalla de usuarios y no se puede eliminar. El (usuario) propietario identifica al usuario inicial u original existente por defecto, y que fue empleado en el proceso de configuración inicial del dispositivo móvil.
810. La pantalla de “Usuarios [Usuarios y perfiles]” muestra en la primera entrada al usuario actual, identificado como “Tú” y entre paréntesis el nombre del usuario (si no se definió un nombre para el usuario, aparecerá el texto “Owner”) [Ref.- 211].
811. Concretamente, el nombre por defecto es el que se proporcionó en el campo “Nombre y apellidos” durante el proceso de instalación del dispositivo móvil. Si no se rellenó este campo, se mostrará el texto “Owner”. Este nombre se puede cambiar pulsando sobre la entrada del propietario (“Owner”) y rellenando la “Información de perfil”.



812.El propietario puede utilizar el botón “+ Añadir usuario” para añadir nuevos usuarios. Si se quiere permitir que otros usuarios puedan añadir a su vez más usuarios, se pueden seleccionar los tres puntos situados a la derecha de “Usuarios” y marcar la opción “Añadir usuarios con disp. bloqueado”. Se desaconseja por completo activar esta opción desde el punto de vista de seguridad, ya que se perdería el control a la hora de poder añadir nuevos usuarios autorizados.

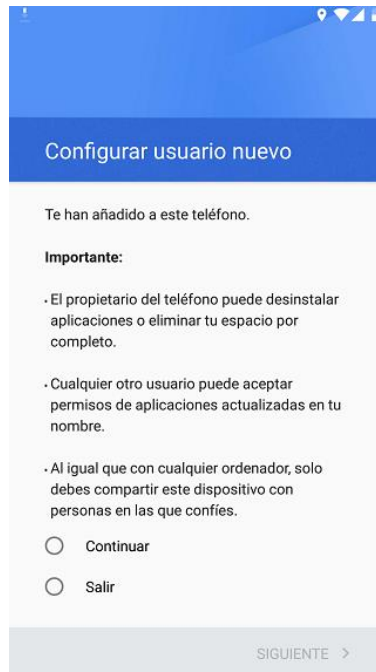


813.Cuando se añade un nuevo usuario, se informa de que dicho usuario debe configurar su espacio de usuario, y se pregunta si se desea configurarlo en ese mismo momento, o no.

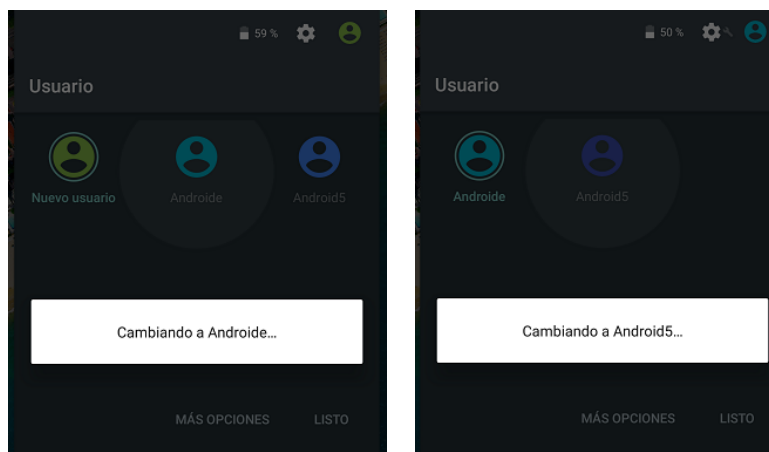


814.Si se opta por no configurar ahora el perfil del usuario, simplemente se mostrará una entrada en la lista de usuarios con el nombre genérico “Nuevo usuario” y, entre paréntesis, se mostrará el estado: “Sin configurar”. Este nombre genérico se actualizará con la información que el usuario proporcione en el apartado “Nombre y apellidos” cuando inicie su proceso de configuración.

815. Al pulsar sobre el nombre de un usuario de la lista disponible bajo “Ajustes [Dispositivo] - Usuarios”, el terminal cambiará al perfil de ese usuario. Si no está configurado, se ofrecerá la opción de realizar la configuración de igual modo que cuando se añadió dicho usuario. Si el usuario opta por la opción “Salir” y no continúa con el proceso de configuración, dicho usuario será borrado del dispositivo y, en caso de requerirse su existencia, deberá ser creado de nuevo.

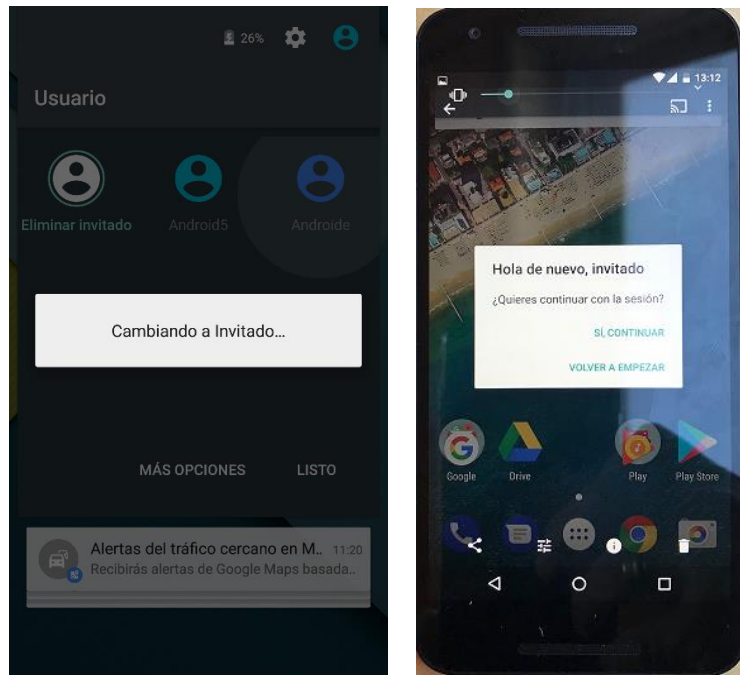


816. La opción más rápida para cambiar entre usuarios es seleccionar el icono correspondiente a un rostro en la barra de ajustes rápidos y elegir el nombre del usuario al que se desea cambiar:



817. En un dispositivo móvil pueden existir múltiples usuarios además del propietario, pero sólo se dispone de un usuario invitado.
818. Para poder utilizar el perfil de invitado por primera vez, o tras resetear el perfil de invitado, es necesario entrar en “Ajustes [Dispositivo] - Usuarios” o desde la barra de ajustes rápidos (bajo el menú circular con el símbolo de perfil seguido de “Más opciones”) como usuario propietario, y seleccionar el perfil “invitado”. Con esta acción, el sistema creará el perfil de invitado y cambiará a él. Hasta que no se haya creado el perfil de invitado con este método, ningún usuario distinto del propietario podrá utilizar el perfil invitado.

819.Una vez creado el perfil invitado, el menú de usuarios de la barra de ajustes rápidos mostrará ese perfil, y cualquier usuario podrá utilizarlo.



820.Un usuario distinto del propietario puede añadir nuevas redes Wi-Fi, que estarán disponibles para todos los usuarios del dispositivo móvil, con las negativas implicaciones de seguridad asociadas.

821.Cualquier usuario tiene acceso al menú de ajustes rápidos con la configuración por defecto de Android. Este aspecto es también muy delicado desde el punto de vista de seguridad, porque el propietario podría haber personalizado este menú para, por ejemplo, eliminar el acceso rápido al modo avión, que, sin embargo, se mostraría para cualquier otro usuario del terminal, incluido el perfil de invitado.

822.Asimismo, los usuarios tienen acceso a muchos ajustes de configuración, si bien no a todos.

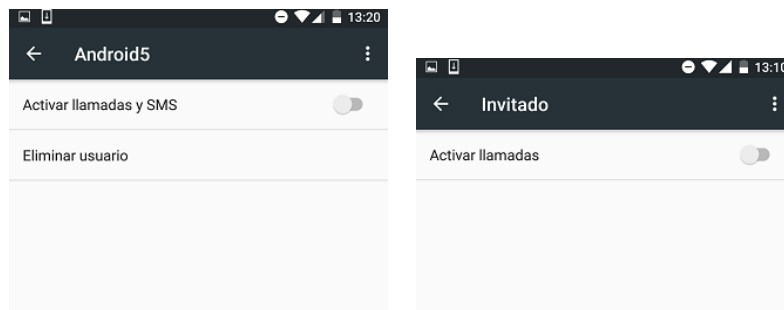
823.Los usuarios distintos del invitado tienen su propio espacio en el dispositivo móvil con opciones de configuración, aplicaciones (apps), cuentas y pantallas de inicio personalizadas, entre otros elementos.

824.Un usuario puede añadir su cuenta de Google al dispositivo e instalar aplicaciones desde Google Play. Las apps instaladas por un usuario son solo visibles para él (otros usuarios o el propietario no las vería). Si una app que un usuario elige instalar ya está instalada por otro usuario, se creará un espacio virtual (o *sandbox*, diferenciado) para el nuevo usuario dentro de esa aplicación (o app), de modo que cada usuario dispondrá únicamente de acceso a sus datos dentro de la app.

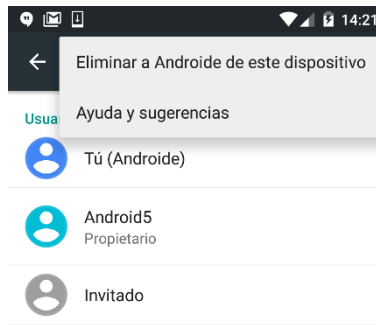
825.Si un usuario elige actualizar una aplicación y dicha aplicación también existe para otro usuario, se actualizará la versión de la aplicación para ambos. Es decir, la actualización de apps se lleva a cabo a nivel global dentro del dispositivo móvil.

826.Asimismo, cualquier usuario puede aceptar nuevos permisos en el proceso de actualización de apps, afectando globalmente desde el punto de vista de seguridad al dispositivo móvil y al resto de usuarios.

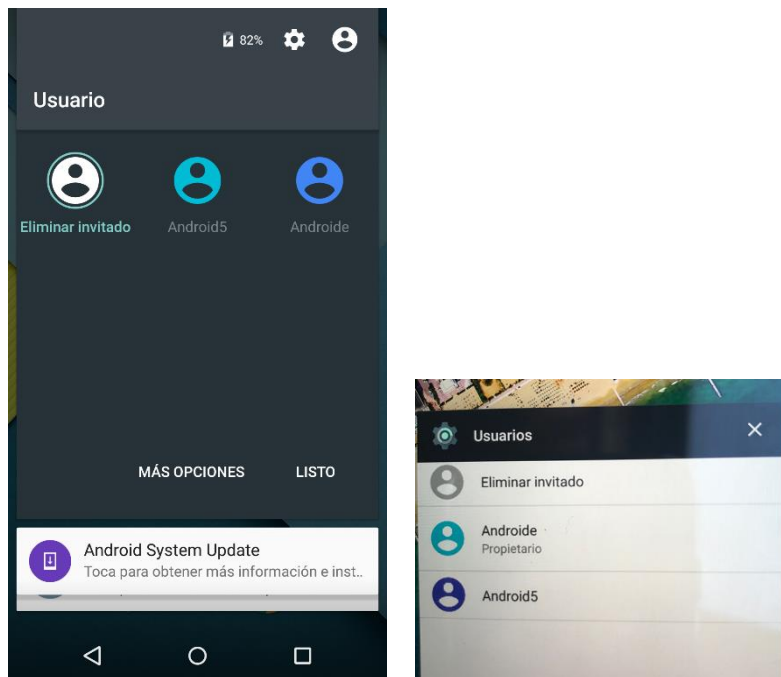
827. Cualquier usuario, incluyendo el invitado, tiene opción de cambiar a otro usuario, incluido el propietario (u “Owner”) del dispositivo móvil, a través de la barra de ajustes rápidos sin que se solicite ningún código para realizar esta acción (el menú de ajustes rápidos y la barra de notificaciones están disponibles tal como se detalló en el apartado “9.12. Menú de ajustes rápidos y barra de notificaciones”). Si el usuario al que se cambia tiene configurado un código de acceso, aparecerá la pantalla de bloqueo, y será necesario introducir su código. Si el usuario al que se cambia no tiene definido un código de acceso, se entrará en su espacio de usuario sin requerirse ningún tipo de autenticación.
828. Por defecto, un usuario no tiene permisos para utilizar los servicios de telefonía. Si se desea otorgárselos, hay que seleccionar “Ajustes - [Dispositivo] Usuarios - Nombre del usuario”, mediante el botón de ajustes situado a la derecha del nombre del usuario y marcar el interruptor “Activar llamadas y SMS”. Para el invitado, la opción se denomina “Activar llamadas”.



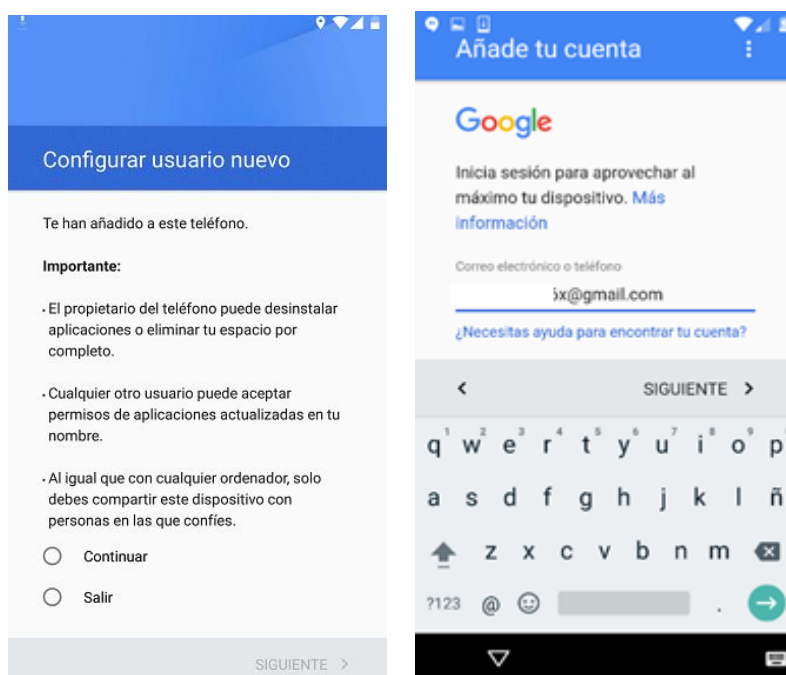
829. Para eliminar un usuario, hay que seleccionar “Usuarios - Nombre del usuario”, mediante el botón de ajustes situado a la derecha del nombre del usuario y marcar la opción “Eliminar usuario”. Aparecerá una ventana de confirmación que indica que se eliminarán los datos y las aplicaciones. Si la aplicación solo ha sido instalada por ese usuario, se borrará del dispositivo móvil; si algún otro usuario la instaló, únicamente se borrará de la aplicación el espacio de datos asociado a ese usuario.
830. Además, un usuario puede eliminarse a sí mismo sin más que entrar en su perfil, seleccionar en el símbolo de usuario de la barra de ajustes rápidos, mediante “Más Opciones - [Usuarios] tres puntos (...) - Eliminar a <nombre de usuario> de este dispositivo”.



831. Cuando se cambia de un usuario a otro, se presenta la pantalla de bloqueo del usuario destino y, tras desbloquearla, se llegará a la pantalla que este usuario tuviera activa la última vez que usó el terminal. Se mantienen por tanto todos los datos de la sesión activa.
832. Ningún usuario distinto del propietario tiene acceso a la opción de “Copia de seguridad y restauración”, por lo que no pueden realizar copias de seguridad o backups de sus datos ni acceder a eliminar los datos del dispositivo móvil (pueden eliminar los datos propios borrando su perfil).
833. Para eliminar al usuario invitado, hay que entrar en el perfil de invitado y, desde la barra de ajustes rápidos o desde el menú “Ajustes - Usuarios [Usuarios y perfiles]”, seleccionar “Eliminar invitado”. El propietario del dispositivo, que sí puede borrar otros usuarios, no puede eliminar al usuario invitado. Para hacerlo, tiene que entrar en el perfil del invitado y eliminarlo desde ahí. Es importante tener esto en cuenta en caso de haber habilitado temporalmente un usuario invitado para no dejarlo disponible y activo por descuido en el dispositivo móvil.



834.El proceso de configuración de un nuevo usuario (desde la pantalla de desbloqueo) conlleva un proceso similar al de configuración inicial del dispositivo móvil, pero en los aspectos relacionados específicamente con el nuevo usuario. Permite por ejemplo añadir (opcionalmente) la cuenta de Google del usuario (ofreciéndose la posibilidad de crear una cuenta de usuario de Google si no se dispone de una), determinar si se permitirá a las apps hacer uso de los servicios de ubicación y con qué precisión, solicitar el nombre del usuario para personalizar algunas apps, confirmar la aceptación de actualizaciones a través de los servicios de Google, y permite al usuario personalizar la pantalla de inicio. El proceso es idéntico al descrito en el apartado “20. Cuenta de usuario de Google”.



835.La implementación multi-usuario de Android asigna un identificador (o ID) a cada usuario (que es independiente de los identificadores o UIDs asignados a las apps a nivel de Linux), empezando por el identificador 0, que es asignado al usuario propietario.

836. La información de cada usuario se almacena en el directorio “/data/system/users/<ID>”, donde se guardan los ajustes de configuración del usuario, las personalizaciones de su pantalla de inicio, y la lista de apps actualmente instaladas y disponibles para ese usuario.
837. Los binarios de las apps se comparten entre los usuarios, para evitar duplicidades y un consumo innecesario de la memoria de almacenamiento, pero el directorio o *sandbox* de trabajo de la app es independiente para cada usuario, obteniéndose una copia del original en el momento de la instalación (o activación) de la app para un usuario concreto.
838. Las capacidades multi-usuario de Android modifican el modelo de asignación de identificadores o IDs para las apps descrito en el apartado “7.2. Sandbox de ejecución de las apps”, ya que al ser instalada para un usuario concreto, cada app recibe un nuevo identificador efectivo combinación del ID de usuario y del ID de la app [Ref.- 195].
839. Desde el punto de vista empresarial o corporativo, no se recomienda la compartición de los dispositivos móviles entre distintos usuarios, por lo que se desaconseja el uso de las capacidades para disponer de múltiples perfiles de usuario en Android.
840. En caso de identificarse escenarios donde debe compartirse el uso de un mismo dispositivo móvil Android entre distintos usuarios (por ejemplo, un terminal utilizado para un servicio de guardia con rotación entre varias personas), se recomienda llevar a cabo un análisis detallado de los requisitos, planificar adecuadamente su implementación e investigar minuciosamente las posibles implicaciones de seguridad de la puesta en marcha de las capacidades multi-usuario para la versión concreta de Android empleada.

10. CIFRADO DE DATOS EN ANDROID

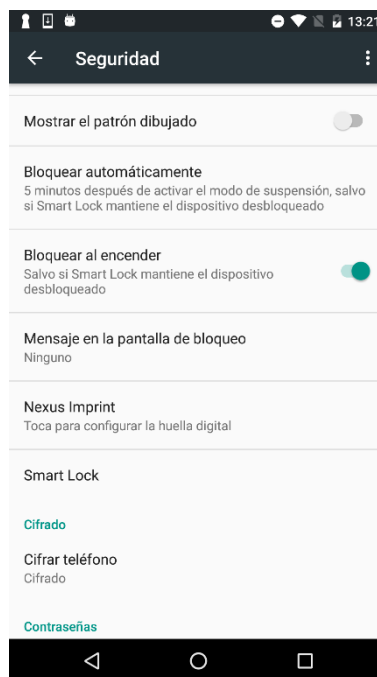
10.1. CIFRADO DEL DISPOSITIVO MÓVIL

841. Android 6.x dispone de capacidades para el cifrado de los datos almacenados en la memoria interna del dispositivo móvil de forma nativa, de forma que los mismos sólo se puedan consultar cuando el dispositivo está desbloqueado [Ref.- 85].
842. Desde la versión 3.0 de Android (“Honeycomb”) [Ref.- 31], orientada a dispositivos móviles de tipo tableta, se añadieron capacidades de cifrado nativas a los dispositivos móviles basados en Android [Ref.- 85] (basadas en dm-crypt⁵²), junto a otras mejoras en las políticas de cifrado y de contraseñas (complejidad, expiración e histórico).
843. Lógicamente, la opción de cifrado completo del dispositivo móvil también está disponible en versiones posteriores, como Android 5.x (y versiones futuras), para teléfonos móviles o *smartphones*, tanto del teléfono como (potencialmente) de la tarjeta de almacenamiento externa (en aquellos dispositivos móviles que disponen de una tarjeta SD real).
844. Por otro lado, existen numerosas apps de cifrado en Google Play (ej. OpenPGP para Android, AGP⁵³) que permiten el cifrado de otros datos, como por ejemplo notas, información confidencial o contraseñas, pero no de la totalidad del dispositivo móvil.

⁵² <https://code.google.com/p/cryptsetup/wiki/DMCCrypt>

⁵³ <https://play.google.com/store/apps/details?id=org.thialfiar.android.apg&hl=es>

845. Los mecanismos de cifrado han ido variando a lo largo de las diferentes versiones de Android, con el objetivo de proteger el cifrado de los datos frente a ataques de fuerza bruta (dado que el cifrado del dispositivo móvil está basado, o depende, del código de acceso empleado en el mecanismo de bloqueo del dispositivo).
846. En Android 5.x (Lollipop) la contraseña de cifrado depende sólo parcialmente del código de acceso al dispositivo móvil, interviniendo también otros elementos (que serán descritos posteriormente) en su protección [Ref.- 134].
847. En septiembre de 2014 Google anunció que sería obligatorio que cualquier terminal con Android viniera cifrado de fábrica. Sin embargo, alegando problemas de rendimiento, finalmente el cifrado de fábrica se incluyó como “una recomendación” y no como una obligación para los demás fabricantes.
848. Aunque Google informó públicamente de que los terminales que se fabricasen a partir de Android 5.x (Lollipop) vendrían cifrados de fábrica [Ref.- 140], los dispositivos Nexus 4, Nexus 5, Nexus 7 y Nexus 10 no se cifran de forma predeterminada⁵⁴.
849. Los dispositivos móviles como el empleado para la elaboración de la presente guía (Nexus 5X con Android 6.x) sí vienen cifrados de fábrica y no es posible deshabilitar las capacidades de cifrado. Los pasos detallados a continuación para proceder al cifrado corresponden a un dispositivo de otro fabricante que no obliga a que el dispositivo esté cifrado:



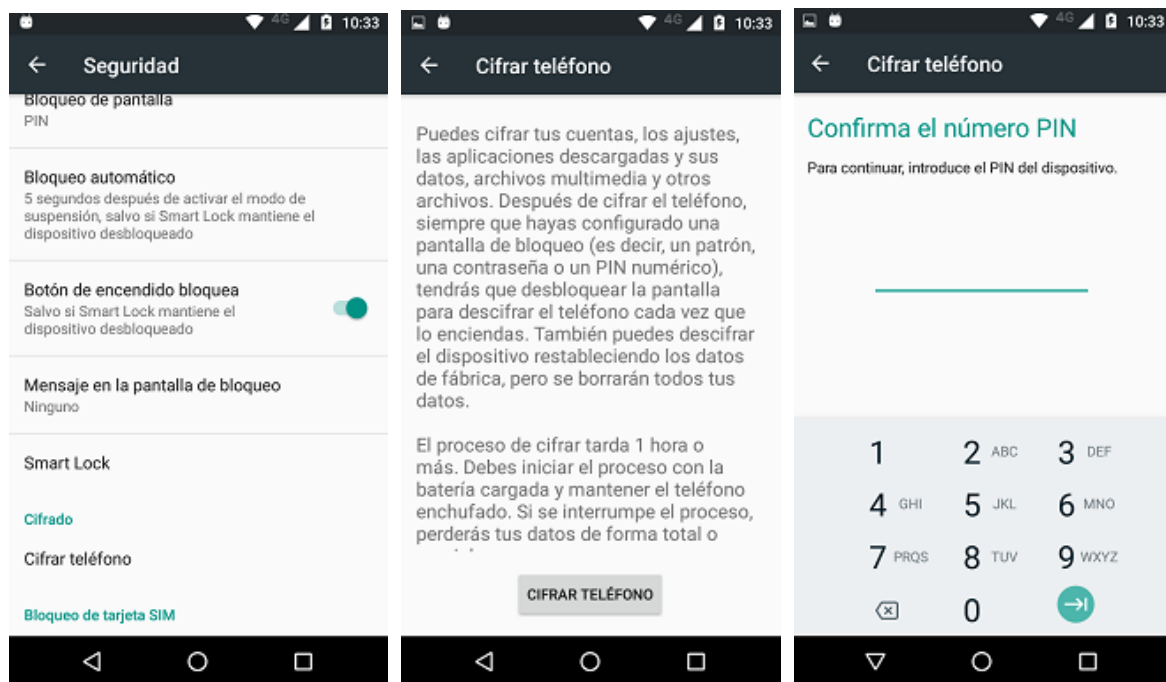
850. La única opción disponible bajo el menú “Ajustes - [Personal] Seguridad - [Cifrado] Cifrar teléfono” una vez la memoria del dispositivo móvil ha sido cifrada es la indicación de que la memoria está cifrada (mediante el texto “Cifrado”, tal como ilustra la imagen superior).
851. El proceso de cifrado es irreversible y no es posible devolver al terminal a una configuración sin cifrar. Si un dispositivo que partía de una versión de Android que no obligaba al cifrado se cifra posteriormente, la única opción posible para deshabilitar las

⁵⁴ <https://support.google.com/nexus/answer/2844831?hl=es>

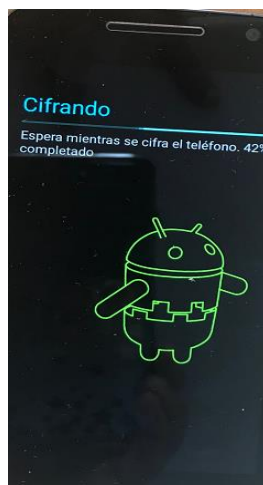
capacidades de cifrado es restablecer el dispositivo móvil a sus ajustes de fábrica (lo que eliminará todos los datos de usuario del terminal) y restaurar posteriormente los datos de usuario desde una copia de seguridad. Es decir, en ningún caso es posible revertir el cifrado de la partición de datos de usuario.

852. En caso de que el terminal no viniese cifrado de fábrica y sí ofreciese la posibilidad de ser cifrado posteriormente, antes de proceder a cifrarlo se recomienda realizar una copia de seguridad completa del dispositivo móvil (ver apartado “21. Copias de seguridad”), y conectar el dispositivo a la corriente eléctrica, para evitar que el proceso de cifrado pueda interrumpirse sin haberse completado por agotarse la batería.

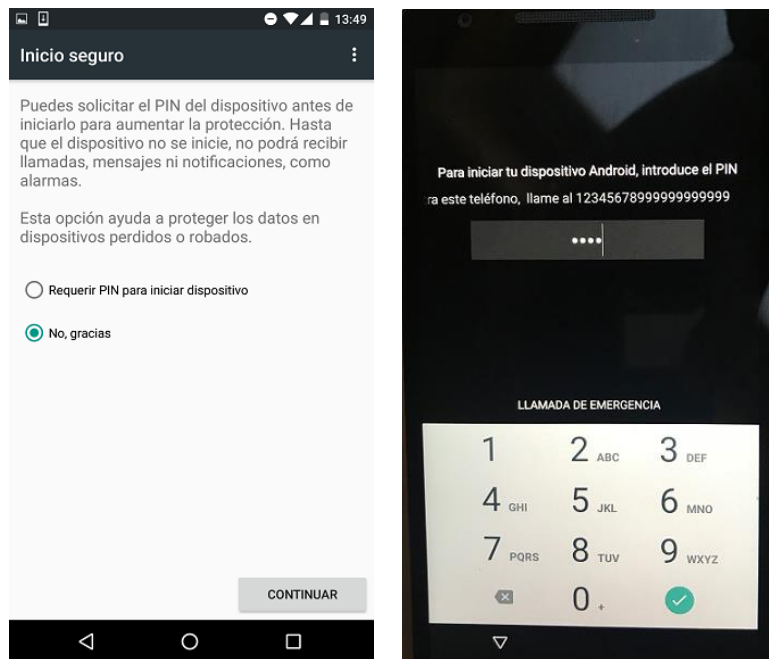
853. La opción “Cifrar teléfono” (o *tableta*) está disponible desde el menú “Ajustes [Personal] - Seguridad [Cifrado]”:



854. Durante el proceso de cifrado, el terminal se reiniciará y mostrará el porcentaje de avance de dicho proceso hasta llegar al 100%, tras lo cual se reiniciará. El tiempo total requerido para completarlo dependerá del tamaño actual ocupado por la partición de datos de usuario del dispositivo móvil (dependiente de la capacidad de almacenamiento total del dispositivo):



855. Es muy importante reseñar que, aunque en su página oficial de soporte⁵⁵, Google indica que se debe establecer un código de acceso en el dispositivo móvil en forma de contraseña o PIN para proceder al cifrado (configurable desde “Ajustes - [Personal] Seguridad - Bloqueo de Pantalla - PIN - [Inicio Seguro]”), un terminal se puede cifrar sin que se encuentre activo ningún código de acceso, como se ilustra a continuación. Este hecho, que también se constata en Android 5.x, contrasta con el comportamiento de versiones de Android 4.x y anteriores, en las que disponer de un código de acceso era obligatorio para llevar a cabo el proceso de cifrado:



856. Los dispositivos móviles que vienen cifrados de fábrica, que no tienen configurado ningún código de acceso, utilizarán como contraseña para proteger la clave de cifrado el valor “default_password”⁵⁶.

857. Si el usuario no define un código de acceso propio, para cifrar el terminal se empleará también la contraseña por defecto “default_password”.

858. Si, a pesar de que se haya definido un código de acceso, no se ha seleccionado la opción “Inicio Seguro - Requerir PIN para iniciar dispositivo”, el cifrado también se realizará en base a la contraseña por defecto.

859. La contraseña por defecto, que protege (junto a la semilla) a los dispositivos cifrados frente a ataques “off-device” (es decir, ataques que se realizan sin acceso físico al dispositivo móvil), no protege frente ataques que se realicen sobre el propio dispositivo (como en caso de pérdida o robo). Por tanto, para proteger realmente los datos del dispositivo móvil, es necesario cifrarlo y establecer un código de acceso que se solicite durante el proceso de arranque. De este modo, el código de acceso definido por el usuario se empleará para envolver la clave de cifrado y no será posible descifrar la partición de datos si no se dispone de dicho código de acceso.

860. Android 6.x, al igual que Android 5.x, implementa el mecanismo denominado FDE (*Full Device Encryption*, o *Full-Disk Encryption*), el cual, pese a su nombre, en realidad sólo

⁵⁵ <https://support.google.com/nexus/answer/2844831?hl=es>

⁵⁶ https://source.android.com/security/encryption/full-disk# how_android_encryption_works

cifra la partición o sistema de ficheros con los datos de usuario (*user data*), correspondiente al punto de montaje “/data”, y no toda la memoria (o “disco”) del dispositivo móvil.

861. La implementación de cifrado del dispositivo móvil (FDE, *Full-Disk Encryption*) de Android está basada en cryptfs (dm-crypt) empleando AES 128 bits en modo CBC y con ESSIV:SHA256 [Ref.- 157] y PBKDF2 con 2000 iteraciones para la derivación de la clave empleada para cifrar la clave maestra [Ref.- 85]. Es decir, los sectores del disco (o memoria de almacenamiento) se cifran con AES-CBC empleando la clave maestra, derivando los vectores de inicialización (IVs, Initialisation Vectors) de los sectores con ESSIV:SHA256.
862. La clave maestra se almacena en la memoria del dispositivo móvil, junto a una cabecera con los detalles del cifrado y una semilla (o *salt*), cifrada con una clave AES de 128 bits (KEK, *Key Encryption Key*) derivada a partir del código de acceso del usuario y las 2000 iteraciones de PBKDF2.
863. Desde la versión 4.4 de Android (KitKat) se emplea scrypt en lugar de PBKDF2 como función de derivación de claves (KDF, *Key Derivation Function*), que ha sido diseñado específicamente para dificultar los ataques de *cracking* de contraseñas mediante GPUs (*Graphics Processor Units*) al requerir grandes cantidades de memoria. Los dispositivos móviles cifrados con versiones previas de Android migran a scrypt en el primer arranque tras actualizar a KitKat [Ref.- 158].
864. Por tanto, la clave maestra se almacena cifrada con una clave (KEK) derivada aplicando scrypt sobre el código de acceso del usuario y una semilla aleatoria.
865. Desde la versión 5.x de Android se añadieron capacidades para almacenar la clave de cifrado en un procesador criptográfico o repositorio de almacenamiento de claves hardware (*hardware-backed*), en aquellos dispositivos móviles que disponen de éste, empleando una implementación de TEE (*Trusted Execution Environment*), concretamente, la TrustZone de ARM [Ref.- 135], como por ejemplo en los procesadores basados en chips Qualcomm con QSEE (*Qualcomm Secure Execution Environment*). Con Android 5.1, y para eliminar los problemas de rendimiento que el cifrado provocaba en dispositivos con versión Android 5.0, se aprovecharon las capacidades hardware de los terminales para acelerar el proceso de cifrado/descifrado [Ref.- 237].
866. Las capacidades de protección adicionales añadidas en Android 5.x, con el objetivo de limitar ataques criptográficos *offline* sin disponer del dispositivo móvil, se basan en almacenar la clave maestra al igual que para Android 4.4, pero en este caso, durante el proceso de cifrado la clave KEK (empleada para cifrar la clave maestra) se firma previamente (de nuevo con scrypt) empleando una nueva clave que reside únicamente en el hardware del dispositivo móvil (TEE), y haciendo uso de las capacidades de firma criptográfica del TEE [Ref.- 85].
867. Asimismo, se añadió la posibilidad de hacer uso de un cifrado más rápido basado en cifrar únicamente los bloques con datos de la partición de usuario, evitando así que el primer proceso de arranque tras habilitar el cifrado se alargase demasiado en el tiempo [Ref.- 85].
868. Android 5.x añadió soporte para poder hacer uso del cifrado del dispositivo móvil utilizando un patrón de desbloqueo como alternativa al código de acceso basado en un PIN o contraseña.



Nota: Aunque los dispositivos Nexus sí soportan el uso del patrón junto al cifrado, es importante reseñar que no todos los fabricantes de dispositivos móviles lo soportan. Por tanto, se recomienda ser cuidadoso a la hora de optar por el patrón como método de acceso con un terminal cifrado, pues en la realización de las pruebas de cifrado de esta guía se ha observado algún caso en el que, al cambiar el método de acceso PIN por un patrón en un terminal cifrado, el dispositivo ha quedado inutilizable y ha sido necesario restablecerlo a fábrica.

869. Por otro lado, una sutil diferencia añadida en Android 5.x es que el código de acceso sólo se le solicita al usuario una única vez al arrancar el dispositivo móvil, en lugar de en dos ocasiones como ocurría previamente, al arrancar el dispositivo móvil y, de nuevo, para desbloquearlo una vez éste ha arrancado.
870. Debe tenerse en cuenta que la implementación del cifrado completo del dispositivo móvil (FDE) empleada por Android hace uso del mismo código de acceso tanto para el cifrado como para el desbloqueo del terminal.
871. Este modelo de cifrado ha sido empleado por Android desde los orígenes de FDE (es decir, desde Android 3.0, Honeycomb), y tiene numerosas implicaciones negativas desde el punto de vista de seguridad. Debido a que se emplea el mismo código, y a que los usuarios deben introducir el código de acceso o desbloqueo del terminal en múltiples ocasiones a lo largo del día, tenderán a elegir un código más sencillo y fácil de utilizar, y por tanto de adivinar, y que puede potencialmente ser obtenido mediante técnicas de ataque de fuerza bruta sobre la memoria (o partición de datos) del dispositivo móvil.
872. Por otro lado, el código de cifrado está limitado a 16 caracteres (por diseño de Android[Ref.- 153]), por lo que no es posible hacer uso de frases de paso (*passphrases*) en lugar de contraseñas (*passwords*). Existen herramientas disponibles públicamente para llevar ataques de fuerza bruta sobre la partición de datos del dispositivo móvil y obtener la contraseña de cifrado, y en consecuencia, el código de acceso.

873. Adicionalmente, un potencial atacante podría ver como el usuario teclea el código de acceso en la pantalla del terminal, mediante técnicas de *shoulder surfing*, y obtener a su vez la contraseña de cifrado.
874. Mientras el código de acceso sólo debe proteger frente a ataques *online* (es decir, que requieren de acceso físico al dispositivo en el momento del ataque), protegido por técnicas que limitan el número de intentos fallidos a través de la pantalla de desbloqueo, la contraseña de cifrado debe también proteger frente a ataques *offline* (los que pueden llevarse a cabo sin acceso físico al dispositivo en el momento del ataque, como en caso de haber obtenido un volcado de la memoria), en los cuales es posible probar un mayor número de combinaciones por unidad de tiempo y sin limitaciones.
875. Como resultado, un potencial atacante dispondría del código de acceso que le permitiría tanto desbloquear y acceder al dispositivo móvil, como descifrar los contenidos de una imagen (o copia) de la memoria del terminal. Esta debilidad fue ya notificada a Google en abril de 2012 mediante el caso (*issue*) 29468 [Ref.- 154].
876. Debe tenerse en cuenta que es posible en Android modificar la contraseña de cifrado (e independizarla del código de acceso) a través de las utilidades de gestión de los volúmenes y particiones del dispositivo móvil, pero para ello es necesario disponer de permisos de root [Ref.- 157]. Por este motivo, esta información sólo se proporciona a modo informativo:
- ```
vdc cryptfs changepw <nueva_contraseña>
```
877. Algunas alternativas similares existentes, en forma de apps de Android, como por ejemplo EncPassChanger [Ref.- 155] o Cryptfs Password [Ref.- 156] (que también requieren disponer de permisos de root), permiten establecer dos códigos diferentes (contraseña de cifrado y código de acceso).
878. Debe tenerse en cuenta que, al emplear estas herramientas de personalización, cada vez que se modifique el código de acceso del dispositivo móvil será necesario modificar de nuevo la contraseña de cifrado, por lo que sería preferible que el proceso se unificara de forma nativa en Android y automáticamente para el usuario.
879. Se considera que los usuarios podrían aceptar de manera más confortable disponer de un código más complejo y de mayor longitud para el cifrado del dispositivo móvil, que únicamente debe ser introducido una vez durante el proceso de arranque, y otro código menos robusto, que les permita desbloquear y acceder al dispositivo múltiples veces a lo largo del día de manera más cómoda.
880. El uso de scrypt en lugar de PBKDF2 en Android 4.4 (o superior), dificulta ligeramente este tipo de ataques ralentizando su ejecución, especialmente cuando se emplean GPUs en lugar de CPUs para los ataques de fuerza bruta. Adicionalmente, en Android 5.x se mitigan algunos de estos ataques mediante las protecciones hardware descritas previamente.
881. Aunque desde Android 5.x Google ya recomendaba que los dispositivos móviles que se comercializaran con Android 5.x viniesen cifrados de fábrica, queda a criterio del fabricante proporcionar capacidades de cifrado nativas del dispositivo móvil desde el primer arranque. De hecho, determinados problemas de rendimiento observados en dispositivos con Android 5.x relacionados con el cifrado llevaron a que no se fijase el cifrado de fábrica como requisito obligatorio.

- 882.El estado de cifrado del dispositivo móvil no cambia con la actualización a Android 6.x desde una versión de Android inferior.
- 883.Sin embargo, debe tenerse en cuenta que algunos dispositivos móviles que hayan sido actualizados a Android 6.x desde versiones previas en las que no estuvieran cifrados, al restablecerse los ajustes de fábrica podrían dejar de estar cifrados, mientras que aquellos dispositivos móviles para los que el fabricante ha forzado que estén cifrados desde el primer arranque no pueden presentar un estado que no haga uso del cifrado. Por tanto, siempre se recomienda verificar el estado de las capacidades de cifrado tras el proceso de configuración inicial a través del menú “Ajustes [Personal] - Seguridad [Cifrado]”.
- 884.Android 6.x extiende las capacidades de cifrado a las unidades de almacenamiento externo, como tarjetas SD.
- 885.Se recomienda habilitar el cifrado completo del dispositivo móvil con el objetivo de evitar ataques de acceso a los datos almacenados en caso en el que un potencial atacante disponga de acceso físico al dispositivo móvil y desconozca la contraseña de acceso.

## 10.2. ALMACENAMIENTO ADOPTABLE

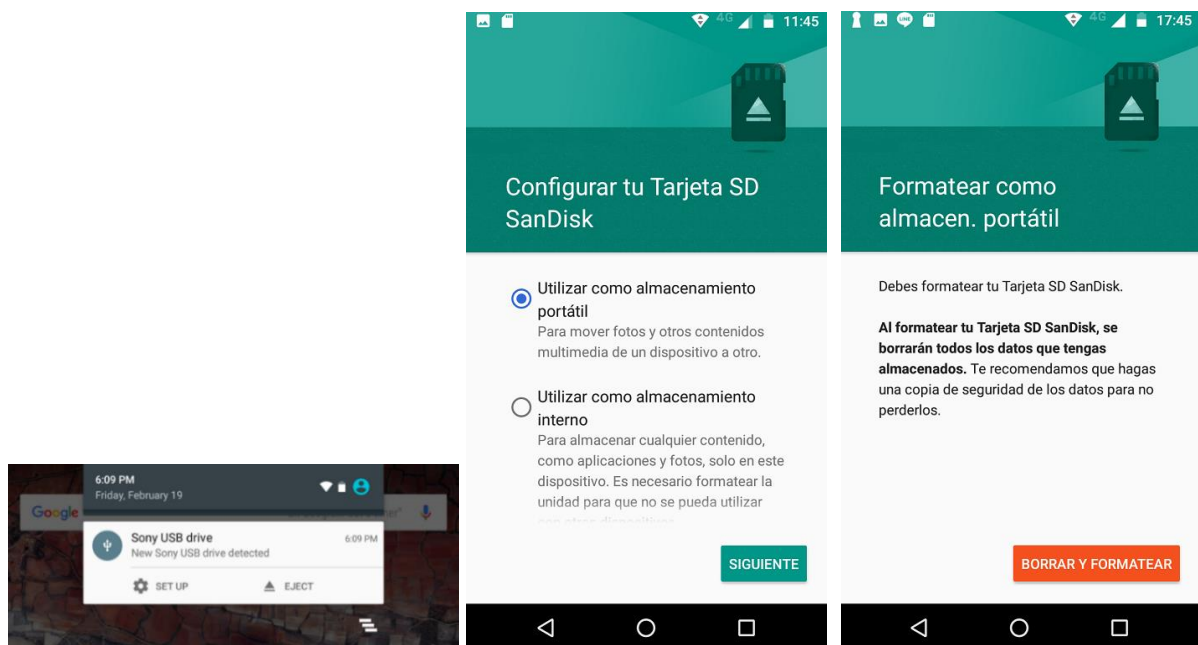
- 886.Android 6.x introduce el concepto de dispositivos de almacenamiento flexibles o adoptables [Ref.- 603], es decir, dispositivos de almacenamiento externos como, por ejemplo, tarjetas SD o discos USB, que el usuario puede incorporar al dispositivo móvil, ampliando así sus capacidades de almacenamiento totales.
- 887.Para la conexión de dispositivos USB, se requiere como interfaz físico un cable o un adaptador USB OTG (On-the-Go).
- 888.Un dispositivo de almacenamiento adoptable puede configurarse, bien como almacenamiento portátil (para datos que pueden accederse desde distintos dispositivos móviles como, por ejemplo, contenido multimedia), o como almacenamiento interno (como complemento al almacenamiento interno del dispositivo móvil, para almacenar aplicaciones y los datos privados de éstas).
- 889.Android 6.x es capaz de detectar una unidad de almacenamiento externa de forma automática, y lanzará una notificación para permitir al usuario su configuración.
- 890.Los dos tipos de configuración de un dispositivo externo son *portable* (portátil) o *internal* (interno). Los dispositivos de almacenamiento que se definan como internos se formatearán utilizando ext4 como sistema de archivos, mientras que los externos se formatearán con FAT32.
- 891.Los dispositivos OTG sólo pueden configurarse como almacenamiento portátil, salvo que se fuerce lo contrario mediante un comando ADB específico (detallado posteriormente).
- 892.El tipo de configuración de una tarjeta SD externa que ya ha sido definida en el dispositivo móvil puede cambiarse posteriormente a través de “Ajustes - [Dispositivo] Almacenamiento y USB”. Esta operación requerirá formatear de nuevo la tarjeta, por lo que los datos existentes se perderán.

### 10.2.1. ALMACENAMIENTO ADOPTABLE EXTERNO

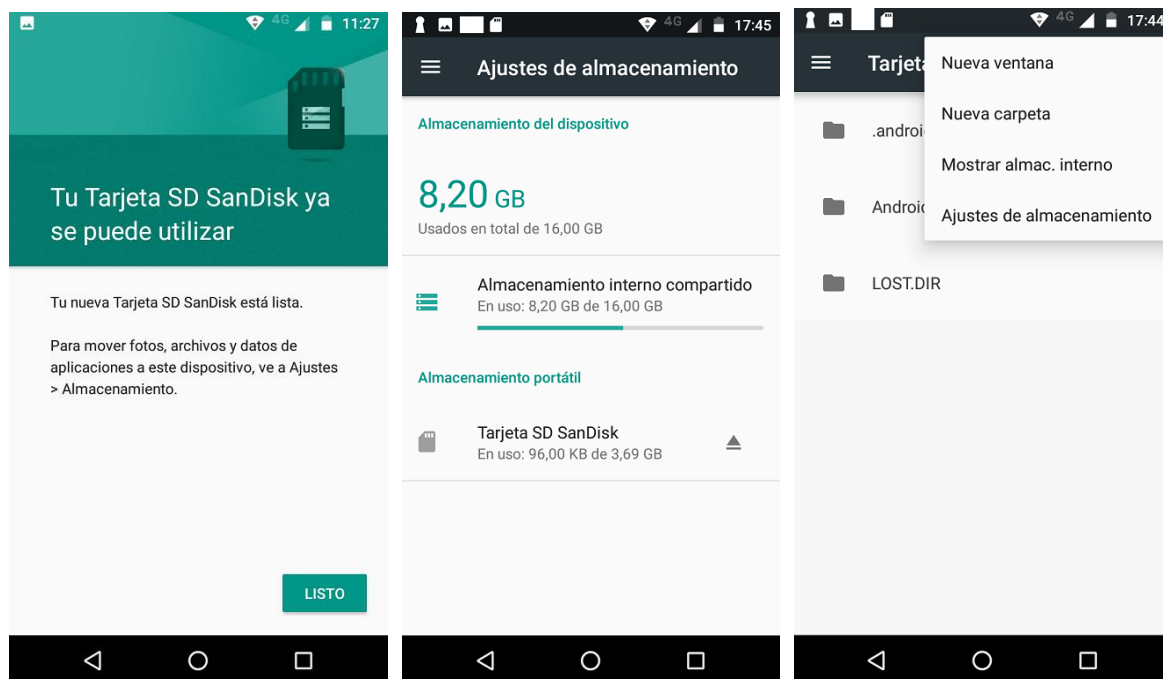
893. Dado que los dispositivos Nexus como el empleado en la presente guía no tienen ranura física para la inserción de una tarjeta SD externa, la configuración e imágenes que se detallan a continuación corresponden a la configuración de un terminal de otro fabricante, por lo que pueden no coincidir exactamente con las pantallas que se muestren en un terminal de otros fabricantes de dispositivos móviles Android.

894. El almacenamiento externo definido como portátil es uno de los mecanismos disponibles en Android para compartir datos y ficheros entre apps, almacenar contenidos multimedia por parte del usuario (como por ejemplo fotos y vídeos), y para compartir datos con un ordenador conectado por USB al dispositivo móvil.

895. Al insertar una tarjeta SD externa en un dispositivo móvil que presente una ranura física, se lanzará una notificación similar a la mostrada a continuación. Una vez se seleccione la notificación, se lanzará el menú que permite configurar la tarjeta SD (por defecto, la opción para usar la tarjeta como almacenamiento portátil estará seleccionada):



896. El formateo de una tarjeta SD externa que se va a usar como almacenamiento portátil en un dispositivo móvil que presente una ranura física se llevará a cabo usando FAT32, por lo que su contenido será accesible desde cualquier otro dispositivo que pueda montar un sistema de archivos FAT o VFAT.



897. Una vez configurada la tarjeta, es posible acceder a ella a través de “Ajustes - [Almacenamiento y USB] <Nombre de la tarjeta> - <...> - Ajustes de almacenamiento”, como se ilustra en las imágenes previas.

898. Adicionalmente, debe tenerse en cuenta que el sistema de ficheros (FAT o FAT32; VFAT) empleado por defecto en la tarjeta de almacenamiento externa configurada como portátil no establece permisos ni impone ninguna restricción, por lo que cualquier app con permisos de acceso sobre la tarjeta SD dispondrá de acceso a todos los datos almacenados en ella (de lectura o de escritura).

899. En los dispositivos móviles que no disponen de capacidades de almacenamiento externas reales, en forma de un *slot* o ranura para tarjetas SD removibles, sin embargo, también se dispone de almacenamiento externo desde el punto de vista de Android, entendiendo como tal un espacio de almacenamiento virtual o emulado en la memoria interna (y, por tanto no removable) que se asocia a una partición anclada al punto de montaje “/sdcard” (o “/storage”). Esta partición se trata como si fuera una tarjeta de almacenamiento externa, por lo que se puede acceder a ella desde un ordenador que se conecte por USB al dispositivo móvil. Aunque este área de almacenamiento se trata como si fuera almacenamiento externo, realmente reside en la memoria interna del dispositivo móvil. En él se almacenan, entre otros, las fotografías y capturas de pantalla.

900. Desde un equipo Windows, la referencia a “/sdcard” en el sistema de ficheros (que normalmente apunta a “/data/media/0” o a “/storage/sdcard0s”) se gestionará como una unidad de almacenamiento FAT32 al conectar el dispositivo móvil por USB a un ordenador, aunque en realidad la partición donde reside hace uso del sistema de ficheros ext4 (y se emplea FUSE para la conversión entre distintos sistemas de ficheros<sup>57</sup>).

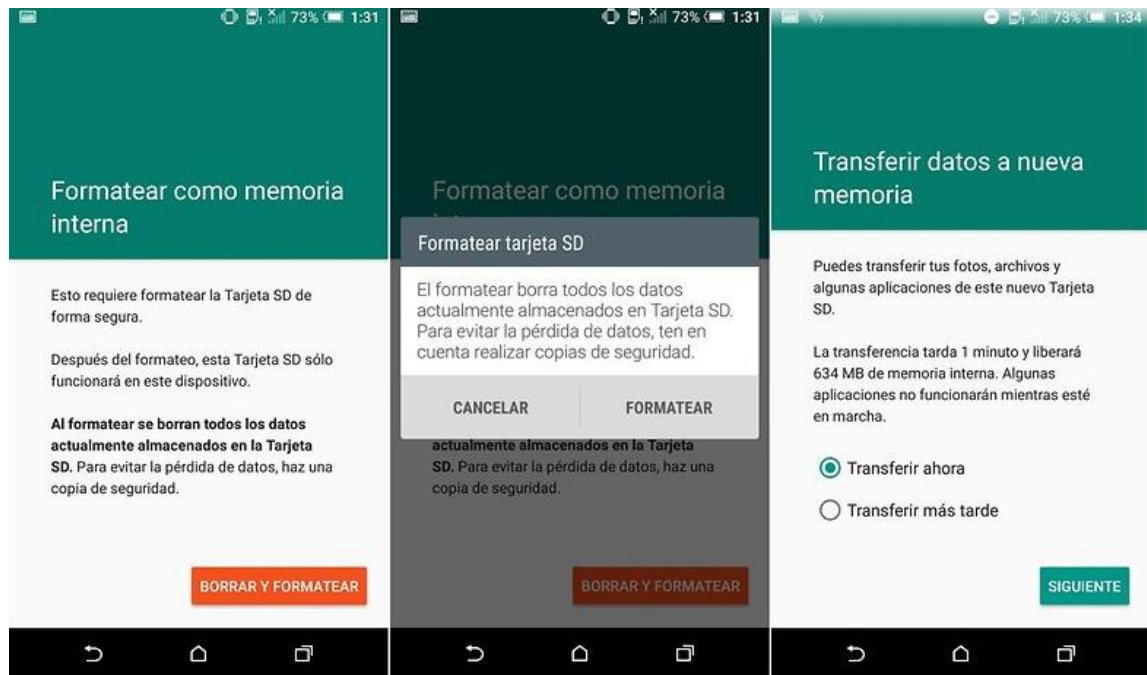
<sup>57</sup> <http://forum.xda-developers.com/google-nexus-5/general/info-storage-nexus-5-data-info-loss-t2534010>

### 10.2.2. ALMACENAMIENTO ADOPTABLE INTERNO

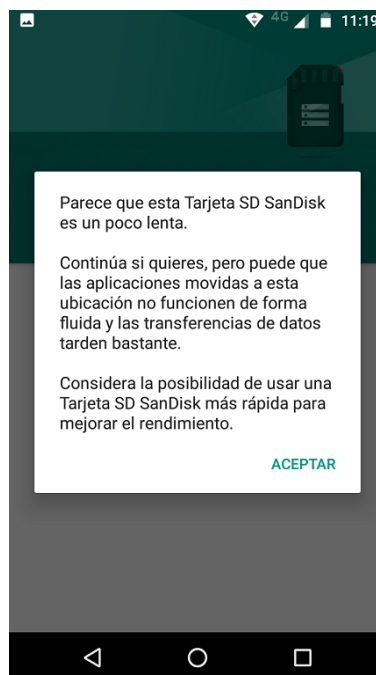
- 901.El almacenamiento adoptable (típicamente asociado a tarjetas SD que se insertan en una ranura física del dispositivo móvil) que se configure como interno tiene como misión expandir la memoria física del dispositivo, por lo que sobre él se podrán instalar aplicaciones y sus datos asociados.
- 902.Es importante reseñar que el almacenamiento adoptable configurado como “interno” no debería extraerse del dispositivo, ya que se monta como parte del sistema de ficheros ext4 cuando se arranca el terminal, y dará lugar a fallos si deja de estar accesible.
- 903.Si la memoria física del dispositivo está cifrada, el contenido de un dispositivo configurado como almacenamiento interno también lo estará. En este caso, el dispositivo externo se cifrará mediante una clave AES de 128 bits, la cual se almacena en la memoria interna del dispositivo móvil, lo que impide que pueda montarse en otro dispositivo distinto a menos que se extraiga la clave del dispositivo original.
- 904.Las apps que quieren leer o escribir en el almacenamiento adoptable interno deben solicitar los permisos “READ\_EXTERNAL\_STORAGE” y “WRITE\_EXTERNAL\_STORAGE” respectivamente<sup>58</sup>, siendo únicamente necesario el permiso de escritura para ambas tareas (ya que éste conlleva explícitamente el permiso de lectura).
- 905.Desde Android 4.4 estos permisos no son necesarios si la app sólo requiere disponer de acceso a ficheros privados de la propia app, mediante el uso de directorios privados a la app dentro del almacenamiento externo.
- 906.Desde Android 4.x se dispone (potencialmente) de capacidades para el cifrado de los datos que vayan a ser guardados en tarjetas de almacenamiento externas de forma nativa.
- 907.Con el objetivo de evitar el acceso a los datos almacenados en tarjetas externas por parte de un potencial atacante, se recomienda habilitar esta opción de cifrado.
- 908.Si, tras insertar una tarjeta SD en un dispositivo móvil, se opta por darla de alta como almacenamiento interno, el sistema Android solicitará su formateo (que implica el borrado de todos los datos que se encontrasen en la tarjeta) y preguntará al usuario si desea transferir datos al almacenamiento adoptado:

---

<sup>58</sup> <http://developer.android.com/guide/topics/data/data-storage.html#filesExternal>

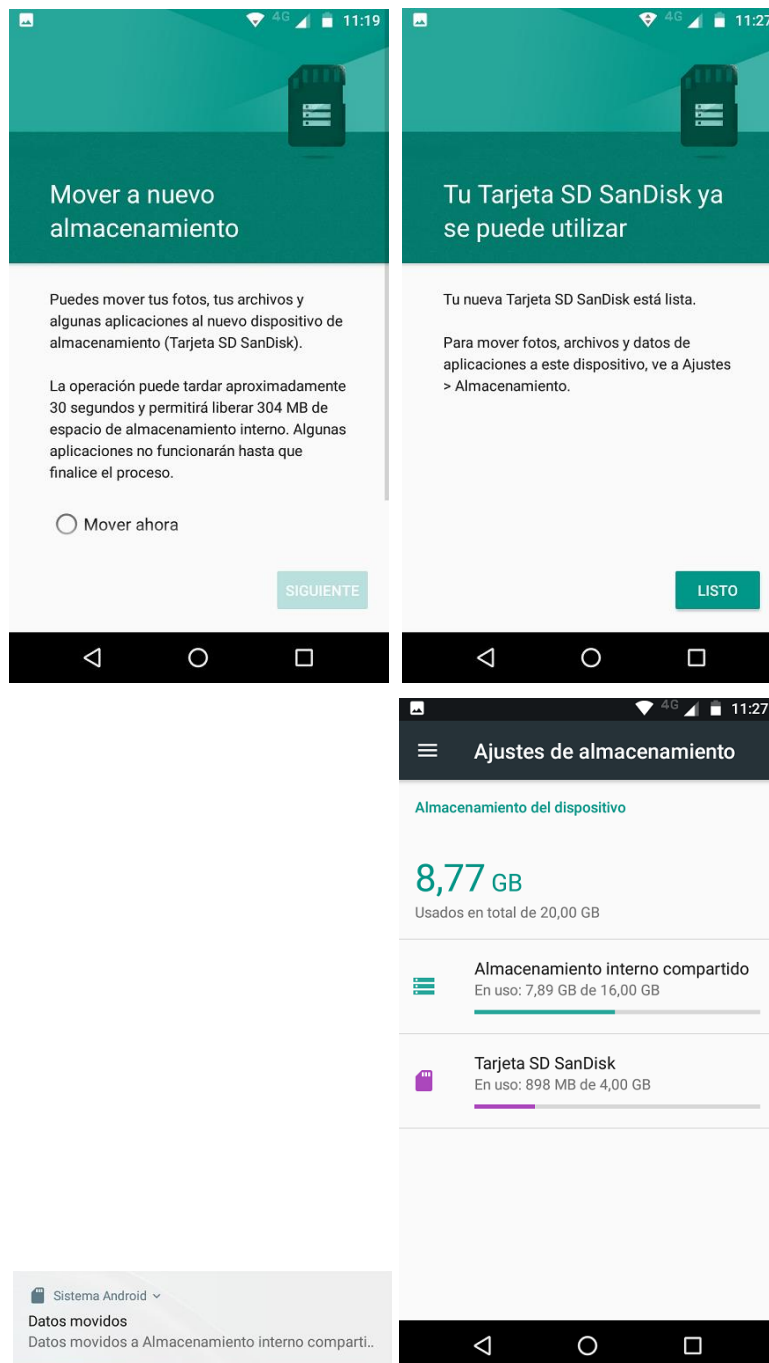


909.El sistema Android computará ciertas medidas de rendimiento y, si se detecta que la tarjeta es demasiado lenta, mostrará el siguiente aviso:





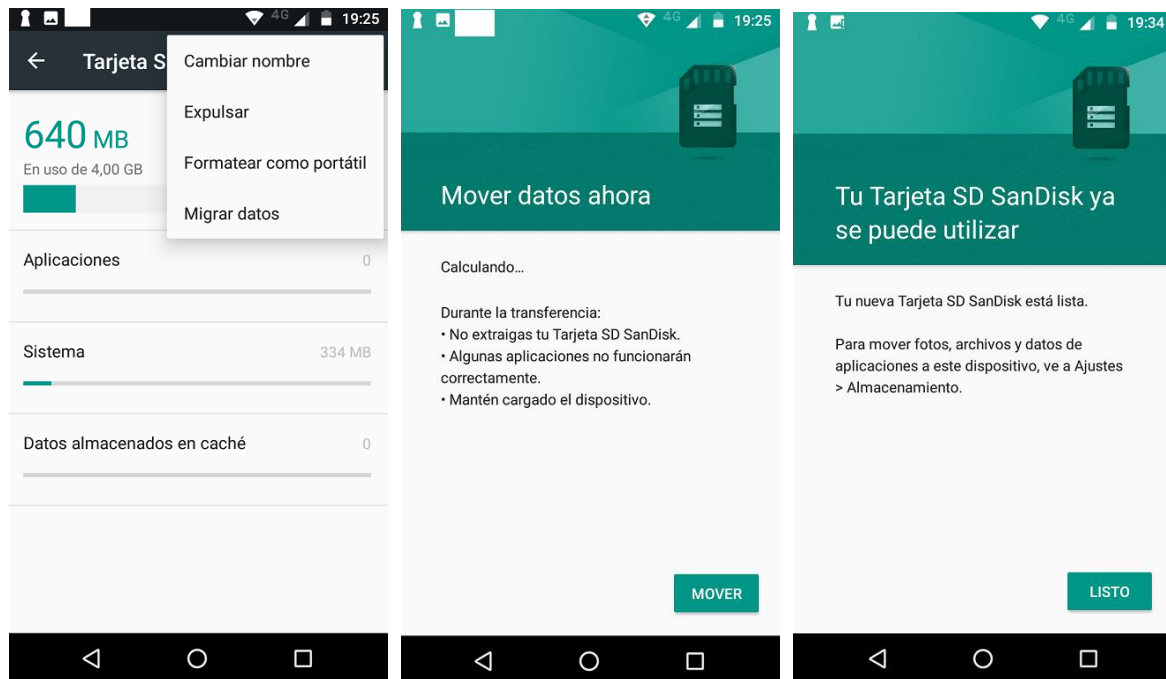
910. Si se opta por mover parte del contenido del almacenamiento interno del dispositivo móvil a la tarjeta adoptada, se mostrará la siguiente notificación, y la nueva tarjeta se mostrará en el menú de “Ajustes - [Dispositivo] Almacenamiento y USB”:



911. Al igual que ocurría en versiones previas de Android (desde Android 2.2 o nivel de API 8) [Ref.- 612], de nuevo, las apps pueden ser movidas por el usuario manualmente desde la memoria interna a la memoria externa (configurada como interna), y viceversa.

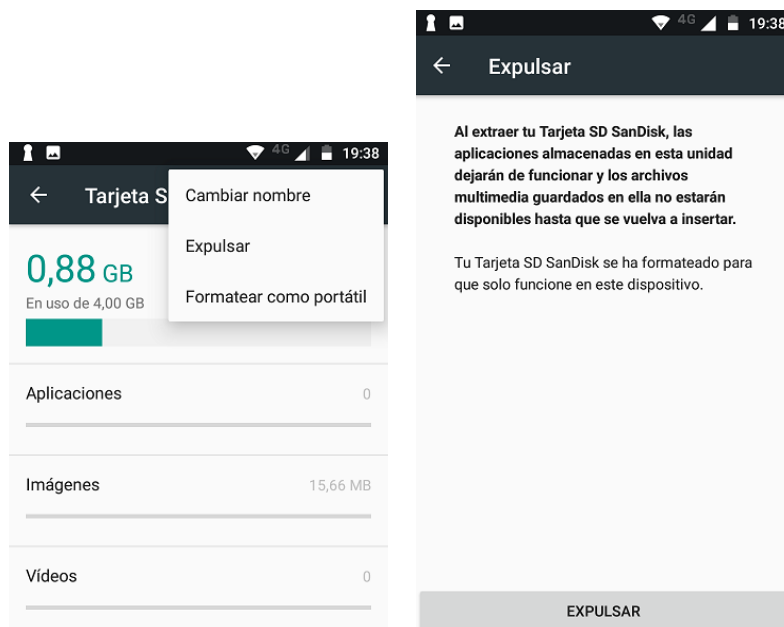
912. En el caso de Android 2.2 los ficheros binarios (DEX), los datos privados de la app, y las librerías nativas permanecen aún en el almacenamiento interno [Ref.- 613]. Por tanto, la principal diferencia es que en Android 6.x también los datos privados de la app pueden ser almacenados en el almacenamiento externo adoptado.
913. Asimismo, en Android 2.2 se empleaban contenedores cifrados individuales para cada app, haciendo uso de una clave aleatoria generada y asociada al dispositivo móvil, y por tanto, no permitiéndose el uso de la tarjeta SD en otro dispositivo.
914. En Android 6.x, sin embargo, se cifra el dispositivo de almacenamiento adoptado que se usa como almacenamiento interno al completo. El cifrado de la tarjeta SD (o de cualquier otro tipo de dispositivo de almacenamiento adoptable configurado como interno) no utiliza un cifrado basado en el TEE, a diferencia del cifrado del almacenamiento propio del dispositivo móvil. Por tanto, si la clave de cifrado se extrae del dispositivo móvil, los datos podrían accederse desde un equipo externo, existiendo la posibilidad de montarlo en un equipo o dispositivo diferente si se hace uso de la clave extraída asociada al almacenamiento adoptado [Ref.- 614].
915. La clave estática empleada para el cifrado de todo el volumen o partición de datos está disponible en el fichero `"/data/misc/vold/expand_<hash>.key"` (únicamente accesible por root). Esta clave corresponde a una clave de 128 bits empleada por dm-crypt al hacer uso del algoritmo AES 128 bits, `"aes-cbc-essiv:sha256"`, de manera similar a la implementación de FDE.
916. Android respetará la preferencia de la app establecida en su fichero *manifest*<sup>59</sup> para su instalación, respecto a la localización en las unidades de almacenamiento, no pudiendo instalarla en el almacenamiento externo si la app indica que sólo quiere ser instalada en el interno (`"internalOnly"`).
917. En Android 6.x, conviene recordar que los dispositivos de almacenamiento externos que se configuren como portátiles no se cifran. Por tanto, desde el punto de vista de seguridad, no se recomienda almacenar en ellos ningún contenido sensible.
918. Se ha de tener cautela a la hora de extraer una tarjeta adoptable configurada como almacenamiento interno, ya que, si se extrae sin haberla desmontado correctamente, algunas aplicaciones dejarán de funcionar, e incluso se puede corromper la memoria interna del dispositivo móvil.
919. Si se desea eliminar del terminal un dispositivo adoptable configurado como almacenamiento interno, se debe asegurar que los datos residentes en él se migran al almacenamiento interno del terminal mediante `"Ajustes - [Dispositivo] Almacenamiento - <seleccionar el dispositivo adoptable> - <...> - Migrar datos"`:

<sup>59</sup> <https://developer.android.com/guide/topics/manifest/manifest-element.html#install>

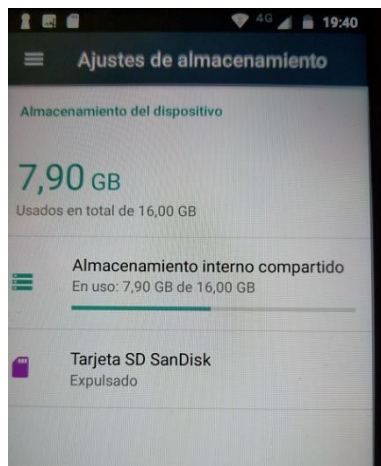


920. Si, durante esa operación, alguna aplicación que acceda al dispositivo adoptable trata de acceder a él, fallará (como en caso de tomar una captura de pantalla) y el sistema mostrará una notificación informativa.

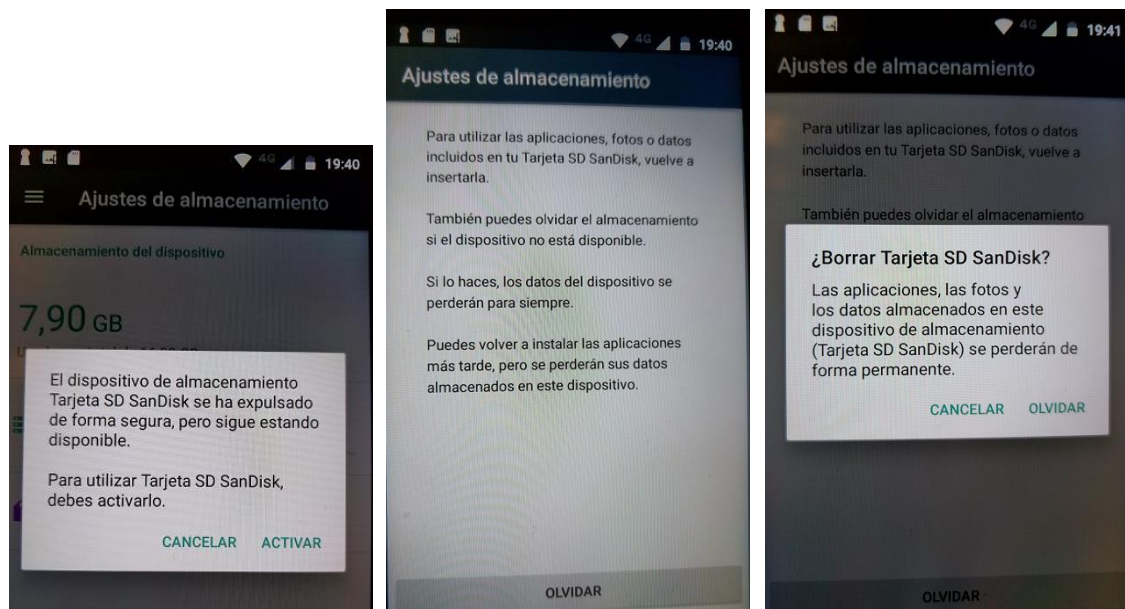
921. Una vez migrados los datos al almacenamiento interno del dispositivo móvil, se podrá expulsar la tarjeta SD mediante “Ajustes - [Dispositivo] Almacenamiento - <seleccionar el dispositivo adoptable> - <...> - Expulsar”:



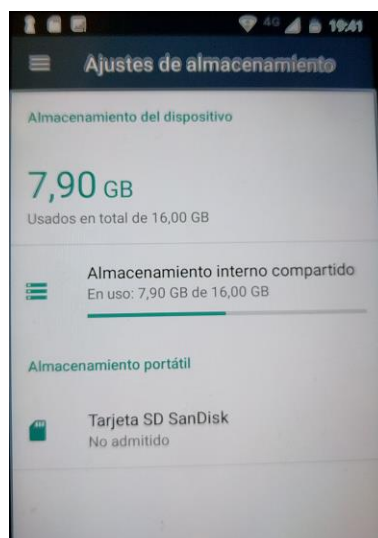
922. Pese a que se expulse correctamente, el sistema Android podrá seguir mostrando errores y solicitar que se vuelva a insertar el dispositivo externo:



923. Para resolver el problema, se debe abrir la notificación “Falta tarjeta SD <nombre>” y seleccionar el botón “Cancelar”, lo cual despliega una ventana que permite “Olvidar” el dispositivo y confirmar la acción:



924. Tras completarse esta acción, la tarjeta será vista dentro del apartado “Almacenamiento portátil” como “No admitido”:



925. Teniendo en cuenta todas las consideraciones anteriores, se recomienda utilizar con cautela el almacenamiento adoptable interno, pues puede dar lugar a una corrupción del sistema de ficheros que solo se podría resolver restableciendo el terminal a fábrica.

### 10.3. DISPOSITIVOS DE ALMACENAMIENTO OTG (ON-THE-GO)

926. Numerosos dispositivos móviles comercializados con Android no disponen de ranura física que permita la inserción de una tarjeta SD que pueda ser empleada como almacenamiento complementario al del dispositivo, como por ejemplo el dispositivo Nexus empleado en la elaboración de la presente guía.

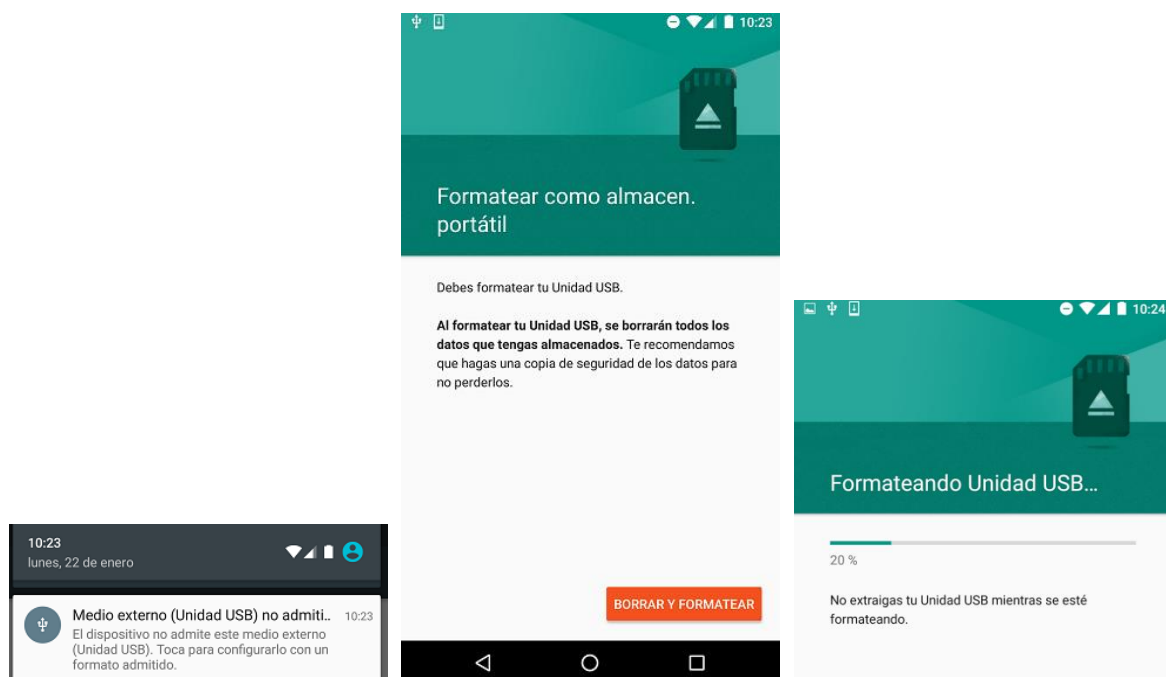
927. USB OTG (On-the-Go) es una norma que extiende el protocolo USB 2.0 para invertir el papel del puerto USB, de forma que el dispositivo móvil pase de tener rol de esclavo al rol de *host* en la conexión. Ello permite que el dispositivo móvil pueda acceder como maestro a otros dispositivos, como un disco USB, un *pendrive*, etc.

928. Por defecto, los dispositivos conectados a través de USB OTG no pueden ser configurados como almacenamiento interno. Si se desea utilizarlos de este modo, se necesita ejecutar el siguiente comando mediante ADB [Ref.- 614]:

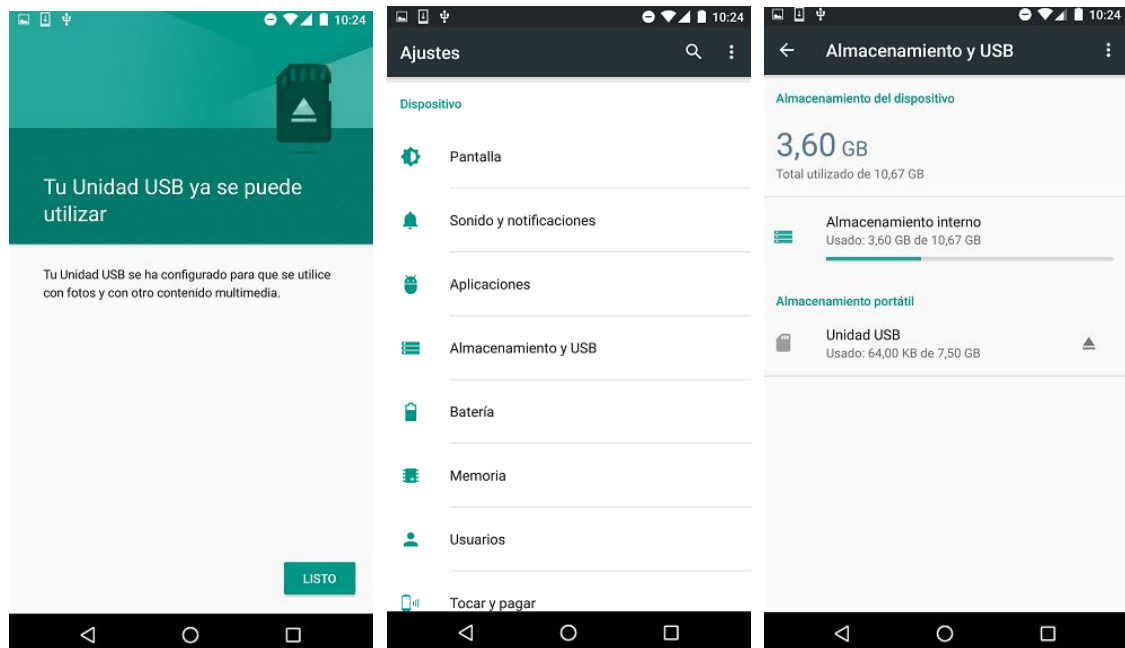
```
C:\> adb shell sm set-force-adoptable true
```

929. No obstante, el uso de dispositivos OTG como almacenamiento interno no es práctico ni recomendable, ya que una expulsión fortuita del dispositivo provocaría un fallo del sistema y, potencialmente, la corrupción del sistema de ficheros que forma parte de la memoria interna. Se recomienda pues utilizar los dispositivos OTG como almacenamiento portátil.

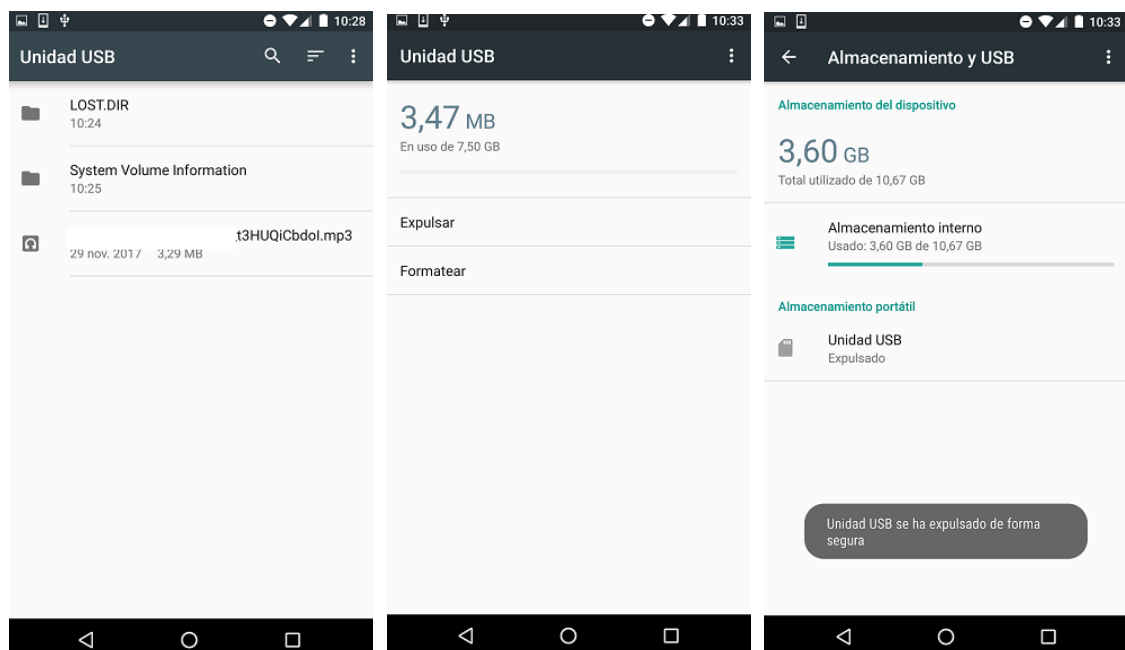
930. Para configurar un dispositivo OTG como almacenamiento portátil, Android 6.x no requiere habilitar ninguna opción oculta. Al conectar un dispositivo OTG al terminal móvil, se mostrará una notificación que permite iniciar su configuración:



931. Una vez concluya el formateo, la unidad estará accesible desde “Ajustes - Almacenamiento y USB”:



932. El botón situado a la derecha del nombre del almacenamiento portátil (“Unidad USB” en el ejemplo) permite expulsar el dispositivo externo de forma segura. Si se pulsa sobre el nombre del dispositivo externo, se abrirá un explorador que permitirá ver sus contenidos, junto al menú “...” que da acceso a su formateo y a su expulsión:



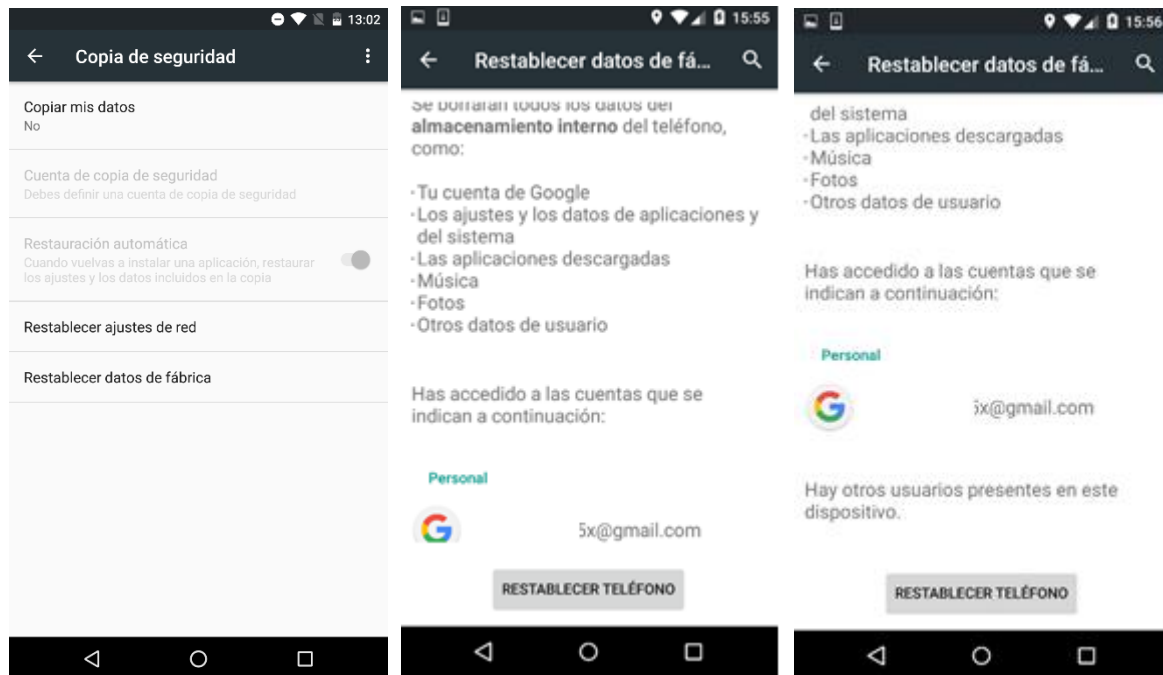
933. En Android 6.x no existe ninguna opción para cifrar el contenido de un dispositivo de almacenamiento portátil, por lo que, desde el punto de vista de seguridad, no se recomienda utilizarlos para guardar información potencialmente sensible, sino únicamente contenidos que puedan llevarse a cualquier otro dispositivo sin comprometer la privacidad ni la seguridad de su propietario.



## 10.4. ELIMINACIÓN DE DATOS DEL DISPOSITIVO MÓVIL

934.El objetivo de las capacidades de cifrado de Android es evitar que un tercero sin autorización disponga de acceso a los datos almacenados en el dispositivo móvil. Estas capacidades pueden ser complementadas con la funcionalidad que permite, tanto de forma local como remota, eliminar los datos del usuario del dispositivo móvil.

935.Android 6.x proporciona capacidades locales para la eliminación de todos los datos almacenados en el dispositivo móvil a través del menú “Ajustes [Personal] - Copia de seguridad” y la opción “Restablecer datos de fábrica”. Antes de poder lanzar la operación, el dispositivo móvil solicitará el código de acceso:



936.El proceso de restablecimiento eliminará todos los datos del teléfono, incluyendo cuentas de Google, configuración y datos de apps y del sistema, así como apps de terceros previamente descargadas e instaladas. No se eliminará el software del sistema operativo ni las actualizaciones de sistema ya aplicadas, es decir, el propio Android, ni los datos de las tarjetas de almacenamiento externas. También se eliminarán datos de otros usuarios si se han empleado las capacidades multi-usuario descritas en el apartado “9.19. Múltiples perfiles de usuario”.

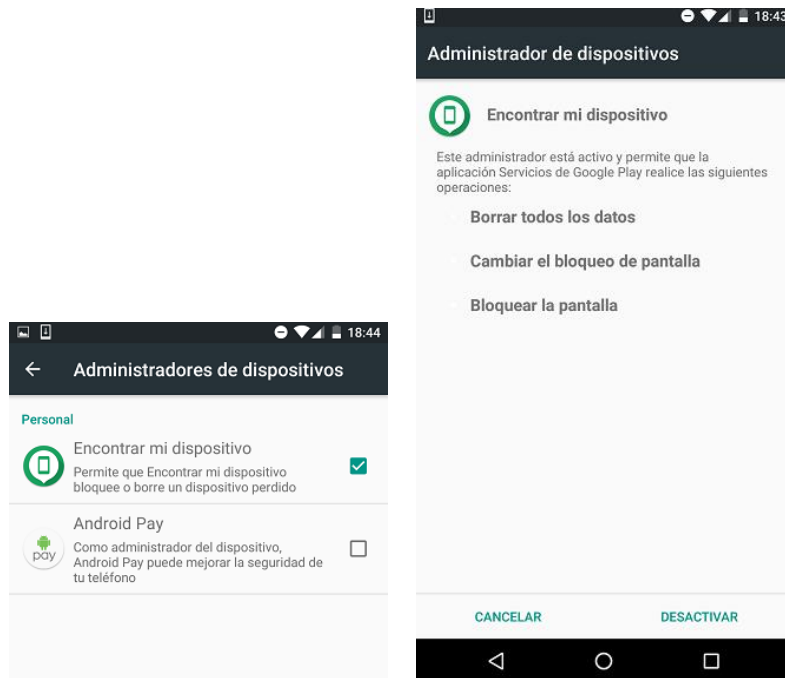
937.Para confirmar esta operación crítica es necesario introducir el código de acceso tras seleccionar el botón “Restablecer teléfono” de la pantalla que informa de que se borrarán todos los datos. Si existen otros usuarios en el dispositivo móvil, también se informará de este hecho por si se desea informarles antes de proceder al borrado de los datos.

938.Estas capacidades de borrado de datos local también pueden ser activadas tras llevarse a cabo un número determinado de intentos de acceso incorrectos, pudiendo configurarse a través de las políticas de seguridad de los mecanismos de gestión empresarial de dispositivos móviles Android (ver apartado “8. Gestión empresarial de dispositivos móviles basados en Android”).

939.Las aplicaciones administradoras del dispositivo móvil pueden ser activadas o desactivadas en función de las necesidades del usuario. Antes de su ejecución, siempre

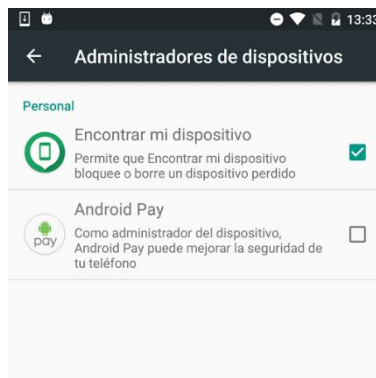


verificarán si están activadas, y en caso de no estarlo, solicitarán al usuario su activación. Para verificar el estado de dichas aplicaciones, se puede acceder al menú “Ajustes - [Personal] Seguridad - [Administración de dispositivos] Administradores de dispositivos”:



940. Además de mediante las capacidades de gestión empresarial de dispositivos móviles, el propietario de un dispositivo que lo haya asociado a su cuenta de Google puede efectuar labores de gestión remota (incluyendo el borrado de datos del dispositivo) siguiendo las indicaciones descritas en el apartado “8.1. Gestión remota de dispositivos Android por parte del usuario”.

941. En Android 6.x, se incorpora “Android Pay” como un administrador de dispositivos. El objeto es permitir que los datos almacenados como medio de pago en Android Pay puedan ser borrados de forma remota en caso de pérdida o robo del dispositivo móvil, protegiendo así al usuario:



## 11. GESTIÓN DE CERTIFICADOS DIGITALES Y CREDENCIALES

### 11.1. ANDROID KEYSTORE SYSTEM: ALMACENAMIENTO DE CREDENCIALES

942. Desde Android 1.6, Android dispuso de un almacén de credenciales a nivel de sistema. Este almacén sólo se usaba inicialmente para almacenar claves privadas y certificados Wi-Fi y VPN, y no existía ninguna API pública para acceder a él<sup>60</sup>.
943. Android 4.0 integró el almacén de credenciales en el sistema operativo, e introdujo una API pública que se denominó “KeyChain” que proporcionaba acceso a claves privadas y certificados gestionados por el sistema operativo. Pero esta API no proporcionaba mecanismos de gestión para las apps que requiriesen almacenar material criptográfico (claves, tokens, certificados, etc.).
944. El acceso al almacén de credenciales se realizaba a través del demonio *keystore*, que cifraba las claves mediante una clave maestra AES 128 bits. Esta clave maestra se derivaba del mecanismo de control de acceso configurado en el dispositivo (contraseña o PIN).
945. Cada clave se almacenaba como un fichero residente en el directorio “/data/misc/keystore/”. Las apps podían acceder a sus claves, pero no a las de otras apps (lo cual se garantizaba porque la clave se ligaba al UID del proceso que la creó).
946. Al no estar la clave maestra ligada al dispositivo móvil, los ataques de fuerza bruta sobre los ficheros de claves llevados a otros dispositivos eran posibles.
947. Con la versión 4.3 de Android, el sistema de almacenamiento de credenciales (entendiendo como tal certificados digitales y, en todo caso, el par de claves pública y privada asociadas a los certificados digitales propios) pasó a denominarse oficialmente “Android Key Store” [Ref.- 144], y, para su acceso, se publicó un interfaz, librería o API que permitía a las apps almacenar certificados digitales, incluso independientes por usuario (en dispositivos Android multi-usuario). Esta API asociada al HAL (Hardware Abstraction Layer) proporcionaba capacidades para firma digital, además de generación e importación de claves asimétricas, y permitía determinar si el almacenamiento de credenciales era *hardware-backed* o solo mediante software, según el fabricante y modelo del dispositivo móvil.
948. Oficialmente, este repositorio no proporcionaba funciones para el almacenamiento de contraseñas, u otras credenciales y secretos por parte de las apps<sup>61</sup>, o de claves simétricas hasta Android 6.x (y versiones posteriores)<sup>62</sup>.
949. Con Android 6.x (Marshmallow), se produjo una evolución importante del denominado “Android Key Store”, que se convirtió en el “*Android Keystore System*” (en adelante, AKS), que es el subsistema que gestiona el material criptográfico del dispositivo móvil, tanto a nivel de sistema como de aplicaciones.
950. El AKS permite almacenar material criptográfico en un contenedor o almacén de credenciales denominado a su vez *keystore*, protegido por mecanismos de cifrado. En el *keystore* se almacenan, por ejemplo, los certificados digitales asociados a redes VPN y

<sup>60</sup> <https://nelenkov.blogspot.com.es/2012/05/storing-application-secrets-in-androids.html>

<sup>61</sup> <https://github.com/nelenkov/android-keystore>

<sup>62</sup> <https://source.android.com/security/keystore/>

redes Wi-Fi (ver los apartados correspondientes en la presente guía), o los empleados desde el navegador web, el cliente de correo electrónico y otras apps. También permite almacenar claves secretas (mediante cifrado simétrico).

951.El AKS puede accederse por:

- La API KeyChain [Ref.- 250], para el acceso a credenciales a nivel de sistema (el interfaz de usuario de sistema determina qué apps pueden acceder a qué credenciales).
- El Android Keystore Provider (introducido con Android 4.3, API nivel 18), que se registra como un keystore para almacenar credenciales propias de una app que sólo son accesibles por ella misma [Ref.- 630].

952.Android 6.x extendió sus APIs para proporcionar nuevas capacidades al keystore, como AES y HMAC, y un sistema de control de acceso para claves gestionadas por un dispositivo criptográfico de tipo hardware [Ref.- 621]. Los controles de acceso se definen durante la generación de la clave y mientras ésta sea válida. Por ejemplo, se puede restringir el acceso a la clave solo cuando el usuario se haya autenticado, durante un cierto periodo de tiempo tras la autenticación, o bajo ciertas condiciones como, por ejemplo, el uso de dispositivos asociados a un sensor corporal<sup>63</sup>.

953.Adicionalmente, Android 6.x incorpora parámetros en la generación e importación de claves, los cuales se almacenan junto a las mismas como etiquetas, como son el uso válido o permitido para la clave (cifrado/descifrado o firma/verificación), el modo de cifrado en bloques, o el *padding* [Ref.- 629]. Estas propiedades de las claves son válidas tanto para claves simétricas como asimétricas.

954.Además, el AKS está diseñado de forma que las claves no puedan ser extraídas del dispositivo móvil, ni siquiera por las apps que las utilizan. Para ello, se restringe el material criptográfico a través de dos medidas de seguridad [Ref.- 630]:

- Las operaciones criptográficas que pueda requerir una app se llevan a cabo por un proceso de sistema, es decir, el material criptográfico se mantiene fuera del sandbox de las apps, y nunca se accede directamente por parte de sus procesos.
- El material criptográfico puede residir en un hardware específico si el dispositivo lo incorpora (por ejemplo, el TEE o *Trusted Execution Environment*), con lo cual un potencial atacante no podría extraerlo de él y realizar ataques *off-device*.

955.Las opciones existentes oficialmente para el almacenamiento de otros datos, secretos y contraseñas (aunque desaconsejado) por parte de las apps pasan por hacer uso de las preferencias compartidas (*SharedPreferences*) de la app, o del *AccountManager*<sup>64</sup> (gestor de cuentas), siempre debiendo ser muy cuidadosos los desarrolladores de apps de Android a la hora de almacenar información sensible en el *sandbox* de la app<sup>65</sup>.

956.En Android 6.x la Keystore dispone del Gatekeeper [Ref.- 631], un subsistema encargado de la gestión y verificación de los códigos de acceso y de tokens de autorización en el TEE. Cuando el usuario introduce una clave, el subsistema Gatekeeper recurre a la clave secreta derivada del TEE y firma una declaración de autenticación para permitir a una

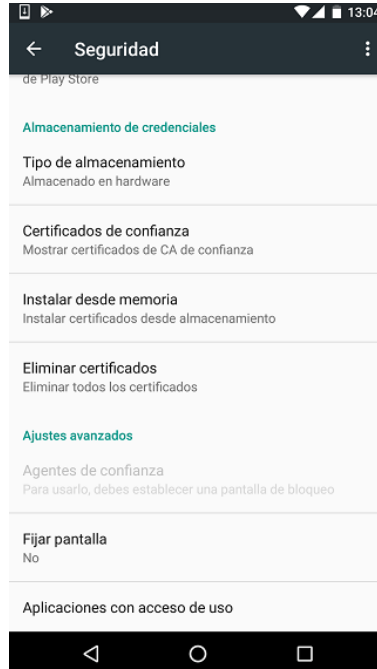
<sup>63</sup> <https://source.android.com/security/keystore/tags>

<sup>64</sup> <http://developer.android.com/reference/android/accounts/AccountManager.html>

<sup>65</sup> <http://android-developers.blogspot.com.es/2013/02/using-cryptography-to-store-credentials.html>

app acceder a las claves que ha almacenado. A nivel de sistema, existe un demonio “*gatekeeperd*” que ejecuta como proceso independiente y que proporciona a las APIs de Android acceso al HAL y al Keystore.

957. A nivel de usuario, la sección “Almacenamiento de Credenciales” está disponible desde el menú “Ajustes - [Personal] Seguridad”, en la parte inferior:



958. La opción “Tipo de almacenamiento” indica los detalles de implementación del repositorio de credenciales. En el caso del dispositivo móvil bajo estudio, las credenciales se almacenan en un almacén seguro implementado en el hardware del dispositivo: “Almacenado en hardware”<sup>66</sup>.

959. Si la implementación del almacén es de tipo hardware, las claves son generadas y almacenadas en dicho almacén seguro, independiente del sistema operativo Android, y no deberían estar accesibles directamente, ni siquiera para el usuario “root”.

960. La implementación del almacén seguro mediante hardware, por ejemplo en algunos dispositivos móviles Nexus basados en los SoC (System on a Chip) Qualcomm, emplea las capacidades TrustedZone de los procesadores ARM, y en concreto, el Qualcomm Secure Execution Environment (QSEE) [Ref.- 191] [Ref.- 144][Ref.- 145]. Otras implementaciones son posibles haciendo uso de Secure Elements (SEs), Trusted Platform Modules (TPMs) o Universal Integrated Circuit Cards (UICCs; por ejemplo, una tarjeta SIM).

961. Si la implementación del almacén es de tipo software, las claves son cifradas mediante AES [Ref.- 189] con una clave maestra para cada usuario, y almacenadas bajo “/data/misc/keystore/user\_N/” (donde por defecto “N” es igual a “0” para el usuario inicial o propietario del dispositivo móvil, es decir, “.../user\_0/”). En el siguiente ejemplo el nombre de los ficheros corresponde al nombre asignado al certificado, “raul (DinoSec)”:

<sup>66</sup> Es necesario analizar en detalle los componentes hardware del modelo de dispositivo móvil concreto para conocer las capacidades de almacenamiento seguro de credenciales disponibles a través de la Keystore.

```

root@mobile:/data/misc/keystore/user_0 # ls -l
-rw----- keystore keystore 1300 2015-01-19 12:07
1000_CACERT_raul+P+XDinoSec+Y
-rw----- keystore keystore 1412 2015-01-19 12:07
1000_USRCERT_raul+P+XDinoSec+Y
-rw----- keystore keystore 1652 2015-01-19 12:07
1000_USRPKEY_raul+P+XDinoSec+Y

```

**Nota:** El dispositivo móvil utilizado en la elaboración de la presente guía no permite almacenamiento de credenciales por software, por lo que no es posible detallar la estructura de ficheros asociados a las claves. La estructura final puede depender de la implementación del almacén de credenciales que realice cada fabricante.

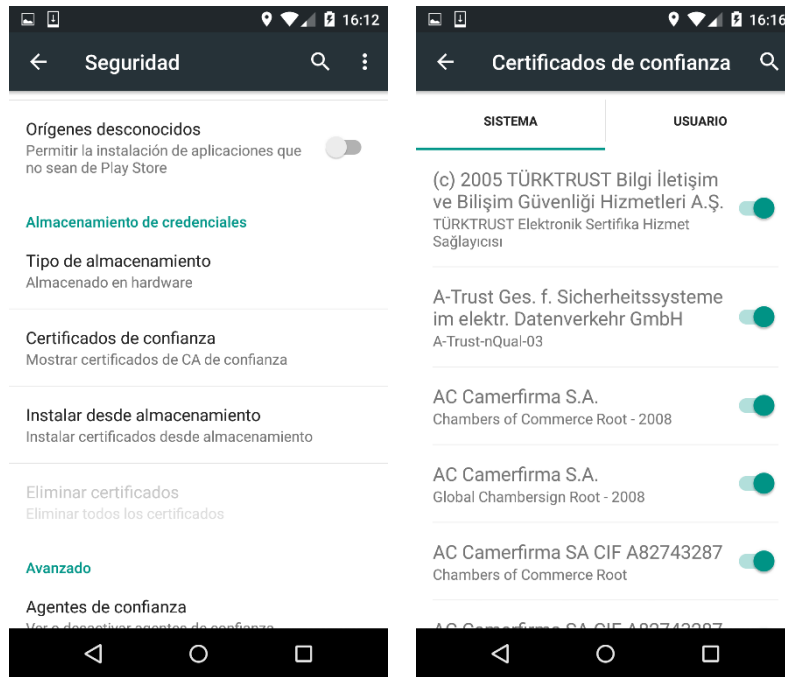
## 11.2. CERTIFICADOS DIGITALES DE SISTEMA Y DE USUARIO

962. Un certificado digital es un mecanismo electrónico que acredita la identidad de su titular ante cualquier otra entidad que lo solicite. Para ello, el certificado digital debe venir firmado electrónicamente por una autoridad certificadora (CA), la cual emite el par de claves pública y privada asociadas al certificado.

963. Un certificado digital puede ser de usuario o de sistema. En Android, los certificados de sistema corresponden a la lista de autoridades certificadoras (CAs) raíz reconocidas por defecto en esa versión concreta de Android. Los certificados de usuario corresponden a los certificados digitales tanto de CAs como personales que han sido añadidos posteriormente por el usuario.

964. Los certificados digitales se almacenan en el repositorio de credenciales.

965. Los de sistema pueden ser visualizados a través del menú “Ajustes - [Personal] Seguridad - [Almacenamiento de Credenciales] - Certificados de confianza”, así como al seleccionar, a través del menú correspondiente de las aplicaciones que hacen uso de él (por ejemplo, la configuración de redes VPN (ver apartado “19.6. Redes VPN”) o de redes Wi-Fi basadas en 802.1x EAP (ver apartado “16.3. Recomendaciones de seguridad para la conexión a redes Wi-Fi”), el certificado concreto.



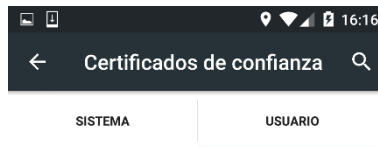
966. Los de usuario sólo se pueden visualizar a través de los menús de las apps que hacen uso de ellos (por ejemplo, la configuración de redes VPN (ver apartado “19.6. Redes VPN”) o de redes Wi-Fi basadas en 802.1x EAP (ver apartado “16.3. Recomendaciones de seguridad para la conexión a redes Wi-Fi”).

967. En las versiones 2.x de Android, por defecto, no era posible acceder al listado de CAs reconocidas por el dispositivo móvil desde el interfaz gráfico de usuario, y mucho menos disponer de opciones en el interfaz de usuario que permitieran modificar y gestionar la lista de CAs raíz.

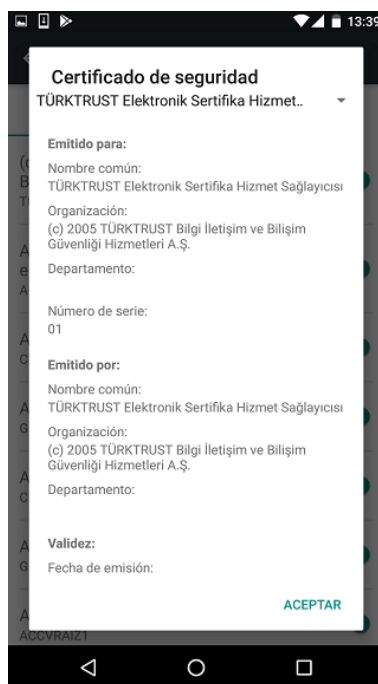
968. Sin embargo, desde la versión 4.0 de Android sí es posible acceder al repositorio de certificados de confianza, tanto de usuario como de sistema, desde la sección “Almacenamiento de Credenciales”, disponible a través del menú “Ajustes [Personal] - Seguridad [Almacenamiento de Credenciales]”, y en concreto, mediante la opción “Certificados de confianza”.

969. Este repositorio de certificados de confianza también se conoce como el “Trust Store” [Ref.- 189] y es un elemento clave para la seguridad de Android.

970. Esta sección dispone de dos pestañas, la primera de ellas asociada al “Sistema”, es decir, a la lista de autoridades certificadoras (CAs) raíz reconocidas por defecto en esa versión concreta de Android, y la segunda asociada al “Usuario” (vacía inicialmente hasta que el usuario añada manualmente algún certificado de CA)

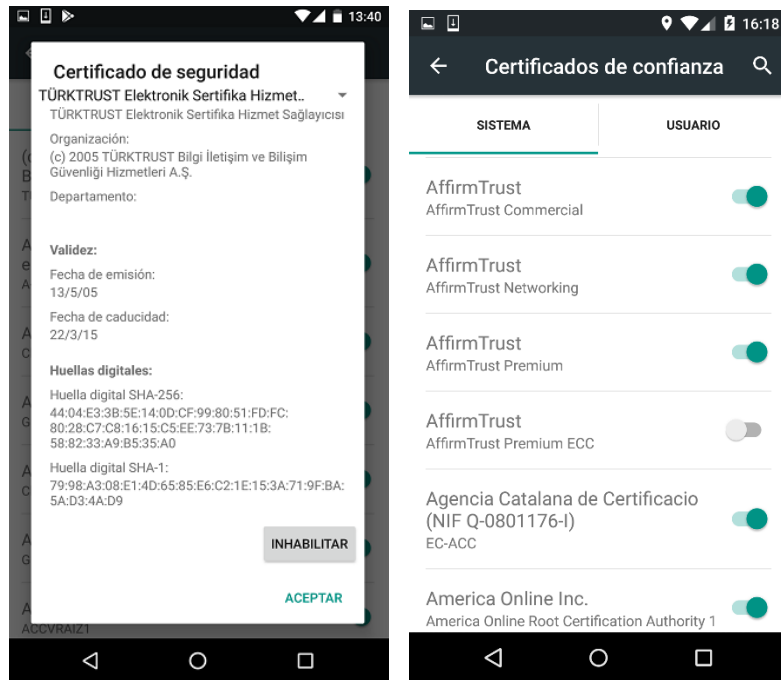


971. Desde la pestaña “Sistema” es posible visualizar la lista completa de CAs de confianza existente por defecto, pudiendo ver todos los detalles de sus certificados digitales al seleccionar cualquiera de las CAs de la lista, así como desactivar de forma independiente cada uno de los certificados raíz de cada CA contenidos en este repositorio:



972. Las CAs pueden ser deshabilitadas empleando el botón “Inhabilitar” situado en la parte inferior de la pantalla que muestra los detalles del certificado:

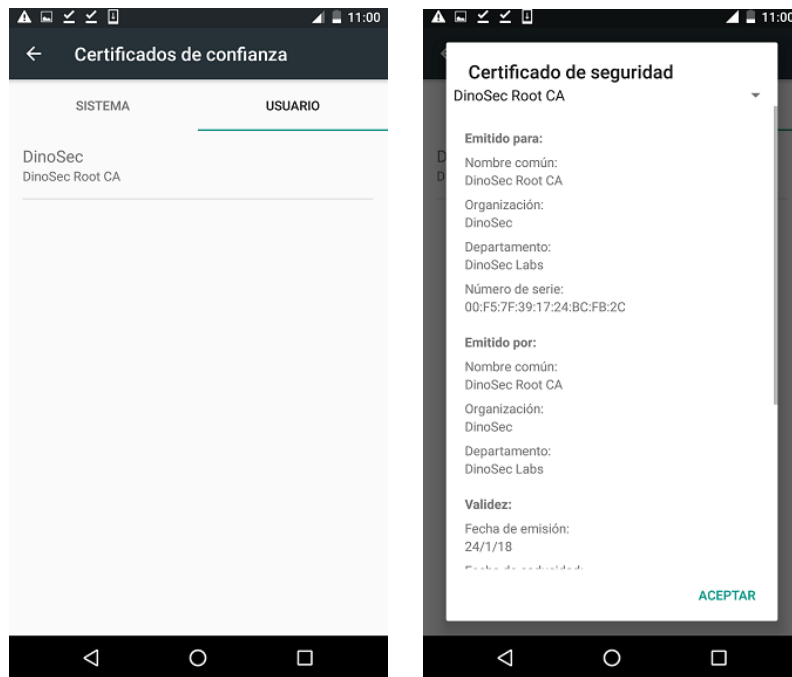




973. En cualquier momento una CA deshabilitada previamente puede volver a ser habilitada, de nuevo empleando el botón “Habilitar” situado en la parte inferior de la pantalla que muestra los detalles del certificado:



974. La pestaña “Usuario” no contiene ningún certificado digital hasta que no se importe manualmente un certificado de CA. Una vez se importa un certificado de CA (ver apartado “11.3. Gestión de certificados digitales”), los detalles del mismo están disponibles a través de esta pantalla. Contrariamente a lo que cabría esperar, la pestaña “Usuario” sólo mostrará los certificados digitales de CAs añadidas por el usuario, pero no los certificados personales (ni de servidor ni de usuario final):



975. Mediante el SDK (Software Development Kit) de Android es posible inspeccionar y extraer manualmente desde un ordenador, a través del puerto USB, el conjunto de certificados raíz asociado a las autoridades certificadoras (CAs) existentes por defecto en el dispositivo móvil, accediendo a través de ADB (*Android Debug Bridge*).

976. La modificación de los certificados digitales de las CAs reconocidas por defecto requiere disponer de un dispositivo móvil Android *rooteado*, por lo que en su lugar se recomienda hacer uso del interfaz de usuario disponible para estas gestiones desde Android 4.x (descrito previamente).

977. El directorio “/system/etc/security/cacerts” contiene un fichero por cada uno de los certificados digitales asociados a las CAs reconocidas por Android, en lugar de estar todos ellos contenidos en un único fichero contenedor “cacerts.bks” (BKS, BouncyCastle Key Store [Ref.- 27]), dentro del mismo directorio, tal como ocurría en versiones de Android previas a la versión 4.x:

```
shell@mobile:/system/etc/security $ ls -l
drwxr-xr-x root root 1970-07-29 02:16 cacerts
-rw-r--r-- root root 1931 2014-11-07 01:30 mac_permissions.xml
-rw-r--r-- root root 1433 c1970-07-29 02:33 otacerts.zip
shell@mobile:/system/etc/security $ cd cacerts
shell@mobile:/system/etc/security/cacerts $ ls -l
...
-rw-r--r-- root root 5940 2014-11-07 01:30 fb126c6d.0
-rw-r--r-- root root 4692 2014-11-07 01:30 fde84897.0
-rw-r--r-- root root 5136 2014-11-07 01:30 ff783690.0...
```

978. El nombre de cada fichero corresponde al *hash* del certificado digital que contiene [Ref.- 43], y mediante herramientas estándar, como por ejemplo “openssl”, es posible añadir nuevos certificados (en dispositivos móviles Android *rooteados*).

979. Para poder inspeccionar el contenido de cada uno de estos ficheros “\*.0” es simplemente necesario abrirlos con un editor de texto, ya que contienen el certificado

digital en formato PEM (base64), junto a la representación del mismo en ASCII para poder ver sus detalles:

```
shell@mobile:/system/etc/security/cacerts $ cat ff783690.0
-----BEGIN CERTIFICATE-----
MIIEEdCCAlygAwIBAgIQRL4Mi1AAJLQR0zYq/mUK/TANBgkqhkiG9w0BAQUFADCB
...
-----END CERTIFICATE-----
Certificate:
 Data:
 Version: 3 (0x2)
 Serial Number:
 44:be:0c:8b:50:00:24:b4:11:d3:36:2a:fe:65:0a:fd
 Signature Algorithm: sha1WithRSAEncryption
 Issuer: C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Nerdware
 Validity
 Not Before: Jul 9 18:10:42 1999 GMT
 Not After : Jul 9 18:19:22 2019 GMT
```

980. Por tanto, este directorio contiene la lista de todos los certificados digitales raíz con las CAs disponibles por defecto en Android.

981. Desde el punto de vista de seguridad, se recomienda evaluar la necesidad de confiar en todas y cada una de las CAs disponibles por defecto en Android, gestionadas por empresas privadas de referencia en la industria, gobiernos, empresas privadas menos conocidas e institutos de investigación, y deshabilitar todas aquellas que no se consideran de confianza [Ref.- 192].

982. Por ejemplo, en un estudio realizado sobre éstas, 15 CAs raíz todavía hacían uso de un certificado digital basado en una clave RSA de 1.024 bits, longitud considerada insuficiente actualmente (desde finales del año 2013<sup>67</sup>), recomendándose al menos el uso de claves de 2.048 bits. Por otro lado, 6 CAs raíz todavía hacían uso de un certificado digital basado en una firma o *hash* obtenida mediante MD5 (considerado insuficiente desde hace años), mientras que 115 CAs raíz todavía hacían uso de firmas obtenidas mediante SHA-1 (considerado insuficiente más recientemente, recomendándose la utilización de SHA-256).

983. Adicionalmente, como se ha descrito previamente, desde Android 4.0 se extiende la posibilidad de añadir nuevos certificados al repositorio de certificados de confianza ("Trust Store") del sistema (certificados existentes por defecto) [Ref.- 188]. Estos se almacenan bajo `/data/misc/keychain` (sólo accesible por `"root"/"system"`), en los directorios `"cacerts-added"` (que contiene los certificados digitales añadidos por el usuario, visibles desde la pestaña "Usuario") y `"cacerts-removed"` (que contiene los certificados digitales de sistema deshabilitados por el usuario, gestionados desde la pestaña "Sistema"), y complementan al directorio que almacena los certificados del sistema descrito previamente, `"/system/etc/security/cacerts"`:

```
root@mobile:/data/misc/keychain/cacerts-added # ls -l
-rw-r--r-- system system 883 2015-01-19 22:07 17f1599a.0
-rw-r--r-- system system 712 2015-01-20 14:01 9a5ba575.0

root@mobile:/data/misc/keychain/cacerts-removed # ls -l
ls -l
-rw-r--r-- system system 1023 2015-01-22 11:35 84cba82f.0
-rw-r--r-- system system 979 2015-01-22 11:35 c3a6a9ad.0
```

<sup>67</sup> <http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf>

984. Debido a que la partición de sistema (“/system”) donde se almacena el repositorio de certificados de confianza del sistema es de sólo lectura, cuando se deshabilita un certificado digital éste no puede ser eliminado, sino que en su lugar se incluye en el directorio “cacerts-removed” bajo “/data/misc/keychain”.

985. Por otro lado, desde Android 4.1 se extienden las capacidades de gestión de la confianza depositadas en el repositorio de certificados de confianza del sistema mediante listas negras (*blacklisting*) [Ref.- 190], que afectan tanto a apps como al navegador web y componentes WebView.

986. Se dispone de dos listas negras de sistema para añadir las claves públicas de CAs comprometidas, y los números de serie de certificados digitales de entidades finales (End Entity, EE) comprometidos. Ambas listas son almacenadas tanto en la base de datos de la app “Ajustes”, como en ficheros bajo “/data/misc/keychain” (sólo accesible por “root”/“system”):

|                                                                                                                                                   |
|---------------------------------------------------------------------------------------------------------------------------------------------------|
| - CAs certificates blacklist: /data/misc/keychain/pubkey_blacklist.txt<br>- EE serial numbers blacklist: /data/misc/keychain/serial_blacklist.txt |
|---------------------------------------------------------------------------------------------------------------------------------------------------|

987. El proceso para añadir certificados digitales raíz específicos para su utilización en conexiones Wi-Fi (o en redes VPN), se detalla en el apartado “16.3. Recomendaciones de seguridad para la conexión a redes Wi-Fi” (y en los apartados correspondientes para VPN).

988. Las implicaciones del uso de certificados digitales en funciones de seguridad críticas requiere que el propietario del dispositivo móvil sea muy cuidadoso a la hora de añadir nuevos certificados digitales al dispositivo móvil, y especialmente, al almacén de certificados raíz (o autoridades certificadoras reconocidas).

### 11.3. GESTIÓN DE CERTIFICADOS DIGITALES

989. Android permite añadir al dispositivo móvil (importar) nuevos certificados digitales, tanto correspondientes a una autoridad certificadora (CA), raíz o intermedia, como certificados finales u hoja, entre los que se incluyen los certificados cliente o personales y los de servidor, complementando así los existentes por defecto.

990. Dentro de las capacidades de gestión de certificados digitales de Android se dispone tanto de capacidades para añadir como para eliminar certificados digitales existentes por defecto (que también pueden ser deshabilitados temporalmente) o previamente importados.

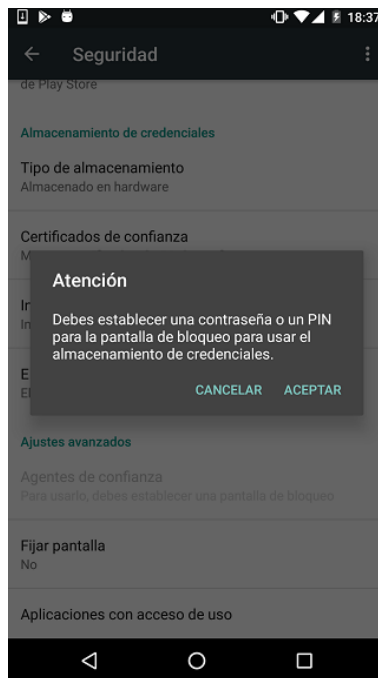
#### 11.3.1. GESTIÓN DE CERTIFICADOS DIGITALES DE AUTORIDADES CERTIFICADORAS

991. Los certificados digitales raíz asociados a una nueva CA pueden ser obtenidos (e importados) desde el almacenamiento del dispositivo, ya sea interno o externo, a través de la opción “Instalar desde almacenamiento” disponible desde el menú “Ajustes [Personal] - Seguridad [Almacenamiento de Credenciales]”<sup>68</sup>.

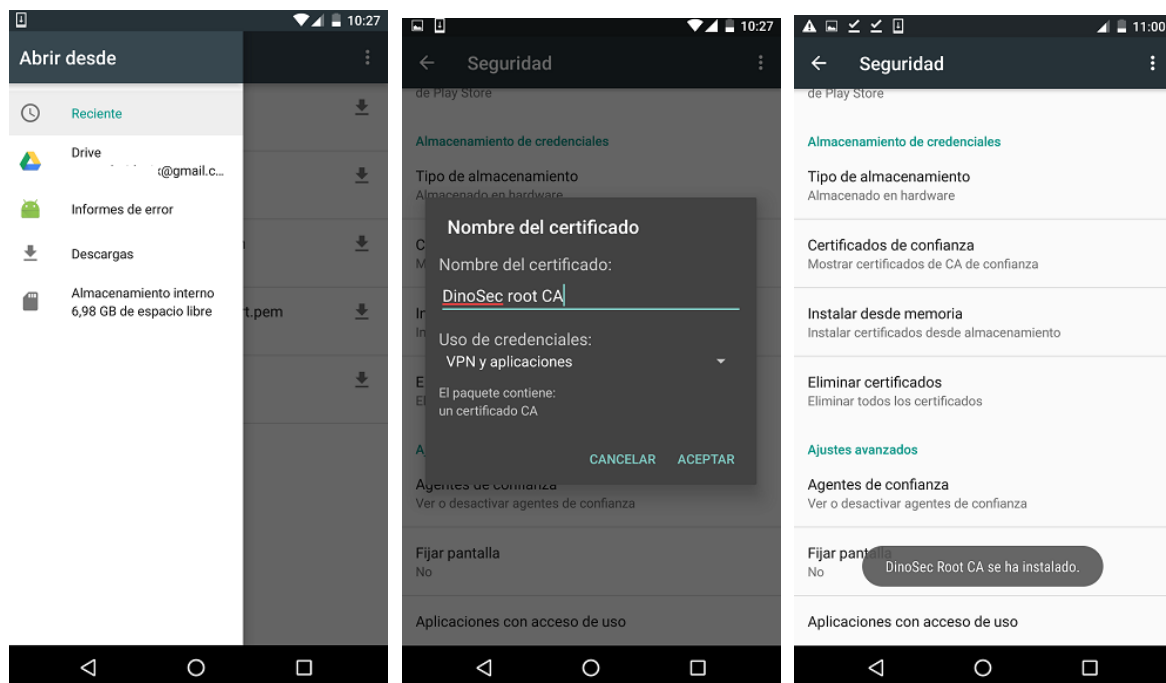
992. Para poder añadir un nuevo certificado de CA al repositorio de credenciales, es indispensable que el acceso al dispositivo esté protegido por un método de acceso. Si el

<sup>68</sup> En versiones previas de Android (2.x) el fichero del certificado digital debía almacenarse directamente en el directorio raíz del almacenamiento interno del dispositivo móvil (o tarjeta SD), no en un subdirectorio.

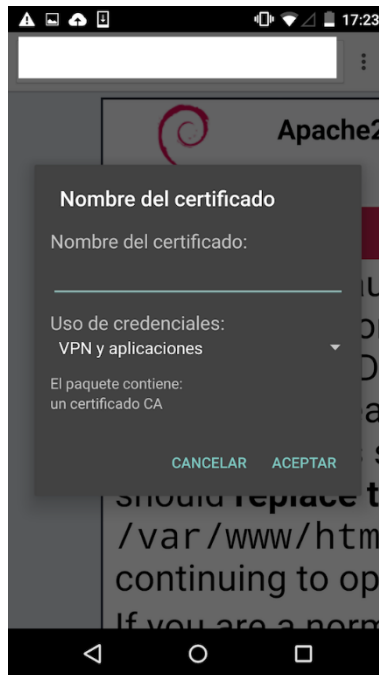
dispositivo no tiene ninguno, al seleccionar el nombre del fichero que contiene el certificado, el sistema informará al usuario de que debe configurar un método de acceso, y llevará al menú de configuración de selección del tipo de bloqueo si se pulsa el botón “Aceptar”:



993. Si el certificado digital es obtenido desde la web, por ejemplo a través del navegador web existente por defecto, Chrome, Android lo almacenará en la carpeta “Descargas” (o “Download”, dentro del almacenamiento interno):



994. En versiones anteriores de Android, era posible importar directamente en el navegador Chrome certificados digitales cuya extensión del fichero correspondiente fuese reconocida como un certificado digital válido (por ejemplo, los ficheros de extensión “.crt”). En esas versiones, Android presentaba al usuario directamente la ventana para importar el certificado digital en el dispositivo móvil:



995. Esta opción ya no está disponible por defecto en Android 6.x, por lo que cualquier certificado que se desee instalar (ya sea de CA o de usuario final) debe instalarse desde una unidad de almacenamiento.

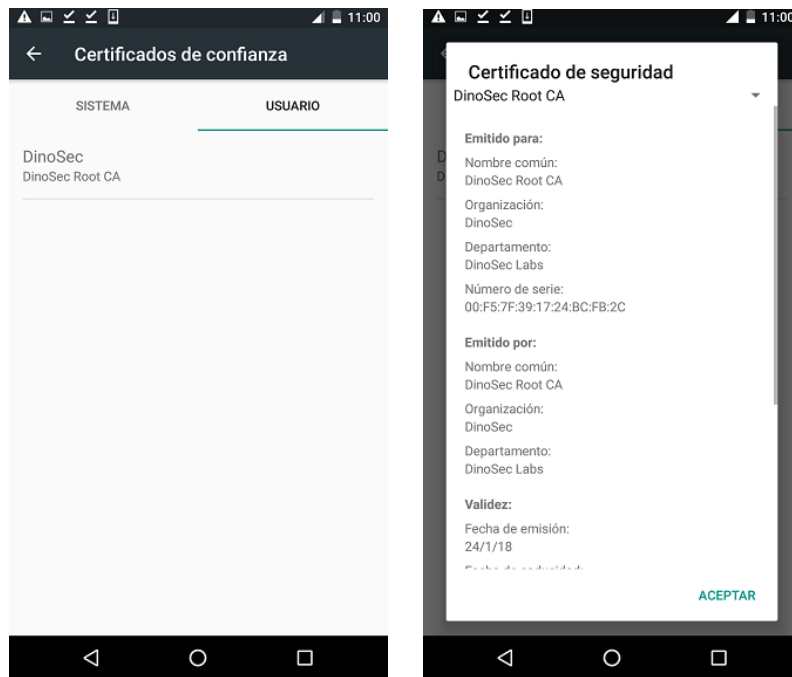
996. Android admite certificados X.509 codificados en formato DER (binario) y PEM (ASCII en base64). Sin embargo, debe tener obligatoriamente una extensión válida reconocida por Android, como “.pem”, “.cer” o “.crt” (no siendo “.der” una extensión válida en Android) [Ref.- 185].

997. Al seleccionar el fichero correspondiente al certificado digital se solicitará al usuario un nombre para su identificación, y el propósito del mismo: “VPN y aplicaciones” o “Wi-Fi”, tal como se mostró en las pantallas anteriores. Es importante reseñar que, si se va a utilizar un certificado con ambos usos (Wi-Fi y VPN y aplicaciones), el certificado deberá importarse dos veces, una para cada escenario de uso.

**Nota:** Los certificados raíz importados mediante estos métodos (desde Android 4.0) no sólo afectan a las conexiones Wi-Fi y a las redes VPN que hacen uso de certificados digitales, sino también a otro tipo de conexiones, como por ejemplo sesiones web autenticadas y cifradas mediante HTTPS, establecidas desde el navegador web o el cliente de correo electrónico, o cualquier otra app cliente, de ahí que la categoría para las redes VPN se denomine “VPN y aplicaciones” [Ref.- 189].

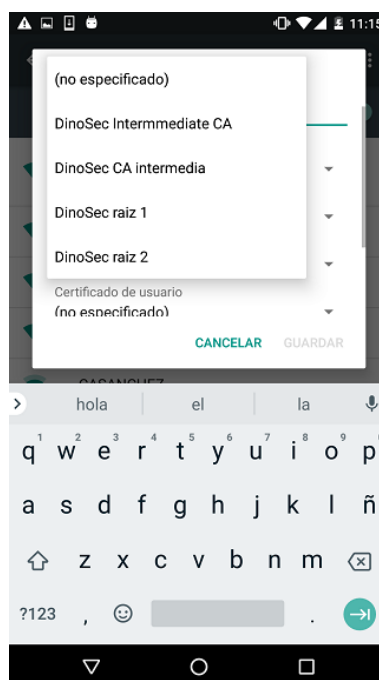
998. El proceso de instalación del nuevo certificado digital no muestra los detalles del mismo, por lo que es muy importante ser especialmente cuidadoso a la hora de importar nuevos certificados, especialmente los descargados directamente desde la web.

999. El nombre dado por el usuario durante la importación del certificado correspondiente a una CA no es necesariamente el que se visualizará en la pestaña “Usuario” del menú “Certificados de Confianza”, ya que el nombre que se muestra en esa sección será el que indique el campo “*Common Name*” (CN) definido en el certificado. Mediante la selección del certificado digital es posible ver todos sus detalles:



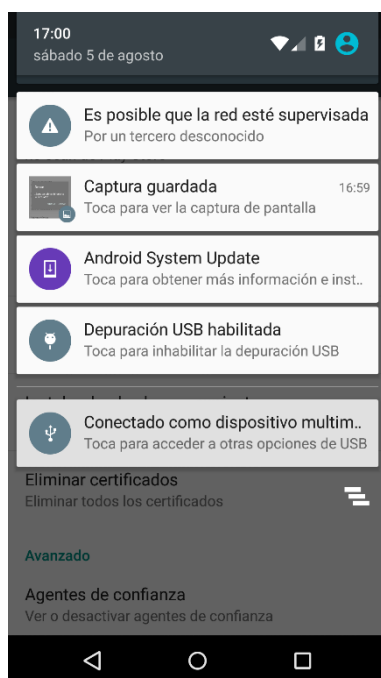
**Nota:** Android permite importar un mismo certificado digital raíz tantas veces como se quiera, pero en el listado de certificados de confianza, pestaña “Usuario”, sólo aparecerá una vez el certificado digital (independientemente del nombre proporcionado al importarlo cada vez).

1000. El nombre que el usuario defina para el certificado durante su importación sólo se utiliza en el menú de configuración de Wi-Fi y VPN. Si se realiza la importación de un mismo certificado más de una vez empleando distintos nombres, aunque en el menú “Certificados de confianza - [Usuario]” sólo aparecerá una entrada correspondiente al CN del mismo, en el menú de configuración Wi-Fi se mostrarán tantas entradas para el certificado como nombres diferentes se emplearon para su importación:





1001. Para eliminar el certificado digital añadido recientemente de manera selectiva es necesario acceder a la lista de certificados de confianza, y desde la pestaña “Usuario”, ver los detalles del mismo, pudiendo hacer uso del botón “Eliminar” disponible en la parte inferior.
1002. El certificado digital es importado en la pestaña “Usuario”, aunque se trate de un certificado digital correspondiente a una CA, ya que ha sido añadido a posteriori por el usuario y no forma parte de la configuración por defecto del sistema (pestaña “Sistema”).
1003. Aunque en versiones anteriores de Android la importación de certificados por parte del usuario imposibilitaba la supresión del código de acceso en el dispositivo móvil (siendo necesario resetear el repositorio de credenciales, eliminando todos los certificados previamente importados para poder hacer esto) en Android 6.x sí es posible eliminar el código de acceso y seguir haciendo uso de los certificados instalados con anterioridad a esta acción. Sin embargo, no se podrán añadir certificados nuevos mientras el terminal siga sin un código de acceso configurado. No obstante, suprimir el método o código de acceso es una opción totalmente desaconsejada desde el punto de vista de seguridad.
1004. Desde Android 4.x, tras llevar a cabo la instalación de un certificado digital asociado a una CA, la sección “Seguridad” del menú “Ajustes” muestra un triángulo de aviso. Asimismo, se muestra al usuario de manera permanente una notificación a través de la barra superior de menú. Al seleccionar el triángulo se informa al usuario de que se ha instalado una nueva CA, lo que puede permitir a un tercero supervisar las actividades del usuario mediante la interceptación de su tráfico de red cifrado.
1005. Sin embargo, desde Android 5.x y vigente en Android 6.x, desapareció el aviso de triángulo de la sección “Seguridad” del menú “Ajustes”, y se lanzó el aviso sólo como parte de una notificación que no se puede descartar con un icono de triángulo. Al seleccionar la misma, se indicará que la red puede estar supervisada:



1006. Esta notificación no se mostrará si el certificado de la CA sólo se ha importado como parte de un certificado cliente (consultar apartado “11.3.3. Gestión de certificados digitales cliente”).

### 11.3.2. GESTIÓN DE CERTIFICADOS DIGITALES SERVIDOR

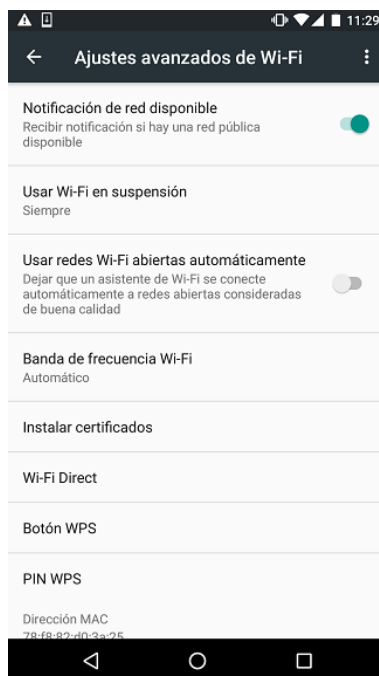
1007. Los certificados digitales de servidor se importan de forma similar a los certificados correspondientes a una autoridad certificadora, tal como se detalla en el apartado anterior. Sin embargo, estos certificados no se mostrarán en el menú “Ajustes - [Personal] Seguridad - [Almacenamiento de credenciales]”, pues en dicho menú sólo se detallan las CAs añadidas por el usuario.

1008. Por tanto, el único modo de eliminar certificados de servidor importados por el usuario reseteando por completo el repositorio de credenciales.

### 11.3.3. GESTIÓN DE CERTIFICADOS DIGITALES CLIENTE

1009. Los certificados digitales cliente (o de usuario<sup>69</sup>) asociados, por ejemplo, a redes VPN, servidores web o redes Wi-Fi, pueden ser importados desde el almacenamiento (interno o externa) del dispositivo, a través de la opción “Instalar desde almacenamiento” disponible desde el menú “Ajustes [Personal] - Seguridad [Almacenamiento de Credenciales]”.

1010. Además, para el caso de las redes Wi-Fi empresariales, es posible añadir el certificado cliente a través del menú de configuración de la red Wi-Fi (“Ajustes - [Conexiones inalámbricas y redes] Wi-Fi - <...> Ajustes avanzados - Instalar certificados”):

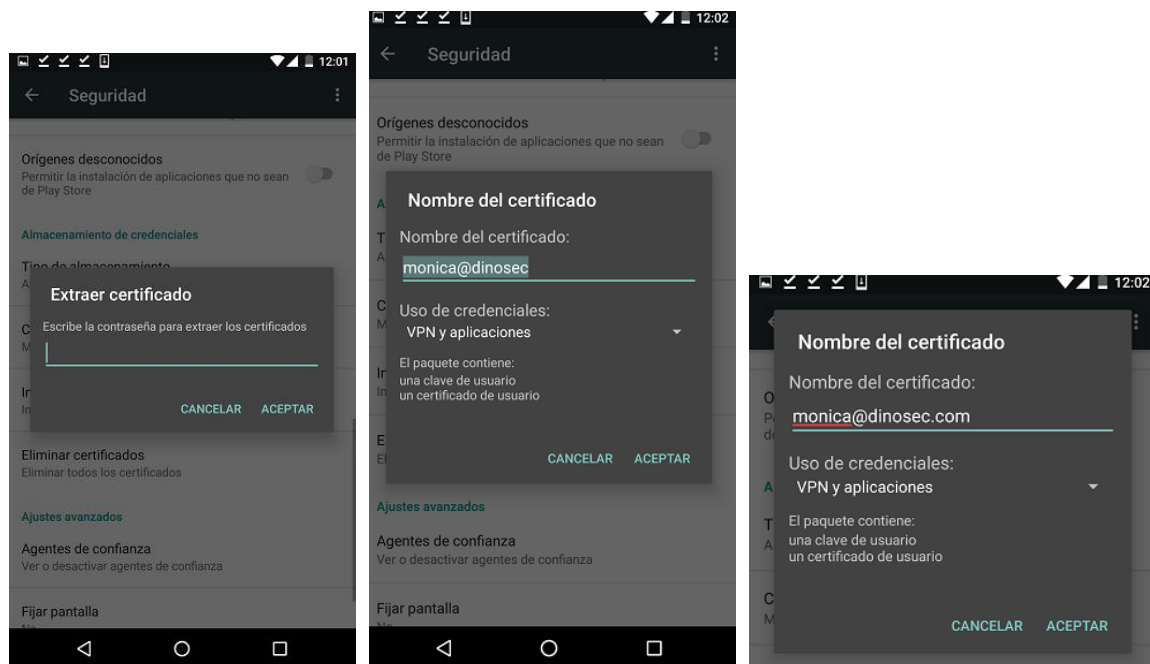


1011. Al igual que en el caso de los certificados digitales raíz (ver apartado “11.3.1. Gestión de certificados digitales de Autoridades Certificadoras”), Android solicitará al usuario

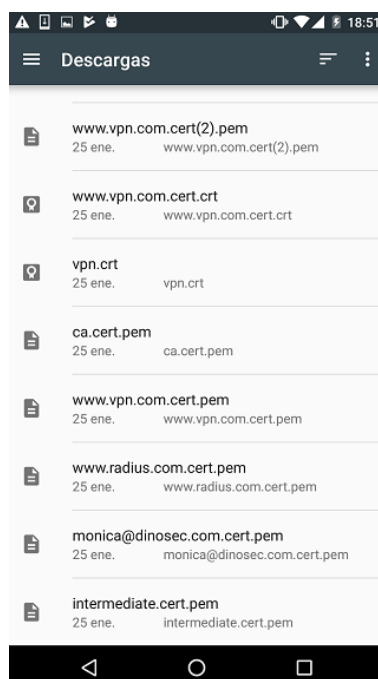
<sup>69</sup> Se hace uso del término certificado digital cliente para referirse a los certificados empleados para la autenticación del usuario, en lugar de emplearse el término certificado digital de usuario, con el objetivo de evitar confusiones con la pestaña “Usuario” de Android, que muestra tanto certificados de cliente como de CAs.

establecer una contraseña o código de acceso en el dispositivo móvil para poder hacer uso del repositorio de credenciales, si aún no se ha establecido una.

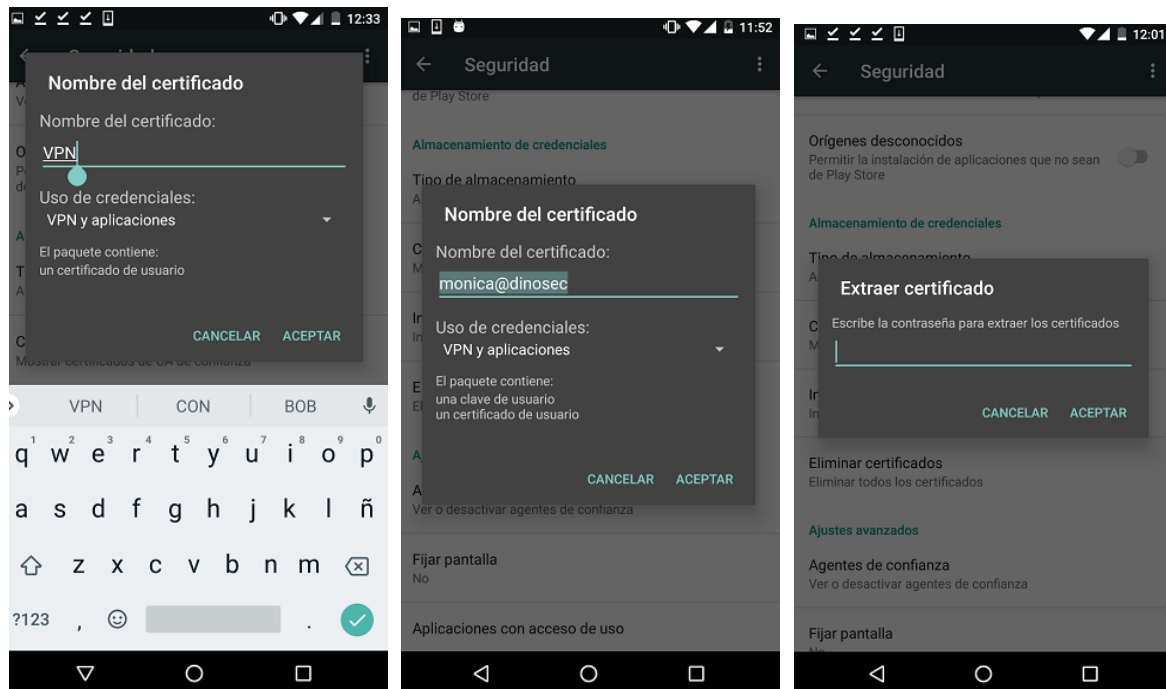
1012. Para archivos que actúan como almacén de claves, Android soporta certificados X.509 codificados como PKCS#12. Estos ficheros deberán tener extensión .p12 o .pfx [Ref.- 185]. Al seleccionar el fichero correspondiente al certificado digital cliente se solicitará al usuario la contraseña que fue empleada para proteger el fichero PKCS#12 que contiene el certificado digital y la clave privada, y poder así extraer los certificados del fichero:



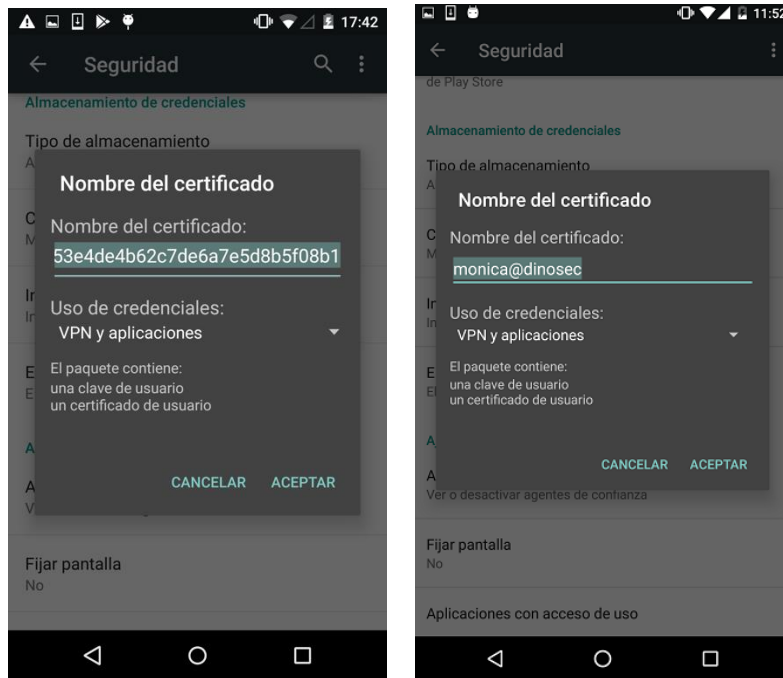
1013. La lista de ficheros que se muestra al seleccionar la carpeta donde reside un certificado identifica el tipo de certificado contenido en cada fichero a través de un pequeño icono situado a la derecha del nombre del fichero: un símbolo de tipo documento para los ficheros con formato “.pem” y un símbolo de condecoración para los ficheros de tipo “.crt” o “.pfx”:



1014. Si el fichero del certificado corresponde a un archivo de certificado estándar (que, por tanto, no incluye clave privada), el texto dentro del campo “El paquete contiene” sólo incluirá “un certificado de usuario”:



1015. Si el fichero correspondiente al certificado fuese un almacén de claves y contuviese además la clave privada del cliente, Android mostrará el texto “una clave de usuario” y “un certificado de usuario” dentro del campo “El paquete contiene”, como se ilustra en la imagen superior central. En ese caso, se solicitaría la contraseña asociada a la clave privada para importarla.
1016. Si el fichero correspondiente al certificado contuviese además la clave pública de la CA que firmó dicho certificado, Android mostrará el texto “un certificado de CA” y “un certificado de usuario” dentro del campo “El paquete contiene”. Este escenario resulta útil para evitar tener que añadir primero el certificado de la CA y luego el del cliente. Los ficheros que contienen clave de usuario deben estar en formato PKCS#12.
1017. Adicionalmente, ni en Android 6.x ni en versiones anteriores existe una opción que permita consultar qué certificados cliente se han instalado en el dispositivo, de ahí que no sea posible eliminarlos de forma selectiva, sino todos en bloque. De nuevo, únicamente es posible ver si se ha añadido algún certificado cliente a través del menú de configuración de Wi-Fi empresarial (basadas en 802.1x EAP) y VPN.
1018. Tras extraer el certificado digital cliente (que contiene la clave pública), y la clave privada asociada (y opcionalmente, el certificado de la CA que lo ha emitido), se solicitará al usuario un nombre para su identificación y el propósito del mismo: “VPN y aplicaciones” o “Wi-Fi”. En versiones anteriores de Android (hasta Android 5.x inclusive), por defecto se mostraba como nombre para el certificado el identificador local de la clave, “localKeyID”, como muestra la imagen inferior izquierda), pero en Android 6.x el nombre por defecto corresponde al denominado “friendlyName” definido en el certificado (ver imagen inferior derecha):



```
$ openssl pkcs12 -info -in monica@dinosec.com.pfx
Enter Import Password:
MAC:shal Iteration 2048
PKCS7 Encrypted data: pbeWithSHA1And40BitRC2-CBC, Iteration 2048
Certificate bag
Bag Attributes
 localKeyID: 05 D0 CE 0A 19 AA 97 A0 D5 51 21 4F DE BA 1B 85 FB 0E C6 D9
 friendlyName: monica@dinosec.com
subject=/C=ES/ST=Madrid/L=Madrid/O=DinoSec/OU=DinoSec Labs/CN=DinoSec
Intermediate CA/emailAddress=monica@dinosec.com
issuer=/C=ES/ST=Madrid/O=DinoSec/OU=DinoSec Labs/CN=DinoSec Intermediate
CA/emailAddress=info@dinosec.com
```

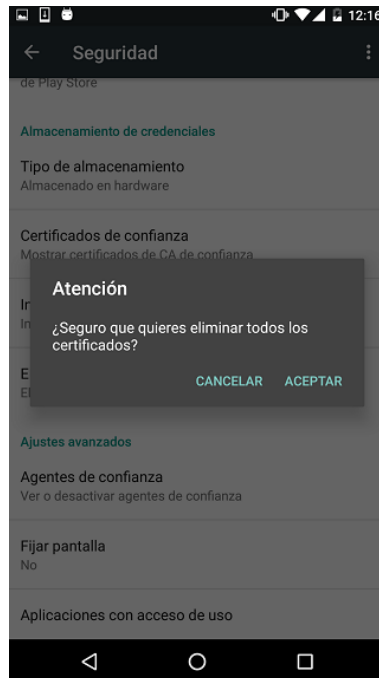
1019. Se recomienda proporcionar un nombre de certificado que permita la identificación del mismo de forma sencilla desde las aplicaciones cliente que hacen uso de éste. Este nombre será mostrado posteriormente al seleccionar el certificado digital cliente, por ejemplo, en el proceso de configuración de una red Wi-Fi Empresarial o de una red VPN.

**Nota:** Android permite importar un mismo certificado digital cliente en múltiples ocasiones, apareciendo múltiples veces en el listado de certificados digitales cliente (o de usuario) disponible a la hora de hacer uso del mismo, por ejemplo, al configurar una red Wi-Fi Empresarial. Cada una de las instancias del certificado digital aparecerá con el nombre proporcionado al importarlo, y en el caso de duplicar dicho nombre durante el proceso de importación, se sobrescribirá la entrada existente previamente.

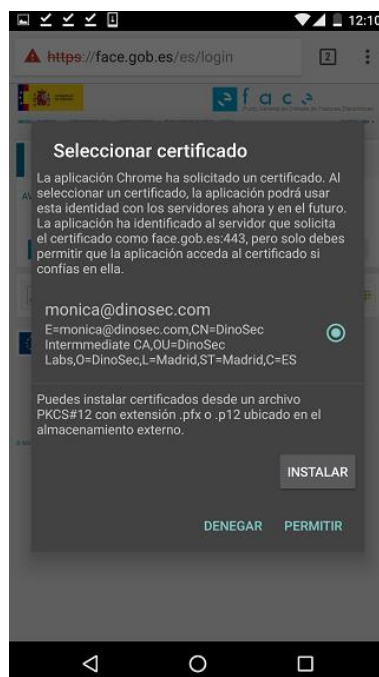
1020. Si se incluye un certificado de una CA junto con el certificado digital cliente, éste se instalará de forma simultánea. El certificado digital correspondiente a la CA emisora del certificado digital cliente, si está incluido en el fichero PKCS#12, es también importado en la pestaña “Usuario”<sup>70</sup>, al tratarse de un certificado digital correspondiente a una CA, y que ha sido añadido a posteriori por el usuario (y que por tanto no forma parte de la configuración por defecto del sistema, pestaña “Sistema”).

<sup>70</sup> A diferencia de como ocurría en versiones previas de Android (2.x), el certificado digital importado (ya sea de una CA o personal) no es eliminado de la tarjeta de almacenamiento externa una vez se ha completado la operación de importación.

1021. No es posible eliminar un certificado de forma individual (únicamente se puede inhabilitarlo). La opción del menú “Seguridad - [Almacenamiento de credenciales] Eliminar certificados” eliminará todos los certificados existentes en el repositorio de credenciales simultáneamente que hayan sido añadidos por el usuario. Es decir, esta opción permite resetear el repositorio de credenciales para volver a hacer uso del mismo desde la versión de fábrica (formado por las CAs reconocidas por Android):



1022. Los certificados digitales cliente que se importen con su clave privada podrán ser utilizados en aquellas apps que requieran autenticación mediante este método, como por ejemplo, al acceder con un navegador web a un servicio web que requiere disponer de un certificado de usuario:



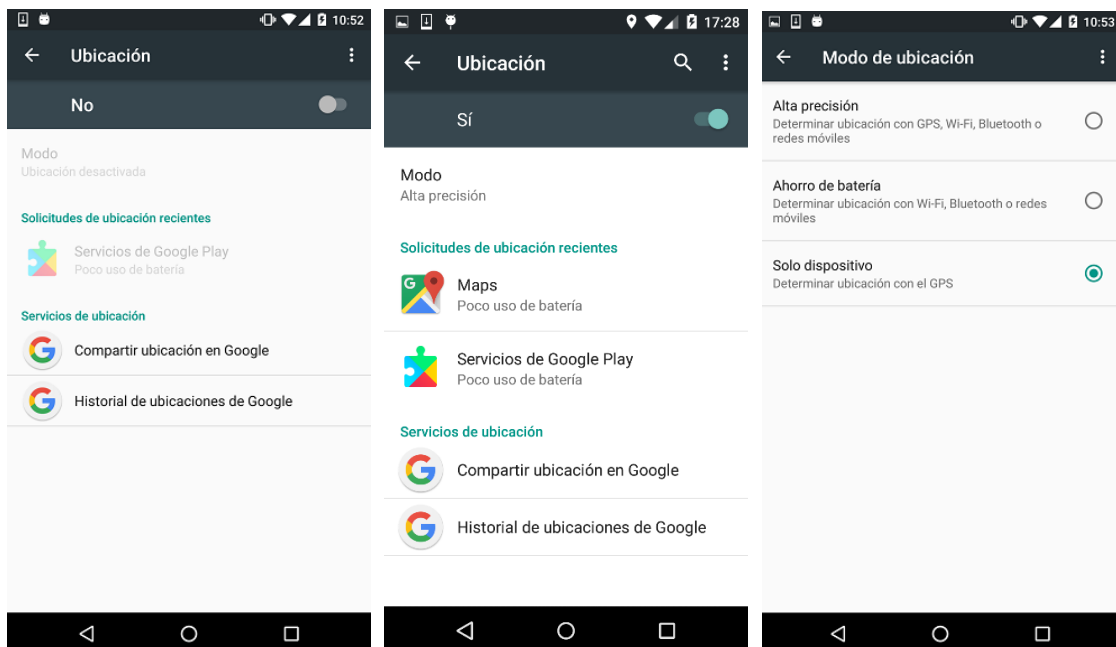
## 12. LOCALIZACIÓN (O UBICACIÓN) GEOGRÁFICA

1023. Las capacidades de localización (o ubicación) del dispositivo móvil a través del módulo de GPS, o de las redes de datos (telefonía móvil y Wi-Fi), pueden ser activadas y desactivadas por el usuario en función de su utilización.

1024. El uso del GPS, o de los servicios de localización, en el dispositivo móvil Android viene reflejado por un conjunto específico de iconos mostrados a través de la barra superior de estado.

**Nota:** El dispositivo o módulo GPS en Android está activo únicamente cuando se está haciendo uso de una app con capacidades de localización, es decir, que hace uso del GPS, y en base a la configuración específica (modos), de los servicios de localización de Android.

1025. Desde el menú “Ajustes [Personal] - Ubicación”, y en concreto a través del interruptor “[SI | NO]” disponible en la parte superior derecha, es posible habilitar las capacidades de localización del dispositivo móvil:



1026. Desde Android 4.4 (KitKat) se proporciona un mayor control sobre los diferentes modos de localización (o ubicación) disponibles [Ref.- 149]: alta precisión, ahorro de batería o solo en dispositivo.

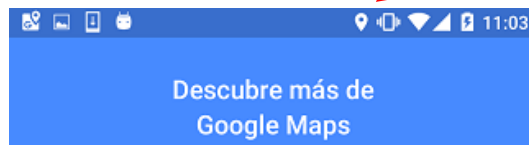
1027. La opción o el modo “Alta precisión” hace uso del módulo GPS, de las conexiones Bluetooth (las cuales no se empleaban para el servicio de ubicación en Android 5.x y anteriores), de las redes Wi-Fi y de telefonía móvil, y de otros sensores, para obtener la ubicación más rápida y precisa posible en el dispositivo móvil. El modo “Ahorro de batería” emplea como fuentes para la obtención de la ubicación del dispositivo móvil las redes Wi-Fi, las conexiones Bluetooth y las redes de telefonía móvil, ya que llevan a cabo un menor consumo de energía en comparación al módulo GPS. Por último, el modo “Solo en dispositivo” hace uso únicamente del módulo GPS del dispositivo móvil.

1028. La nueva funcionalidad y API empleada por las apps para acceder a los servicios de localización, especialmente al usar el modo “Ahorro de batería”, reduce drásticamente el consumo de batería. Previamente, cada app que necesitaba hacer uso de los servicios

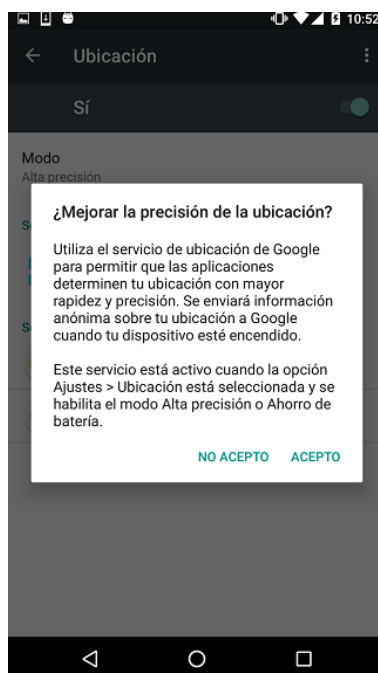


de localización despertaba al módulo GPS hardware y obtenía su información de ubicación propia individualmente.

1029. Cuando una aplicación o servicio del dispositivo móvil interactúa con los servicios de ubicación, se mostrará en la barra de ajustes rápidos el icono asociado, que aparece a continuación junto al símbolo del modo vibración:



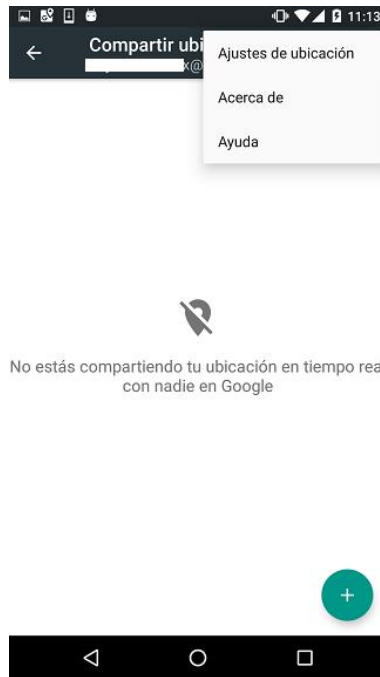
1030. Todos estos modos están disponibles en los servicios de ubicación de Google, que extienden las capacidades del módulo GPS del dispositivo móvil con otras tecnologías.
1031. La opción (o modo) habilitada por defecto dependerá de las opciones seleccionadas en la pantalla de “Ubicación y Google” durante el proceso inicial de instalación y configuración del dispositivo móvil (ver apartado “24. Apéndice A: Proceso de instalación y configuración inicial”).
1032. Debe tenerse en cuenta que el modo avión de Android deshabilitará los servicios de ubicación, no permitiendo ninguna transmisión inalámbrica ni con los satélites GPS, ni con las redes Wi-Fi o de telefonía móvil, ni con dispositivos Bluetooth.
1033. Desde el punto de vista de seguridad, si se desea que no se genere ningún tráfico desde el dispositivo móvil hacia los servicios de Google, se recomienda seleccionar la opción o modo “Solo en dispositivo”, pese a que tenga asociado un mayor consumo de batería y tarde más tiempo en localizar la ubicación del dispositivo inicialmente.
1034. En el caso de habilitar las capacidades de localización a través de redes y conexiones inalámbricas (Wi-Fi, Bluetooth y telefonía móvil), mediante la selección de los modos “Alta precisión” o “Ahorro de batería”, Android solicitará confirmación por parte del usuario para recopilar los datos de las señales inalámbricas recibidas y la ubicación del terminal de forma anónima:



**Nota:** Existen estudios pasados que reflejan que la información de localización intercambiada entre el dispositivo móvil Android y Google no es completamente anónima, ya que, aparte de incluir detalles de las señales de las redes inalámbricas recibidas y la ubicación del terminal, se incluye un identificador único del dispositivo móvil [Ref.- 82], lo cual puede afectar a la privacidad del usuario.

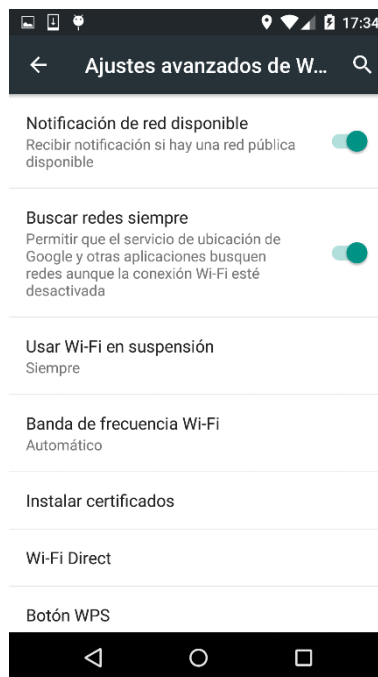
Adicionalmente, la información de las redes Wi-Fi recopilada por Google a través de los coches del programa StreetView y de los dispositivos móviles Android estuvo disponible en el pasado para su consulta a través de la API de Google y de páginas web externas [Ref.- 83], siendo posible conocer la ubicación de una red Wi-Fi a nivel mundial en base a su dirección MAC o BSSID. El acceso a través de este servicio no está disponible actualmente de manera pública.

1035. Es posible consultar las apps que han solicitado información sobre la ubicación del dispositivo móvil recientemente a través del menú “Ajustes [Personal] - Ubicación”, y de la sección “Solicitudes de Ubicación Recientes”.
1036. Mediante la visualización de las apps en la lista, bajo su nombre, es posible identificar el impacto en la batería debido al uso de los servicios de ubicación por parte de cada app: “Uso de batería elevado” o “Poco uso de batería”.
1037. Mediante la selección de una app de la lista se accede a la información de la app (información también disponible desde el menú “Ajustes [Dispositivo] - Aplicaciones - Todas”).
1038. Adicionalmente, una vez se ha configurado una cuenta de usuario de Google en el dispositivo móvil, a través del menú “Ajustes [Personal] - Ubicación”, y de la sección “Servicios de Ubicación”, es posible seleccionar “Historial de ubicaciones de Google” y acceder a los ajustes de configuración para activar o desactivar los informes de ubicación y el historial de ubicaciones de la cuenta de usuario de Google (ver apartado “12.5. Historial de ubicaciones”).
1039. La opción “Ajustes - [Personal] Ubicación - [Servicios de Ubicación] Compartir ubicación en Google” permite ver con quién se está compartiendo la ubicación en un momento concreto. La opción de “Compartir ubicación” se habilita en el menú lateral de la aplicación “Google Maps”. Cuando se selecciona, aparecerá un menú que permite especificar el tiempo durante el cual se compartirá la ubicación, así como los contactos con los que se desea compartir (que deben poseer también una cuenta de Google). Es posible incluso crear un enlace que se puede enviar a través de aplicaciones de mensajería, Bluetooth, etc., de modo que los contactos elegidos o que reciban el enlace puedan realizar el seguimiento en tiempo real de la posición del dispositivo en un mapa. Por este motivo y debido a las implicaciones en la privacidad, una vez se comparte la ubicación con alguien, el usuario recibirá una notificación informándole de ello a modo de recordatorio. Para más detalles, consultar el apartado “12.2. Google Maps”.

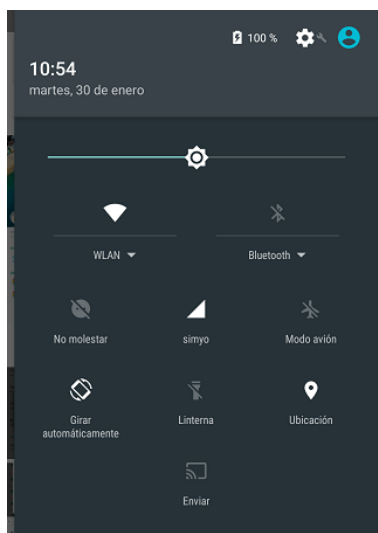


1040. Adicionalmente, si se hace uso de alguno de los modos que emplean las redes Wi-Fi para obtener información sobre la ubicación del dispositivo móvil, es posible configurar si se permite el uso de las capacidades Wi-Fi del dispositivo móvil para estos servicios y, en concreto, para la búsqueda e identificación de redes Wi-Fi, aunque la conexión o el interfaz Wi-Fi esté desactivado.

1041. Esta opción de configuración también está disponible en el proceso de instalación y configuración inicial del terminal, ver apartado “24. Apéndice A: Proceso de instalación y configuración inicial”), y se puede acceder a la misma posteriormente desde el menú “Ajustes - [Conexiones Inalámbricas y Redes] Wi-Fi - [...] - Ajustes avanzados - Buscar redes siempre”:



1042. Por último, la activación de los servicios de ubicación en el dispositivo móvil también está disponible a través de los ajustes rápidos, accesibles desde la barra superior de estado:



1043. Para que el servicio “Encontrar mi dispositivo” (consultar apartado “8.1. Gestión remota de dispositivos Android por parte del usuario”) esté operativo, es requisito indispensable que las capacidades de ubicación estén activas.
1044. Se recomienda valorar el uso de las capacidades de localización del dispositivo móvil, buscando el equilibrio entre privacidad y funcionalidad. En caso de querer hacer uso de sus capacidades y evitar otras implicaciones de privacidad, se recomienda activar únicamente la localización mediante GPS, no haciendo uso de las capacidades de localización mediante redes Wi-Fi o redes de telefonía móvil.
1045. En noviembre de 2017, la empresa Quartz publicó un informe en el que desvelaba que, desde el comienzo de dicho año, todos los dispositivos móviles Android recolectan información sobre la ubicación de las torres de telefonía móvil cercanas, y que envían esos datos a Google cuando se conectan a Internet, incluso aunque los servicios de ubicación hayan sido deshabilitados por el propietario del terminal. Google confirmó esta información alegando que los datos no se almacenaban, sino que se empleaban para mejorar el servicio de mensajes y notificaciones. En el momento de elaboración de la presente guía, no existe ninguna opción para deshabilitar este comportamiento en el dispositivo móvil, ni se incluye referencia alguna a esta práctica en la política de privacidad de Google [Ref.- 252].

## 12.1. SERVICIOS DE UBICACIÓN DE GOOGLE

1046. Durante el proceso de configuración inicial del dispositivo móvil empleado para la elaboración de la presente guía, Android solicita al usuario si desea usar los servicios de ubicación de Google, incluso aunque se haya declinado la asociación del dispositivo a una cuenta de usuario de Google.
1047. Las opciones disponibles “Usar el servicio de ubicación de Google” y “Ayudar a mejorar los servicios de ubicación” están habilitadas por defecto, por lo que se recomienda desactivarlas hasta determinar el uso que se desea hacer de ellas (ver apartado “24. Apéndice A: Proceso de instalación y configuración inicial”).
1048. Los servicios de ubicación o localización de Google (*Google Location Services*), permiten a las apps conocer la ubicación geográfica aproximada del dispositivo móvil, y por tanto del usuario, aun sin disponer de señal GPS, y hacer uso de esa información en

los servicios de búsqueda (y otros servicios) de Google, o desde cualquier app con los permisos adecuados, teóricamente de una forma más rápida y precisa.

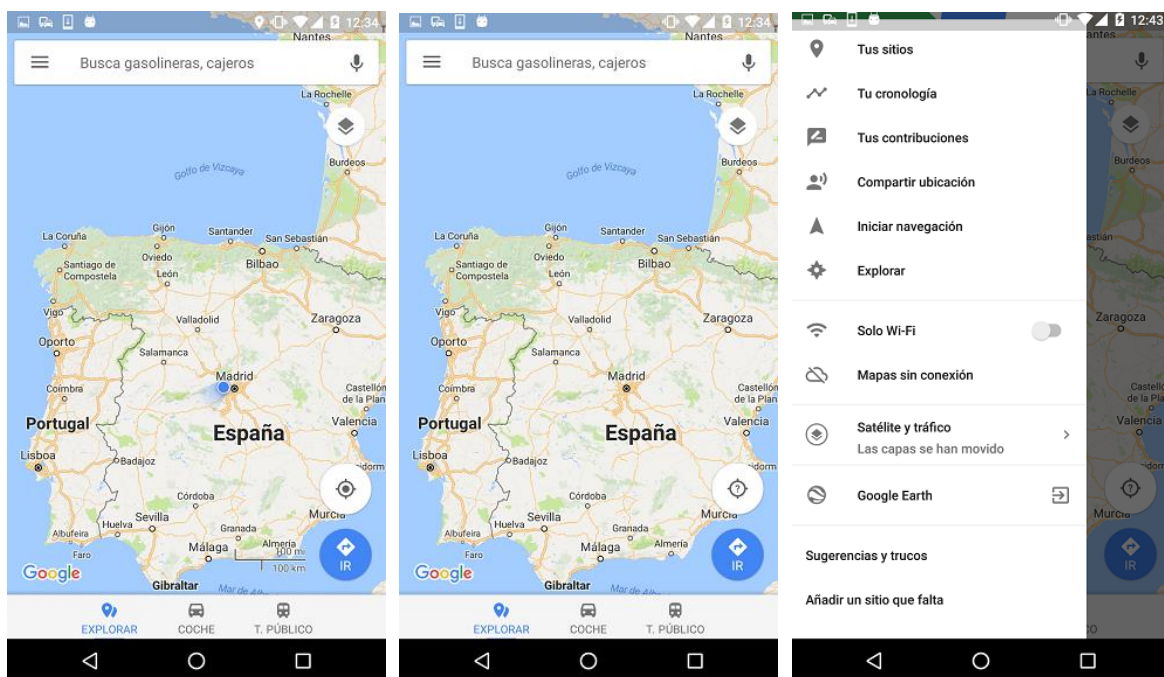
1049. La ubicación se obtiene a través de la información de localización disponible sobre torres (o redes) de telefonía móvil y redes Wi-Fi, y la señal recibida en cada momento por el dispositivo móvil para ambas tecnologías (telefonía móvil y Wi-Fi), en lugar de emplear información más precisa como la proporcionada por el dispositivo o módulo GPS.
1050. Para hacer uso de la geolocalización en base a redes Wi-Fi, el dispositivo escaneará los puntos de acceso Wi-Fi que estén en su rango de alcance (independientemente de su nivel de seguridad) y, en base a las respuestas recibidas, y tras enviar los detalles a los servicios de Google, la respuesta obtenida por parte de estos le permitirá interpolar su ubicación aproximada.
1051. El servicio de ubicación a través de Bluetooth se basa en el uso de las denominadas balizas Bluetooth LE y la tecnología conocida como *beacons*. Un *beacon* es un dispositivo inalámbrico que envía periódicamente un anuncio BLE (*Bluetooth Low Energy*) con su identificador, de forma que una app pueda extraer su ubicación a través de una base de datos con la posición de estas balizas. El dispositivo móvil recibe ese anuncio y la app (o el servicio de ubicación del sistema operativo) puede determinar así la ubicación aproximada.
1052. Las dos principales (aunque no las únicas) tecnologías de *beacons* que existen actualmente en el mercado son iBeacon (de Apple) [Ref.- 253] y EddyStone (de Google) [Ref.- 254].
1053. La utilización de los servicios de ubicación de Google puede conllevar por tanto el envío, supuestamente anónimo, a Google de los datos recopilados sobre las redes Wi-Fi, de telefonía móvil y de dispositivos Bluetooth basados en tecnologías basadas en *beacons* sobre la ubicación aproximada en la que se encuentra el dispositivo móvil, incluso aunque no se esté utilizando ninguna app.
1054. En resumen, estas peticiones de información hacia Google pueden desvelar información de las redes Wi-Fi, de telefonía móvil y de las balizas BLE existentes en el área de cobertura del dispositivo móvil, así como otros detalles relevantes del terminal, potencialmente a cualquiera que esté capturando el tráfico de datos generado desde el dispositivo móvil. Las respuestas de los servicios de ubicación de Google, en formato binario, contienen información de la ubicación estimada del dispositivo móvil.
1055. Se recomienda limitar el uso de estos servicios, especialmente a través de redes de datos inseguras, por parte de cualquier app como por ejemplo “Google Maps” (ver siguiente apartado), y específicamente su utilización cuando se emplea algo más que el módulo GPS, ya que los servicios de ubicación de Google a través de torres de telefonía móvil y redes Wi-Fi desvelan detalles privados del dispositivo móvil y de su ubicación.

## 12.2. GOOGLE MAPS

1056. Los servicios de ubicación de Google son utilizados, entre otros, tanto por el propio sistema operativo Android como por las apps disponibles por defecto o proporcionadas por terceros, como por ejemplo la app “Maps” o “Google Maps” (<https://maps.google.com>) que, en el caso del dispositivo móvil empleado para la

elaboración de la presente guía, está disponible como app por defecto a través de la app “Maps” (disponible desde el *Launcher*).

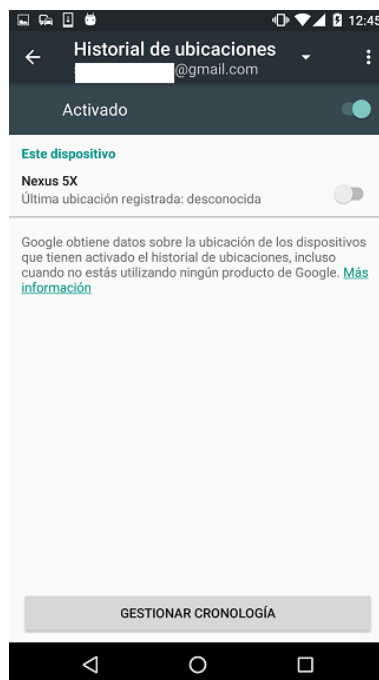
1057. Tras aceptar los términos y condiciones del servicio (al ejecutar la app la primera vez), y en función de la configuración de los servicios de ubicación, la recopilación de información será activada y se permitirá su utilización por defecto por parte de las apps que hacen uso de los servicios de ubicación.
1058. Desde Maps es posible hacer uso de la información de localización, en concreto, empleando el botón circular con una cruceta, que centrará el mapa en la localización actual del usuario (identificada por un indicador azul). Si el indicador de posición se muestra como un punto gris, significa que Maps no consigue detectar la ubicación actual y está mostrando la última ubicación que determinó anteriormente para el dispositivo móvil.



1059. La versión de la aplicación Maps se puede consultar dentro del menú de la app, “Ajustes - Información, condiciones y privacidad”.
1060. Al hacer uso de apps que requieren conocer la ubicación del usuario, como Maps, y si han sido habilitadas, se emplearán las capacidades para localizar la ubicación del dispositivo móvil incluso cuando no se disponga de módulo GPS (o éste no esté activo o no haya cobertura de los satélites GPS), a través de A-GPS, que emplea la información de localización disponible a través de servicios de terceros (ver apartado “12.3. A-GPS”), y la funcionalidad extendida de los servicios de ubicación de Google descritos previamente, haciendo uso de la información de las redes Wi-Fi, las balizas BLE y las torres de telefonía móvil.
1061. Los servicios de ubicación de Google integrados en Google Maps, así como los datos e información obtenida por la app (mapas, información extra, etc.), en el caso de la versión 9.69.1 de la app Maps (última versión disponible a fecha de elaboración de la presente guía) emplean únicamente conexiones mediante HTTPS (cifradas) desde el dispositivo móvil hacia múltiples servidores de Google. Versiones pasadas de los servicios de localización de Google enviaban tráfico no cifrado mediante HTTP.



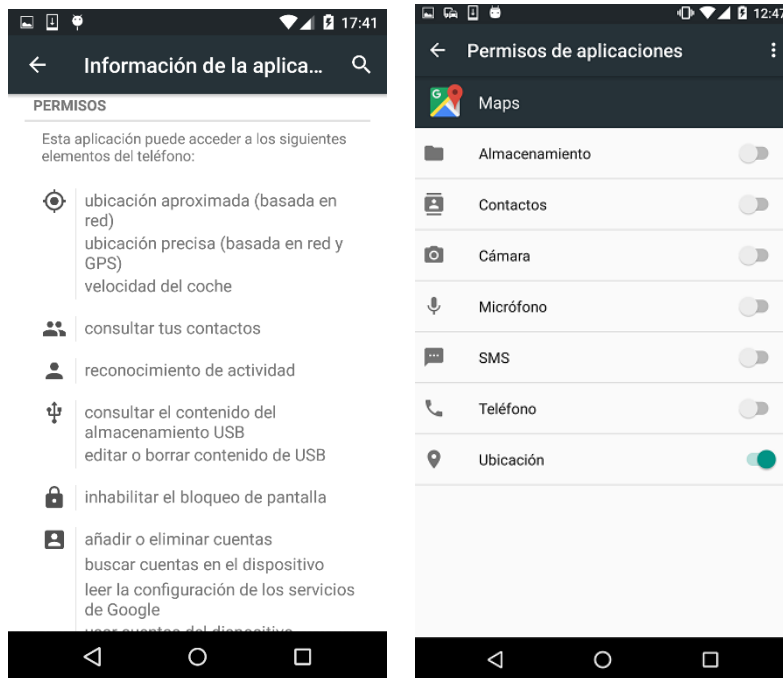
1062. Este cambio en el funcionamiento respecto al comportamiento de versiones previas de la app y versiones previas de Android evita que un potencial atacante acceda fácilmente al tráfico de red y pueda obtener detalles de la ubicación del usuario y de las redes inalámbricas (como por ejemplo el nombre de red, SSID, y su dirección MAC, BSSID) y de las torres de telefonía móvil (como por ejemplo el identificador de torre, y los códigos de área (LAC), operador de telefonía móvil (MNC) y país (MCC)) existentes en el área de cobertura del dispositivo móvil.
1063. En versiones de Google Maps anteriores a 2017, se requería disponer de una conexión de datos (telefonía móvil o Wi-Fi) para funcionar y acceder a la información cartográfica de los mapas. Sin embargo, una de las capacidades que se añadieron a la aplicación Maps fue la de “zonas sin conexión”, que posibilita la navegación aunque no haya conexión de datos activa si se ha descargado previamente el mapa correspondiente a esa zona. Todos los detalles sobre el uso y configuración de las zonas sin conexión pueden consultarse en [Ref.- 227].
1064. A partir de la versión 9.12 de Google Maps para Android, se incorporó la opción de menú “Tu cronología” [Ref.- 228].
1065. Para crear la cronología, además de la ubicación, el historial de ubicaciones debe estar activo en “Ajustes - [Personal] Ubicación - [Servicios de ubicación] Historial de ubicaciones de Google” (consultar apartado 12.5. Historial de ubicaciones). Dado que esta opción se habilita para la cuenta de Google del usuario, el activarla implica que Google recordará la ubicación en todos los dispositivos en los que se inicie sesión con esa cuenta de Google. No obstante, se puede desactivar la opción correspondiente al dispositivo móvil si no se desea que los datos que se recopilen de él pasen a formar parte del historial de ubicaciones:



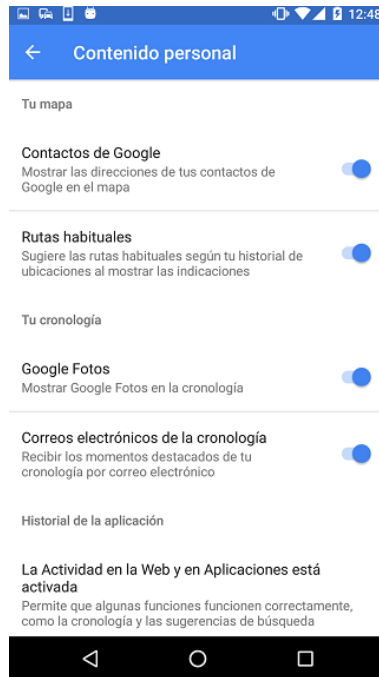
1066. Tal y como informa la nota que aparece en este menú, se enviarán a Google datos de ubicación de los dispositivos que tengan activa la opción del historial de ubicaciones, aunque no se esté utilizando ningún producto de Google.
1067. Si los servicios de ubicación están activos, el dispositivo móvil compartirá la ubicación con las aplicaciones que tengan permiso para ello.



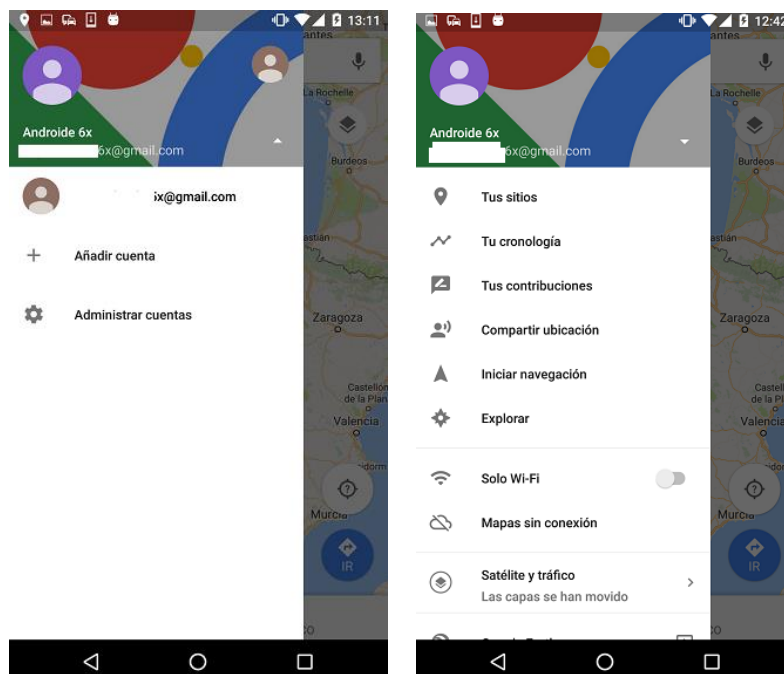
1068. Con el cambio en el modelo de permisos de Android, la aplicación Maps dejó de tener concedidos por defecto permisos muy sensibles, como “inhabilitar el bloqueo de pantalla”, “añadir o eliminar cuentas”, “editar o borrar el contenido de USB”, como ilustra la imagen inferior izquierda. Para verificar qué permisos tiene concedidos en un momento dado en el dispositivo móvil, se recurrirá a “Ajustes - [Dispositivo] Aplicaciones - Maps - Permisos”. Para evitar potenciales vulnerabilidades de seguridad, se recomienda mantener la app actualizada y conceder únicamente el permiso de ubicación, que es el único que requiere para su correcto funcionamiento:



1069. Hay que resaltar que estos permisos hacen referencia a permisos de sistema, no a las capacidades que tiene la aplicación Maps para interactuar con otros servicios de Google (como Google Fotos) y que afectan directamente a la privacidad del usuario. Por ejemplo, la opción “Contactos de Google” disponible en “Maps - Ajustes - Contenido personal”, marcada por defecto, hará que las direcciones de los contactos de Google se muestren en el mapa:



1070. Si el dispositivo móvil tiene varias cuentas de usuario de Google dadas de alta, es posible seleccionar qué cuenta se utilizará para la actividad registrada por la app Maps. Para cambiar entre cuentas (o añadir una nueva), se deben abrir los ajustes de Maps y seleccionar la cuenta a emplear (en versiones anteriores de Google Maps, era preciso marcar la opción “Cerrar sesión en Google Maps” para poder acceder a la configuración de otra cuenta). Desde el menú desplegable de las cuentas dadas de alta en Maps es posible también añadir cuentas adicionales:

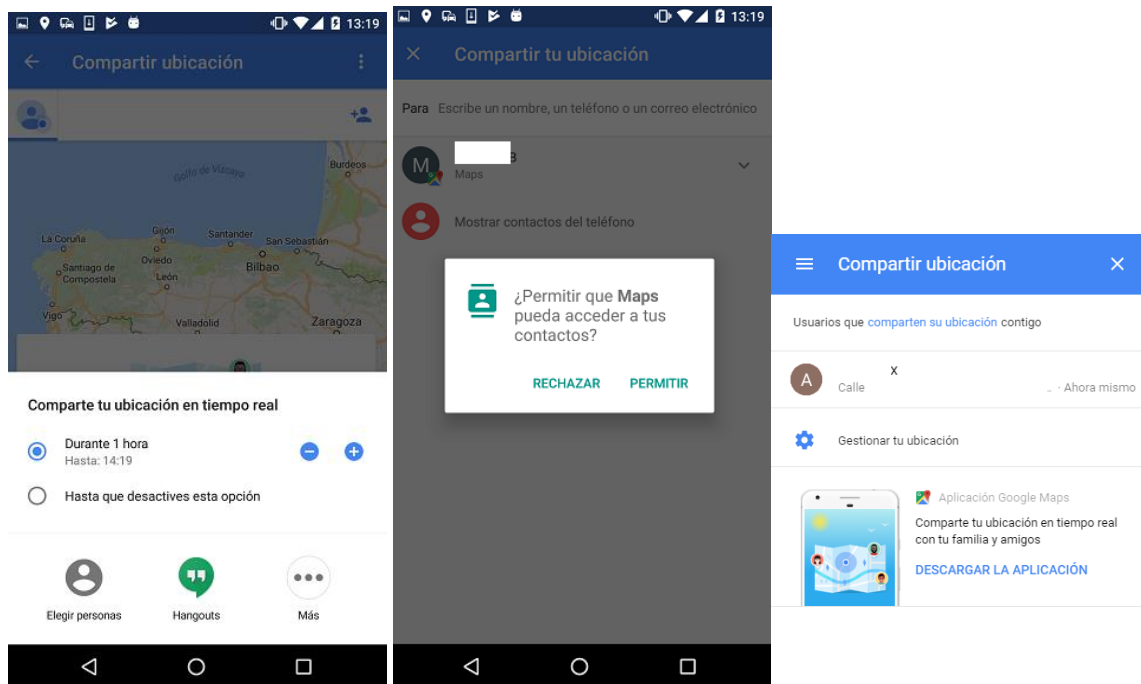


1071. La cuenta de usuario que está siendo utilizada por la app Maps es la que se muestra en la parte superior del menú de “Ajustes de Maps”, que figura tras el icono de un rostro.

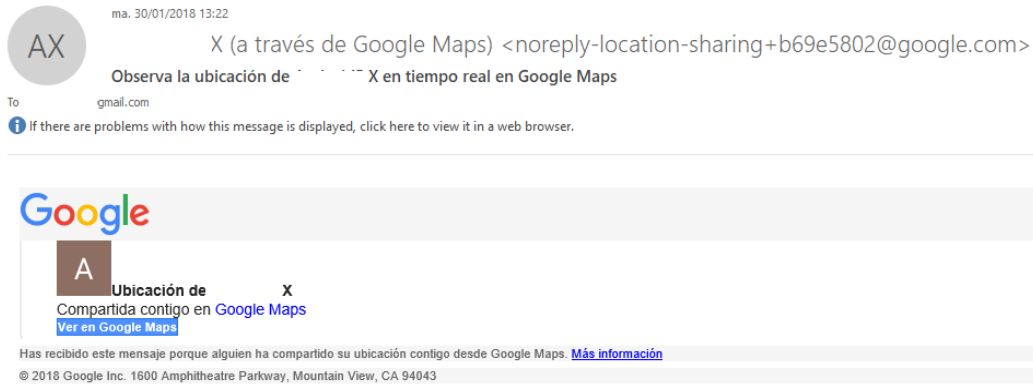
1072. Dada la sensibilidad de los datos que pueden recopilarse mediante Google Maps, y para preservar la privacidad del usuario, se recomienda deshabilitar el historial de ubicaciones y eliminarlo si ha estado activo en algún momento. Para ello, se puede

acceder al menú “Ajustes [Personal] - Ubicación [Servicios de ubicación] Historial de ubicaciones de Google” o emplear el menú “Ajustes de Maps - Ajustes de ubicación de Google”.

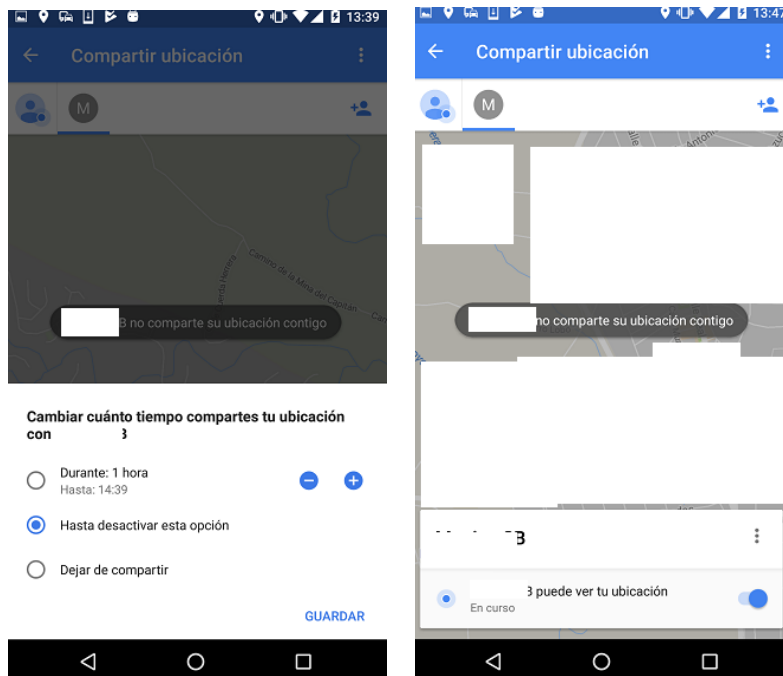
1073. Una opción que se añadió a la app Maps en las versiones posteriores a marzo del 2017 fue la de “Compartir ubicación” [Ref.- 230], que permite que el usuario comparta su posición geográfica con los contactos de su elección.
1074. Dicha opción permite conceder permisos para ver la ubicación en tiempo real del dispositivo durante el tiempo especificado por el usuario. Esta opción se habilita a través del menú de la app Maps denominado “Compartir ubicación”.
1075. Durante el proceso de compartición de ubicación, Maps solicitará al usuario acceso a sus contactos en el teléfono. Es importante reseñar que, aunque este permiso no se conceda, y que, por tanto, los contactos no se puedan recopilar de los contactos del teléfono, Maps sí tendrá acceso a los contactos que el usuario haya añadido a su cuenta de Google. Por tanto, el denegar acceso a los contactos no implica que la app Maps pueda consultarlos a través de la cuenta de Google activa:



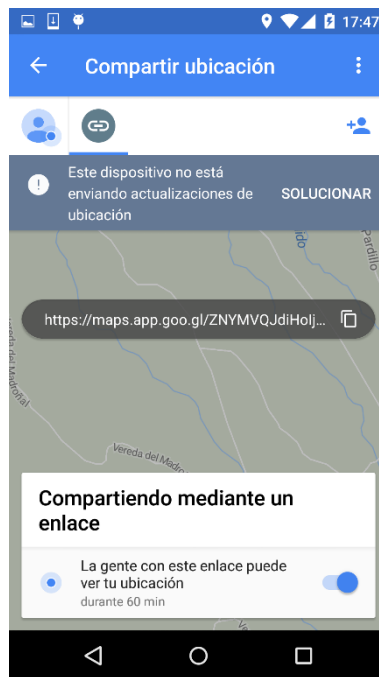
1076. Si se desea compartir la ubicación con un contacto, éste ha de disponer de una cuenta de usuario de Google. En ese caso, el usuario con el que se ha compartido la ubicación recibirá un mensaje de correo en su cuenta de Gmail que le informa de que otra persona ha compartido su ubicación con él:



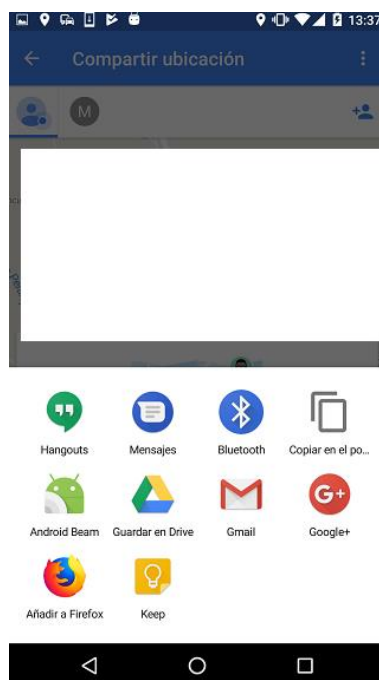
1077. En versiones anteriores de Maps, la compartición de la ubicación con otros usuarios tenía una duración de 1 hora (por defecto) y de un máximo de 72 horas. En la versión empleada para la elaboración de la presente guía, no hay un máximo de tiempo definido, sino un interruptor que desactiva la compartición:



1078. Si el contacto no dispone de una cuenta de usuario de Google o no se desea hacer uso de ella para acceder a la ubicación del dispositivo, se ha de crear un enlace mediante el menú de la app Maps, "Compartir ubicación - Más - Copiar en el portapapeles". Seguidamente, se puede compartir el enlace creado mediante la aplicación o servicio que se desee, y así se dará acceso a la ubicación durante un máximo de 1 hora.



1079. Es posible también elegir una aplicación de mensajería instalada en el dispositivo móvil para compartir la ubicación seleccionando la misma a través del menú de la app Maps, “Compartir ubicación - Más - [seleccionar la aplicación de la lista mostrada]”.



1080. Para poder compartir la ubicación, es necesario habilitar el historial de ubicaciones, tal como se informa en el mensaje que aparece al intentar compartir la ubicación.



1081. Las opciones de uso de la opción “Compartir ubicación” están disponibles en la ayuda oficial de Google Maps en tiempo real [Ref.- 231].
1082. Por cuestiones de privacidad, se recomienda no hacer uso de esta funcionalidad. En caso de requerirse por alguna circunstancia, se debe verificar que el canal de compartición es seguro y limitar el acceso en tiempo a la misma todo lo posible.
1083. Por cuestiones de privacidad, no se recomienda en absoluto dar de alta la dirección de casa o del trabajo en el área de “Ajustes de Map - Ajustes - Editar casa o trabajo”.
1084. El resto de opciones de uso de la app Maps para navegación quedan fuera del alcance de la presente guía, pero se puede obtener información detallada al respecto en la “Ayuda de Google Maps” [Ref.- 229].

### 12.3. A-GPS

1085. *Assisted GPS* (A-GPS o aGPS) es un sistema de ayuda para mejorar la obtención de información y la precisión de los datos de localización obtenidos mediante GPS, que permite disponer de una estimación de la ubicación del dispositivo móvil más rápidamente.
1086. Especialmente A-GPS permite agilizar significativamente el tiempo necesario para ubicar inicialmente el dispositivo móvil, parámetro conocido como TTFF (Time-To-First-Fix).
1087. El módulo A-GPS está (teóricamente) disponible en dispositivos móviles Android con GPS, especialmente cuando se hace uso del modo de alta precisión.
1088. El sistema A-GPS es un sistema híbrido que se basa en obtener información de las torres de telefonía móvil detectadas desde la ubicación del dispositivo móvil (y que proporcionan información auxiliar o de asistencia sobre la ubicación), y adicionalmente, hace uso de las conexiones de datos (habitualmente 2/3/4G, o Wi-Fi) del dispositivo

móvil para obtener información actualizada de dónde se encuentran los diferentes satélites GPS en un momento temporal (información con datos de las órbitas y de sincronización - reloj - de los satélites, conocido también como almanaque).

1089. Por tanto, la funcionalidad A-GPS también es visible a través del tráfico de datos del dispositivo móvil. Android 6.x, en diferentes momentos temporales como por ejemplo durante el proceso de arranque del dispositivo móvil, envía tráfico no cifrado hacia los servidores de gpsOneXTRA (ver apartado “12.4. gpsOneXTRA”).
1090. Debe tenerse en cuenta que, pese a que el uso del módulo GPS está siempre habilitado por defecto si los servicios de ubicación están activos, salvo que se haga uso del modo de ahorro de batería, hay escenarios en los que no es posible obtener señal de GPS (por ejemplo, en el interior de edificios), por lo que las apps como Maps harán uso automáticamente de las capacidades de ubicación sin hacer uso del módulo GPS si estas han sido habilitadas, por ejemplo, en el modo de alta precisión.
1091. En resumen, se recomienda deshabilitar la funcionalidad A-GPS mediante la activación del modo “Solo en dispositivo” salvo que se quiera hacer uso explícito de estas capacidades, con el objetivo de evitar desvelar información de la ubicación del dispositivo móvil (por ejemplo, torres de telefonía móvil o redes Wi-Fi cercanas) a través del tráfico de datos cifrado destinado a los servidores de Google.

## 12.4. GPSONEXTRA

1092. Con el objetivo de agilizar el proceso de localización, complementando las coordenadas obtenidas del módulo GPS y su precisión, los dispositivos móviles Android pueden disponer de la funcionalidad asociada a la asistencia mediante gpsOneXtra (aplicación conocida como QuickGPS en otras plataformas móviles).
1093. Hasta Android 5.x inclusive, esta funcionalidad se conectaba a un servidor web del dominio “gpsoneextra.net” (xtra1, xtra2 ó xtra3) para descargar la información semanal de la localización de los satélites GPS alrededor del planeta (o almanaque). Por defecto, la descarga automática de esta información está habilitada en Android. A partir de Android 6.x, la conexión se realiza con servidores web del dominio “izatcloud.net” (en el ejemplo utilizado para la presente guía, concretamente con el servidor “xtrapath1”).
1094. La descarga se lleva a cabo mediante el protocolo HTTP (TCP/80), sin cifrar, hacia los servidores de “izatcloud.net” mencionados previamente, descargándose el fichero “/xtra2.bin”. Para ello, Android emplea el siguiente agente de usuario que permite identificar el tipo de cliente: “User-Agent: Android”.

```
GET /xtra2.bin HTTP/1.1
Accept: */*, application/vnd.wap.mms-message, application/vnd.wap.sic
x-wap-profile:
http://www.openmobilealliance.org/tech/profiles/UAPROF/ccppschema-20021212#
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0.1; Nexus 5X Build/MTC20K)
Host: xtrapath1.izatcloud.net
Connection: close
Accept-Encoding: gzip, deflate
```

**Nota:** La configuración interna de Android tanto del servidor de tiempos NTP (ver apartado “19.2. Seguridad en TCP/IP”), como de los servidores de gpsOneXTRA y A-GPS (ver apartado “12.3. A-GPS”) está disponible en el fichero “/system/etc/gps.conf”, aunque no se dispone



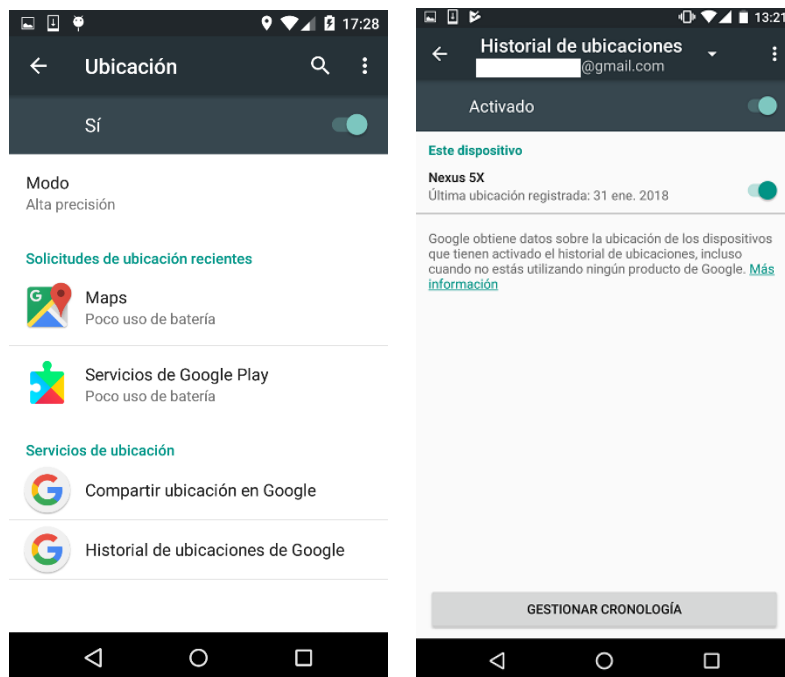
de ningún ajuste de configuración a través del interfaz gráfico de usuario de Android para modificar estos parámetros. Ejemplo (parcial) del fichero “gps.conf”:

```
XTRA_SERVER_1=http://xtrapath1.izatcloud.net/xtra2.bin
XTRA_SERVER_2=http://xtrapath2.izatcloud.net /xtra2.bin
XTRA_SERVER_3=http://xtrapath3.izatcloud.net /xtra2.bin
```

1095. Las conexiones gpsOneXTRA (“xtrapathN.izatcloud.net”, TCP/80), para incrementar la precisión de localización del GPS, se llevan a cabo (por ejemplo) cada vez que se enciende el dispositivo móvil y éste dispone de acceso a Internet.
1096. A finales del año 2016 se identificó una vulnerabilidad de denegación de servicio que afectaba a los dispositivos móviles Android y que podía ser explotada mediante la manipulación de los ficheros de posicionamiento obtenidos mediante el servicio gpsOneXtra [Ref.- 223].

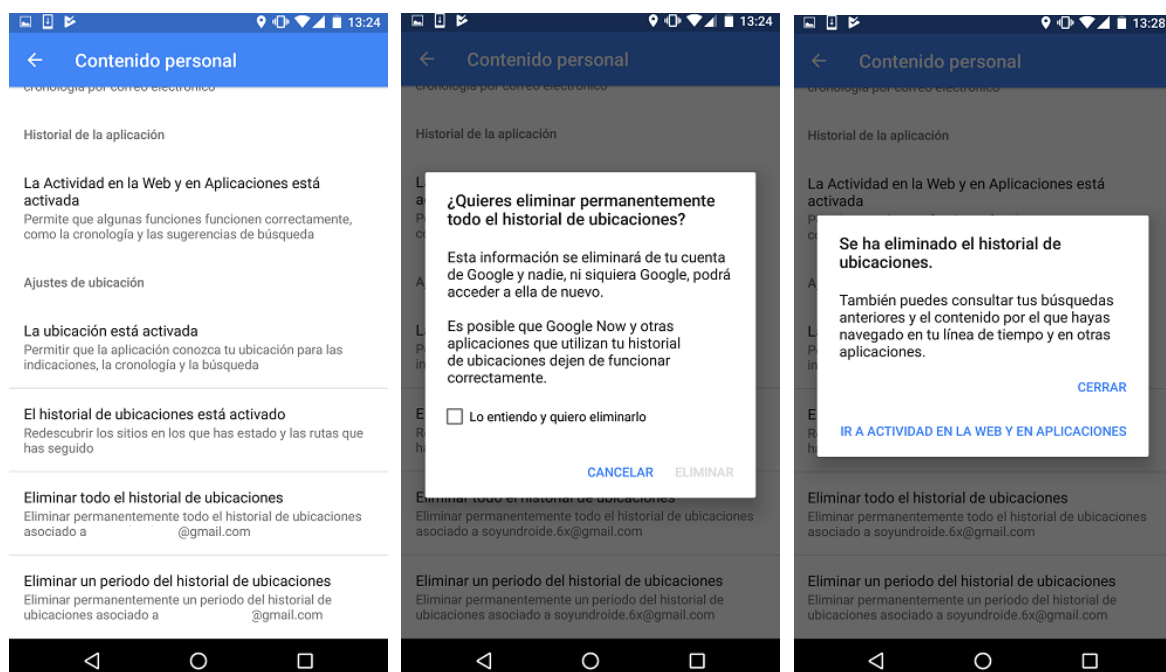
## 12.5. HISTORIAL DE UBICACIONES

1097. Los servicios de Google pueden hacer uso de los datos del historial de ubicaciones para, por ejemplo, mejorar los resultados de búsqueda de Google Maps (mediante la app Maps) en función de los sitios frecuentados habitualmente por el usuario [Ref.- 167].
1098. El historial de ubicaciones almacena un registro histórico de la ubicación del usuario procedente de todos los dispositivos móviles en los que el usuario haya iniciado sesión con su cuenta de usuario de Google. Para que se envíe la información al historial, y se pueda almacenar, el dispositivo móvil debe tener habilitado el historial de ubicaciones.
1099. El uso de la opción “historial de ubicaciones” permite a Google utilizar (y potencialmente almacenar) periódicamente los datos de ubicación más recientes del dispositivo móvil, así como la información sobre las actividades que conllevan movimiento (conducir, caminar, pasear en bicicleta, etc.) y asociarlos a la cuenta de usuario de Google, incluso aunque no se esté utilizando ningún producto o servicio de Google.
1100. La frecuencia con la que los informes de ubicación actualizan los datos de ubicación no es fija y depende de diferentes factores, como la batería del dispositivo móvil, si el usuario se está desplazando, o la velocidad a la que se desplaza.
1101. A través del menú “Ajustes [Personal] - Ubicación”, y de la sección “Servicios de Ubicación”, es posible seleccionar “Historial de ubicaciones de Google” y acceder a los ajustes de configuración para activar o desactivar el historial de ubicaciones de la cuenta de usuario de Google, tanto a nivel global como a nivel de dispositivo:

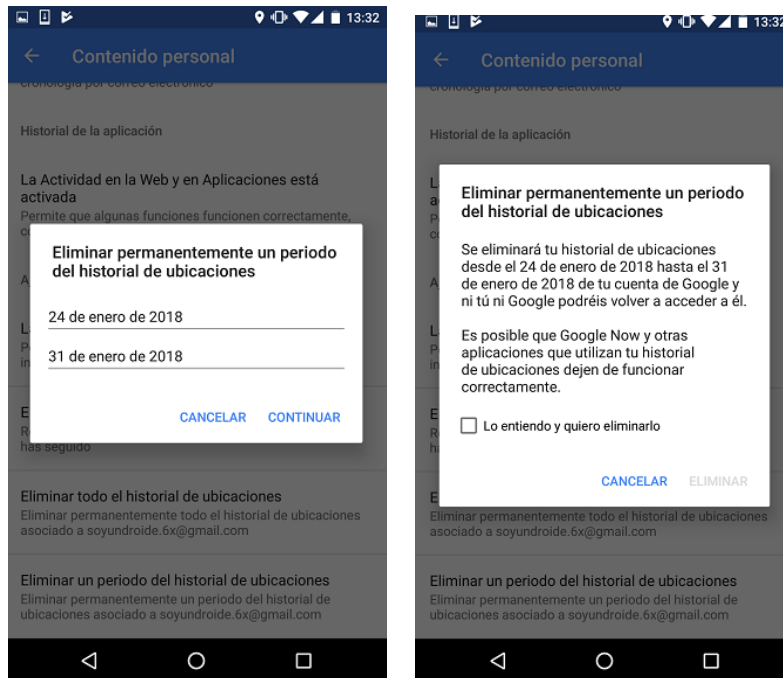


1102. La configuración del historial de ubicaciones está disponible a través del menú mencionado previamente, pero, aunque se desactive a través de las opciones descritas, no se eliminarán los datos recopilados hasta ese momento.

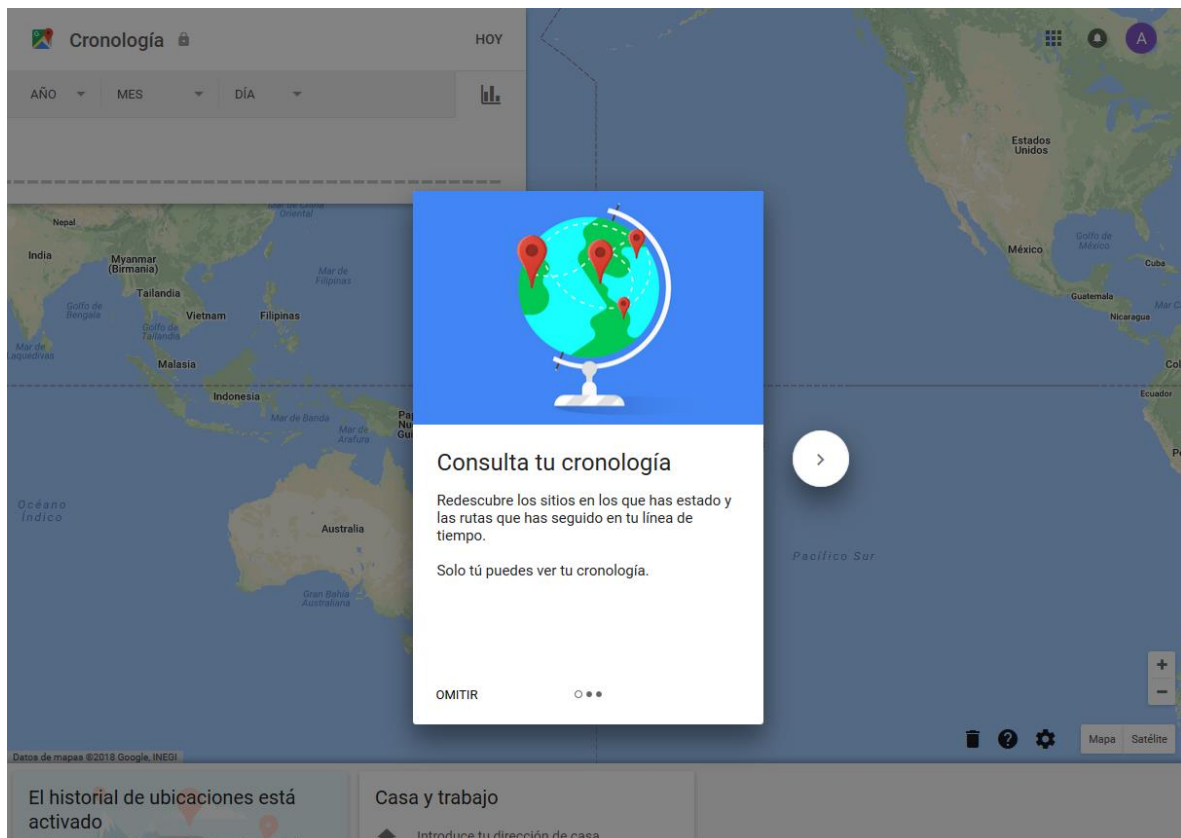
1103. Si se desea eliminar el histórico, es necesario acceder a “Ajustes - [Personal] Ubicación - [Servicios de Ubicación] Historial de ubicaciones de Google - <...> Ver/Administrar”, o, alternatively, pulsar en el botón “Gestionar Cronología”. Esto hará que se lance la app Maps (app empleada por defecto) en una ventana que muestra la ubicación actual y las demás ubicaciones registradas para el día actual; desde el menú “<...>” accesible desde la esquina superior derecha de la pantalla, se puede seleccionar “Ajustes - [Contenido personal] - Eliminar todo el historial de ubicaciones”. Tras aceptar el mensaje de confirmación, se borrarán los datos de ubicaciones previamente almacenados por Google:



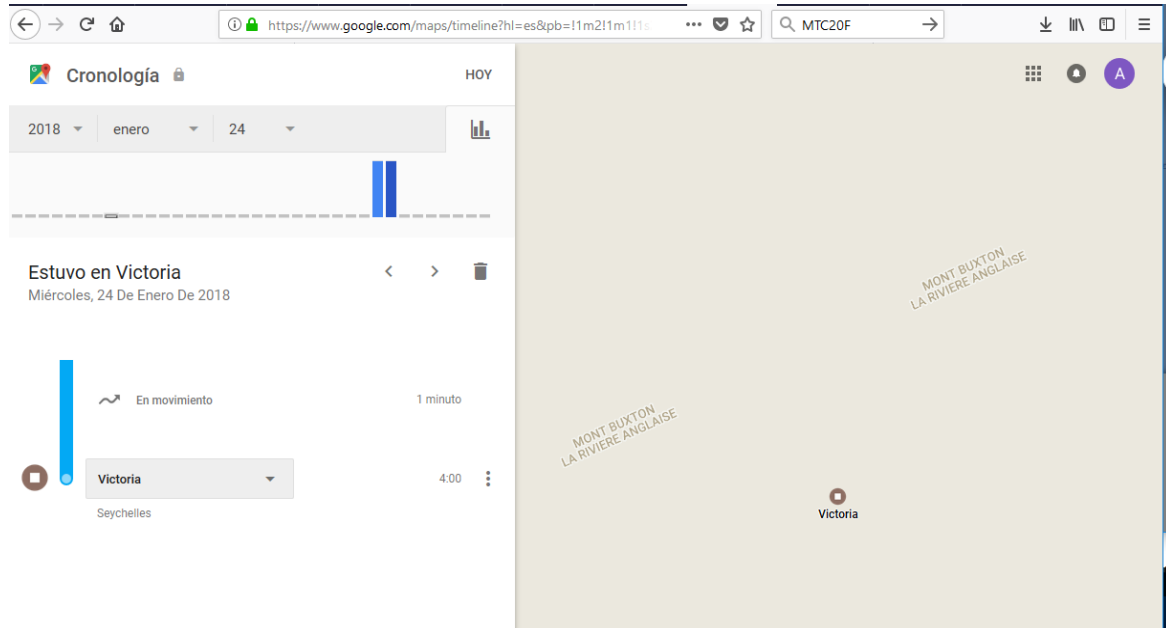
1104. También es posible eliminar un periodo concreto del historial, seleccionando la fecha de inicio y de fin.



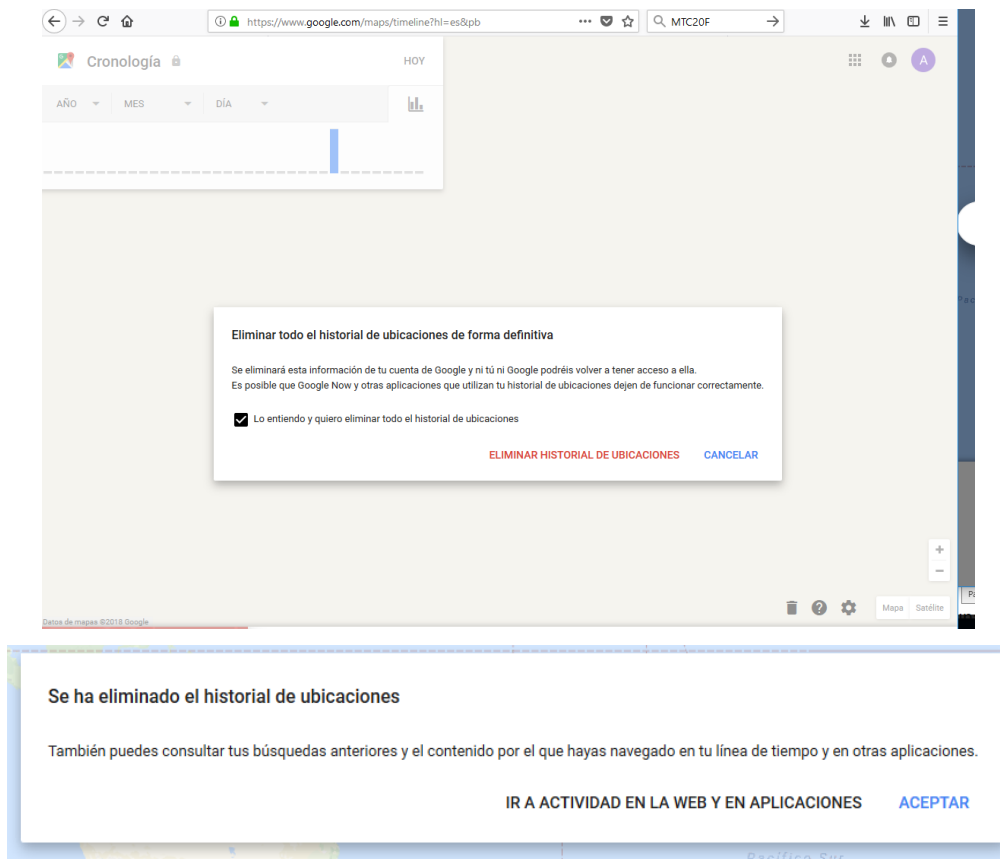
1105. Finalmente, un usuario puede también acceder y administrar el historial de ubicaciones vinculado a su cuenta de usuario de Google a través de la siguiente URL: "<https://maps.google.com/locationhistory/>". Esta funcionalidad está asociada al "Historial de la cuenta", disponible desde "<https://myaccount.google.com/activitycontrols>" (y que también permite el acceso al historial de actividad web y de aplicaciones, ver apartado "23.1.3. Historial de actividad web y de aplicaciones").

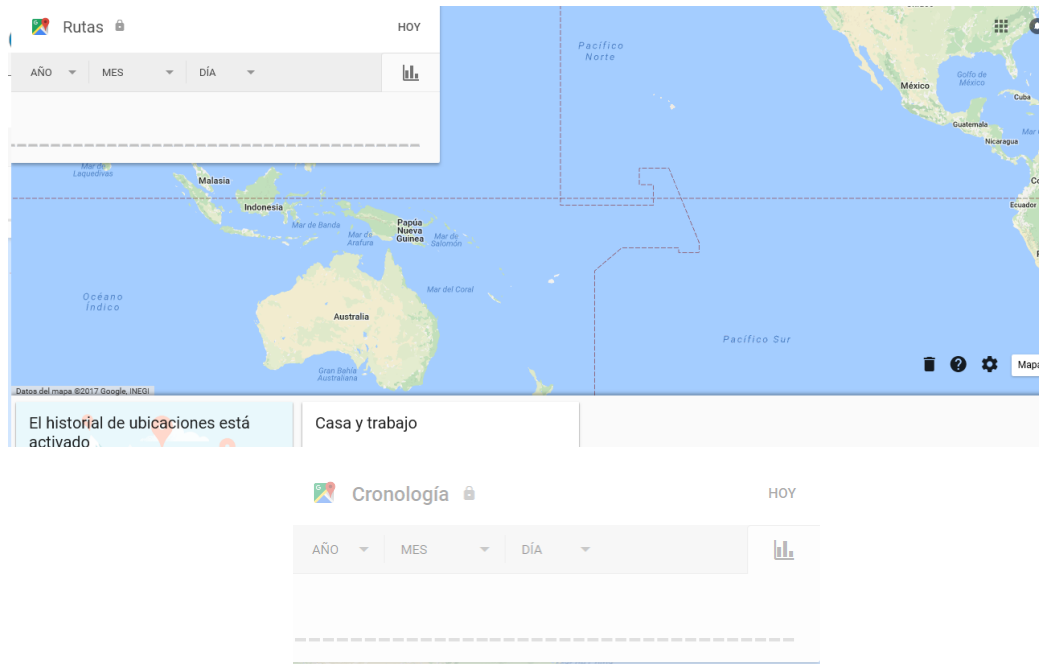


1106. Desde la misma es posible obtener los detalles de las ubicaciones registradas para el usuario, incluso clasificadas por fechas y horas, y obtener información de distancias entre ubicaciones:



1107. Desde las opciones situadas en el margen inferior derecho de la página web, es posible eliminar los registros del historial y pausar la recolección de datos. Cuando el historial ha sido eliminado, desde el dispositivo móvil o desde la página web, no se dispone de datos asociados a esta funcionalidad:





1108. En resumen, desde el punto de vista de seguridad, y, especialmente, de la privacidad del usuario, no se recomienda hacer uso del historial de ubicaciones (es decir, permitir a Google que almacene un histórico de todos los datos de ubicación). Adicionalmente, se recomienda borrar el historial de ubicaciones actualmente existente en la cuenta de usuario de Google.

## 12.6. OTRAS APPS QUE HACEN USO DE LA LOCALIZACIÓN

**Nota:** Queda fuera del alcance de la presente guía realizar un análisis detallado de seguridad de las diferentes apps que hacen uso de los servicios de localización de Google en Android, así como de la existencia de posibles vulnerabilidades en las mismas.

A continuación se muestran ejemplos de algunas apps existentes por defecto que hacen uso de los servicios de localización. Únicamente se recomienda verificar que las mismas hagan uso de tráfico cifrado mediante HTTPS, y si exponen o no los datos intercambiados entre ellas y los servidores remotos mediante tráfico no cifrado, normalmente empleando el protocolo HTTP. A modo de ejemplo, en algunos casos el valor del agente de usuario (o "User-Agent") desvelado por las apps proporciona numerosos detalles sobre la app y el dispositivo móvil asociado.

Se recomienda no hacer uso de apps o servicios que desvelan información detallada de la ubicación del usuario y del dispositivo móvil empleado, y que hacen uso de conexiones HTTP no cifradas, salvo que explícitamente se desee acceder a la información que éstos proporcionan. La mayoría de apps mencionadas requieren de una conexión de datos (telefonía móvil o Wi-Fi) para funcionar y acceder a la información necesaria para su funcionalidad.

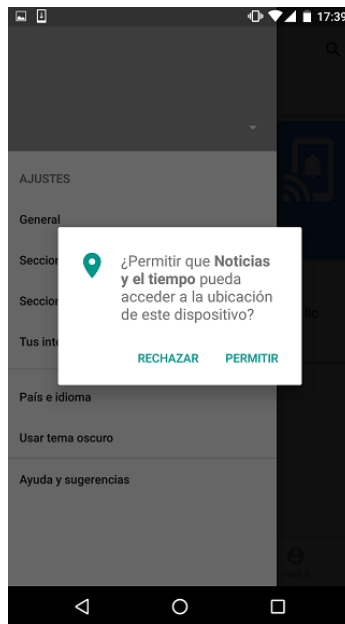
### 12.6.1. GOOGLE MAPS: NAVEGACIÓN

1109. Las capacidades de localización del dispositivo móvil también pueden ser empleadas por otras apps (adicionalmente a la app Maps), o por funcionalidades adicionales de

apps existentes, como por ejemplo las capacidades de navegación dentro de la app Maps<sup>71</sup>, que en Android 6.x están integradas dentro de dicha app y hacen uso de HTTPS.

### 12.6.2. NOTICIAS Y EL TIEMPO

1110. La app “Noticias y el tiempo”, que proporciona noticias informativas e información meteorológica (tiempo), disponible también como componente dentro de los servicios de Google Now, hace uso de las capacidades de localización de Android, y solicita para ello el permiso correspondiente a ubicación cuando se lanza por primera vez.

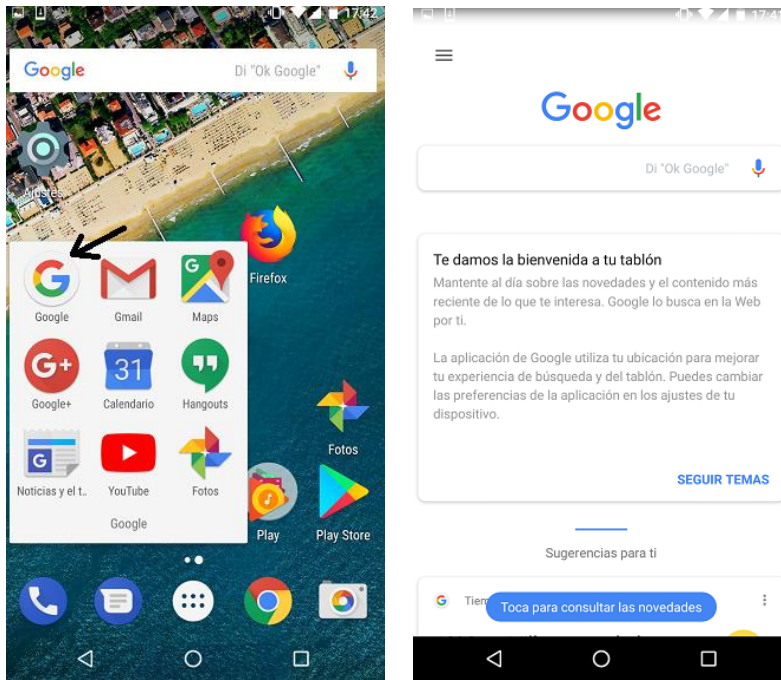


### 12.6.3. BUSCADOR DE GOOGLE

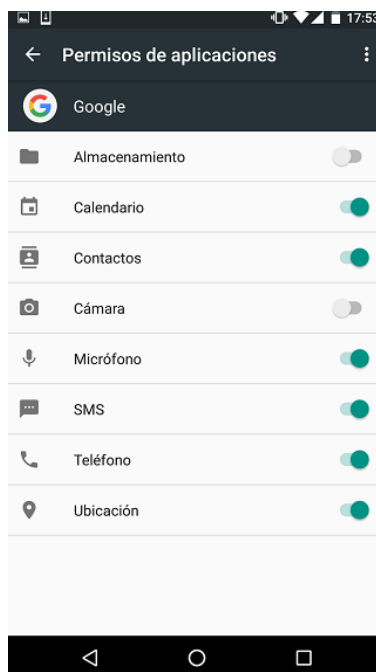
1111. La app “Google”, que proporciona acceso directo al buscador de Google y a otros servicios de la compañía, puede hacer uso también de los servicios de localización, integrándolos directamente en sus búsquedas y en las capacidades de notificaciones personalizadas asociadas a la actividad del usuario.

1112. El buscador de Google está integrado en la aplicación “Google”, y se accede a él pulsando en la barra de búsqueda situada bajo el banner “Google”:

<sup>71</sup> <http://www.google.com/mobile/maps/>

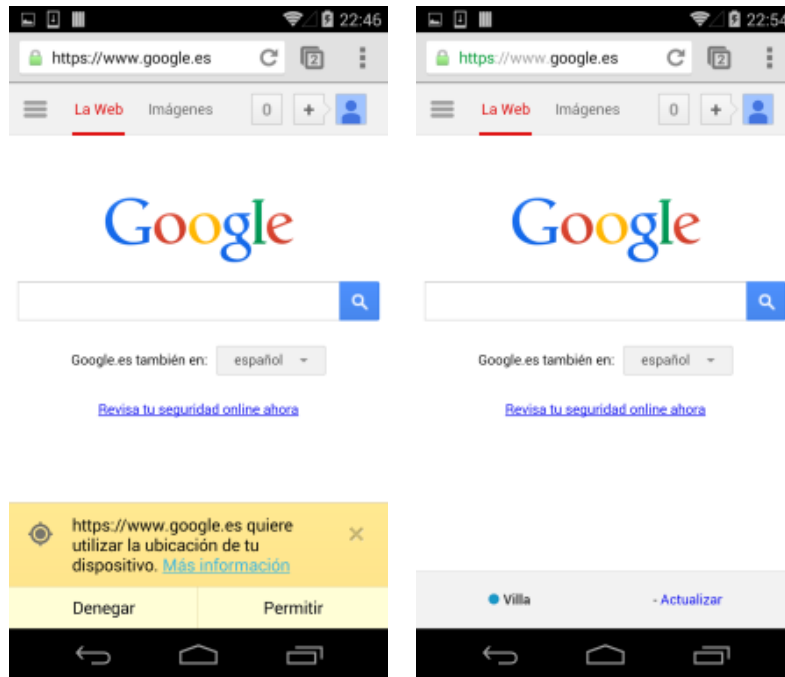


1113. Android concede a la app Google durante su instalación multitud de permisos, entre los que se encuentra el de ubicación. Se recomienda deshabilitarlo salvo que se requiera por alguna causa:



1114. En versiones anteriores de Android, el acceso al buscador de Google directamente desde el navegador web de Android (descrito posteriormente en el apartado “12.6.5. Navegador web”), solicitaba al usuario utilizar la ubicación del dispositivo móvil, pudiendo éste permitir o denegar dicho acceso (dicho comportamiento se ilustra en las imágenes siguientes). Sin embargo, con Android 6.x y las versiones más recientes del navegador web y de la app Google, el permiso de ubicación está concedido por defecto para ambas, por lo que ya no lo solicitan explícitamente al usuario.





1115. Los permisos habilitados anteriormente para ciertos sitios web pueden ser modificados posteriormente (ver apartado “12.6.5. Navegador web”).

#### 12.6.4. REDES SOCIALES

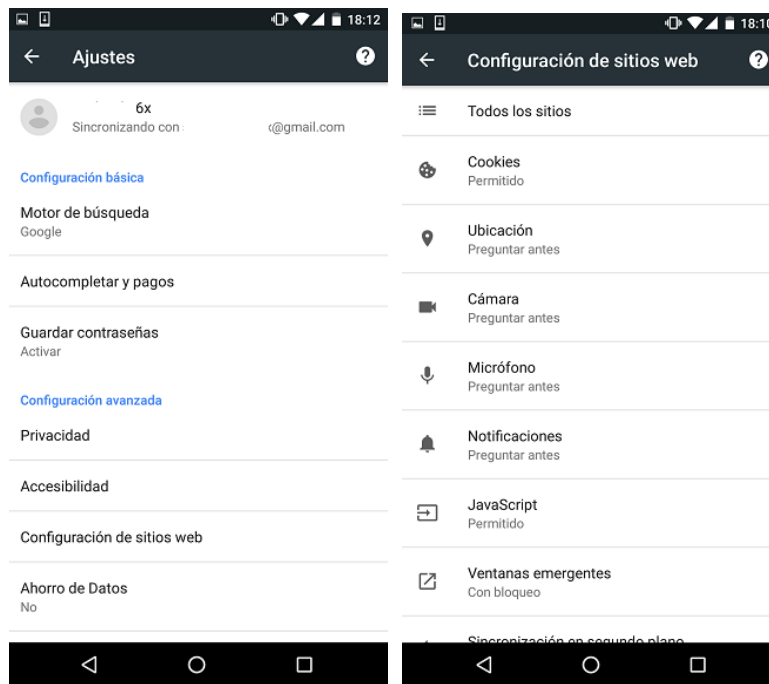
1116. La información de localización puede integrarse también con las apps de acceso a redes sociales, siendo posible la publicación de la ubicación del usuario a través, por ejemplo, de Twitter o Facebook.

1117. Debido a que las apps asociadas a estas redes sociales no están disponibles por defecto en Android 6.x (sí lo estaban en versiones previas de Android), no se profundizará en los detalles centrados en deshabilitar el uso de los servicios de localización desde las mismas.

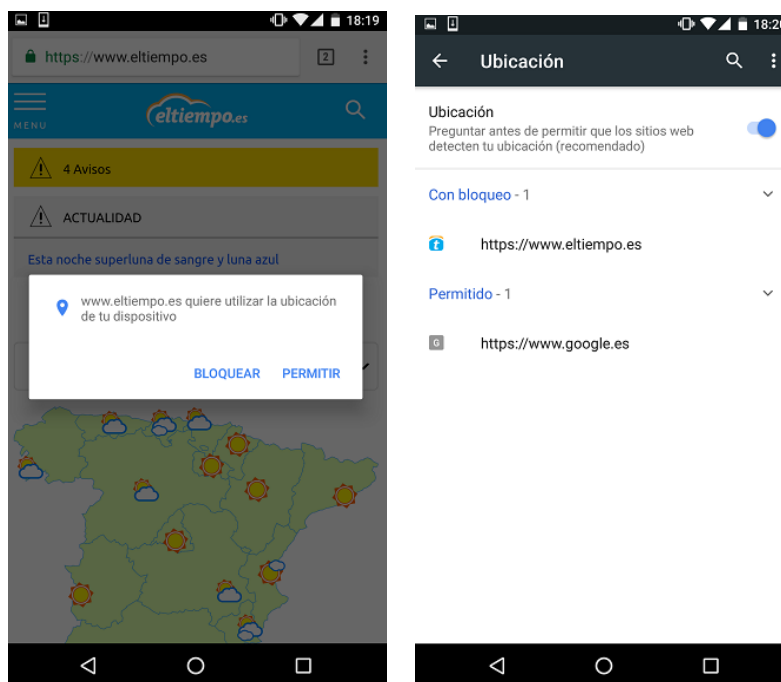
1118. Desde el punto de vista de seguridad, se recomienda no hacer pública la ubicación en la que se encuentra el usuario en redes sociales o servicios avanzados similares con el objetivo de proteger su privacidad.

#### 12.6.5. NAVEGADOR WEB

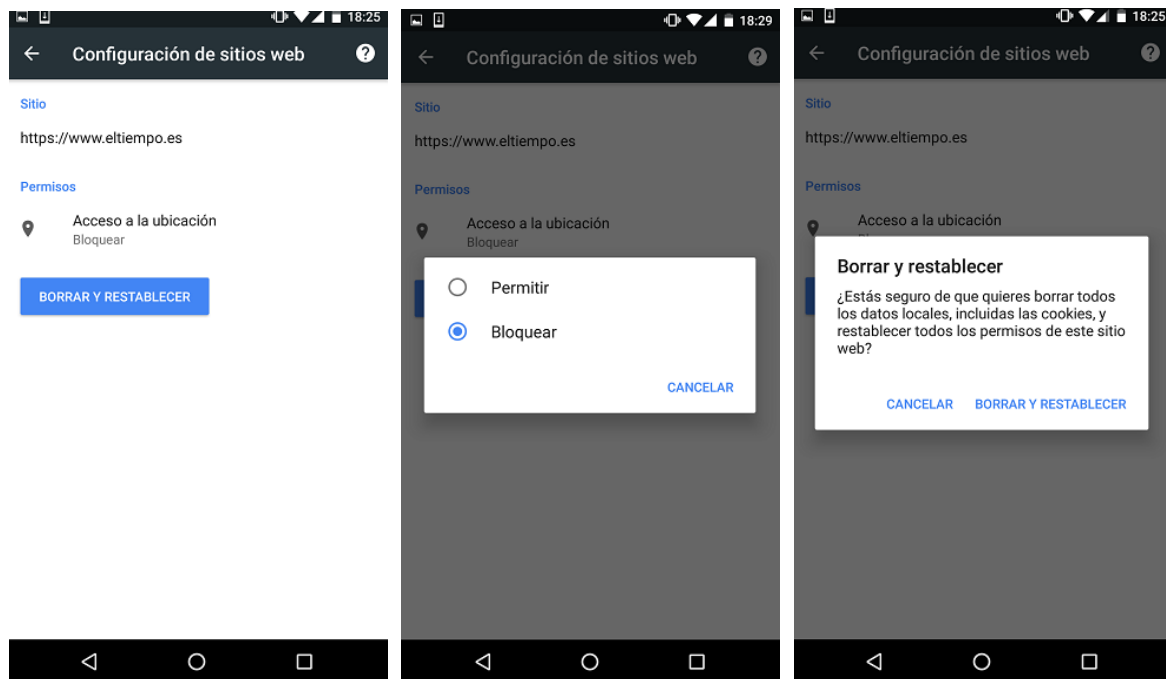
1119. El navegador web existente por defecto en Android, Chrome, permite autorizar el acceso a la información de localización (o ubicación del dispositivo móvil) o bloquearlo de manera general. Para ello, se ha de acceder al menú de “Ajustes” de “Chrome”, y en concreto a través de la opción “Ajustes - [Configuración avanzada] Configuración de sitios web - Ubicación”. La opción asociada permite que se solicite al usuario autorización cuando una página web trate de detectar la ubicación del usuario o, si se desactiva, bloquear cualquier solicitud de ubicación por parte de cualquier página web. Esta opción sólo entrará en juego si Chrome tiene concedido el permiso de ubicación a nivel de aplicación en los ajustes de configuración de Android.



1120. Si Chrome tiene permiso de ubicación y la opción “Ubicación - Preguntar antes” está activa, tan pronto se visite una página web que solicite acceso a la ubicación del usuario, se creará bajo el menú anterior la lista “Permitido” (si se concedió acceso) o la lista “Con bloqueo” (si se denegó el acceso).



1121. Los permisos de acceso a la ubicación habilitados anteriormente para ciertos sitios web pueden ser modificados posteriormente desde el menú de “Ajustes” de “Chrome”, y en concreto a través de la opción “Ajustes - [Opciones avanzadas] Configuración de sitios web - Ubicación”. Android dispone de capacidades granulares para alterar el acceso a la información de localización para cada sitio web. Tras seleccionar un sitio web concreto, se puede cambiar su permiso “Acceso a la ubicación” seleccionando el nombre del sitio y eligiendo entre las opciones “Permitir” o “Bloquear”:



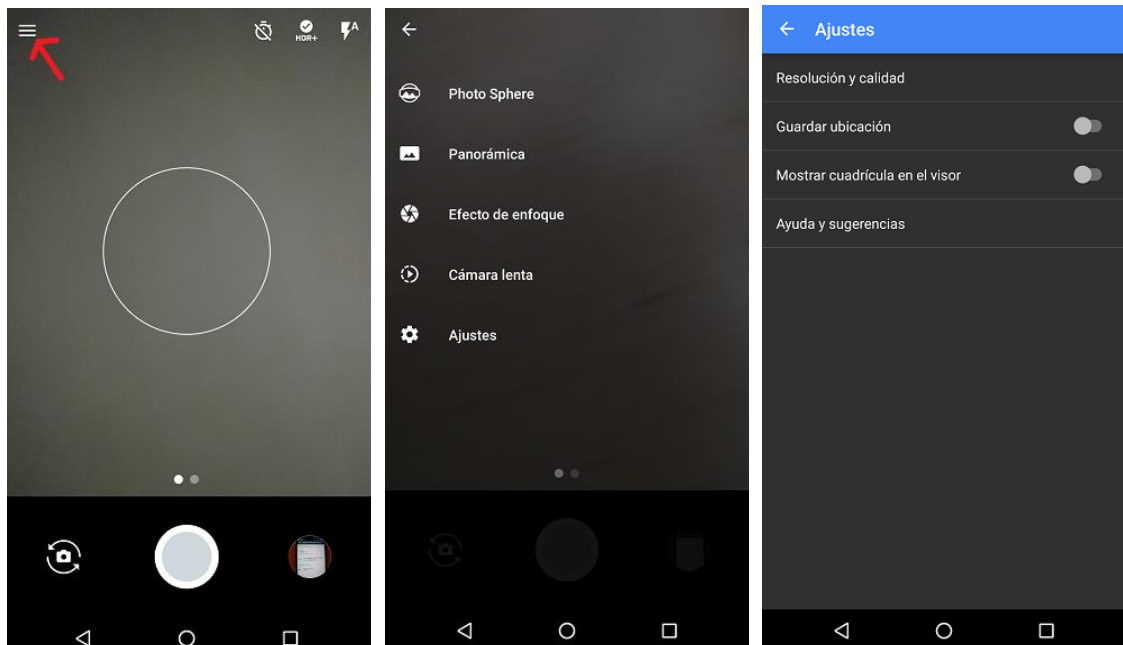
1122. El botón “borrar y restablecer” provocará que se elimine la configuración de permisos asociada al sitio web, además de borrar sus cookies.
1123. Desde el punto de vista de seguridad se recomienda deshabilitar la opción “Ubicación” para todos los sitios web, con el objetivo de no permitir a ningún sitio web disponer de acceso a la información de localización, incluso aunque tuvieran este acceso previamente permitido de manera individual.

## 12.7. INFORMACIÓN GEOGRÁFICA EN FOTOGRAFÍAS

1124. Android permite añadir información de la localización geográfica a las fotografías y vídeos realizados con la cámara del dispositivo móvil. Al realizar la fotografía (o vídeo) se añaden las coordenadas GPS en el momento de tomar la instantánea a la cabecera EXIF de la imagen.
1125. La primera vez que se ejecuta la app “Cámara” se pregunta al usuario si desea etiquetar las fotografías y vídeos con la información de la ubicación dónde se han realizado (opción habilitada por defecto), información también accesible para otras apps:



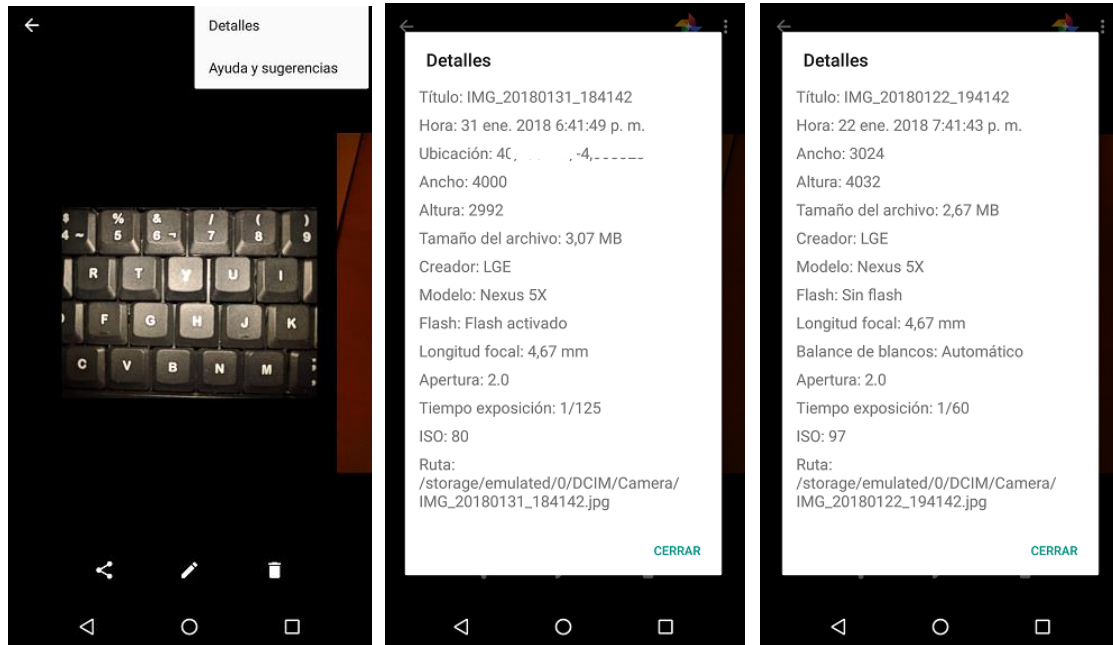
1126. Desde el punto de vista de seguridad se recomienda deshabilitar esta funcionalidad con el objetivo de no desvelar detalles de las ubicaciones del usuario.
1127. Esta funcionalidad puede ser habilitada y deshabilitada en cualquier momento a través del menú de configuración de la cámara. Para ello es necesario abrir la cámara mediante la app “Cámara” desde el *Launcher*, pinchar en el menú de ajustes señalado con una flecha en la siguiente imagen y seleccionar “Ajustes”:



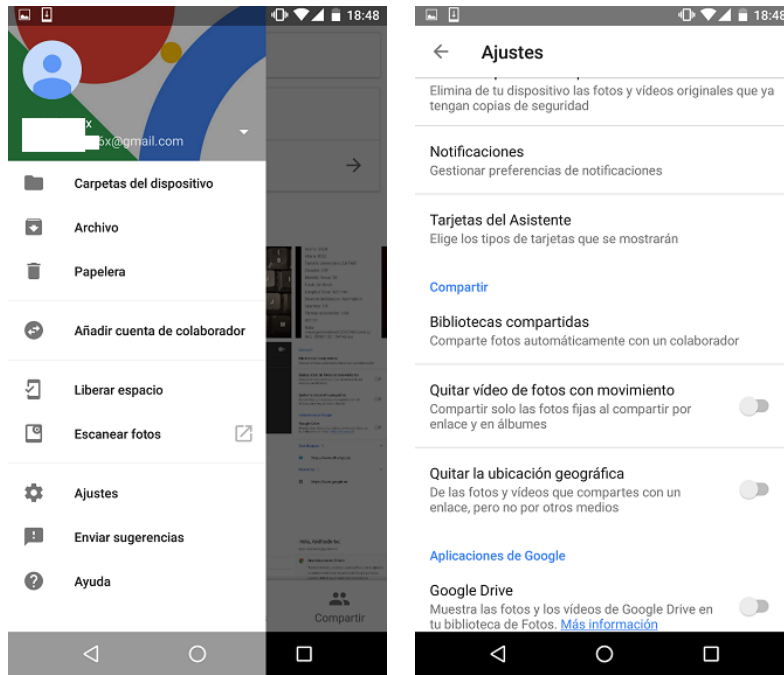
1128. La opción “Guardar ubicación” permite habilitar o deshabilitar esta funcionalidad. En caso de elegir su almacenamiento, la app “Cámara” guarda las coordenadas GPS que tenía el dispositivo en el momento de tomarse la fotografía.
1129. Los detalles de ubicación de las fotografías pueden ser visualizados desde el dispositivo móvil Android, y en concreto, desde la galería de imágenes de la cámara. La galería está disponible tanto desde la app “Cámara”, desplazando desde la derecha hacia la izquierda la imagen de la cámara, o también desde la app “Fotos” (en versiones

anteriores de Android, existía también la app “Galería”, pero en Android 6.x ya no está disponible, y la funcionalidad que ésta tenía asociada se integra dentro de la app “Fotos”).

1130. Para ello es necesario emplear el botón de menú, y la opción “Detalles” (ejemplo asociado a la app “Cámara”):



1131. El campo “Ubicación” (al comienzo de la lista de atributos de la imagen) indicará la ubicación dónde fue tomada (latitud y longitud). En caso de no disponer de la información de ubicación de la imagen, este campo o atributo no será mostrado.
1132. Respecto a la app “Fotos”, dentro de sus ajustes incluye una opción (“Quitar la ubicación geográfica”) que permite que, aunque una imagen o un vídeo hayan sido tomados con el permiso de ubicación activo para la cámara, al compartir dicho elemento a través de un enlace, se elimine la información de ubicación. Se recomienda activar dicha opción para evitar que la información de ubicación pueda compartirse inadvertidamente a través de otra app.



1133. Aunque dentro de los ajustes de la app “Fotos” Google sugiere utilizar la ubicación para facilitar la organización y la búsqueda de imágenes, se recomienda no hacer uso de la funcionalidad que incluye la información del GPS en fotografías o vídeos, especialmente para su publicación o distribución en Internet, salvo que se quiera hacer uso explícito de estas capacidades. En caso contrario, las imágenes y vídeos revelarán los detalles exactos de donde han sido tomadas.

### 13. COMUNICACIONES USB

1134. La conexión USB del dispositivo móvil a un ordenador proporciona dos funcionalidades o tipos de conexiones diferentes: [Ref.- 224]

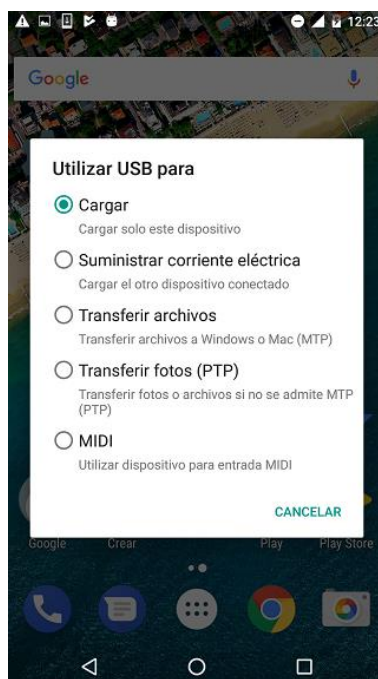
- Modo “accesory”: el uso principal que se hace de este modo es para que el dispositivo móvil Android se comporte como una unidad de disco, compartiendo la tarjeta de almacenamiento externa (en caso de disponer de una) y otras capacidades de almacenamiento internas desde el dispositivo móvil al ordenador.
  - Los dispositivos móviles Android que no disponen de una tarjeta de almacenamiento externa física, simulan su existencia compartiendo parte de las capacidades de almacenamiento internas del dispositivo móvil.
- Modo “host”: un ejemplo de utilización de este modo es la posibilidad de ofrecer la conexión de telefonía móvil de datos, o *tethering*, para compartir la conexión de datos 2/3/4G o Wi-Fi del dispositivo móvil con el ordenador.
  - La compartición de la conexión a Internet a través de USB o Bluetooth puede hacer uso tanto de la conexión de datos 2/3/4G como de la conexión Wi-Fi del dispositivo móvil. La compartición a través de Wi-Fi (punto de acceso o zona Wi-Fi) sólo puede hacer uso de la conexión de datos 2/3/4G, ya que el interfaz Wi-Fi no puede actuar simultáneamente de cliente y de punto de acceso.

1135. Ambas funcionalidades USB, “accesory” y “host”, no pueden ser utilizadas simultáneamente. En caso de estar usando las capacidades de *tethering*, éstas deben ser deshabilitadas para tener acceso al almacenamiento vía USB, y viceversa.
1136. El modo de conexión por defecto a través del puerto USB del dispositivo móvil es el de sólo carga (no disponiéndose de capacidades de intercambio de datos) [Ref.- 602]. Para poder transferir datos, el usuario debe seleccionar otro modo de conexión a través de la notificación correspondiente (es decir, seleccionando la notificación que informa del tipo de conexión USB que está activa en ese momento), no estando disponible esta opción desde el menú de “Ajustes [Dispositivo] - Almacenamiento & USB - [...] - Conexión USB a ordenador” (tal como sí ocurría en versiones previas de Android).

### 13.1. ALMACENAMIENTO USB

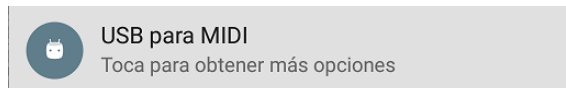
**Nota:** El acceso al dispositivo móvil como unidad de almacenamiento USB puede estar disponible incluso con el modo de depuración USB habilitado en Android. En caso de conflictos, si está habilitado, basta con deshabilitar este modo (opción recomendada desde el punto de vista de seguridad), para disponer únicamente de las capacidades de almacenamiento USB estándar. El modo de depuración se puede deshabilitar mediante el menú “Ajustes [Sistema] - Opciones de desarrollo” (una vez habilitadas), desactivando la opción “Depuración USB”.

1137. Para acceder a las capacidades de almacenamiento USB basta con conectar el dispositivo móvil al ordenador mediante el puerto USB. Como resultado, se generará una notificación correspondiente en la barra superior de estado, “USB para cargar”, ya que, por defecto, ésa es la acción configurada tan pronto se detecte la conexión USB. Este tipo de conexión no involucra ninguna transferencia de datos entre el ordenador y el dispositivo móvil.
1138. Para habilitar otros usos del puerto USB (el de carga se mantiene en paralelo a otros que se puedan seleccionar), se abrirá la notificación y se elegirá el modo deseado en el menú “Utilizar USB para”. Las opciones disponibles (además de “Cargar”) son:

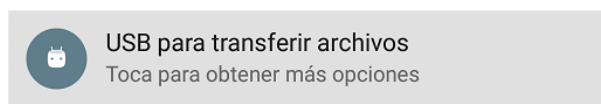




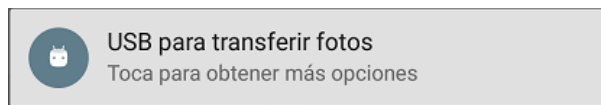
- “Suministrar corriente eléctrica”: en caso de querer que el dispositivo móvil se comporte como una fuente de alimentación para el otro equipo conectado vía USB.
- “MIDI”: esta opción se introdujo con Android 6.x, y permite conectar al dispositivo móvil un dispositivo tipo MIDI (como un teclado) a controlar por una app específica (como un sintetizador).



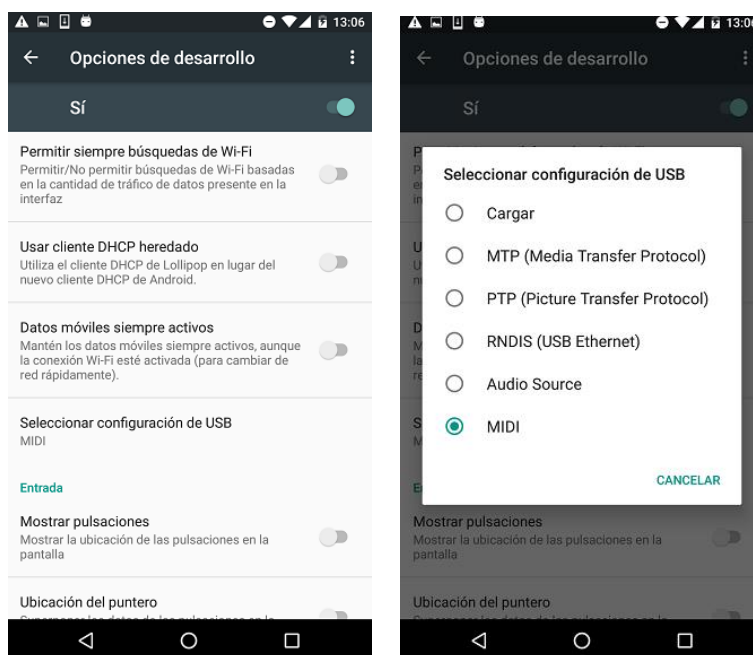
- “Transferir archivos”: a través del protocolo MTP (Media Transfer Protocol), se permite que el dispositivo móvil emule a un dispositivo multimedia que proporciona acceso a distintos tipos de ficheros a través de múltiples carpetas, incluyendo las de la cámara (descritas a continuación). Este tipo de conexión permite el intercambio de ficheros entre el dispositivo móvil y el otro dispositivo en ambas direcciones.



- “Transferir fotos”: a través del protocolo PTP (Photo Transfer Protocol), el dispositivo móvil emula una cámara de fotos (y/o vídeo) y proporcionará acceso únicamente a las fotos y vídeos desde dos carpetas, “DCIM” y “Pictures”.

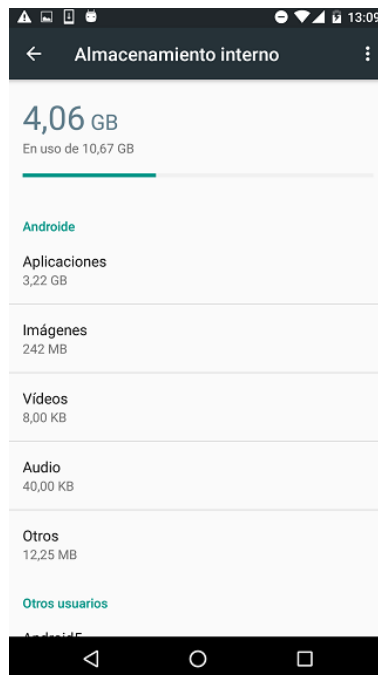


1139. También es posible seleccionar el modo de conexión del dispositivo a través del menú “Ajustes - [Sistema] Opciones de desarrollo - [Redes] Seleccionar configuración de USB”:



1140. La implementación de las capacidades de almacenamiento externo en el dispositivo móvil empleado para la elaboración de la presente guía (específicas en función del modelo de dispositivo móvil basado en Android), al no disponer de una tarjeta de

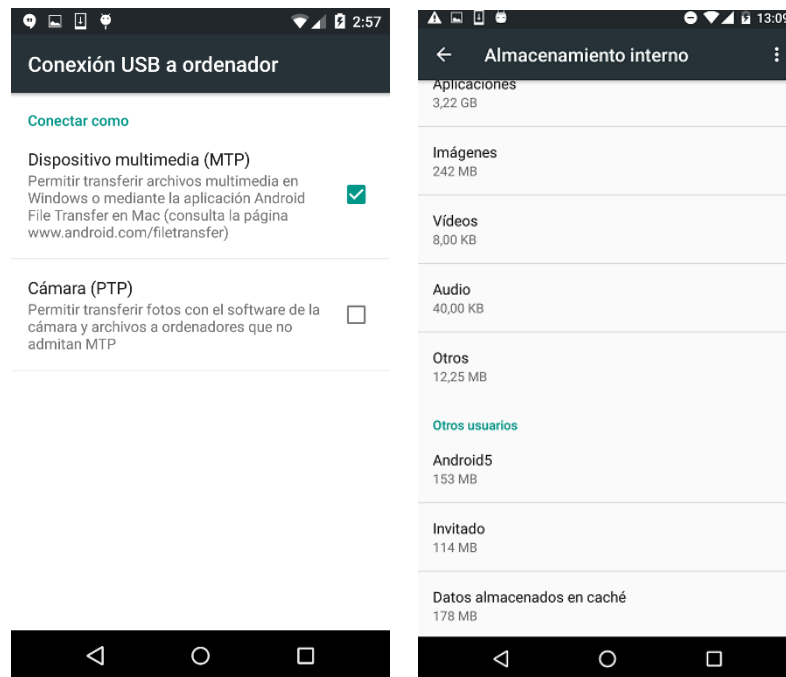
almacenamiento externa (o tarjeta SD) real o física (ver apartado “10.2. Almacenamiento adoptable”), no permiten acceder a esos contenidos como un sistema de almacenamiento masivo USB real (UMS, *USB Mass Storage*), no siendo por ejemplo posible asignar una letra de unidad en Windows a este espacio de almacenamiento. Sin embargo, esta limitación permite que tanto el dispositivo móvil como el ordenador puedan acceder simultáneamente al almacenamiento externo (virtual) del terminal. El acceso desde el dispositivo móvil se realiza accediendo a “Ajustes - [Dispositivo] Almacenamiento y USB”:



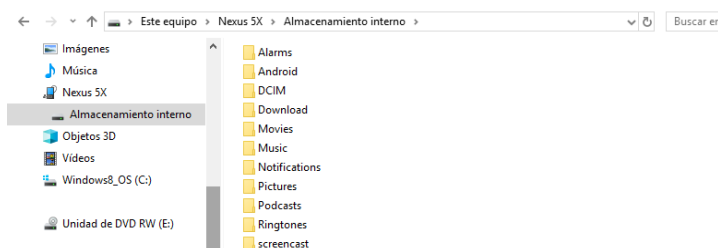
1141. Si se conecta una unidad de almacenamiento USB a través de la conexión USB del dispositivo móvil, Android montará dicha unidad con los siguientes parámetros:

```
shell@bullhead:/sdcard $ mount |grep media_rw
/dev/block/vold/public:8,1 /mnt/media_rw/5678-11AA vfat
rw,dirsync,nosuid,nodev,noexec,relatime,uid=1023,gid=1023,fmask=0007,dmask=0007,allow_utime=0020,codepage=437,iocharset=iso8859-1,shortname=mixed,utf8,errors=remount-ro 0 0
```

1142. Es posible seleccionar los dos modos de conexión mediante la interacción con la notificación, y la utilización de los botones correspondientes a ambos estados: “Dispositivo multimedia (MTP)” o “Cámara (PTP)”. Estas opciones también están disponibles a través del menú “Ajustes - [Dispositivo] Almacenamiento - [...] - Conexión USB a ordenador”:



1143. Tras arrancar el dispositivo móvil, si se ha establecido un código de acceso y éste aún no ha sido introducido, la conexión USB desde el ordenador permite identificar la presencia del dispositivo móvil, pero no proporciona de acceso a sus contenidos.
1144. Para poder acceder a sus contenidos es necesario al menos haber desbloqueado una vez el dispositivo móvil desde su arranque. Una vez desbloqueado al menos en una ocasión, ya es posible disponer de acceso a sus contenidos en cualquier momento, incluso aunque el dispositivo móvil se encuentre de nuevo bloqueado:



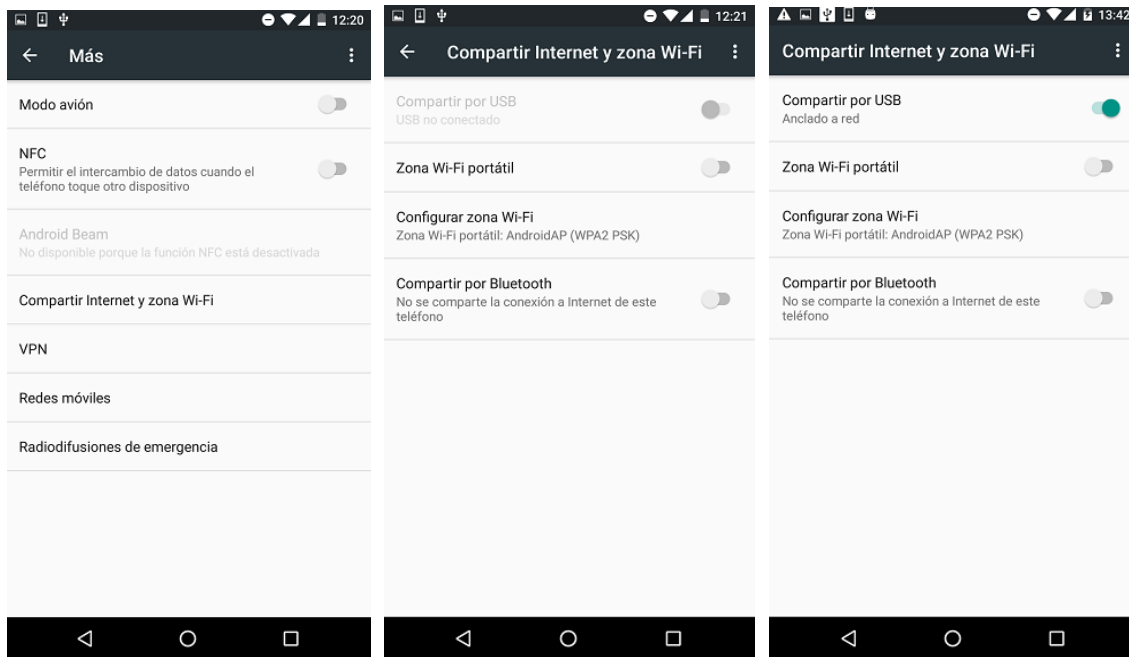
1145. La unidad de almacenamiento compartida con el ordenador corresponde a una sección denominada “Almacenamiento interno”, ya que, por ejemplo, el dispositivo móvil empleado para la elaboración de la presente guía no dispone de una tarjeta de almacenamiento externo (o tarjeta SD) física o real.
1146. Debe prestarse especial atención a la configuración de seguridad del ordenador, y en concreto, a los mecanismos de auto-ejecución de Windows (autorun y autoplay), para evitar la propagación de software malicioso (como por ejemplo el troyano Ambler u otros códigos dañinos, como en el caso de Vodafone y Android en 2010 [Ref.- 400] desde la tarjeta de almacenamiento externa del dispositivo móvil compartida con el ordenador.

## 13.2. CONEXIÓN DE RED COMPARTIDA POR USB (*TETHERING*)

1147. La opción de conexión compartida, o *tethering*, permite compartir la conexión de datos de telefonía móvil (2/3/4G) o Wi-Fi del terminal con un ordenador. Desde el punto

de vista de seguridad se recomienda hacer uso de *tethering* mediante cable USB, en lugar de mediante Bluetooth (en particular) o de Wi-Fi [Ref.- 94].

1148. Las capacidades de *tethering* (tanto por USB como por Bluetooth, ver apartado “15.7. Conexión de red compartida por Bluetooth”) y de punto de acceso Wi-Fi (ver apartado “16.6. Punto de acceso o zona Wi-Fi”) pueden ser utilizadas simultáneamente en Android, proporcionando conexión de red a otros dispositivos u ordenadores a la vez tanto por USB como por Bluetooth o por Wi-Fi:



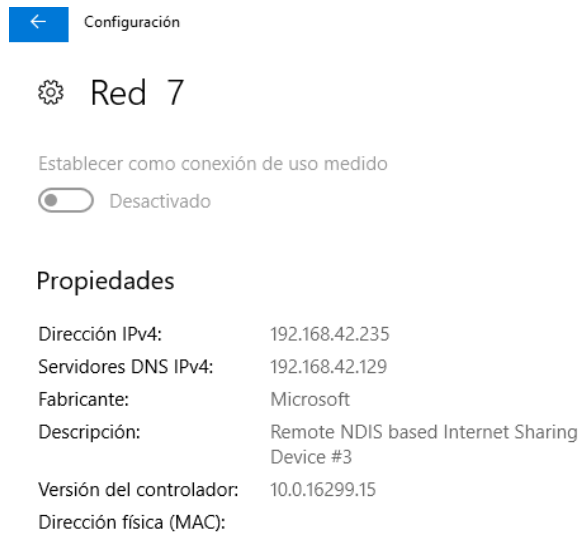
1149. Android proporciona capacidades nativas de *tethering* para Windows Vista/7/8/10<sup>72</sup> y Linux, pero no así para macOS. Para hacer uso de estas capacidades es necesario conectar el dispositivo móvil al ordenador mediante USB y acceder al menú “Ajustes [Conexiones Inalámbricas y Redes] - Más... - Compartir Internet y zona Wi-Fi”, y en concreto a la opción “Anclaje por USB”.
1150. A través de la opción “Compartir por USB” (ver imagen superior) es posible habilitar el servicio de *tethering*, de forma que el ordenador utilice el dispositivo móvil como su conexión de red.

**Nota:** Aunque en versiones anteriores de Android el habilitar la conexión de red por USB o *tethering* deshabilitaba el modo de depuración USB de las opciones de desarrollo, en Android 6.x no se observa este comportamiento.

1151. Tras establecerse la conexión de red con un ordenador en Windows 10, se crea automáticamente un interfaz de red de tipo “Remote NDIS based Internet Sharing Service” configurado con una dirección IP dinámica (DHCP) por defecto de clase C (/24), como por ejemplo 192.168.42.235:

```
Adaptador de Ethernet Ethernet 3:
 Sufijo DNS específico para la conexión. . . :
 Dirección IPv4. : 192.168.42.235
 Máscara de subred. : 255.255.255.0
 Puerta de enlace predeterminada. : 192.168.42.129
```

<sup>72</sup> Siendo necesaria una configuración adicional en Windows XP (versión ya obsoleta de este sistema operativo).



1152. Este interfaz de red NDIS del ordenador tiene asociada una dirección MAC con el OUI “82:77:95” (por ejemplo), que corresponde a una dirección MAC administrada localmente y, por tanto, no asignada a ningún vendedor públicamente.

1153. La configuración de este interfaz de red emplea por defecto DHCP (a través del servidor DHCP de Android), y toma todos los valores por defecto existentes en el sistema operativo del ordenador. Así por ejemplo en Windows 10 la pila de comunicaciones de IP versión 6 está activa, al igual que NetBIOS sobre TCP/IP.

1154. Se recomienda modificar y restringir la configuración de este interfaz de red para habilitar únicamente los protocolos y servicios que se consideren necesarios en el ordenador.

1155. El dispositivo móvil, con dirección IP 192.168.42.129, actúa de gateway, router o pasarela por defecto, de servidor DHCP, y de servidor DNS, y es alcanzable mediante ping (ICMP).

**Nota:** El direccionamiento IP empleado por Android para la conexión de red compartida a través de USB (192.168.42.x/24) no puede ser modificado salvo en dispositivos móviles Android *rooteados* [Ref.- 99].

1156. La dirección MAC asociada al interfaz de red empleado para proporcionar la conexión de red compartida a través de USB por el dispositivo móvil tiene asociado un OUI con valor “72:c2:e6” (por ejemplo), que corresponde a una dirección MAC administrada localmente (al igual que ocurría en el interfaz de red del ordenador al que proporciona servicio) y, por tanto, no asignada a ningún vendedor públicamente.

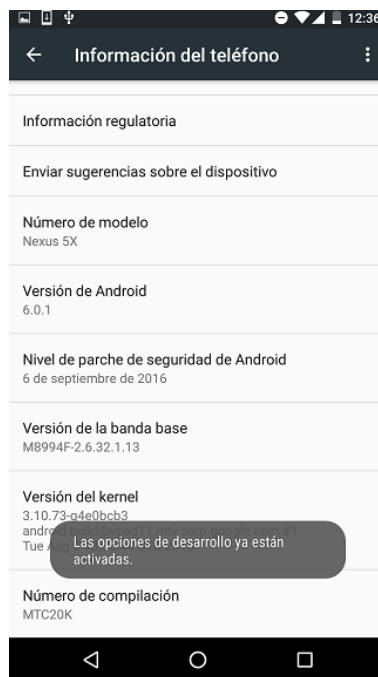
1157. Un análisis de los puertos TCP/IP y servicios disponibles en el interfaz de red del dispositivo móvil empleado para proporcionar la conexión de red compartida a través de USB permite obtener las siguientes conclusiones:

- El único puerto TCP abierto es el correspondiente al servidor DNS (53/tcp). El servidor DNS es identificado por nmap como “dnsmasq 2.51”.
- Los únicos puertos UDP abiertos son los correspondientes al servidor DNS (53/udp) y al servidor DHCP (67/udp).

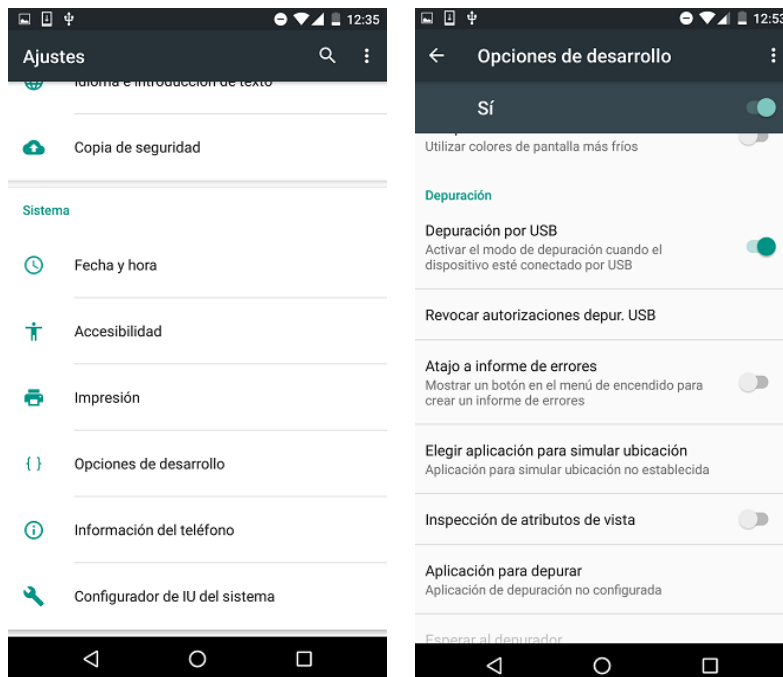
1158. Es posible finalizar la compartición de la conexión de datos deshabilitando la opción “Anclaje de USB” habilitada previamente, opción recomendada desde el punto de vista de seguridad una vez no se desea disponer de la conexión de red compartida.

### 13.3. OPCIONES DE DESARROLLO Y DEPURACIÓN USB

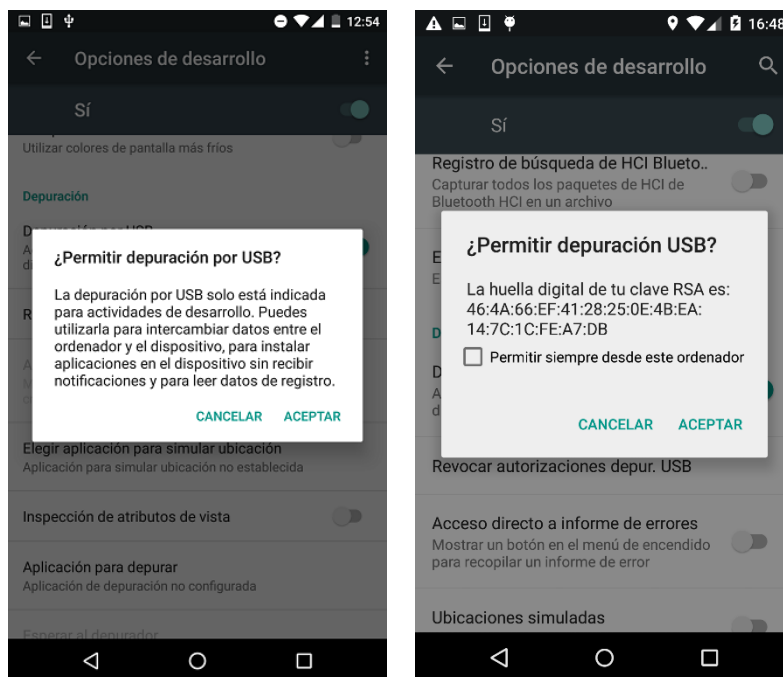
1159. Android proporciona acceso a funciones avanzadas y de bajo nivel a través del puerto USB desde un ordenador, por ejemplo, mediante el *Android Debug Bridge* (ADB) [Ref.-110]. Estas capacidades son normalmente empleadas por los desarrolladores de apps para Android, con el objetivo de llevar a cabo tareas de depuración, mediante el kit de desarrollo de software de Android, SDK (Software Development Kit).
1160. Desde la versión 4.2 de Android, el menú que proporciona el acceso para habilitar las opciones de desarrollo está oculto por defecto.
1161. Para habilitar dicho menú es necesario acceder al menú “Ajustes [Sistema] - Información del teléfono”, y pulsar en siete ocasiones sobre la opción “Número de compilación”, disponible en la parte inferior:



1162. Al completar las pulsaciones, aparecerá un nuevo menú, “Opciones de desarrollo”, en la sección de “Ajustes [Sistema]”, antes de la opción “Información del teléfono”:

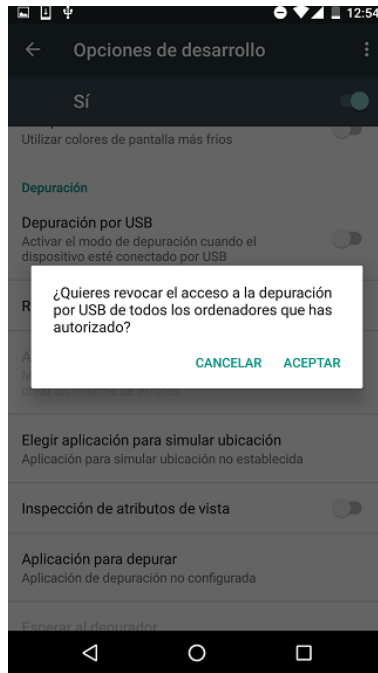


1163. A través de este nuevo menú es posible disponer de acceso a múltiples opciones para el desarrollo y depuración de apps en Android, incluyendo la opción “Depuración USB”, que permite el acceso a través de USB a las opciones avanzadas de depuración del dispositivo móvil:



1164. Desde el punto de vista de seguridad, se recomienda habilitar las opciones de desarrollo en el dispositivo móvil sólo para aquellas acciones que lo requieran (por ejemplo, realizar un backup a través de “ADB”), y deshabilitarlas una vez realizada la acción que llevó a su activación. Tras deshabilitarlas, se recomienda lanzar la opción “Revocar autorizaciones depur. USB” para que se eliminen del dispositivo las huellas digitales, o asociaciones, correspondientes al ordenador conectado:





1165. Alternativamente, es posible conectarse al dispositivo móvil a través de TCP/IP y poder ejecutar comandos utilizando el protocolo ADB sin necesidad de disponer de una conexión USB física. Es necesario que el dispositivo móvil y el equipo desde el que se va a efectuar la conexión se encuentren en la misma red Wi-Fi, para que ambos puedan comunicarse con el otro.
1166. Para ello, se requiere conectar el dispositivo por USB en una primera ocasión y ejecutar el comando `"adb tcpip <puerto>"` (dónde típicamente `<puerto>` toma el valor 5555). Una vez se constate que el demonio de ADB se ha reiniciado en modo TCP, se realizará la conexión al dispositivo mediante el comando `"adb connect <IP_del_dispositivo>"` (para obtener la IP del dispositivo, consultar el apartado "19. Comunicaciones TCP/IP").

```
C:\> adb tcpip 5555
restarting in TCP mode port: 5555
C:\> adb connect 172.16.32.125
connected to 172.16.32.125:5555
C:\> adb devices
List of devices attached
172.16.32.125:5555 device
C:\> adb shell
shell@bullhead:/exit
```

1167. Para finalizar la conexión con el dispositivo, se ejecutará el comando `"adb kill-server"`. Para volver a las capacidades de depuración por USB, se puede ejecutar `"adb usb"`.
1168. Debido a que no es posible restringir las comunicaciones entrantes al dispositivo móvil filtrando por la IP de origen, al habilitar la conexión ADB a través de TCP/IP se está permitiendo que cualquier equipo con acceso a la red Wi-Fi pueda conectarse al dispositivo móvil y enviarle comandos a través de ADB. Esto supone un riesgo importante de cara a la seguridad, por lo que se recomienda no activar el acceso ADB por TCP/IP a menos que exista un motivo justificado. Una vez realizadas las operaciones requeridas, se ejecutará el comando `"adb kill-server"`, junto a `"adb usb"`, para evitar que el puerto ADB quede abierto y un tercero pueda conectarse a él.

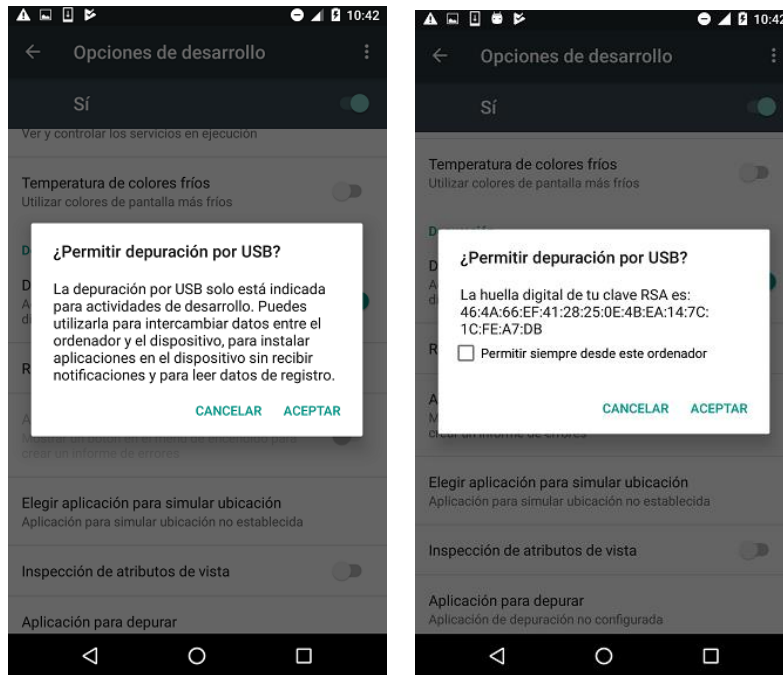
## 13.4. RELACIONES DE CONFIANZA A TRAVÉS DE USB

1169. Desde la versión 4.2.2 de Android (Jelly Bean), antes de poder hacer uso de estas capacidades de depuración USB, es necesario establecer una relación de confianza entre el dispositivo móvil y el ordenador conectado a través del puerto USB, permitiendo acceso al terminal a través de una conexión USB de depuración más segura, por ejemplo, mediante ADB [Ref.- 146].
1170. El establecimiento de relaciones de confianza a través de USB en Android se ha implementado mediante claves RSA de 2.048 bits. Estas claves son almacenadas en el ordenador bajo “\$HOME/.android” en Linux y macOS, o “%USERPROFILE%/.android” en Windows, en los ficheros “adbkey” (clave privada, en formato PEM) y “adbkey.pub” (clave pública, en base64).
1171. El dispositivo móvil Android, una vez el usuario acepta una clave de forma permanente, la almacena en el fichero “/data/misc/adb/adb\_keys”, añadiendo una nueva línea (o entrada) en este fichero correspondiente a la clave contenida en el fichero “adbkey.pub” del ordenador al que se ha conectado por USB:

```
root@movil:/data/misc/adb # ls -l
-rw-r----- system shell 717 2016-05-17 20:00 adb_keys
root@movil:/data/misc/adb # cat adb_keys
QAAAAHOy...<...>...EAAQA= unknown@unknown
```

**NOTA:** Para acceder a estos ficheros con las claves es necesario disponer de un dispositivo móvil Android *rooteado*.

1172. Este mecanismo de protección no puede ser deshabilitado a través de los ajustes de configuración del dispositivo móvil, opción preferida desde el punto de vista de seguridad.
1173. Al habilitar la opción de “Depuración USB”, el dispositivo móvil mostrará un mensaje de autorización que deberá ser aprobado por el usuario para poder establecer la conexión a través del puerto USB:



1174. El mensaje de autorización muestra el hash MD5 de la clave pública del ordenador con el que se ha establecido la conexión vía USB. Para poder comprobar que el valor mostrado por el dispositivo móvil corresponde con el de la clave pública del ordenador al que está conectado, es necesario obtener el fichero “adbkey.pub” del ordenador y extraer su *hash* MD5. Por ejemplo, en Linux puede emplearse el siguiente comando [Ref.- 146]:

```
$ awk '{print $1}' < adbkey.pub | openssl base64 -A -d -a | \
openssl md5 -c | awk '{print $2}' | tr '[:lower:]' '[:upper:]'
```

1175. En el momento de autorizar la relación de confianza, ésta puede permitirse únicamente para la sesión actual (opción por defecto), o de forma permanente, confiando en ese ordenador para futuras conexiones vía USB, mediante la opción “Permitir siempre desde este ordenador” (deshabilitada por defecto).
1176. Este mecanismo de seguridad asegura que sólo ordenadores previamente autorizados por el usuario podrán establecer una conexión mediante el puerto USB cuando el dispositivo móvil está bloqueado y se desconoce el código de acceso.
1177. Mientras la relación de confianza no ha sido aprobada, el dispositivo aparece como “unauthorized” en la respuesta del comando “adb devices” (el identificador del dispositivo móvil corresponde a su número de serie):

```
C:\> adb devices
List of devices attached
0111fb177f642917 unauthorized
C:\> adb devices
List of devices attached
0111fb177f642917 device
C:\> adb shell
shell@bullhead:/ $
```

#### Número de serie

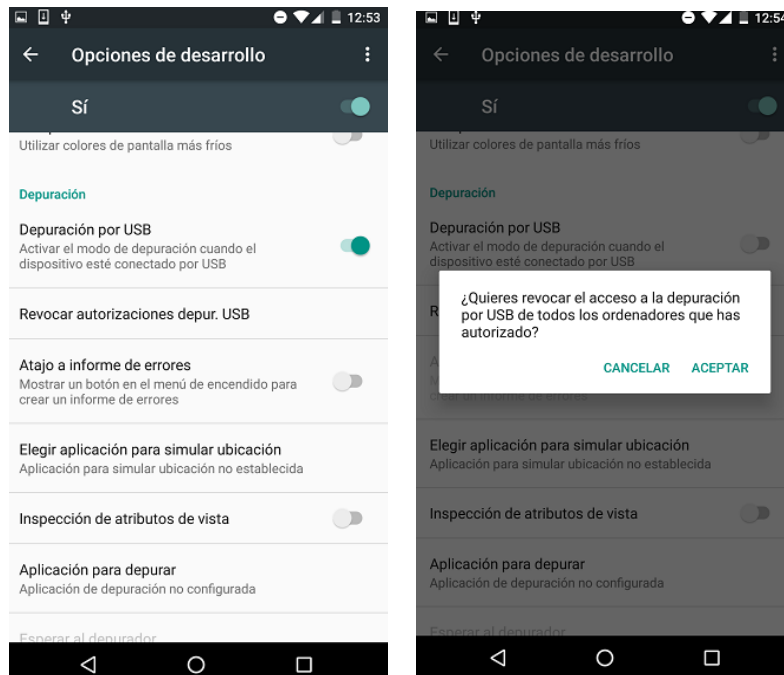
0111fb177f642917

#### Tiempo de actividad

73:12:47

1178. Una vez la relación de confianza ha sido aprobada, el dispositivo aparecerá como disponible, “device”, en la respuesta del comando “adb devices” y se podrá acceder a él, por ejemplo, mediante ADB.

1179. En el caso de dispositivos móviles Android multi-usuario, únicamente el usuario propietario (o usuario principal) puede autorizar el acceso USB a un ordenador, por lo que para autorizar el mensaje y habilitar la depuración mediante USB es necesario cambiar al usuario principal.
1180. Las relaciones de confianza establecidas previamente por USB pueden ser eliminadas en su conjunto, es decir, no selectivamente, mediante el menú “Ajustes [Sistema] - Opciones de desarrollo [Depuración] - Revocar autorizaciones depur. USB”:



## 14. COMUNICACIONES NFC

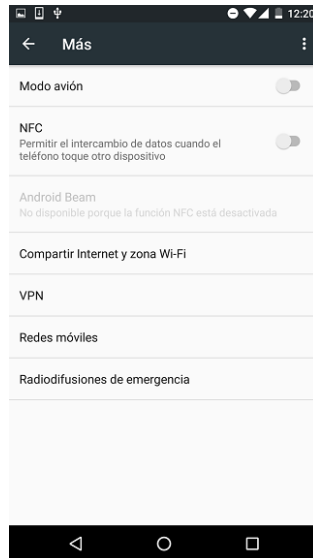
### 14.1. UTILIZACIÓN DE LAS COMUNICACIONES NFC

1181. Android dispone de capacidades de comunicación inalámbricas de corto alcance mediante tecnologías NFC (*Near Field Communication*), en concreto en aquellos dispositivos móviles cuyo *hardware* dispone de un interfaz, módulo o controlador NFC.
1182. El soporte inicial para NFC en Android se introdujo en la versión 2.3, extendiéndose su funcionalidad significativamente en Android 4.4.
1183. La principal recomendación de seguridad asociada a las comunicaciones NFC en dispositivos móviles es no activar el interfaz inalámbrico NFC salvo en el caso en el que se esté haciendo uso del mismo, evitando así la posibilidad de ataques sobre el *hardware* del interfaz, el driver o la pila de comunicaciones NFC, incluyendo la funcionalidad adicional implementada sobre NFC, como por ejemplo Android Beam [Ref.- 182].
1184. Android no dispone de ninguna indicación en la barra superior de estado, pantalla de inicio o pantalla de bloqueo que indique si el interfaz o controlador NFC está activo, por lo que es necesario acceder a los ajustes de configuración para verificar su estado actual.
1185. En Android 6.x la funcionalidad de Android Beam está disponible a través del menú “Compartir”, para poder intercambiar también datos mediante NFC.

1186. Las apps de pago, como por ejemplo apps bancarias, disponen de la posibilidad de registrar su identificador de app NFC (AID) dinámicamente y de fijar como preferencia el servicio de emulación de tarjeta que se desea utilizar cuando las actividades están ejecutando en segundo plano.

## 14.2. CONFIGURACIÓN DE NFC

1187. El interfaz inalámbrico NFC puede ser desactivado en Android, ya que está habilitado por defecto, a través del menú “Ajustes [Conexiones Inalámbricas y Redes] - Más”, y en concreto a través de la opción “NFC”:

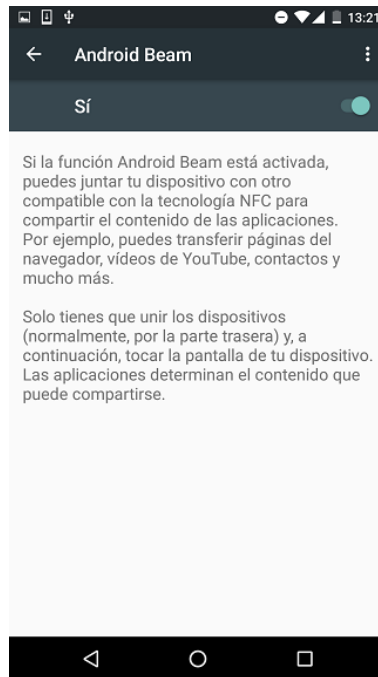


1188. Desafortunadamente, Android no proporciona a través del interfaz de usuario acceso a otros ajustes de configuración más avanzados relacionados con NFC.

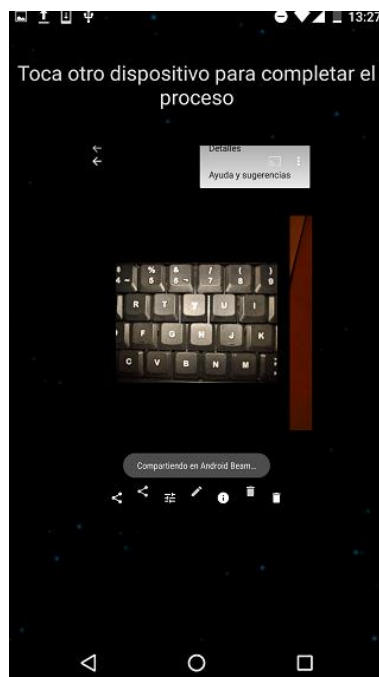
1189. Por otro lado, Android permite compartir contenidos mediante NFC entre dos dispositivos móviles, tales como páginas web, fotografías, vídeos, contactos, enlaces a apps en Google Play, ubicaciones en Maps y otros datos, a través de Android Beam (habilitado por defecto y disponible desde la versión 4.0 de Android). El proceso de transmisión se lleva a cabo al aproximar el interfaz NFC de ambos dispositivos móviles, normalmente situado en la parte trasera de los mismos.

1190. La transferencia efectiva se realiza mediante Bluetooth, pero no se requiere que la conexión Bluetooth esté habilitada inicialmente.

1191. Para ello es necesario que los dos dispositivos móviles dispongan del interfaz NFC activo, así como de la funcionalidad Android Beam habilitada [Ref.- 182]. Android Beam puede ser habilitado a través del menú “Ajustes [Conexiones Inalámbricas y Redes] - Más” y la opción “Android Beam” (junto al botón “[SI | NO]” asociado), debiendo estar la opción “NFC” activa previamente:

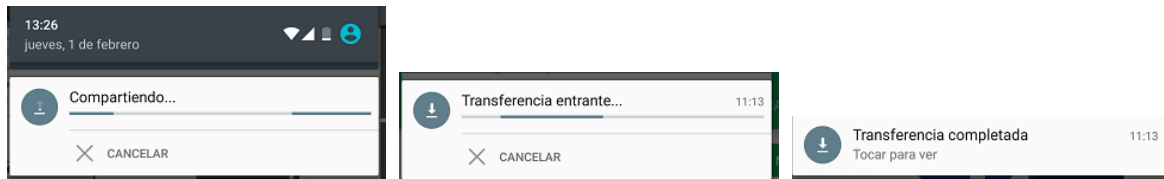


1192. Para compartir el contenido sólo es necesario disponer de la app con el contenido a intercambiar abierta, aproximar los dos dispositivos móviles, y autorizar la transmisión de datos mediante la opción “Toca para compartir”, seleccionada desde el dispositivo emisor. Ambos dispositivos deben estar desbloqueados.
1193. Por ejemplo, para compartir una imagen, se seleccionará la misma en el dispositivo móvil emisor y se utilizará la opción de “Compartir” (símbolo de grafo de tres puntos situado en la esquina inferior izquierda del menú); al aproximar el dispositivo móvil receptor, una señal acústica confirmará que se ha establecido la conexión NFC, y se solicitará confirmación de la transacción al usuario del dispositivo móvil emisor (mediante el botón “Toca para compartir”).



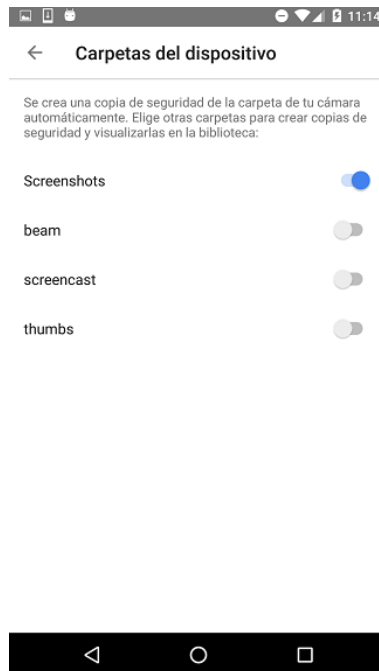
1194. La flecha en movimiento que se muestra en el menú de notificaciones informa de que la transferencia se ha iniciado. Esta flecha apuntará hacia arriba si el fichero se comparte desde el dispositivo móvil hacia otro dispositivo NFC y apuntará hacia abajo si

es un segundo dispositivo móvil el que está compartiendo un elemento con el dispositivo actual; al desplegarla, se puede cancelar la transacción:



1195. Si la compartición de datos NFC corresponde a un enlace a una aplicación o servidor web que ha sido compartido desde el navegador web, el receptor recibirá la URL asociada a dicha página web y la abrirá automáticamente en su navegador web.

1196. Cuando se transfieren imágenes por primera vez a través de Android Beam, se creará en el almacenamiento interno del dispositivo receptor una carpeta denominada “beam”:



1197. Para que una app pueda realizar una transferencia por NFC, debe solicitar en su fichero *manifest* el permiso “android.permission.NFC”.

### 14.3. PAGOS (Y OTROS SERVICIOS) MEDIANTE NFC

1198. En versiones previas de Android, la utilización del dispositivo móvil para la realización de pagos, por ejemplo, mediante Google Wallet<sup>73</sup> (disponible desde septiembre de 2011 en USA), no tuvo una aceptación muy extendida, principalmente porque era necesario disponer de una adecuada integración entre Android (software) y el controlador NFC del dispositivo móvil (hardware), y de acceso al *Secure Element* (SE) existente en el dispositivo móvil. En muchos modelos de terminal este acceso estaba limitado o restringido, especialmente la instalación de nuevas *applets* en el SE.

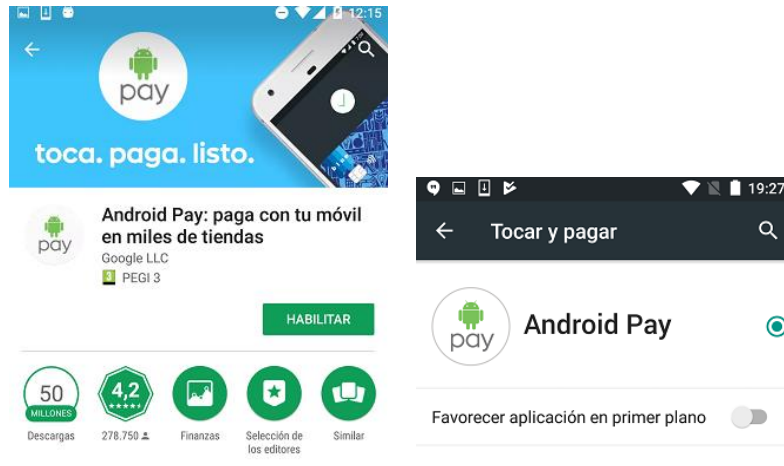
<sup>73</sup> <https://wallet.google.com>



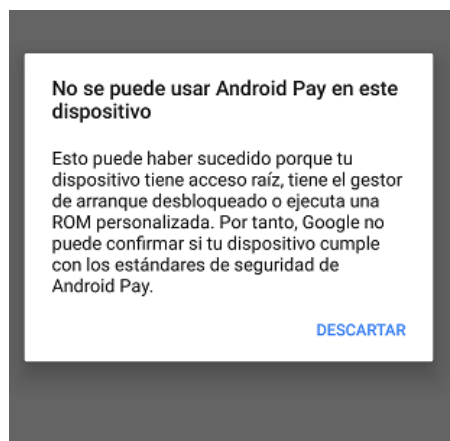
1199. El *Secure Element* (SE) es un componente *hardware* (implementado como el chip de las tarjetas inteligentes, o *smartcards*) que proporciona tanto capacidades de almacenamiento seguro para, por ejemplo, guardar claves de autenticación u otro material sensible, como un entorno de ejecución seguro para la ejecución de código y tareas críticas.
1200. El SE suele estar integrado en los dispositivos móviles actuales como una *Universal Integrated Circuit Card* (UICC, es decir, una tarjeta SIM), embebido en el propio hardware del terminal, o a través de una tarjeta SD especial. Si el dispositivo móvil dispone de soporte para NFC, el SE normalmente está embebido en el terminal y conectado al controlador NFC.
1201. Dentro de la gama de dispositivos móviles Nexus de Google (y posteriormente Pixels), el primer modelo con capacidades NFC fue el Nexus S, seguido de sus sucesores el Galaxy Nexus y el Nexus 4. Todos estos modelos, además de disponer de un interfaz o controlador NFC, disponían de un SE embebido (denominado eSE, *embedded SE*).
1202. Android, desde la versión 4.4 (KitKat), implementa una nueva arquitectura más abierta para realizar pagos NFC, que funciona con cualquier operador móvil y que permite a las apps gestionar la información sobre pagos en “la nube” o en cualquier dispositivo móvil.
1203. Estas capacidades permiten (por ejemplo, a los dispositivos móviles Nexus o Pixel de Google) “Tocar y pagar” (Tap & Pay), por ejemplo inicialmente con Google Wallet (únicamente disponible en USA), o mediante otras apps, en tiendas que admiten pagos sin contacto (*contactless*):



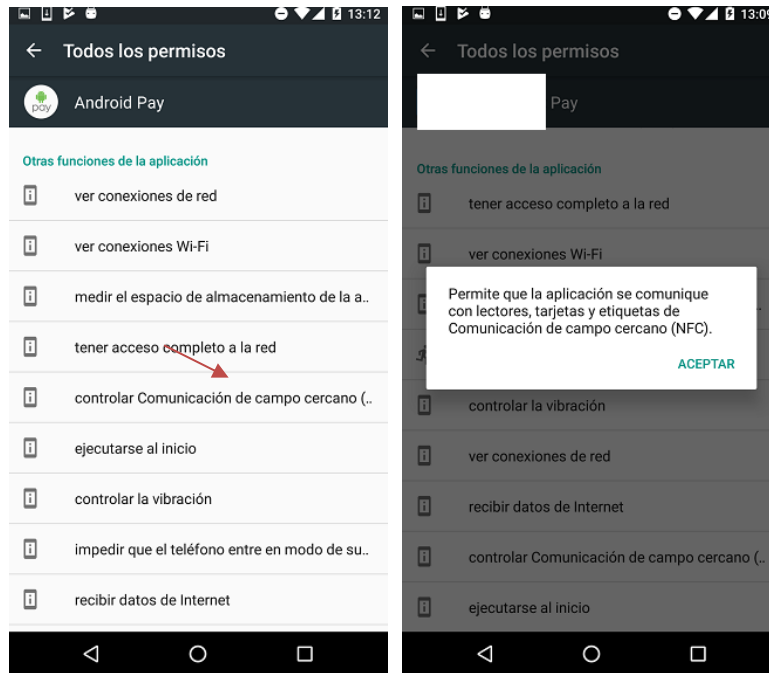
1204. Adicionalmente, NFC puede ser empleado para gestionar las tarjetas de fidelización, tarjetas de transporte, tarjetas de identificación y otros servicios similares.
1205. La funcionalidad de “Tocar y pagar” (Tap & Pay) [Ref.- 183] accesible a través del menú de “Ajustes [Dispositivo] - Tocar y pagar” no estaba disponible por defecto en Android 5.x, siendo necesario instalar una app con capacidades para pagos. En Android 6.x se dispone por defecto de la app Android Pay, pero la misma se encuentra inicialmente sin habilitar.



1206. Android Pay no puede ser utilizado en dispositivos móviles Android *rooteados* (indicado como “acceso raíz” en el siguiente mensaje de error), ni tampoco en aquellos que tengan el gestor de arranque desbloqueado, o hagan uso de una versión de firmware (o ROM) de Android personalizada (como, por ejemplo, LineageOS). Estas comprobaciones son llevadas a cabo a través de las librerías del servicio SafetyNet de Google. Cuando se intenta configurar Android Pay en un dispositivo móvil que incumple alguna de estas condiciones, se mostrará un mensaje de error:

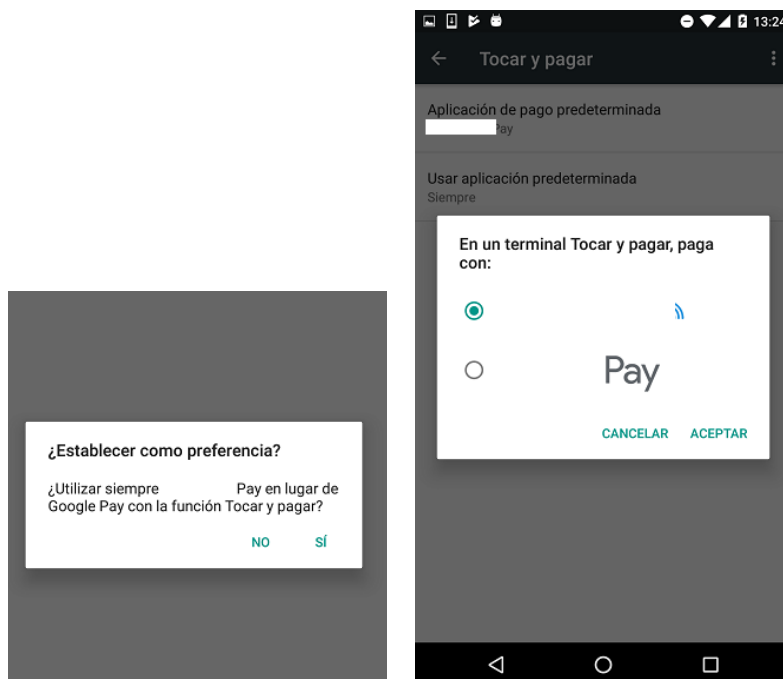


1207. Adicionalmente, para hacer uso de Android Pay se requiere haber definido un código de acceso para el dispositivo móvil.
1208. Android Pay se incorpora como una app administrador de dispositivo, con capacidades para bloquear el terminal remotamente y para borrar los datos de pago de forma que, si el usuario pierde el dispositivo móvil, no se pueda utilizar el terminal para realizar pagos.
1209. El servicio “Tocar y pagar” puede ser deshabilitado desde la app de pago asociada (si dispone de esta posibilidad), o en su defecto, deshabilitando el interfaz NFC en Android.
1210. Android Pay hace uso de HCE (*Host Card Emulation*, descrito posteriormente) en lugar del modelo existente previamente basado en SE (anteriormente descrito).
1211. Con el nuevo modelo de permisos de Android introducido en la versión 6.x (consultar apartado “7.1. Modelo de permisos de Android”), el permiso de acceso al interfaz NFC se ve englobado en el apartado “Permisos adicionales”, se considera normal, y no se solicita confirmación al usuario para utilizarlo en tiempo de ejecución. Para verificar qué permisos posee una app para el pago vía NFC, se debe acceder a “Ajustes - [Dispositivo] Aplicaciones - Android Pay - Permisos ... - Todos los permisos”:



1212. El acceso al interfaz NFC se refleja como “controlar Comunicación de campo cercano (NFC)”.

1213. Si se instala una nueva app para la función “Tocar y pagar”, la misma podrá solicitar convertirse en la app de pagos por defecto. El usuario podrá elegir en cualquier momento cuál emplear en el apartado “Ajustes - [Dispositivo] Tocar y pagar - Aplicación de pago predeterminada”:



1214. A fecha de elaboración de la presente guía, Google ha liberado el servicio “Google Pay”, que pretende unificar los distintos medios de pago (Android Pay y Google Wallet) como parte del servicio ofrecido al usuario a través de su cuenta de Google. El objetivo del servicio es que la configuración de pago esté disponible en cualquier dispositivo en el que se configure la cuenta de usuario de Google, y que se pueda usar tanto para compras vía web a través de Chrome, en apps de Android con compras integradas, en pagos vía NFC en comercios físicos, etc. [Ref.- 255].

1215. Desde Android 4.4 (KitKat), Android dispone de soporte para *Host Card Emulation* (HCE) [Ref.- 181]. Mediante HCE cualquier app en Android puede emular una tarjeta NFC (*smartcard*)<sup>74</sup> y por tanto, iniciar transacciones NFC, no siendo necesario obligatoriamente hacer uso del *Secure Element* (SE) y de las *applets* instaladas en el propio SE.
1216. Anteriormente sólo era posible hacer uso del modo de emulación de tarjeta si se hacía uso del SE conectado al controlador NFC. Con HCE, las apps actúan como tarjetas sin contacto virtuales (*virtual contactless smartcards*).
1217. Adicionalmente a HCE, las apps pueden funcionar en modo lectura (*Reader Mode*) con capacidades directas de lectura de tarjetas NFC cuando las apps ejecutan en primer plano, o en modo P2P (*Point-to-Point*) con funcionalidad básica de intercambio de datos.
1218. Por otro lado, las apps pueden declarar el tipo de etiquetas NFC (*tags*) en las que están interesadas, en función de la tecnología de las etiquetas, y cuando el servicio de NFC de Android descubra una nueva etiqueta NFC, enrutará la petición para su procesamiento a la app (o apps) correspondientes previamente registradas [Ref.- 159].
1219. Debido al soporte para HCE introducido por Android desde la versión 4.4, los nuevos modelos de dispositivos móviles Nexus de Google, como el Nexus 5 o el Nexus 7 (2013), así como los modelos Pixel, no disponen de un SE embebido (en favor de HCE).
1220. Desde el punto de vista de seguridad, y debido al tipo de información sensible y de transacciones y pagos asociada a esta funcionalidad, se recomienda deshabilitar el interfaz NFC y las opciones o servicios adicionales (Android Beam, “Tocar y pagar”, etc.), salvo que se quiera hacer un uso explícito y controlado de los mismos.
1221. Aunque más incómodo para el usuario, se recomienda habilitar temporalmente estas capacidades únicamente en el momento de ir a hacer uso de las mismas, volviendo a deshabilitar el interfaz NFC tan pronto se haya completado la transacción o el intercambio de datos mediante esta tecnología inalámbrica.
1222. A pesar de que la transacción en las operaciones de pago a través de Google Pay y Android Pay no revela la numeración real tarjeta al receptor del pago, sino un número de cuenta virtual que se asocia durante la operación de alta de la tarjeta en el servicio, desde el punto de vista de seguridad no se recomienda hacer uso de estos sistemas sin evaluar las implicaciones de seguridad en la utilización de los mismos.
1223. Si no obstante, se desea hacer uso del servicio Google Pay, se recomienda ser extremadamente cauteloso en las medidas de protección de la cuenta de usuario de Google, y aplicar las recomendaciones del apartado “20.3. Inicio de sesión y seguridad”.

## 15. COMUNICACIONES BLUETOOTH

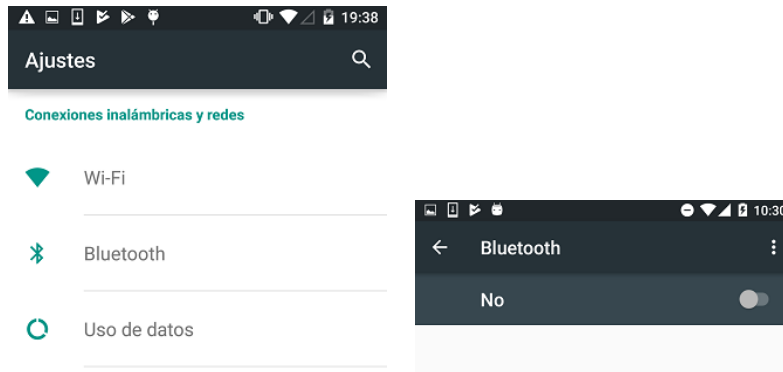
### 15.1. UTILIZACIÓN DE LAS COMUNICACIONES BLUETOOTH

1224. La principal recomendación de seguridad asociada a las comunicaciones Bluetooth (802.15) en dispositivos móviles es no activar el interfaz inalámbrico Bluetooth salvo en el caso en el que se esté haciendo uso del mismo, evitando así la posibilidad de ataques

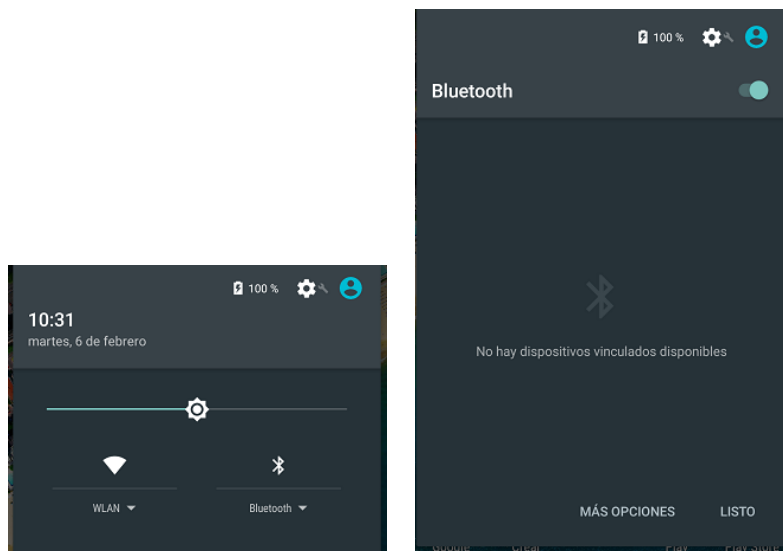
---

<sup>74</sup> Android HCE emula tarjetas ISO/IEC 7816 que hacen uso del protocolo ISO/IEC 14443-4 (ISO-DEP) para las transmisiones sin contacto (*contactless*).

sobre el hardware del interfaz, el driver o la pila de comunicaciones Bluetooth, incluyendo los perfiles Bluetooth disponibles [Ref.- 50].



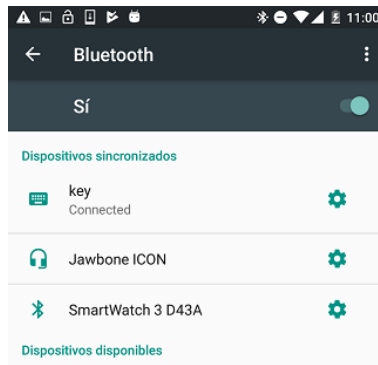
1225. El interfaz inalámbrico Bluetooth puede ser desactivado en Android, estado por defecto, a través del menú "Ajustes [Conexiones Inalámbricas y Redes] - Bluetooth"<sup>75</sup>, mediante el botón "SÍ|NO" de la opción "Bluetooth". También es posible activarlo/desactivarlo desde el menú de ajustes rápidos del dispositivo:



1226. El estado del interfaz Bluetooth puede ser verificado de forma rápida y sencilla por el usuario del dispositivo móvil a través de la barra superior de estado, ya que tan pronto el interfaz está activo, se mostrará el icono de Bluetooth.

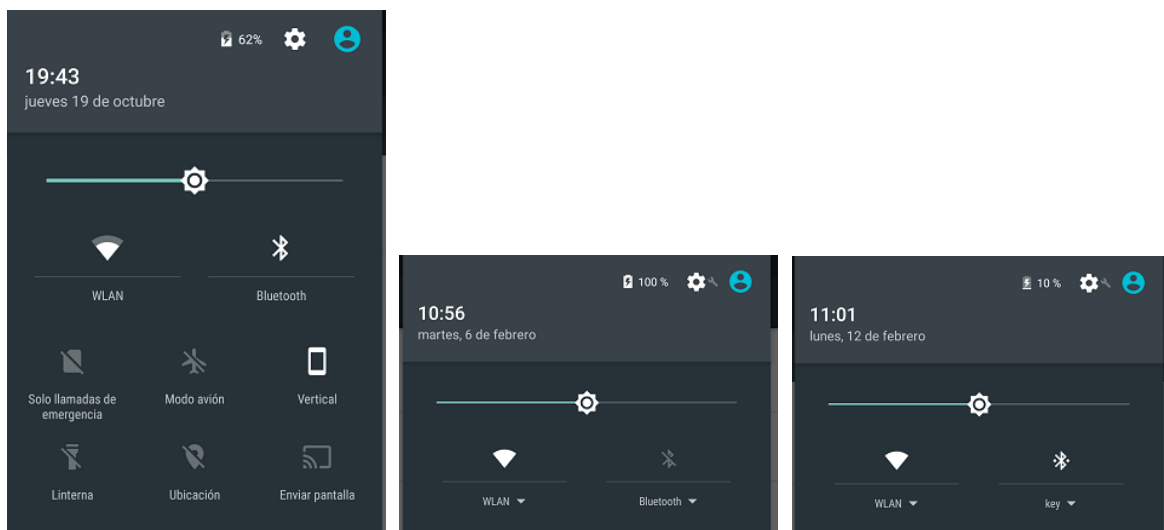
1227. Android proporciona información en la barra superior de estado sobre el estado del interfaz Bluetooth, y si existe una conexión establecida actualmente, a través de un conjunto específico de iconos que muestran el logotipo de Bluetooth. Por ejemplo, el icono de Bluetooth tendrá un par de pequeños puntos (uno a cada lado) indicando la existencia de una conexión (ver la barra de notificaciones de la imagen inferior):

<sup>75</sup> A partir de este momento, por simplificar, el menú "Ajustes [Conexiones Inalámbricas y Redes] - Bluetooth" se abreviará como "Ajustes - Bluetooth".

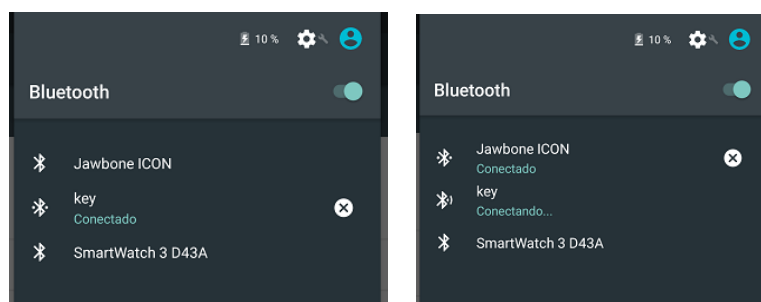


1228. Cuando el interfaz Bluetooth está activo pero no hay conexiones establecidas, se mostrará el símbolo de Bluetooth sin los puntos a ambos lados.

1229. Desde el menú de ajustes rápidos también es posible ver el estado actual del interfaz Bluetooth: el interfaz activo pero sin conexiones se muestra en color blanco y el texto “Bluetooth” (imagen inferior izquierda), el interfaz desactivado en color gris y con una línea diagonal (imagen central) y la existencia de alguna conexión con el símbolo de Bluetooth en blanco y un punto a cada uno de sus lados seguido del nombre del dispositivo con el que se ha establecido la conexión (imagen inferior derecha):



1230. Desde el menú de ajustes rápidos es posible gestionar tanto el estado del interfaz Bluetooth (activar/desactivar) como las conexiones con los dispositivos vinculados. El menú muestra el nombre del dispositivo con el que está establecida la conexión (si hay más de una, el nombre que tenga precedencia por orden alfabético). Para ver todas las conexiones activas, se pulsará sobre la flecha situada a la derecha del nombre del dispositivo conectado, lo cual desplegará un menú con todos los dispositivos vinculados:



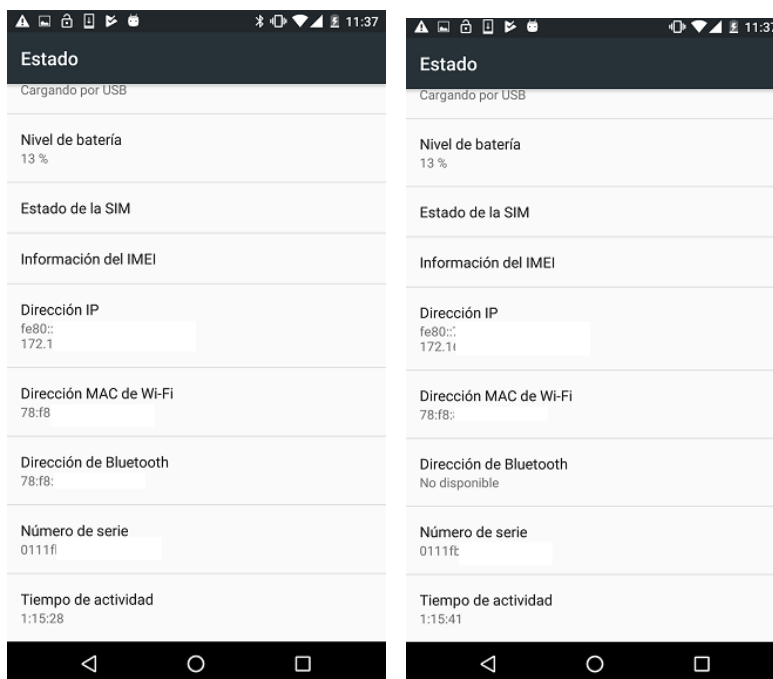
1231. Cuando se reactiva el interfaz Bluetooth después de haber sido inhabilitado, por defecto Android intentará establecer la conexión con el primero de los dispositivos de

su lista de emparejamiento (por orden alfabético) que esté disponible. Si se desea establecer conexiones adicionales, habrá que pulsar manualmente sobre el nombre de los demás dispositivos.

1232. Android mantiene el estado del interfaz Bluetooth tras reiniciar el dispositivo móvil, es decir, si el interfaz Bluetooth estaba activo al apagar el terminal, al encender el dispositivo móvil seguirá activo.
1233. La activación inicial del interfaz Bluetooth se llevará a cabo tan pronto el dispositivo móvil se haya reiniciado, incluso aunque aún no haya sido desbloqueado por primera vez tras encenderlo (igual que el interfaz Wi-Fi).
1234. Igualmente, al salir del modo avión el estado del interfaz Bluetooth será restaurado, activándose de nuevo en el caso de haber estado activo previamente (antes de activar el modo avión; igual que el interfaz Wi-Fi).
1235. El interfaz Bluetooth también permanece activo cuando el dispositivo móvil está en espera o *stand-by*, es decir, encendido pero con la pantalla apagada y bloqueado.

**Nota:** Tras un restablecimiento de fábrica, o *hard-reset*, el interfaz Bluetooth del dispositivo móvil empleado para la elaboración de la presente guía está deshabilitado por defecto. Una vez el interfaz es habilitado por el usuario, éste responde a peticiones Bluetooth (en modo oculto o no visible por defecto).

1236. La dirección del interfaz Bluetooth, BD\_ADDR (Bluetooth Device Address) está disponible a través del menú “Ajustes - Información del teléfono - Estado”, y en concreto, en el campo “Dirección de Bluetooth”. La dirección no es visible, se muestra el mensaje “No disponible” en su lugar (a diferencia del interfaz Wi-Fi), si el interfaz Bluetooth no se encuentra activo:



**Nota:** La parte de la dirección Bluetooth (BD\_ADDR) asociada al fabricante, NAP+UAP (primeros tres *bytes* de la dirección) puede permitir identificar el tipo de dispositivo móvil. En el ejemplo analizado, el valor “64:89:9A” está asignado por el IEEE (<http://standards.ieee.org/regauth/oui/index.shtml>) a “LG”:



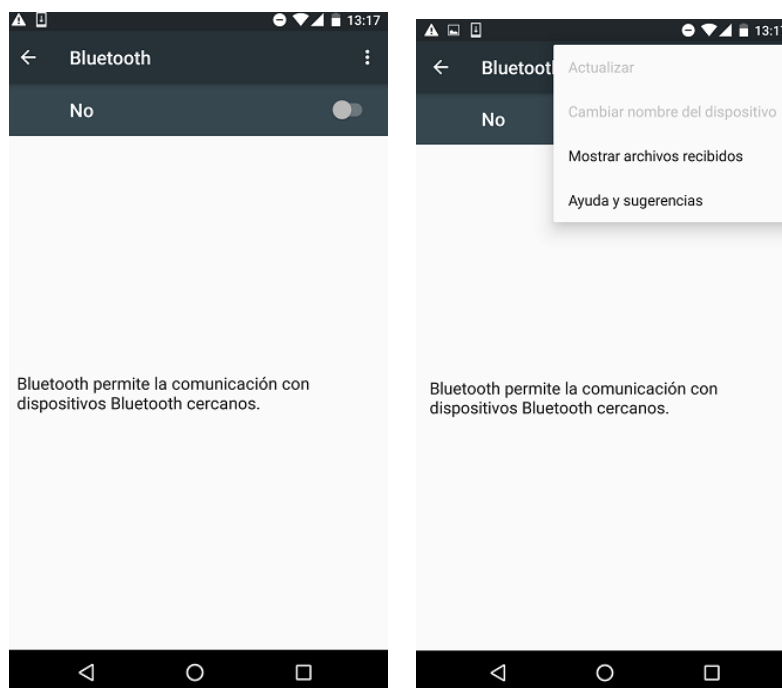
|          |           |                                        |
|----------|-----------|----------------------------------------|
| 78-F8-82 | (hex)     | LG Electronics (Mobile Communications) |
| 78F882   | (base 16) | 60-39, Gasan-dong, Geumcheon-gu        |
|          |           | Seoul Seoul 153-801                    |
|          |           | KOREA, REPUBLIC OF                     |

1237. Con objeto de proteger la privacidad del usuario, Android 6.x bloquea el acceso directo a los identificadores hardware del dispositivo móvil de cara a las apps; por ejemplo, para las direcciones MAC asociadas a las APIs de Wi-Fi y Bluetooth [Ref.- 602], si una app solicita conocer una de estas direcciones, en lugar de la dirección MAC real, Android devolverá el valor “02:00:00:00:00:00”.

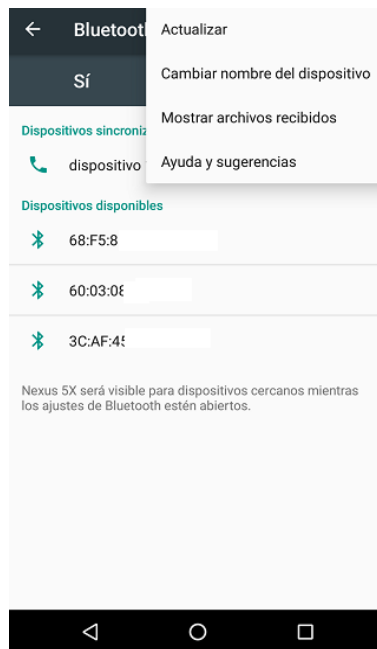
1238. Complementariamente, y también con el objetivo de proteger la privacidad del usuario, cuando un dispositivo móvil con Android 6.x inicia un escaneo Bluetooth de fondo o *background* (este aspecto también aplica a los escaneos Wi-Fi), la operación se lleva a cabo empleando una dirección MAC origen aleatoria, por lo que los dispositivos externos no pueden identificar de manera directa la dirección MAC real del dispositivo móvil. Sin embargo, debe tenerse en cuenta que si, posteriormente, el dispositivo móvil establece una conexión con un dispositivo externo, el dispositivo hará uso de su dirección MAC real, desvelándose su valor [Ref.- 602].

## 15.2. CONFIGURACIÓN GENERAL DE BLUETOOTH

1239. Debe tenerse en cuenta que, al igual que para el interfaz Wi-Fi, para poder llevar a cabo la configuración de la pila de comunicaciones Bluetooth a través del interfaz de usuario del dispositivo móvil es obligatorio activar el interfaz (como se muestra en las dos siguientes imágenes, salvo para ver los archivos recibidos) por lo que se recomienda activar el interfaz y realizar las modificaciones de la configuración en un entorno seguro, para evitar potenciales ataques cuando los mecanismos de seguridad no han sido aún aplicados:



1240. Desde la pantalla de activación del interfaz Bluetooth se accede a las opciones avanzadas a través del botón con tres puntos "...". Estas opciones permiten configurar el nombre del dispositivo móvil empleado para las conexiones Bluetooth, iniciar la búsqueda de dispositivos en rango y mostrar los archivos recibidos por Bluetooth.

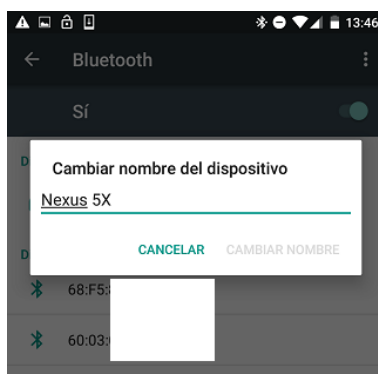


1241. La posibilidad de configurar el estado del interfaz Bluetooth (oculto o visible) y el tiempo de visibilidad, o de buscar otros dispositivos Bluetooth con los que conectarse, ya no se puede gestionar desde las opciones avanzadas, al contrario de lo que ocurría en versiones previas de Android.
1242. Desde Android 5.x, el dispositivo móvil está visible desde el punto de vista de Bluetooth mientras permanezca en la pantalla de configuración de Bluetooth, tal como indica el mensaje disponible en la parte inferior de la misma. Igualmente, el dispositivo móvil automáticamente buscará otros dispositivos Bluetooth una vez se encuentre en esta pantalla:

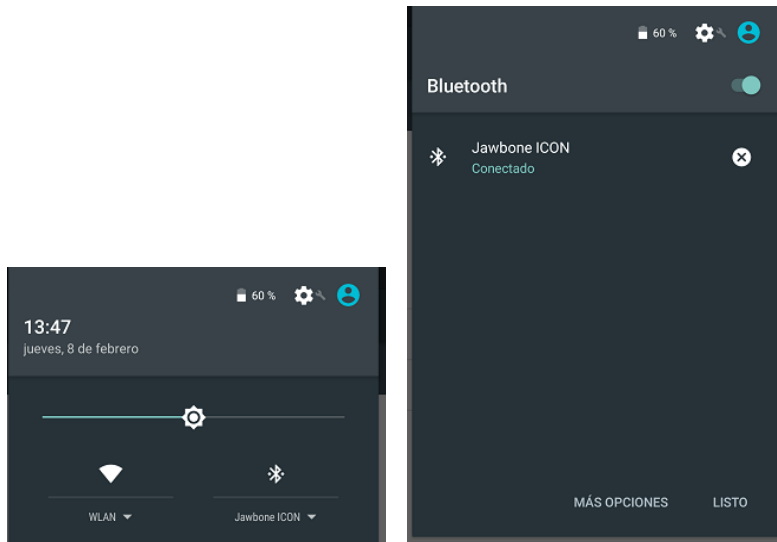


**Nota:** En ocasiones puede ser necesario deshabilitar y volver a habilitar el interfaz Bluetooth para que el emparejamiento entre dispositivos sea exitoso. Si se detectan problemas en el proceso de emparejamiento, además de consultar las instrucciones de emparejamiento del otro dispositivo, conviene probar a deshabilitar y habilitar el interfaz Bluetooth del dispositivo móvil.

1243. En caso de no especificar ningún nombre para Bluetooth, el valor por defecto empleado como nombre de dispositivo móvil para las conexiones Bluetooth por Android es “Nexus 5X” (correspondiente al tipo y modelo exacto de dispositivo móvil empleado para la elaboración de la presente guía), tal como se indica en el menú correspondiente a “Cambiar nombre del dispositivo” en los ajustes de Bluetooth:



1244. Debido a que el nombre por defecto desvela el tipo de dispositivo móvil empleado, se recomienda modificarlo por un valor que no revele detalles ni del dispositivo móvil (fabricante o modelo) ni del propietario (evitando tanto referencias al nombre de la persona como de la organización asociadas al mismo), como por ejemplo “bt0001” (“Bluetooth device 0001”).
1245. En el caso de activar el interfaz Bluetooth para hacer uso de esta tecnología, se recomienda configurar el mismo en modo oculto o no visible, con el objetivo de no desvelar su presencia frente a las operaciones de búsqueda de otros dispositivos Bluetooth.
1246. Por defecto, al activar el interfaz Bluetooth, éste se encuentra en modo oculto o no visible, opción recomendada desde el punto de vista de seguridad. Sin embargo, desde Android 5.x, al permanecer en la pantalla de configuración de Bluetooth, el dispositivo móvil estará visible.
1247. Para activar el interfaz Bluetooth en modo oculto, se recomienda hacerlo desde el menú de ajustes rápidos del dispositivo móvil, en lugar de desde la pantalla principal de configuración de Bluetooth.
1248. La cantidad de tiempo que el dispositivo permanecerá en estado visible depende del tiempo que el usuario permanezca en la pantalla de configuración de Bluetooth.
1249. Se recomienda minimizar la visibilidad del dispositivo al mínimo tiempo necesario para realizar el emparejamiento, en caso de establecer la conexión desde el dispositivo móvil (y no desde el otro dispositivo Bluetooth, ya que sólo es necesario que uno de los dos dispositivos se encuentre en estado visible para establecer el emparejamiento inicial).



1250. Al llevar a cabo conexiones Bluetooth y otras operaciones de emparejamiento con otros dispositivos desde el dispositivo móvil, al estar en la pantalla de configuración, se obliga a que el interfaz Bluetooth del dispositivo móvil permanezca en modo visible.

### 15.3. DISPOSITIVOS BLUETOOTH EMPAREJADOS

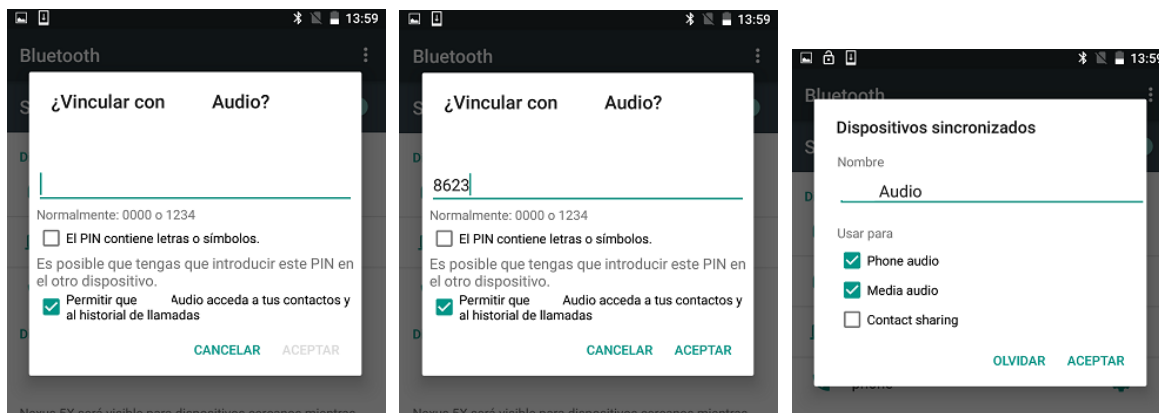
1251. Android lleva a cabo de forma automática búsquedas de dispositivos Bluetooth visibles (por ejemplo, al habilitar el interfaz Bluetooth), proceso indicado por una rueda giratoria en la parte derecha junto al texto “Dispositivos disponibles”, mostrando los mismos bajo dicha sección de la pantalla de configuración de Bluetooth:



1252. La operación de búsqueda puede llevarse a cabo también de forma manual, o alternativamente, saliendo de la sección de ajustes de Bluetooth y volviendo a entrar en la misma.
1253. Para realizar una búsqueda o descubrimiento de otros dispositivos Bluetooth cercanos desde la pantalla de configuración, es necesario emplear las opciones

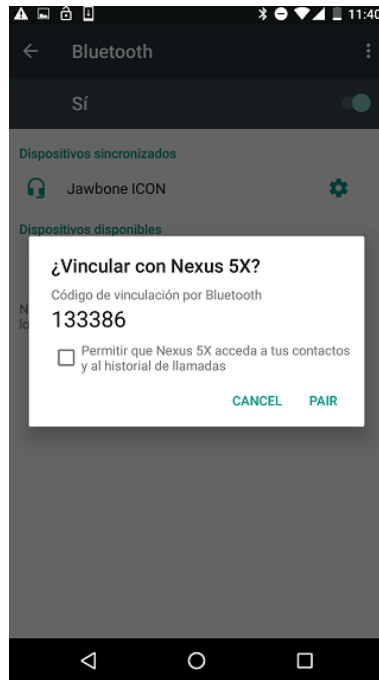
avanzadas disponibles desde el botón con tres puntos "...", y en concreto, la opción "Actualizar".

1254. Mediante la selección de un dispositivo visible de la lista es posible realizar el emparejamiento con el mismo. Android establecerá la comunicación Bluetooth con el otro dispositivo y llevará a cabo el proceso de emparejamiento, solicitando al usuario el PIN o contraseña Bluetooth si el otro dispositivo así lo requiere.
1255. En función de la versión de Bluetooth que soporte el dispositivo con el que se va a establecer la vinculación, la operación puede requerir o no la introducción de un código de emparejamiento (PIN o contraseña).
1256. Hasta la versión o especificación 2.0 de Bluetooth (inclusive), el emparejamiento se llevaba a cabo con un código de emparejamiento compartido (*Legacy Pairing*). Normalmente, es el fabricante el que define el código de emparejamiento, que puede ser fijo, como en el caso de dispositivos que no disponen de pantalla o interfaz de usuario, o variar como, por ejemplo, en dispositivos que tienen la capacidad de mostrar un código por pantalla (por ejemplo, una radio de un vehículo). En este caso, el usuario deberá de introducir en Android el código mostrado por el otro dispositivo con el que se vinculará.
1257. En el emparejamiento "legacy", el usuario deberá introducir el PIN o contraseña Bluetooth en el dispositivo móvil. Dicho código de emparejamiento se mostrará en la pantalla al ser introducida por el usuario, sin disponer Android de ninguna opción para ocultar su valor, por lo que debe prestarse especial atención a que nadie, aparte del usuario, disponga de acceso visual a la pantalla durante el proceso de emparejamiento.



1258. A partir de la especificación 2.1 de Bluetooth (core version 2.1) [Ref.- 256], se introdujo en los dispositivos un nuevo método de emparejamiento mediante SSP (*Secure Simple Pairing*), que introduce protección frente a ataques de interceptación (*eavesdropping*) y MitM (*Man-in-the-Middle*). SSP define cuatro métodos o modos de asociación:

- *Numeric comparison* (comparación numérica): este método se emplea cuando ambos dispositivos tienen una pantalla en la que mostrar un código de 6 dígitos y un mecanismo para aceptar/rechazar el código visualizado en dichas pantallas. Si el código coincide en ambos extremos de la comunicación, se seleccionará la opción correspondiente para aceptar el emparejamiento. Este escenario es típico en dispositivos móviles (como el empleado en la presente guía), *smartwatches*, ordenadores, etc.



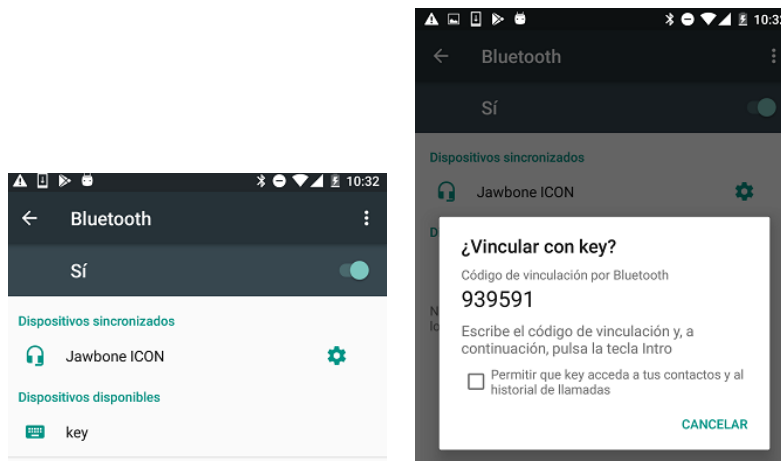
- “Just Works”: este método se emplea cuando al menos uno de los dos dispositivos carece de pantalla o de mecanismo de aceptación de un código. Internamente, los dos dispositivos intercambiarán un número, de forma similar al caso anterior, pero el usuario no verá dicho número y no se le solicitará confirmación para el emparejamiento. Este escenario es típico en el emparejamiento entre un dispositivo móvil y un auricular inalámbrico o manos libres. Este método no ofrece protección frente a ataques MitM, aunque sí frente a ataques de interceptación.



- *Out-of-Band* (OOB, o mecanismo de comunicación fuera de banda): el propósito de este método es que el proceso de descubrimiento de dispositivos se realice a través de un canal alternativo, que también se emplearía para el intercambio de los códigos de emparejamiento. Este canal debería ser inmune a ataques MitM. Por ejemplo, a través de NFC (o a través de Wi-Fi), enfrentando físicamente los

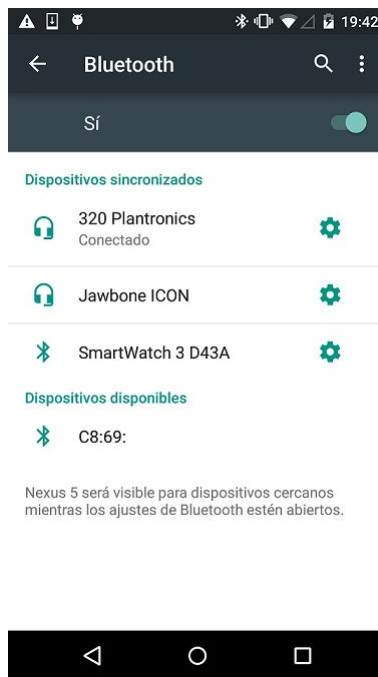
dos dispositivos se podría realizar el intercambio de la información de descubrimiento (por ejemplo, las direcciones Bluetooth) y del material criptográfico. Uno de los dispositivos establecería la conexión y se emplearía la información obtenida previamente para formalizar el emparejamiento con el otro dispositivo.

- *Passkey entry* (introducción de clave): en este método, típico de escenarios en los que uno de los dispositivos sí tiene capacidades para introducir datos pero no para mostrarlos (por ejemplo, un teclado Bluetooth que se conecta a un ordenador), el dispositivo con pantalla mostrará al usuario un código de 6 dígitos y solicitará al usuario su introducción en el otro dispositivo, permitiendo la vinculación si ambos valores coinciden. La principal diferencia con el método de “legacy pairing” de la especificación 2.0 y anteriores de Bluetooth es que el código de emparejamiento es independiente del algoritmo de seguridad, por lo que conocer dicho código no permite descifrar los datos intercambiados entre ambos dispositivos.

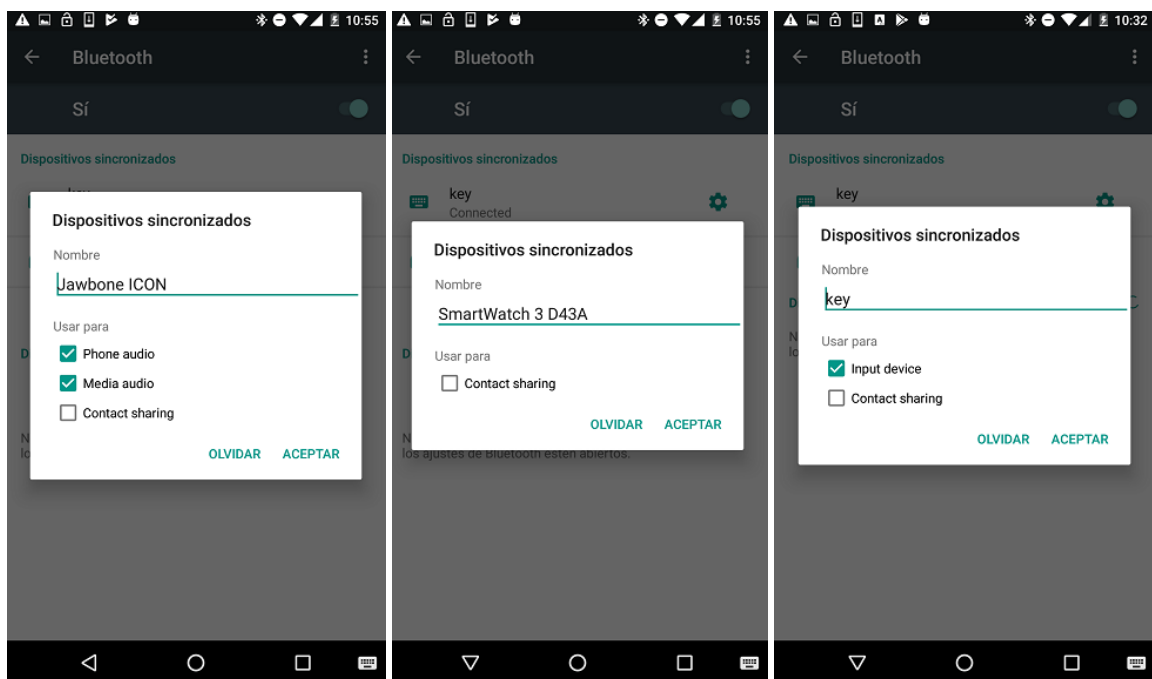


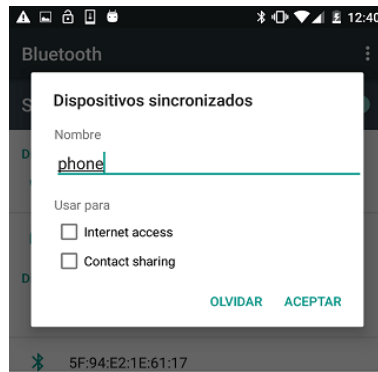
1259. Una vez se ha realizado la vinculación o emparejamiento con otro dispositivo, éste será mostrado bajo la sección “Dispositivos sincronizados” de la pantalla de configuración de Bluetooth. Además, se mostrará un icono descriptivo de la función (o clase Bluetooth) del dispositivo con el que se ha realizado el emparejamiento.
1260. No se han identificado opciones en Android para poder consultar y obtener la dirección Bluetooth (BD\_ADDR) de cada dispositivo con el que se ha realizado el emparejamiento (o que ha sido descubierto), muy útil a la hora de reconocer (y confirmar) otros dispositivos asociados al terminal.
1261. La información de la dirección sólo es mostrada temporalmente durante el proceso inicial de descubrimiento, hasta que es reemplazada por el nombre Bluetooth del dispositivo correspondiente. En caso de no poder obtener el nombre, sí se seguirá mostrando la dirección Bluetooth.



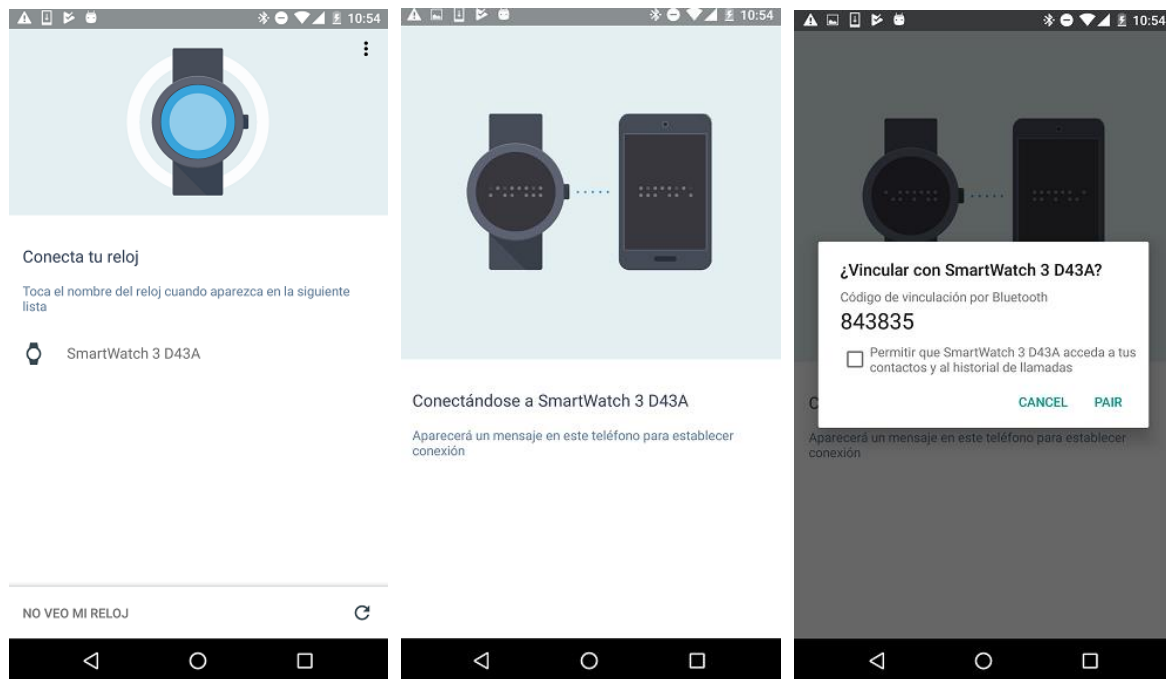


1262. En Android 6.x, mediante la selección de los ajustes de configuración (icono con un engranaje) disponible a la derecha del nombre Bluetooth de los dispositivos emparejados, es posible identificar los posibles usos proporcionados por cada dispositivo, en función de los perfiles Bluetooth que estos declaran durante el proceso de descubrimiento:





1263. Asimismo, las opciones de configuración del dispositivo sincronizado permiten modificar el nombre empleado para identificarlo dentro de la lista de dispositivos emparejados con el dispositivo móvil y poder así determinar más fácilmente si las conexiones con el dispositivo móvil deben ser autorizadas.
1264. Para la conexión de Android con un *smartwatch* (especialmente los basados en Android Wear), se requiere la instalación de la app “Android Wear” a través de Google Play, y realizar el emparejamiento a través de ella (a modo de ejemplo, se muestran sólo algunas imágenes relativas a este proceso, ya que la configuración de *smartwatches* queda fuera del alcance de la presente guía):



## 15.4. CONFIGURACIÓN AVANZADA DE BLUETOOTH

1265. La implementación de Bluetooth de Android, por defecto incluye diferentes perfiles (especificaciones de la funcionalidad y servicios proporcionados por los dispositivos Bluetooth), que dependen de la versión y dispositivo móvil utilizados.
1266. Algunos de los perfiles Bluetooth disponibles para el dispositivo móvil empleado para la elaboración de la presente guía son: “Headset Gateway” (para el envío de audio), “Handsfree Gateway” (perfil para dispositivos tipo manos libres), “AV Remote Control Target” (para control remoto de audio y vídeo), “Advanced Audio” (streaming de audio), “Personal Area Networking” (redes de área personal), “Android Network User”, “MAP

SMS” (Message Access Profile)<sup>76</sup>, “OBEX Phonebook Access Server” (acceso a contactos) y “OBEX Push” (transferencia de objetos). La lista completa de los servicios Bluetooth se puede consultar en la documentación oficial de Bluetooth para Android [Ref.- 632].

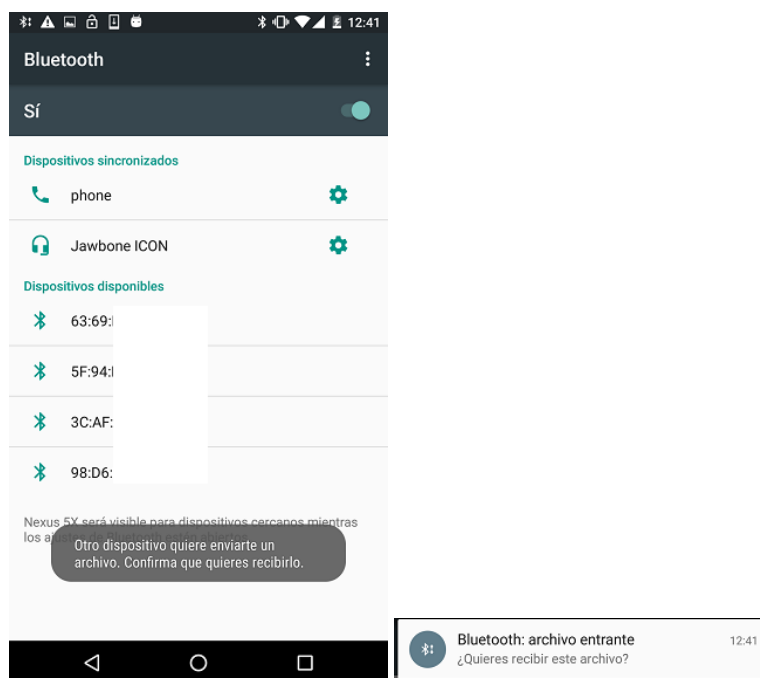
1267. No se han identificado en Android opciones de configuración avanzadas que permitan establecer restricciones de conectividad (autenticación, autorización y/o cifrado), obtener información, o configurar opciones específicas, para los diferentes perfiles Bluetooth disponibles (como por ejemplo para la configuración de red, de audio, de transferencia de archivos, etc.).

## 15.5. OBEX PUSH

1268. Android dispone por defecto de capacidades para el intercambio de objetos, asociadas al perfil Bluetooth estándar OBEX Push (en ocasiones referenciado como OBEX Object Push).

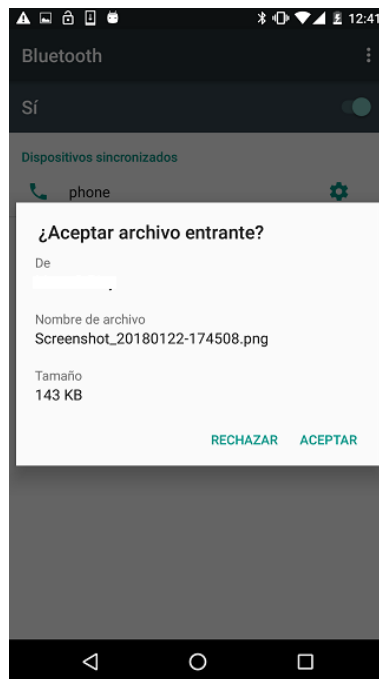
1269. El perfil de recepción de objetos (OBEX - *Object Exchange* - Push) a través de Bluetooth está habilitado por defecto y no se ha identificado ninguna opción de configuración para deshabilitarlo.

1270. Cuando otro dispositivo Bluetooth se comunica con este perfil e intenta enviar un objeto (por ejemplo, un archivo), Android solicita autorización por parte del usuario a través de una notificación vía la barra superior de estado antes de permitir la operación de intercambio, e informa de ello a través de un mensaje en la pantalla activa:

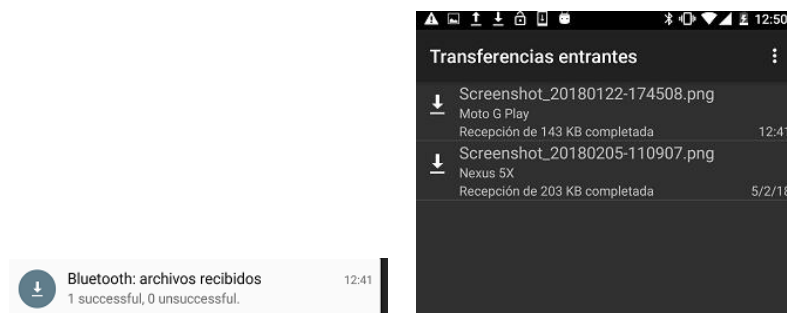


1271. Mediante la selección de dicha notificación, el usuario es informado sobre los detalles de la transferencia, que incluyen el nombre del dispositivo Bluetooth remitente, el nombre los datos transferidos (nombre del archivo), y el tamaño:

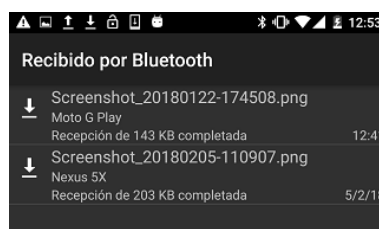
<sup>76</sup> El perfil de Bluetooth MAP permite al dispositivo móvil intercambiar mensajes con vehículos equipados con tecnología Bluetooth.



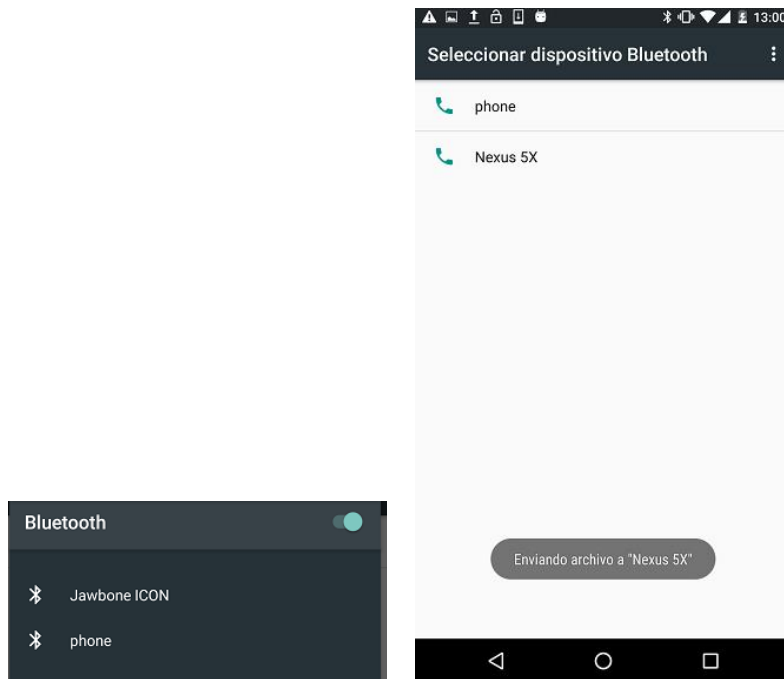
1272. Si la transferencia de datos a través del perfil OBEX Push tiene éxito, tras confirmar los mecanismos de autorización por parte del usuario desde la notificación, se indica el resultado al usuario mediante otra notificación de confirmación (desde la que es también posible acceder directamente al archivo).



1273. El objeto (o fichero) recibido se almacena por defecto en el directorio “bluetooth” del área de almacenamiento interno del dispositivo móvil (ej. “/sdcard/bluetooth/”).
1274. El acceso a los archivos recibidos mediante Bluetooth está disponible desde “Ajustes - Bluetooth - [...] - Mostrar archivos recibidos”, incluyendo tanto los que han tenido éxito como los intentos fallidos, cancelados o rechazados por el usuario:



1275. El perfil OBEX Push no dispone del mecanismo de autenticación habilitado por defecto, debido a su modelo de uso, en el que no es necesario emparejarse previamente con el otro dispositivo para transferir datos (u objetos, OBEX), tal como ilustran las siguientes imágenes (la inferior izquierda muestra los dispositivos vinculados, la derecha los dispositivos con los que se puede compartir un archivo mediante OBEX Push):



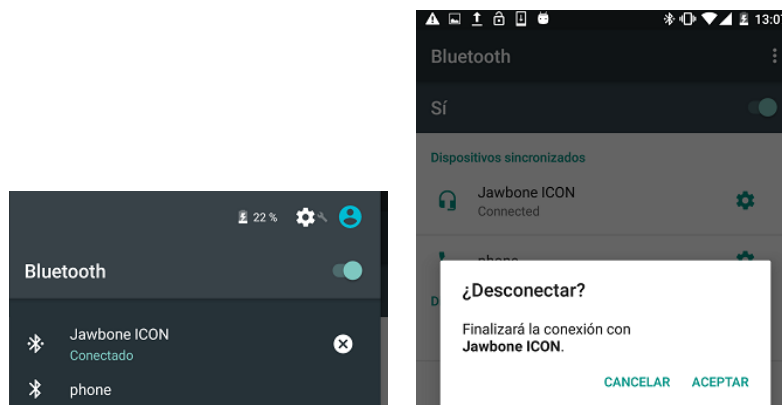
1276. El comportamiento de solicitud de autorización al usuario descrito previamente se presenta tanto con dispositivos Bluetooth con los que previamente se ha emparejado Android (es decir, autenticados), como con dispositivos nuevos.

## 15.6. MANOS LIBRES BLUETOOTH

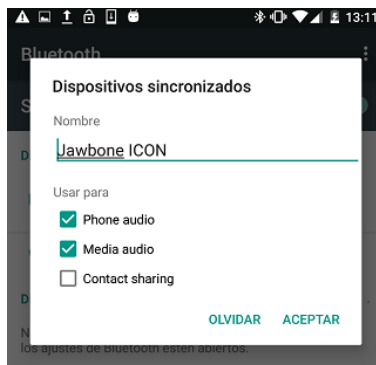
1277. El emparejamiento con dispositivos Bluetooth manos libres puede no requerir el introducir ningún PIN o contraseña, proceso conocido como emparejamiento automático o *auto pairing* (método “Just Works” de la especificación Bluetooth 2.1), debido a que Android dispone de conocimiento de los PINs empleados comúnmente por defecto (no modificables) por los fabricantes de manos libres Bluetooth.
1278. El emparejamiento automático se lleva a cabo por ejemplo con dispositivos que emplean valores de PIN por defecto, como por ejemplo “0000”.
1279. Una vez vinculado el dispositivo móvil con un dispositivo manos libres, el interfaz Bluetooth del dispositivo móvil, cada vez que es habilitado, intenta establecer automáticamente una conexión con los dispositivos manos libres disponibles en la lista de dispositivos emparejados, proceso también conocido como conexión automática o *auto connect*. Si el dispositivo Bluetooth se encuentra en el rango de alcance del dispositivo móvil, y fueron emparejados previamente, se establecerá la conexión, estado identificado en Android por el icono de estado de Bluetooth en la barra superior de estado.
1280. El proceso de conexión automática no tiene asociada ninguna solicitud de confirmación por parte del usuario ni puede ser deshabilitado mediante opciones de configuración en Android (salvo deshabilitando el interfaz Bluetooth).



1281. Una vez se ha establecido la conexión Bluetooth con otro dispositivo, es posible desconectarse del mismo bien a través del símbolo “x” del menú de ajustes rápidos, bien al seleccionarlo a través del menú de ajustes de Bluetooth y pulsando el botón “Aceptar”:



1282. Una vez se ha establecido la conexión Bluetooth con otro dispositivo (independientemente de su tipo o del perfil empleado), al seleccionar su botón de configuración asociado (disponible en la parte derecha, junto a su nombre), se dispone de un menú de opciones. A través del mismo es posible modificar el nombre empleado localmente para identificar al otro dispositivo, eliminar la vinculación o emparejamiento previos mediante el botón “Olvidar”, o seleccionar los perfiles ofrecidos por el otro dispositivo que se desean utilizar:

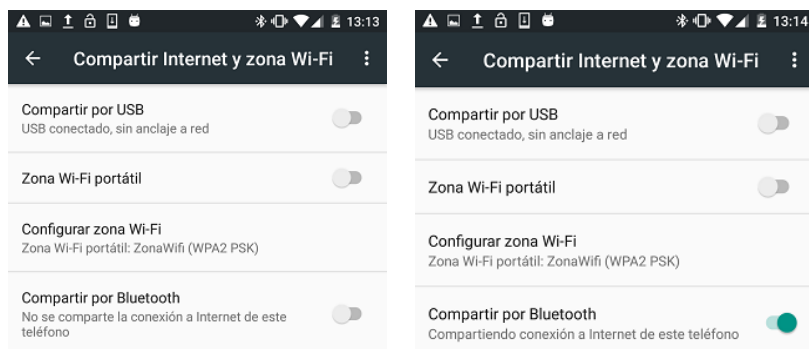


1283. No se han identificado en Android opciones de configuración avanzadas que permitan configurar los perfiles de Bluetooth asociados a la conexión con dispositivos manos libres.

## 15.7. CONEXIÓN DE RED COMPARTIDA POR BLUETOOTH

1284. Android proporciona capacidades nativas de *tethering* a través de USB (ver apartado “13.2. Conexión de red compartida por USB (*Tethering*)”).

1285. Para hacer uso de estas capacidades mediante Bluetooth (Personal Area Network, PAN) es necesario acceder al menú “Ajustes [Conexiones Inalámbricas y Redes] - Más... - Compartir Internet y zona Wi-Fi”, y en concreto a la opción “Compartir por Bluetooth”:



1286. A través de la opción “Compartir por Bluetooth” es posible habilitar el servicio de *tethering*, de forma que el ordenador utilice el dispositivo móvil como su conexión de red a través de una conexión Bluetooth. Para ello es necesario que previamente el ordenador y el dispositivo móvil se hayan emparejado.

1287. La configuración empleada para Bluetooth es similar a la utilizada para compartir la conexión mediante USB (ver apartado “13.2. Conexión de red compartida por USB (*Tethering*)”) o Wi-Fi (ver apartado “16.6. Punto de acceso o zona Wi-Fi”).

1288. Tras establecerse la conexión de red, y tomando Windows 10 como sistema operativo del ordenador de referencia, se crea automáticamente un interfaz de red de tipo “Bluetooth Device (Personal Area Network)” (PAN) configurado con una dirección IP dinámica (DHCP) por defecto de clase C (/24), como por ejemplo 192.168.44.191.

```
Adaptador de Ethernet Conexión de red Bluetooth:
Sufijo DNS específico para la conexión. . . :
Dirección IPv4. : 192.168.44.191
Máscara de subred : 255.255.255.0
Puerta de enlace predeterminada : 192.168.44.1
```

1289. Este interfaz de red Bluetooth del ordenador tiene asociada la dirección MAC del adaptador Bluetooth empleado en el ordenador.

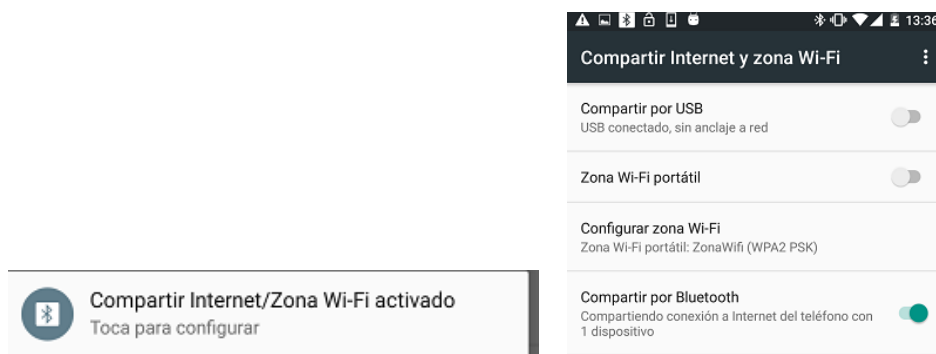


1290. La configuración de este interfaz de red emplea por defecto DHCP (a través del servidor DHCP de Android), y toma todos los valores por defecto existentes en el sistema operativo del ordenador. Así por ejemplo en Windows 10 la pila de comunicaciones de IP versión 6 está activa, al igual que NetBIOS sobre TCP/IP.
1291. Se recomienda modificar y restringir la configuración de este interfaz de red para habilitar únicamente los protocolos y servicios que se consideren necesarios en el ordenador.
1292. El dispositivo móvil, con dirección IP 192.168.44.1, actúa de gateway, router o pasarela por defecto, de servidor DHCP, y de servidor DNS, y es alcanzable mediante ping (ICMP).

```
shell@bullhead:/ $ ifconfig
bt-pan Link encap:UNSPEC
 inet addr:192.168.44.1 Bcast:192.168.44.255 Mask:255.255.255.0
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:102 errors:0 dropped:0 overruns:0 frame:0
 TX packets:15 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:500
 RX bytes:9419 TX bytes:1823
```

**Nota:** El direccionamiento IP empleado por Android para la conexión de red compartida a través de Bluetooth (192.168.44.x/24) no puede ser modificado salvo en dispositivos móviles *rooteados* [Ref.- 99].

1293. La dirección MAC asociada al interfaz de red empleado para proporcionar la conexión de red compartida a través de USB por el dispositivo móvil tiene asociada la dirección MAC del interfaz Bluetooth del dispositivo móvil.
1294. El dispositivo móvil informa de la compartición de la conexión Bluetooth a través de una notificación (accesible desde la barra superior de notificaciones):



1295. Es posible finalizar la compartición de la conexión de datos deshabilitando la opción “Compartir por Bluetooth” habilitada previamente, opción recomendada desde el punto de vista de seguridad una vez no se desea disponer de la conexión de red compartida.

## 15.8. BLUETOOTH LOW ENERGY (BLE)

1296. Android 5.x añadió capacidades de Bluetooth Low Energy (BLE) para que el dispositivo móvil pueda actuar como un periférico (realizando anuncios, o actuando en modo periférico de BLE), en lugar de únicamente como el elemento central,

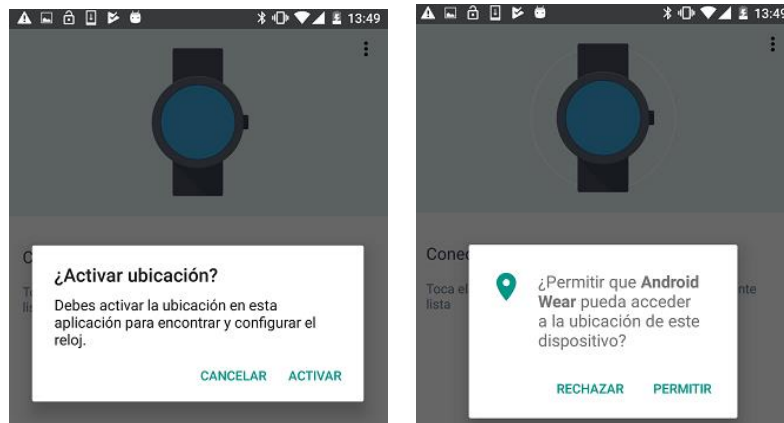
funcionalidad introducida en Android 4.3 (realizando escaneos, o actuando en modo central de BLE).

1297. Las apps pueden hacer uso de esta nueva funcionalidad para anunciar su presencia de cara a otros dispositivos cercanos. Así, una app puede actuar como un sensor o monitor de salud y proporcionar los datos recolectados a otro dispositivo BLE.
1298. Para ello las apps disponen de la posibilidad de enviar anuncios de difusión (*broadcast advertisements*), escanear las respuestas recibidas y establecer las conexiones asociadas. Esta funcionalidad requiere que la app declare el permiso `BLUETOOTH_ADMIN`, que se considera un permiso estándar o normal (ver apartado “7.1.3. Permisos normales y peligrosos”), por lo que no se solicitará explícitamente su concesión al usuario en tiempo de instalación y/o ejecución si la app lo declara en su fichero *manifest*, ni se podrá habilitar/deshabilitar de forma independiente:



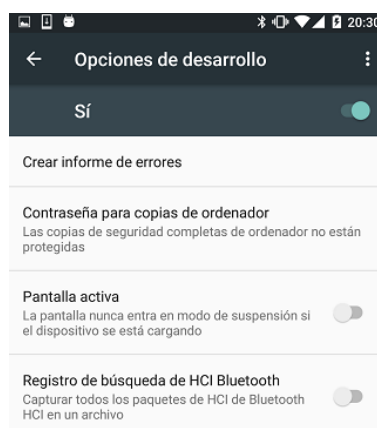
1299. Asimismo, Android 5.x introdujo capacidades BLE para que una app pueda aplicar filtros durante el proceso de escaneo y sólo descubra aquellos dispositivos en los que está interesada.
1300. En Android, un dispositivo BLE puede ser accedido por más de una app al mismo tiempo. La conexión física la gestiona el sistema operativo, y cada app accede a ella como si tuviese la conexión en exclusiva.
1301. Android 6.x añade mejoras para las apps que hacen escaneos BLE, pudiendo recibir notificaciones del sistema tan pronto se reciba un anuncio BLE vinculado al filtro de escaneo especificado, mejorando así el consumo energético asociado a este tipo de tareas [Ref.- 603].
1302. Cuando se establece una conexión con un dispositivo BLE, la app debe pasar un parámetro, *autoconnect*, que determina si Android debería reintentar la conexión en caso de que ésta se vea interrumpida (salvo que la interrupción se deba a la inhabilitación del interfaz Bluetooth o a que la app solicite la desconexión deliberadamente). Éste es el caso de la conexión con un *smartwatch*, de forma que, si éste sale del rango de alcance, cuando vuelva a entrar en él, se restablezca la conexión.

1303. Cuando el parámetro *autoconnect* tiene valor “verdadero”, no se establecerá un temporizador para los intentos de conexión. Si tiene valor “falso”, se establecerá un temporizador de 30 segundos para la conexión.
1304. Para permitir el escaneo BLE, en Android 6.x se requiere habilitar el servicio de ubicación y conceder a la app permiso de localización (este requisito no existía en versiones anteriores de Android). Este requisito (permiso considerado peligroso por Google) se solicita al usuario en tiempo de instalación (por ejemplo, cuando se instala la app Android Wear para la gestión de *smartwatches*) o de ejecución desde Android 6.x.



1305. Existe una opción de desarrollo que permite rastrear las conexiones Bluetooth establecidas por el dispositivo móvil. Esta opción, que se ilustra en la imagen siguiente, al activarse provoca que se cree un fichero de log en la ubicación especificada por la variable de configuración correspondiente del fichero “/etc/bluetooth/bt\_stack.conf”:

```
shell@bullhead:/ $ cat etc/bluetooth/bt_stack.conf | grep BtSnoopFileName
BtSnoopFileName=/sdcard/btsnoop_hci.log
```



1306. El fichero “btsnoop\_hci.log” puede leerse con Wireshark [Ref.- 257], y en el mismo se registra toda la actividad tanto entre el dispositivo móvil y los dispositivos Bluetooth externos, como entre el denominado “controller” (hardware local responsable del procesamiento de tráfico Bluetooth) y el denominado “host” (la pila software Bluetooth que implementa el propio sistema operativo Android).

## 16. COMUNICACIONES WI-FI

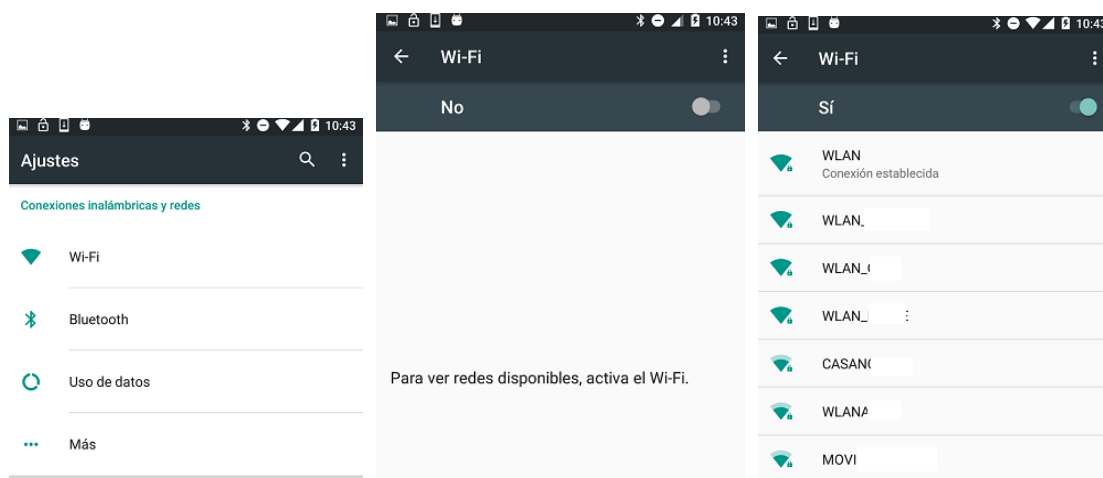
### 16.1. UTILIZACIÓN Y CONFIGURACIÓN DE LAS COMUNICACIONES WI-FI

1307. La principal recomendación de seguridad asociada a las comunicaciones Wi-Fi (802.11) en dispositivos móviles es no activar el interfaz inalámbrico Wi-Fi salvo en el caso en el que se esté haciendo uso del mismo, evitando así la posibilidad de ataques sobre el hardware del interfaz, el driver o la pila de comunicaciones Wi-Fi [Ref.- 48].

**Nota:** Durante el proceso de configuración inicial del dispositivo móvil empleado para la elaboración de la presente guía (que se inicia automáticamente la primera vez que se enciende el terminal, según se ilustra en el apartado “24. Apéndice A: Proceso de instalación y configuración inicial”), tanto si se omite el establecimiento de una conexión a una red Wi-Fi como si no, el interfaz Wi-Fi estará habilitado por defecto.

Desde el punto de vista de seguridad se recomienda deshabilitar el interfaz Wi-Fi y habilitarlo posteriormente, una vez el usuario se encuentre en un entorno seguro y de confianza para poder establecer una conexión a una red Wi-Fi.

1308. El interfaz inalámbrico Wi-Fi puede ser desactivado en Android a través del menú “Ajustes [Conexiones Inalámbricas y Redes] - Wi-Fi”<sup>77</sup>, mediante el botón “SÍ|NO” de la opción “Wi-Fi”:



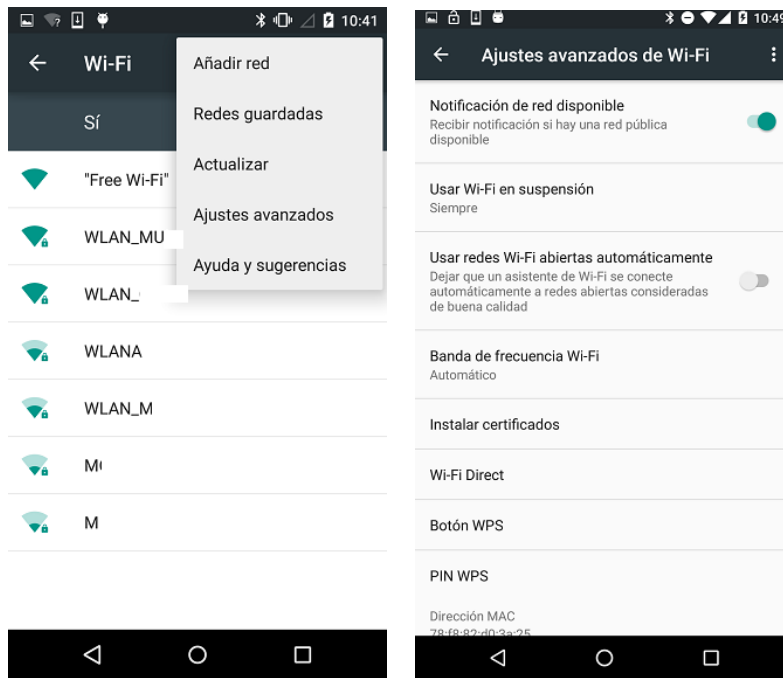
1309. Android proporciona información en la barra superior de estado sobre la disponibilidad de redes Wi-Fi abiertas y si se está o no conectado a una red Wi-Fi actualmente, a través de un conjunto específico de iconos que muestran las ondas de las señales Wi-Fi.

1310. La disponibilidad de redes Wi-Fi abiertas se muestra con un símbolo de interrogación en las ondas de las señales Wi-Fi, en la zona izquierda de la barra superior de estado (correspondiente a las notificaciones), acompañado de un nuevo mensaje de notificación:

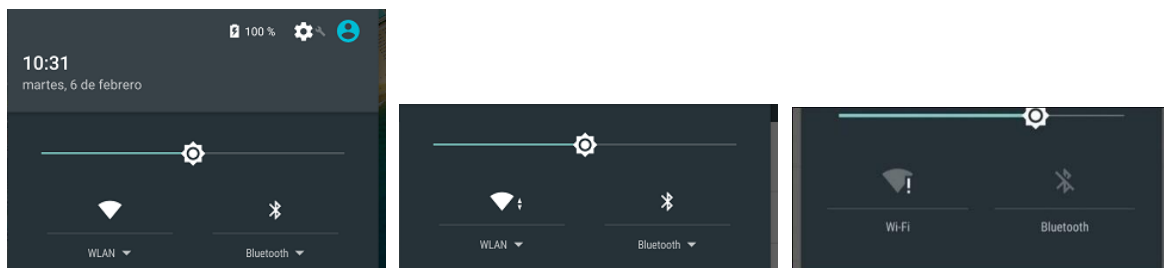


<sup>77</sup> A partir de este momento, por simplificar, el menú "Ajustes [Conexiones Inalámbricas y Redes] - Wi-Fi" se abreviará como "Ajustes - Wi-Fi".

1311. La notificación respecto a la disponibilidad de redes Wi-Fi abiertas puede ser configurada a través del menú “Ajustes - Wi-Fi - [...] - Ajustes avanzados”, y en concreto mediante la opción “Notificación de red disponible” (habilitada por defecto). Esta opción puede ser modificada únicamente una vez el interfaz Wi-Fi ha sido habilitado. Adicionalmente, se ofrece una opción que permite que el dispositivo móvil se conecte de forma automática a redes Wi-Fi abiertas. Esta opción se considera totalmente desaconsejada desde el punto de vista de seguridad, ya que a través suyo el propietario del dispositivo pierde el control sobre las redes Wi-Fi con las que se establecerá conexión:



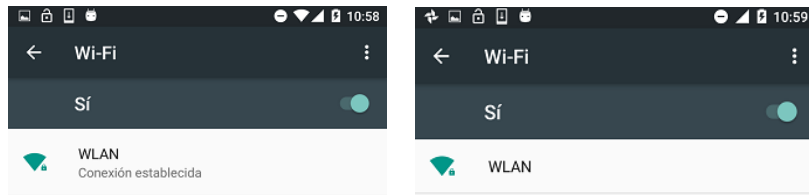
1312. Dado que desde el punto de vista de seguridad se desaconseja el establecer conexiones con redes Wi-Fi abiertas, se recomienda desactivar también la opción de “Notificación de red disponible”.
1313. Los ajustes rápidos, disponibles al desplazar hacia abajo la barra de menú superior, permiten conocer más detalles sobre el interfaz Wi-Fi. Por ejemplo, si las ondas Wi-Fi aparecen con una admiración, ésta puede indicar que se han detectado problemas de conectividad hacia Internet<sup>78</sup>.



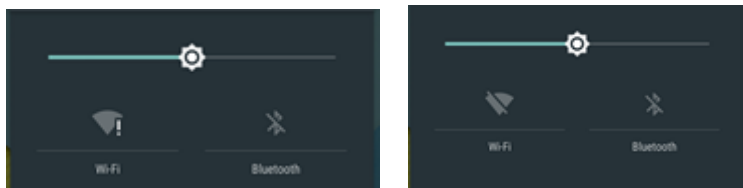
1314. El estado del propio interfaz Wi-Fi no puede ser verificado de forma rápida y sencilla por el usuario del dispositivo móvil a través de la barra superior de estado o menú. Desafortunadamente, la barra superior de estado no proporciona información sobre el

<sup>78</sup> En algunas versiones de Android, la existencia de flechas hacia arriba y hacia abajo en el icono Wi-Fi indican que el dispositivo móvil está transmitiendo o recibiendo datos, respectivamente.

estado del interfaz Wi-Fi, no siendo posible saber si el mismo está activo o no, salvo que el dispositivo móvil esté conectado a una red Wi-Fi actualmente:



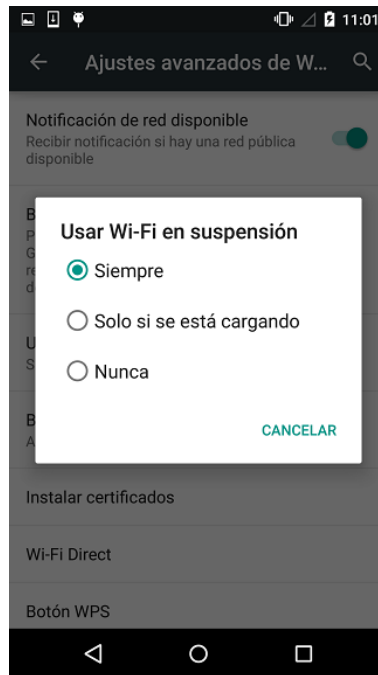
1315. Únicamente desde los ajustes rápidos, o desde el menú de “Ajustes” (pero éste no permite un acceso sencillo, ágil y rápido), es posible ver el estado actual del interfaz Wi-Fi a través del icono asociado: el texto “Wi-Fi” con un icono con ondas indica que el interfaz Wi-Fi está activado, aunque no esté conectado a ninguna red actualmente, mientras que el texto “Wi-Fi” con un icono con ondas cruzado por una línea diagonal indica que el interfaz Wi-Fi está desactivado.



1316. Android mantiene el estado del interfaz Wi-Fi tras reiniciar el dispositivo móvil, es decir, si el interfaz Wi-Fi estaba activo al apagar el terminal, al encender el dispositivo móvil seguirá activo, incluso con el terminal bloqueado.
1317. Igualmente, al salir del modo avión el estado del interfaz Wi-Fi será restaurado, activándose de nuevo en el caso de haber estado activo previamente (antes de activar el modo avión).
1318. Cuando el dispositivo móvil está conectado a una red, el interfaz Wi-Fi permanece activo tras pasar al estado de espera o *stand-by* (desatendido), es decir, el estado en que el dispositivo móvil está encendido pero con la pantalla apagada y bloqueado (ver posteriormente la opción avanzada de configuración asociada), y sigue generando tráfico periódicamente.
1319. En caso de no estar conectado a una red Wi-Fi, en el estado de espera (o suspendido) el dispositivo móvil genera por defecto el tráfico 802.11 asociado a las tramas de verificación de disponibilidad de redes Wi-Fi (*probe request*).

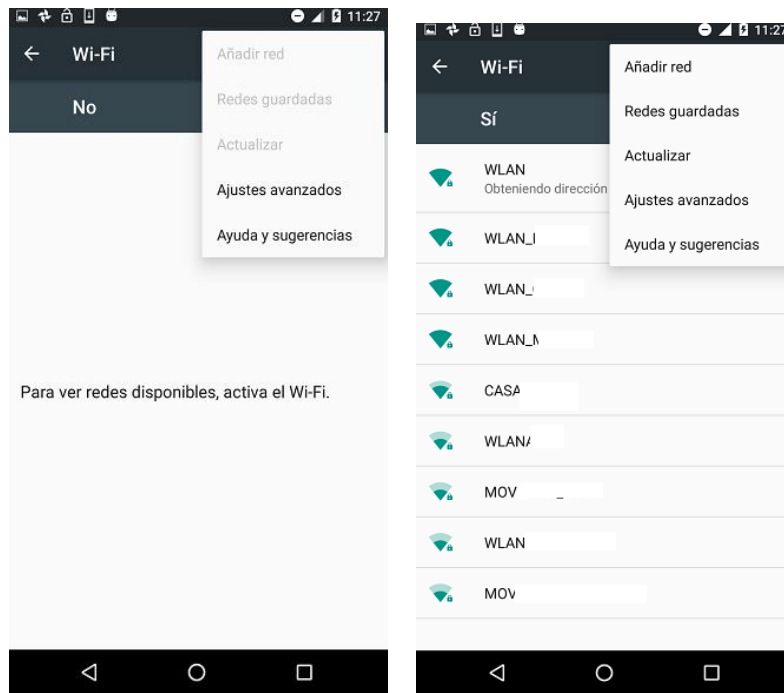
**Nota:** Por ejemplo, inicialmente cada 10 segundos por defecto, y mientras el dispositivo móvil no está conectado a ninguna red Wi-Fi, el dispositivo móvil genera tramas *probe request* de tipo *broadcast* para verificar la disponibilidad de redes Wi-Fi en su zona de alcance. Posteriormente, este intervalo puede ser mayor, de unos 15 segundos aproximadamente, y en ocasiones superándose este valor, por ejemplo, hasta 20 segundos; la frecuencia de escaneo es dependiente de la versión de Android y del estado del interfaz Wi-Fi.

1320. El comportamiento del interfaz Wi-Fi respecto a las operaciones de ahorro de energía del dispositivo móvil puede ser configurado desde el menú “Ajustes - Wi-Fi - Ajustes avanzados”, a través de las siguientes opciones:
1321. La opción “Usar Wi-Fi en suspensión” permite acceder a las diferentes alternativas de configuración disponibles: “Siempre” (opción por defecto), “Sólo si se está cargando”, o “Nunca (aumenta el uso de datos)”:



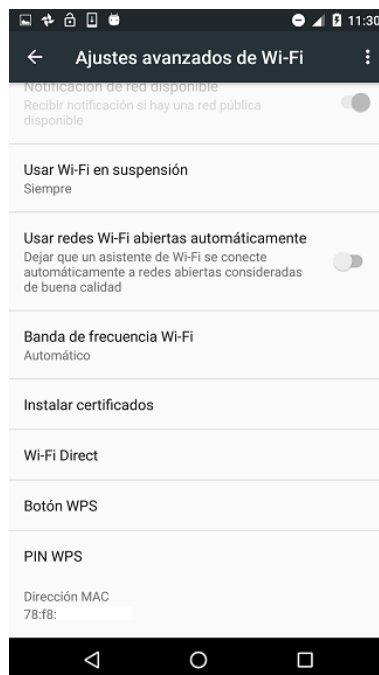
1322. La primera opción permite que el interfaz Wi-Fi esté activo y sea utilizado siempre, incluso cuando el dispositivo móvil está suspendido; la segunda opción permite el uso de Wi-Fi con el dispositivo móvil suspendido sólo si está conectado a la electricidad (cargando); la tercera opción nunca hace uso de Wi-Fi si el dispositivo móvil está suspendido, por lo que en ese caso se hará uso de la conexión de datos de telefonía móvil (aumentando potencialmente el consumo de datos).
1323. La opción “Optimización de Wi-Fi”, al igual que la opción “Solo conexiones estables” (existentes ambas en versiones previas de Android hasta 4.4.x) fue eliminada a partir de Android 5.x, por lo que no está disponible en Android 6.x.
1324. Una vez deshabilitado el interfaz Wi-Fi, el dispositivo móvil sólo hará uso de las capacidades de datos de telefonía móvil (ver apartado “16.2. Selección de la red de datos en Android”).
1325. La configuración detallada de las redes Wi-Fi puede llevarse a cabo a través del menú “Ajustes - Wi-Fi - Ajustes avanzados”.
1326. La opción “Banda de frecuencia Wi-Fi” permite seleccionar entre una configuración automática (por defecto) o manual, eligiendo sólo la banda de 2,4 Ghz o sólo la de 5 Ghz. Estas opciones no tienen implicaciones desde el punto de vista de seguridad.
1327. Debe tenerse en cuenta que, al igual que ocurría con el interfaz Bluetooth, para poder llevar a cabo la configuración completa de la pila de comunicaciones Wi-Fi a través del interfaz de usuario del dispositivo móvil es obligatorio activar el interfaz, por lo que se recomienda realizar las modificaciones de la configuración en un entorno seguro, evitando así potenciales ataques cuando los mecanismos de seguridad no han sido aún aplicados:





1328. Por ejemplo, la funcionalidad asociada a la opción para añadir una red Wi-Fi manualmente, mediante el menú “Añadir red” no está disponible (o habilitada) hasta que el interfaz Wi-Fi no ha sido activado.

1329. Sin embargo, en el caso de Wi-Fi, algunos ajustes de configuración avanzados sí están disponibles incluso con el interfaz Wi-Fi desactivado, como por ejemplo los siguientes:



1330. La dirección del interfaz Wi-Fi está disponible a través del menú “Ajustes - Información del teléfono - Estado”, y en concreto, en el campo “Dirección MAC de Wi-Fi”. La dirección es visible tanto si el interfaz Wi-Fi se encuentra activo como si está desactivado. También se dispone de la dirección en la parte inferior de la pantalla de ajustes avanzados:



**Nota:** La parte de la dirección Wi-Fi asociada al fabricante (primeros tres *bytes* de la dirección) puede permitir identificar el tipo de dispositivo móvil. En el ejemplo analizado, el valor “78:f8:82” está asignado por el IEEE (<http://standards.ieee.org/regauth/oui/index.shtml>) a “LG”:

|          |           |                                        |
|----------|-----------|----------------------------------------|
| 78-F8-82 | (hex)     | LG Electronics (Mobile Communications) |
| 78F882   | (base 16) | 60-39, Gasan-dong, Geumcheon-gu        |
|          |           | Seoul Seoul 153-801                    |
|          |           | KOREA, REPUBLIC OF                     |

1331. Es aconsejable comparar la dirección Wi-Fi del dispositivo móvil con su dirección Bluetooth (ver apartado “15. Comunicaciones Bluetooth”), con el objetivo de identificar si se trata de direcciones correlativas. En caso afirmativo, un potencial atacante podría obtener la dirección de Bluetooth a partir de la dirección Wi-Fi, con los riesgos que ello conlleva [Ref.- 400], al emplearse la ocultación de la dirección Bluetooth en diferentes escenarios como mecanismo de seguridad.

1332. En el caso del dispositivo móvil empleado para la elaboración de la presente guía ambas direcciones comparten el mismo rango del fabricante, pero sin ningún otro elemento común (asignación aleatoria dentro de ese rango).

## 16.2. SELECCIÓN DE LA RED DE DATOS EN ANDROID

**Nota:** La selección de la red de datos en Android afecta principalmente a la red de datos de telefonía móvil 2/3/4G (analizada en el apartado “18. Comunicaciones móviles: voz y datos”) y al interfaz Wi-Fi (ver el presente apartado).

1333. Debido a las múltiples opciones de conectividad de datos disponibles en los dispositivos móviles, como Bluetooth, y principalmente Wi-Fi y 2/3/4G, en caso de haber múltiples opciones habilitadas y disponibles, Android gestiona cual es la mejor conexión de datos a usar en cada momento a través del servicio Connectivity Service (o Connectivity Manager) [Ref.- 51]. De esta forma evita que el usuario tenga que decidir

constantemente que conexión utilizar y proporciona la conectividad necesaria a las apps que ejecutan en el dispositivo móvil.

1334. El Connectivity Service emplea diferentes criterios para seleccionar y mantener la mejor y única opción de conexión de datos, que por defecto da prioridad al interfaz Wi-Fi frente al interfaz de telefonía móvil (2/3/4G):

- Si Wi-Fi está activo y se activa 2/3/4G, este segundo no llegará a ser utilizado.
- Si 2/3/4G está activo y se activa Wi-Fi, la conexión 2/3/4G dejará de ser utilizada y pasará a hacerse uso de la conexión Wi-Fi.
- Si Wi-Fi está activo y se desactiva, el servicio comprobará el estado y la configuración de 2/3/4G, y si está disponible, lo habilitará y hará uso de este interfaz de red.

1335. Los eventos de activación y desactivación de los dos interfaces, Wi-Fi y 2/3/4G, pueden ser visualizados a través de los iconos del menú superior de Android.

1336. El comportamiento del interfaz Wi-Fi, y en consecuencia del interfaz 2/3/4G, respecto a las operaciones de ahorro de energía del dispositivo móvil cuando éste se encuentra en estado suspendido, puede ser configurado desde el menú de ajustes de Wi-Fi, tal y como se detalla en el apartado “16.1. Utilización y configuración de las comunicaciones Wi-Fi”.

1337. El Connectivity Service no permite disponer de varias conexiones activas simultáneamente, opción recomendada desde el punto de vista de seguridad para evitar escenarios *dual homing* donde la conexión Wi-Fi y la conexión de datos de telefonía móvil (2/3/4G) están activas simultáneamente, con el objetivo de que el dispositivo móvil no actúe de pasarela entre distintas redes.

1338. Desde el punto de vista de seguridad podría considerarse más seguro cursar todo el tráfico de datos a través de las redes de telefonía móvil (cuando estén disponibles según la cobertura existente) en lugar de a través de redes Wi-Fi (especialmente si se quiere hacer uso de redes Wi-Fi abiertas, opción desaconsejada desde el punto de vista de seguridad), siempre que se fuerce a que la conexión de datos de telefonía móvil emplee tecnologías 3/4G frente a 2G (ver apartado “18. Comunicaciones móviles: voz y datos”). Para ello sería necesario deshabilitar el interfaz Wi-Fi y habilitar las comunicaciones móviles de datos.

1339. En caso contrario, es decir, si se requiere cursar todo el tráfico de datos a través de redes Wi-Fi (con un nivel de seguridad adecuado) se recomienda consultar el apartado “18. Comunicaciones móviles: voz y datos”, que contiene información detallada de cómo deshabilitar el interfaz de datos de telefonía móvil 2/3/4G.

1340. Cuando ambas conexiones de datos han sido activadas, a través del comando “*ifconfig*” (vía “adb shell”) es posible ver que sólo el interfaz Wi-Fi (de mayor prioridad), tiene asignada una dirección IP. El interfaz asociado a las capacidades de datos de telefonía móvil (“rmnet\_data0”), anteriormente denominado “rmnet0”, se encuentra en estado inactivo (o “DOWN”), motivo por el que no es mostrado en la imagen inferior, al estar activo (o “UP”) el interfaz Wi-Fi (“wlan0”).

```

Selecionar Windows PowerShell
127 shell@bullhead:/ $ ifconfig
rmnet_ipa0 Link encap:UNSPEC
 UP RUNNING MTU:2000 Metric:1
 RX packets:151 errors:0 dropped:0 overruns:0 frame:0
 TX packets:187 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:7372 TX bytes:10856

wlan0 Link encap:UNSPEC
 inet addr:172.16.32.110 Bcast:172.16.32.255 Mask:255.255.255.0
 inet6 addr: fe80::7af8:82ff:fed0:3a25/64 Scope: Link
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:2688 errors:0 dropped:0 overruns:0 frame:0
 TX packets:1890 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:3000
 RX bytes:1020442 TX bytes:802713

dummy0 Link encap:UNSPEC
 inet6 addr: fe80::f41d:80ff:fee8:3d84/64 Scope: Link
 UP BROADCAST RUNNING NOARP MTU:1500 Metric:1
 RX packets:0 errors:0 dropped:0 overruns:0 frame:0
 TX packets:3 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:0
 RX bytes:0 TX bytes:210

p2p0 Link encap:UNSPEC
 UP BROADCAST MULTICAST MTU:1500 Metric:1
 RX packets:0 errors:0 dropped:0 overruns:0 frame:0
 TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:3000
 RX bytes:0 TX bytes:0

rmnet_data0 Link encap:UNSPEC
 inet6 addr: fe80::a48c:5b1c:c91a:5aa5/64 Scope: Link
 UP RUNNING MTU:3000 Metric:1
 RX packets:151 errors:0 dropped:0 overruns:0 frame:0
 TX packets:187 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:6040 TX bytes:10856

lo Link encap:UNSPEC
 inet addr:127.0.0.1 Mask:255.0.0.0
 inet6 addr: ::1/128 Scope: Host
 UP LOOPBACK RUNNING MTU:65536 Metric:1
 RX packets:968 errors:0 dropped:0 overruns:0 frame:0
 TX packets:968 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:0
 RX bytes:81000 TX bytes:81000

shell@bullhead:/ $

```

**Nota:** En versiones anteriores de Android (hasta la 5.x inclusive), existía el comando *netcfg*, que permitía visualizar la configuración de las redes de forma rápida. El comando *netcfg* se eliminó en Android 6.x<sup>79</sup>, y se reemplazó por el comando *ifconfig* (heredado de Linux).

1341. En el caso del interfaz Wi-Fi (“wlan0”), cuando se deshabilita, dejará de mostrarse en la salida del comando *ifconfig* (al no encontrarse en estado activo o “UP”). El interfaz asociado a las capacidades de datos de telefonía móvil (“rmnet\_data0”) pasará a tener asociada la dirección IP que le otorgue el proveedor del servicio de telefonía por DHCP, y el tráfico entre el dispositivo móvil e Internet se cursará a través suyo:

<sup>79</sup> [https://github.com/bbc/device\\_api-android/issues/92](https://github.com/bbc/device_api-android/issues/92)

```

Windows PowerShell
shell@bullhead:/ $ ifconfig
rmnet_ipa0 Link encap:UNSPEC
UP RUNNING MTU:2000 Metric:1
RX packets:199 errors:0 dropped:0 overruns:0 frame:0
TX packets:248 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:16908 TX bytes:18724

dummy0 Link encap:UNSPEC
inet6 addr: fe80::f41d:80ff:fee8:3d84/64 Scope: Link
UP BROADCAST RUNNING NOARP MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:3 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0 TX bytes:210

rmnet_data0 Link encap:UNSPEC
inet addr:100.80.138.160 Mask:255.255.255.192
inet6 addr: fe80::9585:3052:f134:567c/64 Scope: Link
UP RUNNING MTU:1500 Metric:1
RX packets:48 errors:0 dropped:0 overruns:0 frame:0
TX packets:61 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:9600 TX bytes:7868

r_rmnet_data0 Link encap:UNSPEC
inet6 addr: fe80::a48c:5b1c:c91a:5aa5/64 Scope: Link
UP RUNNING MTU:3000 Metric:1
RX packets:151 errors:0 dropped:0 overruns:0 frame:0
TX packets:187 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:6040 TX bytes:10856

lo Link encap:UNSPEC
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope: Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:968 errors:0 dropped:0 overruns:0 frame:0
TX packets:968 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:81000 TX bytes:81000

shell@bullhead:/ $

```

1342. Mediante la tabla de rutas (“/proc/net/route”) es posible validar el comportamiento descrito y el interfaz prioritario para el intercambio de datos. La parte superior de la siguiente imagen muestra como el tráfico es dirigido a través del interfaz Wi-Fi (“wlan0”) pese a estar ambos interfaces de red activos, empleando el router por defecto para la red 172.16.32.0 (en hexadecimal, y con los valores de los octetos invertidos, 0x002010AC); la parte inferior, muestra cómo el tráfico se enruta a través del interfaz de telefonía móvil empleando el router por defecto para la red 100.81.255.160 (en hexadecimal, y con los valores de los octetos invertidos, 0xA0FF5164):

```

shell@bullhead:/ $ cat /proc/net/route

```

| Interface | Destination | Gateway  | Flags | RefCnt | Use | Metric | Mask     | MTU | Window | IRTT |
|-----------|-------------|----------|-------|--------|-----|--------|----------|-----|--------|------|
| wlan0     | 002010AC    | 00000000 | 0001  | 0      | 0   | 0      | 00FFFFFF | 0   | 0      | 0    |

```

l|shell@bullhead:/ $ cat /proc/net/route

```

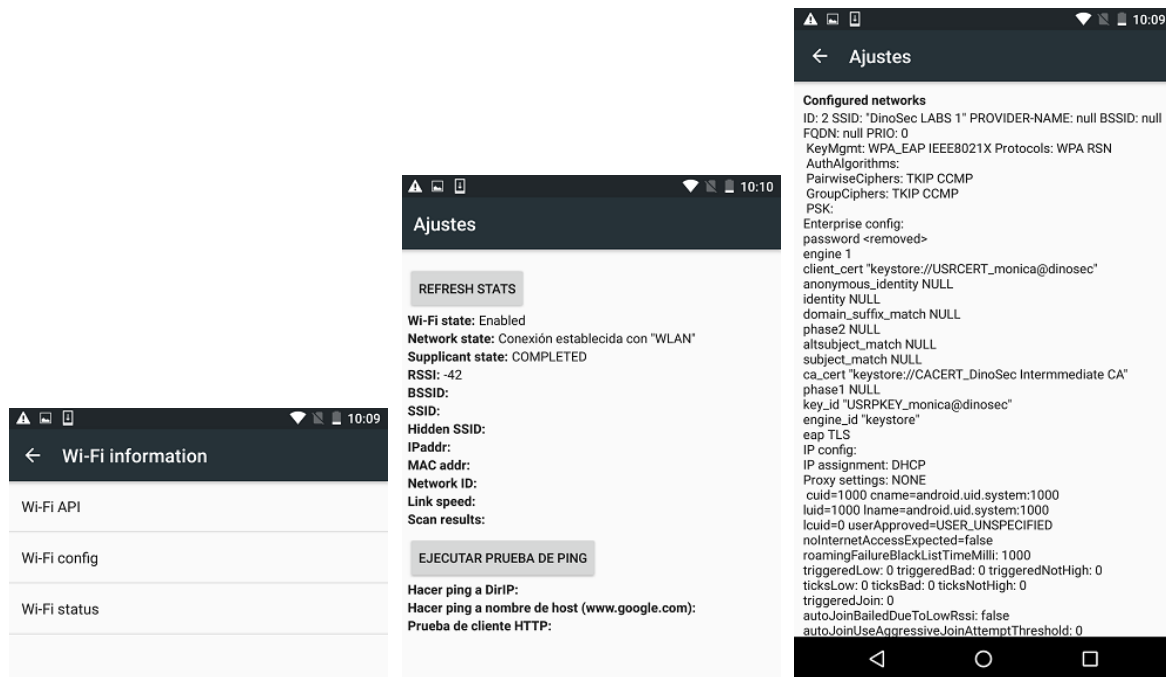
| Interface   | Destination | Gateway  | Flags | RefCnt | Use | Metric | Mask     | MTU | Window | IRTT |
|-------------|-------------|----------|-------|--------|-----|--------|----------|-----|--------|------|
| rmnet_data0 | A0FF5164    | 00000000 | 0001  | 0      | 0   | 0      | E0FFFFFF | 0   | 0      | 0    |

```

shell@bullhead:/ $

```

1343. Adicionalmente, en el menú de “Prueba” (o *testing*) accesible mediante la marcación del código **##\*#4636#\*#\*** en el dispositivo móvil, se ofrece el menú “Wi-Fi information”, que a su vez contiene las opciones “Wi-Fi Status” (ver imagen inferior central), “Wi-Fi Config” (ver imagen derecha) y “Wi-Fi API”:



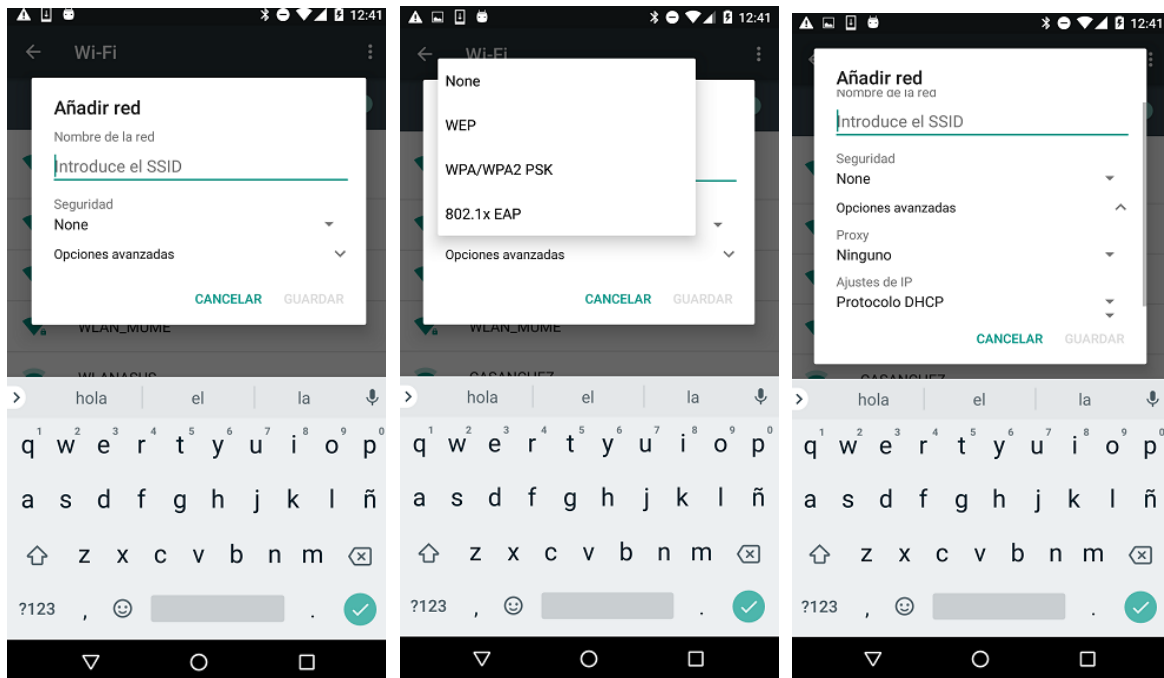
1344. La opción “Wi-Fi API” alberga opciones que actúan como comandos sobre el interfaz Wi-Fi. Es importante reseñar que se trata de opciones no soportadas, por lo que no se recomienda recurrir a ellas. Por ejemplo, “disableNetwork” deshabilita la red cuyo identificador se proporcione; “disconnect” desconecta el interfaz Wi-Fi por completo; “enableNetwork” habilita la red que se pase como parámetro; “getConfiguredNetworks” y “getConnectionInfo” no funcionan con la versión 6.0.1 en el dispositivo Nexus 5x utilizado en la elaboración de la presente guía.



### 16.3. RECOMENDACIONES DE SEGURIDAD PARA LA CONEXIÓN A REDES WI-FI

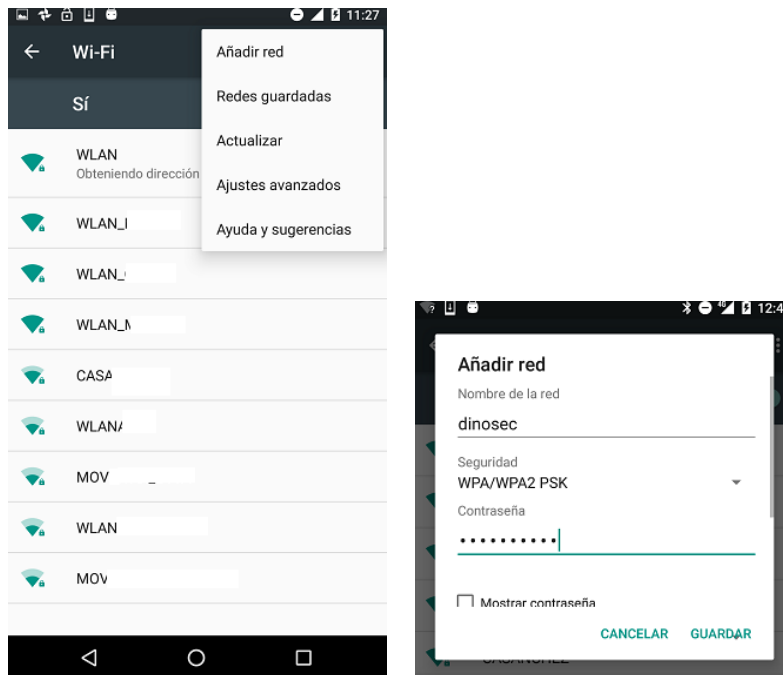
1345. Este apartado proporciona recomendaciones de configuración a través de los diferentes parámetros y opciones disponibles en Android para la conexión segura a redes Wi-Fi.
1346. La configuración manual y detallada de las redes Wi-Fi se puede realizar desde el menú “Ajustes - Wi-Fi”, y en concreto mediante la opción de añadir una red Wi-Fi manualmente, a través del menú “Añadir red” de la parte superior (disponible con el interfaz Wi-Fi activo).
1347. Esta opción permite seleccionar todas las opciones de configuración de conexión de una nueva red Wi-Fi, incluyendo el nombre de red (o SSID), y el mecanismo de seguridad a emplear (abierta o ninguna, WEP, WPA/WPA2 PSK o 802.1x EAP; todos ellos

analizados posteriormente). La opción “Opciones avanzadas” permite seleccionar el proxy y la configuración de la dirección IP:

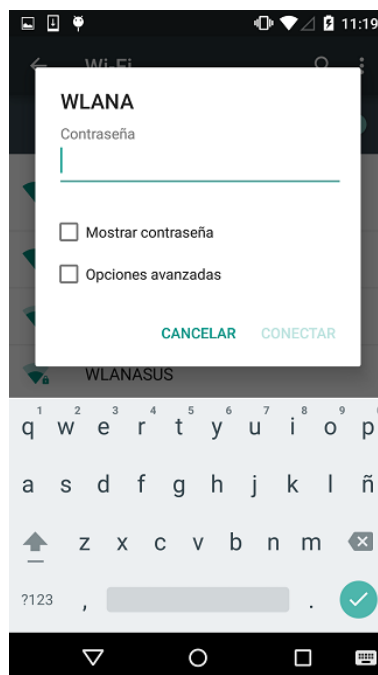


1348. Adicionalmente, mediante la selección de una de las redes disponibles al alcance del dispositivo móvil (listadas en la misma pantalla bajo la sección “Wi-Fi”) es posible seleccionar la red Wi-Fi con la que se desea establecer la conexión.
1349. Como se explicará posteriormente en detalle, desde el punto de vista de seguridad se recomienda seleccionar la red Wi-Fi con la que se quiere establecer la conexión de la lista de redes visibles, en lugar de añadirla manualmente a través del menú “Añadir red”.
1350. Habitualmente se recomendaba hacer uso del mecanismo de configuración manual frente a seleccionar la red Wi-Fi desde el listado de redes disponibles, ya que, en este segundo caso, no se dispone de tanta flexibilidad y granularidad para seleccionar los diferentes parámetros de configuración y los mecanismos de seguridad de la red. Sin embargo, en el caso de Android se recomienda añadir la red Wi-Fi desde el listado de redes disponibles (ver apartado “16.5. Conexión automática a redes Wi-Fi: ocultas o visibles y restricción de conexión”) para evitar una vulnerabilidad existente al añadir la red Wi-Fi de forma manual.
1351. Las redes aparecen clasificadas en la lista (por defecto) en orden según la intensidad de señal de cada una de ellas, siendo las redes de la zona superior las de mayor intensidad de señal (de mayor a menor intensidad). La lista permite de manera muy limitada identificar los mecanismos de seguridad empleados por cada una de la redes Wi-Fi mediante el icono disponible junto al nombre de cada red:





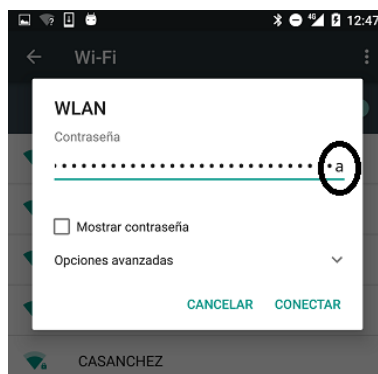
1352. La existencia de algún mecanismo o tipo de seguridad en cada red Wi-Fi viene únicamente reflejado por un icono de un candado, pero no se indica el tipo de seguridad concreto empleado por la red.
1353. Para establecer la conexión con una red próxima únicamente es necesario introducir la contraseña de acceso a la red (ver imagen superior derecha) en caso de estar protegida por una contraseña (WEP o WPA/WPA2 PSK). En el caso de redes abiertas directamente se establece la conexión con la red una vez ha sido seleccionada por parte del usuario de la lista (o una vez se ha proporcionado su nombre si se añadiera manualmente):



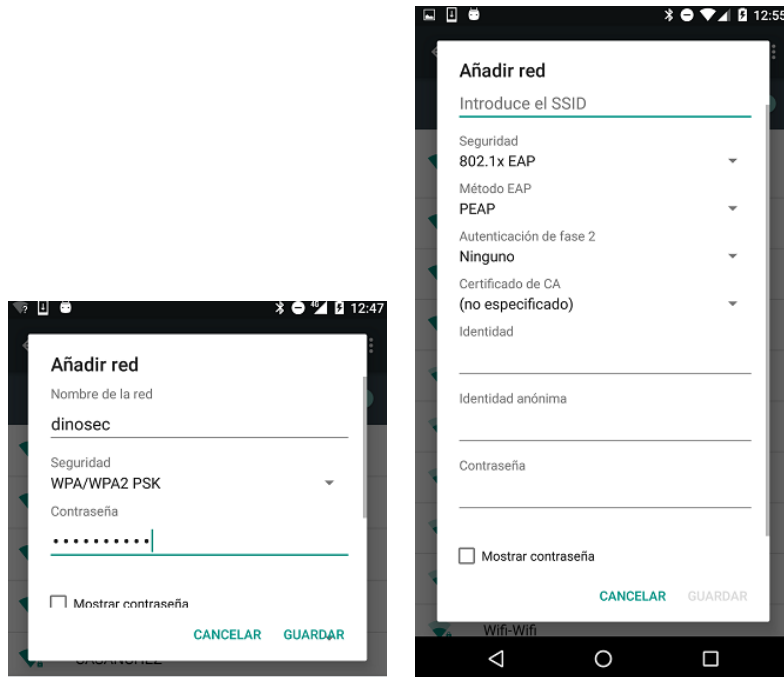
1354. Todas las redes que implementan algún tipo de mecanismo de seguridad, WEP, WPA ó WPA2, aparecen con un candado en el icono de la red y, a partir de Android 5.x no se puede diferenciar el mecanismo de seguridad empleado específicamente desde el listado de redes disponibles, tal como ocurría en versiones previas de Android, como

4.4.x, donde se proporcionaban los detalles bajo el nombre de la red, y se permitía diferenciar, por ejemplo, entre redes WPA y WPA2.

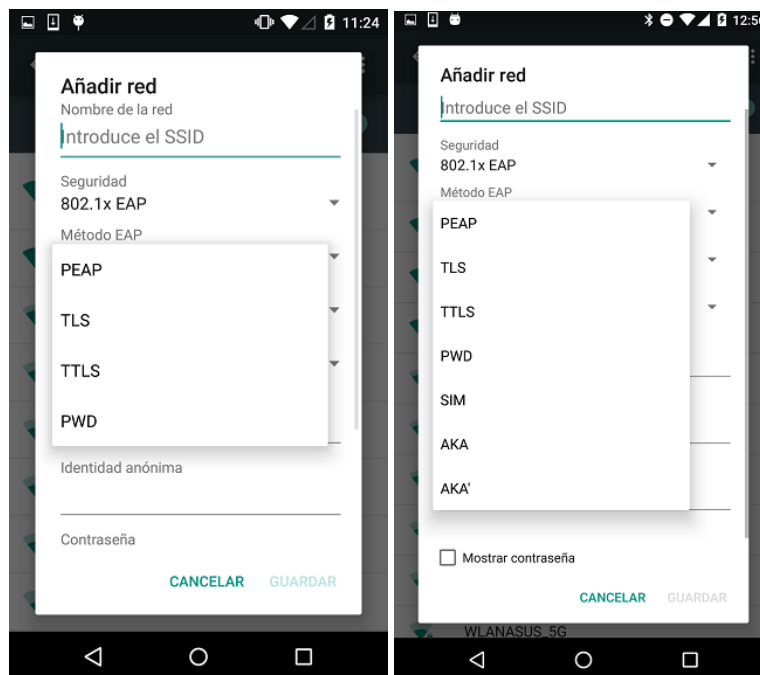
1355. Al establecer una primera conexión con una nueva red Wi-Fi, se recomienda agregar la nueva red Wi-Fi de forma automática a través del listado de redes disponibles (debido a una vulnerabilidad al añadirla manualmente que se describirá posteriormente), pese a que no sea posible visualizar y especificar todas las opciones de configuración disponibles que se detallan a continuación.
1356. El proceso de configuración de la contraseña puede permitir al usuario no ocultar el texto introducido en pantalla (por ejemplo, con el carácter “.”) mediante la opción “Mostrar contraseña” (no habilitada por defecto). Hay que señalar, no obstante, que cada carácter que se introduce sí se muestra brevemente tras ser introducido, por lo que conviene prestar atención y evitar configurar la red si no se dispone de la privacidad suficiente.



1357. En caso de habilitar la opción de “Mostrar contraseña”, desaconsejada desde el punto de vista de seguridad, el usuario debe prestar atención a cómo y dónde introduce la contraseña de conexión a la red Wi-Fi para evitar que un potencial atacante la obtenga mediante acceso visual a la pantalla del dispositivo móvil.
1358. Dentro de las opciones de configuración de una nueva red Wi-Fi, la primera pantalla de configuración hace posible especificar el nombre de la red (SSID) y el mecanismo de seguridad a emplear: Ninguna (opción por defecto), WEP, WPA/WPA2 PSK o 802.1x EAP.
1359. En caso de seleccionar una red WEP o WPA/WPA2 PSK, es necesario especificar la contraseña de la red:



1360. En el caso de seleccionar una red 802.1x EAP, es necesario especificar el tipo de método EAP a emplear: PEAP, TLS, TTLS, PWD<sup>80</sup>, SIM, AKA o AKA' y el método de autenticación de fase 2 (Ninguno, MSCHAPV2 o GTC, *Generic Token Card*), junto a los certificados asociados (opcionalmente) y a las credenciales del usuario (descritos posteriormente):



**Nota:** En la versión de Android 5.x únicamente se soportaban los métodos PEAP, TLS, TTLS y PWD para las redes 802.1x EAP (ver imagen superior izquierda). A partir de Android 6.x, se incorporan también los métodos SIM (*Subscriber Identity Module*, empleado para autenticación e intercambio de claves a través de redes GSM), AKA (Authentication and Key Agreement, para autenticación e intercambio de claves a través de UMTS) y AKA' (variante del AKA para redes 3G).

<sup>80</sup> Los tres últimos tipos de métodos EAP corresponden según los estándares a EAP-TLS, EAP-TTLS y EAP-PWD.

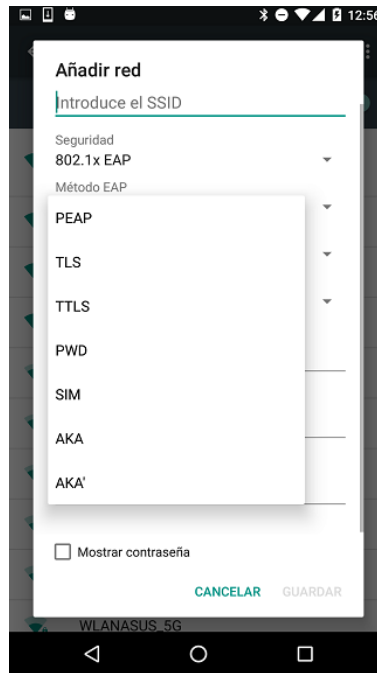
1361. Desafortunadamente, Android no permite especificar detalladamente los mecanismos de autenticación y de cifrado de datos, no siendo posible diferenciar entre redes WPA y redes WPA2 (tanto Personal, PSK, como Empresarial, o Enterprise o 802.1x), ni el tipo de cifrado: TKIP, AES o ambos.
1362. Por otro lado, tampoco es posible especificar si se permiten conexiones a redes con infraestructura, es decir, puntos de acceso, a redes entre equipos o ad-hoc, o ambas.
1363. Android por defecto sigue sin permitir conexiones Wi-Fi ad-hoc (IBSS, Independent Basic Service Set), permitiendo únicamente conexiones a redes Wi-Fi con infraestructura, es decir, basadas en puntos de acceso. La pantalla que muestra el listado de redes Wi-Fi disponibles directamente no muestra las redes ad-hoc.

**Nota:** Esta limitación del gestor de conexiones Wi-Fi de Android está implícita en el diseño del sistema y es conocida desde las primeras versiones de Android [Ref.- 39].

Aunque desde el punto de vista de seguridad es preferible conectar a redes Wi-Fi con infraestructura, dado que hoy en día es también posible hacer uso de redes ad-hoc con un nivel de seguridad razonable, existe la posibilidad de modificar este comportamiento existente por defecto y habilitar el soporte para redes *ad-hoc* en dispositivos móviles Android *rooteados* a través de un conjunto de parches y modificaciones disponibles, por ejemplo, en distribuciones de Android de terceros, como LineageOS (previamente CyanogenMod [Ref.- 40]).

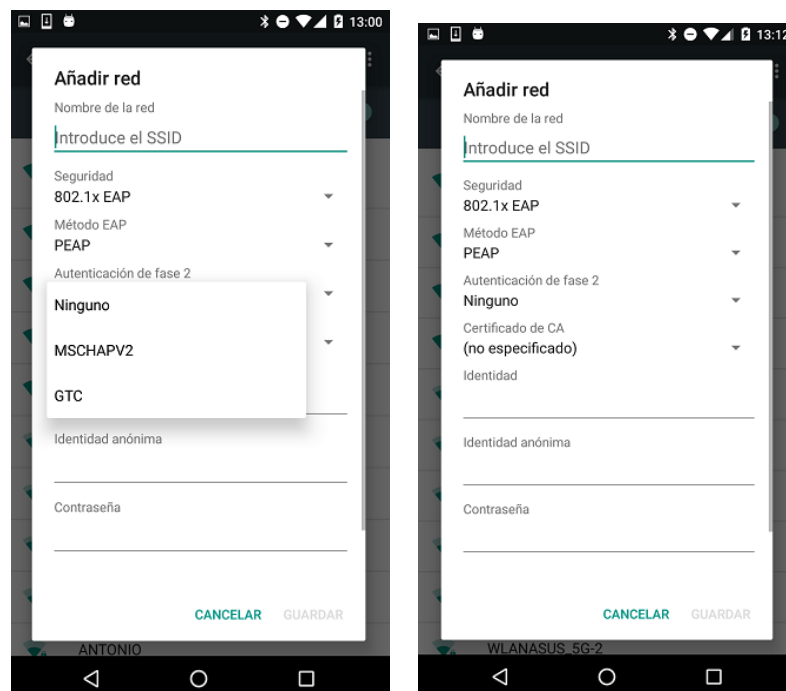
Las versiones 2.3, 4.0 (y posteriores) de Android implementan soporte para Wi-Fi Direct (“P2P”, ver apartado “16.7. Wi-Fi Direct (“P2P”)”), un estándar de comunicación Wi-Fi directa entre dispositivos que es similar (pero no sustituye completamente) a las comunicaciones *ad-hoc* [Ref.- 41], y añade mejoras de seguridad, facilidad de configuración, rendimiento y consumo.

1364. Igualmente, el proceso de configuración de las redes Wi-Fi en Android no permite claramente, y de forma explícita, especificar o comprobar si la red Wi-Fi es oculta o visible (ver apartado “1389. En caso de que sea necesario conectarse temporalmente a redes inalámbricas no ocultas (ver apartado “16.5. Conexión automática a redes Wi-Fi: ocultas o visibles y restricción de conexión”), o que, siendo ocultas, no sean de uso reiterado, se aconseja proceder a borrar la red a través del botón “Olvidar” para eliminar su almacenamiento y configuración del dispositivo móvil Android, y evitar así ataques basados en la suplantación de redes Wi-Fi cuyo nombre (o SSID) sea conocido por el dispositivo móvil.
1365. Conexión automática a redes Wi-Fi: ocultas o visibles”).
1366. Se recomienda conectarse únicamente a redes que emplean WPA2 (Personal, WPA2-PSK, o Enterprise, WPA2) como mecanismo de autenticación, y AES como mecanismo de cifrado. En su defecto, debería emplearse WPA/TKIP (desaconsejado actualmente), pero en ningún caso se debe hacer uso de WEP.
1367. En caso de emplear WPA2 (o WPA) en su versión Enterprise, es decir, con mecanismos basados en 802.1x/EAP, la pantalla de ajustes permite especificar los parámetros de configuración asociados al tipo de mecanismo EAP empleado:



1368. Todos los campos posibles de configuración están disponibles en el interfaz de usuario de Android para los distintos tipos de EAP, lo que puede crear cierta confusión, ya que no todos los tipos de EAP hacen uso de todos y cada uno de los diferentes campos mostrados.

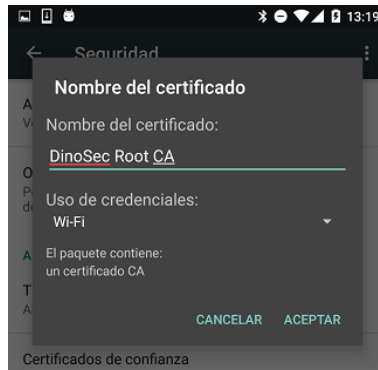
1369. Una vez seleccionado el tipo de método EAP a emplear, en primer lugar es necesario definir el tipo de autenticación interna (o de fase 2): Ninguno, MSCHAPV2 (PEAPv0) o GTC (EAP-GTC, *Generic Token Card*).



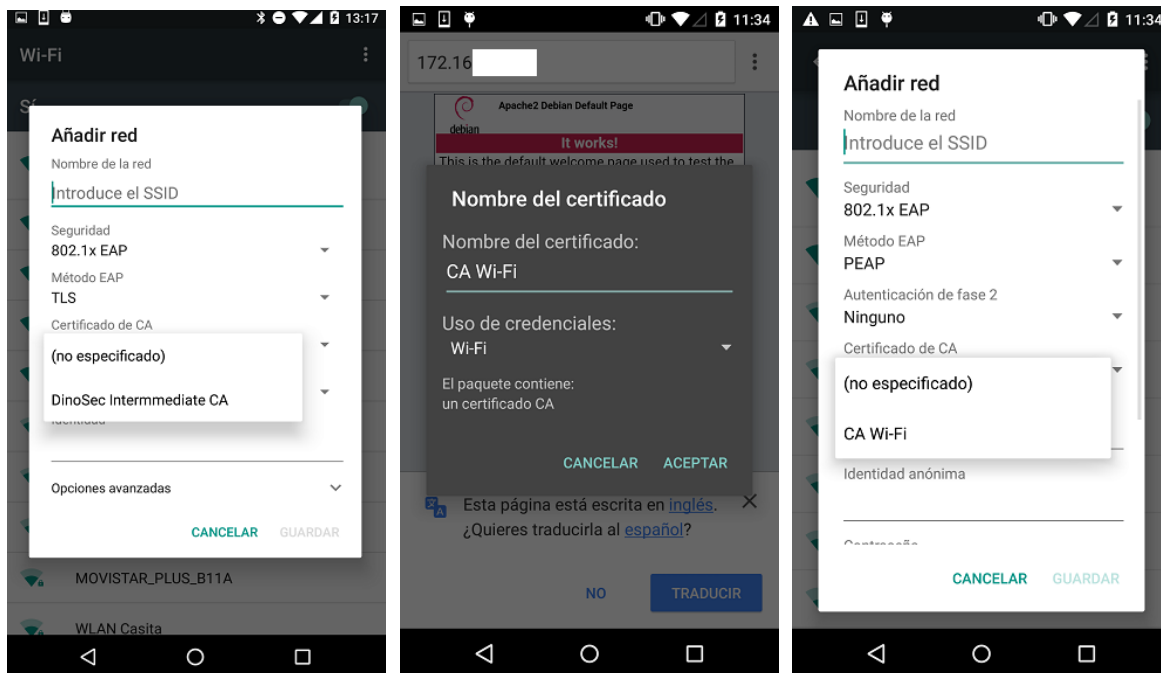
1370. Adicionalmente, para PEAP (Protected EAP) debe definirse el certificado digital raíz de la autoridad certificadora (CA) que ha emitido el certificado digital del servidor de autenticación de la red Wi-Fi (RADIUS), mediante el campo “Certificado de CA”, que debe haber sido añadido previamente al dispositivo móvil (ver apartado “11.3. Gestión de certificados digitales”). Asimismo, deben proporcionarse las credenciales del usuario

(nombre de usuario y contraseña, y opcionalmente el dominio Windows (por ejemplo “DOMINIO\usuario”) en los campos “Identidad” y “Contraseña” (ver imágenes superiores).

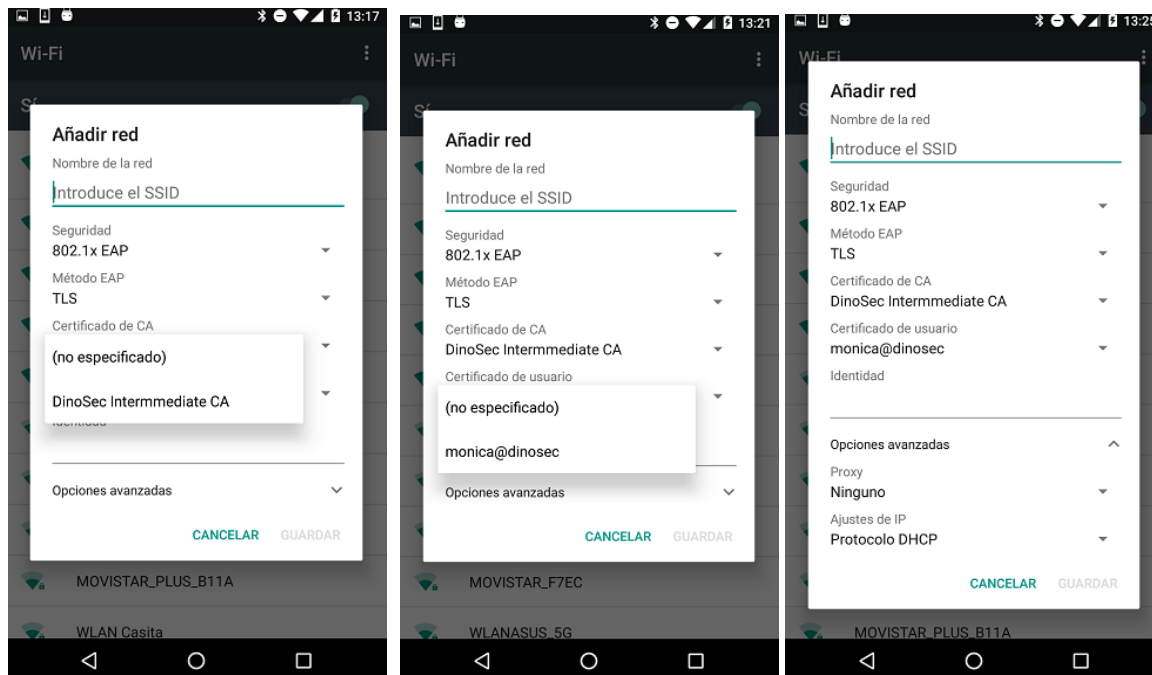
1371. Por otro lado, para TTLS (conocido como EAP-TTLS) es necesario definir los mismos elementos que para PEAP, pero haciendo uso de la identidad anónima a utilizar para la autenticación externa o de fase 1, mediante el campo “Identidad anónima” (por ejemplo, con el valor estándar “anonymous”).
1372. Por último, para TLS (conocido como EAP-TLS) es necesario definir los mismos elementos que para PEAP, pero sustituyendo las credenciales tradicionales del usuario (nombre de usuario y contraseña) por un certificado digital cliente personal y que identifica al usuario, mediante el campo “Certificado de usuario”, y que también debe haber sido añadido previamente al dispositivo móvil (ver apartado “11.3. Gestión de certificados digitales”).
1373. Tanto en el caso de autenticación PEAP como TLS o TTLS, es necesario (aunque opcional) importar previamente en Android el certificado digital de la autoridad certificadora (CA), raíz o intermedia, empleada para generar los certificados digitales asociados al servidor de autenticación de la red Wi-Fi (servidor RADIUS).
1374. Incluso en el caso en el que se usen certificados emitidos por una de las CAs públicas ya existentes por defecto en Android, éstas no son mostradas por defecto en el campo “Certificado de CA”, por lo que también es necesario importarlas manualmente, especificando que su propósito es utilizarlas para redes Wi-Fi, como ilustra la imagen siguiente:



1375. Para instalar el certificado basta con transferir el fichero del certificado digital al dispositivo móvil, a través de un servidor web (preferiblemente propio, frente a servidores públicos de terceros [Ref.- 45]), correo electrónico, o mediante una tarjeta de almacenamiento externa, o el almacenamiento interno del propio dispositivo móvil (ver apartado “11.3. Gestión de certificados digitales”).
1376. Una vez el certificado ha sido importado en el dispositivo móvil, estará disponible a través del menú de configuración de la red Wi-Fi 802.1x EAP basada en PEAP, TTLS o TLS, desde el campo “Certificado de CA”:



1377. En el caso de emplear EAP-TLS siempre es necesario importar el certificado digital personal del cliente (en formato PKCS#12) en el dispositivo móvil. Para instalar el certificado personal basta con transferir el fichero del certificado digital personal (".pfx" o ".p12") al dispositivo móvil, por ejemplo, a través de una tarjeta de almacenamiento externa, o el almacenamiento interno del propio dispositivo móvil, un correo electrónico, o desde un servidor web privado.



1378. Igualmente, una vez el certificado personal ha sido importado en el dispositivo móvil (ver apartado "11.3. Gestión de certificados digitales"), estará disponible a través del menú de configuración de la red Wi-Fi 802.1x EAP basada en TLS, desde el campo "Certificado de usuario" (ver imágenes superiores).

**Nota:** El certificado digital cliente (o de usuario) es identificado por defecto con un *string* con letras y números, correspondientes al identificador de la clave, si no se modificó su nombre



asociado durante el proceso de importación (ver apartado “11.3. Gestión de certificados digitales”). En caso de que se modifique su nombre, el certificado es mostrado con el nombre elegido por el usuario. Android permite importar el mismo certificado digital cliente con diferentes nombres múltiples veces.

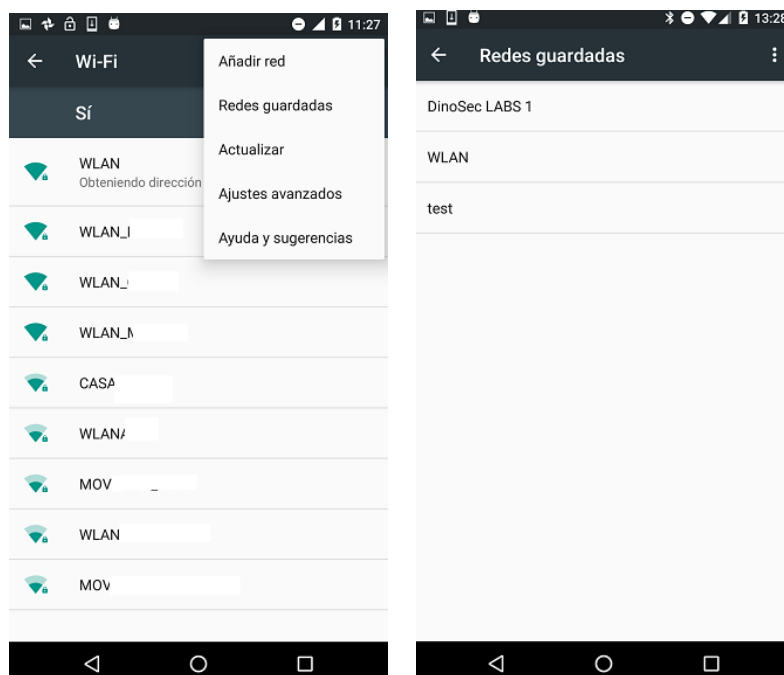
1379. El certificado de la CA puede ser importado simultáneamente junto con el certificado digital cliente empleado para EAP TLS (en este caso, ambos certificados, tanto el cliente como el de la CA, son identificados con el mismo nombre), o de manera independiente (tal como se describió previamente).

## 16.4. LISTA DE REDES PREFERIDAS (PNL)

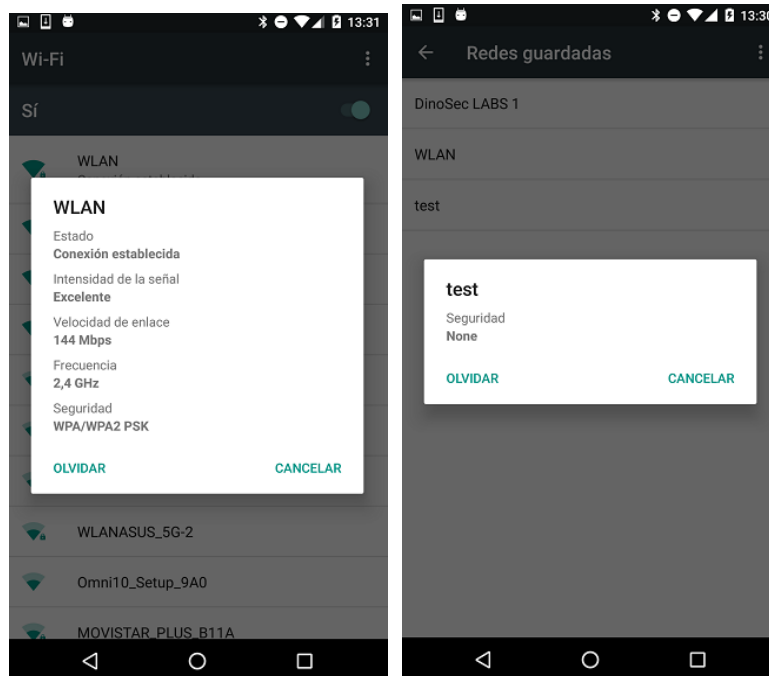
1380. La lista de redes preferidas (PNL, *Preferred Network List*), es decir, a las que se ha conectado previamente el dispositivo móvil o que han sido configuradas en el mismo (ver apartado “16.5. Conexión automática a redes Wi-Fi: ocultas o visibles y restricción de conexión”), no puede ser visualizada tras habilitar el interfaz Wi-Fi, desde el menú “Ajustes - Wi-Fi”, y en concreto, al final de la lista de redes disponibles actualmente, mediante el texto “Fuera de rango” (tal como ocurría en versiones previas de Android, como 4.4.x).

1381. En su lugar, las redes almacenadas en la PNL en Android 6.x están disponibles a través de las opciones avanzadas, mediante el menú “Redes guardadas”. Las redes Wi-Fi son identificadas por su nombre o SSID.

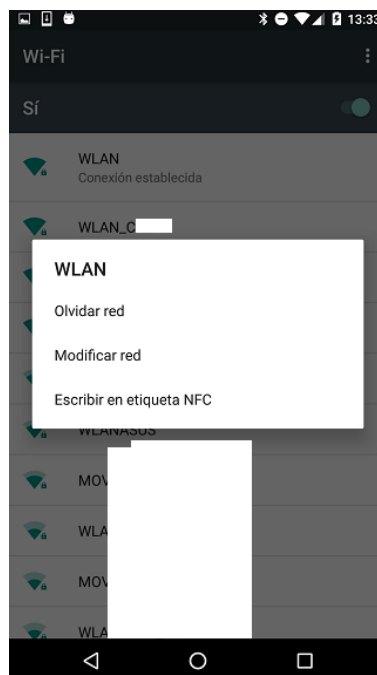
1382. Las redes existentes en la PNL que están disponibles actualmente (suponiendo que el dispositivo móvil está conectado a otra red conocida, por ejemplo a la red Wi-Fi “WLAN”) aparecerán en la lista de redes disponibles con un distintivo que las identifica como redes con las que previamente se ha establecido una conexión, mediante el texto “Guardado” (por ejemplo, la red “pruebas” en la imagen inferior), salvo que se trate de la red Wi-Fi a la que está actualmente conectado el dispositivo móvil, ya que ésta aparecerá con el texto “Conexión establecida”:



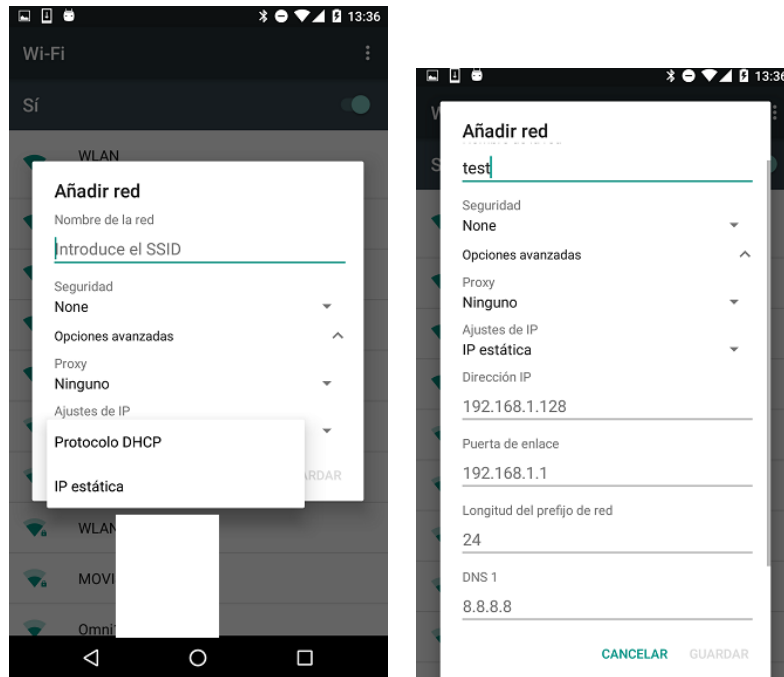
1383. Mediante la selección de una red existente en la PNL desde la pantalla con el listado de redes Wi-Fi (con una pulsación breve sobre la misma), es posible eliminarla de la PNL a través del botón “Olvidar” (tanto si es visible actualmente y hay establecida una conexión con ella, imagen izquierda, como si es visible pero no hay una conexión establecida, imagen central, o como si no es visible actualmente pero está en la PNL, imagen derecha):



1384. Mediante la selección de una red existente en la PNL desde la pantalla con el listado de redes Wi-Fi (con una pulsación prolongada sobre la misma), es también posible eliminarla de la PNL a través de la opción “Olvidar red” o editar sus detalles (como la contraseña de acceso) a través de la opción “Modificar red” (tanto si no es visible actualmente, como si lo es):



1385. Por defecto, la configuración de TCP/IP empleada para la conexión a las redes Wi-Fi hace uso de una dirección IP obtenida dinámicamente mediante el protocolo DHCP (ver apartado “19. Comunicaciones TCP/IP”).
1386. Android permite, a través de la opción “Opciones avanzadas”, fijar una dirección IP estática (junto a la puerta de enlace, la máscara o prefijo de red, y los servidores DNS primario y secundario):



1387. Para llevar a cabo la configuración de TCP/IP, o modificaciones en la misma, sí es necesario que el interfaz Wi-Fi esté activo para poder seleccionar la red Wi-Fi de la lista de redes visibles o de la PNL.
1388. En resumen, desde el punto de vista de seguridad de Android como cliente Wi-Fi, se recomienda hacer uso de redes inalámbricas no ocultas (ver apartado “16.5. Conexión automática a redes Wi-Fi: ocultas o visibles y restricción de conexión”), basadas en WPA2 con cifrado AES, y autenticación de tipo Personal, con una contraseña de acceso (PSK, *Pre-Shared Key*) suficientemente robusta (de más de 20 caracteres), o autenticación de tipo Enterprise, basada en mecanismos de autenticación 802.1x/EAP, y empleando EAP-TLS (con certificados digitales cliente) preferiblemente, y correctamente configurada y gestionada.

**Nota:** Con el objetivo de proteger el dispositivo móvil y aumentar su nivel de seguridad, se desaconseja el uso de redes inalámbricas públicas y abiertas, con un nivel de seguridad reducido o inexistente (sin mecanismos de autenticación y cifrado), como por ejemplo *hotspots* Wi-Fi disponibles en hoteles, aeropuertos o centros de conferencias [Ref.- 194].

Los riesgos de seguridad asociados a este tipo de entornos incluyen la captura e interceptación del tráfico y datos por parte de un potencial atacante, la posibilidad de inyección de tráfico para la realización de ataques directos y de accesos no autorizados contra el dispositivo móvil, ataques de suplantación de la red, y ataques de denegación de servicio (DoS), entre otros.

1389. En caso de que sea necesario conectarse temporalmente a redes inalámbricas no ocultas (ver apartado “16.5. Conexión automática a redes Wi-Fi: ocultas o visibles y

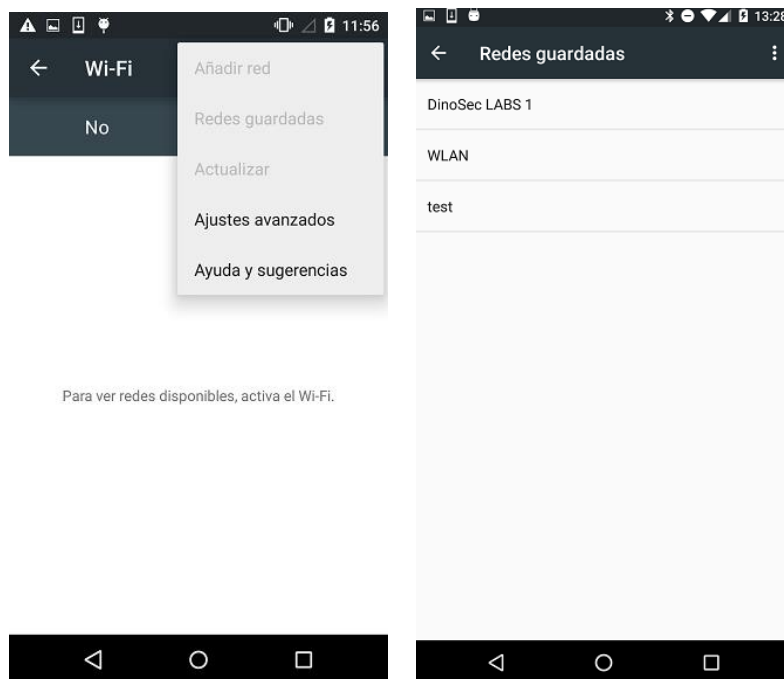
restricción de conexión”), o que, siendo ocultas, no sean de uso reiterado, se aconseja proceder a borrar la red a través del botón “Olvidar” para eliminar su almacenamiento y configuración del dispositivo móvil Android, y evitar así ataques basados en la suplantación de redes Wi-Fi cuyo nombre (o SSID) sea conocido por el dispositivo móvil.

## 16.5. CONEXIÓN AUTOMÁTICA A REDES WI-FI: OCULTAS O VISIBLES Y RESTRICCIÓN DE CONEXIÓN

1390. Si el interfaz Wi-Fi está activo y se detecta una red Wi-Fi activa cuyo nombre (o SSID) coincide con el de alguna red existente en la lista de redes preferidas del dispositivo (PNL, *Preferred Network List*), Android intentará conectarse automáticamente dicha red.

1391. La lista de redes preferidas (PNL) está disponible a través del menú “Ajustes - Wi-Fi” (ver apartado “16.4. Lista de redes preferidas (PNL)”). En el caso de redes no disponibles, aparecerán dentro del menú “Redes guardadas”. En el caso de redes disponibles, aparecerán a lo largo de la lista de redes (según la intensidad de su señal), identificadas con el texto “Guardado” (si no es la red a la que está conectado el dispositivo móvil actualmente) o “Conexión establecida” (si se trata de la red a la que está conectado el dispositivo móvil actualmente).

1392. La lista de redes preferidas sólo está disponible cuando el interfaz Wi-Fi está habilitado, no siendo posible acceder a ellas (para su borrado o edición) si éste está deshabilitado:



1393. Debe tenerse en cuenta que no existe la opción de desconectarse de la red a la que el dispositivo móvil está conectado actualmente. La única opción disponible es deshabilitar el interfaz Wi-Fi o seleccionar otra red conocida disponible.

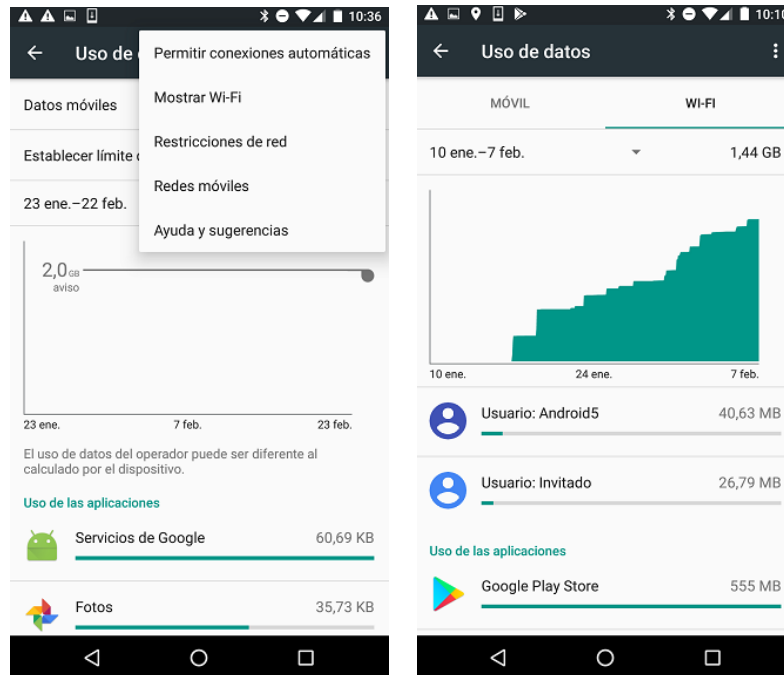
1394. Android no proporciona ninguna opción de configuración global que permita deshabilitar el proceso de conexión automática a redes Wi-Fi si el interfaz Wi-Fi se encuentra activo.

1395. No obstante, Android 6.x introdujo la posibilidad de restringir las conexiones a determinadas redes, de forma que no se genere tráfico hacia ellas ni por parte de apps

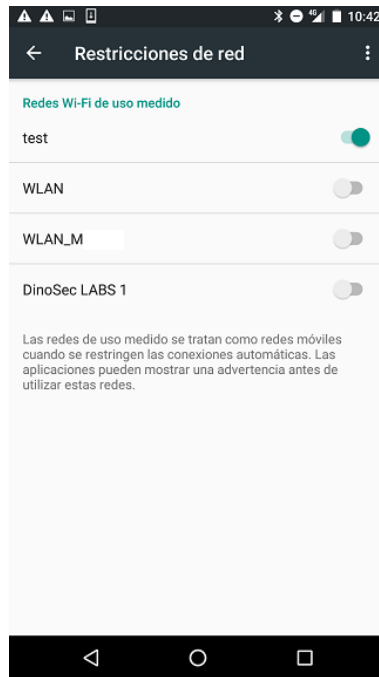
que ejecuten en segundo plano ni por parte de apps que, ejecutando en primer plano, intenten transferir un volumen de datos significativo. Esta opción no implica que no se realicen conexiones a dicha red, pero sí avisará si se intenta descargar actualizaciones de sistema operativo o apps o ficheros de cierto tamaño a través de ella.

1396. La opción para establecer restricciones de red requiere los siguientes pasos:

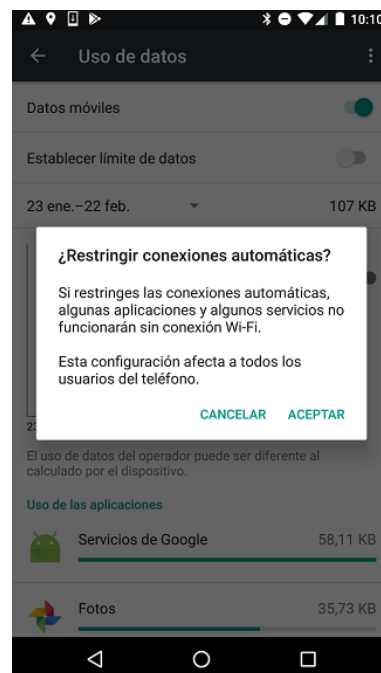
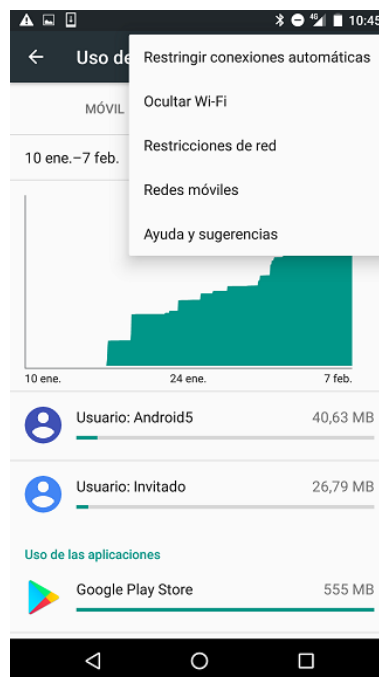
- Abrir el menú “Ajustes - [Conexiones inalámbricas y redes] Uso de datos - ... - Mostrar Wi-Fi - [Wi-Fi]”:



- Pinchar en el menú “...” de la parte superior derecha y marcar “Restricciones de red”. Con ello se mostrará la lista de redes guardadas, que son aquellas a las que el dispositivo ha intentado conectarse alguna vez, con o sin éxito. Los interruptores a la derecha del nombre de cada red determinarán si dicha red se incluirá en la lista de redes restringidas cuando se habilite la opción “Restringir conexiones automáticas” (descrita a continuación).



- Una vez seleccionadas las redes Wi-Fi sobre las que se desea restringir las conexiones, se retrocederá al menú anterior de “Uso de datos” y se seleccionará “... - Restringir conexiones automáticas”:



- Esta opción de restringir conexiones automáticas podría resultar también útil cuando se comparte la conexión de datos del terminal con otro dispositivo. Esta compartición de datos, como se describe en el apartado “16.6. Punto de acceso o zona Wi-Fi”, se lleva a cabo a través de una conexión Wi-Fi que se establece entre ambos dispositivos, aunque lo que se comparta en realidad sea la conexión de datos móviles a través de un punto de acceso Wi-Fi creado por el dispositivo móvil.
- Aunque no se indica que sea necesario reiniciar el interfaz Wi-Fi para que los cambios tengan efecto, se han observado escenarios que sí lo precisan, por lo que

se recomienda hacerlo para garantizar que los cambios en los ajustes se aplican correctamente.

1397. Un ejemplo de funcionamiento de este escenario de conexión restringida a una red de datos o Wi-Fi es el de la aplicación “Fotos”, que no realizará su copia de seguridad sobre redes Wi-Fi que se hayan definido como de uso medido (*metered*) si se ha habilitado la opción “Restringir conexiones automáticas”. El mensaje de notificación que se mostrará es “Esperando red Wi-Fi”, pese a que el dispositivo móvil está actualmente a una red Wi-Fi restringida:



1398. Android avisa de la existencia de la restricción de conexiones automáticas a través de una notificación general que no se puede descartar. Aunque las apps podrían avisar mediante algún mensaje o notificación propio en caso de que alguna de sus actividades haya quedado bloqueada a causa de dicha restricción, no siempre informan apropiadamente de manera particular, por lo que, en caso de observarse comportamientos anómalos, se recomienda revisar esta opción (y notificación):

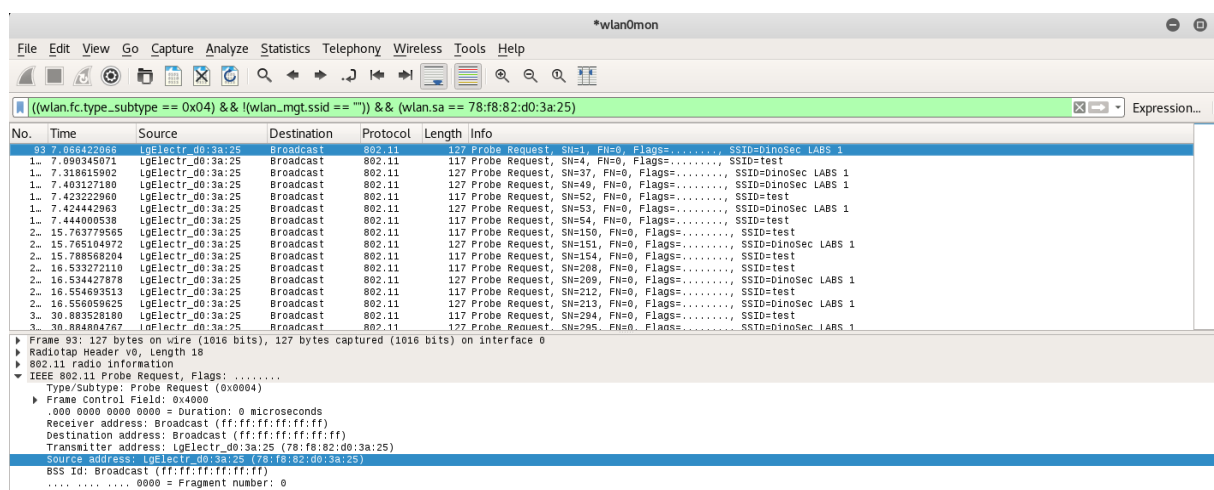


1399. Dado que no existe una opción de configuración en el interfaz de usuario de Android para deshabilitar el proceso de conexión automática a redes Wi-Fi si el interfaz Wi-Fi se encuentra activo, lo más recomendable es deshabilitar el interfaz Wi-Fi cuando no se esté haciendo uso del mismo.
1400. Las redes Wi-Fi pueden ser configuradas en dos modos: oculto o visible. Las redes ocultas son aquellas que no especifican el nombre de la red (SSID, *Service Set Identifier*) en las tramas de anuncio de *broadcast* o *beacons*, redes también conocidas como *nonbroadcast*. Las redes visibles son las que sí incluyen el nombre de red en esas tramas.
1401. Desde el punto de vista de seguridad, y con el objetivo de proteger a los clientes de la red Wi-Fi, se recomienda no hacer uso de redes Wi-Fi ocultas.
1402. Aunque en primera instancia puede parecer que el uso de redes Wi-Fi ocultas es una opción más segura, en realidad no es así, ya que es sencillo para un potencial atacante descubrir su existencia e incluso el nombre de esas supuestas redes ocultas.
1403. Sin embargo, el uso de una red oculta implica reducir el nivel de seguridad en los clientes Wi-Fi que se conectan a ella, como por ejemplo los dispositivos móviles basados en Android. Si una red está oculta, los clientes Wi-Fi se verán obligados a comprobar de forma explícita si está presente, generando tramas (de tipo *probe request*) dirigidas que desvelan necesariamente el nombre de la red, y lo que es más crítico, que les exponen frente a ataques de suplantación de dicha red por parte de un potencial atacante (especialmente cuando la red no emplea mecanismos de seguridad).
1404. Desafortunadamente, Android no implementa ningún mecanismo explícito para definir si una red es oculta o no, por lo que en función de cómo se añada la red Wi-Fi al



dispositivo móvil la primera vez, ésta será considerada como una red Wi-Fi oculta o visible.

1405. Si la red Wi-Fi es añadida al dispositivo, y en consecuencia a la PNL, seleccionándola de la lista de redes disponibles (situación que sólo se puede presentar si la red es visible), será añadida como red visible (escenario que aporta mayor seguridad a la configuración de Android).
1406. Si la red Wi-Fi es añadida al dispositivo, y en consecuencia a la PNL, manualmente mediante el menú “Añadir red” disponible en la parte superior (situación necesaria a la hora de añadir redes ocultas), será añadida como red oculta (escenario vulnerable desde el punto de vista de Android).
1407. Este es el comportamiento más vulnerable (existente previamente pero corregido en algunos sistemas operativos y ordenadores portátiles y de sobremesa desde hace años), ya que obliga a Android a generar tráfico que desvela la lista de redes Wi-Fi configuradas en el dispositivo móvil (conocida como la PNL). Este comportamiento presenta un escenario similar al existente en equipos de escritorio basados en Windows XP sin la actualización de seguridad KB917021 aplicada, y conocida desde el año 2007 [Ref.- 49].
1408. Adicionalmente, debe tenerse en cuenta que una vez una red Wi-Fi ha sido añadida al dispositivo móvil y está en la PNL, no se dispone de un mecanismo a través del interfaz gráfico de Android para determinar si es realmente considerada oculta o visible.
1409. Resumiendo: para todas aquellas redes configuradas o añadidas a través del menú “Añadir red”, Android generará tráfico que desvelará estas redes Wi-Fi disponibles en su lista de redes preferidas e intentará conectarse a ellas, escenario que puede ser empleado por un potencial atacante para suplantar dicha red, disponer de conectividad con el dispositivo móvil y proceder a explotar vulnerabilidades en el mismo.
1410. Por tanto, no se recomienda añadir ninguna red Wi-Fi manualmente al dispositivo móvil a través del menú “Añadir red”, aunque es una práctica común desde el punto de vista de seguridad para disponer de mayor control sobre la configuración y ajustes de la red Wi-Fi a añadir.
1411. En la imagen inferior, el dispositivo móvil Android intenta descubrir la presencia de las redes Wi-Fi disponibles en su PNL, “Dinosec LABS 1”, y “test”, una vez que el interfaz Wi-Fi ha sido activado, así como periódicamente, e incluso potencialmente aunque esté conectado a otra red Wi-Fi diferente en la actualidad:



1412. Esta vulnerabilidad de revelación de información en función de cómo han sido añadidas las redes Wi-Fi a Android (manualmente o automáticamente desde la lista de redes Wi-Fi) fue confirmada por el Android Security Team (Google), aunque parece que no publicará una actualización para solucionarla [Ref.- 95].

**Nota:** La versión 2.2 de Android introdujo este cambio en el comportamiento de la pila de comunicaciones Wi-Fi, ya que en versiones previas (versiones previas a 2.2 y a la compilación FRF91 empleada para la elaboración de una versión previa de la presente guía) no era posible conectarse con redes Wi-Fi ocultas (tal como identifica el *bug* 1041 de Android [Ref.- 42]); en el pasado incluso aparecieron apps en Google Play para añadir esta funcionalidad.

En cualquier caso, siempre antes de poder establecer una conexión con una red Wi-Fi oculta es necesario añadirla al dispositivo móvil de forma manual, para que éste conozca su existencia, y pueda preguntar sobre su disponibilidad (empleando el comportamiento vulnerable descrito previamente).

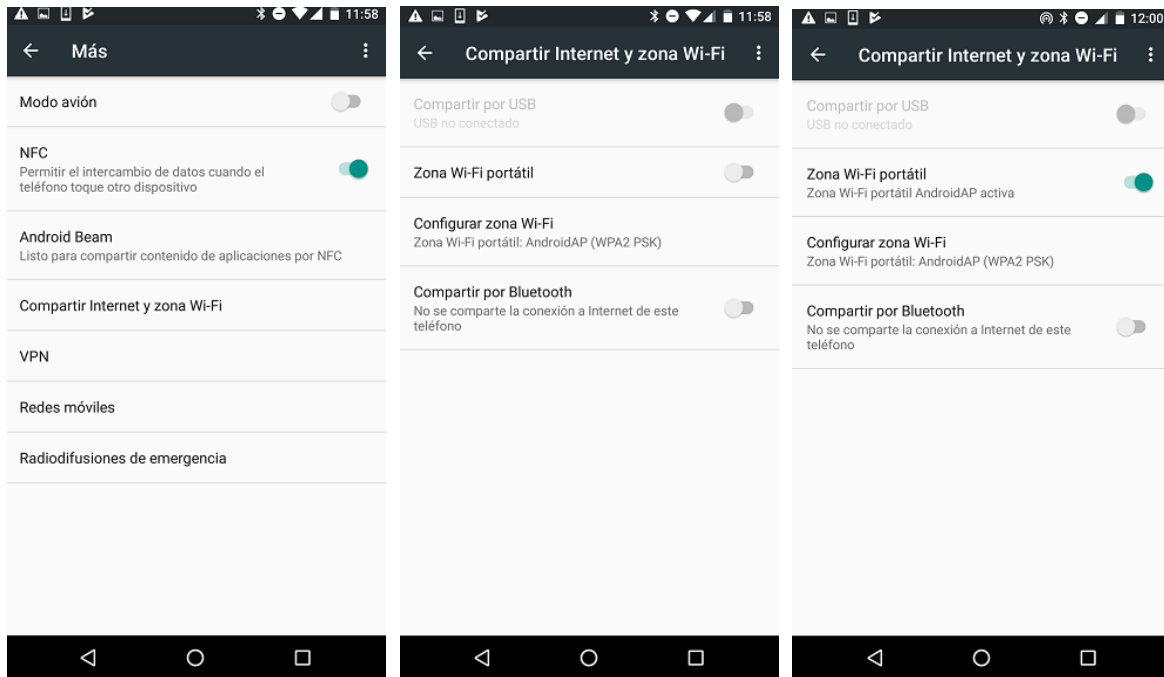
1413. Desafortunadamente, los dispositivos móviles Android no sólo desvelan el contenido de su PNL cuando disponen de redes Wi-Fi ocultas configuradas, sino también en numerosos otros escenarios.

1414. En concreto, el hecho de que el dispositivo móvil empleado desvele su PNL depende de múltiples factores asociados a la versión de Android, modelo de dispositivo móvil, tipo de interfaz Wi-Fi y *chipset* empleado, así como del estado del mismo. Algunos dispositivos móviles desvelan su PNL continuamente, incluyendo tanto las redes Wi-Fi ocultas como visibles existentes en la misma, mientras que otros lo hacen esporádicamente en función de estos diferentes factores. Habitualmente, los dispositivos móviles más modernos, junto a la utilización de las últimas versiones de Android, son menos propensos a desvelar de manera frecuente y habitual su PNL.

## 16.6. PUNTO DE ACCESO O ZONA WI-FI

1415. Android dispone de capacidades nativas para actuar como punto de acceso o zona Wi-Fi y router (o enrutador) hacia Internet, proporcionando acceso a múltiples dispositivos (u ordenadores, hasta un máximo de 10) vía Wi-Fi a su conexión de datos de telefonía móvil (2/3/4G) [Ref.- 94]. Para ello es necesario habilitar la conexión de datos móviles previamente (ver apartado “18. Comunicaciones móviles: voz y datos”).

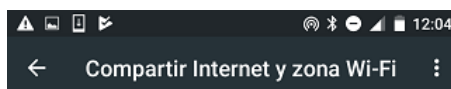
1416. Para hacer uso de estas capacidades es necesario acceder al menú “Ajustes [Conexiones Inalámbricas y Redes] - Más... - Compartir Internet y zona Wi-Fi”:



1417. A través de la opción “Zona Wi-Fi portátil” es posible habilitar el servicio de punto de acceso Wi-Fi (referido en ocasiones como *hotspot* o zona Wi-Fi), de forma que otros ordenadores y dispositivos puedan utilizar el dispositivo móvil como punto de acceso Wi-Fi para conectarse a Internet a través de su conexión de datos de telefonía móvil (2/3/4G).
1418. Curiosamente, la zona Wi-Fi puede ser activada en Android incluso aunque el dispositivo móvil no disponga de conexión de datos a través de las redes de telefonía móvil, o incluso sin insertar una tarjeta SIM.
1419. Debe tenerse en cuenta que, a diferencia del interfaz Wi-Fi (cliente) y Bluetooth, para poder llevar a cabo la configuración del punto de acceso Wi-Fi a través del interfaz de usuario del dispositivo móvil no es obligatorio activar esta funcionalidad, por lo que se recomienda modificar y completar su configuración antes de activar la funcionalidad, para evitar potenciales ataques cuando los mecanismos de seguridad no han sido aún aplicados.
1420. Mediante la opción “Configurar zona Wi-Fi”, es posible configurar los diferentes ajustes del punto de acceso, incluyendo el nombre de la red Wi-Fi (o SSID) y las características de seguridad:



1421. Por defecto, el punto de acceso Wi-Fi hace uso de WPA2-PSK (*Pre-Shared Key*, o WPA2-Personal), basado en el uso de una contraseña o clave precompartida, opción recomendada desde el punto de vista de seguridad. Android permite también la creación de puntos de acceso Wi-Fi abiertos (“Ninguna”), es decir, que no implementen ningún mecanismo de seguridad (opción desaconsejada).
1422. Por defecto el dispositivo móvil selecciona una contraseña aleatoria de 12 caracteres de longitud, hexadecimales. Sin embargo, se recomienda hacer uso de una contraseña propia, de mayor longitud y que pueda ser recordada más fácilmente por el usuario.
1423. La habilitación de la zona Wi-Fi se refleja en la barra superior de estado a través del símbolo que se muestra a la izquierda del símbolo de Bluetooth en la imagen inferior:



1424. Cuando el dispositivo móvil actúa de punto de acceso Wi-Fi, las apps de Android no pueden utilizar la conexión Wi-Fi como dispositivo cliente. Si previamente a su activación la conexión Wi-Fi cliente estaba activa, ésta será deshabilitada automáticamente. Igualmente, tras desactivar el punto de acceso Wi-Fi, la conexión Wi-Fi cliente será habilitada de nuevo automáticamente.
1425. Debido a la inhabilitación de la conexión Wi-Fi cliente del dispositivo móvil, las aplicaciones que tengan impedido el uso de datos móviles dejarán de poder transferir datos según las restricciones que se hayan definido para este escenario (consultar apartado “18. Comunicaciones móviles: voz y datos”).
1426. Se recomienda no habilitar las capacidades de punto de acceso Wi-Fi en el dispositivo móvil salvo que se quiera hacer un uso limitado y controlado de esta funcionalidad. En caso de ser utilizada, la red Wi-Fi asociada debe ser protegida y configurada mediante WPA2-PSK con una contraseña o clave precompartida suficientemente larga (más de 20 caracteres) y difícilmente adivinable [Ref.- 48].

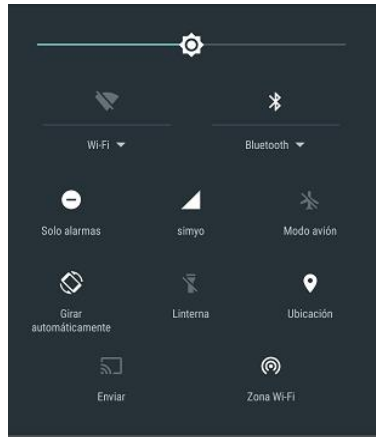
1427. El mecanismo de cifrado para WPA2-PSK empleado por defecto por el punto de acceso Wi-Fi proporcionado por Android es AES-CCMP, opción recomendada desde el punto de vista de seguridad.
1428. En caso de activar el punto de acceso Wi-Fi, se recomienda también modificar el nombre de la red Wi-Fi (o SSID) anunciada por el dispositivo móvil por defecto (“AndroidAP”), con el objetivo de no desvelar que se trata de un punto de acceso basado en Android.
1429. La red Wi-Fi creada es de tipo punto de acceso (o infraestructura), se anuncia en el canal 6 (de 802.11b/g/n), y proporciona incluso capacidades de servidor DHCP para la asignación de direcciones IP a los dispositivos cliente y ordenadores que se conectan a ella.
1430. Tras establecerse la conexión de red a través de la red Wi-Fi creada por Android, y tomando Windows 10 como sistema operativo del ordenador de referencia, el interfaz de red Wi-Fi funciona al estar configurado con una dirección IP dinámica (DHCP), asignándose por defecto una dirección IP de clase C (/24), como por ejemplo 192.168.43.98:

```
Adaptador de LAN inalámbrica Wi-Fi:
 Sufijo DNS específico para la conexión. . . :
 Dirección IPv4. : 192.168.43.98
 Máscara de subred : 255.255.255.0
 Puerta de enlace predeterminada : 192.168.43.1
```

1431. El dispositivo móvil (por ejemplo, con dirección IP 192.168.43.1) actúa de gateway, router o pasarela por defecto, de servidor DHCP, y de servidor DNS, y es alcanzable mediante ping (ICMP).

**Nota:** El direccionamiento IP empleado por Android para el punto de acceso Wi-Fi (192.168.43.x/24) no puede ser modificado salvo en dispositivos móviles *rooteados* [Ref.-99].

1432. La dirección MAC asociada al interfaz de red del punto de acceso Wi-Fi tiene asociado un OUI con valor “02:1A:11” (por ejemplo), qué corresponde a una dirección MAC administrada localmente y, por tanto, no asignada a ningún vendedor públicamente.
1433. Un análisis de los puertos TCP/IP y servicios disponibles en el interfaz de red empleado para el punto de acceso Wi-Fi del dispositivo móvil permite obtener las siguientes conclusiones:
- El único puerto TCP abierto es el correspondiente al servidor DNS (53/tcp). El servidor DNS es identificado por Nmap como “dnsmasq 2.51”.
  - Los únicos puertos UDP abiertos son los correspondientes al servidor DNS (53/udp) y al servidor DHCP (67/udp).
1434. Es posible interrumpir la disponibilidad del punto de acceso Wi-Fi deshabilitando la opción “Zona Wi-Fi portátil” habilitada previamente (para ello se puede recurrir al menú de ajustes rápidos, como ilustra la imagen inferior), opción recomendada desde el punto de vista de seguridad una vez no se desea disponer de la conexión de red Wi-Fi.



## 16.7. WI-FI DIRECT (“P2P”)

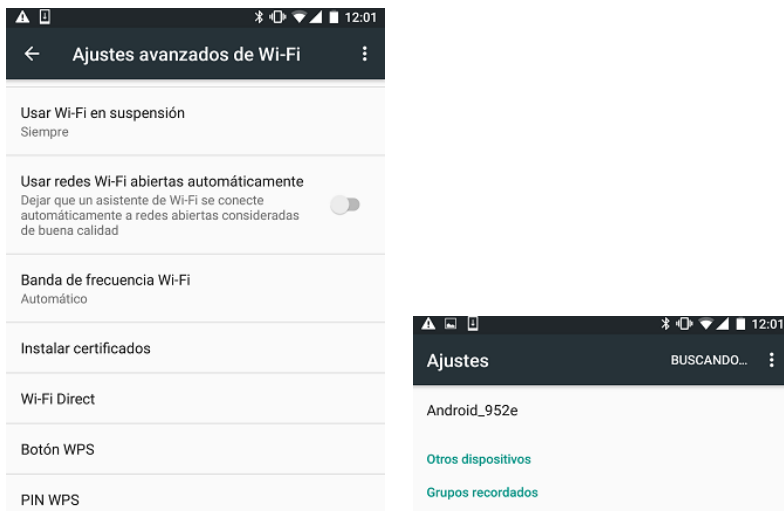
1435. La tecnología Wi-Fi Direct, un estándar publicado por la Wi-Fi Alliance [Ref.- 52], permite el establecimiento de conexiones Wi-Fi directamente entre dispositivos, punto a punto (“P2P”, Peer-to-Peer), sin hacer uso de una infraestructura, red o punto de acceso Wi-Fi.
1436. Wi-Fi Direct (y sus servicios asociados) permite a un dispositivo móvil interactuar con otros dispositivos directamente, como por ejemplo mostrar su pantalla y cualquier contenido multimedia (o juegos) en un televisor, monitor o proyector<sup>81</sup>, imprimir un documento en una impresora inalámbrica, compartir e intercambiar ficheros con otros dispositivos, como por ejemplo cámaras, o sincronizar datos con un ordenador.
1437. Para hacer uso de Wi-Fi Direct no es necesario disponer de conexión a Internet, aunque esta tecnología también puede ser empleada para compartir el acceso a Internet de un dispositivo con otros dispositivos compatibles con Wi-Fi Direct.
1438. Wi-Fi Direct permite tanto conexiones individuales entre dos dispositivos, como conexiones en grupo de varios dispositivos. Un dispositivo se encargará de proporcionar la red o el grupo Wi-Fi Direct, actuando como punto de acceso (denominado GO, Group Owner) y de gestionar dicha red y su conectividad (por ejemplo, proporcionando un servidor DHCP).
1439. El establecimiento de las conexiones Wi-Fi Direct se puede llevar a cabo mediante la pulsación de un botón, acercando dos dispositivos con capacidades NFC, o mediante la introducción de un PIN, empleando el estándar Wi-Fi Protected Setup (WPS).
1440. La especificación técnica asociada a Wi-Fi Direct, y denominada Wi-Fi Peer-to-Peer (“P2P”) define mecanismos para que los dispositivos puedan anunciar y descubrir los servicios ofrecidos por otros dispositivos cercanos a través de Wi-Fi Direct.
1441. Adicionalmente, a finales de 2014 se ratificó la estandarización de algunas mejoras de los servicios Wi-Fi Direct para llevar a cabo las tareas más comunes de forma sencilla, bajo el principio “descubrir, conectar y hacer” en un sólo paso, como por ejemplo<sup>82</sup>: (Wi-Fi Direct) “Send”, para el envío de contenidos, “Print”, para la impresión de documentos, “for DLNA”, para el descubrimiento de dispositivos, y “Miracast”, para la transmisión de contenidos multimedia.

<sup>81</sup> Por ejemplo, las conexiones multimedia Miracast pueden ser llevadas a cabo sobre Wi-Fi Direct.

<sup>82</sup> <http://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-enhances-wi-fi-certified-wi-fi-direct>

1442. La comunicación Wi-Fi Direct hace uso de WPA2 con AES para cifrar y autenticar los datos intercambiados.

1443. Las capacidades de Wi-Fi Direct, en concreto para iniciar una comunicación desde Android, están disponibles a través del menú “Ajustes - Wi-Fi - [...] - Ajustes Avanzados - Wi-Fi Direct”, siendo necesario que el interfaz Wi-Fi esté activo:



1444. Tras acceder a dicho menú, el dispositivo móvil Android comienza a buscar a otros dispositivos con capacidades Wi-Fi Direct, tal como indica el botón superior (“Buscando...”) que se muestra en la imagen superior derecha.

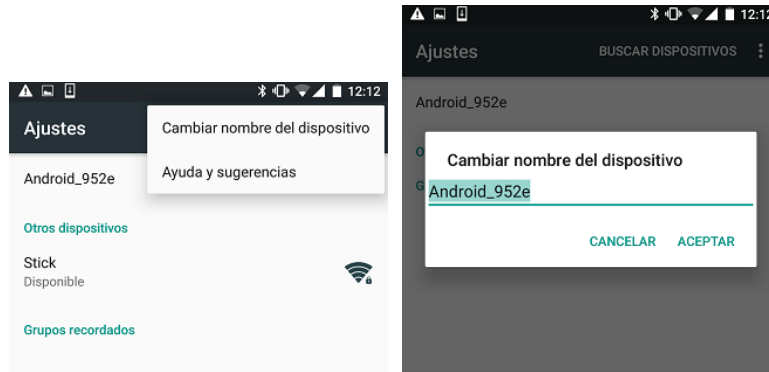
1445. Para ello, envía tramas de tipo *probe request* con el nombre de red, o SSID, “DIRECT-” por defecto, y que desvelan el uso de Wi-Fi Direct. Como origen de estas tramas se emplea una variante de la dirección MAC Wi-Fi del dispositivo móvil, que, por ejemplo, comienza por “7A” en lugar de por “78” (convirtiéndola en una dirección administrada localmente). Por ejemplo, la dirección Wi-Fi que comienza por “78:f8:82” es convertida en “7a:f8:82”, respetando el resto de bytes de la dirección.

1446. Adicionalmente, estas tramas 802.11 incluyen un campo asociado a Wi-Fi Direct (o P2P) con el valor “Wi-FiAll”, y que contiene detalles de sus capacidades P2P (“P2P Capability”), tanto a nivel de dispositivo como de grupo, y el canal en el que escucha (normalmente, los canales disponibles son 1, 6 y 11 en la banda de frecuencias de 2.4GHz, heredados de los canales disponibles y recomendados en USA):

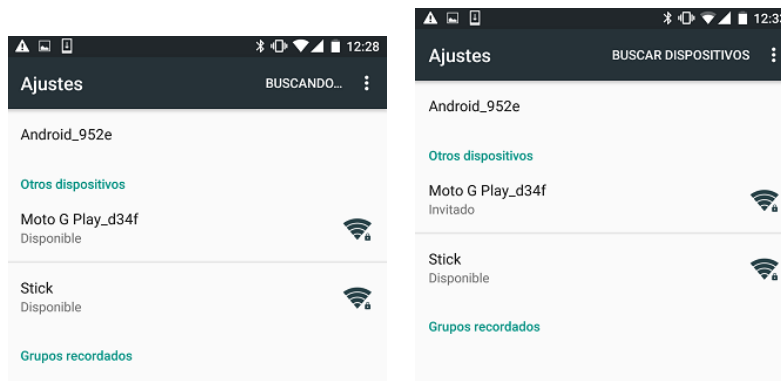
|                                                                                           |              |                   |           |        |                                                                   |
|-------------------------------------------------------------------------------------------|--------------|-------------------|-----------|--------|-------------------------------------------------------------------|
| 4..                                                                                       | 36.958299436 | lgElectr_d0:3a:25 | Broadcast | 802.11 | 127 Probe Request, SN=437, FN=0, Flags=....., SSID=DinoSec LABS 1 |
| 4..                                                                                       | 37.837854577 | lgElectr_d0:3a:25 | Broadcast | 802.11 | 117 Probe Request, SN=438, FN=0, Flags=....., SSID=test           |
| 4..                                                                                       | 37.058065401 | lgElectr_d0:3a:25 | Broadcast | 802.11 | 113 Probe Request, SN=441, FN=0, Flags=....., SSID=Broadcast      |
| 4..                                                                                       | 40.771165876 | 7a:f8:82:d0:3a:25 | Broadcast | 802.11 | 254 Probe Request, SN=312, FN=0, Flags=....., SSID=DIRECT-        |
| 4..                                                                                       | 40.784334703 | 7a:f8:82:d0:3a:25 | Broadcast | 802.11 | 254 Probe Request, SN=313, FN=0, Flags=....., SSID=DIRECT-        |
| 4..                                                                                       | 40.797544135 | 7a:f8:82:d0:3a:25 | Broadcast | 802.11 | 254 Probe Request, SN=314, FN=0, Flags=....., SSID=DIRECT-        |
| 4..                                                                                       | 45.612053607 | 7a:f8:82:d0:3a:25 | Broadcast | 802.11 | 254 Probe Request, SN=363, FN=0, Flags=....., SSID=DIRECT-        |
| 4..                                                                                       | 45.625033880 | 7a:f8:82:d0:3a:25 | Broadcast | 802.11 | 254 Probe Request, SN=364, FN=0, Flags=....., SSID=DIRECT-        |
| 4..                                                                                       | 45.638293799 | 7a:f8:82:d0:3a:25 | Broadcast | 802.11 | 254 Probe Request, SN=365, FN=0, Flags=....., SSID=DIRECT-        |
| 4..                                                                                       | 49.603571120 | 7a:f8:82:d0:3a:25 | Broadcast | 802.11 | 254 Probe Request, SN=414, FN=0, Flags=....., SSID=DIRECT-        |
| 4..                                                                                       | 49.608993624 | 7a:f8:82:d0:3a:25 | Broadcast | 802.11 | 254 Probe Request, SN=415, FN=0, Flags=....., SSID=DIRECT-        |
| 4..                                                                                       | 49.620882714 | 7a:f8:82:d0:3a:25 | Broadcast | 802.11 | 254 Probe Request, SN=416, FN=0, Flags=....., SSID=DIRECT-        |
| 4..                                                                                       | 49.639094888 | 7a:f8:82:d0:3a:25 | Broadcast | 802.11 | 254 Probe Request, SN=417, FN=0, Flags=....., SSID=DIRECT-        |
| 4..                                                                                       | 50.126790343 | 7a:f8:82:d0:3a:25 | Broadcast | 802.11 | 254 Probe Request, SN=428, FN=0, Flags=....., SSID=DIRECT-        |
| 4..                                                                                       | 50.138970986 | 7a:f8:82:d0:3a:25 | Broadcast | 802.11 | 254 Probe Request, SN=429, FN=0, Flags=....., SSID=DIRECT-        |
| 4..                                                                                       | 50.151268725 | 7a:f8:82:d0:3a:25 | Broadcast | 802.11 | 254 Probe Request, SN=430, FN=0, Flags=....., SSID=DIRECT-        |
| ▶ Frame 431: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits) on interface 0 |              |                   |           |        |                                                                   |
| ▶ Radiotap Header v0, Length 16                                                           |              |                   |           |        |                                                                   |
| ▶ 802.11 radio information                                                                |              |                   |           |        |                                                                   |
| ▶ IEEE 802.11 Probe Request, Flags: .....                                                 |              |                   |           |        |                                                                   |
| ▼ IEEE 802.11 Wireless LAN management frame                                               |              |                   |           |        |                                                                   |
| ▼ Tagged parameters (212 bytes)                                                           |              |                   |           |        |                                                                   |
| ▶ Tag: SSID parameter set: DIRECT-                                                        |              |                   |           |        |                                                                   |
| ▶ Tag: Supported Rates 0, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]                           |              |                   |           |        |                                                                   |
| ▶ Tag: Extended Capabilities (9 octets)                                                   |              |                   |           |        |                                                                   |
| ▶ Tag: Vendor Specific: Microsoft: WPS                                                    |              |                   |           |        |                                                                   |
| ▼ Tag: Vendor Specific: Wi-FiAll: P2P                                                     |              |                   |           |        |                                                                   |
| Tag Number: Vendor Specific (221)                                                         |              |                   |           |        |                                                                   |
| Tag length: 17                                                                            |              |                   |           |        |                                                                   |
| OUI: 50-6f-9a (Wi-FiAll)                                                                  |              |                   |           |        |                                                                   |
| Vendor Specific OUI Type: 9                                                               |              |                   |           |        |                                                                   |
| ▶ P2P Capability: Device 0x25 Group 0x0                                                   |              |                   |           |        |                                                                   |
| ▶ Listen Channel: Operating Class 81 Channel Number 11                                    |              |                   |           |        |                                                                   |
| ▶ Tag: HT Capabilities (802.11n D1.10)                                                    |              |                   |           |        |                                                                   |
| ▶ Tag: VHT Capabilities (IEEE Std 802.11ac/D3.1)                                          |              |                   |           |        |                                                                   |
| 0020: 3a 25 ff ff ff ff ff ff 80 13 00 07 44 48 52 45 :%.....:DIRECT                      |              |                   |           |        |                                                                   |



1447. Por defecto, el nombre empleado por Android en Wi-Fi Direct es “Android\_<código>”, donde “<código>” corresponde con el comienzo del número asociado al nombre o *hostname* empleado por el dispositivo móvil, por ejemplo “android\_952e” (ver apartado “7.10. Configuración por defecto del dispositivo móvil”<sup>83</sup>), por lo que se recomienda modificarlo a través del botón superior “Cambiar Nombre del Dispositivo” (para Wi-Fi Direct) por un valor que no desvele ningún detalle del terminal, como por ejemplo “dm0001” (“dispositivo móvil 0001”):

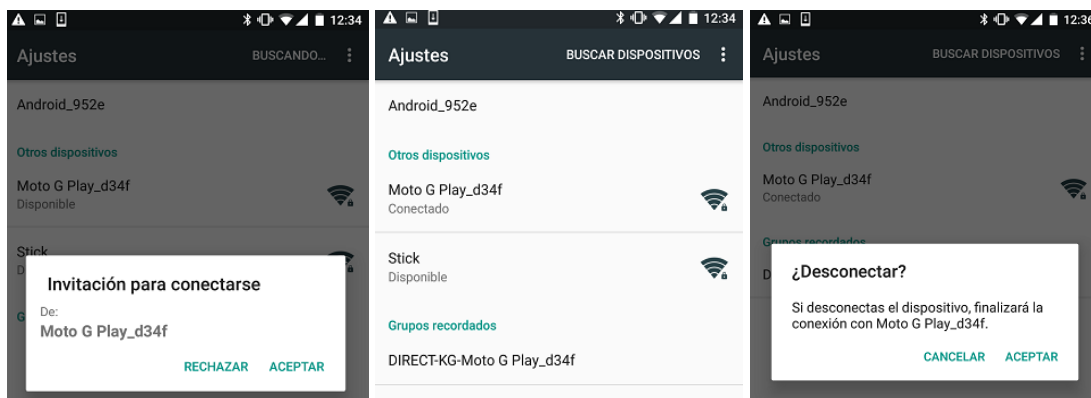


1448. Una vez el dispositivo móvil descubre otros dispositivos con capacidades Wi-Fi Direct, puede iniciar una comunicación enviando una invitación para establecer la conexión. Si el otro dispositivo acepta la invitación, se establecerá un nuevo grupo de Wi-Fi Direct, y se llevará a cabo la conexión:



1449. Asimismo, el dispositivo móvil puede recibir una invitación de comunicación mediante Wi-Fi Direct proveniente de otros dispositivos. El tiempo máximo para aceptar la invitación es de 30 segundos.
1450. Para efectuar la desconexión, basta con pulsar sobre el campo correspondiente al dispositivo y aceptar la confirmación:

<sup>83</sup> El valor numérico del nombre cambia aleatoriamente tras restablecer los valores de fábrica.



1451. Cuando un dispositivo móvil quiere establecer una conexión P2P vía Wi-Fi Direct y envía una invitación, puede, bien solicitar la creación de un grupo al que unirse, bien iniciar la creación de un grupo a través de una trama de “GO Negotiation request” (GO - group owner).
1452. En Android 6.x, cuando se establece la conexión con otro dispositivo vía Wi-Fi Direct, el grupo creado para esa conexión se almacena en el campo “Grupos recordados”, de forma que las conexiones futuras desde ese dispositivo se realizarán de forma automática, no recibándose ningún mensaje de confirmación de invitación.
1453. Por tanto, si la conexión Wi-Fi Direct se realiza para una operación puntual, se recomienda eliminar el grupo cuando finalice dicha conexión.
1454. Para el dispositivo móvil empleado en la elaboración de la presente guía, Google no ofrece la opción de crear grupos Wi-Fi Direct, sino que crea un grupo nuevo para cada conexión Wi-Fi Direct aceptada (por tanto, los grupos serán entre dos dispositivos).

## 17. COMUNICACIONES MÓVILES: MENSAJES DE TEXTO (SMS)

1455. Las capacidades de mensajería de texto (SMS, *Short Message Service*) de los dispositivos móviles permite el envío de mensajes cortos empleando la infraestructura GSM (*Global System for Mobile communications*, o 2G), UMTS (*Universal Mobile Telecommunications System*, o 3G) y LTE (*Long Term Evolution* o 4G).
1456. El primer nivel de protección asociado al sistema de mensajería de texto pasa por la concienciación del usuario desde el punto de vista de seguridad, teniendo en cuenta que la implementación de este módulo en los dispositivos móviles actuales proporciona numerosas funcionalidades, y no únicamente la visualización de mensajes de texto.
1457. Entre las funcionalidades avanzadas se encuentra la posibilidad de mostrar contenidos de texto, contenidos web (enlaces, HTML, JavaScript, etc.), gestionar datos binarios, como tonos de llamada, e intercambiar ficheros multimedia (audio, vídeo e imágenes), sobre todo en sus variantes avanzadas: EMS (*Enhanced Messaging Service*) y MMS (*Multimedia Message Service*).
1458. Debido a las diferentes vulnerabilidades asociadas al módulo de mensajería de texto existentes en el pasado en múltiples dispositivos móviles actuales, incluyendo Android [Ref.- 400], se recomienda que el usuario actúe con prudencia ante la lectura de nuevos mensajes de texto, especialmente los recibidos de fuentes desconocidas.
1459. Durante el año 2009 se publicaron diferentes vulnerabilidades de denegación de servicio (DoS) en el módulo SMS de dispositivos Android [Ref.- 400]. El proceso que

gestiona los mensajes SMS en Android (SMSManager<sup>84</sup> o Provider) es una aplicación Java:



1460. Se recomienda no abrir ningún mensaje de texto no esperado o solicitado, práctica similar a la empleada para la gestión de correos electrónicos (o e-mails). A la hora de acceder y procesar los contenidos del buzón de entrada de mensajes de texto del dispositivo móvil, el usuario debería seguir las mejores prácticas de seguridad, como por ejemplo:

- No deberían abrirse mensajes de texto recibidos desde números desconocidos, ni ejecutar o permitir la instalación de contenidos adjuntos (configuraciones, binarios o multimedia) asociados a mensajes SMS/MMS no esperados.
- En su lugar, se debería proceder a borrar el mensaje directamente.
- En caso de acceder a los mensajes, debería desconfiarse de su contenido, y tener especial cuidado, por ejemplo, con la utilización de enlaces a sitios web externos.

1461. Adicionalmente, es necesario tener en cuenta que los mensajes de texto pueden contener información sensible y confidencial. Por ejemplo, al gestionar el buzón de voz de un usuario, los operadores de telefonía móvil pueden enviar todos los detalles de acceso al buzón de voz, incluido el PIN, mediante un mensaje de texto. El acceso a dicho mensaje por parte de un potencial atacante permitiría disponer de control completo del buzón de voz del usuario.

1462. Los nuevos mecanismos de autenticación de la banca online también emplean los mensajes de texto para el envío de contraseñas de un solo uso para la realización de operaciones bancarias críticas. El acceso a dicho mensaje por parte de un potencial atacante permitiría completar la operación, como por ejemplo, una transferencia bancaria.

1463. La recepción de mensajes SMS por parte del dispositivo móvil cuando la pantalla de acceso está bloqueada, depende de la configuración seleccionada inicialmente por el

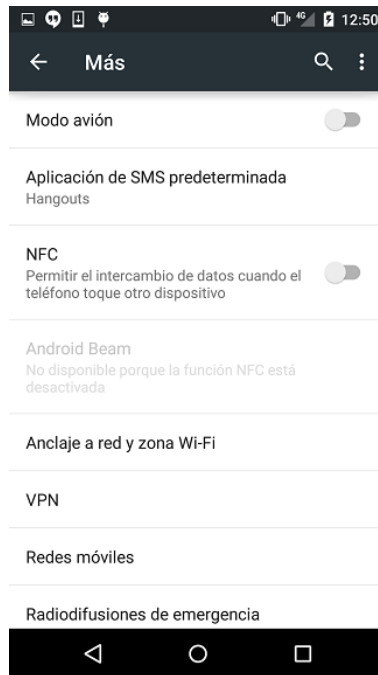
<sup>84</sup> <http://developer.android.com/reference/android/telephony/SmsManager.html>

usuario durante el proceso de configuración de un código de acceso respecto a las notificaciones.

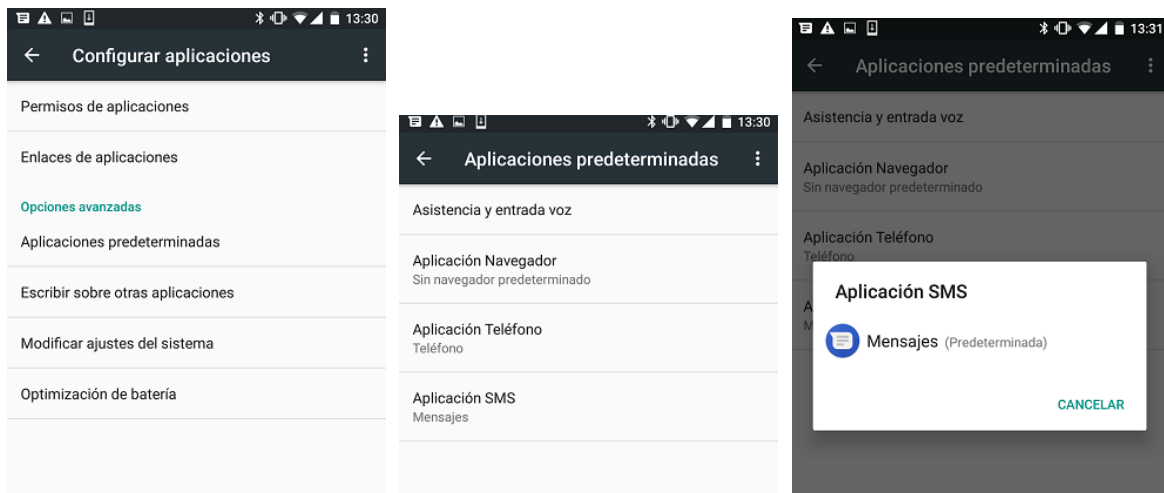
1464. Si la opción seleccionada fue “Mostrar todas las notificaciones”, opción más insegura, Android muestra los contenidos del mensaje mediante una notificación en la pantalla de bloqueo. Adicionalmente, muestra dichos contenidos mediante una notificación en la barra superior de estado, en el centro de notificaciones, donde se dispone de acceso a los contenidos confidenciales del SMS:



1465. Los ajustes de configuración de las notificaciones están disponibles bajo “Ajustes - Sonido y notificaciones - Con dispositivo bloqueado”, proporcionándose tres opciones: “Mostrar contenido de notificaciones” (opción más insegura), “Ocultar notificaciones sensibles” y “No mostrar notificaciones” (opción más segura, pero que limita la funcionalidad de notificaciones en la pantalla de bloqueo). Para más información, consultar el apartado “9.8.- Notificaciones”.
1466. Por otro lado, el envío de mensajes de texto (SMS) a servicios *Premium* ha sido una técnica muy comúnmente utilizada por software malicioso (*malware*) móvil para obtener beneficios económicos. Especialmente, esta técnica de obtención de financiación de manera ilegal ha sido empleada al infectar dispositivos móviles basados en Android, debido a las facilidades existentes para el envío de SMS *Premium* en esta plataforma móvil en versiones previas de Android y al coste asociado para el usuario por cada mensaje enviado (por ejemplo, un euro por SMS).
1467. Por este motivo, Android 4.2 introdujo nuevos mecanismos de protección a la hora de enviar mensajes SMS *Premium*, por ejemplo por parte de una app, generándose un mensaje de notificación que debe ser aprobado por el usuario antes de proceder al envío del SMS al servicio *Premium*, con cargos adicionales [Ref.- 86].
1468. Por otro lado, desde Android 4.4 (KitKat), la plataforma permite definir cuál es la app por defecto encargada de la gestión de mensajes SMS (*default SMS app*) [Ref.- 30], pudiendo haber únicamente una app gestionando la entrada de nuevos SMS (o MMS) al dispositivo móvil, y especialmente, disponiendo de capacidades de escritura en el proveedor de telefonía de Android.
1469. En la versión 5.x de Android, la app encargada de la gestión de mensajes SMS se definía a través del menú “Ajustes [Conexiones Inalámbricas y Redes] - Más... - Aplicación de SMS predeterminada”:



1470. Sin embargo, en Android 6.x desaparece esta opción de menú, y la app responsable de la gestión de SMS se configura a través de “Ajustes - [Dispositivo] Aplicaciones - Engranaje de ajustes - [Opciones avanzadas] Aplicaciones predeterminadas - Aplicación SMS”:



**Nota:** Existieron en el pasado soluciones propietarias de cifrado de mensajes de texto (que reemplazan o complementan a los SMS) y de mensajería en general (chat), como TextSecure (de código abierto), proporcionadas por terceras compañías a través de Google Play, que cifran los mensajes de texto tanto durante su almacenamiento en el dispositivo móvil como durante su transmisión a otros usuarios de la app TextSecure [Ref.- 33]. TextSecure hace uso del protocolo OTR (*Off The Record*), con mejoras<sup>85</sup>, para cifrar los mensajes de texto. TextSecure puede ser empleado para el envío de mensajes cifrados entre terminales Android, o también con terminales basados en iOS mediante la app Signal<sup>86</sup>, empleando las comunicaciones de datos (Wi-Fi o 2/3/4G) de los dispositivos móviles, o la infraestructura SMS de los operadores. El uso de la infraestructura de SMS asociada a los proveedores u

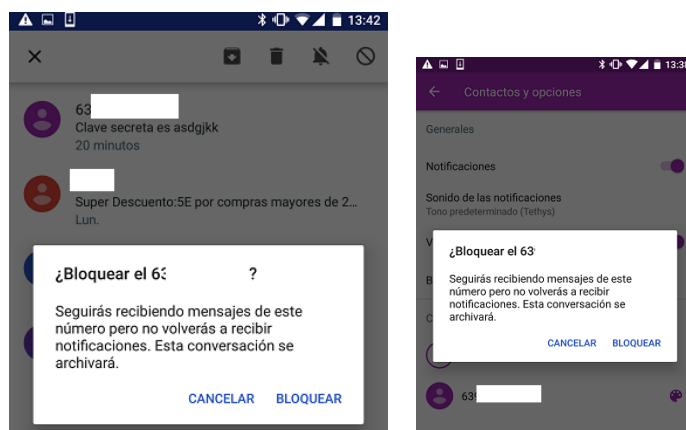
<sup>85</sup> <https://whispersystems.org/blog/simplifying-otr-deniability/>

<sup>86</sup> <https://github.com/WhisperSystems/Signal-iOS>

operadores de telecomunicaciones para el envío de mensajes de texto puede revelar información en los metadatos de dichas conversaciones.

Actualmente, las soluciones y apps de mensajería (WhatsApp, Signal, Telegram, Line, Viber, etc.) han reemplazado de manera generalizada el uso de los mensajes SMS, haciendo una amplia utilización de diferentes mecanismos de cifrado, y en algunos casos como Signal [Ref.- 32], sustituyendo por completo apps previas, como TextSecure.

1471. La aplicación “Mensajes” permite bloquear las notificaciones asociadas a los SMS procedentes de determinados números. Ello no implica que se dejen de recibir SMS de dichos números, sino que no se mostrarán al usuario. Para activar esta funcionalidad, se ha de acceder al interfaz de la aplicación, seleccionar el icono asociado al emisor del mensaje y pulsar el icono “prohibido” de la barra superior. También se puede seleccionar un mensaje de dicho emisor y pulsar sobre “[...] - Contactos y opciones - [Generales] Bloquear el <número de teléfono>”:



## 18. COMUNICACIONES MÓVILES: VOZ Y DATOS

### 18.1. DESACTIVACIÓN DE LAS COMUNICACIONES DE VOZ Y DATOS MÓVILES

1472. La principal recomendación de seguridad asociada a las comunicaciones de voz (y SMS) a través de las redes de telefonía móvil en dispositivos móviles es ser cauteloso a la hora de activar las distintas capacidades de telefonía del terminal. Así, por ejemplo, si se está conectado a una red Wi-Fi, se puede deshabilitar temporalmente el uso de datos móviles.

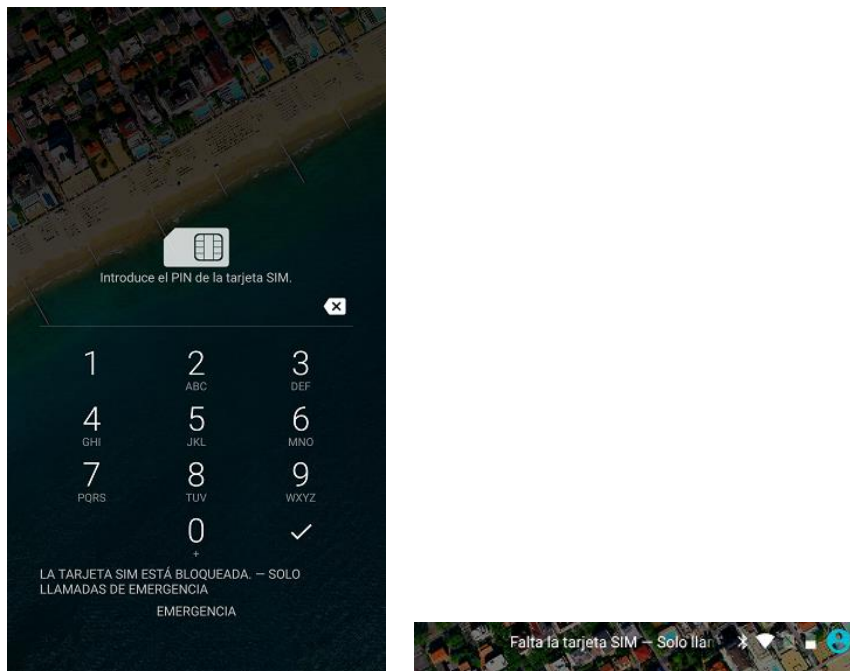
**Nota:** Durante el proceso de configuración inicial del dispositivo móvil empleado para la elaboración de la presente guía (activado automáticamente la primera vez que se enciende el terminal), el interfaz de telefonía móvil para comunicaciones de voz está habilitado, solicitando en primer lugar el PIN de la tarjeta SIM, si ésta está insertada.

Se recomienda desactivar el interfaz de telefonía móvil tan pronto finalice el proceso de configuración inicial, para proceder a la aplicación de las medidas de seguridad seleccionadas.

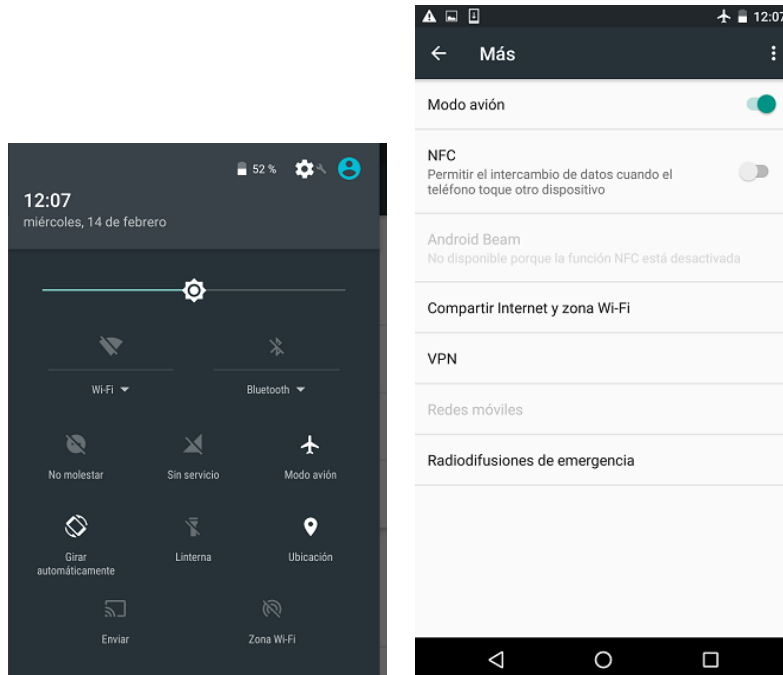
1473. En Android 6.x, y en concreto para el dispositivo móvil analizado, cada vez que se inserta una nueva tarjeta SIM se solicita al usuario el PIN asociado, no siendo necesario reiniciar el dispositivo para poder hacer uso de las capacidades de telefonía móvil (acceso a la red móvil). Al insertar una tarjeta SIM, Android solicitará al usuario el PIN asociado a ella; al extraer la tarjeta SIM, se mostrará un mensaje en la barra de



notificaciones que informa de que la misma no está disponible. En versiones previas de Android, y en otros modelos de terminal, puede ser necesario reiniciar el dispositivo móvil cada vez que se inserte o extraiga la tarjeta SIM:

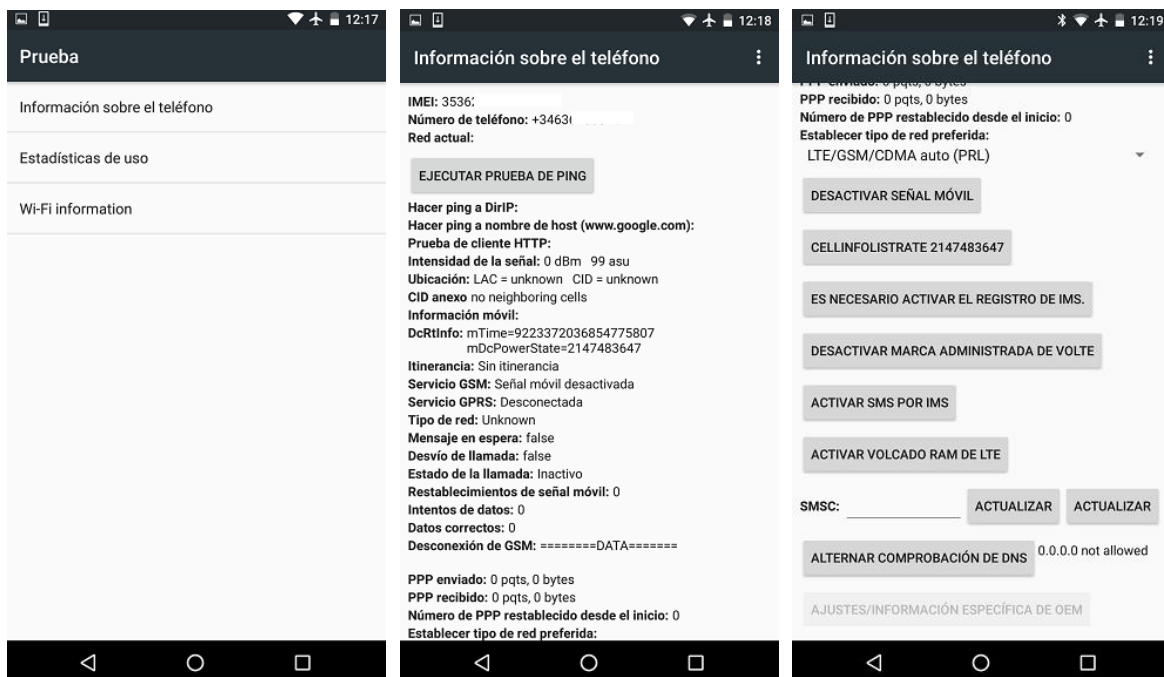


1474. Android no permite a través del interfaz de usuario estándar deshabilitar de forma individualizada las capacidades de telefonía móvil (voz y SMS); la única opción para ello es activar el “Modo avión”, bien a través del menú “Ajustes [Conexiones Inalámbricas y Redes] - Más...” o del menú de ajustes rápidos.
1475. Al activar el modo avión en Android, tanto la conectividad a redes Wi-Fi como la conectividad de Bluetooth puede ser habilitada posteriormente y de forma independiente, pero no es posible activar la conectividad de telefonía móvil en ese modo, ni tampoco la conectividad móvil 2/3/4G, directamente ligada al modo avión:

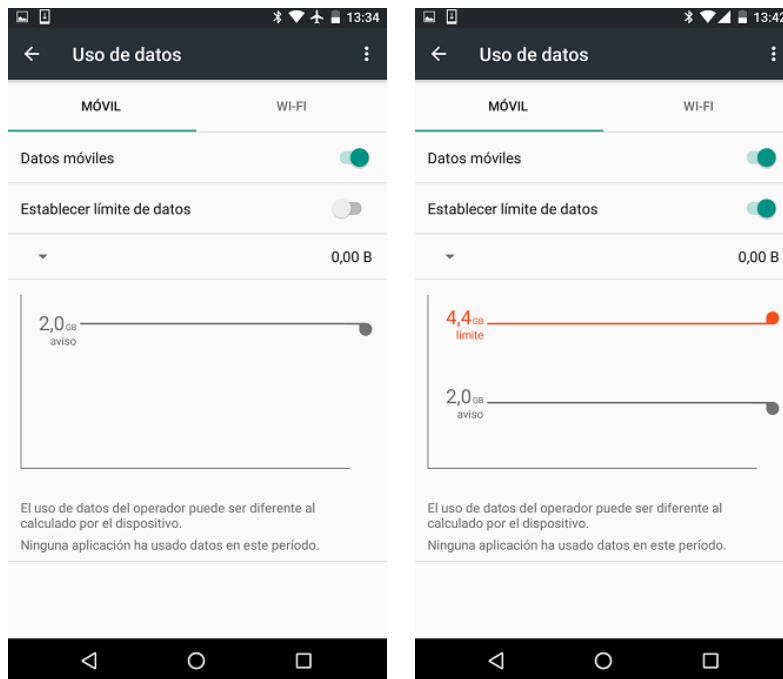




1476. Debido a este comportamiento, no resulta posible desactivar las capacidades de voz únicamente, ni siquiera en el caso de tabletas que emplean el SIM exclusivamente para conexión de datos.
1477. Sin embargo, sí es posible realizar una configuración avanzada accediendo al menú denominado “Prueba” (o *testing*) disponible en Android tras marcar el siguiente código en el menú de marcación telefónica: `*##4636#` (o `*##info##`). Esta funcionalidad permite independizar la desconexión de los diferentes interfaces de comunicaciones inalámbricos, es decir, Bluetooth, Wi-Fi y telefonía móvil 2/3/4G.
1478. Para ello, y sin necesidad de activar el modo avión, e independientemente del estado de activación de los interfaces Bluetooth y Wi-Fi, se puede seleccionar la opción “Información sobre el teléfono” y acceder a un menú que permite desconectar únicamente el interfaz de telefonía móvil 2/3/4G:

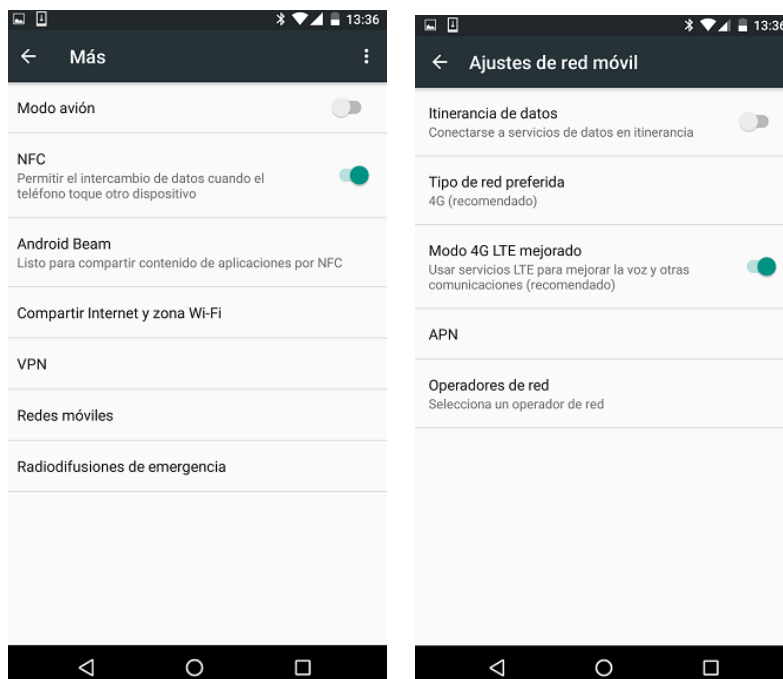


1479. El botón “Desactivar señal móvil” que aparece al descender en la pantalla desactivará únicamente y por completo (voz y datos) el interfaz de radio de telefonía móvil, pudiendo permanecer los interfaces de Bluetooth y Wi-Fi activos, tal y como denotan los iconos de la barra superior de estado.
1480. Este cambio de configuración no prevalece tras reiniciar el dispositivo móvil, donde de nuevo el interfaz de radio de telefonía móvil será activado automáticamente tras introducir el PIN de la tarjeta SIM.
1481. Por otro lado, la principal recomendación de seguridad asociada a las comunicaciones de datos a través de las infraestructuras de telefonía móvil en dispositivos móviles es no activar las capacidades de transmisión y recepción de datos salvo en el caso en el que se esté haciendo uso de éstas, evitando así la posibilidad de ataques sobre el hardware del interfaz, el driver, la pila de comunicaciones móviles y cualquiera de los servicios y apps disponibles a través de esa red y la conexión a Internet.
1482. Las conexiones de datos a través de la red de telefonía móvil (2/3/4G), GPRS, UMTS o LTE, pueden ser deshabilitadas a través del menú “Ajustes [Conexiones Inalámbricas y Redes] - Uso de datos - Datos móviles” y en concreto el interruptor “[SI | NO]”.



1483. También es posible establecer un límite de datos, de forma que el sistema Android desactive automáticamente los datos móviles cuando se alcance el umbral definido, impidiendo así que las aplicaciones puedan consumir datos. Para configurar dicho límite, se dispone de la opción “Establecer límite de datos” (ver imagen superior derecha), que permite, desplazando la barra horizontal del gráfico, marcar tanto el umbral de aviso como el umbral de desactivación.

1484. La opción “Itinerancia de datos” (o *roaming*), disponible a través del menú “Ajustes [Conexiones Inalámbricas y Redes] - Más... - Redes móviles”, permite configurar si se desea hacer uso de las capacidades de datos de telefonía móvil del dispositivo cuando se viaja al extranjero y el terminal se encuentra en una red de otro operador al que puede asociarse su tarjeta SIM:

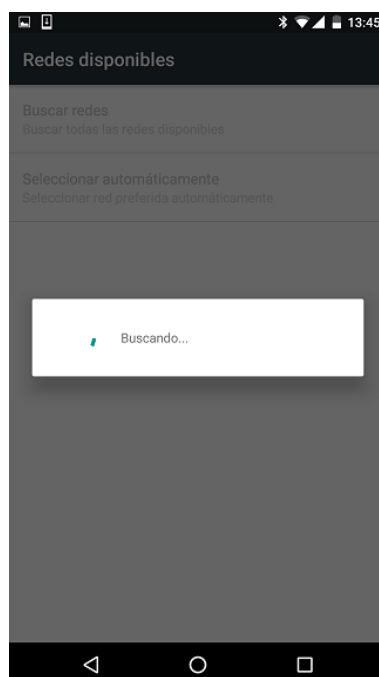


**Nota:** Además de la seguridad, una de las preocupaciones de los usuarios de dispositivos móviles sin tarifa plana de conexión de datos son los cargos asociados al uso de las comunicaciones de datos a través de las redes de telefonía móvil (2/3/4G), especialmente cuando el contrato tiene gastos asociados por la cantidad de datos transmitidos y/o por tiempo o número de conexiones establecidas, o se viaja internacionalmente (itinerancia o *roaming*). Múltiples apps en Android pueden iniciar este tipo de conexiones de datos en diferentes momentos del día.

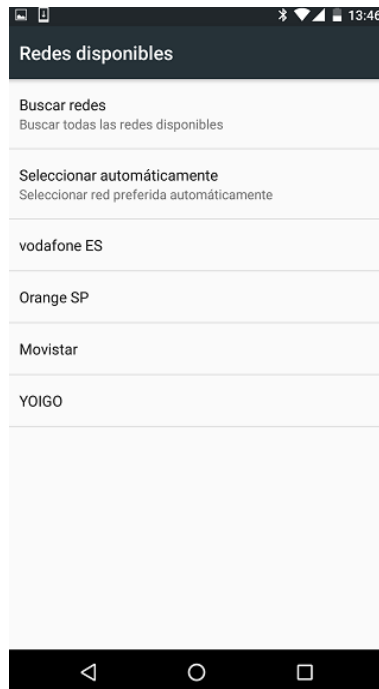
1485. Por defecto en Android (configuración de fábrica) el interfaz de datos de telefonía móvil está habilitado (con los APNs que han sido definidos por la tarjeta SIM empleada).
1486. Android mantiene el estado del interfaz de telefonía de datos tras reiniciar el dispositivo móvil, es decir, si el interfaz de telefonía de datos estaba activo al apagar el terminal, al encender el dispositivo móvil e introducir el PIN de la tarjeta SIM, seguirá activo.
1487. Igualmente, al salir del modo avión el estado del interfaz de datos de telefonía móvil será restaurado, y se activará en el caso de haber estado activo previamente (antes de activar el modo avión).
1488. Tras desactivar la conexión de datos, si alguna app requiere disponer de conectividad (por ejemplo, acceso a la web desde el navegador web existente por defecto) la conexión de telefonía de datos no será activada automáticamente.

## 18.2. CONFIGURACIÓN Y SELECCIÓN DE LA RED (VOZ) DE TELEFONÍA MÓVIL

1489. Android permite al usuario utilizar la red de telefonía móvil configurada automáticamente a través de la tarjeta SIM, así como seleccionar de forma manual el operador de telecomunicaciones móviles (voz y SMS).
1490. Desde el menú de configuración del teléfono (“Ajustes [Conexiones Inalámbricas y Redes] - Más... - Redes móviles”) y a través de la opción “Operadores de red”, es posible acceder a las opciones para seleccionar el operador de red, tanto de forma automática como manual:

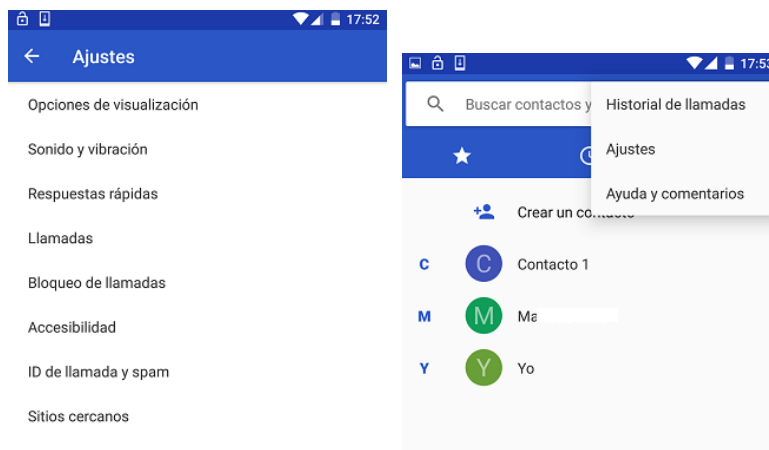


1491. Android llevará a cabo una búsqueda automática de las redes disponibles en la ubicación actual del dispositivo móvil, y mostrará al usuario la lista de operadores de telecomunicaciones identificados:



1492. La selección de red permite definir si la red de telefonía será seleccionada de forma automática (opción por defecto) por el dispositivo móvil en función de la tarjeta SIM y de la intensidad de la señal, o si el usuario puede definir de forma manual la red a la que desea conectarse de la lista de redes disponibles.

1493. Adicionalmente, Android dispone en sus versiones más recientes de otras capacidades y ajustes de configuración asociados a la app del teléfono<sup>87</sup> que pueden tener implicaciones desde el punto de vista de seguridad. Para acceder a estas capacidades, se abrirá la app “Teléfono” y se pulsará la opción “...” de la esquina superior derecha seguida de “Ajustes”:

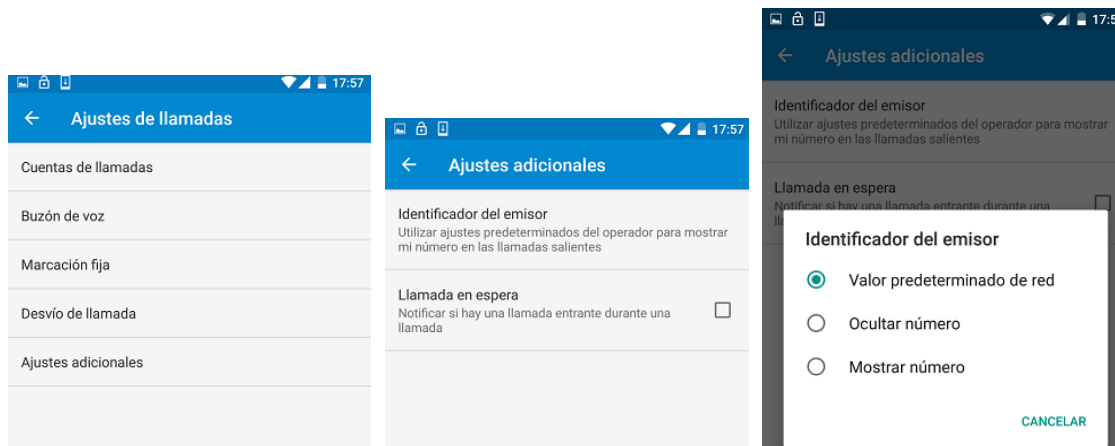


1494. Con el objetivo de proteger la privacidad del usuario, el módulo de telefonía de Android, en concreto la app del teléfono, permite al usuario definir en qué tipo de llamadas se enviará la información de identificación como autor de la llamada: “Valor

<sup>87</sup> <https://support.google.com/nexus/answer/2895524>

predeterminado de red” (opción por defecto), “Ocultar número” (siempre se ocultará) o “Mostrar número” (siempre se mostrará para todas las llamadas realizadas).

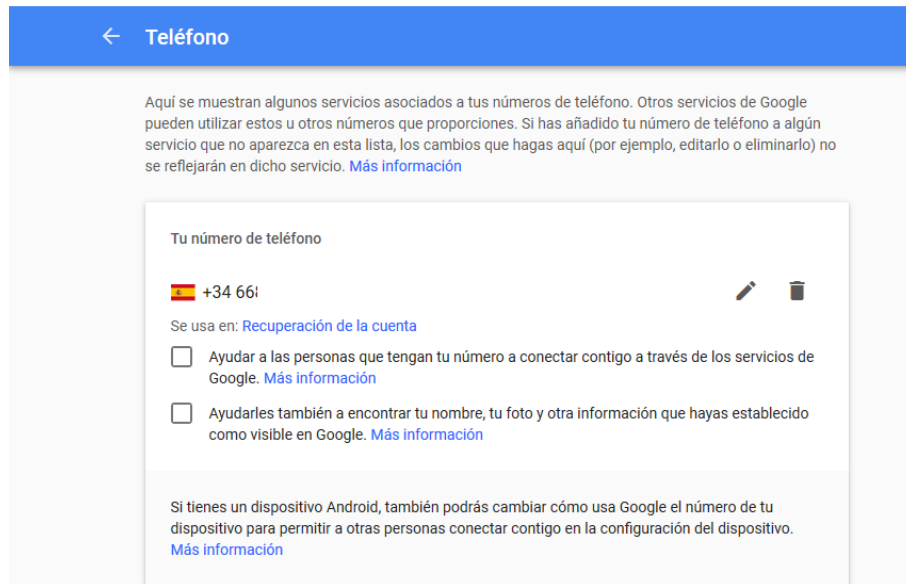
1495. Desde la app del teléfono, mediante el menú de opciones avanzadas disponible en la parte superior derecha, a través del menú “Ajustes - Llamadas - Ajustes adicionales”, “Identificador del emisor”, es posible configurar la opción deseada:



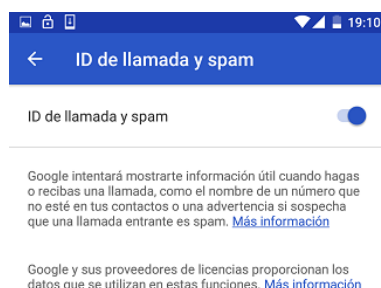
**Nota:** El menú para acceder al ajuste de identificador del emisor en cada dispositivo móvil depende de la versión de la app “Teléfono”, por lo que puede no coincidir con el descrito en la descripción anterior. La versión de la app “Teléfono” empleada para la elaboración de la presente guía es la 16.0.184899494.

1496. Desde la versión Android 4.4 (KitKat), Google ha implementado la identificación de llamadas inteligente, también denominada identificación de llamada de Google [Ref.-148]. Cuando se recibe (o se realiza) una llamada de alguien que no está en la agenda o lista de contactos, el teléfono buscará coincidencias para las personas en base a la información disponible en su cuenta de usuario de Google (desde el año 2014<sup>88</sup>) y para las empresas que tengan una ficha local en Google My Business.
1497. En el caso de compañías y organizaciones que hagan uso de cuentas de trabajo, o de centros educativos, el servicio tratará de buscar coincidencias en los directorios propios para ver si contienen información sobre dichos contactos.
1498. La visibilidad del número de teléfono propio para otras personas puede ser modificada a través de los ajustes de la cuenta de usuario de Google, en concreto, desde el siguiente enlace “<https://myaccount.google.com/phone?pli=1>”, mediante la opción disponible en la parte inferior:

<sup>88</sup> <https://plus.google.com/photos/+android/albums/5942570061497141729>



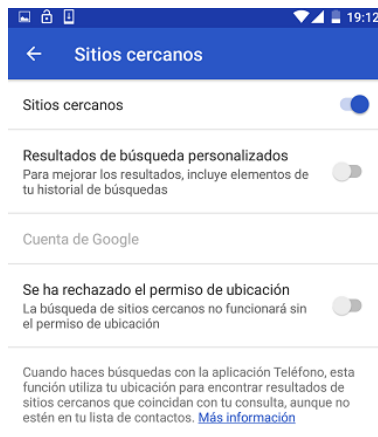
1499. La modificación del número de teléfono asociado a la cuenta de usuario de Google afecta a los servicios de Google listados en la página web anterior. Debe tenerse en cuenta que existen numerosos servicios que pueden hacer uso del número de teléfono del usuario<sup>89</sup>.
1500. La visibilidad del número de teléfono en la cuenta de usuario de Google está habilitada por defecto, por lo que se recomienda deshabilitarla si no se desea compartir el número de teléfono propio con otros usuarios. Si se deja habilitada, otros usuarios podrán enviar un mensaje (no sólo a través de aplicaciones como Hangouts que usan el número de teléfono, sino también mensajes de correo electrónico), o consultar el nombre o la foto del perfil al establecer una llamada.
1501. Adicionalmente, existe una opción que permite que, al recibir o cursar una llamada asociada a un número que no forma parte de los contactos, se intente ofrecer información sobre el otro interlocutor. Esta funcionalidad está disponible en Android desde la app del teléfono, mediante el menú de opciones avanzadas disponible en la parte superior derecha, a través del menú "... - Ajustes - ID de llamada y spam" (opción que por defecto está habilitada) [Ref.- 147]:



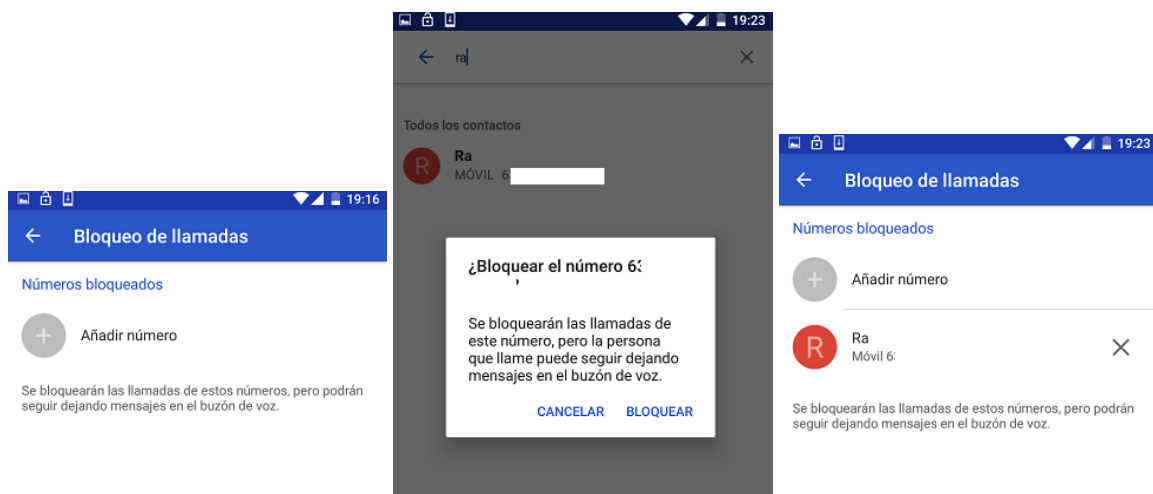
1502. Los identificadores de llamada de Google no se añaden automáticamente a la lista de contactos. Desde el punto de vista de seguridad, si no se desea hacer uso de esta funcionalidad, se recomienda deshabilitarla.

<sup>89</sup> <https://support.google.com/accounts/answer/3463280?p=modifynumber>

1503. En resumen: por un lado, desde la configuración del número de teléfono de la cuenta de usuario de Google, el propietario del dispositivo móvil puede definir si desea que otros usuarios tengan capacidad para localizarle en base al número de teléfono propio; por otro lado, desde los ajustes de la app “Teléfono” en Android es posible configurar si se desea localizar a otros usuarios (que lo permitan) a través de la funcionalidad del identificador de llamada de Google.
1504. También en Android 6.x se dispone de capacidades en el teléfono para utilizar la ubicación del dispositivo móvil con el fin de encontrar sitios cercanos que coincidan con las búsquedas realizadas en el dispositivo móvil, aunque la información proporcionada no esté disponible en la agenda o lista de contactos, actuando de guía telefónica.

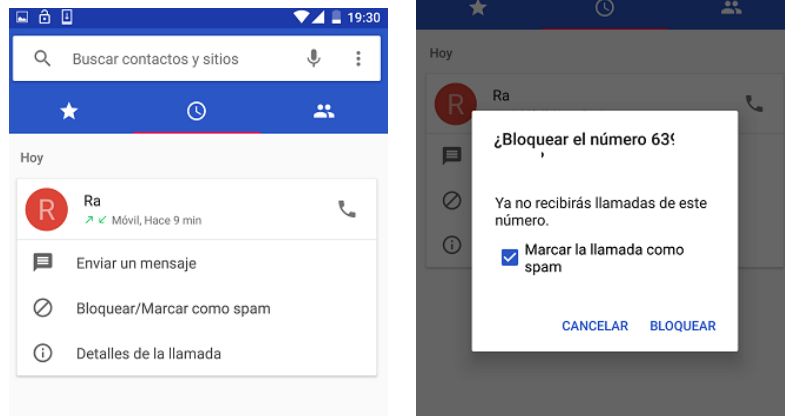


1505. La opción “Se ha rechazado el permiso de ubicación” aparecerá inactiva si se denegó el permiso de ubicación a la app “Teléfono”. Si se activa este interruptor, se abrirá un menú que solicitará de nuevo al usuario el permiso de ubicación para dicha app.
1506. Aunque en algunas versiones de la app “Teléfono” no existe una opción directa para bloquear números de teléfono de los cuales no se desea recibir llamadas, en la versión empleada en la elaboración de la presente guía sí está disponible desde el menú “Ajustes de la app Teléfono - Bloqueo de llamadas”.

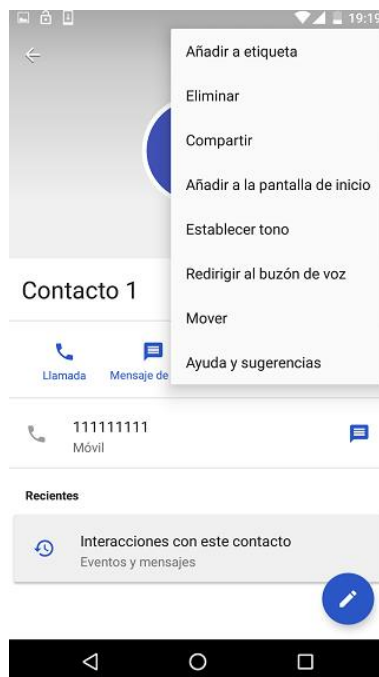


1507. Otra opción para bloquear un número es seleccionarlo desde la lista de contactos con una pulsación larga y marcar “Bloquear/Marcar como spam”:

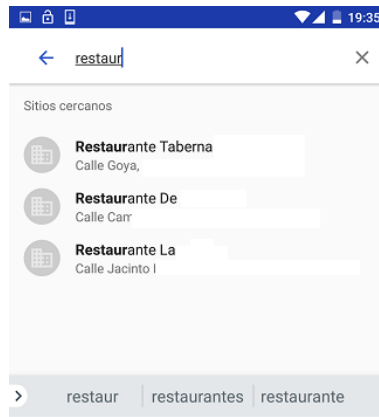




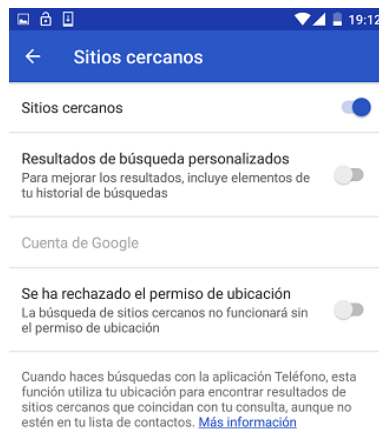
1508. Adicionalmente, se puede seleccionar un número del historial de llamadas, o un contacto de la lista de contactos, y pulsar sobre los tres puntos “(...)” que representan los ajustes en la parte superior derecha de la app, seguido de la opción “Redirigir al buzón de voz”. De este modo, las llamadas procedentes de ese número no se cursarán hacia el dispositivo móvil. Sin embargo, sí se recibirán los SMS desde dicho número.



1509. Cuando se realiza una búsqueda en la agenda o lista de contactos desde la app “Teléfono”, el teléfono buscará información relacionada de sitios cercanos y la mostrará en la parte superior. Para ello es necesario que estén activos los servicios de localización en Android:



1510. La configuración de esta funcionalidad está disponible desde la app del teléfono, mediante el menú de opciones avanzadas disponible en la parte superior derecha, a través del menú “Ajustes de la app Teléfono - Sitios cercanos” (por defecto la opción está habilitada):



1511. Los teléfonos sugeridos para sitios cercanos no se añaden automáticamente a la lista de contactos, aunque sí se pueden guardar posteriormente de forma manual, mediante la opción “Añadir a contactos”. De nuevo, desde el punto de vista de seguridad, si no se desea hacer uso de esta funcionalidad, se recomienda deshabilitarla.

**Nota:** Android 4.4 (KitKat) y versiones posteriores permiten la realización de llamadas por Internet (VoIP, *Voice over IP*) mediante el protocolo SIP (*Session Initiation Protocol*) de señalización si el proveedor de telefonía ofrece dichas capacidades y el dispositivo móvil está conectado a una red Wi-Fi<sup>90</sup>.

Existen soluciones propietarias de cifrado extremo a extremo de las comunicaciones y llamadas de voz, como RedPhone (de código abierto), proporcionadas por terceras compañías a través de Google Play [Ref.- 29]. RedPhone hace uso del protocolo ZRTP para negociar las claves de cifrado empleadas en el protocolo SRTP, utilizado para cifrar las comunicaciones de Voz sobre IP (VoIP) entre dos terminales Android (o también con terminales basados en iOS mediante la app Signal<sup>91</sup>), haciendo uso de redes Wi-Fi o de la infraestructura de datos de los operadores de telefonía móvil, y empleando comunicaciones de datos cifradas mediante TLS con los servidores de RedPhone (para el protocolo de señalización) y mensajes SMS cifrados para el establecimiento de las llamadas.

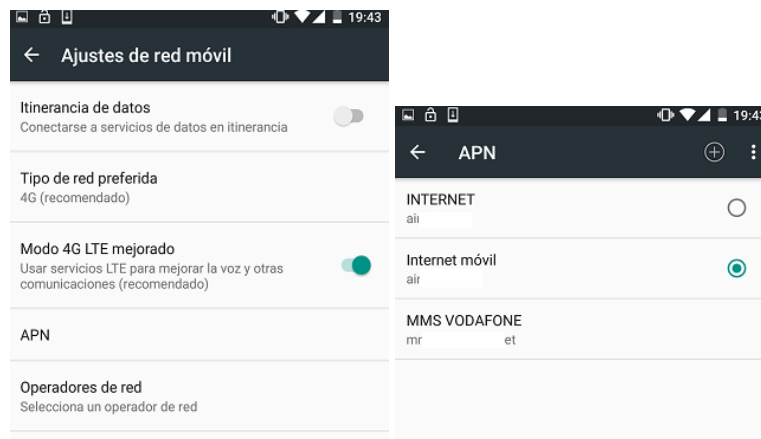
<sup>90</sup> <https://support.google.com/nexus/answer/2811843>

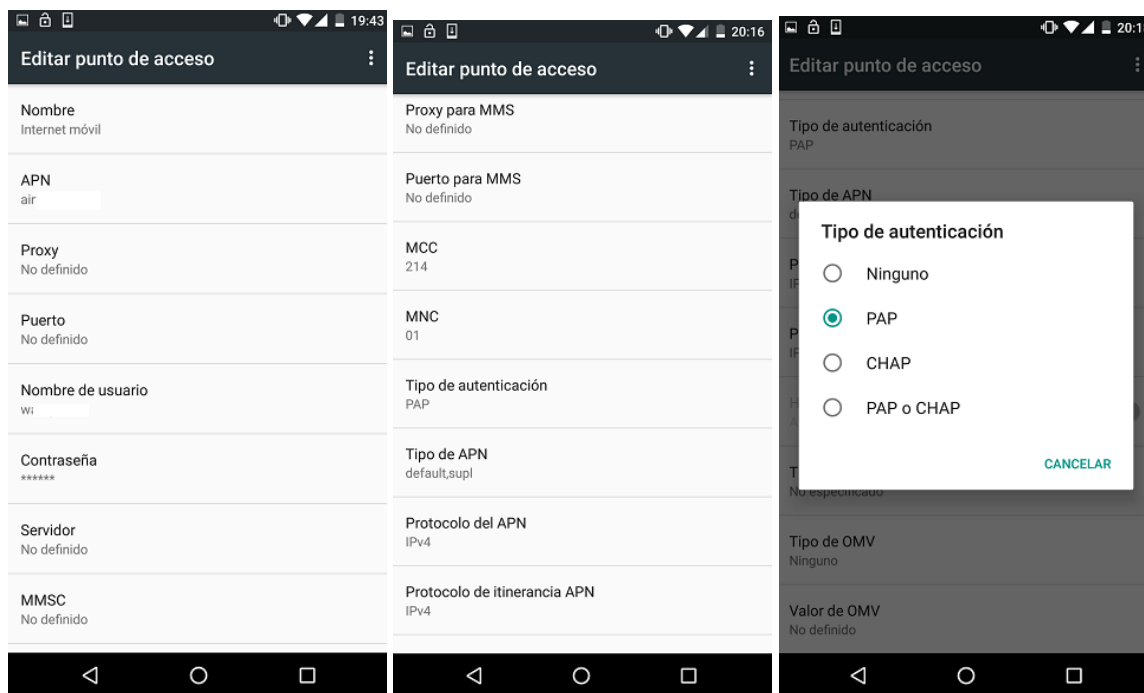
<sup>91</sup> <https://github.com/WhisperSystems/Signal-iOS>

Actualmente, las soluciones y apps de mensajería (WhatsApp, Signal, Telegram, Line, Viber, etc.) han incorporado capacidades para la realización de llamadas de voz en tiempo real mediante VoIP, haciendo una amplia utilización de diferentes mecanismos de cifrado, y en algunos casos como Signal [Ref.- 32], sustituyendo apps previas como RedPhone.

### 18.3. CONFIGURACIÓN DE LA RED DE DATOS MÓVILES

1512. Android permite al usuario, al igual que para la red de telefonía móvil (SMS y voz), utilizar la red de datos configurada automáticamente a través de la tarjeta SIM, así como seleccionar de forma manual tanto el operador de telecomunicaciones móviles como el APN (*Access Point Name*) para las conexiones de datos.
1513. En dispositivos móviles Android como el empleado para la elaboración de la presente guía, al introducir la tarjeta SIM en el dispositivo móvil se lleva a cabo automáticamente el proceso de configuración de las opciones de conectividad de datos asociadas a las redes de telefonía móvil, incluyendo los APNs y su configuración: nombre, APN, proxy y puerto, credenciales (usuario y contraseña), servidor, dispositivos de mensajes multimedia (MMS: MMSC, proxy y puerto MMS), MCC, MNC, tipo de autenticación y tipo de APN.
1514. En función de la tarjeta SIM empleada y de la configuración de datos que ésta tenga asociada, se mostrarán automáticamente los ajustes de conexión disponibles en la lista de APNs, o ningún APN si no dispone de los datos correspondientes (en cuyo caso habrá que añadirlo manualmente).
1515. Desde el menú de “Ajustes [Conexiones Inalámbricas y Redes] - Más... - Redes móviles”, y a través de la opción “APN”, es posible acceder a las opciones para seleccionar el APN empleado para las conexiones de datos. Mediante la selección del APN de la lista es posible editar la configuración de los APNs existentes, y a través de los botones de la parte superior derecha es posible añadir nuevos APNs o restablecer la configuración inicial:



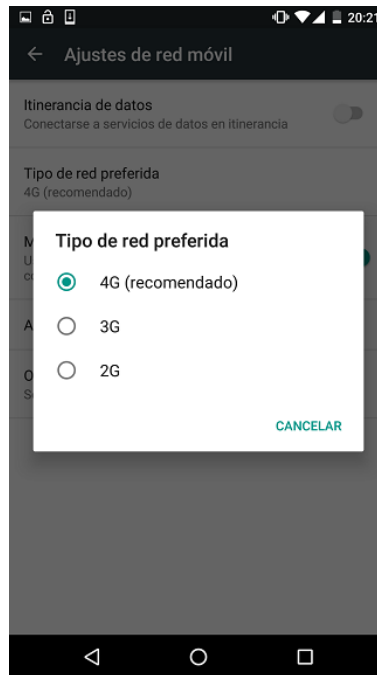


1516. Al definir un nuevo APN deben emplearse los valores proporcionados por el operador de telecomunicaciones. Desde el punto de vista de seguridad, y si el operador admite diferentes protocolos de autenticación, se recomienda seleccionar autenticación mediante CHAP, dentro de las cuatro alternativas disponibles en la opción “Tipo de autenticación” (Ninguno, PAP, CHAP, y “PAP o CHAP”). Por defecto, el tipo de autenticación no está definido en el perfil del APN, como se ilustra en la imagen superior derecha:
1517. En el escenario de autoconfiguración existente por defecto, desde el punto de vista de seguridad, se recomienda acceder a la configuración de datos de telefonía móvil y, en concreto, a la lista de APNs para adecuar la configuración a la deseada por el usuario cada vez que se cambia la tarjeta SIM.

#### 18.4. SELECCIÓN DE LA RED DE DATOS MÓVILES

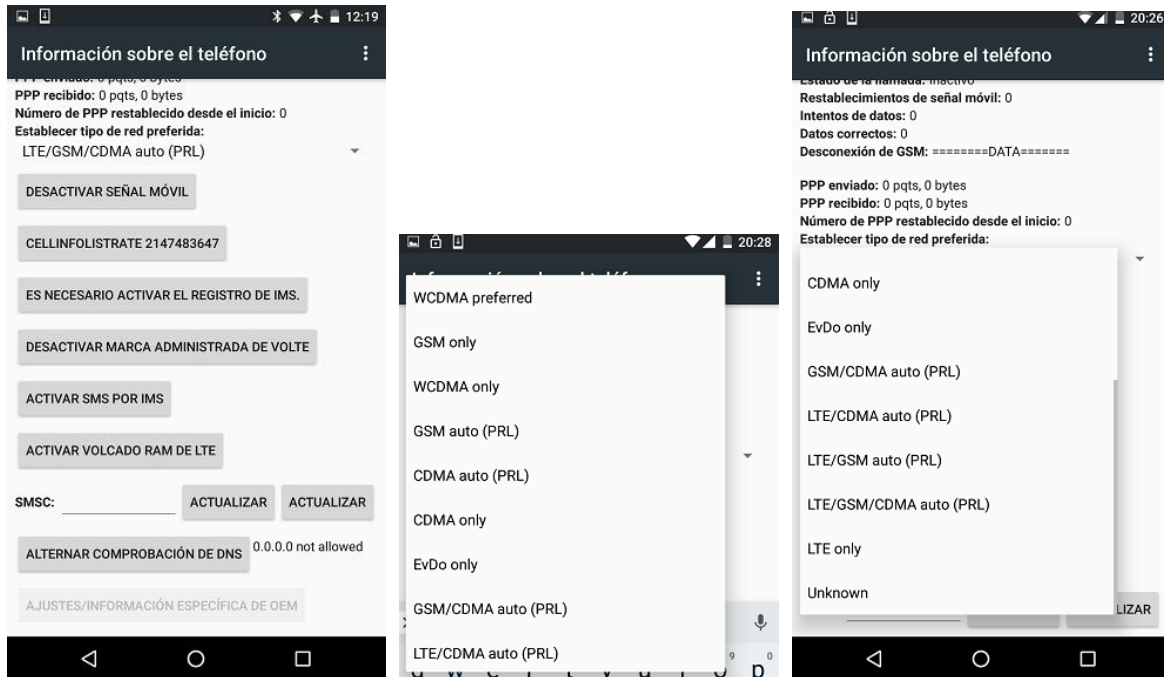
1518. Las redes de telefonía 2G (o GSM) presentan diferentes vulnerabilidades en la actualidad, como por ejemplo la posibilidad de suplantación de la red por parte de un potencial atacante debido a debilidades en los mecanismos de autenticación, o la posibilidad de capturar y descifrar el tráfico de voz GSM debido a debilidades en los algoritmos de cifrado, A5/1 [Ref.- 400].
1519. Con el objetivo de mitigar las vulnerabilidades existentes actualmente en las redes de telefonía móvil 2G (o GSM), se recomienda forzar al dispositivo móvil a conectarse únicamente, tanto para comunicaciones de voz como de datos, a las redes de telefonía 3G (UMTS) o 4G (LTE).
1520. Android no permite restringir las comunicaciones de telefonía móvil sólo a redes 3G o 4G a través del interfaz de usuario estándar (ver opciones mediante el menú de prueba o *testing* posteriormente).
1521. A través del menú “Ajustes [Conexiones Inalámbricas y Redes] - Más... - Redes móviles”, y en concreto de la opción “Tipo de red preferida”, es posible indicar que sólo se haga uso de redes 2G (GSM - GPRS o EDGE), una opción indicada para disminuir el

consumo de batería del terminal, pero desaconsejada desde el punto de vista de seguridad:

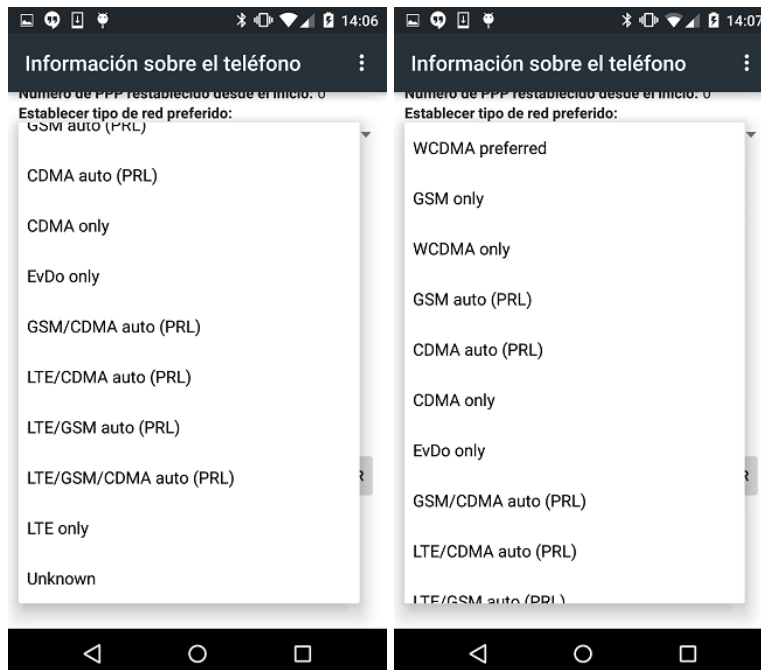


1522. La opción por defecto es “4G (recomendado)”. Se recomienda no modificar esta opción, especialmente al valor “2G”, pese a que el dispositivo móvil hará uso automáticamente de redes 2G en zonas donde no se disponga de suficiente cobertura por parte de las redes 3G o 4G.
1523. El principal inconveniente de esta configuración (no modificable) es que si el usuario se encuentra en una zona en la que no se dispone de cobertura 3G (o superior, 3.5G o 4G), se podrá hacer uso del dispositivo móvil a través de 2G, premiando la disponibilidad del servicio de telefonía (voz y datos) por encima de la seguridad.
1524. Android proporciona información en la barra superior de estado a través de un conjunto de iconos específico sobre las tecnologías de telefonía móvil de datos para las que se dispone de cobertura, que representan la disponibilidad y el estado de la conexión para una red 4G (LTE), 3G o 3.5G (WCDMA/UMTS o HSPA), 2.75G (EDGE) y 2G (GPRS).
1525. La cobertura y conectividad existentes están identificadas por un icono con forma de triángulo (barras en progresión ascendente), que indica la cobertura existente en función del número de barras activas, o que no se dispone de cobertura si el icono con forma de triángulo está vacío (no dispone de ninguna barra).
1526. La configuración por defecto del dispositivo móvil premia la conectividad, permitiendo el uso de redes de telefonía móvil 2G, 3G o 4G de forma automática en función de su cobertura y disponibilidad.
1527. Adicionalmente, es posible obtener y configurar información avanzada a través del menú de prueba (o *testing*), disponible en Android tras marcar el siguiente número de teléfono: \*##4636##\* (o \*##info##\*). Se debe ser muy cuidadoso a la hora de hacer uso de las diferentes opciones que este menú ofrece, ya que permite cambiar opciones asociadas a la telefonía que podrían afectar a la funcionalidad del terminal, como por ejemplo la selección de bandas de frecuencia de USA, no válidas en Europa.

1528. Mediante la selección de la opción “Información sobre el teléfono” se dispone de numerosos detalles de la red de telefonía móvil, siendo posible configurar el tipo de red preferida en la parte inferior de dicha pantalla, mediante la opción “Establecer tipo de red preferida”:



1529. De las diferentes opciones disponibles, desde el punto de vista de seguridad se recomienda seleccionar la opción “LTE only” o “WCDMA only” para forzar al dispositivo móvil a conectarse únicamente a redes 4G o 3G. Por defecto la opción seleccionada es “LTE/GSM auto (PRL)”, donde el término PRL hace referencia a la “Preferred Roaming List” definida por los operadores de telefonía móvil:



1530. Este cambio de configuración prevalece incluso tras reiniciar el dispositivo móvil y fuerza a que el dispositivo móvil sólo haga uso de redes 4G o 3G, más seguras que las redes 2G.

1531. Se debe ser muy cauteloso a la hora de acceder al menú de prueba, y únicamente aplicar las recomendaciones expuestas en la presente guía, dado que algunas de ellas pueden provocar comportamientos inesperados en el dispositivo móvil.

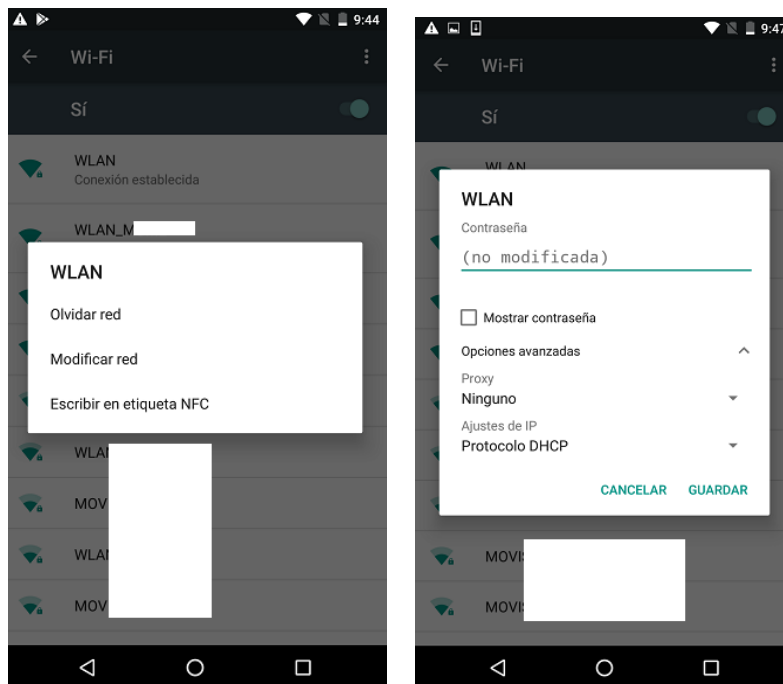
## 19. COMUNICACIONES TCP/IP

1532. Esta sección proporciona recomendaciones de seguridad para la pila de comunicaciones TCP/IP del dispositivo móvil, incluyendo recomendaciones generales para TCP/IP (IPv4), SSL/TLS, IPv6 y redes VPN.

### 19.1. ADAPTADORES DE RED

1533. La información del adaptador de red disponible en el dispositivo móvil para las comunicaciones mediante tecnologías Wi-Fi (interfaz Wi-Fi) está disponibles desde el menú “Ajustes [Conexiones Inalámbricas y Redes] - Wi-Fi”, una vez se ha establecido una conexión con una red Wi-Fi, mediante una pulsación prolongada sobre dicha red en la lista de redes Wi-Fi disponibles, ya que se mostrará el menú que permite borrar o modificar dicha red.

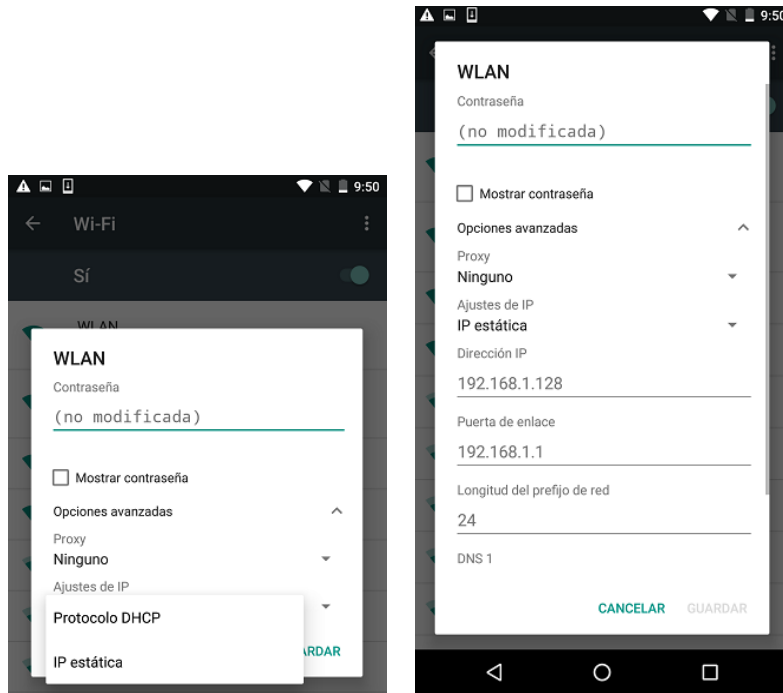
1534. La opción “Modificar red” permite disponer de acceso a la configuración de la red, y mediante la opción “Opciones avanzadas” es posible visualizar y cambiar la configuración del adaptador de red Wi-Fi:



1535. La pantalla de ajustes avanzados permite seleccionar si se utilizará una dirección IP estática o dinámica (DHCP). Por defecto, la configuración de TCP/IP empleada para la conexión a las redes Wi-Fi hace uso de una dirección IP dinámica obtenida mediante el protocolo DHCP.

1536. La configuración de la dirección IP estática permite definir la dirección IP, la puerta de enlace (o router por defecto), la máscara (o prefijo) de red, así como los (dos) servidores DNS:

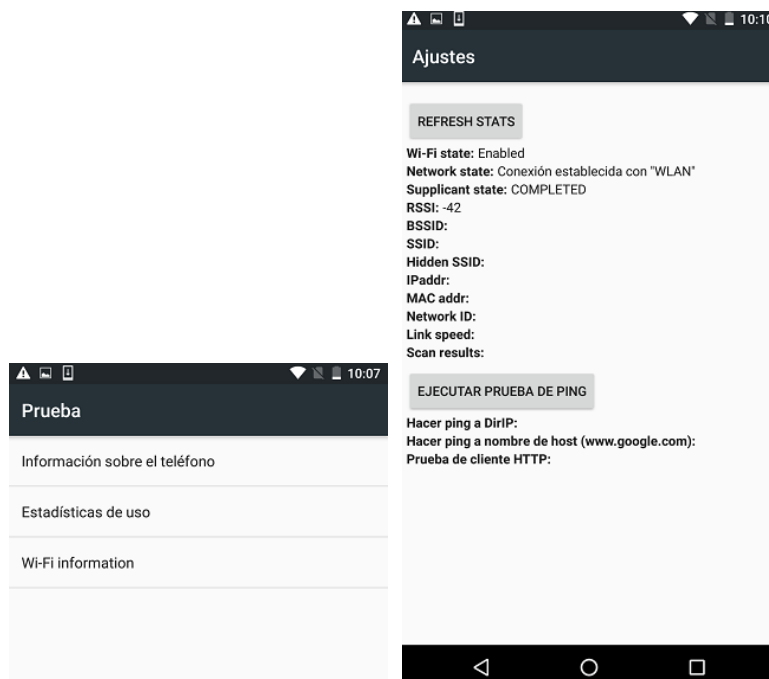




1537. La configuración del direccionamiento IP del interfaz Wi-Fi es independiente para cada una de las redes Wi-Fi configuradas (desde la versión 4.0 de Android, “Ice Cream Sandwich”), en lugar de disponerse de una configuración o perfil de red único para todas las red Wi-Fi, tal como ocurría en versiones previas de Android, como 2.x [Ref.-96].
1538. En el caso de emplear una dirección IP asignada dinámicamente por DHCP, es posible obtener información de la misma a través de la entrada correspondiente a la red inalámbrica con la que se ha establecido la conexión Wi-Fi. Desde el menú “Ajustes [Conexiones Inalámbricas y Redes] - Wi-Fi, se muestra la lista de redes Wi-Fi visibles y aquélla a la que estamos conectados.
1539. Mediante una pulsación breve sobre dicha red, “WLAN” en el ejemplo, se mostrará una pantalla con los datos de conexión a dicha red, pero que en Android 6.x no incluyen la dirección IP que ha sido asignada al dispositivo móvil por el servidor DHCP, tal como ocurría en versiones previas de Android hasta la 4.4.x.
1540. Para acceder a la información de la dirección IP es necesario acceder a la parte inferior de la pantalla de ajustes avanzados de Wi-Fi, a través del menú superior derecho, o acceder a la información de estado del dispositivo móvil, a través de “Ajustes - Información del teléfono - Estado”:



1541. Adicionalmente, es posible obtener esta información a través del menú de prueba (o testing), disponible en Android tras marcar el siguiente número de teléfono: **\*\*\*4636\*\*\*** (o **\*\*\*info\*\*\***):



1542. La opción “Wi-Fi information - Wi-Fi status”, tras pulsar el botón “Refresh stats” en caso de no disponer de datos, proporciona los detalles de conexión de la red Wi-Fi actual, en el ejemplo, red “WLAN” (ver imágenes superiores).
1543. Android no proporciona ningún método a través del interfaz de usuario estándar para consultar la dirección IP asignada de forma dinámica por el operador de telefonía móvil al utilizar las redes de datos de telefonía móvil 2/3/4G.
1544. En versiones anteriores de Android, esta información podía obtenerse a través del menú de prueba disponible tras marcar el siguiente número de teléfono: **\*\*\*4636\*\*\*** (o **\*\*\*info\*\*\***). Bajo la opción “Información sobre el teléfono”, en concreto en la

sección inferior denominada “Desconexión de GSM”, era posible visualizar la dirección IP asignada al dispositivo móvil en el interfaz de datos 2/3/4G (“rmnet0”), junto a las direcciones IP del gateway y de los servidores DNS. Para el dispositivo móvil con la versión 6.0.1 de Android no se muestra la configuración a nivel IP del interfaz de datos de telefonía del dispositivo móvil.

1545. Si se precisa conocer la información de la configuración TCP/IP para el interfaz de telefonía móvil, existe la posibilidad de emplear el comando “ifconfig” (previa invocación del comando “adb shell” desde un ordenador). El direccionamiento IP se muestra como “wlan0” para el interfaz Wi-Fi (“wlan0”) y como “rmnet\_data0” para el interfaz de telefonía:

```

Windows PowerShell
shell@bullhead:/ $ ifconfig
rmnet_ipa0 Link encap:UNSPEC
 UP RUNNING MTU:2000 Metric:1
 RX packets:199 errors:0 dropped:0 overruns:0 frame:0
 TX packets:248 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:16908 TX bytes:18724

dummy0 Link encap:UNSPEC
 inet6 addr: fe80::f41d:80ff:fee8:3d84/64 Scope: Link
 UP BROADCAST RUNNING NOARP MTU:1500 Metric:1
 RX packets:0 errors:0 dropped:0 overruns:0 frame:0
 TX packets:3 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:0
 RX bytes:0 TX bytes:210

rmnet_data0 Link encap:UNSPEC
 inet addr:100.80.138.160 Mask:255.255.255.192
 inet6 addr: fe80::19585:3052:f134:567c/64 Scope: Link
 UP RUNNING MTU:1500 Metric:1
 RX packets:48 errors:0 dropped:0 overruns:0 frame:0
 TX packets:61 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:9600 TX bytes:7868

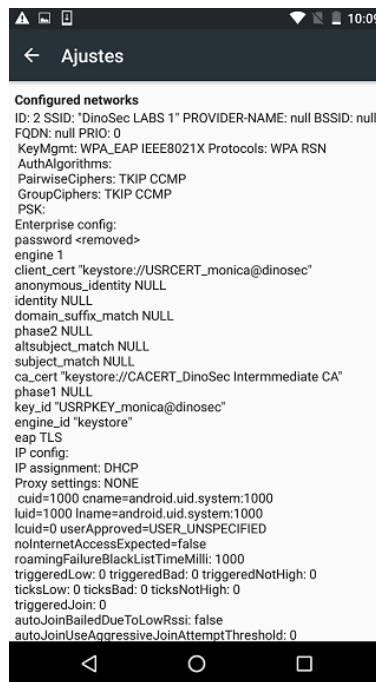
r_rmnet_data0 Link encap:UNSPEC
 inet6 addr: fe80::a48c:5b1c:c91a:5aa5/64 Scope: Link
 UP RUNNING MTU:3000 Metric:1
 RX packets:151 errors:0 dropped:0 overruns:0 frame:0
 TX packets:187 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:6040 TX bytes:18856

lo Link encap:UNSPEC
 inet addr:127.0.0.1 Mask:255.0.0.0
 inet6 addr: ::1/128 Scope: Host
 UP LOOPBACK RUNNING MTU:65536 Metric:1
 RX packets:968 errors:0 dropped:0 overruns:0 frame:0
 TX packets:968 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:0
 RX bytes:81000 TX bytes:81000

shell@bullhead:/ $

```

1546. La opción “Wi-Fi information - Wi-Fi config” proporciona los detalles de todas las redes que forman parte de la PNL (en la que se incluyen las redes a las que el dispositivo móvil se ha conectado y las que se han añadido de forma manual). Entre los detalles que se muestran, se incluye el tipo de seguridad Wi-Fi de la red y, si procede, la relación de certificados digitales asociados a cada red:



## 19.2. SEGURIDAD EN TCP/IP

1547. Con el objetivo de incrementar el nivel de seguridad de la pila TCP/IP empleada para las conexiones de datos en Android, se recomienda evaluar su comportamiento y (de ser posible) modificar ciertos parámetros de configuración que condicionan su funcionamiento y nivel de seguridad.

1548. Teóricamente desde el punto de vista de seguridad, se recomienda deshabilitar el procesamiento de paquetes de *ping*, es decir, paquetes ICMP *echo request* entrantes y sus respuestas asociadas, paquetes ICMP *echo response* salientes, con el objetivo de limitar el descubrimiento del dispositivo móvil en la red (habilitados por defecto en Android).

**Nota:** No se ha identificado ningún mecanismo, ni opción de configuración, en Android que permita deshabilitar el procesamiento de paquetes de *ping*, es decir, la recepción de paquetes ICMP *echo request* y sus respuestas asociadas, ICMP *echo response*.

Igualmente, no se han encontrado mecanismos que permitan modificar los diferentes parámetros de configuración de bajo nivel de la pila TCP/IP mencionados en este apartado.

1549. Android también responde a otros tipos de mensajes ICMP de petición y respuesta, como por ejemplo ICMP *timestamp*, aunque no responde a mensajes ICMP *address subnet mask*.

1550. La identificación del dispositivo móvil también se puede llevar a cabo a través del protocolo DHCP, ya que en las peticiones DHCP (DHCP *Discover* y *Request*) Android incluye varios datos identificativos.

1551. Las peticiones de Android añaden la opción 60 de DHCP, identificación del vendedor (*Vendor class identifier*), con el mensaje "dhcpcd-5.5.6", es decir, hace uso del cliente DHCP estándar de Linux DHCPD (DHCP Client Daemon), versión 5.5.6.

1552. Debe tenerse en cuenta que la última versión disponible de dhcpcd para Linux puede ser mucho mayor a la utilizada por Android, y solucionar diferentes vulnerabilidades de seguridad conocidas públicamente [Ref.- 47].

**Nota:** Por ejemplo, en septiembre de 2014 se publicó una vulnerabilidad de denegación de servicio (DoS) en dhcpcd que afectaba a todas las versiones desde la 4.0.0 hasta la 6.4.2. Se confirmó que la versión 5.5.6 de dhcpcd disponible en Android 4.4.x era vulnerable, estando solucionada esta vulnerabilidad en Android 5.0 (Lollipop), pese a hacer uso del mismo número de versión de dhcpcd [Ref.- 196]. Más información:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6060>

<http://roy.marples.name/projects/dhcpcd/ci/1d2b93aa5ce25a8a710082fe2d36a6bf7f5794d5?sbs=0>

1553. Las peticiones también incluyen la opción 12 de DHCP, nombre de equipo (*Host Name*), con el valor “android\_<código>”, donde “<código>” es un string de 16 caracteres hexadecimales correspondiente al ANDROID\_ID (asociado a la propiedad “net.hostname”; ver apartado “7.10. Configuración por defecto del dispositivo móvil”).

1554. Adicionalmente, por defecto el dispositivo móvil Android envía peticiones NTP (*Network Time Protocol, UDP/10203*) para su sincronización horaria hacia servidores NTP disponibles en Internet periódicamente.

### 19.3. ESCANEOS DE PUERTOS TCP Y UDP

1555. A continuación, se analiza el comportamiento de la pila TCP/IP de Android frente a intentos de conexión TCP y UDP a través del interfaz Wi-Fi. El análisis se ha realizado en la configuración por defecto del dispositivo móvil, es decir, sin haber realizado ninguna configuración específica o instalación adicional de software.

1556. Android responde con un paquete TCP *Reset* a las peticiones de conexión hacia puertos TCP cerrados.

1557. Por defecto, Android no dispone de ningún puerto TCP abierto o filtrado, es decir, los 65.536 puertos TCP están cerrados.

1558. Android responde con paquetes ICMP de tipo 3 y código 3 (destino inalcanzable, puerto inalcanzable), limitados a uno por segundo, a las peticiones de conexión hacia puertos UDP cerrados.

1559. Por defecto, Android no dispone de ningún puerto UDP abierto, tanto si DHCP está configurado en el interfaz Wi-Fi como cuando se utiliza una dirección IP estática.

1560. El comportamiento por defecto de la pila TCP/IP, y especialmente la ausencia de mecanismos de filtrado de tráfico (cortafuegos personal) y sus peculiaridades a nivel de TCP y UDP, podrían hacer posible la identificación de los dispositivos móviles basados en Android.

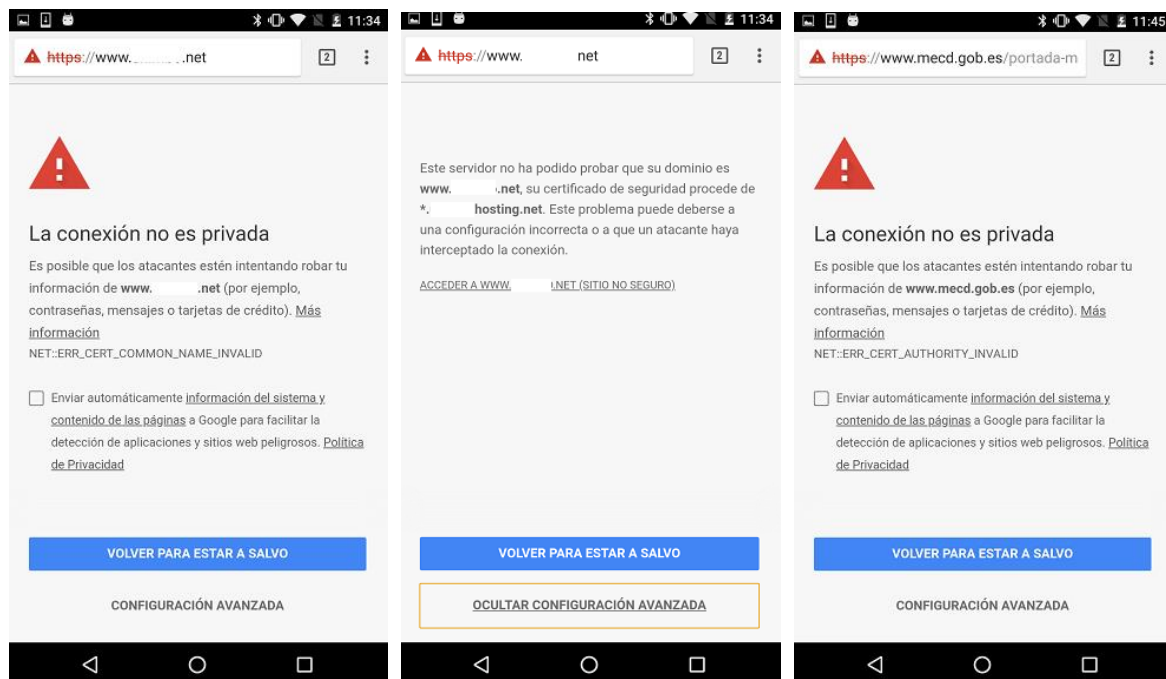
1561. Este tipo de identificación remota a través de la red facilitaría a un potencial atacante la realización de ataques dirigidos sobre vulnerabilidades conocidas, por lo que se enfatiza la necesidad de mantener el software del dispositivo móvil completamente actualizado en todo momento.

**Nota:** El comportamiento de la pila TCP/IP frente a escaneos de puertos a través del interfaz de telefonía móvil de datos (cuando está conectado a la red real del operador) no puede ser analizado de forma fiable. Este comportamiento a través del interfaz de telefonía móvil de

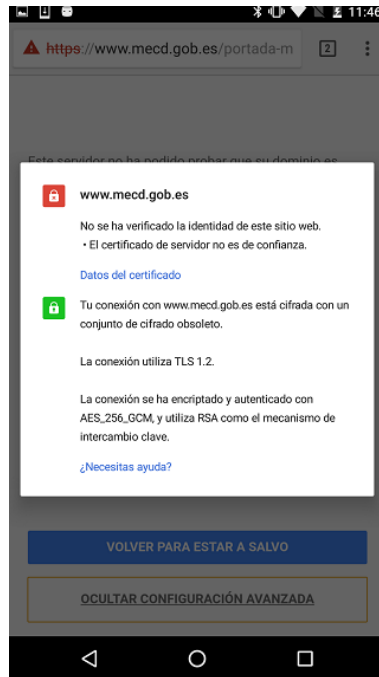
datos está condicionado por la infraestructura de comunicaciones y los mecanismos de filtrado de los operadores de telefonía móvil, que por ejemplo, pueden no permitir comunicaciones mediante ping (*ICMP echo request* y *reply*) o pueden disponer de *proxies* transparentes en la red, por ejemplo para protocolos como FTP o HTTP.

## 19.4. HTTPS: SSL/TLS

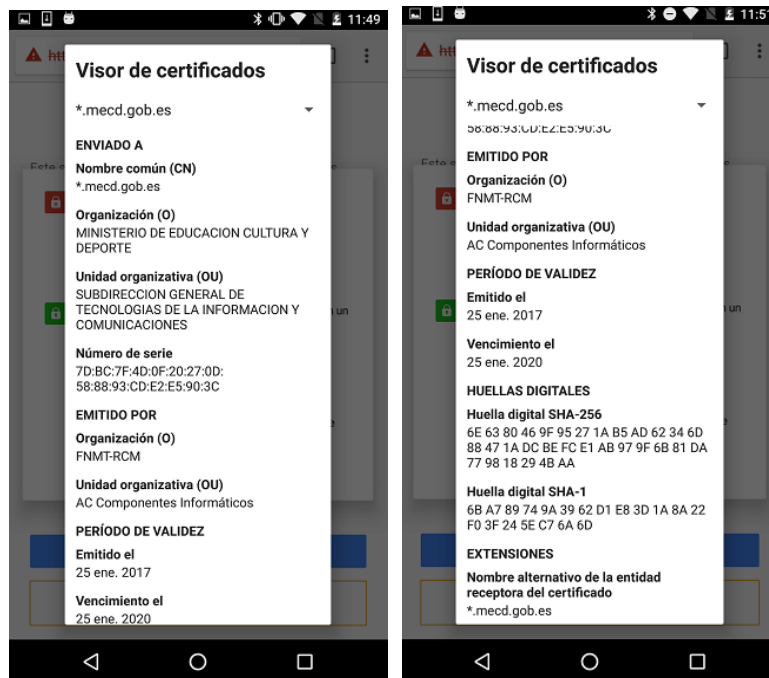
1562. Android dispone de una implementación de los protocolos SSL, Secure Socket Layer, y TLS, Transport Layer Security, a través del paquete Java denominado “*javax.net.ssl*”, con soporte para SSL v3.0 y hasta TLS v1.2, basado (parcialmente) en la implementación de *The Legion of the Bouncy Castle* y de OpenSSL [Ref.- 102].
1563. Desde Android 6.x, Google migró internamente a una implementación propia de la librería de SSL y TLS denominada BoringSSL, empleada también por Chromium y otros servicios de Google [Ref.- 622].
1564. Desde enero de 2017, al acceder a un sitio web mediante HTTPS utilizando el navegador web existente en Android por defecto (app “Chrome” en Android 6.x), el dispositivo móvil intentará verificar el certificado digital asociado y su cadena de confianza, hasta la autoridad certificadora (CA, *Certificate Authority*) raíz reconocida correspondiente.
1565. En caso de que no sea posible verificar la validez de un certificado, el navegador web de Android generará un mensaje de advertencia, indicando el motivo del error y permitiendo al usuario ver y analizar algunos detalles del motivo a través del enlace de opciones avanzadas:



1566. Sin embargo, la información detallada del certificado digital obtenido no está disponible directamente. Es necesario pulsar el icono superior de color rojo con un triángulo, disponible en la barra de navegación o URL, y seleccionar “Detalles” para así poder obtener la información del certificado digital:



1567. El enlace “Datos del certificado” permite obtener los detalles del certificado digital a través del “Visor de certificados”, que incluye elementos clave para su verificación, como por ejemplo el número de serie del certificado, las huellas o *fingerprints* SHA-1 o SHA-256, información de la autoridad certificadora involucrada en su emisión, etc.:



1568. La pantalla con el enlace “Datos del certificado” también puede proporcionar, en su parte inferior, algunos detalles de la conexión TLS y de los algoritmos y parámetros negociados entre el navegador web y el servidor web (ver imágenes superiores).
1569. Si se acepta un certificado digital, éste será válido hasta que se cierre la instancia, proceso, o sesión actual del navegador web en Android.
1570. El aceptar un certificado que no es de confianza tiene el riesgo asociado de que el certificado digital aceptado, y desconocido, puede pertenecer a un potencial intruso que se encuentra realizando un ataque de interceptación del tráfico del usuario, MitM (Man-



in-the-Middle), sobre el protocolo SSL/TLS y las comunicaciones (supuestamente) cifradas.

1571. Como se describe en el apartado “11. Gestión de certificados digitales y credenciales”, en Android 6.x el repositorio de certificados raíz está accesible a través del interfaz de usuario de Android. Por tanto, el usuario puede gestionar la lista autoridades certificadoras (o CAs, *Certificate Authorities*) que son consideradas de confianza por Android.
1572. Android desde la versión 4.0 (Ice Cream Sandwich) soporta la utilización de mecanismos de autenticación web basados en certificados digitales cliente a través del navegador web existente por defecto [Ref.- 120], al igual que es posible hacer uso de certificados cliente para la conexión a redes Wi-Fi o redes VPN (ver apartado “11. Gestión de certificados digitales y credenciales”).
1573. La funcionalidad para el uso de certificados digitales cliente en el navegador web añadida finalmente en Android versión 4.0 [Ref.- 121] permite gestionar (visualizar, deshabilitar, habilitar, instalar, eliminar, etc.) las CAs desde el interfaz de usuario de Android y la sección “Ajustes - Seguridad”, así como gestionar certificados digitales cliente para el dispositivo móvil y las apps (como el navegador web o los clientes de correo electrónico) a través de un nuevo KeyChain (o gestor de credenciales y certificados) [Ref.- 122] [Ref.- 188].
1574. Previamente se disponía de un gestor de credenciales y certificados global para todo el sistema pero únicamente accesible para la conexión a redes Wi-Fi y VPN, a través de “Ajustes” [Ref.- 188]. Las apps debían hacer uso de sus propios gestores de certificados privados, ya que no disponían de una API para acceder a los certificados existentes en el repositorio del sistema.
1575. En Android 4.x, los certificados digitales cliente guardados en el repositorio de credenciales están disponibles para su utilización por parte del navegador web [Ref.- 185].
1576. Existen otros navegadores web de terceros (como por ejemplo Firefox para Android, junto al *add-on* o extensión Cert Manager<sup>92</sup>, SandroB, etc.), que también disponen de capacidades de autenticación web basada en certificados digitales cliente, y que adicionalmente definen su propio gestor de certificados cliente (KeyManager) y su propio gestor de confianza (TrustManager, para gestionar sus propias CAs) a través de “javax.net.ssl.SSLContext”.
1577. Android 5.x introdujo cambios en la configuración de TLS/SSL empleada, por ejemplo, para las conexiones HTTPS (entre otras), incluyendo soporte para TLS v1.1 y v1.2, AES-GCM (AEAD), y dando preferencia a los algoritmos con capacidades de *forward secrecy*, como ECDHE y DHE. Por otro lado, se deshabilita el soporte para MD5, 3DES, y los algoritmos ECDH con claves estáticas.
1578. El proveedor de seguridad de Google Play Services también ofrece estas capacidades para versiones de Android previas hasta la 2.3.
1579. El uso de SSLSocketFactory y SSLSocket directamente por parte de una app puede emplearse para establecer comunicaciones cifradas de bajo nivel sin hacer uso de la

<sup>92</sup> <https://addons.mozilla.org/en-US/mobile/addon/cert-manager/>

configuración y prerequisites del sistema previamente indicados, permitiendo el uso de algoritmos más inseguros.

## 19.5. IPV6

1580. El protocolo IP versión 6 (IPv6) está soportado y activado por defecto en Android para las comunicaciones de datos mediante Wi-Fi y telefonía móvil 2/3/4G.

1581. En Android 6.x el usuario dispone de capacidades para visualizar la información de las direcciones IPv6 a través del menú “Ajustes - Información del teléfono - Estado”, y en concreto, en el campo “Dirección IP”<sup>93</sup>, aunque no dispone de ninguna opción de configuración relacionada con IPv6 desde el interfaz gráfico de usuario (o GUI):



**Nota:** La disponibilidad de IPv6 para las comunicaciones de datos a través de la infraestructura de telefonía móvil en Android es dependiente tanto de la versión del sistema operativo, como del modelo de dispositivo móvil y del operador de telefonía móvil empleados [Ref.- 53].

1582. Por otro lado, y desde el punto de vista de la funcionalidad, es necesario evaluar si Android soporta únicamente redes de datos basadas en IPv6, sin hacer uso de la pila TCP/IP versión 4 [Ref.- 56]. Las redes de telefonía móvil 2/3/4G basadas sólo en IPv6 están soportadas por Android, y las redes Wi-Fi también lo están, aunque inicialmente con problemas conocidos de conectividad relacionados con la coexistencia de IPv6 e IPv4.

1583. Para disponer de conectividad IPv6 completa en Android y obtener una dirección IPv6 a través de mensajes RA (Router Advertisement) enviados por un router con soporte de IPv6 es necesario que el interfaz Wi-Fi disponga también de dirección IPv4 (estática o mediante DHCP).

<sup>93</sup> <https://plus.google.com/+KevinOtte/posts/JUHVxyW1AB3>

1584. Es posible forzar el uso exclusivo de IPv6 en el interfaz Wi-Fi de Android, y evitar los problemas conocidos mencionados, estableciendo una dirección IP fija para la red Wi-Fi igual a 0.0.0.0, el mismo valor que también debe ser asignado al *gateway* [Ref.- 56].

**Nota:** Las limitaciones del uso exclusivo de IPv6 en el interfaz Wi-Fi de Android están relacionadas también con problemas en el soporte para otras funcionalidades de IPv6:

- RFC3315 (DHCPv6): <https://code.google.com/p/android/issues/detail?id=32621>
- RFC6106 (RDNSS): <https://code.google.com/p/android/issues/detail?id=32629><sup>94</sup>

1585. Durante el proceso de inicialización de conectividad de datos, el dispositivo móvil Android genera peticiones IPv6 de solicitud de vecinos y de router mediante ICMPv6, empleando como dirección origen “fe80::6489:9aff:fe01:0203” (donde su dirección MAC es 64:89:9a:01:02:03), y añadiendo también su dirección MAC como dirección de enlace.

1586. La utilización de la dirección MAC en la dirección IPv6 sin hacer uso de las Privacy Extensions de IPv6 (RFC 4941) presenta problemas de seguridad y permite el seguimiento de los dispositivos móviles Android en Internet [Ref.- 54].

1587. Finalmente, Android 4.0 añadió soporte para las Privacy Extensions de IPv6, pero sin capacidades de configuración, ya que su utilización está configurada por defecto, pero no puede ser deshabilitada en caso de que sea necesario (aunque no recomendado desde el punto de vista de seguridad) [Ref.- 58].

1588. Adicionalmente, el dispositivo móvil Android envía periódicamente mensajes IPv6 de informes multicast (“Multicast Listener Report Message v2”).

1589. Se recomienda deshabilitar la disponibilidad de IPv6 en Android por completo, salvo que se vaya hacer uso de sus capacidades de comunicación, aunque esta opción no está disponible actualmente en la versión de Android analizada (salvo en dispositivos Android *rooteados*).

**Nota:** No se ha identificado ningún mecanismo, ni opción de configuración, en Android que permita deshabilitar o gestionar la pila de comunicaciones de IPv6.

## 19.6. REDES VPN

1590. Android, desde la versión 4.0 (Ice Cream Sandwich), proporciona soporte para las siguientes tecnologías y protocolos empleados por redes VPN (*Virtual Private Networks*, o redes privadas virtuales) [Ref.- 21]:

- PPTP: Point-to-Point Tunneling Protocol (TCP/1723).
- L2TP/IPSec: Layer Two Tunneling Protocol (L2TP; UDP/1701) en combinación con Internet Protocol Security (IPSec; protocolos IP 50 y 51 + IKE: UDP/500).
  - L2TP/IPSec PSK
  - L2TP/IPSec RSA
- IPSec: Internet Protocol Security (protocolos IP 50 y 51 + IKE: UDP/500).
  - IPSec Xauth PSK
  - IPSec Xauth RSA<sup>95</sup>

<sup>94</sup> Resuelto en Android 5.0 (Lollipop): <https://code.google.com/p/android/issues/detail?id=32630>

- IPSec Hybrid RSA<sup>96</sup>

1591. La opción recomendada desde el punto de vista de seguridad es hacer uso de redes VPN basadas en IPSec o L2TP/IPSec.
1592. Desde el punto de vista de seguridad no se recomienda hacer uso de redes VPN basadas en PPTP, ya que este protocolo hace uso de MSCHAPv2 para el proceso de autenticación, y éste es vulnerable a ataques de fuerza bruta con un 100% de éxito (representado por la totalidad de posibilidades asociadas a una clave DES, es decir,  $2^{56}$ )<sup>97</sup>.
1593. Adicionalmente, en el caso hacer uso de redes VPN basadas en L2TP/IPSec o IPSec, se debe definir el método de autenticación a emplear: certificados digitales (opción “RSA”) o clave precompartida (opción “PSK”, *Pre-Shared Key*).
1594. Se recomienda emplear certificados para la autenticación de L2TP/IPSec o IPSec al ser un mecanismo más seguro que el establecimiento de una clave precompartida (PSK) entre el servidor de VPN y el dispositivo móvil (que además es conocida por todos los usuarios de la red VPN y puede ser usada en ataques MitM<sup>98</sup>).
1595. En el caso de IPSec Xauth RSA tanto el cliente como el servidor se autentican inicialmente empleando certificados digitales durante la fase 1 de IKE (autenticación mutua). Posteriormente, el cliente se autentifica de nuevo mediante Xauth (ej. usuario y contraseña). En el caso de IPSec Hybrid RSA el cliente no se autentifica durante la fase 1 de IKE, sino que sólo verifica que está hablando con el servidor legítimo, lo que simplifica el despliegue de la solución VPN al no ser necesaria la emisión de certificados digitales cliente, pero constituye una solución más robusta que IPSec Xauth PSK. Posteriormente, de nuevo, el cliente se autentifica mediante Xauth (ej. usuario y contraseña).
1596. Desde el menú “Ajustes [Conexiones Inalámbricas y Redes] - Más... - VPN” es posible añadir una nueva red VPN a través del botón con el símbolo “+” de la parte superior:

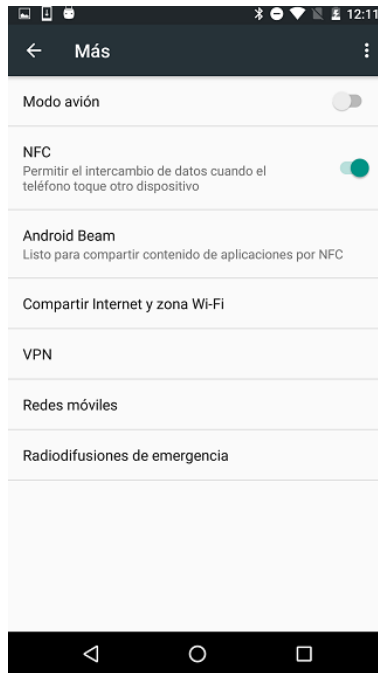
---

<sup>95</sup> <http://tools.ietf.org/html/draft-ietf-ipsec-isakmp-xauth>

<sup>96</sup> <http://tools.ietf.org/html/draft-ietf-ipsec-isakmp-hybrid-auth>

<sup>97</sup> <https://www.cloudcracker.com/dictionaries.html> (*servicio no disponible actualmente*).

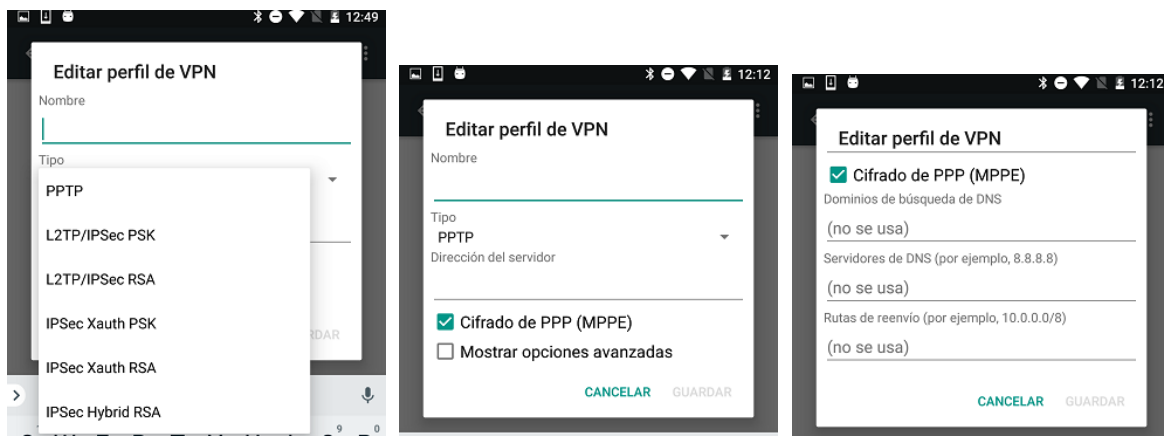
<sup>98</sup> [http://www.cisco.com/en/US/tech/tk583/tk372/technologies\\_security\\_notice09186a0080215981.html](http://www.cisco.com/en/US/tech/tk583/tk372/technologies_security_notice09186a0080215981.html)



1597. A través de las diferentes opciones disponibles asociadas al perfil de la red VPN es posible configurar todos los detalles de la conexión VPN. Una vez se han establecido las opciones de configuración según el tipo de red (descritas a continuación), mediante el botón “Guardar” es posible almacenar la nueva configuración.

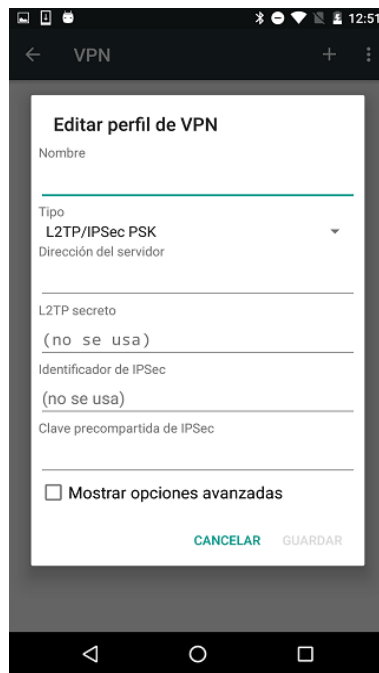
1598. Todas las redes VPN, basadas en PPTP, L2TP/IPSec e IPSec, requieren disponer del nombre de la red VPN, del tipo de red VPN y del nombre o dirección IP del servidor VPN.

1599. En el caso de redes PPTP, Android permite deshabilitar el cifrado mediante la opción “Encriptación de PPP (MPPE)”, que está habilitada por defecto. Se desaconseja deshabilitar este mecanismo de cifrado desde el punto de vista de seguridad:

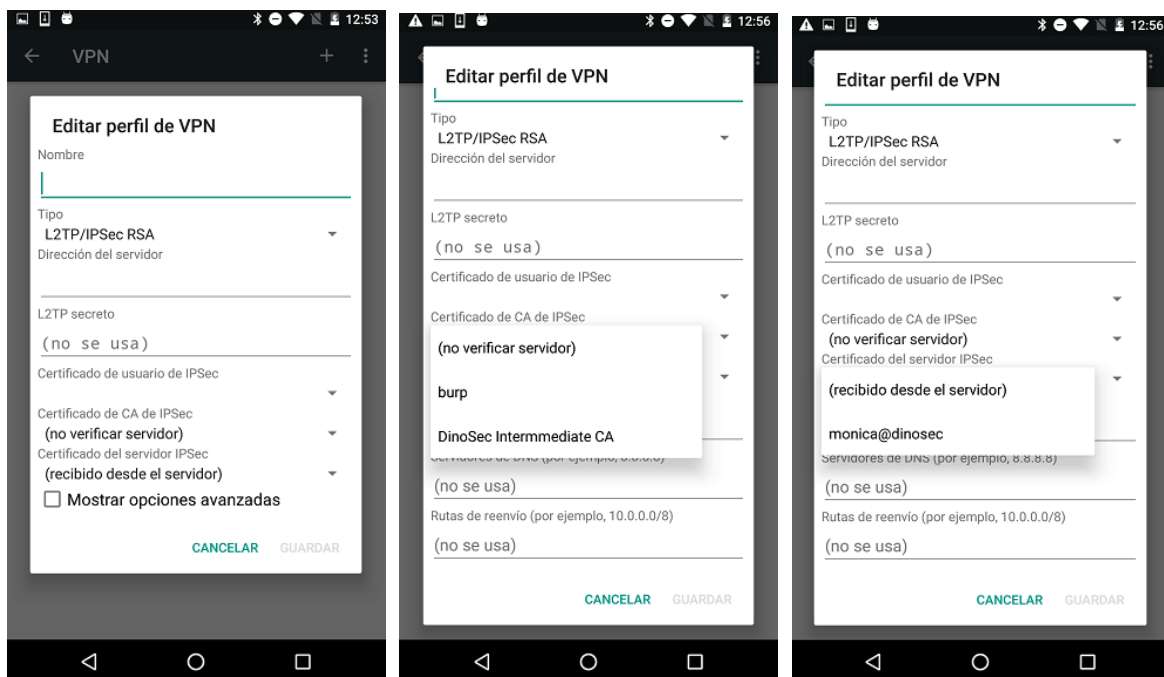


1600. La opción “Mostrar opciones avanzadas” permite especificar los dominios de búsqueda de DNS, los servidores DNS, y posibles rutas para el envío del tráfico de red, es decir, modificar elementos relacionados con la pila TCP/IP de Android y, en concreto, con la resolución de nombres (DNS) y la tabla de enrutamiento de Android, como se ilustra en la imagen superior derecha.

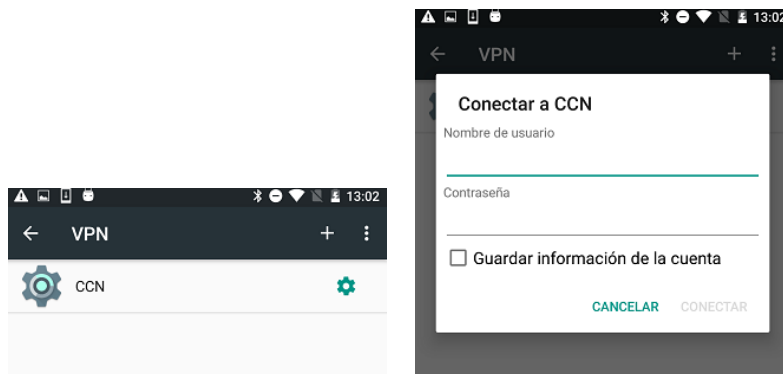
1601. En el caso de redes L2TP/IPSec PSK, y de redes IPSec Xauth PSK, Android permite establecer la clave precompartida para el acceso a la red:



1602. Tanto para redes L2TP/IPSec PSK como RSA, Android, en función del tipo de red VPN, también permite habilitar un secreto L2TP (deshabilitado por defecto), opción que facilita autenticar el propio túnel L2TP mediante un secreto compartido entre el cliente y el servidor (y que puede ser necesario en función de la configuración del servidor VPN).
1603. En el caso de redes L2TP/IPSec RSA, y de redes IPSec Xauth RSA, Android permite establecer el certificado digital cliente de usuario de IPSec, el certificado de la autoridad certificadora (CA) que ha emitido el certificado del servidor o concentrador VPN, y específicamente, el certificado digital del servidor o concentrador VPN (si no se especifica un certificado digital concreto, Android por defecto aceptará el certificado recibido al establecer la conexión, opción desaconsejada desde el punto de vista de seguridad):



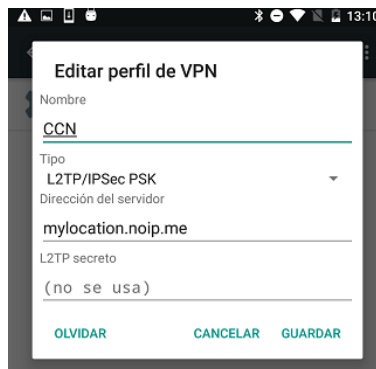
1604. Por defecto, Android no obliga a que la configuración de la red VPN basada en L2TP/IPSec RSA verifique el certificado de la CA que ha emitido el certificado del servidor o concentrador VPN.
1605. Esta es la opción desaconsejada desde el punto de vista de seguridad ya que, al no verificarse la CA, se permite que un potencial atacante suplante al servidor o concentrador VPN y se haga pasar por el servidor legítimo. En su lugar, siempre se debe seleccionar el certificado digital de la CA que está siendo empleado por la red VPN, y que debe haber sido importado previamente en el almacén de certificados de Android (ver apartado “11. Gestión de certificados digitales y credenciales”).
1606. El certificado digital cliente necesario para L2TP/IPSec es de tipo personal, y permitirá autenticar al dispositivo móvil y a su propietario. Adicionalmente, como se ha recomendado previamente, es necesario instalar un certificado raíz (perteneciente a la CA), y asociado a la generación del certificado digital empleado por el servidor de la red VPN.
1607. En el caso de redes L2TP/IPSec basadas en certificados digitales, al seleccionar el certificado cliente del usuario y de la CA, Android mostrará los certificados disponibles en el repositorio de credenciales, previamente importados (ver apartado “11. Gestión de certificados digitales y credenciales”).
1608. En el caso de redes IPSec Hybrid RSA se pueden definir los certificados de la CA y del servidor o concentrador VPN, pero no se hace uso de un certificado digital cliente ni de una clave precompartida (opciones Xauth previas).
1609. Una vez configurada la red VPN, es posible conectarse a la misma seleccionándola de la lista de redes disponibles desde la pantalla “Ajustes [Conexiones Inalámbricas y Redes] - Más... - VPN”, mediante una pulsación corta sobre la misma:



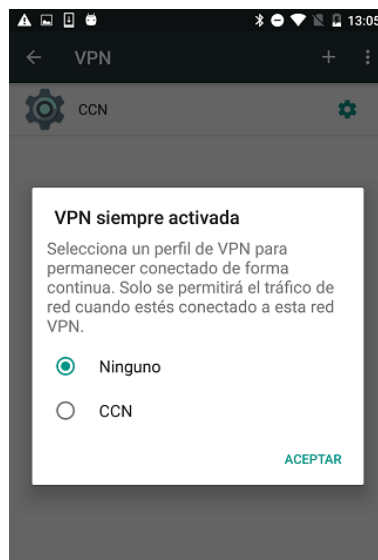
1610. Como resultado, Android solicitará al usuario las credenciales de acceso a la red VPN, es decir, el nombre de usuario y la contraseña para establecer la conexión con la red VPN seleccionada.
1611. Desde el punto de vista de seguridad se recomienda no seleccionar la opción “Guardar información de la cuenta”, ya que, en caso de hacerse, se almacenarán las credenciales de acceso a la red VPN en el dispositivo móvil. Es preferible que cada vez que se establezca una conexión con una red VPN sea necesario proporcionar tanto el usuario como la contraseña.
1612. En el caso de dispositivos móviles Android multi-usuario, únicamente el usuario propietario (o usuario principal) puede modificar la configuración de las redes VPN.



1613. Una vez establecida la conexión con la red VPN, Android restringe las comunicaciones para que todo el tráfico sea cursado a través de la red VPN hasta que el dispositivo móvil se desconecte de ella, es decir, no soporta *split horizon* (conexiones simultáneas directas hacia Internet y a través de la red VPN).
1614. Una vez se ha establecido la conexión con la red VPN, aparecerá un icono con forma de llave en la barra superior de estado y se añadirá una notificación al centro de notificaciones. Para desconectarse de la red VPN, el usuario sólo debe seleccionar dicha notificación, correspondiente a la red VPN activa.
1615. Mediante una pulsación prolongada corta sobre la entrada para la red VPN disponible desde “Ajustes [Conexiones Inalámbricas y Redes] - Más... - VPN”, es posible editar o eliminar el perfil de la red VPN a través del botón “Olvidar”:



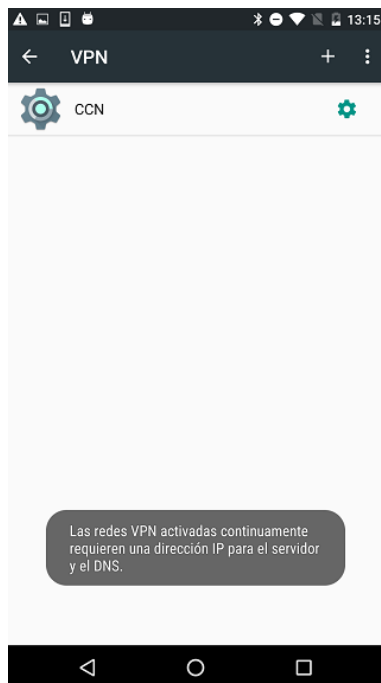
1616. Adicionalmente, si la red VPN lo permite, Android dispone de la posibilidad, a través del botón de menú disponible en la parte superior (“...”) y de la opción “VPN siempre activada”, de forzar que no sea posible cursar ningún tráfico de red (ni recibir, ni enviar) si la conexión a la red VPN no está establecida [Ref.- 21]:



1617. Esta es la opción recomendada desde el punto de vista de seguridad, ya que permite asegurar que no se enviará tráfico no cifrado y potencialmente sensible a través de la red, ya sea la red de datos de telefonía móvil 2/3/4G o una red Wi-Fi.
1618. Para poder hacer uso de esta funcionalidad, sí es necesario seleccionar la opción “Guardar información de la cuenta” (desaconsejada salvo que se haga uso de la conexión VPN siempre activa), con el objetivo de que el dispositivo móvil disponga en todo momento de las credenciales del usuario para el acceso a la red VPN y pueda

restablecer la conexión automáticamente en caso de ser necesario, como en el caso en que la conexión a la red (Wi-Fi o 2/3/4G) se haya interrumpido temporalmente.

1619. Adicionalmente, para poder hacer uso de esta funcionalidad, Android también requiere que se especifique una dirección IP (en lugar de un nombre) para el servidor o concentrador de la red VPN y para el servidor DNS:



1620. El modo “VPN siempre activada” puede ser desactivado a través de la opción “Ninguna”.

1621. Por último, Android no dispone de soporte nativo para redes VPN basadas en OpenVPN, siendo necesario instalar una app de terceros que actúe de cliente OpenVPN para este tipo de conexiones, como por ejemplo el cliente oficial de OpenVPN para Android disponible en Google Play<sup>99</sup>.

## 20. CUENTA DE USUARIO DE GOOGLE

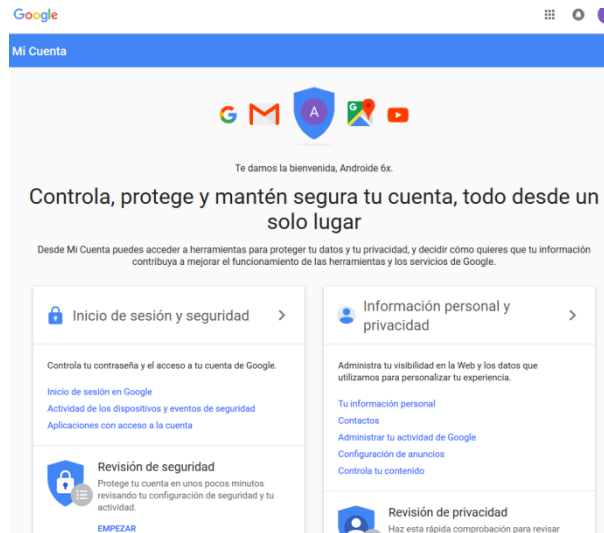
1622. Aunque de cara a la utilización de las capacidades de telefonía y conexiones de datos de un dispositivo móvil basado en Android se puede prescindir de la configuración de una cuenta de usuario de Google, si se pretende hacer uso de las apps de Google en Android, y de otros servicios adicionales de Google, es preciso dar de alta dicha cuenta en el dispositivo móvil. Así por ejemplo, para descargar aplicaciones de Google Play [Ref.- 4] (ver apartado “23.4. Apps de terceros: Google Play”), hacer copias de seguridad de los datos y la configuración en los servidores de Google (ver apartado “21.2. Copia de seguridad en los servidores de Google”) y otros servicios de Google como Gmail, Fotos, Maps, Contactos, Calendario, Drive, YouTube, etc., desde el dispositivo móvil es necesario iniciar sesión en la cuenta de usuario de Google.

1623. Los dispositivos Nexus 5x que vienen de fábrica con Android 6.x traerán integrados, entre otros, los siguientes servicios de Google: Gmail, Google+, Fotos, Maps, Contactos, Calendario, Keep, Drive, YouTube, Hangouts, etc.

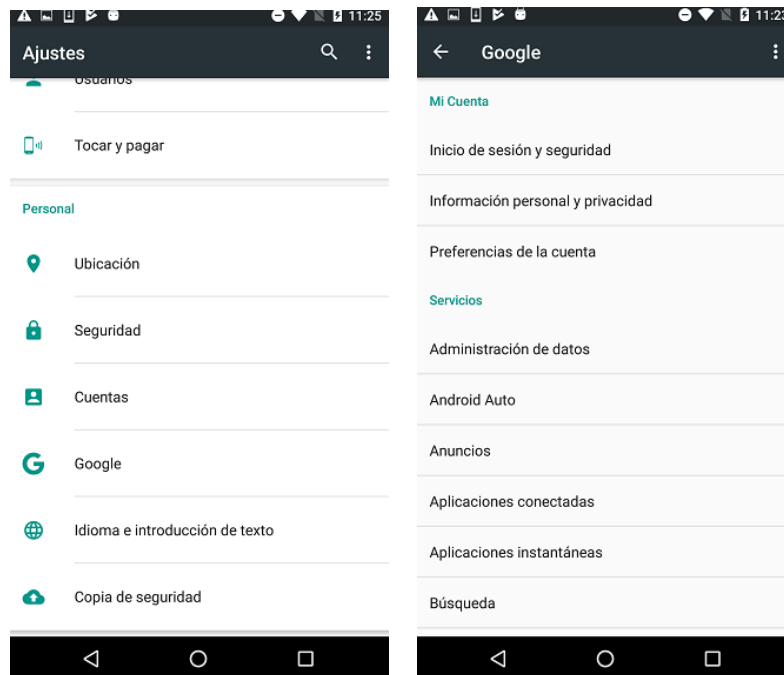
<sup>99</sup> <https://play.google.com/store/apps/details?id=net.openvpn.openvpn>

1624. La configuración de las opciones de la cuenta de usuario de Google puede realizarse a través de dos mecanismos:

- A través del portal web de Google “Mi cuenta” (<https://myaccount.google.com>).

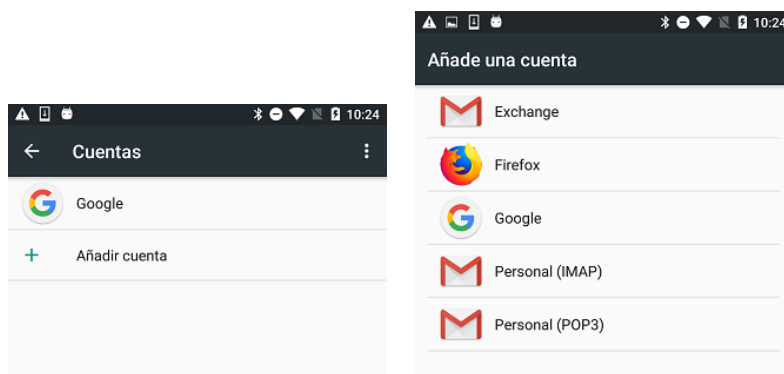


- En el propio dispositivo móvil: en versiones anteriores de Android (hasta la 5.x), la gestión de la cuenta de Google se llevaba a cabo a través de la app “Ajustes de Google”; en Android 6.x, los ajustes de Google dejan de existir como una app independiente y se integran en los ajustes generales del sistema, bajo el apartado “[Personal] - Google”. No obstante, algunos de estos ajustes finalmente acceden al interfaz web “Mi cuenta”, requiriendo para su modificación acceso a Internet:

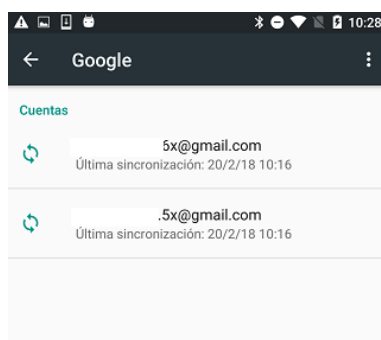


## 20.1. ASIGNACIÓN DE UNA CUENTA DE USUARIO DE GOOGLE AL DISPOSITIVO MÓVIL

1625. La configuración de una cuenta de usuario de Google ya existente y su vinculación al dispositivo móvil Android, o la creación de una nueva cuenta, puede llevarse a cabo mediante el proceso de de instalación y configuración inicial de Android 6.x (ver apartado “24. Apéndice A: Proceso de instalación y configuración inicial”).
1626. Asimismo, una vez el dispositivo móvil ha sido configurado, puede vincularse a una o varias cuentas de usuario de Google desde el menú “Ajustes [Cuentas]”.
1627. El botón “+ Añadir cuenta” permite por defecto añadir tanto una cuenta de usuario de Google como cuentas de usuario de distintos tipos, por ejemplo, de Microsoft Exchange, y cuentas de correo electrónico IMAP y POP3, siendo necesario proporcionar las credenciales de la cuenta existente, es decir, la dirección de correo electrónico del usuario y la contraseña (ver apartado “23.2. Correo electrónico (e-mail) y GMail”):

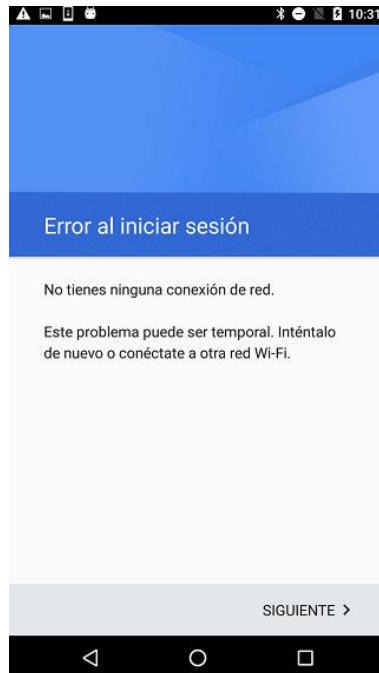


1628. La sincronización de las cuentas de Google es bidireccional, es decir, los cambios del dispositivo móvil se reflejarán en los servicios web de Google, y viceversa.
1629. Adicionalmente, una vez vinculada una cuenta de usuario de Google aparecerá en el menú “Ajustes - [Cuentas]” una nueva entrada denominada “Google”, que permite el acceso a los detalles de las cuentas de usuario de Google:

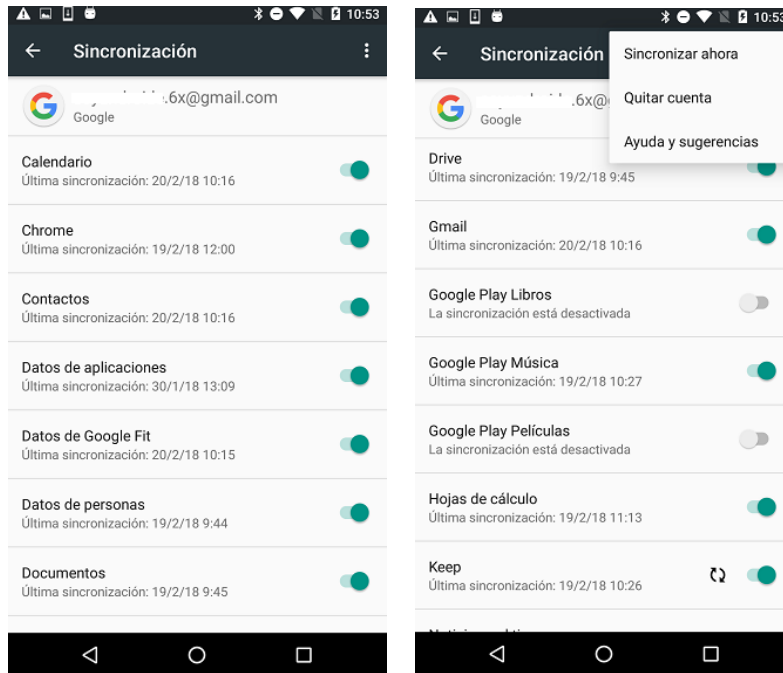


1630. En el caso de las cuentas de usuario de Google, es posible seleccionar si se añadirá una cuenta ya existente (para lo que se solicitarán las credenciales de acceso) o se creará una nueva cuenta.
1631. En versiones anteriores a Android 5.x, tanto el botón “Google”, como el botón “Añadir cuenta”, redirigían al usuario a la configuración del interfaz Wi-Fi y lo activaban (incluso aunque estuviera apagado previamente), con el objetivo de disponer de conexión a Internet y poder hacer uso de la cuenta de usuario de Google ya existente, o permitir la creación de una cuenta nueva. A partir de Android 5.x, si no hay conexión a

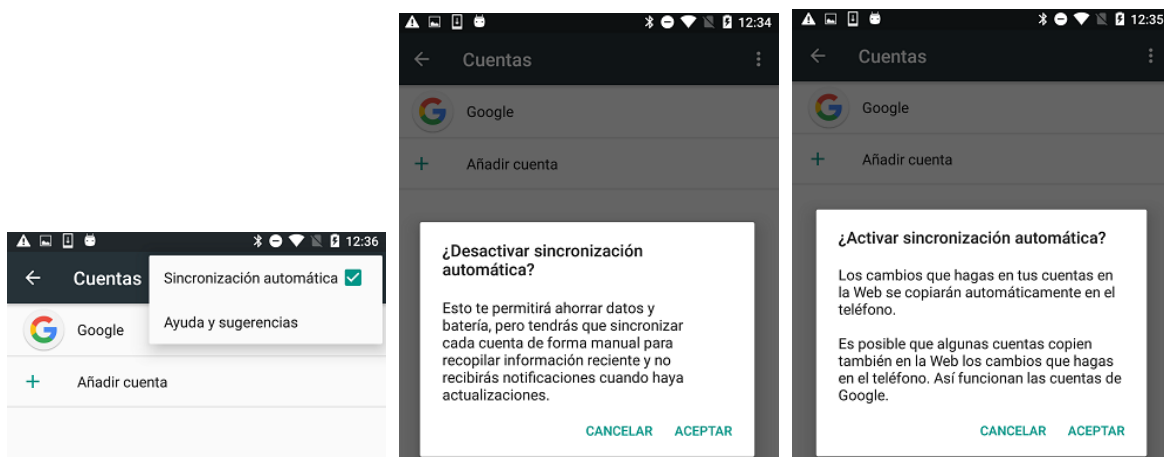
Internet (independientemente del motivo), se mostrará un mensaje informativo, pero no se activará ninguna conexión de datos de forma automática.



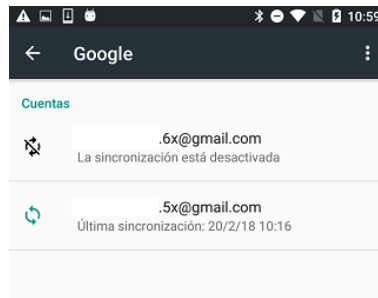
1632. Adicionalmente, para configurar y poder hacer uso de otros servicios críticos y relevantes en Android, como por ejemplo el acceso a Google Play y la instalación de apps de terceros (ver apartado “23.4. Apps de terceros: Google Play”), es también necesario disponer de una cuenta de usuario de Google.
1633. El proceso de vinculación de una cuenta de usuario de Google existente se lleva a cabo mediante una conexión HTTPS inicial con el servidor “www.googleapis.com” (entre otros). Durante el mismo se solicita confirmación por parte del usuario de los términos de uso y de configuración de datos de pago (paso que se puede omitir y que queda fuera del alcance de la presente guía).
1634. Desde el menú “Ajustes - [Personal] Cuentas - [Entrada asociada a la cuenta]” se puede definir qué servicios se sincronizarán con los servicios disponibles en la nube de Google. Desde el menú “[...]” de esa ventana, se puede asimismo lanzar una sincronización de datos o eliminar la cuenta del dispositivo.
1635. El resto de opciones de configuración de cada servicio se definen dentro de los ajustes de las apps que los proporcionan.



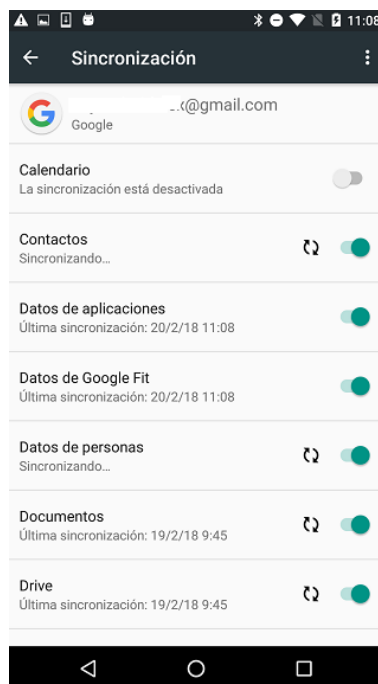
1636. En versiones anteriores a Android 5.x, durante el proceso de alta de la cuenta se solicitaba confirmación para actualizar a Google + y a otros servicios de Google.
1637. Una vez se ha vinculado una cuenta de usuario de Google con el dispositivo móvil, se realizará la sincronización de manera automática.
1638. Para desactivar completamente la sincronización automática, se debe marcar la opción “Ajustes - [Personal] Cuentas [...] Sincronización automática”. Si se desea volver a activar la sincronización, bastará con volver a marcar la opción correspondiente:



1639. También es posible desactivar la sincronización automática servicio a servicio, desmarcando uno a uno todos los interruptores de aquellos servicios que no se desee sincronizar.
1640. El icono compuesto por dos flechas circulares junto al nombre de la cuenta en la pantalla de cuentas de usuario informa sobre el estado de la sincronización automática. Si la sincronización está completamente desactivada, se mostrará en gris y tachado, y bajo el nombre de cuenta de usuario de Google aparecerá el mensaje “La sincronización está desactivada”. Si algún servicio tiene habilitada la sincronización, el icono asociado a la cuenta se mostrará con las flechas circulares en verde (indicando que tiene lugar algún tipo de sincronización de datos):



1641. A través del botón de menú superior es posible forzar la sincronización de todos los servicios, o elementos marcados para sincronizar en la cuenta, mediante la opción “Sincronizar ahora”. Se mostrará una pareja de flechas en los elementos cuya sincronización se esté produciendo en ese momento:



1642. A través del botón de menú superior es posible eliminar la cuenta de usuario del dispositivo móvil, mediante la opción “Quitar cuenta”.

1643. La sincronización de la información de los diferentes servicios de Google en Android 6.x se realiza mediante conexiones HTTPS cifradas<sup>100</sup> [Ref.- 111].

1644. Las opciones de sincronización de la cuenta de usuario de Google permiten establecer qué tipo de datos e información, y por tanto servicios, serán sincronizados entre el dispositivo móvil y Google, y en concreto, en la cuenta de usuario vinculada al mismo (ver imágenes superiores).

1645. Los servicios incluidos para su sincronización en Android 6.x incluyen el calendario, el navegador web Chrome, los contactos, los datos de las apps, datos de Google Fit, Drive, Fotos (de Google+), Gmail, Google Play (incluyendo los libros, el kiosco, la música, y las películas) e información sobre las personas (entre otros).

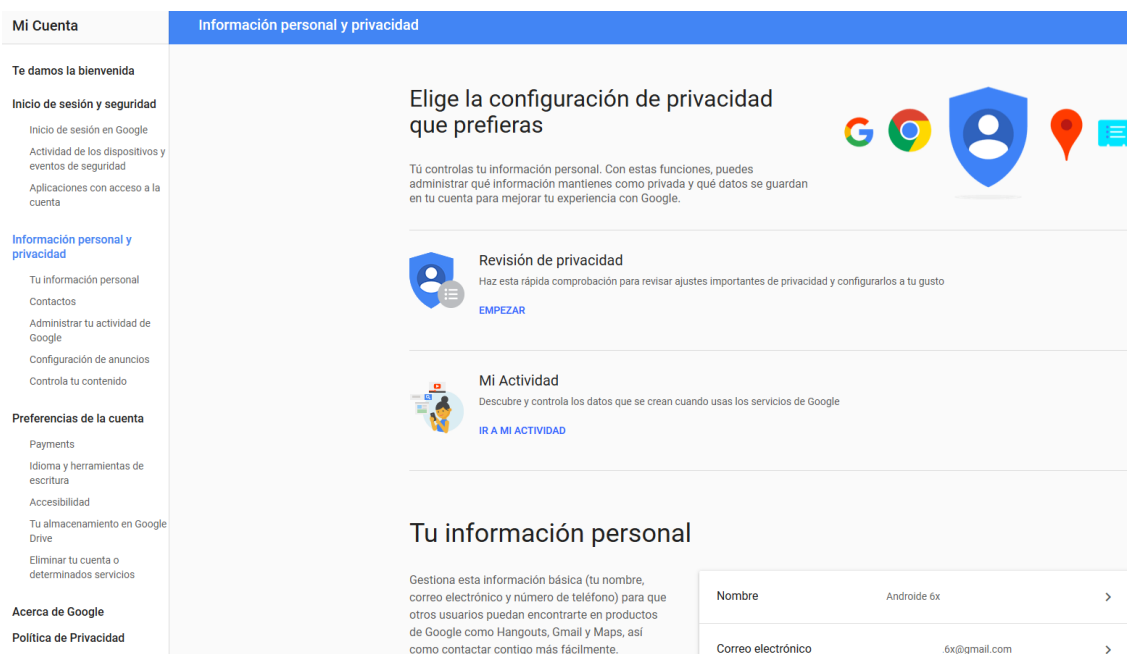
1646. Desde el punto de vista de seguridad se recomienda deshabilitar todos y cada uno de los servicios de los que el usuario no esté haciendo uso y/o para los que no se desea

<sup>100</sup> En versiones previas de Android, 2.x, algunos servicios de Google empleaban tráfico HTTP sin cifrar.



hacer un uso explícito de la sincronización desmarcando la casilla correspondiente de la parte derecha.

1647. Al deshabilitar la sincronización de cada opción o servicio, los datos asociados no serán eliminados del dispositivo móvil. Los datos sólo pueden borrarse eliminando la cuenta.
1648. En el momento de elaboración de la presente guía, el interfaz web que Google pone a disposición de los usuarios para gestionar las diversas opciones de configuración de la cuenta de Google están accesibles desde “https://myaccount.google.com”.
1649. Dicho interfaz contiene diversos apartados que permiten configurar multitud de opciones, servicios adicionales, información general, etc., relativos a la cuenta del usuario. A fecha de elaboración de la presente guía, el aspecto de este interfaz web es el que se ilustra en la imagen inferior, mostrándose a la izquierda del mismo los diferentes apartados disponibles en este momento:



1650. Dado que tanto las opciones disponibles, como la apariencia del interfaz web, dependen de múltiples factores, se han de tomar como orientativas las explicaciones relativas a los mismos que se detallan en la presente guía, debiendo consultar la última documentación disponible en la web de Google para realizar la configuración necesaria en el futuro.

## 20.2. SINGLE SIGN-ON: AUTENTICACIÓN DE USUARIOS DE DISPOSITIVOS MÓVILES EN SERVICIOS Y APPS

1651. Con la expansión de las plataformas móviles y la ampliación de los servicios que se hospedan y proporcionan desde la nube, la verificación de la identidad del usuario se desveló como un problema de seguridad relevante. Cada día surgen nuevas apps y servicios que requieren de un mecanismo de autenticación y protección de la identidad del usuario.
1652. Este hecho lleva asociada otra problemática: la complejidad que supone para el usuario recordar y definir multitud de credenciales para los diferentes servicios, aplicaciones corporativas y otras apps a las que se accede desde el dispositivo móvil.

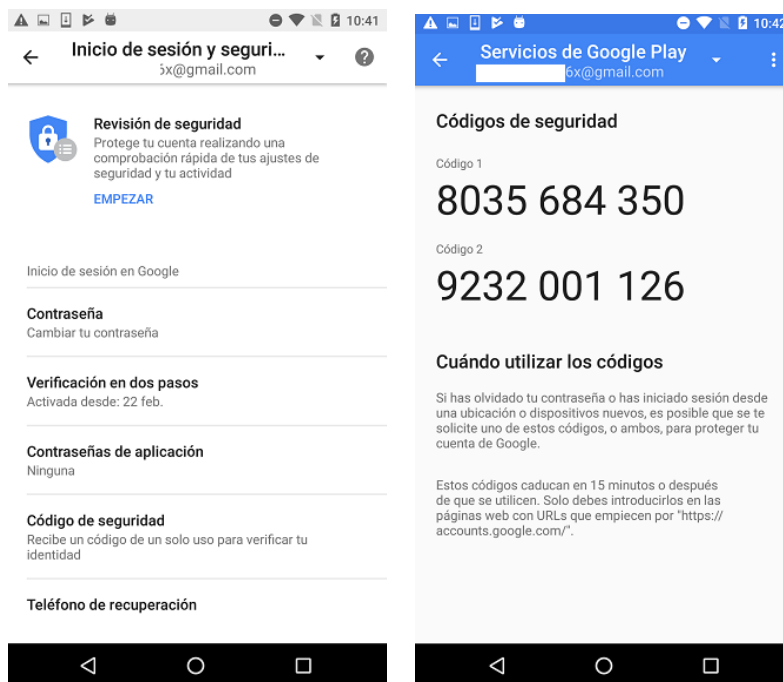
1653. Aunando ambas problemáticas surgió el concepto de “Single Sign-On” (SSO) dentro del mundo Android, que pretende simplificar la situación descrita. Por un lado, SSO delega la gestión de identidad en un servicio de un tercero de confianza, el cual implementa los mecanismos de autenticación y protección de identidad de forma segura, tanto para el usuario como para el proveedor del servicio y, por otro, permite al usuario no tener que dar de alta y recordar nuevas credenciales por cada servicio al que accede.
1654. Llevado al extremo, un ejemplo particular de SSO es el mecanismo de validación de credenciales a través de huella digital que soportan multitud de aplicaciones móviles de banca, delegando el proceso de autenticación parcialmente en un mecanismo propio del dispositivo móvil y su sistema operativo.
1655. En el pasado (hasta abril de 2012), el protocolo de autenticación ClientLogin era empleado por las apps de Android que interactúan con los servicios y APIs de Google para obtener un *token* de autenticación (“authToken”), mediante el envío de las credenciales válidas (usuario y contraseña) de una cuenta de usuario de Google a través de HTTPS. El “authToken”, denominado “auth”, era intercambiado a través de la cabecera “Authorization: GoogleLogin auth=...” de HTTP.
1656. El “authToken” era empleado para el acceso a las interfaces (o APIs) de los servicios de Google, de forma similar al uso de sesiones mediante cookies en aplicaciones web, y su valor era válido durante (como máximo) dos semanas (14 días) [Ref.- 113] [Ref.- 114].
1657. Posteriormente, ClientLogin fue reemplazado por OAuth 2.0 [Ref.- 115] [Ref.- 259], mecanismo de autenticación y autorización que también permite a las apps de Android interactuar con los servicios web y APIs de Google (y de otros proveedores). Con el protocolo OAuth 2.0, el desarrollador de una app debe seguir los siguientes pasos:
- Obtener credenciales OAuth 2.0 de la “Google API console”: un “client ID” y/o un “client secret” (éste último se requiere para un servidor web de aplicaciones) que sólo son conocidos para Google y para la app.
  - Obtener un “Access token” del “Google Authorization Server”: dicho token es necesario para obtener acceso a la API de Google; el token tendrá asociado un ámbito (scope) que determina el conjunto de recursos y operaciones a las que puede dar acceso (por ejemplo, un token emitido para la API de Google+ no permite acceder a la API de Contactos de Google). Los tokens tienen una validez limitada en el tiempo.
  - Enviar el token de acceso a la API de Google a través de una cabecera de autorización HTTP, empleando HTTPS.
1658. El mecanismo “Firebase Authentication” [Ref.- 258], desarrollado por Google, permite a una app conocer (y validar) la identidad del usuario a través de mecanismos como contraseñas, número de teléfono o proveedores de identidad federados (entre los que se encuentran Google, Facebook y Twitter). Con este mecanismo, la cuenta de usuario de Google se convierte en un medio para autenticar al usuario también en la app, lo que facilita a los desarrolladores la programación de su app, al no tener que preocuparse de la implementación de gestión de identidades.
1659. El servicio “Google Sign-In” se basa en permitir al usuario la validación ante un servicio o una app a través de su cuenta de usuario de Google. Las apps que soportan “Google Sign-in” pueden acceder al perfil, email y OpenID del usuario. Un ejemplo típico

de uso de este escenario son las apps que ejecutan en un *smartwatch* en modo *standalone*, es decir, sin la necesidad de una aplicación gemela (con funcionalidad específica) que ejecute en el dispositivo móvil asociado.

1660. Con la aceptación de la cuenta de usuario de Google como medio (casi) universal de autenticación, no sólo para acceder a servicios “básicos” del dispositivo móvil, sino a otra multitud de servicios tanto de Google como de terceros o corporativos, la protección de la cuenta de usuario de Google se convierte irremediablemente en un elemento crítico.

### 20.3. INICIO DE SESIÓN Y SEGURIDAD: VERIFICACIÓN EN DOS PASOS

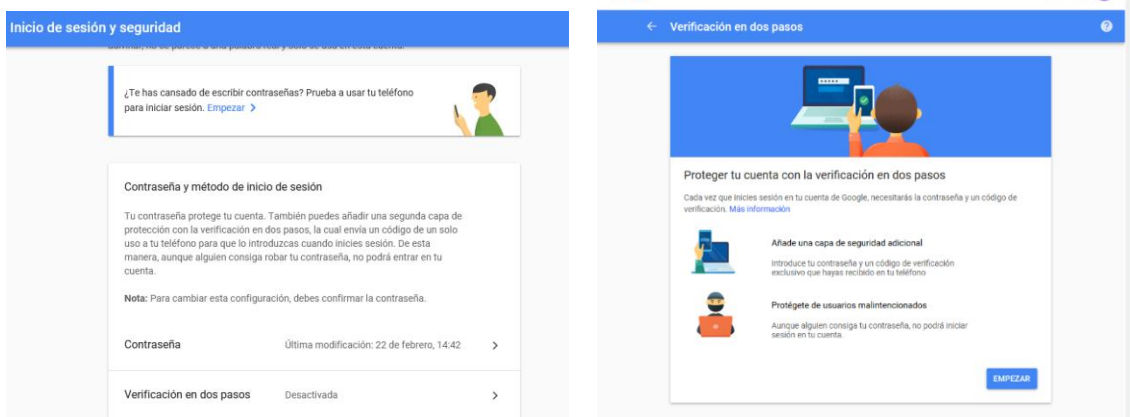
1661. Por defecto, el acceso a la cuenta de usuario de Google nada más crearse se lleva a cabo a través de un proceso de autenticación basado únicamente en usuario/contraseña.
1662. El olvido de la contraseña, o la sospecha por parte de Google de que la misma puede estar siendo utilizada por un tercero no autorizado (por ejemplo, cuando se accede desde un dispositivo nuevo), puede llevar a que se solicite al usuario un código de verificación. Este código, denominado “de seguridad”, se puede obtener a través de “Ajustes - [Personal] Google - [Mi cuenta] - [Inicio de sesión y seguridad] - Código de seguridad”. Si el dispositivo móvil tiene configurado un método o código de acceso, se solicitará al usuario su introducción previa.



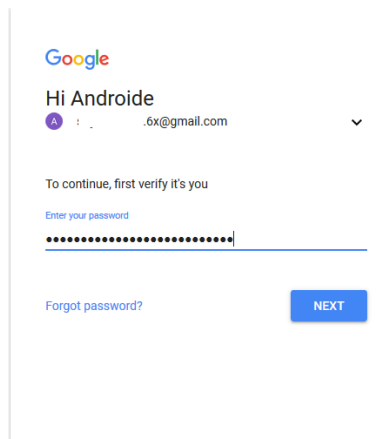
1663. La pantalla mostrará dos códigos, que tienen 15 minutos de validez y varían con cada invocación de esta opción.
1664. En Android 5.x, las opciones asociadas al inicio de sesión y seguridad de la cuenta de usuario de Google se encontraba en “Ajustes - [Personal] Cuentas - Google - Inicio de sesión y seguridad”. En Android 6.x, se encuentra en “Ajustes - [Personal] Google - [Mi cuenta] - Inicio de sesión y seguridad”.
1665. Este menú ofrece información de las cuentas de Google que tienen establecida sesión en el dispositivo móvil, e incluyen un resumen de todas las opciones de seguridad

asociadas a dichas cuentas. Cualquier modificación que se desee realizar conlleva un acceso a “https://myaccount.google.com”, es decir, no se efectúa localmente en el dispositivo móvil y requiere disponer de acceso a Internet.

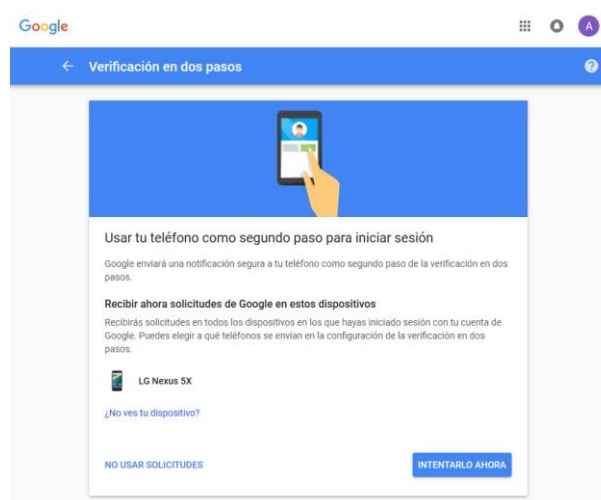
1666. Para incrementar la protección de la cuenta de usuario, Google introdujo en 2016 la posibilidad de iniciar sesión en la cuenta de Google del usuario utilizando su dispositivo móvil, en lugar de la contraseña asociada a la cuenta de usuario.
1667. Si el servicio está activo, Google enviará una notificación al dispositivo que, al ser seleccionada y aceptada por el usuario, permitirá el inicio de sesión.
1668. Este mecanismo, denominado “Verificación en dos pasos”, es más seguro que la utilización de sólo un usuario y su contraseña asociada [Ref.- 15] [Ref.- 20], y minimiza el riesgo que supone que la cuenta de Google pueda ser utilizada por un tercero.
1669. Este segundo factor de autenticación, cuando esté activo, se pondrá en marcha cuando el usuario intente iniciar sesión o realizar cualquier cambio en cualquiera de las opciones asociadas al “Inicio de sesión y seguridad” de su cuenta.
1670. Para poder hacer uso de este servicio, el dispositivo móvil tiene que estar registrado en la cuenta de Google del usuario, y, además, tener una versión actualizada de los servicios de Google Play (o *Google Play Services*, GPS).
1671. El mecanismo de verificación en dos pasos se gestiona desde el interfaz web disponible en “https://myaccount.google.com” y, más concretamente, bajo el recurso “https://myaccount.google.com/signinoptions/two-step-verification/enroll-welcome” [Ref.- 193]:



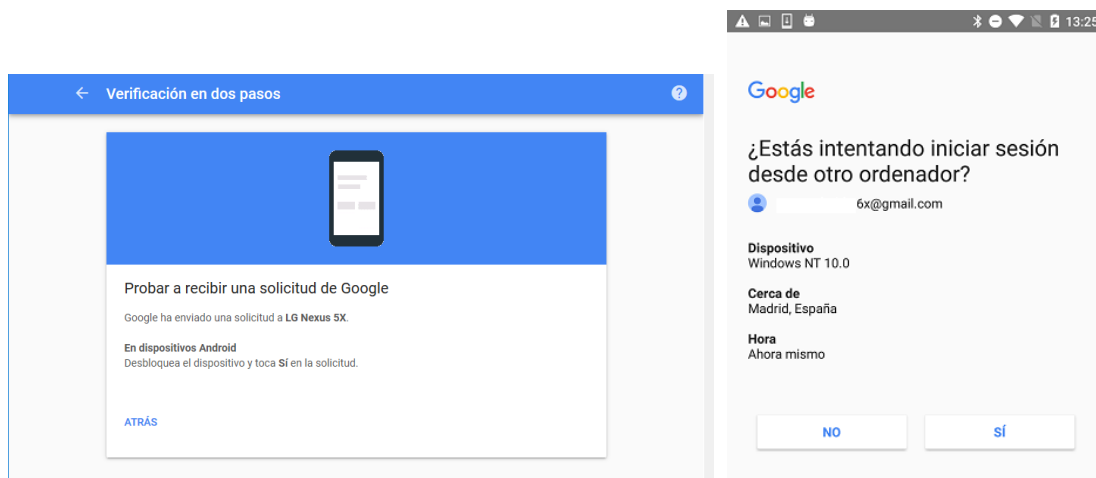
1672. Al pulsar sobre “Verificación en dos pasos” se mostrará la ventana superior derecha, que ofrece el botón “Empezar” para iniciar el proceso de configuración de este mecanismo, solicitando al usuario la contraseña asociada a la cuenta de Google:



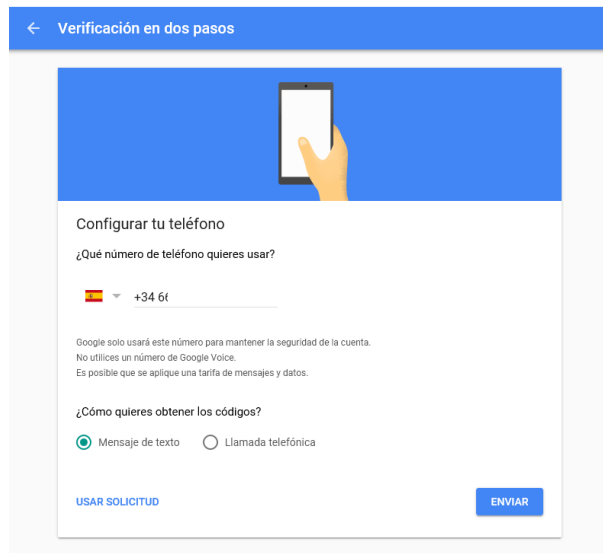
1673. El botón “Next” (o “Siguiente”) ofrecerá la pantalla “Usar tu teléfono como segundo paso para iniciar sesión”:



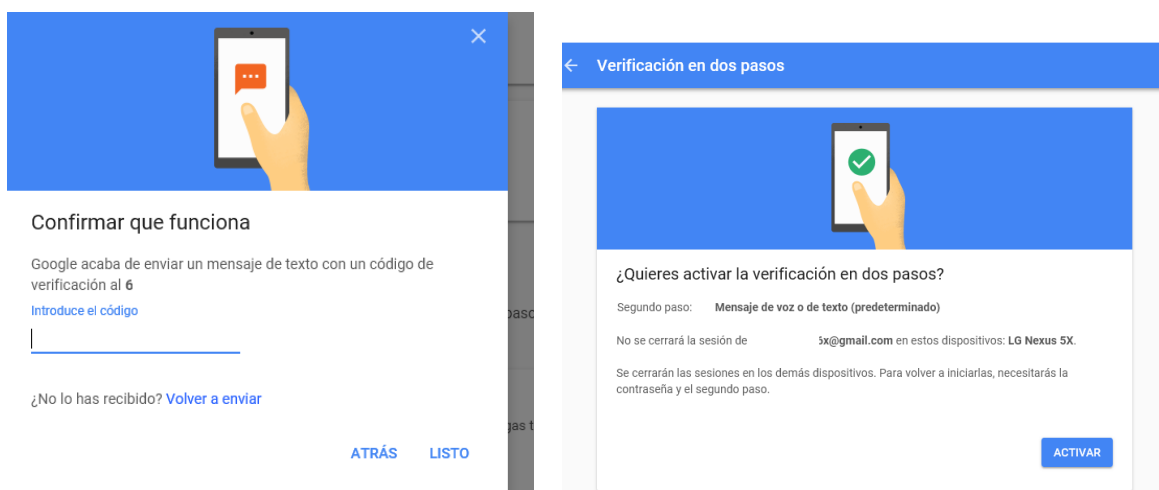
1674. Las dos opciones ofrecidas son: “No usar solicitudes” e “Intentarlo ahora”. La segunda opción se emplea si se desea que el segundo factor de autenticación se lleve a cabo mediante una solicitud que es enviada a través de la conexión de datos hacia Internet del dispositivo móvil, y que se enviará al dispositivo cada vez que se intente acceder a la cuenta de Google del usuario (la ventana inferior derecha muestra la solicitud recibida en el dispositivo móvil):



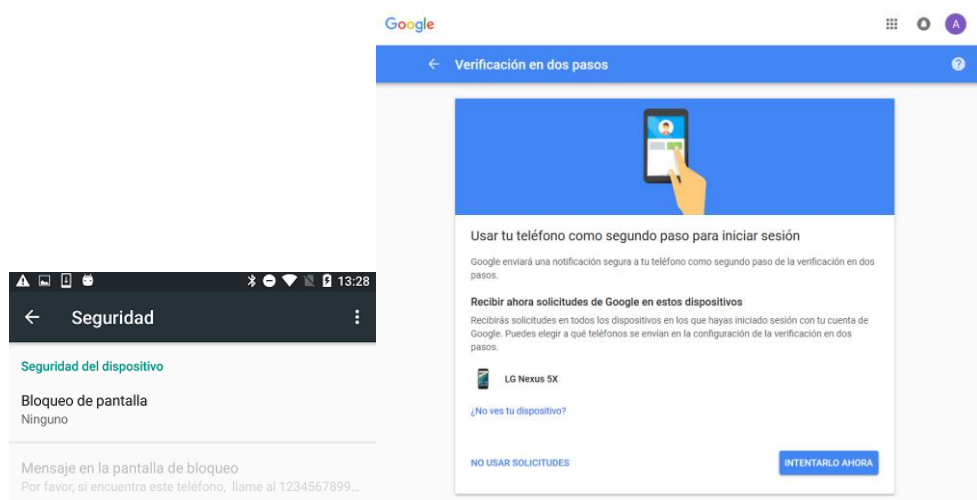
1675. En caso de que no se desee hacer uso de solicitudes, se deberá seleccionar la opción correspondiente, y el interfaz recurrirá entonces a emplear el número de teléfono que indique el usuario para establecer una llamada telefónica, o enviar un SMS, cuando se requiera hacer uso del segundo factor de autenticación:



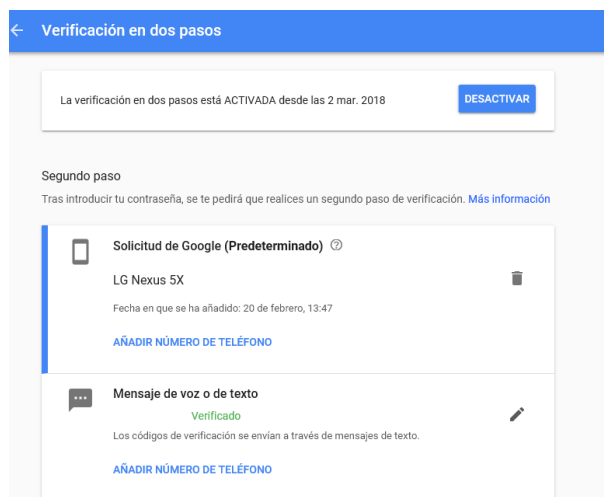
1676. Tras introducir el código recibido en el dispositivo móvil, se mostrará una ventana para confirmar la activación del número de teléfono como segundo factor de autenticación:



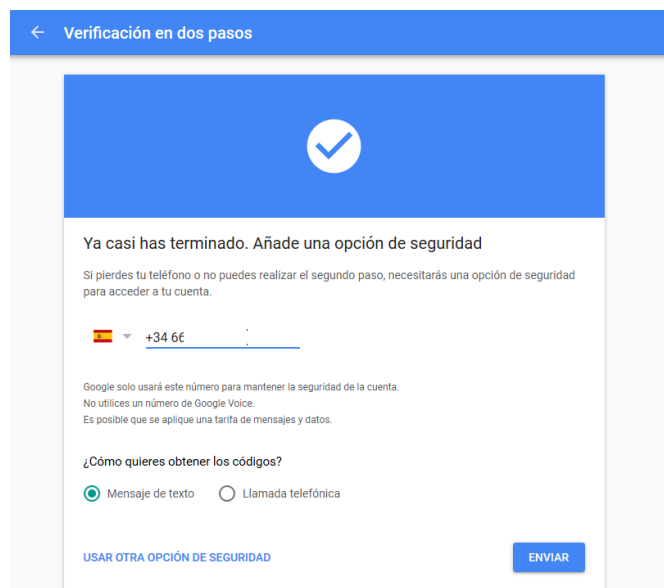
1677. Aunque en el pasado se requería disponer de un código de acceso establecido (a veces denominado bloqueo de pantalla) en el dispositivo móvil para poder llevar a cabo la configuración del segundo factor de autenticación, a fecha de elaboración de la presente guía Google lo plantea como recomendación, pero es posible activar el mecanismo sin que exista un método de bloqueo definido en el dispositivo móvil:



1678. Una vez completada la configuración del método de autenticación basado en solicitudes, las mismas se considerarán como el segundo factor predeterminado:

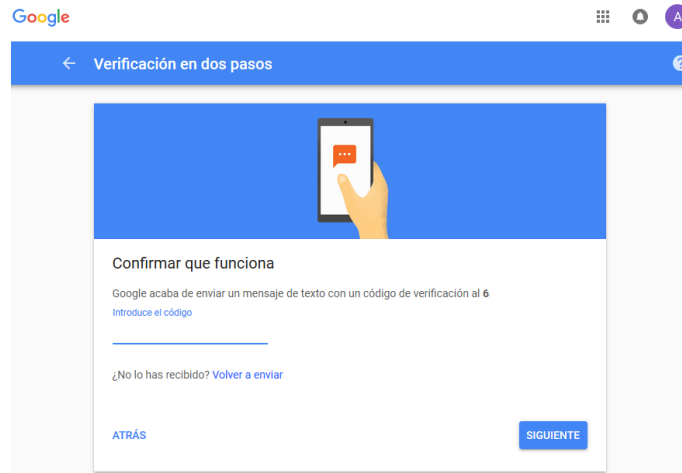


1679. Tras completar la configuración del uso de solicitudes, se ofrecerá la posibilidad de añadir un mecanismo de respaldo para el caso en que no se tenga acceso al dispositivo móvil en el momento de querer entrar en la cuenta de Google del usuario:





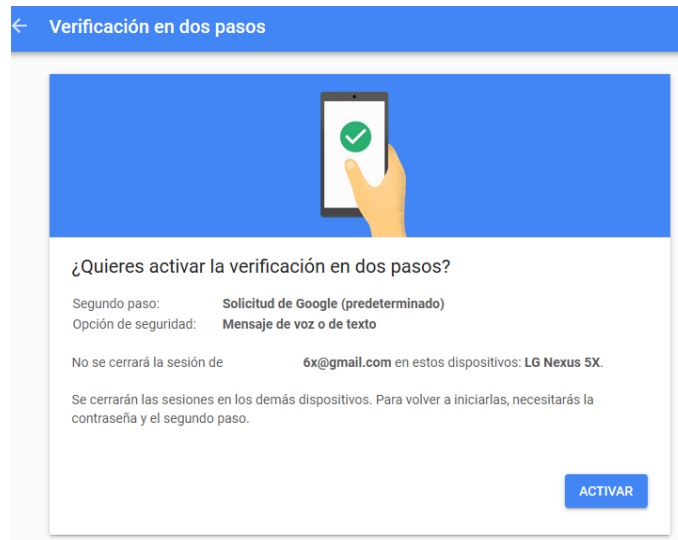
- En este menú, se dispone de las opciones:
  - “Enviar”: provocará que se envíe un SMS (o se realice una llamada de teléfono, en función de lo seleccionado) al número de teléfono indicado, debiéndose introducir el código recibido en el portal web para completar la configuración:



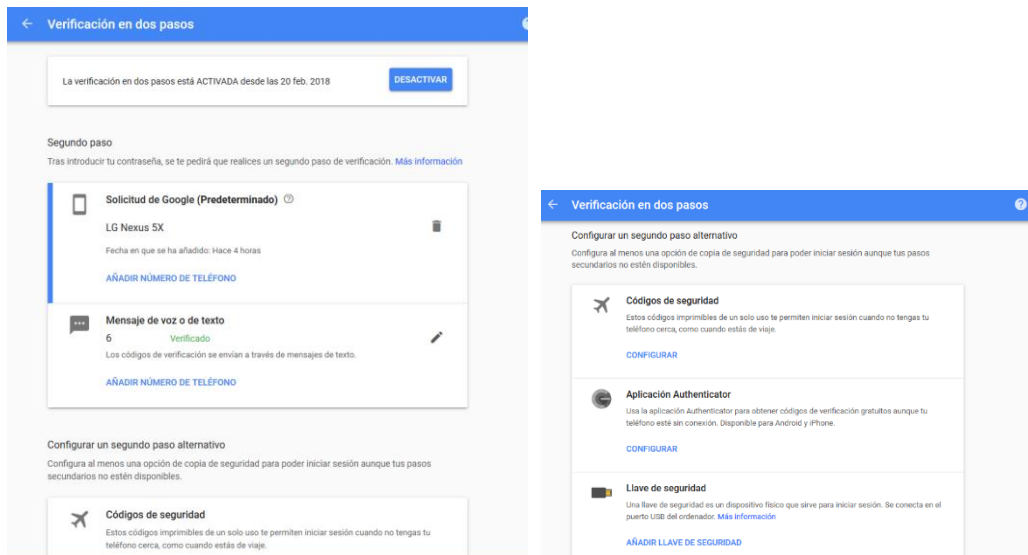
- “Usar otra opción de seguridad”: dado que el método descrito previamente requiere que el usuario disponga de servicio de telefonía móvil durante la configuración del proceso de verificación, se ofrece la alternativa de que el segundo factor sea una lista de códigos de verificación que el usuario podrá emplear si en algún momento debe iniciar sesión en su cuenta de Google y no dispone de servicios de telefonía o incluso de acceso físico al dispositivo móvil:



- Tras seleccionar el botón “Siguiente”, se mostrará el siguiente mensaje:

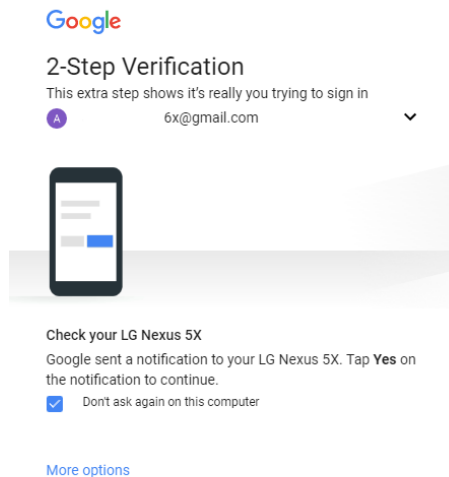


- Si se pulsa el botón “Activar” se formalizará la configuración y/o actualización del mecanismo de verificación en dos pasos y se presentará una ventana con la configuración seleccionada:

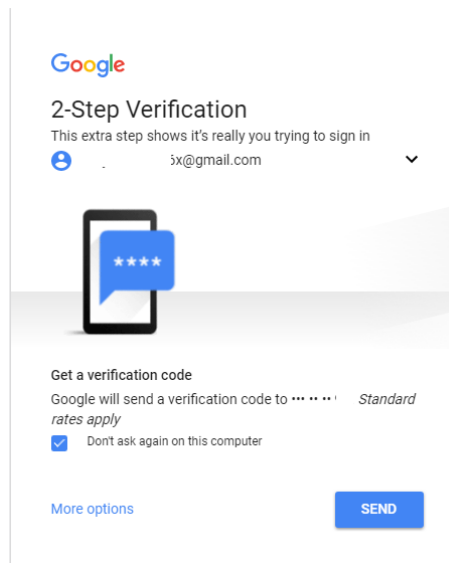


- Como se observa en la imagen superior derecha, existe la posibilidad de configurar como método de verificación alternativo los códigos generados por la aplicación Google Authenticator (descrita en el apartado “20.3.1. Google Authenticator”), y también lo que se denomina una “llave de seguridad” compatible con el estándar abierto “FIDO Universal 2nd Factor (U2F)” [Ref.-261]. La app Google Authenticator permite generar los códigos de seguridad en el dispositivo móvil aunque no se disponga de conexión a Internet, en base a una semilla y a referencias de tiempo. La llave de seguridad es un pequeño dispositivo hardware que se puede conectar a un ordenador a través de USB o al dispositivo móvil a través de Bluetooth Low Energy (BLE) (en ambos casos se requiere disponer de una versión actualizada del navegador Chrome, al menos versión 38 o superior) y que almacena y/o genera los códigos de seguridad de manera segura, por lo que el usuario no se debe preocupar de introducirlos. Este mecanismo queda fuera del alcance de la presente guía.

1680. A partir del momento en el que se ha completado el proceso de verificación en dos pasos mediante solicitudes, cada vez que se intente abrir sesión en la cuenta de usuario de Google en un dispositivo que no sea el propio móvil, se mostrará la siguiente ventana:



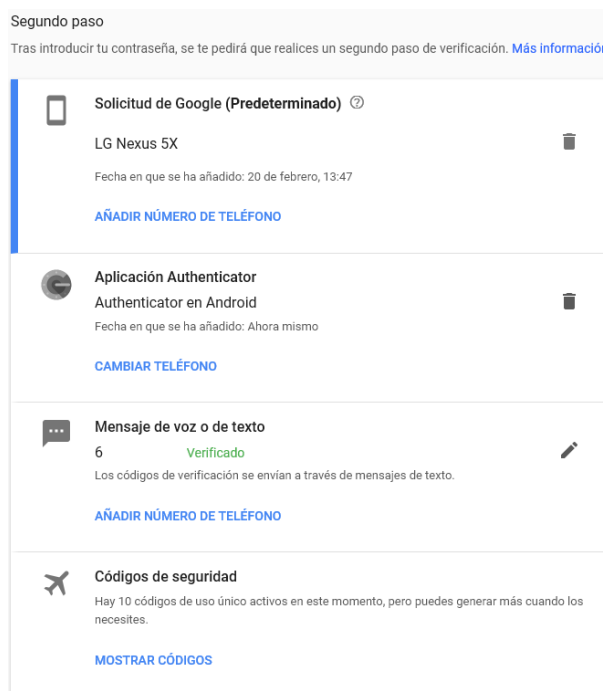
1681. Si los servidores de Google no pueden establecer comunicación con el dispositivo móvil en ese momento, intentarán completar la verificación utilizando el método de verificación alternativo previamente configurado:



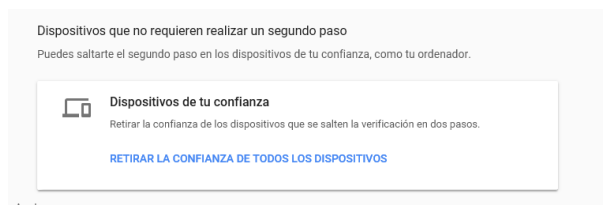
1682. Desde el punto de vista de seguridad, el introducir un segundo paso de verificación, o segundo factor de autenticación, para acceder a la cuenta de usuario de Google es altamente recomendable.

1683. Sin embargo, al no requerirse por parte de Google que el dispositivo móvil tenga definido un código de acceso ni que la pantalla esté bloqueada cuando se envía la solicitud de verificación, se debe ser muy cuidadoso y asegurarse de que se dispone de un método de bloqueo en el dispositivo móvil, para minimizar el riesgo que supondría que el dispositivo móvil pudiera ser utilizado por un tercero sin autorización y hacer uso de las notificaciones empleando el dispositivo móvil como segundo factor de autenticación.

1684. También se recomienda el uso de la app Google Authenticator, siempre teniendo definido un código de acceso en el dispositivo móvil en el que se vaya a emplear esta app, y que impida que un tercero pueda utilizarla. Asimismo, se recomienda evitar que, en el momento de su utilización, un tercero disponga de acceso visual a la pantalla de la app que le permita ver los códigos generados por ésta.
1685. La alternativa más segura corresponde a las llaves de seguridad (previamente mencionadas) que, al tener asociada una clave privada almacenada en un dispositivo hardware específico, con la que se cifran y/o generan los códigos de seguridad, y no requerir el envío de códigos que se puedan interceptar, protege potencialmente contra este tipo de ataques.
1686. Cuando el método asociado a un segundo factor de autenticación está activo, el menú mostrará todas las opciones habilitadas:



1687. El menú de “Verificación en dos pasos” también muestra la lista de dispositivos que el usuario ha designado como “Dispositivos de tu confianza”, que son aquellos para los que el acceso a la cuenta de Google del usuario no requerirá la introducción del código asociado al segundo factor de autenticación:



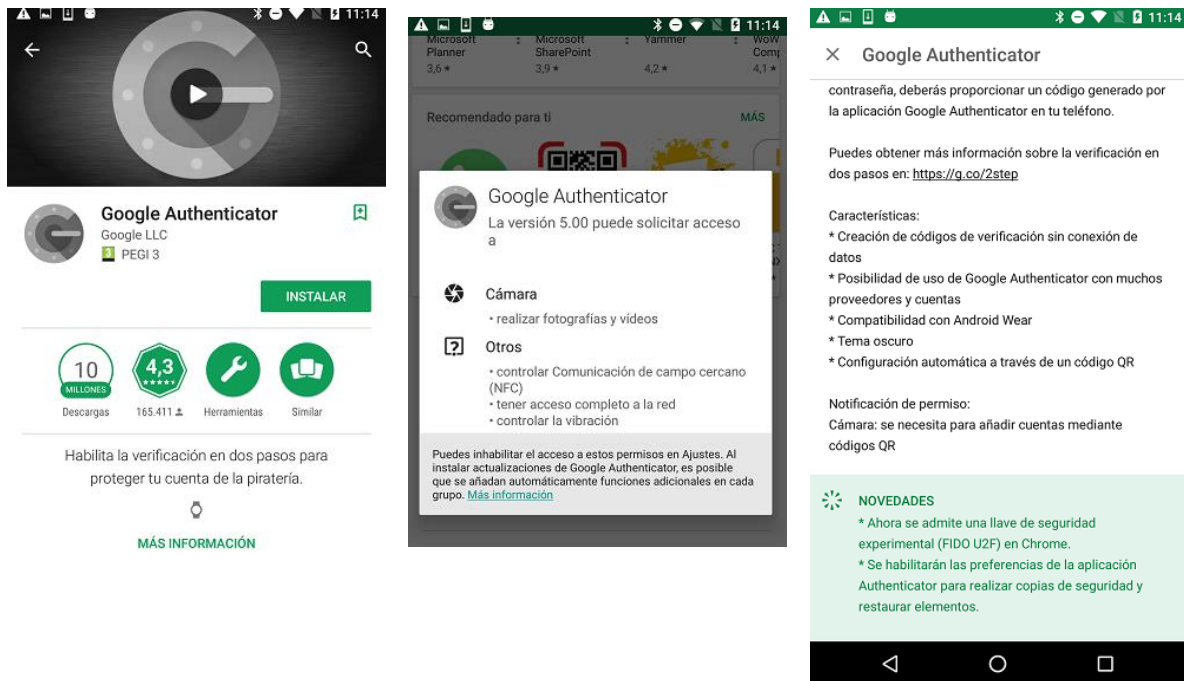
1688. Desde el punto de vista de seguridad, y aunque resulte menos cómodo tener que realizar dos pasos para completar el proceso de autenticación, se desaconseja disponer de servicios y cuentas de usuario en los que no se requiera el segundo factor, ante el riesgo que supondría que uno de ellos fuese utilizado por un tercero no autorizado.

### 20.3.1. GOOGLE AUTHENTICATOR

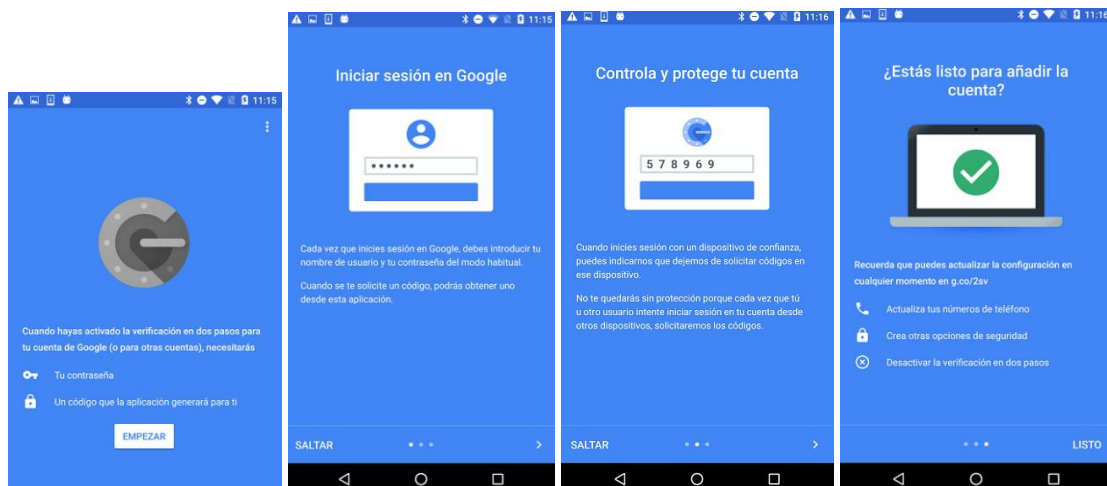
1689. En el año 2014 Google liberó la primera versión de su app Google Authenticator [Ref.- 14] [Ref.- 260].

1690. El objeto de la misma era complementar el uso de contraseñas personales con mecanismos de verificación de un solo uso (OTP, *One Time Password*), que eliminan el riesgo frente a los ataques de diccionario y/o fuerza bruta sobre la contraseña, y palían la amenaza asociada a que frecuentemente los usuarios reutilizan contraseñas, es decir, emplean las mismas (o muy parecidas) contraseñas para distintos servicios.

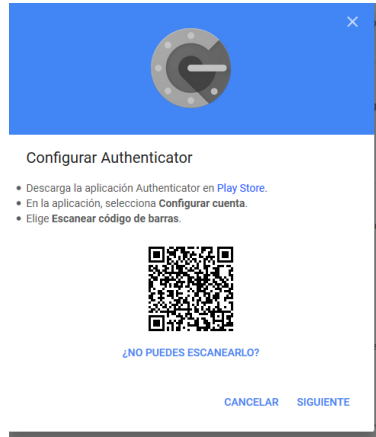
1691. A fecha de elaboración de la presente guía, la versión de la app Google Authenticator disponible en Google Play es la 5.0:



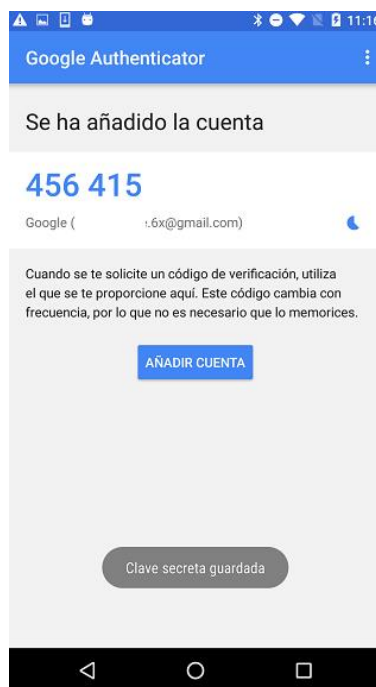
1692. Una vez instalada la app y tras ejecutarse por primera vez, se mostrará la pantalla inferior izquierda. Tras pulsar en “Empezar”, se lanzará un menú-tutorial que describe el propósito de la app:



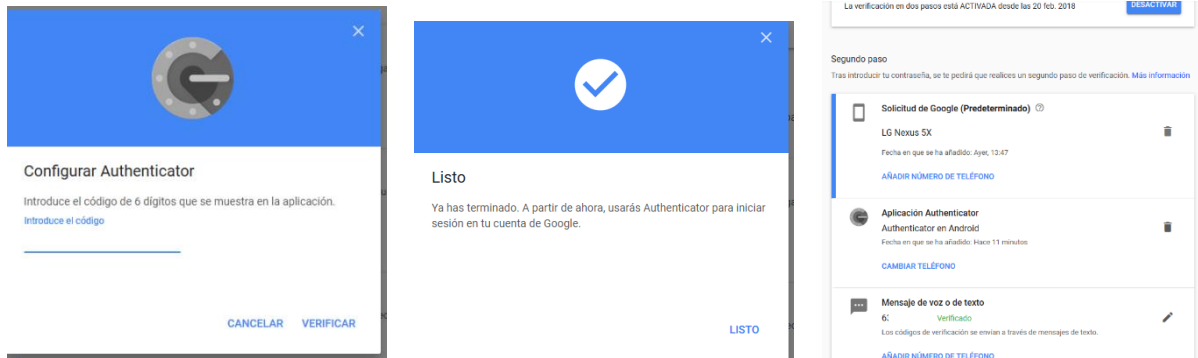
1693. El usuario deberá simultáneamente entrar en el menú de verificación en dos pasos de su cuenta de Google (a través de “https://myaccount.google.com/signinoptions/two-step-verification”) y seleccionar la opción “[Configurar un segundo paso alternativo] - Aplicación Authenticator”. Se mostrará la siguiente ventana que contendrá un código QR, el cual se deberá escanear desde la app Google Authenticator del dispositivo móvil:



1694. Para escanear el código QR desde la app Google Authenticator en el dispositivo móvil, se solicitará el permiso “fotos y vídeo”. Una vez concedido, se abrirá la app Cámara, desde la cual se encuadrará el código QR descrito anteriormente hasta que se muestre la siguiente ventana. En ella, se presentará un código de seis dígitos, el cual tendrá validez mientras se muestre en pantalla (el icono en forma de queso situado a la derecha representa la vida útil que le resta a dicho código):



1695. En el dispositivo móvil en el que se esté dando de alta el servicio mediante Google Authenticator, aparecerá la ventana que se ilustra a continuación, en la que se deberá introducir el código que muestra actualmente la app Google Authenticator. Tras pulsar “Verificar”, se completará la configuración de Google Authenticator como mecanismo para el segundo paso de verificación:



1696. En lo sucesivo, cuando se intente abrir sesión en la cuenta de Google del usuario, se podrá introducir el código mostrado por la app Google Authenticator como segundo factor de verificación.
1697. Tal como se indicó anteriormente, se recomienda utilizar Google Authenticator para añadir una capa extra de seguridad a la cuenta de usuario de Google, que además no requiere disponer de acceso a Internet desde el dispositivo móvil.

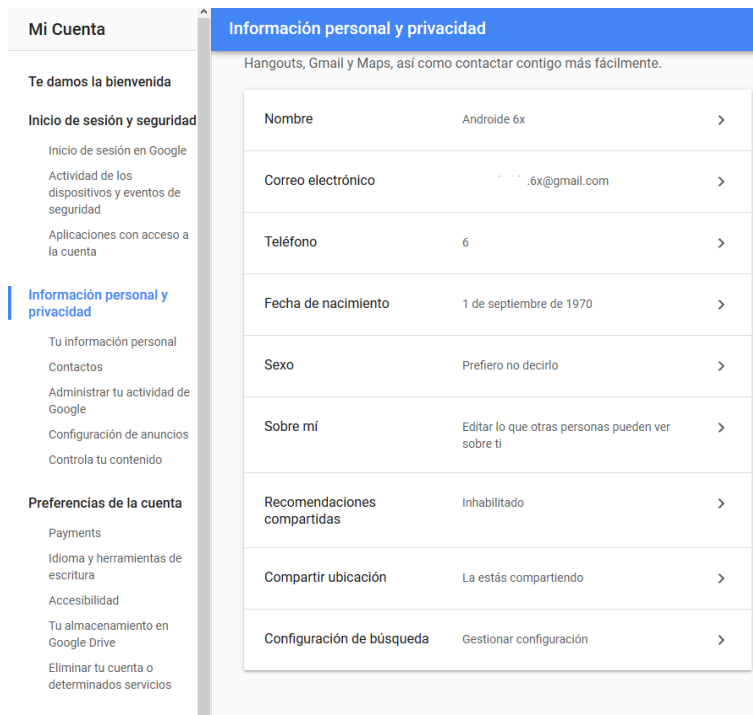
## 20.4. INFORMACIÓN PERSONAL Y PRIVACIDAD

1698. Bajo esta sección de configuración se pueden consultar y modificar elementos como los datos personales (el nombre, correo electrónico y número de teléfono) que se utilizan por los productos y servicios de Google, como Hangouts, Gmail y Maps para que otros usuarios puedan consultarlos, así como administrar la actividad de la cuenta de usuario y controlar su contenido.
1699. Desde el dispositivo móvil, el acceso a esta configuración está en “Ajustes - [Personal] Google - Información personal y privacidad”, que lanza el correspondiente menú del interfaz “Mi cuenta”.
1700. Debido a la extrema sensibilidad de estos datos, se recomienda minimizar en lo posible la información personal a la que dan acceso.

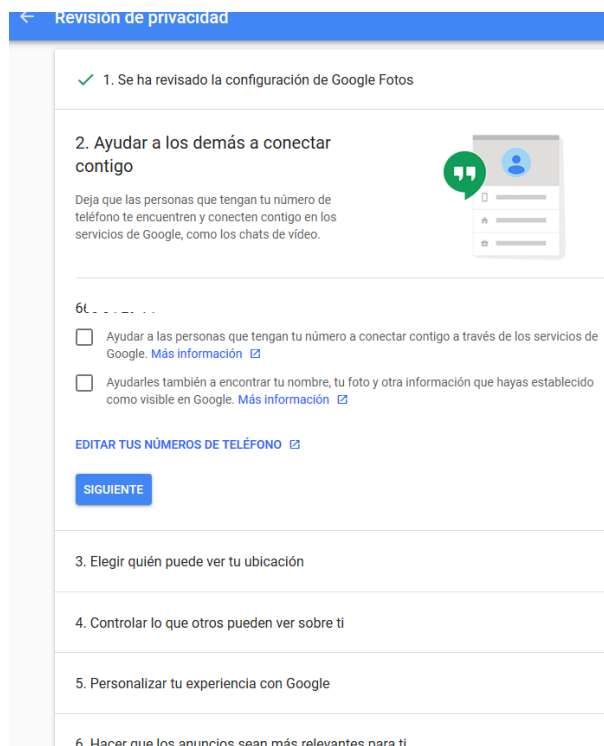
### 20.4.1. “TU INFORMACIÓN PERSONAL”

1701. Los parámetros definidos para la cuenta de usuario se pueden modificar seleccionándolos y a través del icono del lápiz de la página web que se abrirá. A fecha de elaboración de la presente guía, éstas son las opciones que se muestran, tanto desde el interfaz web como desde la pantalla de Android (dado que este servicio se modifica frecuentemente por parte de Google, algunas de las opciones pueden no corresponderse con las aquí descritas):





1702. La opción “Sobre mí” proporciona acceso al portal “<https://aboutme.google.com>”, desde el que se gestiona la información propia visible para otros usuarios de productos de Google. Concretamente, la subopción “Ir a la revisión de privacidad” despliega un menú con múltiples detalles personales, todos ellos editables:



- La opción “Elegir quién puede ver tu ubicación” muestra si se está compartiendo actualmente la ubicación con otros usuarios (ver apartado “12. Localización (o ubicación) geográfica”).
- La opción “Controlar lo que otros pueden ver sobre ti” permite editar los datos personales que serán accesibles por otros usuarios de servicios de Google y que, potencialmente, se pueden emplear en el contexto de recomendaciones

compartidas (es decir, lo que se publica cuando se emite un voto desde una aplicación de Google, incluyendo las que se publican como parte de los anuncios).

- La opción “Controles de la actividad de tu cuenta” se describe en el apartado “22.2. Cuentas y privacidad”.
- La opción “Hacer que los anuncios sean más relevantes para ti” se describe en el apartado “20.4.3. Anuncios”.

1703. Además, el interfaz “Información personal y privacidad” incluye el apartado “Contactos”, en el que se dispone de la opción “Usuarios bloqueados”: este apartado permite consultar si actualmente hay algún usuario cuya cuenta se desea bloquear para que no pueda interactuar con la cuenta propia utilizando los productos de Google, concretamente Google+, Hangouts, Fotos, YouTube y Maps [Ref.- 180]. El bloqueo de un usuario en uno de estos productos implica que su cuenta será bloqueada en todos ellos.

1704. No se incluyen en la lista anterior los usuarios que se han bloqueado a nivel de su cuenta de Google. Por ejemplo, es posible bloquear una dirección de correo en Gmail y un número de teléfono en el dispositivo móvil, pero estas acciones de bloqueo no se muestran en el apartado “Usuarios bloqueados”. Para más información sobre cómo bloquear números de teléfono, consultar el apartado “18.2. Configuración y selección de la red (voz) de telefonía móvil”.

1705. La opción “Administrar tu actividad de Google” se detalla en el apartado “20.4.2. Administrar tu actividad de Google”.

## 20.4.2. ADMINISTRAR TU ACTIVIDAD DE GOOGLE

1706. En esta sección se ofrecen las opciones relativas a cómo se almacena la actividad de la cuenta de Google del usuario:

Información personal y privacidad

### Administrar tu actividad de Google

Tienes muchas herramientas para revisar y controlar tu actividad en Google. Además, pueden ayudarte a decidir cómo mejorar el funcionamiento de los servicios de Google.

#### Controles de la actividad de tu cuenta

Indica a Google los tipos de datos que quieres guardar para mejorar tu experiencia con Google.

Controles de la actividad de tu cuenta

Tú controlas los datos que se guardan en tu cuenta de Google. Puedes activar estas funciones para que los servicios de Google te sean más útiles o detenerlas en cualquier momento.

[IR A CONTROLES DE LA ACTIVIDAD DE TU CUENTA](#)

#### Revisar tu actividad

Aquí puedes consultar y revisar fácilmente tu actividad de Google.

#### Mi Actividad

Redescubre lo que has buscado, lo que has leído y lo que has visto. Tú controlas estos datos y puedes eliminar elementos concretos o temas enteros.

[IR A MI ACTIVIDAD](#)

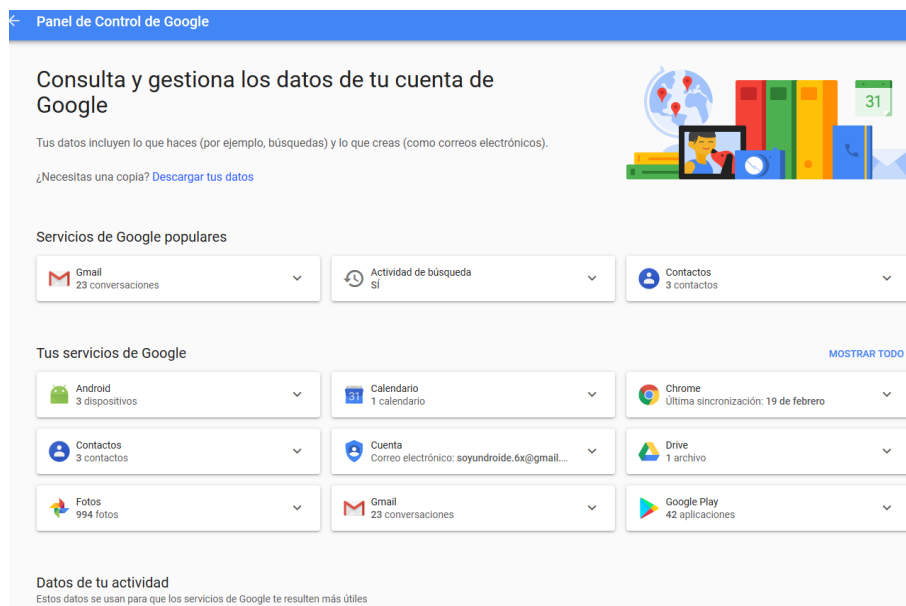
#### Cronología de Google Maps

Ver los sitios que has visitado >

#### Panel de Control de Google

- La opción “Controles de la actividad de tu cuenta” coincide con la descrita en el apartado “22.2. Cuentas y privacidad”.

- La opción “Revisar tu actividad” engloba las opciones “Mi actividad” (corresponde a la descrita en el apartado “23.1.3. Historial de actividad web y de aplicaciones”) y “Cronología de Google Maps” (descrita en el apartado “12.5. Historial de ubicaciones”).
- La opción “Panel de control de Google” ofrece a los usuarios individuales no asociados a un dominio de Google G-Suite (ver apartado “8. Gestión empresarial de dispositivos móviles basados en Android”) acceder a la administración de servicios de la cuenta de usuario, como el tipo de acceso, a través del Panel de Control de Google (o *dashboard*), disponible en “<https://myaccount.google.com/dashboard>”.



1707. Dentro de las opciones disponibles en el *dashboard* o panel de control de Google, se encuentra la gestión de la cuenta de usuario de Google, de los dispositivos móviles vinculados, de todos los servicios de Google (Audio, Calendario, sincronización de Chrome, Cloud Print, Contactos, Gmail, Google Fotos, Google+, histórico de ubicaciones, Play Store o Google Play, perfil, histórico de búsquedas, Talk, y YouTube), siendo posible acceder a todos los detalles de cada servicio, como por ejemplo, gestionar las apps instaladas desde Google Play (a través de un enlace directo a la cuenta de usuario de Google en Google Play: “<https://play.google.com/store/account?hl=es/>”), así como verificar los datos almacenados por Google para los dispositivos móviles vinculados a la cuenta. Estos datos incluyen, entre otros, para cada dispositivo móvil: el modelo, fabricante, operador de telefonía, fecha de registro, fecha de la última actividad, etc., así como una lista de las apps que almacenan una copia de seguridad de sus datos en los servidores de Google:

| Preferencias de correo electrónico                                                                                                                                                                                                         |                                                      |            |          |          |                         |                         |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|------------|----------|----------|-------------------------|-------------------------|
| <input type="checkbox"/> Recibir noticias y ofertas de Google Play<br><input checked="" type="checkbox"/> Quiero recibir notificaciones por correo electrónico cuando los desarrolladores respondan a mis opiniones sobre sus aplicaciones |                                                      |            |          |          |                         |                         |
| Mis dispositivos                                                                                                                                                                                                                           |                                                      |            |          |          |                         |                         |
| APODO                                                                                                                                                                                                                                      | VISIBILIDAD                                          | FABRICANTE | MODELO   | OPERADOR | ÚLTIMO USO              | REGISTRADO EL           |
|  Dispositivo sin nombre                                                                                                                                 | <input checked="" type="checkbox"/> Mostrar en menús | LGE        | Nexus 5X |          | 21 de febrero de 2018   | 21 de noviembre de 2017 |
|  Dispositivo sin nombre                                                                                                                                 | <input checked="" type="checkbox"/> Mostrar en menús | LGE        | Nexus 5X |          | 19 de noviembre de 2017 | 19 de julio de 2017     |
|  Dispositivo sin nombre                                                                                                                                 | <input checked="" type="checkbox"/> Mostrar en menús | LGE        | Nexus 5  |          | 5 de agosto de 2017     | 5 de agosto de 2017     |

### 20.4.3. ANUNCIOS

1708. La configuración de anuncios en Android 6.x no se puede gestionar desde el propio dispositivo móvil (al contrario de lo que sucedía en Android 5.x con la app “Ajustes de Google - [Servicios] Anuncios”).
1709. La única alternativa para gestionar, según las posibilidades que se ofrecen, los anuncios es recurrir a la interfaz web que es accesible desde el siguiente enlace, “<https://myaccount.google.com/privacy?hl=es#ads>”, “Administrar la configuración de anuncios”, que redirige a “<https://adssettings.google.com/authenticated>”.

**Personalización de Anuncios**

Haz que los anuncios que ves te resulten más útiles al usar:

- Los servicios de Google (por ejemplo, la Búsqueda y YouTube)
- Más de dos millones de sitios y aplicaciones que no son de Google y que colaboran con la multinacional para mostrarte anuncios
- ☒ Utiliza también la actividad y la información de tu cuenta de Google para personalizar los anuncios que se muestran en estos sitios web y aplicaciones, y guardar estos datos en tu cuenta de Google

¿Cuáles son los más de dos millones de sitios web y aplicaciones que colaboran con Google para mostrarte anuncios?

¿Qué información personal proporciona Google a los partners?

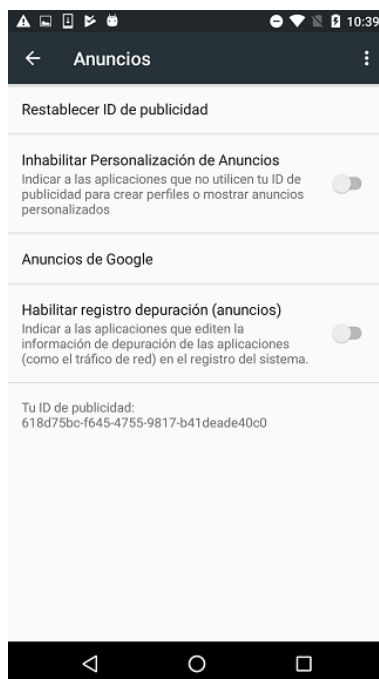
**TEMAS QUE TE GUSTAN** TEMAS QUE NO TE GUSTAN (0)

Quita los temas que no te gusten y añade los que sí para que te mostremos anuncios más útiles. También se añadirán temas a medida que vayas usando algunos servicios de Google (por ejemplo, cuando veas un video en YouTube). Estamos trabajando para incluir temas de otros servicios de Google.

|                                      |                         |                                     |
|--------------------------------------|-------------------------|-------------------------------------|
| Accesorios de Bluetooth              | Android OS              | Aplicaciones iOS                    |
| Aplicaciones web y herramientas o... | Automóviles y vehículos | Banca                               |
| BMW                                  | Coleccionismo deportivo | Comunidades online                  |
| Cupones y descuentos                 | Diseño y desarrollo web | Dispositivos móviles e inalámbricos |
| Empresas e industrias                | Fitness                 | Fútbol                              |
| Informática y electrónica            | Juegos                  | Juegos de cartas coleccionables     |

1710. Hay que recalcar que no es posible inhabilitar la presentación de anuncios, tal y como refleja la política de Google<sup>101</sup>, y que todos los parámetros que se definan afectarán únicamente al tipo de anuncio que se recibirá.
1711. En el caso de la configuración de anuncios, el usuario puede filtrar por temas, utilizar la actividad y la información de la cuenta de usuario de Google para personalizar los anuncios que se muestran en estos sitios web y aplicaciones, y guardar estos datos en la cuenta de Google. Esta opción (habilitada por defecto) no está recomendada desde el punto de vista de la privacidad, pues, aunque deshabilitarla hará que los anuncios mostrados sean más genéricos, y muy probablemente no del interés del usuario, evita que se haga un seguimiento del usuario en este tipo de servicios.
1712. La versión 4.x de los servicios de Google Play introdujo lo que se denomina “ID de publicidad”, un número aleatorio y único (supuestamente anónimo) que se generaba en el momento de la instalación inicial del dispositivo móvil, o cada vez que éste es restablecido a fábrica, y que se emplea por los servicios de anuncios, asociados a Google Play y a las apps de terceros, para hacer un seguimiento del usuario [Ref.- 186].
1713. La configuración del identificador (o ID) de publicidad se encuentra en “Ajustes - [Personal] Google - [Servicios] Anuncios”:

<sup>101</sup> <https://support.google.com/ads/answer/2662922?hl=es>



1714. El ID de publicidad estaba visible en la parte inferior de esta pantalla, y al ser restablecido mediante “Restablecer ID de publicidad” era posible confirmar que cambiaba su valor.

1715. Desde agosto de 2014, y con el objetivo de proteger la privacidad del usuario, Google Play Services (y sus servicios de anuncios) obligó a todas las apps de terceros a hacer uso del ID de publicidad (funcionalidad disponible desde octubre de 2013 mediante la versión 4.0 de los servicios y app de Google Play Services, GPS) para llevar a cabo cualquier tarea de seguimiento del usuario con fines publicitarios, en lugar de emplear (tal como hacían numerosas apps en el pasado) otros identificadores persistentes vinculados al usuario o al dispositivo móvil, como por ejemplo el identificador de la cuenta de usuario de Google, el IMEI del terminal, el IMSI de la tarjeta SIM, etc. [Ref.-124].

1716. La opción “Inhabilitar personalización de anuncios” (deshabilitada por defecto), conviene activarla, impidiendo así que las apps usen el ID de publicidad del usuario para mostrar anuncios en base a sus intereses, pero salvaguardando su privacidad.

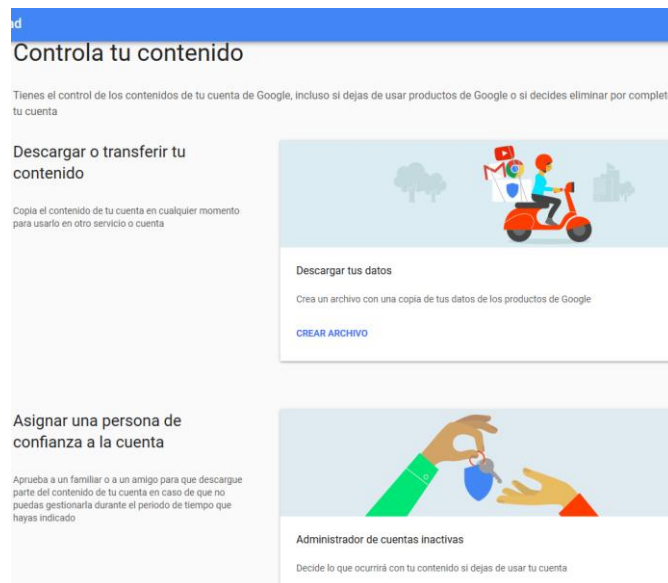
1717. La opción “Habilitar registro depuración (anuncios)”, si se habilita, hará que las apps registren en el log del sistema información relativa a los anuncios. Esta actividad, que no tiene interés desde el punto de vista del usuario final, se puede consultar mediante el comando “adb logcat”:

```
03-02 10:53:38.240 4412 4412 D AdvertisingIdNS: Notifying advertising info
update event for package com.google.android.youtube
```

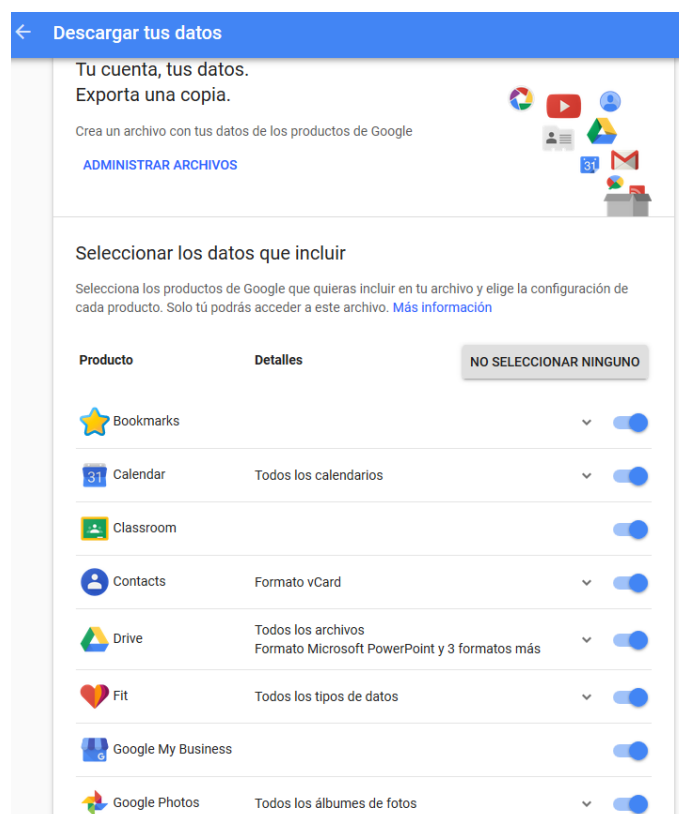
1718. Por último, la opción “Anuncios Google” redirige al usuario a la página web de Google que informa de los servicios de anuncios y publicidad.

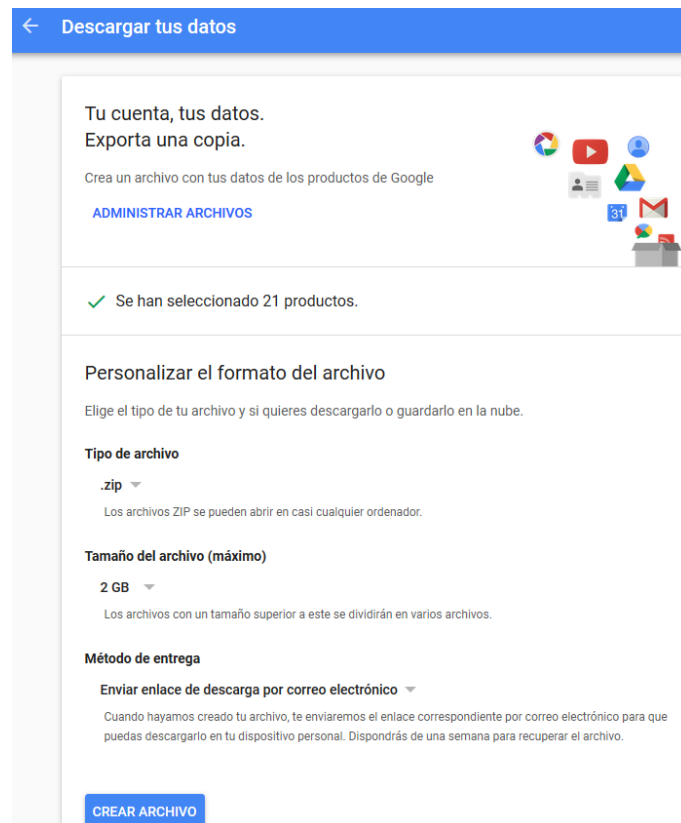
## 20.4.4. CONTROLA TU CONTENIDO

1719. El interfaz “Controla tu contenido” alberga dos subopciones a fecha de elaboración de la presente guía:

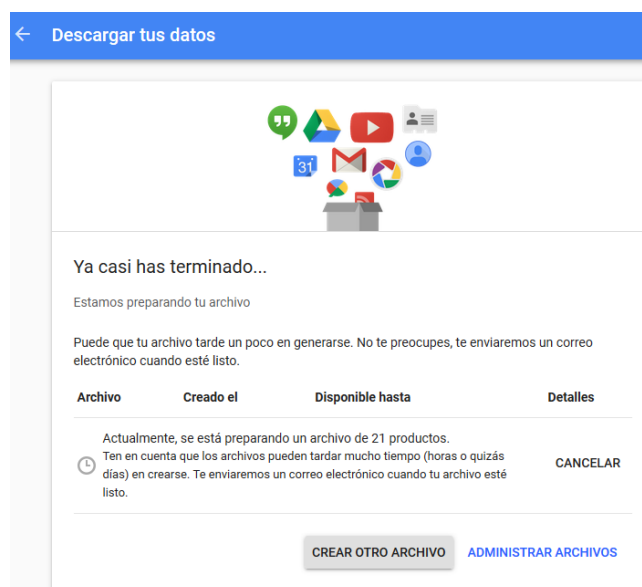


- Descargar o transferir tu contenido: Esta opción permite crear y descargar un archivo con los datos y la configuración de los servicios y aplicaciones de Google que el usuario seleccione.
  - Al seleccionar “Crear archivo”, se ofrece un menú que permite elegir qué datos se salvarán y transmitirán al archivo de copia.





- El formato del archivo puede ser .zip, .tgz o .tbz, y el tamaño máximo de 50 GB.
- Como métodos para obtener el archivo, se puede seleccionar el correo electrónico, Google Drive, Dropbox o Microsoft OneDrive (en cuyo caso el archivo se guardará en el servicio de la nube especificado y el enlace a su ubicación se enviará por correo electrónico a la cuenta de usuario de Google). El detalle de estos servicios queda fuera del alcance de la presente guía.
- Cuando se selecciona “Crear archivo”, se mostrará un mensaje de confirmación:



- Cuando el archivo se encuentre disponible, se recibirá un e-mail en la cuenta de usuario y se podrá descargar el archivo:



Tu archivo de datos de Google está listo Recibidos x

Descarga tus datos de Google <noreply@google.com>  
para mí

### Tu cuenta, tus datos.

El archivo de datos de Google que iniciaste el 21 de febrero de 2018 está preparado. Contiene tus datos de Marcadores, Calendar, Classroom, Contactos, Drive, Fit, Google My Business, Google Fotos, Google Play Libros, Grupos, Handsfree, Hangouts, Hangouts en directo, Keep, Historial de ubicaciones, Mail, Maps (tus sitios), Mi Actividad, Search Contributions, Tasks y YouTube. Estará disponible para su descarga hasta el 28 de febrero de 2018.

[Administrar archivos](#)
[Descargar archivo](#)


Has recibido este mensaje porque has utilizado recientemente el servicio de [descarga de datos de Google](#). [Política de Privacidad](#) | [Condiciones de Servicio](#)



### Descargar los datos: descargas

Si has decidido transferir tus datos a otro servicio, te recomendamos que consultes las políticas de exportación de datos del mismo, puesto que, si más adelante quieres cambiar de servicio, es posible que no puedas transferir algunos datos importantes como, por ejemplo, tus fotos.

No descargues tus archivos en ordenadores públicos ni los subas donde otras personas puedan verlos.

Una vez que descargues tus datos, si quieres explorar otras opciones para administrar tu cuenta, como la eliminación de la cuenta, visita [myaccount.google.com](https://myaccount.google.com).

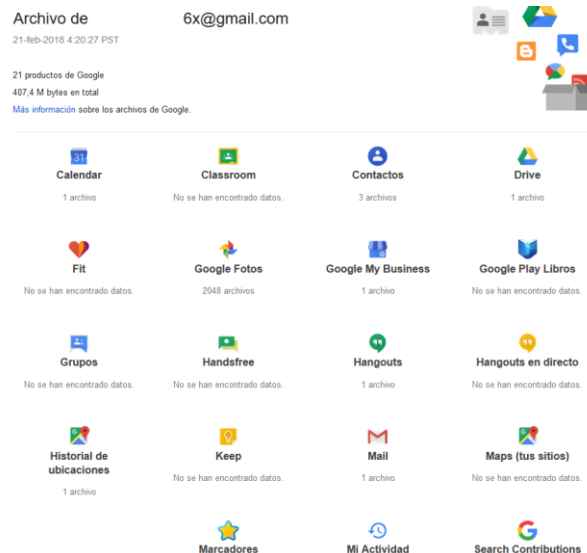
| Archivo                  | Creado el             | Disponible hasta      | Detalles                    |
|--------------------------|-----------------------|-----------------------|-----------------------------|
| 21 productos<br>396,2 MB | 21 de febrero de 2018 | 28 de febrero de 2018 | ▼ <a href="#">DESCARGAR</a> |

[CREAR UN ARCHIVO](#)
[VER HISTORIAL](#)
[LISTO](#)

**Nota:** Tu contenido de Google Play Música no se incluye cuando creas un archivo. Para descargar tu música, utiliza el [Google Play Music Manager](#).

- El archivo tiene la nomenclatura “takeout-fecha-ID.extensión\_designada”. Por ejemplo, “takeout-20180221T115317Z-001.zip”. El contenido del archivo sigue una estructura de subdirectorios, uno por cada aplicación seleccionada, y un fichero index que muestra lo que se ha salvado y, al seleccionar el icono de cada aplicación, el formato empleado (MBOX para el mail, JSON para las búsquedas y Hangouts, ICS para el calendario, HTML para los marcadores, etc.):

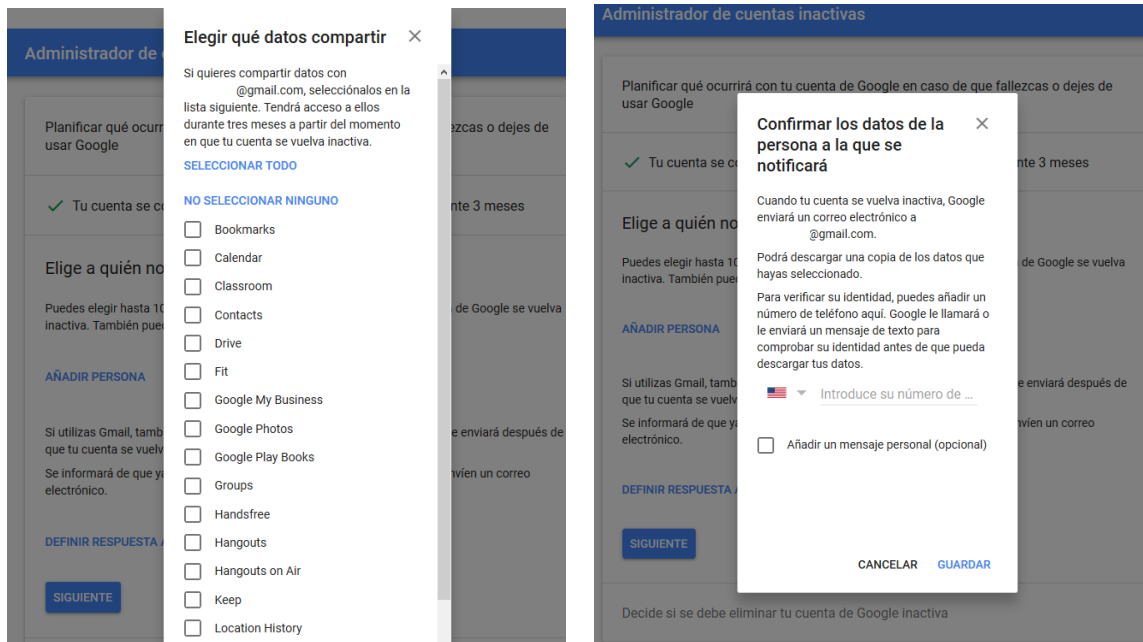
| Data > Local > Temp > takeout-20180221T121841Z-001-1.zip > Takeout > |                       |     |
|----------------------------------------------------------------------|-----------------------|-----|
| Nombre                                                               | Tipo                  | Tan |
| Calendar                                                             | Carpeta de archivos   |     |
| Contactos                                                            | Carpeta de archivos   |     |
| Drive                                                                | Carpeta de archivos   |     |
| Google Fotos                                                         | Carpeta de archivos   |     |
| Google My Business                                                   | Carpeta de archivos   |     |
| Hangouts                                                             | Carpeta de archivos   |     |
| Historial de ubicaciones                                             | Carpeta de archivos   |     |
| Mail                                                                 | Carpeta de archivos   |     |
| Marcadores                                                           | Carpeta de archivos   |     |
| Mi Actividad                                                         | Carpeta de archivos   |     |
| Tasks                                                                | Carpeta de archivos   |     |
| YouTube                                                              | Carpeta de archivos   |     |
| index.html                                                           | Firefox HTML Document |     |



- La creación de un archivo de descarga no elimina ninguna parte de la información almacenada en la cuenta de Google del usuario.
- Este método se puede utilizar si se desea exportar los datos a otro tipo de servicios, y también como una alternativa para realizar una copia de seguridad de los datos.
- Administrador de cuentas inactivas: permite configurar diversas opciones de actuación sobre cuentas de usuario que permanecen inactivas, independientemente del motivo. Al acceder a la opción “Administrador de cuentas inactivas - Cambiar esta configuración”, se abre un interfaz que permite definir un plan para el supuesto en que se deje de utilizar la cuenta de Google del usuario:



- Por defecto, se establece un periodo mínimo de espera de tres meses tras el cual la cuenta se considerará inactiva (el máximo configurable es 18 meses) y a quién se enviarán las alertas antes de que se cumpla el tiempo para que la cuenta se marque como inactiva; además, se puede configurar un máximo de 10 personas a quienes se notificará sobre la designación de la cuenta como inactiva, e incluso darles acceso a los datos que el propietario de la cuenta considere oportunos.



- Además, se puede configurar la opción de eliminar por completo la cuenta en caso de que se declare inactiva según los parámetros definidos anteriormente:

Planificar qué ocurrirá con tu cuenta de Google en caso de que fallezcas o dejes de usar Google

✓ Tu cuenta se considerará inactiva cuando dejes de usarla durante 3 meses

✓ Google no notificará nada a nadie

**Decide si se debe eliminar tu cuenta de Google inactiva**

¿Quieres que eliminemos tu cuenta y todo su contenido cuando se vuelva inactiva?

Si has decidido permitir que alguien descargue tu contenido, podrá hacerlo durante 3 meses antes de que se elimine.

Si eliges eliminar tu cuenta de Google, también se retirarán los datos que hayas compartido públicamente (por ejemplo, videos de YouTube, publicaciones de Google+, blogs de Blogger, etc.). [Más información](#)

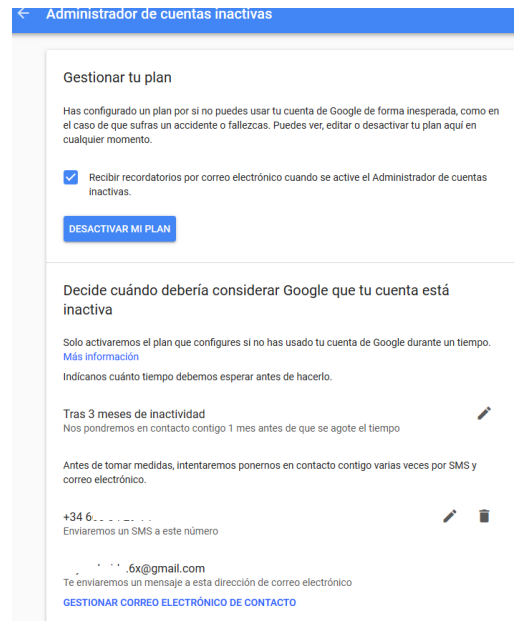
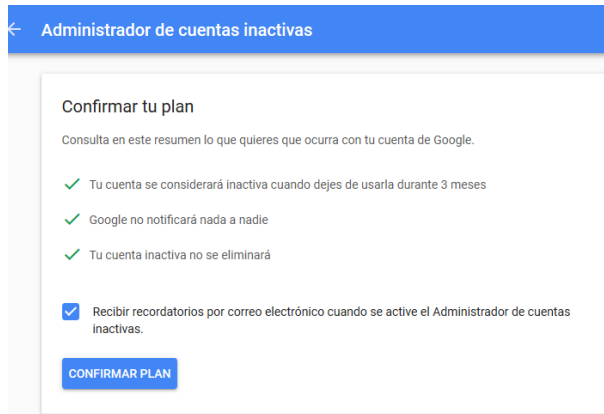
¿Quieres que eliminemos tu cuenta de Google en caso de que se vuelva inactiva?

Sí, eliminar mi cuenta de Google inactiva ☐

Esto ocurrirá tres meses después de que tu cuenta se vuelva inactiva

[REVISAR PLAN](#)

- Una vez finalizada la configuración, se ofrece revisar el plan y, en caso de ser adecuado, confirmarlo:



- Si se añade un contacto de confianza, se ofrecerá la posibilidad de marcar qué datos pueden ser accedidos por dicho contacto. Además de su dirección de correo electrónico, se puede proporcionar un número de teléfono del contacto para comprobar su identidad e impedir accesos no autorizados a los datos. Los contactos de confianza recibirán dicho código de verificación después de que la cuenta se marque como inactiva.

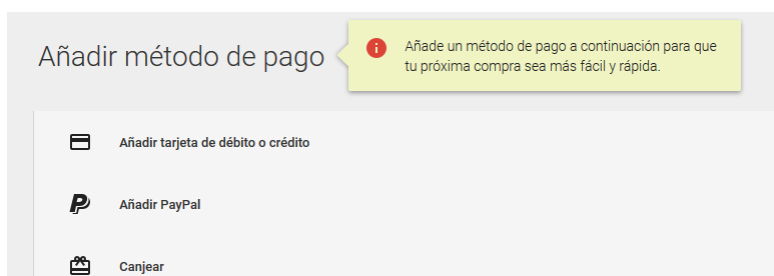
1720. Desde el punto de vista de seguridad y privacidad, no se recomienda hacer uso de la funcionalidad “Administrador de cuentas inactivas”, pues pueden ser múltiples las circunstancias que provoquen que una cuenta deje de ser utilizada y no en todas ellas el propietario podrá revocar una autorización de acceso a sus datos habilitada previamente.

## 20.5. PREFERENCIAS DE LA CUENTA

1721. A fecha de elaboración de la presente guía, el acceso a esta configuración desde el dispositivo móvil se encuentra en “Ajustes - [Personal] Google - Preferencias de la cuenta”, que lanza el correspondiente menú del interfaz “Mi cuenta”.

1722. Bajo esta sección se encuentran las siguientes opciones:

- Payments: el denominado “Centro de pagos de Google” [Ref.- 262] es un servicio que pretende albergar perfiles de pago del usuario para utilizarlos en las compras de productos y servicios de Google (como la Google Play). La configuración detallada de este servicio queda fuera del ámbito de la presente guía.



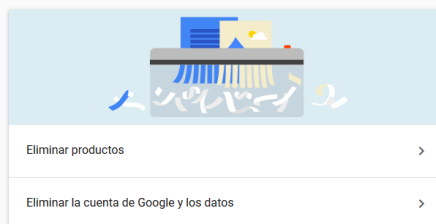
- Idioma y herramientas de escritura: permite definir el idioma predeterminado en el que se mostrará el contenido de la web y añadir otros idiomas, así como

seleccionar las herramientas de introducción de texto, como el formato del teclado.

- **Accesibilidad:** en caso de que sea necesario configurar algún elemento relacionado con este aspecto.
- **Tu almacenamiento en Google Drive:** proporciona la información sobre el espacio ocupado en Google Drive en el momento actual, por aplicaciones, así como contratar espacio adicional.
- **Eliminar tu cuenta o determinados servicios:** permite eliminar servicios que ya no se desea utilizar como parte de la cuenta de usuario, pudiéndose descargar previamente los datos asociados a ellos, e incluso la cuenta de Google en su totalidad.

#### Eliminar tu cuenta o determinados servicios

Si ya no te interesa utilizar servicios concretos de Google, como Gmail o Google+, puedes eliminarlos aquí. También puedes eliminar tu cuenta de Google por completo.



#### Eliminar un servicio de Google

Las cuentas de Google ofrecen muchos servicios y algunos de ellos pueden eliminarse de tu cuenta de forma individual.

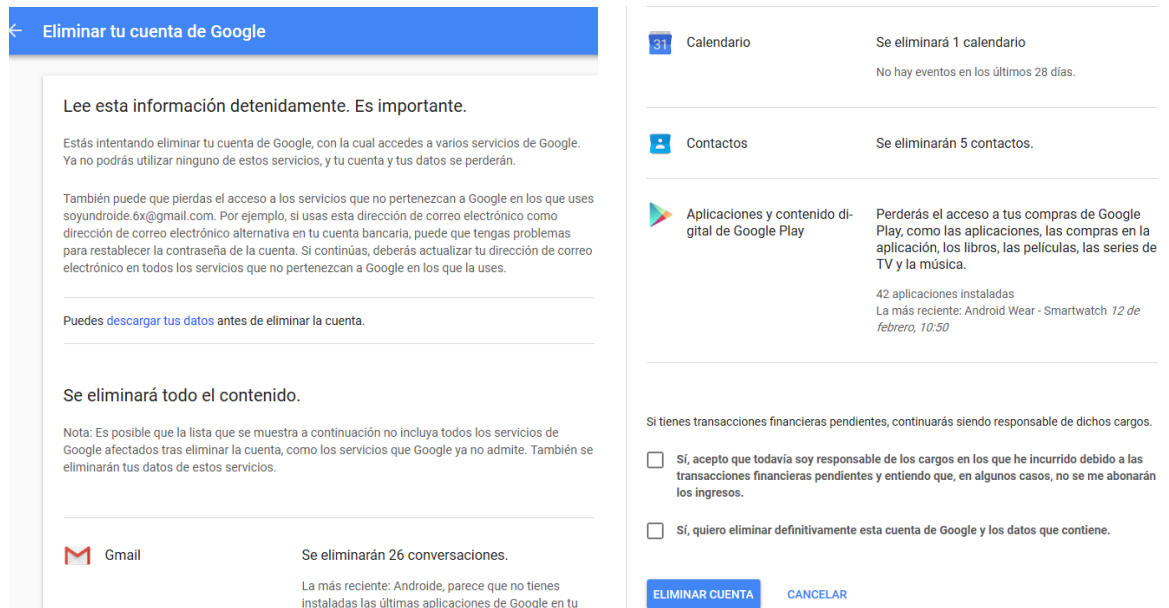
Puedes descargar sus datos antes de eliminar un servicio.

[DESCARGAR DATOS](#)

O elige un servicio a continuación:

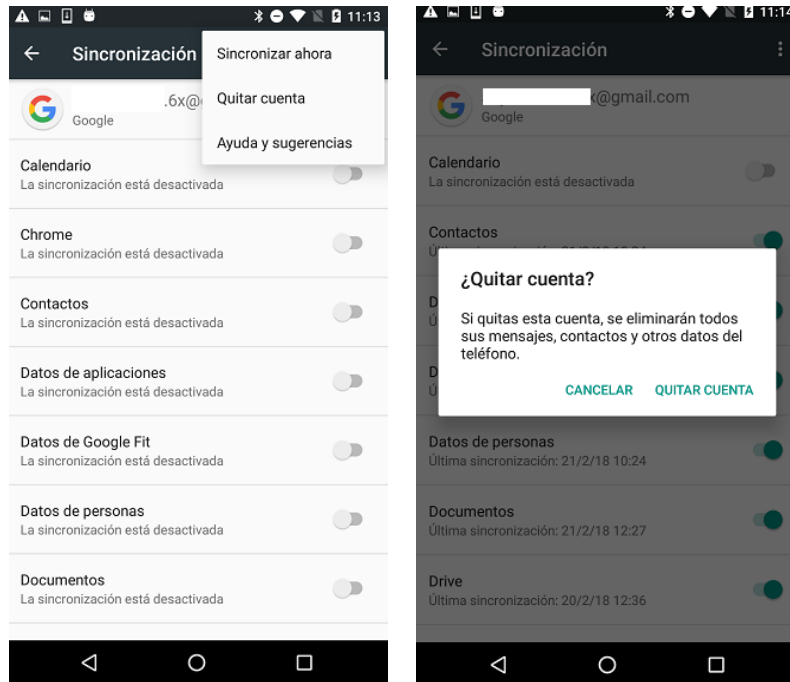


- Por último, la opción “Eliminar la cuenta y los datos de Google” permite eliminar por completo la cuenta, no sólo del dispositivo actual, sino la totalidad de la cuenta. Dado el impacto de esta acción, se solicitará introducir las credenciales del usuario de nuevo, así como confirmación y aceptación de las condiciones del servicio. Además, se instará al usuario a descargar los datos antes de proceder a la eliminación de la cuenta.



## 20.6. GESTIÓN DE LAS CREDENCIALES DE LAS CUENTAS DE USUARIO DE GOOGLE

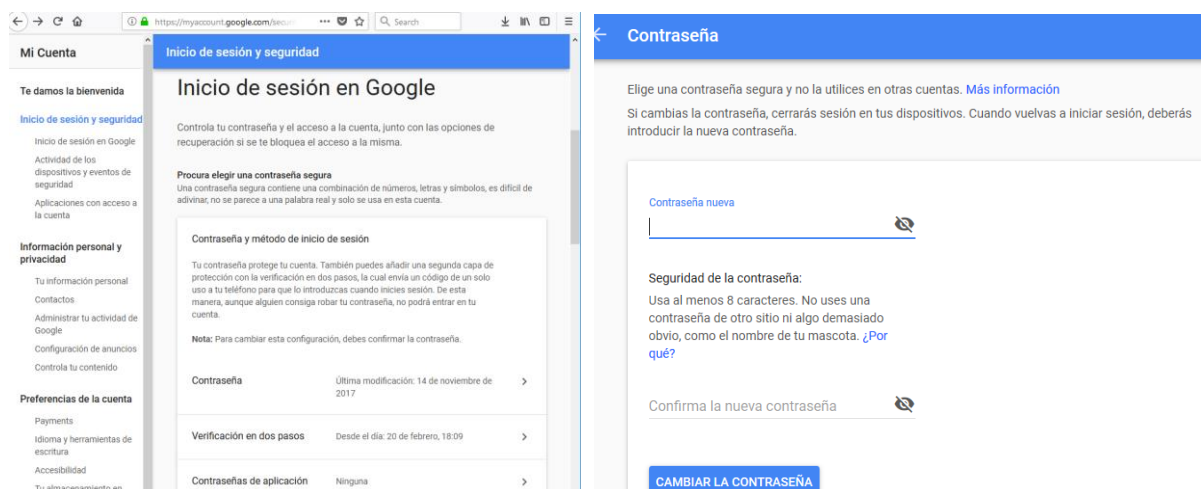
1723. Desde el punto de vista de seguridad, la opción ideal sería no almacenar la contraseña de la cuenta del usuario de Google en el dispositivo móvil, mitigando así el riesgo de que un potencial atacante obtenga acceso al mismo, y como consecuencia, a la cuenta del usuario, junto a todos sus servicios asociados, como por ejemplo Google Play o Gmail.
1724. Sin embargo, no se ha identificado ninguna opción de configuración en el dispositivo móvil, a través de “Ajustes [Cuentas]” o “Ajustes [Personal] - Seguridad” (o en la configuración de la app “Play Store” o “GMail”), para evitar el almacenamiento de la contraseña (o de los *tokens* de autenticación) de la cuenta de usuario de Google.
1725. Es decir, la contraseña (o *token* de autenticación) asociada a la cuenta del usuario queda almacenada automáticamente en el dispositivo móvil, no siendo posible evitar su almacenamiento. Como resultado, tras encender el dispositivo móvil, se dispone de acceso directo y completo a la cuenta del usuario y a todos los servicios asociados.
1726. Este escenario de gestión y almacenamiento automático de contraseñas para las cuentas del usuario es similar para las cuentas de otros servicios, por ejemplo redes sociales como Facebook o Twitter, en los cuales la contraseña queda almacenada en la app y, por tanto, en el dispositivo móvil, no siendo posible evitarlo.
1727. La única alternativa identificada para evitar esta asociación entre cuenta/contraseña y dispositivo móvil es eliminar la cuenta asociada cada vez que se termina de hacer uso de la misma, pero esto no es viable porque se perderían todos los datos asociados a ella en el dispositivo. La pantalla de “Ajustes - [Personal] Cuentas - Google - <nombre de cuenta> ... - Quitar cuenta” permite eliminarla del dispositivo móvil tras confirmar la operación a través del botón “Quitar cuenta”:



1728. Android no proporciona capacidades para modificar la contraseña de la cuenta principal de Google asociada al dispositivo móvil, ni para modificar las contraseñas de otros servicios de Google disponibles en Android.

1729. Las siguientes recomendaciones aplican tanto a la cuenta principal de Google como a las cuentas de otros servicios, como Twitter o Facebook. Para otros servicios será necesario evaluar la secuencia de acciones a seguir independientemente (pero de manera similar a como se describe a continuación), y en todo caso, hacer uso del acceso web estándar a los mismos.

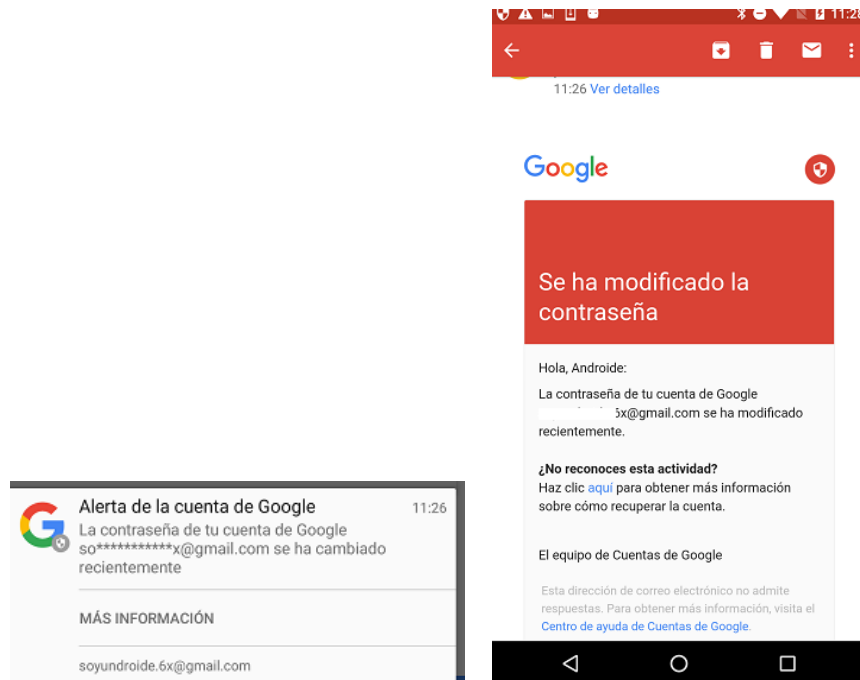
1730. Para invalidar la contraseña almacenada para la cuenta principal de Google asociada al dispositivo móvil, el método más directo pasa por modificar la contraseña a través de la página web estándar del servicio “https://myaccount.google.com - Inicio de sesión y seguridad - Inicio de sesión en Google - Contraseña”, desde otro ordenador o desde el propio navegador web del dispositivo móvil Android.



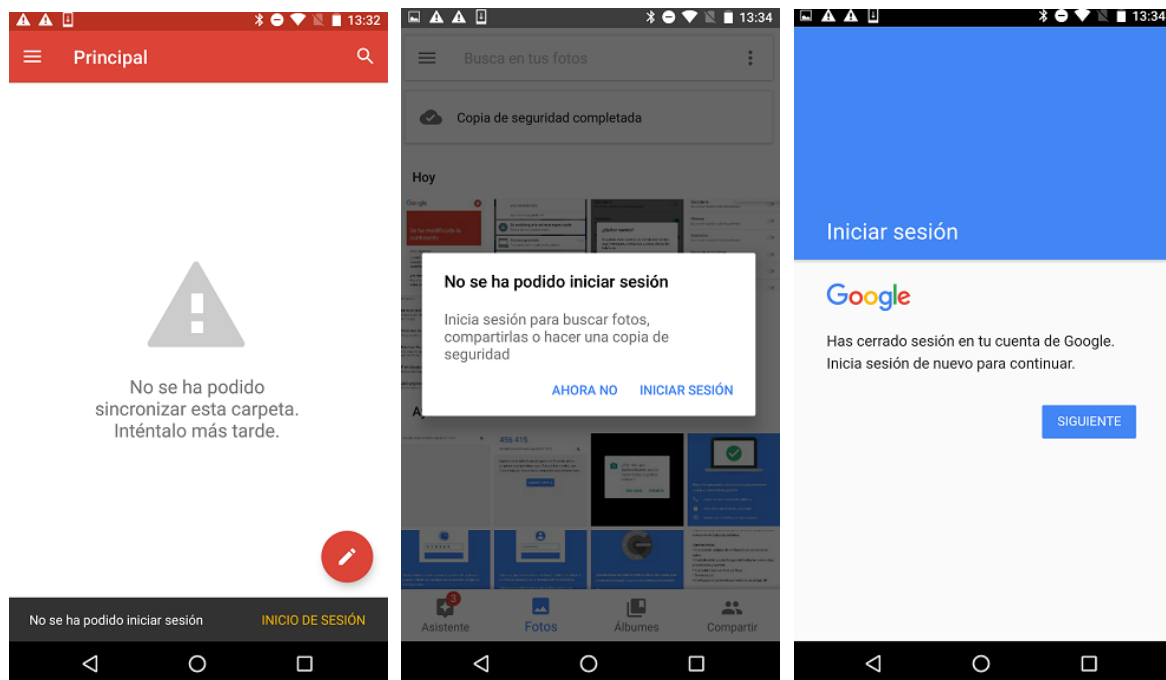
1731. Una vez se accede al menú de cambio de contraseña, se distinguen dos escenarios:



- Cuando el mecanismo de verificación en dos pasos está desactivado y se cambia la contraseña de la cuenta de Google, se cerrará la sesión en el dispositivo móvil y se enviará un mensaje informativo al buzón de Gmail del usuario:

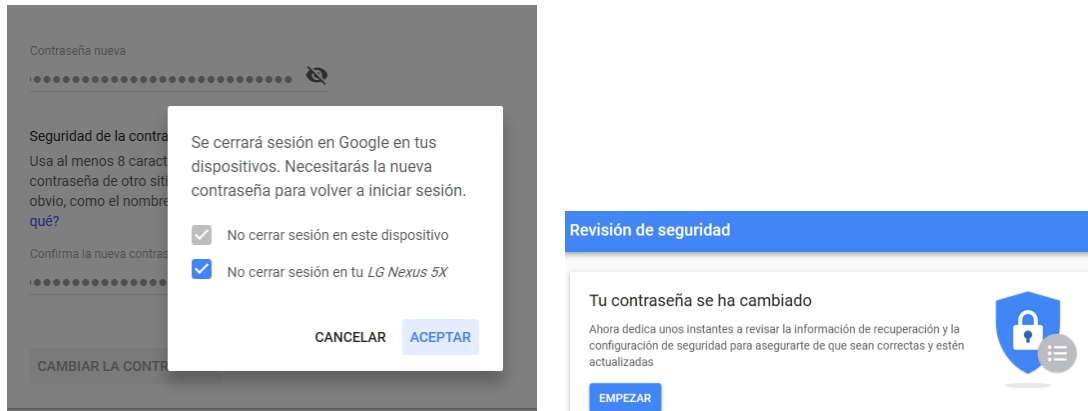


Tan pronto una app que utilice los servicios de Google trate de conectarse a ellos, se producirá un error (en versiones de Android hasta la 5.1.1 inclusive se generaba una notificación de error de sincronización y se instaba al usuario a introducir la nueva contraseña), el cual dependerá de la app concreta, y se llevará al usuario a la pantalla de configuración de la cuenta<sup>102</sup>. Las siguientes imágenes muestran el error de las apps “Gmail” y “Fotos” y la ventana que se muestra cuando se selecciona el mensaje que invita a iniciar sesión:

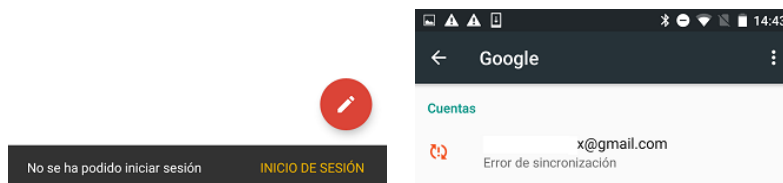
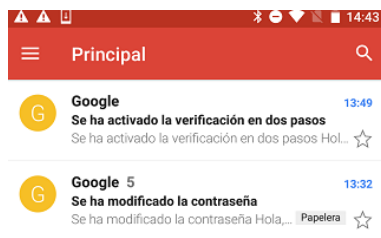


<sup>102</sup> Algunas apps o servicios concretos de Google también pueden generar sus notificaciones, como Google Drive.

- Si el mecanismo de verificación en dos pasos se encuentra activo, el interfaz web de Google presentará la siguiente ventana:



- Si al cambiar la contraseña se deja marcada (configuración por defecto) la opción “No cerrar sesión en tu <dispositivo>”, la sesión correspondiente a la cuenta de usuario de Google del dispositivo móvil no se cerrará, por lo que todos los servicios y apps de Google seguirán funcionando con normalidad, incluso aunque se reinicie el dispositivo móvil.
- Si se desmarca la opción, la situación será similar a la que se presenta cuando la verificación en dos pasos está desactivada, por lo que las apps que se conecten a servicios de Google mostrarán errores y ofrecerán una opción para iniciar sesión de nuevo. Si se consulta la cuenta de Google a través de “Ajustes - [Personal] Cuentas - Google”, se observará un error de sincronización:



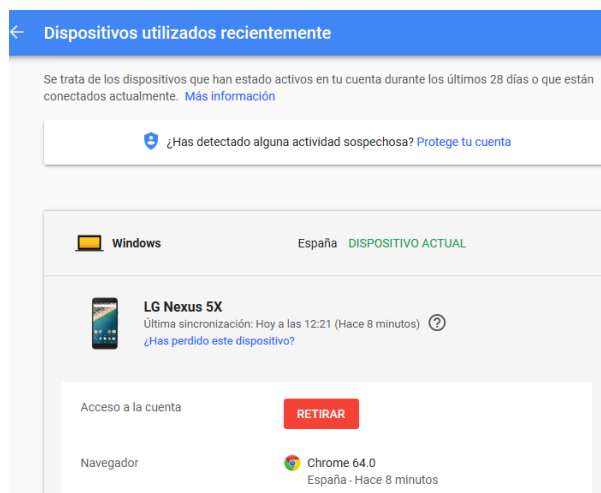
1732. La siguiente tabla muestra la petición de la app Gmail para acceder a la cuenta y sincronizar los mensajes, y la respuesta fallida procedente del servidor, denegando la autorización:

```
POST /mail/g/?version=25&clientVersion=25 HTTP/1.1
Authorization: Bearer ya29.Go4BagV6K1YvWV3dax-r9emD3w_ <...> 55MQQ
Content-Encoding: gzip
```

```
Host: mail.google.com
User-Agent: Android-GmailProvider/60087425 (sw411dp; 420dpi) (bullhead MTC20K);
gzip
Cookie: COMPASS=gmail=CokBAAlriVeYO_TatyWzl0vWZqmlDPo6GEqx_ <...> kJ7g
Cookie2: $Version=1
```

```
HTTP/1.1 401 Unauthorized Content-Type: text/html; charset=UTF-8 WWW-
Authenticate: Bearer realm="https://accounts.google.com/" Server: GSE
<HTML>
<HEAD>
<TITLE>Unauthorized</TITLE>
</HEAD>
<BODY BGCOLOR="#FFFFFF" TEXT="#000000">
<H1>Unauthorized</H1>
<H2>Error 401</H2>
</BODY>
</HTML>
```

1733. Es importante reseñar que no se recibe ninguna notificación que informe al usuario de que el error es debido a un cambio en la contraseña.
1734. Si el cambio de contraseña se debe a que el usuario ha perdido el dispositivo móvil, se deberá desmarcar la opción “No cerrar sesión en tu <nombre\_dispositivo>” para asegurarse de que no se mantendrá abierta la sesión y que un tercero no autorizado con acceso físico al dispositivo móvil pueda tener acceso a toda la funcionalidad de la cuenta de Google del usuario.



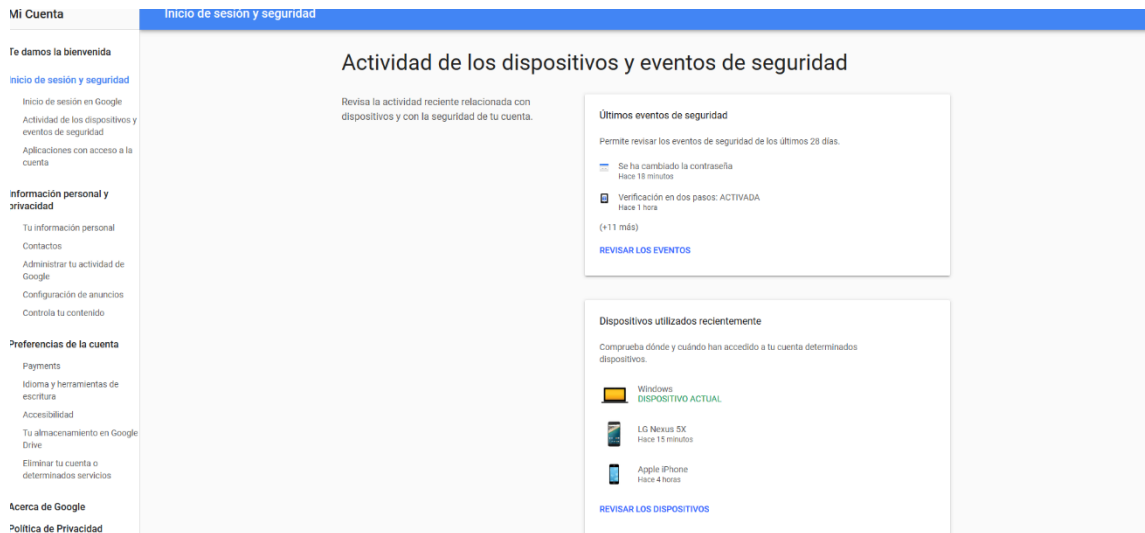
**Nota:** La solicitud de la contraseña asociada a la cuenta del usuario también se puede presentar al cambiar la tarjeta SIM del dispositivo móvil, según la versión de Android y el modelo de dispositivo móvil empleado.

1735. En caso de sustracción o pérdida del dispositivo móvil, este cambio de contraseña a través de la web debería ser una de las primeras tareas a realizar por el usuario.
1736. Por otro lado, debido a que Android está diseñado para trabajar con una cuenta de usuario de Google que esté siempre activa, tampoco proporciona capacidades para desconectarse (o cerrar la sesión actual) de la cuenta de usuario de Google, de forma que la próxima vez que se utilice cualquiera de los servicios asociados, y se establezca una sesión con estos, se solicite de nuevo al usuario la contraseña de la cuenta.

1737. El método disponible para forzar esta desconexión, sin tener que eliminar la cuenta del dispositivo móvil y/o resetear el mismo, pasa por cambiar la contraseña desde la web (como se ha descrito previamente) o utilizar apps de terceros con este propósito.
1738. En versiones previas de Android, 1.x, era posible forzar esta desconexión borrando la caché y los datos asociados a algunos de los servicios críticos de conexión y sincronización con Google (Gmail, Google Apps y Gmail Storage). Los botones “Borrar datos” y “Borrar caché” estaban disponibles a través del menú de “Ajustes - Aplicaciones - Administrar aplicaciones”, desde la pestaña “Todas”, seleccionando una por una estas aplicaciones (o servicios). Esta recomendación no aplica desde Android 2.x.

## 20.7. INICIO DE SESIÓN Y SEGURIDAD

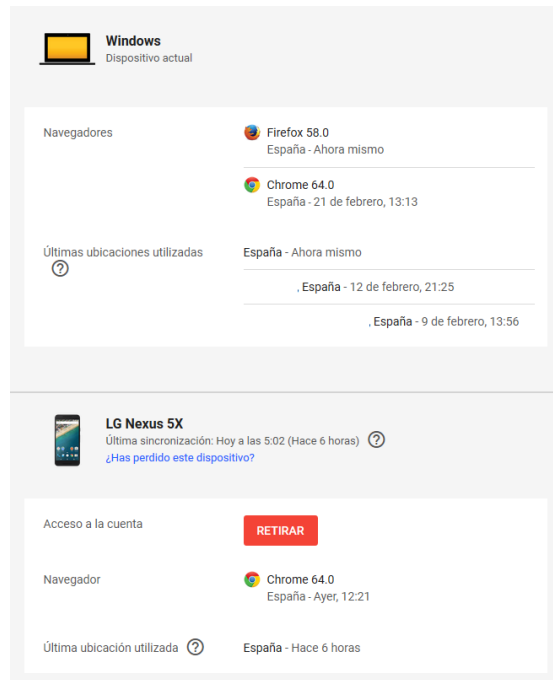
1739. En el 2017 Google añadió al interfaz de administración de la cuenta de usuario de Google el apartado “Inicio de sesión y seguridad - Actividad de los dispositivos y eventos de seguridad”:



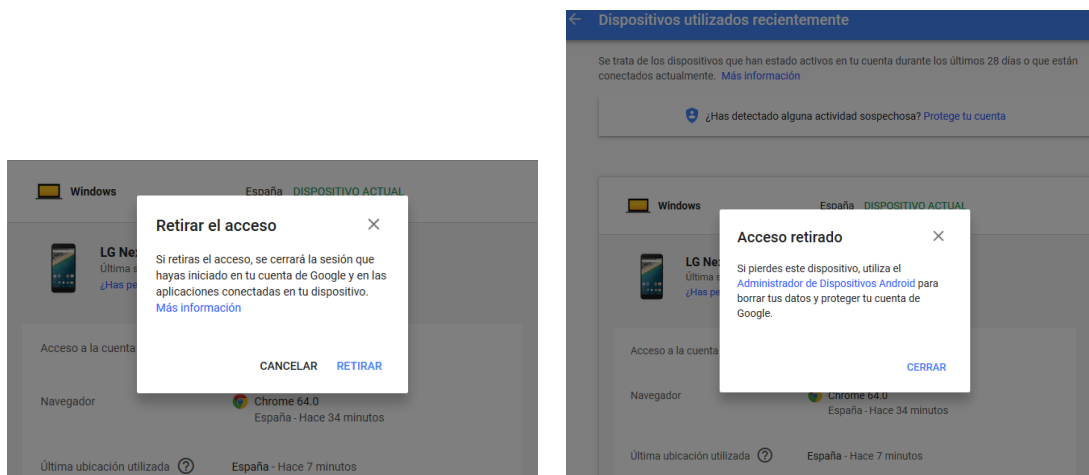
1740. Este apartado permite consultar los eventos de seguridad de los últimos 28 días que Google genera relacionados con la cuenta del usuario, como los cambios de contraseña, la activación/desactivación del mecanismo de verificación en dos pasos, el inicio de sesión en un dispositivo móvil nuevo, y otros eventos:

Últimos eventos de seguridad		
	Se ha cambiado la contraseña	España - Hace 1 hora
	Se ha cambiado la contraseña	España - Hace 1 hora
	Verificación en dos pasos: DESACTIVADA	Hace 1 hora
	Se ha cambiado la contraseña	España - Hace 1 hora
	Se ha cambiado la contraseña	España - Hace 2 horas
	Se ha cambiado la contraseña	España - Hace 3 horas
	Se ha iniciado sesión en un dispositivo nuevo	España - Hace 4 horas
	Verificación en dos pasos: ACTIVADA	20 de febrero, 18:09
	Verificación en dos pasos: DESACTIVADA	20 de febrero, 18:06
	Verificación en dos pasos: ACTIVADA	20 de febrero, 13:47

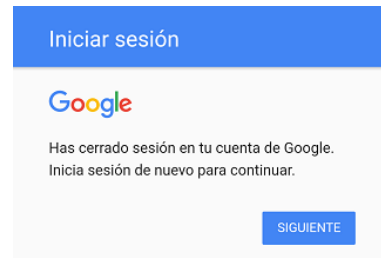
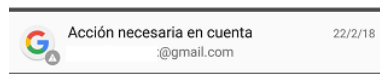
1741. Adicionalmente, permite determinar desde qué dispositivos se ha abierto sesión en la cuenta de Google del usuario. La opción “Revisar los dispositivos” muestra la lista de dispositivos (tanto móviles como tradicionales) que han accedido a la cuenta y la fecha del último acceso. Si se selecciona la entrada de cualquiera de ellos, se indicará el mecanismo empleado para el acceso (por ejemplo, el tipo y versión del navegador web si se accedió mediante éste), y permite retirar el acceso a la cuenta de aquellos dispositivos que hayan iniciado sesión en la cuenta de Google del usuario:



1742. Si se sospecha sobre el origen de alguna actividad en un dispositivo concreto, se puede “Retirar” el acceso a la cuenta desde el mismo mediante el botón correspondiente.



1743. En el dispositivo móvil se perderá el acceso a la cuenta de Google y ninguna aplicación se sincronizará con su servicio asociado.
1744. Una vez se haya retirado el acceso a la cuenta de Google para el dispositivo móvil sospechoso, y que potencialmente está utilizándola de manera no autorizada, se evaluarán las acciones correspondientes a llevar a cabo (por ejemplo, si se el dispositivo móvil se ha extraviado, consultar las recomendaciones indicadas en el apartado “8.1. Gestión remota de dispositivos Android por parte del usuario”).
1745. Además de a través del interfaz web “Inicio de sesión y seguridad”, Google envía a la cuenta de correo de Gmail del usuario mensajes relativos a los eventos de seguridad relevantes. En dichos mensajes, se proporcionan enlaces al interfaz web de gestión de la cuenta (concretamente, al apartado relacionado con el tipo de evento particular).
1746. También se pueden recibir notificaciones como la que se muestra a continuación, que informan de que hay alguna incidencia con la cuenta de Google y, que, al abrirlas, redirigirán a la acción que se considera necesaria por parte de Google:

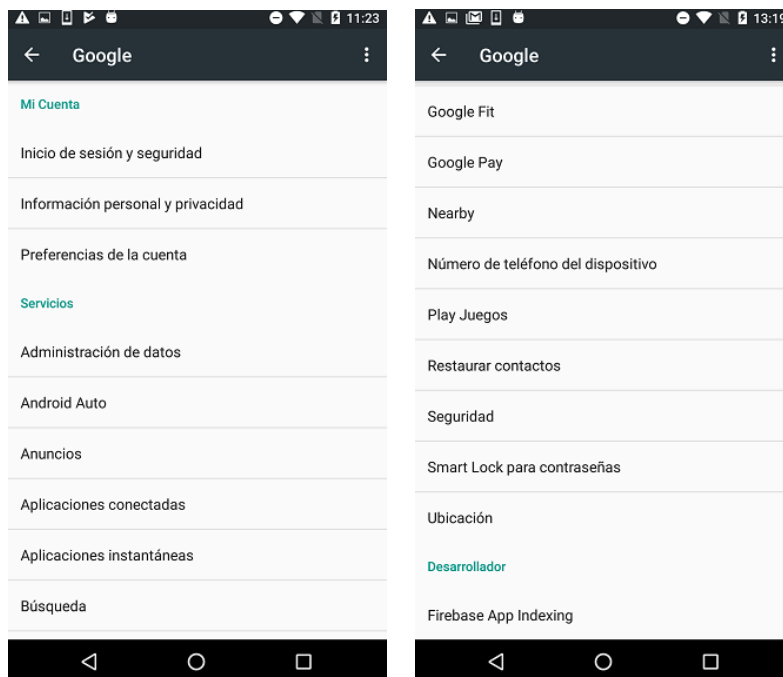


1747. Dada la extrema importancia que tiene la cuenta de usuario de Google, no sólo por lo sensible de la información relativa al usuario que alberga, sino por las acciones que desde ella se pueden realizar, se recomienda encarecidamente prestar atención a los mensajes relativos a eventos de seguridad, y consultar asiduamente el capítulo “Actividad de los dispositivos y eventos de seguridad” para identificar cualquier actividad no reconocida como propia sobre la cuenta de Google y los dispositivos asociados de un modo u otro a estas actividades sospechosas.

1748. Ante cualquier mínima sospecha, se deberán evaluar las acciones pertinentes, empezando por cambiar la contraseña actual de la cuenta de usuario de Google.

## 20.8. OTROS AJUSTES DE GOOGLE

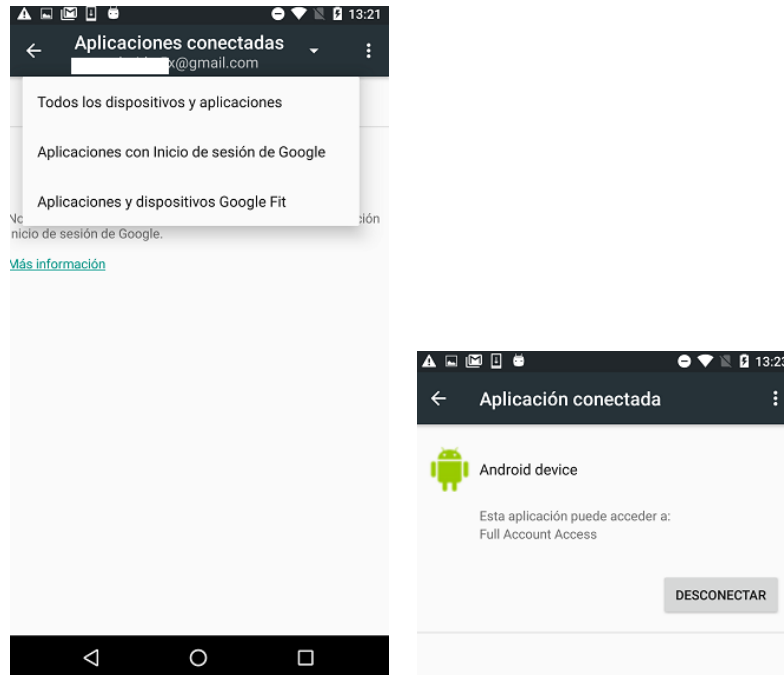
1749. Además de los ajustes ya descritos en los apartados previos, dentro del menú “Ajustes - [Personal] Google” se ofrece el apartado “Servicios”, que alberga otras opciones:



- Administración de datos: determina si la actualización de archivos de apps se realizará sólo por Wi-Fi o también a través de la red de datos móvil.
- Aplicaciones conectadas: permite ver qué apps (además de las propias de Google) se han conectado a la cuenta seleccionada con inicio de sesión o con dispositivos Google Fit. De hecho, si se desea cerrar la sesión en la cuenta de Google en el



dispositivo, se deberá proceder a la desconexión de la app que se muestra como “Android device”:



- Aplicaciones instantáneas: consultar apartado “23.13. Instant Apps”.
- Búsqueda: contiene todas las opciones de configuración relativas a cualquier tipo de búsqueda, tanto del asistente de Google como de “Mi tablón”, del idioma de búsqueda, etc.
- Configura el perfil de trabajo: para dispositivos de uso corporativo.
- Configurar dispositivo cercano: permite configurar un dispositivo en base a la configuración del dispositivo actual.
- Seguridad: ofrece acceso a configuración relativa a la aplicación “Encontrar mi dispositivo” (ver apartado “8.1. Gestión remota de dispositivos Android por parte del usuario”).
- Smart Lock para contraseñas: consultar apartado “23.14. Servicio de contraseñas de Google Smart Lock”.

## 21. COPIAS DE SEGURIDAD

### 21.1. COPIA DE SEGURIDAD LOCAL

1750. Desde la versión 4.0 de Android (*Ice Cream Sandwich*) se dispone de capacidades locales para realizar copias de seguridad de los contenidos del dispositivo móvil en el ordenador del usuario [Ref.- 93], sin necesidad de haber realizado el proceso de *rooting* sobre el mismo.

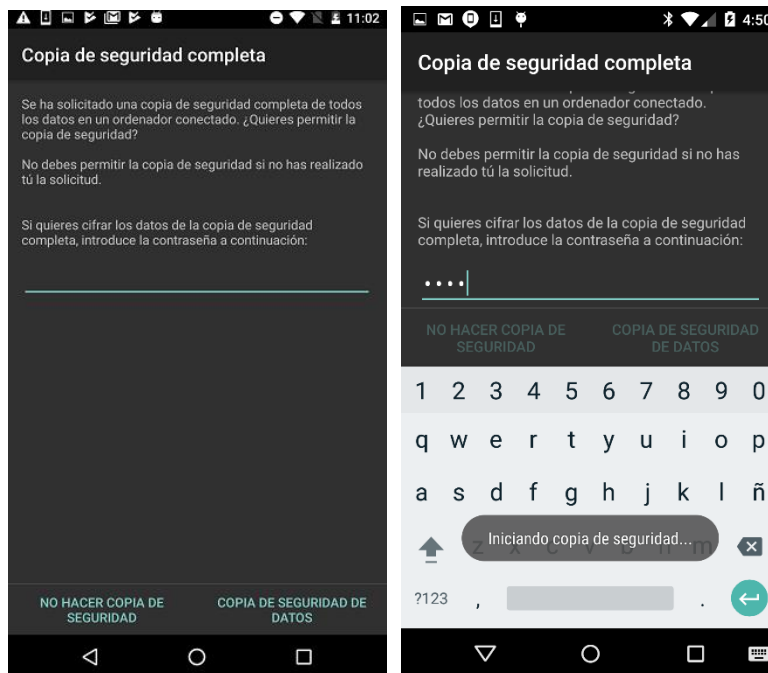
1751. Las copias de seguridad se llevan a cabo a través de ADB, por lo que es necesario disponer de las capacidades de desarrollo y depuración a través de USB habilitadas (ver apartado “13.3. Opciones de desarrollo y depuración USB”).

1752. Desde el punto de vista de seguridad se recomienda habilitar estas capacidades únicamente en el momento de llevar a cabo la copia de seguridad, y volverlas a deshabilitar inmediatamente después.
1753. En concreto, el comando “adb backup” permite realizar la copia de seguridad, pudiéndose especificar el fichero donde se almacenará la misma (mediante la opción “-f”, y por defecto en “backup.ab”). Este comando dispone de diferentes opciones para definir qué contenidos serán añadidos a la copia de seguridad, incluyendo los datos de las apps, tanto de sistema (o apps existentes por defecto) como de terceros, los propios ficheros APK de las apps, los contenidos del almacenamiento compartido (o tarjeta SD), etc. Es también posible especificar que se realice la copia de seguridad sólo de ciertas apps.
1754. Se han observado casos en los que, al utilizar una versión reciente del binario “adb” incluido en las “Platform Tools” del SDK de Android para guardar un backup de una versión de Android 4.x, la invocación del comando “adb backup” da como resultado un fichero de extensión “.ab” vacío o con escaso tamaño. Parece que el problema se debe a que el dispositivo hace uso de una versión antigua del protocolo ADB, en la que los argumentos del comando “adb backup” eran escapados de manera diferente, por lo que es necesario hacer uso de una versión previa del comando “adb” en el ordenador utilizado para realizar la copia de seguridad. Al hacer uso de una versión previa de ADB, como la 1.0.31, sí es posible hacer una copia de seguridad del dispositivo móvil y de sus apps. La versión 1.0.31 de “adb” está disponible en la versión 20 de las “Platform Tools” [Ref.- 506].
1755. Algunas apps pueden especificar en su fichero *manifest* que no permiten que se haga copia de seguridad de ellas, por lo que quedarán excluidas de este proceso.
1756. El fichero creado incluye una cabecera específica para las copias de seguridad de Android (variable según si se usa cifrado o no) y emplea el formato “tar”, con ligeras modificaciones propias de Android [Ref.- 93].

```
C:\> adb backup -f Android_6x_backup.ab -all -system -shared -apk
Now unlock your device and confirm the backup operation...
```

**Nota:** La opción “-all” del comando “adb backup” no guarda los datos del almacenamiento compartido, por lo que aisladamente no realizará un backup completo del dispositivo. Por este motivo ha de incluirse la opción “-shared”. A pesar de ello, se ha de tener precaución, pues la experiencia demuestra que ciertos datos de usuario no se mantienen tras la restauración con el comando “adb restore”, como los asociados a múltiples apps.

1757. Tras ejecutar el comando “adb backup”, el dispositivo móvil mostrará una pantalla de confirmación para autorizar la realización de la copia de seguridad:



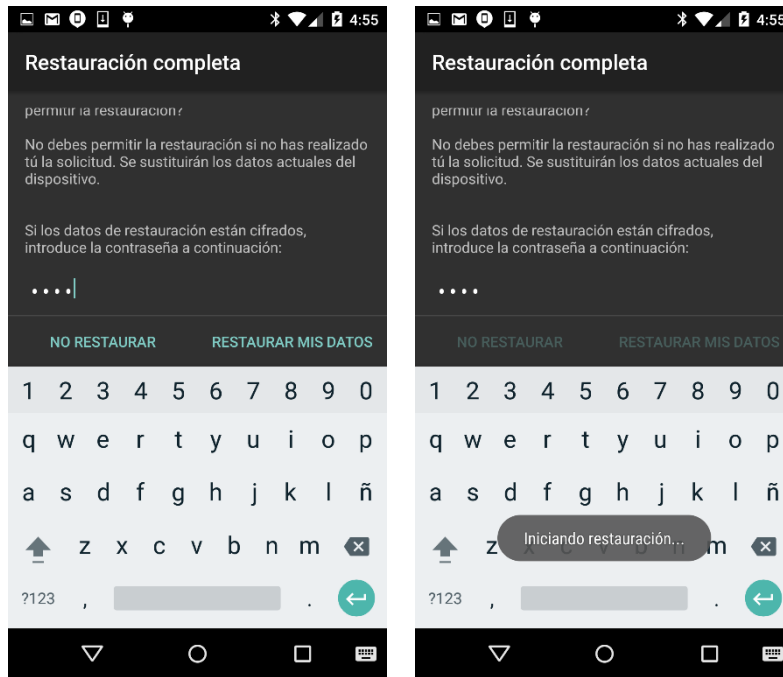
1758. Cabe destacar especialmente la opción que permite establecer una contraseña para cifrar los contenidos de la copia de seguridad mediante AES 256 bits. Se recomienda siempre hacer uso de una contraseña para cifrar los contenidos de la copia de seguridad.
1759. En el caso de Android 6.x, aunque el dispositivo móvil está cifrado, no es obligatorio especificar una contraseña para proteger los contenidos de la copia de seguridad (aunque se recomienda siempre establecer una).
1760. Aunque no se especifica que sea obligatorio tener las aplicaciones cerradas a la hora de hacer un backup, sí se recomienda minimizar las apps que están abiertas, pues se han observado casos de apps que abortan su ejecución durante la operación de backup.
1761. El comando equivalente “adb restore” permite recuperar o restaurar una copia de seguridad realizada previamente en el dispositivo móvil:

```
C:\> adb devices
List of devices attached
0111fb17aa642917 unauthorized

<Tras habilitar en el dispositivo móvil el acceso mediante ADB proveniente del
ordenador, se podrá establecer la conexión y enviar el comando "adb restore">

C:\> adb devices
List of devices attached
0111fb17aa642917 device
C:\> adb restore Android_6x_backup.ab
Now unlock your device and confirm the restore operation.
```

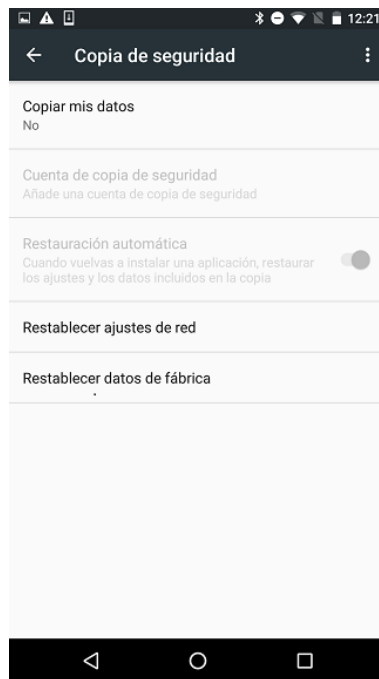
1762. En el caso de que la copia de seguridad esté cifrada, el proceso muestra en la pantalla del dispositivo móvil el campo para especificar la contraseña que fue utilizada a la hora de realizar la copia de seguridad:



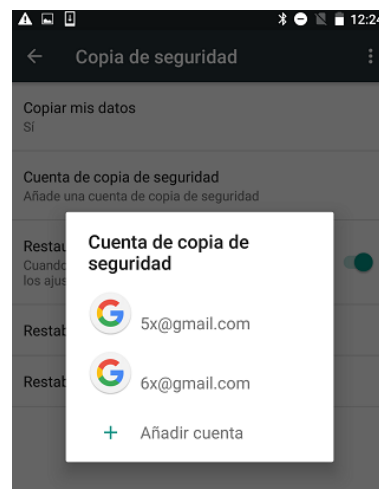
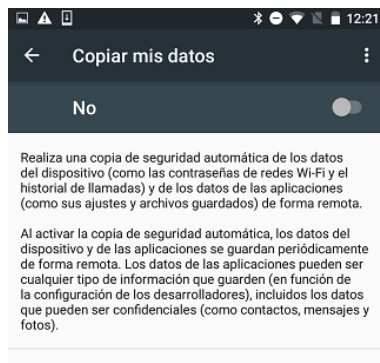
1763. En el caso de que la restauración mediante el comando “adb restore” deba realizarse partiendo de un dispositivo móvil que se acaba de restaurar a fábrica, será necesario habilitar la ejecución del comando ADB siguiendo los pasos detallados en el apartado “13.3. Opciones de desarrollo y depuración USB”.

## 21.2. COPIA DE SEGURIDAD EN LOS SERVIDORES DE GOOGLE

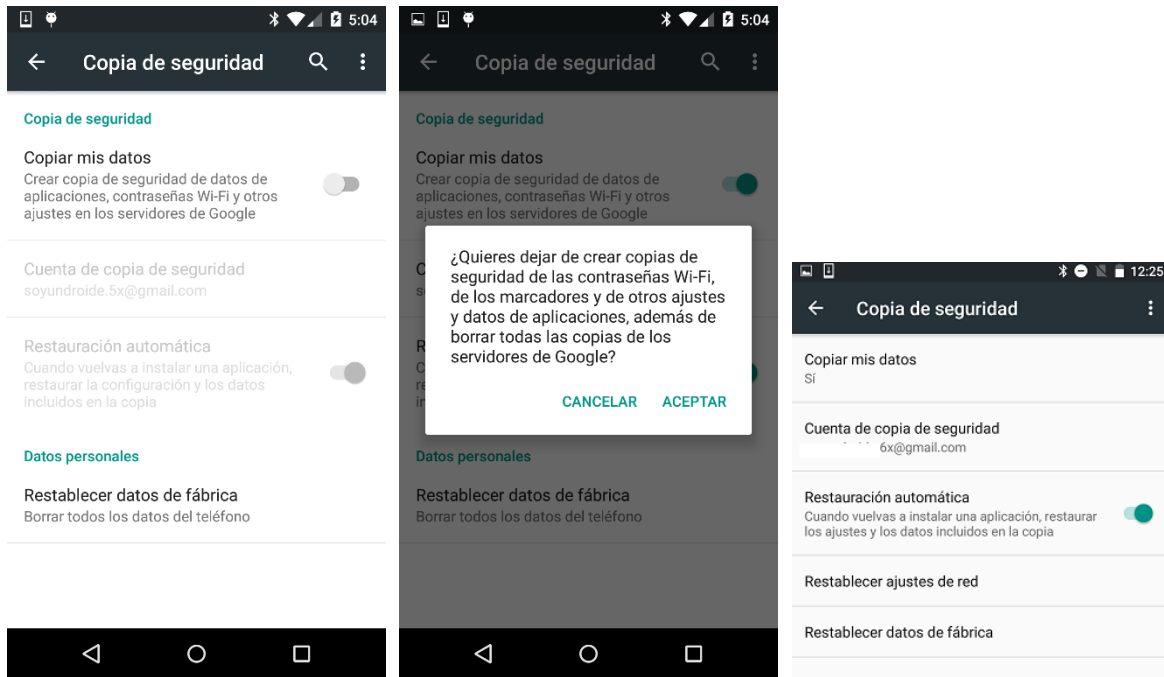
1764. El servicio de copia de seguridad de datos de Google (denominado *Android Backup Service*) permite almacenar información personal y datos del usuario en los servidores de Google, como los favoritos de navegación web, palabras añadidas al diccionario, una lista de las apps instaladas, parámetros de configuración y los datos utilizados por las apps de terceros, las contraseñas de las redes Wi-Fi, la mayoría de parámetros de configuración del dispositivo móvil y de los servicios de Google, etc., siendo posible restaurar los datos posteriormente si fuese necesario reemplazar el dispositivo móvil o reinstalar una app [Ref.- 104].
1765. Durante el proceso de instalación y configuración inicial de Android y vinculación del dispositivo móvil (ver apartado “24. Apéndice A: Proceso de instalación y configuración inicial”) a una cuenta de usuario de Google (y/o de creación de la cuenta) se solicita confirmación por parte del usuario para activar el servicio de copia de seguridad de datos (ver apartado “20. Cuenta de usuario de Google”).
1766. En el caso de dispositivos móviles Android multi-usuario, únicamente el usuario propietario (o usuario principal) puede gestionar las opciones de copia de seguridad y restauración.
1767. El servicio de copia de seguridad de datos en los servidores de Google puede ser activado o desactivado posteriormente a través del menú “Ajustes [Personal] - Copia de seguridad”, y en concreto, mediante la opción “Copiar mis datos” (siendo necesario disponer de una cuenta de usuario de Google vinculada al dispositivo móvil).



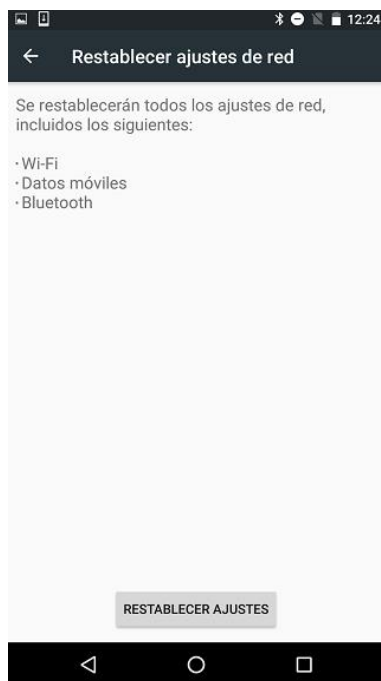
1768. En el caso en que existan varias cuentas de usuario de Google en el dispositivo móvil, será necesario elegir la cuenta de la cual se realizará la copia de seguridad (no es posible realizarla de más de una cuenta). Para seleccionarla, se debe pulsar sobre “Cuenta de copia de seguridad”:



1769. Al desactivar la opción, no se llevarán a cabo más copias de seguridad de los datos en la cuenta de usuario de Google asociada, y las copias de seguridad existentes serán (supuestamente) eliminadas de los servidores de Google.



1770. Si se reinstala una app de terceros (desde Google Play), el servicio puede almacenar y restaurar la configuración y los datos asociados a la app (algunas apps pueden no permitir la realización de copias de seguridad y la restauración de sus datos).
1771. La opción “Restauración automática” permite restaurar la configuración y los datos asociados a una app al instalarla (o reinstalarla) en el dispositivo móvil desde la copia de seguridad disponible en los servidores de Google. Si la app fue instalada y usada en el mismo, o en otro dispositivo móvil, en el que se disponía del servicio de copia de seguridad de datos activo con la misma cuenta de usuario de Google, toda la información de la app será recuperada.
1772. En caso de que el usuario reemplace, sustituya o renueve su dispositivo móvil, este servicio ofrece la posibilidad de restaurar los datos desde la copia de seguridad de Google en el nuevo dispositivo móvil la primera vez que se accede a Google con la cuenta de usuario asociada a este servicio.
1773. Los datos que serán restaurados incluyen, entre otros, los ajustes de calendario y Gmail, los datos de redes Wi-Fi (incluyendo las credenciales y contraseñas de acceso), la configuración de la pantalla de inicio, los ajustes de idioma e introducción de texto, la lista de apps instaladas desde Google Play, junto a sus datos y ajustes de configuración, etc. [Ref.- 104].
1774. La opción “Restablecer ajustes de red” eliminará cualquier configuración que se haya realizado a nivel de comunicaciones en el dispositivo (incluyendo las contraseñas de las redes Wi-Fi, las redes añadidas manualmente, los emparejamientos Bluetooth, etc.):



1775. El usuario u organización propietaria del dispositivo móvil Android debe evaluar en detalle el nivel de confianza depositado en Google para emplear este servicio y almacenar todos los datos personales y confidenciales de los usuarios en el mismo.

### 21.3. COPIA DE SEGURIDAD DE FOTOS Y VÍDEOS

1776. El servicio de copia de seguridad de datos de Google (descrito en el apartado previo) no incluye las fotos (o fotografías) y vídeos disponibles en el dispositivo móvil.

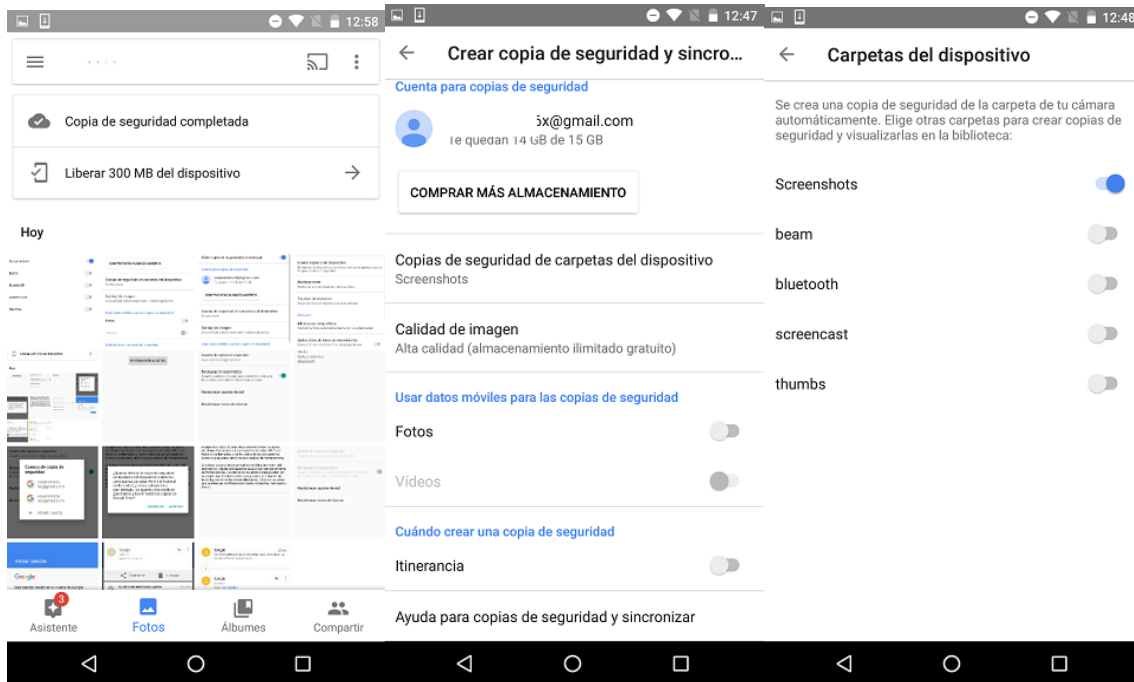
1777. Para hacer una copia de seguridad de las fotos y vídeos automáticamente en la cuenta de usuario de Google es necesario configurar el servicio de copia de seguridad de fotos y vídeos de Google, disponible a través de la app “Fotos” [Ref.- 177]. Al activar este servicio, la copia de seguridad de las fotos y vídeos es (supuestamente) privada, salvo que el usuario decida compartirlas.

1778. Las fotos (y vídeos) incluyen tanto las realizadas con la cámara del terminal, como las capturas de pantalla (*screenshots*), las descargadas desde Internet (*download*) y las que almacenan otras apps, como por ejemplo Hangouts.

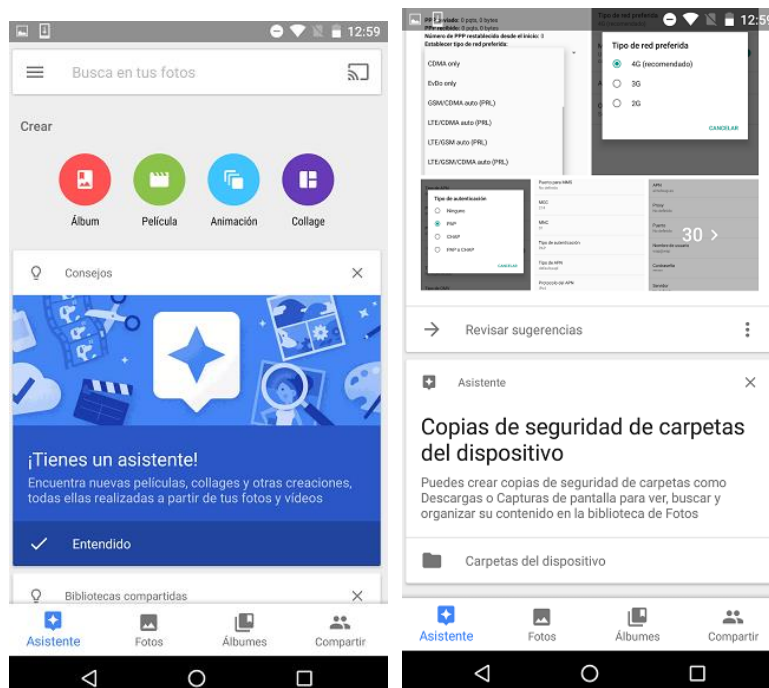
1779. La primera vez que se ejecuta la app “Fotos” se consulta al usuario si quiere hacer copias de seguridad automáticamente de las fotos y vídeos, y si la transferencia de estos contenidos multimedia hacia la cuenta de usuario en Google se hará a través de redes Wi-Fi y redes de telefonía móvil (2/3/4G), con un posible gasto asociado, o sólo mediante redes Wi-Fi.

1780. Es posible activar o desactivar las copias para carpetas concretas mediante la app “Fotos”, desde el botón de menú superior izquierdo, y la opción “Ajustes - Copia de seguridad y sincronización - Crear copia de seguridad y sincroniz...”. Por defecto, únicamente se realizará la copia de la carpeta asociada a la cámara del dispositivo móvil. Si se desea salvar el contenido de otras carpetas, se deberán activar los interruptores correspondientes a ellas (*Screenshots* para capturas de pantalla, *bluetooth* para las imágenes recibidas por Bluetooth, etc.):





1781. Además, el denominado “Asistente” (accesible desde el menú inferior de la app “Fotos”) mostrará tarjetas informando sobre las distintas opciones de configuración: qué carpetas de las existentes en el dispositivo móvil se copiarán (además de las fotos y vídeos realizados con la cámara del dispositivo móvil, es posible incluir en la copia de seguridad las imágenes correspondientes a las capturas de pantalla, *screenshots*, las descargadas desde Internet o por Bluetooth, y las que almacenan otras apps), cuáles se desea archivar, crear álbumes, etc.:

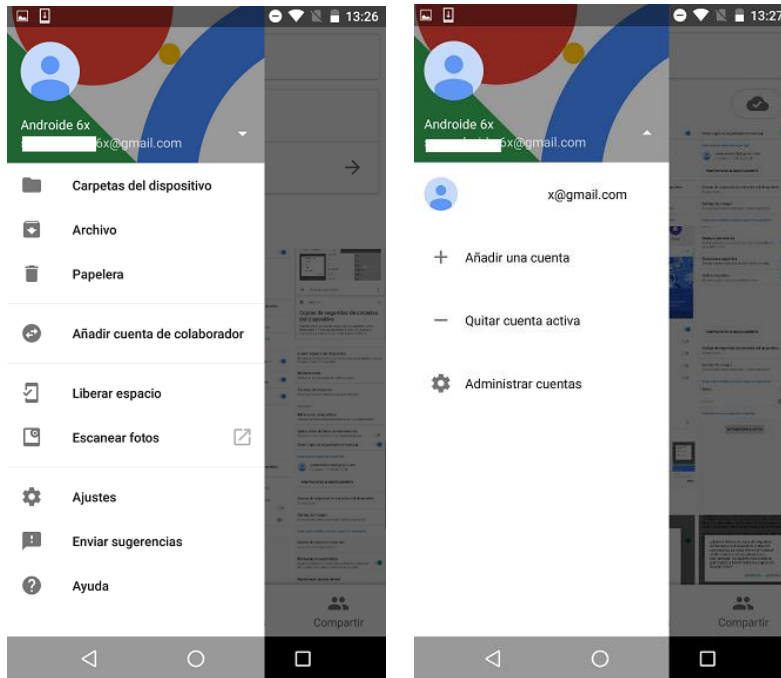


1782. Desde el punto de vista de seguridad se recomienda tener un control estricto de la copia de fotos y vídeos entre los diferentes servicios de Google y no habilitar estas capacidades, salvo que se quiera hacer un uso explícito de las mismas. Se dispone de opciones de configuración (descritas a continuación) para controlar estas funcionalidades.

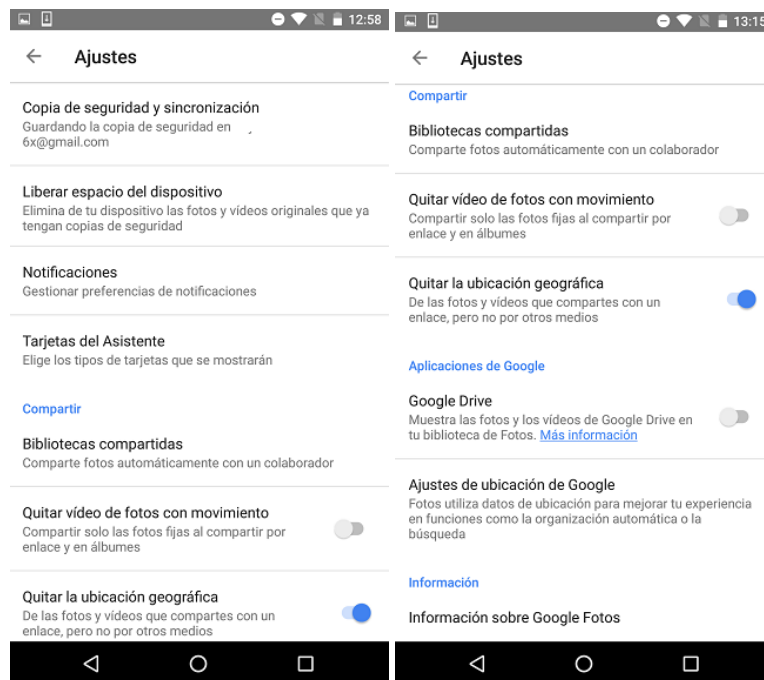
1783. Al habilitar la funcionalidad “Crear copia de seguridad y sincro... - Crear copia de seguridad y sincronizar”, será posible acceder a otros ajustes de configuración avanzados, disponiéndose de información de la cuenta de usuario de Google asociada, del espacio disponible (15 GB por defecto en el momento de elaboración de la presente guía), y detalles como la calidad de la imagen (alta u original), la posibilidad de “Comprar más almacenamiento” con un coste asociado y las carpetas sobre las que se realizará la copia.



1784. Las secciones “Usar datos móviles para las copias de seguridad” y “Cuándo crear una copia de seguridad” permiten respectivamente establecer los ajustes del tipo de redes a emplear para realizar las copias de fotos y vídeos por separado (mencionadas inicialmente) y si se desea hacer uso de la funcionalidad en itinerancia (redes móviles en el extranjero). Se recomienda deshabilitarlas (para evitar incurrir en gastos de telefonía móvil inesperados) y valorar si se desea hacer uso del servicio cuando llegue el momento.
1785. La cuenta de usuario de Google vinculada al dispositivo móvil y en la que se están almacenando las fotos y vídeos se muestra en la parte superior de los ajustes de la app “Fotos” y, pinchando sobre ella, es posible eliminarla o añadir más cuentas de usuario de Google adicionales.

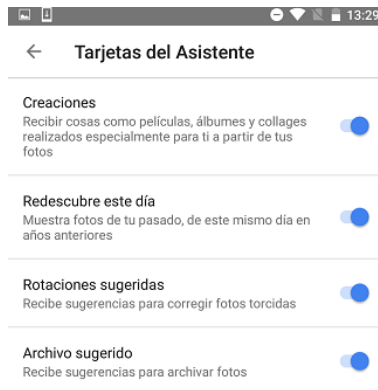


1786. Dentro del menú de “Ajustes” de la app “Fotos” para la cuenta de usuario de Google, es posible configurar si estarán disponibles en Google Fotos las fotos y vídeos de Google Drive, y si se incluirá la ubicación geográfica de las fotos en los álbumes compartidos, pudiéndose cambiar esta configuración mediante la opción “Compartir - Quitar la ubicación geográfica”:

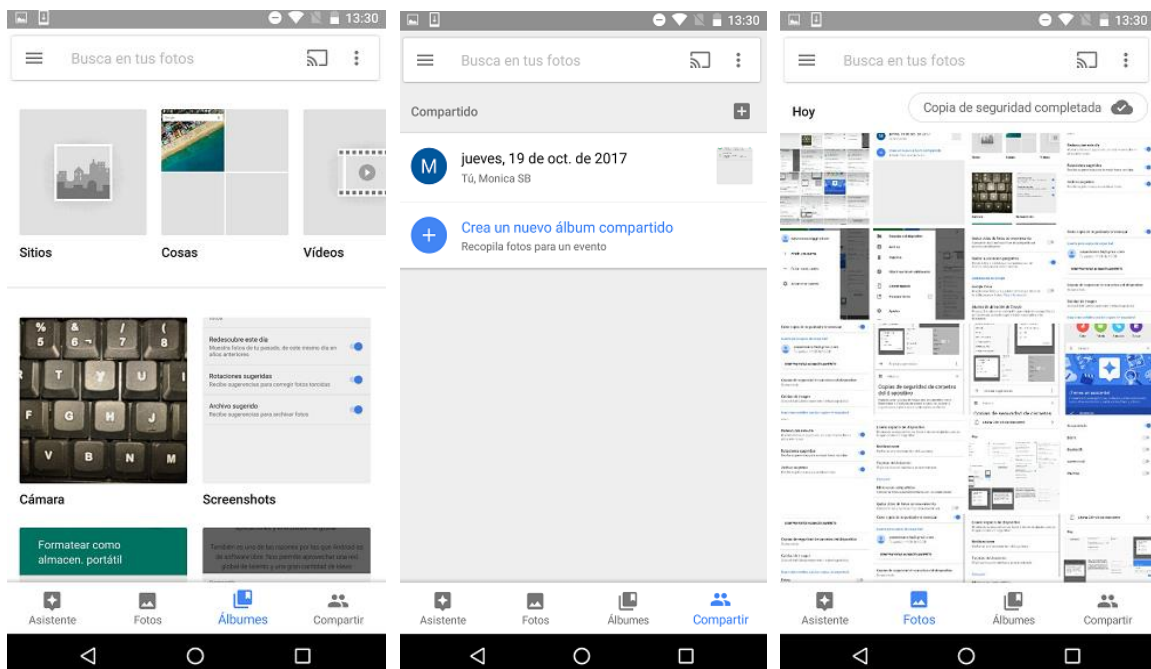


1787. El apartado de “Notificaciones” permite habilitar/deshabilitar las notificaciones de la app “Fotos”. Entre otras, se puede habilitar/deshabilitar la opción “Notificaciones de sugerencias para...”, que se encarga de enviar notificaciones cuando se disponga de nuevas fotos para compartir.

1788. El menú “Tarjetas del asistente” activará las tarjetas de Google Now correspondientes a la aplicación “Fotos” (ver apartado “22. App Google: Asistente de Google, Mi Tablón y Servicios de Búsqueda de Google”).

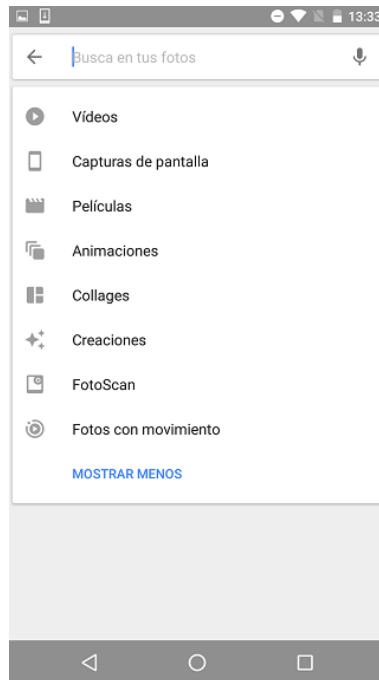


1789. En el menú situado en el margen inferior, se pueden visualizar los “Álbumes” disponibles (algunos de los cuales son proporcionados por defecto según la propia clasificación de la app “Fotos”), “Compartir” un álbum y ver qué se ha compartido con otros usuarios o acceder a “Fotos” para verlas según la clasificación por fecha:



1790. En el pasado, entre las etiquetas asociadas a las fotos (sitios, cosas, vídeos, etc.) existía la categoría “personas”. Esta categoría no se muestra en la versión de la app “Fotos” empleada para la elaboración de la presente guía.

1791. La barra de búsqueda, al ser seleccionada, permitirá realizar búsquedas por categoría:

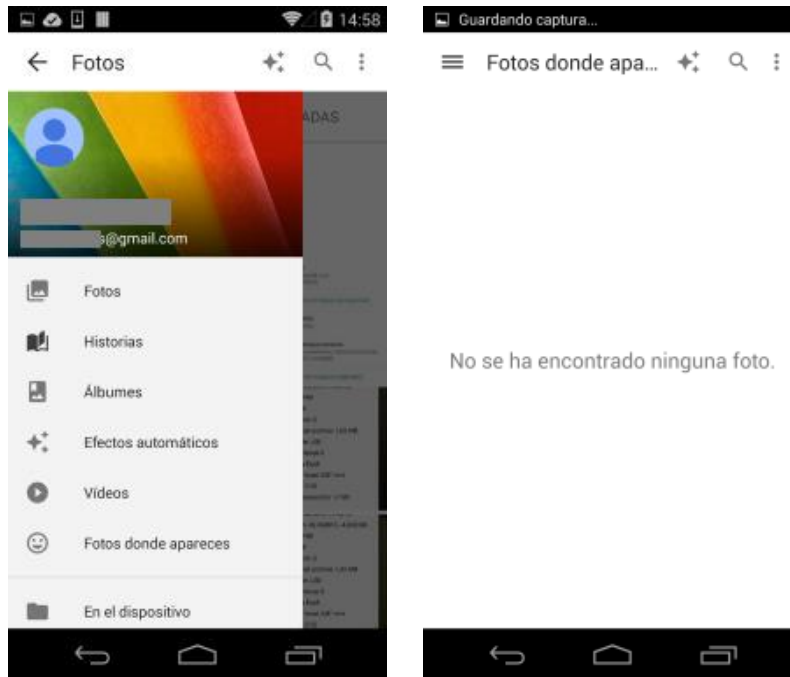


1792. En versiones anteriores de Android, existía la opción "Reconóceme" [Ref.- 178], por medio de la cual se permitía a Google+ solicitar a otros usuarios que se etiquetaran entre ellos en fotos y vídeos, a fin de que fuese posible identificarlos con más facilidad (por cuestiones de seguridad y privacidad, no se recomienda habilitar la integración entre Google + y la app "Fotos").

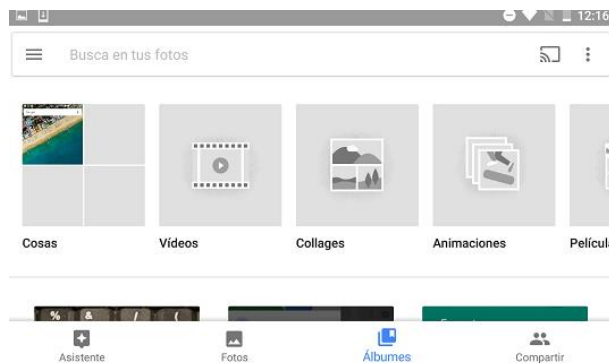
1793. Al activar esta funcionalidad, Google+ creaba un modelo de la cara del usuario en base a las fotos y vídeos en los que ya estaba etiquetado [Ref.- 179]. Este modelo se actualizaba con las nuevas fotos y vídeos recibidos, y podía ser eliminado desactivando esta opción en cualquier momento.

1794. En base a dicho modelo de cara, Google mostraba una sugerencia de etiqueta tanto al usuario como a sus conocidos cuando identificaba ese modelo o patrón de la cara del usuario en una nueva foto o vídeo. Si se desactivaba esta opción, los conocidos del usuario dejaban de recibir sugerencias para etiquetar al usuario en las fotos o vídeos, sin embargo, las etiquetas ya añadidas no se eliminaban.

1795. En versiones posteriores de la app "Fotos", existía una sección denominada "Fotos donde apareces", disponible desde el menú superior izquierdo, que permitía aprobar o rechazar etiquetas (respondiendo a la pregunta "¿Eres tú?"), así como revisar las fotos en las que el usuario había sido etiquetado [Ref.- 179]:

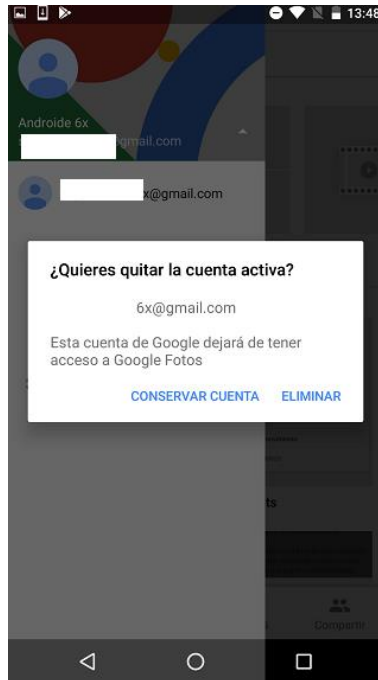


1796. Si se rechazaba la etiqueta, ésta sería eliminada de la foto. Una vez se aprobaba una etiqueta, ésta se asociaba al perfil de Google+ del usuario, y la foto era incluida en la sección “Fotos donde apareces”.
1797. Para eliminar una etiqueta, desde esta misma sección, se requería seleccionar la foto etiquetada y, mediante el icono con una etiqueta en forma de cara de la parte inferior, emplear el icono de borrar (o papelera).
1798. En las versiones más recientes de la app “Fotos”, se dispone de una barra de búsqueda en la parte superior del menú en la que se muestran categorías para simplificar las búsquedas. Estas categorías son: sitios, cosas, vídeos, collages, animaciones y películas.



1799. Adicionalmente, y en función del país que se haya configurado en el dispositivo móvil, pueden aparecer también “personas” y “mascotas”, sobre los cuales también es posible aplicar etiquetas para agruparlos y clasificarlos. Tal y como se indica en la documentación oficial de Google para búsquedas en fotos [Ref.- 633], esta funcionalidad no está disponible en todos los países, y, concretamente, no lo está en España.
1800. Por el anterior motivo, y porque desde el punto de vista de seguridad y de la privacidad del usuario no se recomienda habilitar funcionalidades de reconocimiento del usuario a través de fotografías y vídeos, se desaconseja el hacer uso de las mismas, aunque se disponga de una configuración que sí lo permita.

1801. Finalmente, la opción “Quitar cuenta activa” permite finalizar la sesión actual asociada a la cuenta de usuario de Google, incluida la vinculación entre éste y las fotos y vídeos del dispositivo móvil. Para poder hacer uso de la funcionalidad descrita es necesario volver a añadir una cuenta a través del botón de menú y la opción “Ajustes - Añadir cuenta”:



#### 21.4. COPIA DE SEGURIDAD AUTOMÁTICA DE LOS DATOS DE LAS APPS

1802. Con la introducción de Android 6.x y de la API de nivel 23, se añadió una característica denominada “Auto Backup for Apps” [Ref.- 635], consistente en permitir a las apps definir una política para decidir si hacen uso de las capacidades para salvaguardar los datos (del usuario) en la app en la cuenta de Google Drive asociada a la cuenta de Google del usuario configurada en el dispositivo móvil [Ref.- 634].

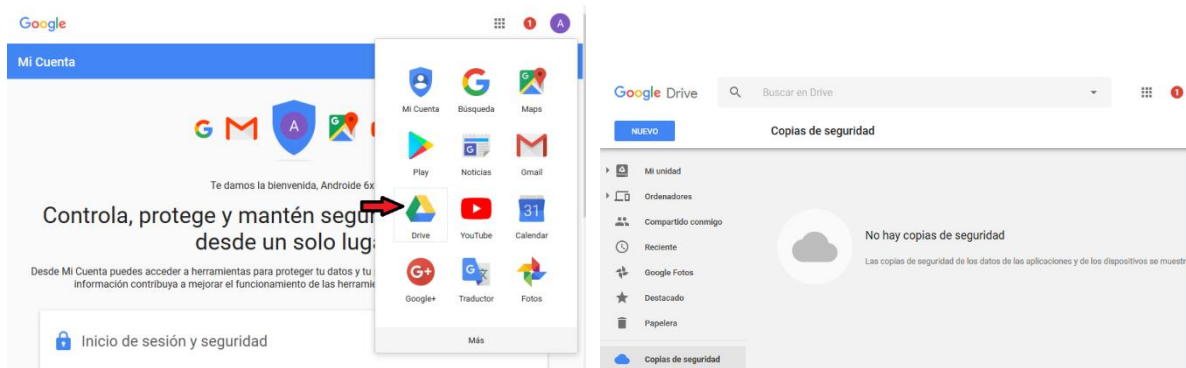
1803. Entre los datos asociados a una app, se distinguen tres categorías:

- “Identity data” (datos de identidad): permiten simplificar el acceso a la app por parte del usuario cuando se instala la app en un nuevo dispositivo móvil, sin tener que introducir de nuevo las credenciales. Para que una app pueda ofrecer esta posibilidad, ha de adoptar el servicio “Google Sign-In” [Ref.- 263], por el cual la autenticación dentro de la app se llevará a cabo utilizando las credenciales de la cuenta de Google del usuario. Adicionalmente, la app dispondrá de acceso a la información que el usuario haya publicado en su perfil de la cuenta de Google.
- “App data” (datos de la aplicación): corresponden al contenido generado por el usuario durante su uso de la app como, por ejemplo, ficheros descargados, imágenes guardadas, etc.
- “Settings data” (ajustes de la aplicación): corresponden a los cambios realizados sobre la configuración por defecto de la app por parte del usuario, como el lenguaje, un tono de aviso, el bloqueo de una acción determinada, etc.

1804. Las opciones de backup disponibles para las apps (siendo ambas excluyentes) son:



- **Auto Backup for Apps:** los datos de la app se salvaguardan en la cuenta de usuario de Google Drive, con un límite de 25 MB por app (que no se descuentan del almacenamiento disponible para el usuario en Google Drive). Los detalles de los ficheros que se almacenan se describen en la documentación de Android para desarrolladores [Ref.- 264], y el usuario puede comprobar qué apps emplean este servicio a través del interfaz de administración de su cuenta de Google, mediante “Drive - Copias de seguridad”.



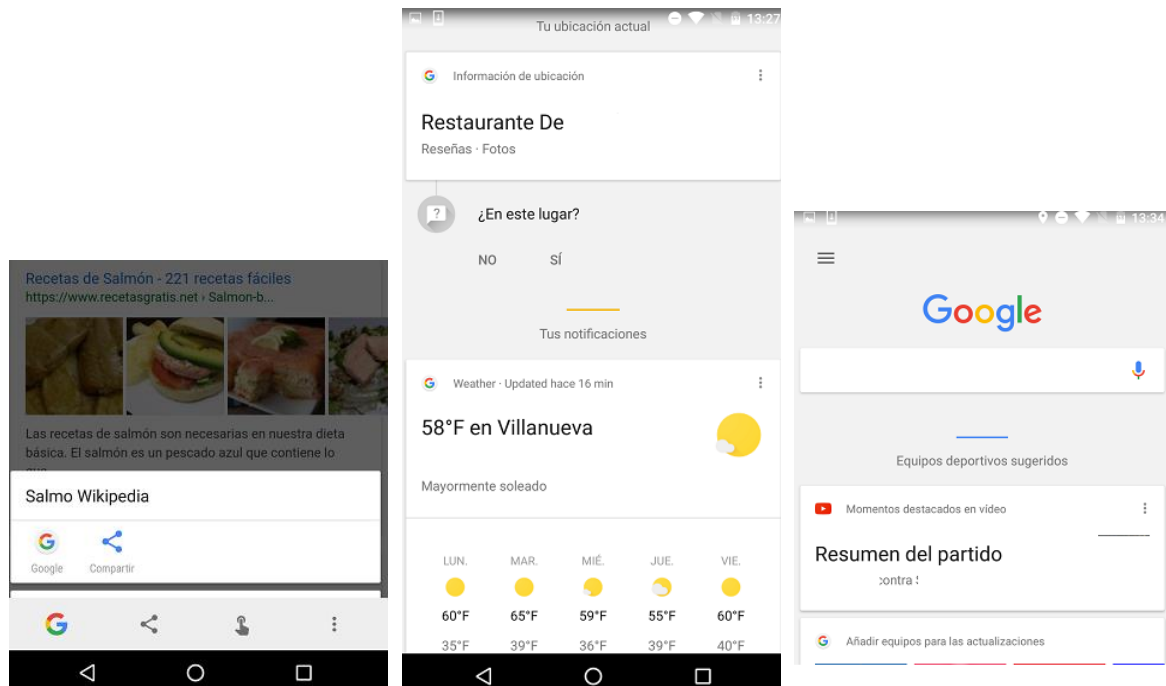
- **Key/Value Backup (clave/valor):** la app debe definir explícitamente qué contenido desea guardar empleando un formato clave-valor. Para ello, deberá implementar dentro de su código un cliente de backup, el cual define qué datos se salvaguardarán y cómo se restaurarán cuando sea invocado por su gestor de backup durante los procesos de copia y restauración [Ref.- 265]. Este método se denominaba anteriormente “Android Backup Service”, y está disponible desde Android 2.2 (API 8) y superiores.
1805. El mecanismo de “Android Auto Backup” permite a las apps incluir y excluir ficheros de la copia de seguridad, y el proceso de backup se realiza de forma automática una vez al día, siempre que el dispositivo móvil tenga acceso a una red Wi-Fi (no puede llevarse a cabo a través de la conexión de datos de telefonía móvil).
  1806. Para poder salvar sus datos a través del mecanismo de “Android Auto Backup”, la app será cerrada por el sistema.
  1807. El mecanismo de “Key/Value Backup” sí puede realizarse sobre una conexión de datos móviles, y es la app la que debe informar de cuándo tiene datos que desea salvar. El sistema no cerrará la app durante el proceso de backup.
  1808. El límite de datos que se pueden salvar a través del mecanismo “Key/Value Backup” es de 5MB por aplicación.
  1809. Dado que es la app y no el usuario quien declara el tipo de servicio de backup que se debe emplear, el único ajuste disponible para el usuario es el de decidir si desea hacer uso del servicio de backup en los servidores de Google a través de “Ajustes - [Personal] Copia de seguridad - Copiar mis datos”, pero será la implementación de la app la que decida el mecanismo a emplear en caso de estar activo el servicio.
  1810. Debe tenerse en cuenta que, si el usuario deshabilita por completo el servicio de copias de seguridad en los servidores de Google, se deshabilitarán tanto las capacidades de copias automáticas de las apps, como las capacidades de backup mediante ADB.

## 22. APP GOOGLE: ASISTENTE DE GOOGLE, MI TABLÓN Y SERVICIOS DE BÚSQUEDA DE GOOGLE

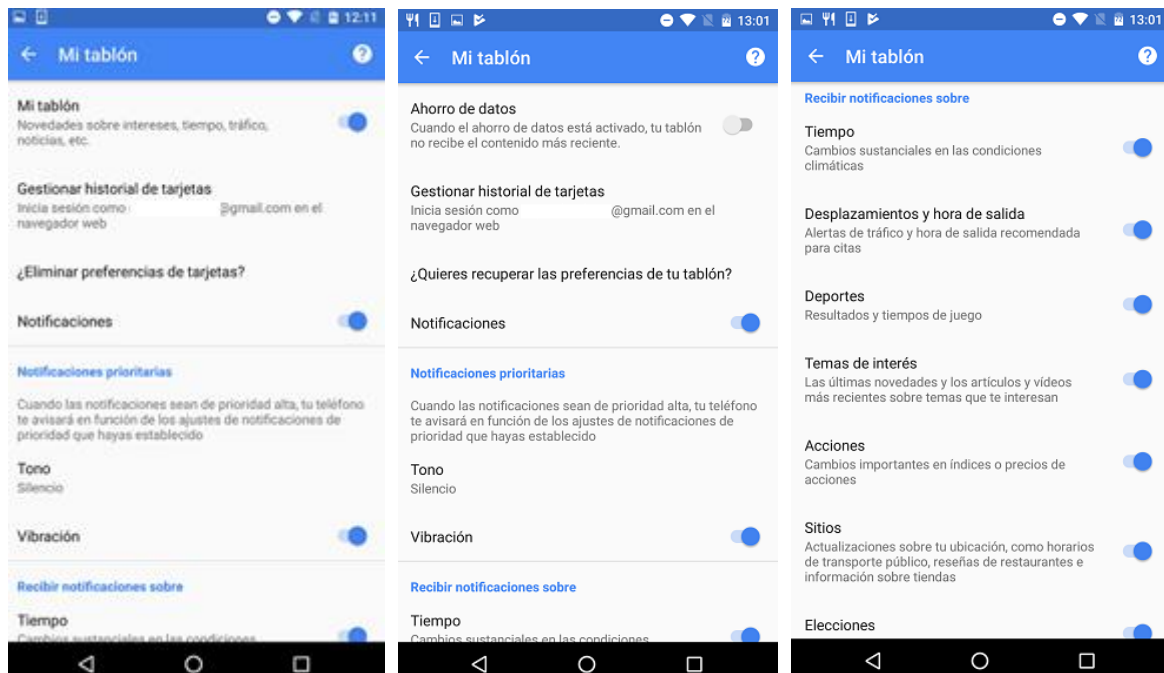
1811. Android 4.1 (“Jelly Bean”) introdujo en 2012 “Google Now”, un asistente personal que se incluyó como un servicio de la aplicación Google Search. Éste hacía uso de una interfaz de usuario de lenguaje natural para responder preguntas, hacer recomendaciones y realizar acciones transmitiendo la petición del usuario a los servicios web correspondientes. Además de responder a consultas del usuario, Google Now ofrecía información al usuario, de forma pasiva, sobre aspectos que podían ser de su interés en función de los hábitos de búsqueda recopilados por las aplicaciones y servicios.
1812. Google Now ha ido evolucionando a lo largo de los años, ampliando su funcionalidad y adaptándose a las aplicaciones del ámbito y ecosistema de Google.
1813. Con las versiones recientes de la aplicación Google (incluyendo la versión 7.14.21.21 empleada en la elaboración de la presente guía), los servicios anteriormente conocidos como “Google Now” se englobaron en lo que pasó a denominarse “*feed*” o “Google Feed”, y se configuran en la nueva versión de la app a través del menú “Mi tablón” de la aplicación Google. Para más información, se recomienda consultar la documentación oficial de usuario de Google [Ref.- 624] [Ref.- 625].

**Nota:** Las opciones de configuración de la aplicación Google son extremadamente dependientes de la versión de la app, por lo que algunos de los puntos descritos en el presente apartado pueden no corresponder con los existentes en otros dispositivos móviles con versiones de la aplicación Google diferentes.

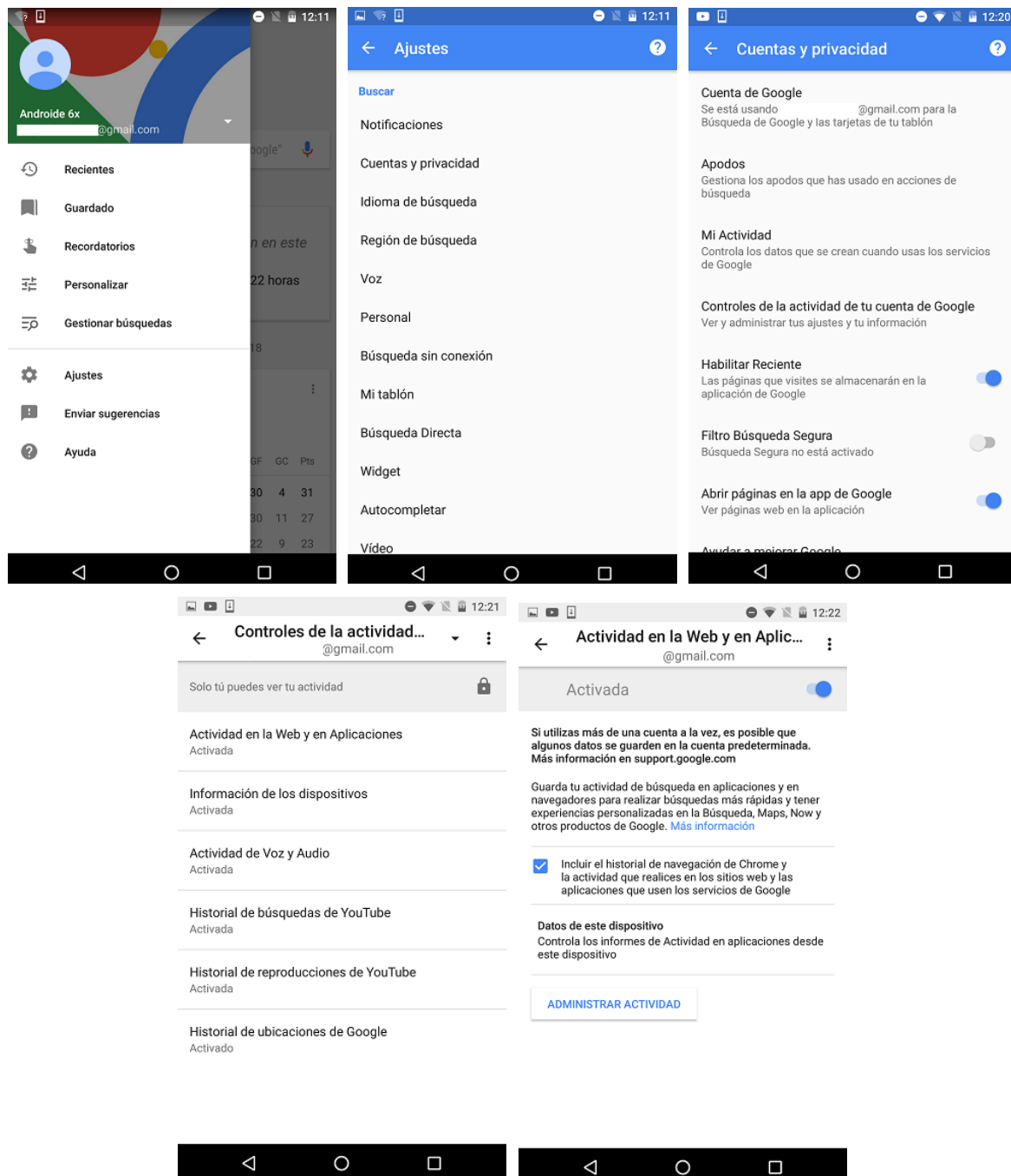
1814. El presente apartado utilizará la nomenclatura empleada por Google a fecha de la elaboración de la presente guía para a los servicios relativos al “*feed*” (o “Google Feed”), es decir “Tablón”, en lugar del término “Google Now” de versiones anteriores de Android.
1815. Los servicios asociados a “Mi Tablón” ejecutan en segundo plano, analizando los datos de la actividad diaria del usuario, su ubicación (e histórico de ubicaciones) y mostrando las tarjetas de información (anteriormente conocidas como tarjetas “Google Now” o tarjetas Now) o notificaciones en función de los eventos que ocurren en tiempo real.
1816. El “Tablón” proporciona su información principalmente a través de la app “Google”, disponible para la realización de búsquedas a través del buscador de Google. La app “Google” está disponible desde una de las pantallas de inicio, desde el *Launcher*, o realizando una pulsación prolongada sobre el botón de inicio (en lugar de deslizando la pantalla desde la parte inferior hacia arriba, como ocurría en la versión 5.1.1 de Android) y permite ver las tarjetas existentes, siempre que se disponga de conexión de datos (Wi-Fi o 2/3/4G):



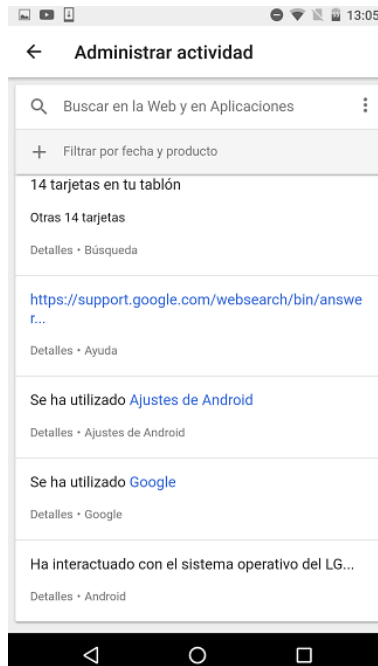
1817. La app Google es el interfaz que permite gestionar las búsquedas (de texto, voz, contenido multimedia, etc.) y otras actividades diversas asociadas a la cuenta de usuario de Google activa en el dispositivo móvil y relativas a aplicaciones de Google. Esta app ha evolucionado desde sus orígenes y está en constante evolución, de forma que resulta muy cambiante entre versiones de la propia app y/o de Android.
1818. Es importante reseñar que las opciones de configuración son muy dependientes de la versión de la app Google que esté instalada. La documentación descrita en la presente guía corresponde a las opciones de la versión de la app Google de noviembre de 2017, disponible para Android 6.0.1. Por tanto, en función de la versión de esta aplicación, los menús y opciones pueden variar y no corresponder con los aquí expuestos. Para conocer la versión de la app instalada, se puede consultar desde el menú “Ajustes - Información” de la app Google, o desde el menú general “Ajustes - [Dispositivo] Aplicaciones - Google”.
1819. La activación de “Mi Tablón” se puede llevar a cabo durante el proceso de instalación y configuración inicial de Android (ver apartado “24. Apéndice A: Proceso de instalación y configuración inicial”), cuando se da de alta una cuenta de usuario de Google en el dispositivo móvil (si no se hizo durante la instalación), o posteriormente a través de los ajustes de la aplicación Google.
1820. Si bien en la versión de la app Google que viene por defecto con Android 6.0.1 era posible activar/desactivar “Mi Tablón” con un único interruptor, como se muestra en la imagen inferior izquierda, en las versiones más recientes de la app Google no existe un único botón que active/desactive globalmente el *feed*, sino que es necesario marcar/desmarcar una a una todas las categorías del tablón, como se ilustra en las imágenes central e inferior derecha:



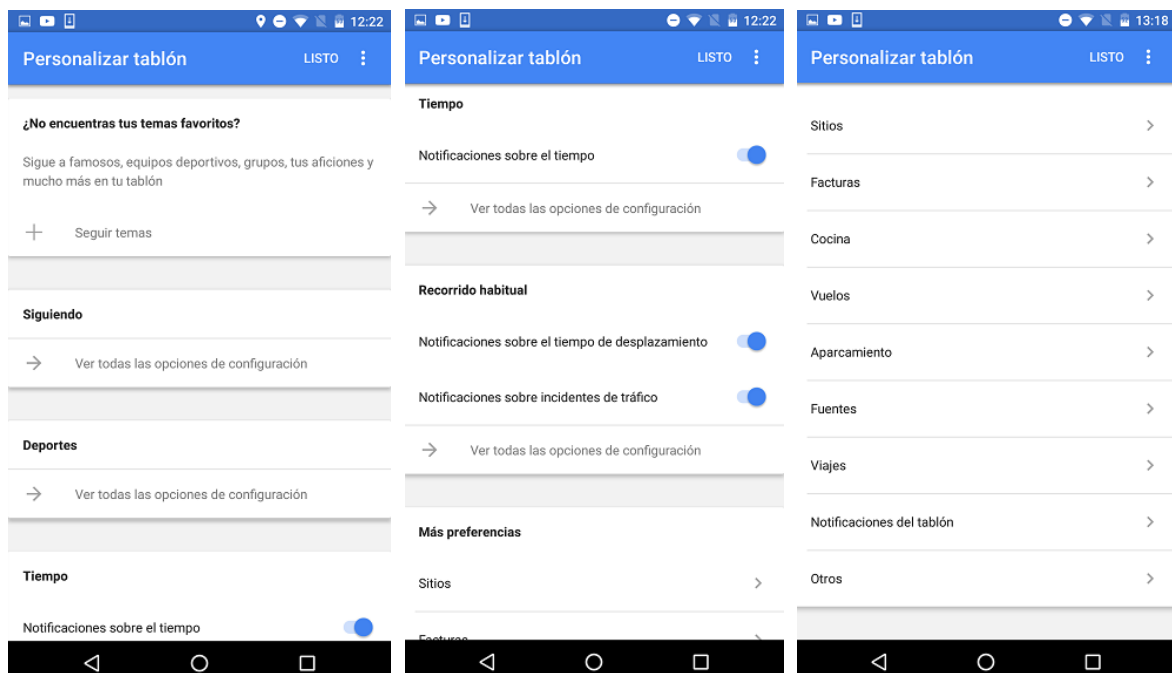
1821. El servicio “Mi tablón” hace uso de los servicios de ubicación (incluyendo el historial de ubicaciones; ver apartado “12.5. Historial de ubicaciones”), datos del calendario del usuario, sus búsquedas web (incluyendo el historial web; ver apartado “23.1.3. Historial de actividad web”) y otros datos del usuario disponibles en los productos y servicios de Google (y/o de terceros).
1822. Desde el punto de vista de seguridad y privacidad, salvo que se desee hacer uso de la funcionalidad ofrecida por el *feed*, se recomienda no activar estas capacidades, debido a que conllevan un uso y análisis intensivo y muy detallado de los datos y actividades diarias del usuario y su cesión a Google.
1823. Si bien en versiones de la app Google anteriores a la analizada en la presente guía el *feed/Google Now/Tablón* puede ser activado y desactivado simplemente poniendo a *on/off* el botón “Mi Tablón” (para más detalles, se recomienda consultar el capítulo 22 de la guía “Guía CCN-STIC-453C - Seguridad de dispositivos móviles: Android 5.x” [Ref.-405]), en la versión analizada en la presente guía esta configuración resulta más compleja y menos intuitiva para el usuario.
1824. Así, para configurar el “Tablón”, es necesario abrir la app Google, seleccionar las líneas horizontales del menú e ir a “[Ajustes de la app Google] - Cuentas y privacidad - Controles de la actividad de tu cuenta de Google - Actividad en la Web - Aplicaciones”.



1825. Una vez activado el botón “Actividad en la Web y en Aplicaciones”, Google comenzará a recabar múltiples datos sobre toda la actividad del usuario, como se ilustra en la siguiente imagen:



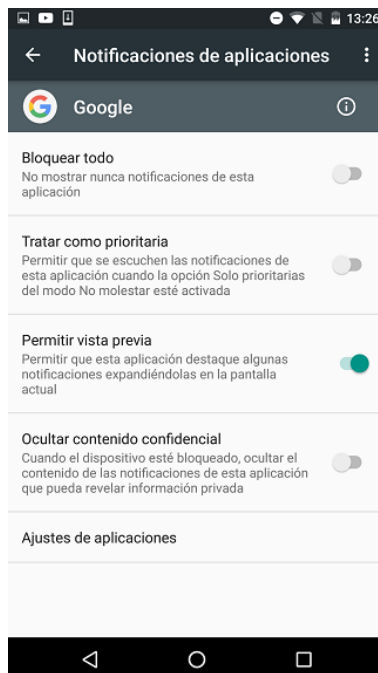
1826. Para configurar las tarjetas que se desee recibir, hay que elegir “Personalizar” en el menú de ajustes de la app Google:



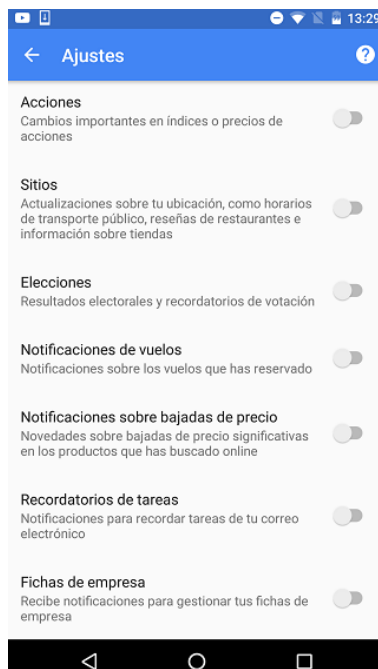
1827. Dada la ingente cantidad de datos personales y potencialmente sensibles que recopila la funcionalidad “Mi Tablón”, desde el punto de vista de seguridad y privacidad se desaconseja vehementemente deshabilitar completamente dicha funcionalidad.

**Nota:** La aplicación Google se representa como una circunferencia con una G de varios colores desde las últimas versiones, pero, en versiones más antiguas, como en la versión que se instala por defecto con la versión 6.0 de Android, se representaba como una G de color azul rodeada de un círculo blanco.

1828. Para no recibir notificaciones del feed de forma puntual, se puede acceder al menú “Ajustes - [Dispositivo] Sonido y notificaciones - Notificaciones de aplicaciones - Aplicación Google”. Para eliminar cualquier tipo de notificación basta con mover a la posición de activación del botón “Bloquear Todo”:

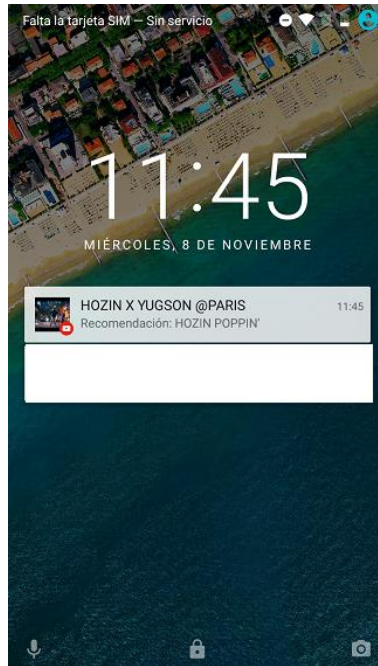


1829. Si se desea desactivar sólo ciertas categorías de notificación, se debe acceder al apartado “Ajustes de aplicaciones” del menú anterior y marcar/desmarcar las opciones deseadas:



1830. Con el servicio “Mi Tablón” activo, se recibirán las notificaciones correspondientes a las categorías habilitadas en el menú anterior:





1831. Además de configurar el servicio de *feed* mediante “Mi tablón”, los ajustes de la aplicación Google incluyen otros apartados, entre los cuales figuran:

- Cuentas y privacidad: se detalla en el apartado “22.2. Cuentas y privacidad”.
- Idioma de búsqueda: por defecto, se usa el idioma definido en la instalación, pero se puede cambiar por otro (no es posible tener varios idiomas simultáneos).
- Voz: configurar el idioma y otras capacidades asociadas a las búsquedas por voz, e incluye la “Detección de OK Google”. Para más información, consultar el apartado “22.3. Asistente personal y “Ok Google””.
- Búsqueda directa, que corresponde a la funcionalidad “Now on Tap” descrita en el apartado “22.1- Google “Now on Tap”” (en versiones más antiguas de la app Google, este campo corresponde a “En aplicaciones” o “Búsqueda en teléfono”): permite a las capacidades de búsqueda de Google utilizar las opciones seleccionadas para consultar información y transferirla al *feed*.
- Vídeo: controla si los vídeos se empezarán a reproducir automáticamente y si lo harán sólo con conexión Wi-Fi o también con conexión a redes de datos móviles.

## 22.1. GOOGLE “NOW ON TAP”

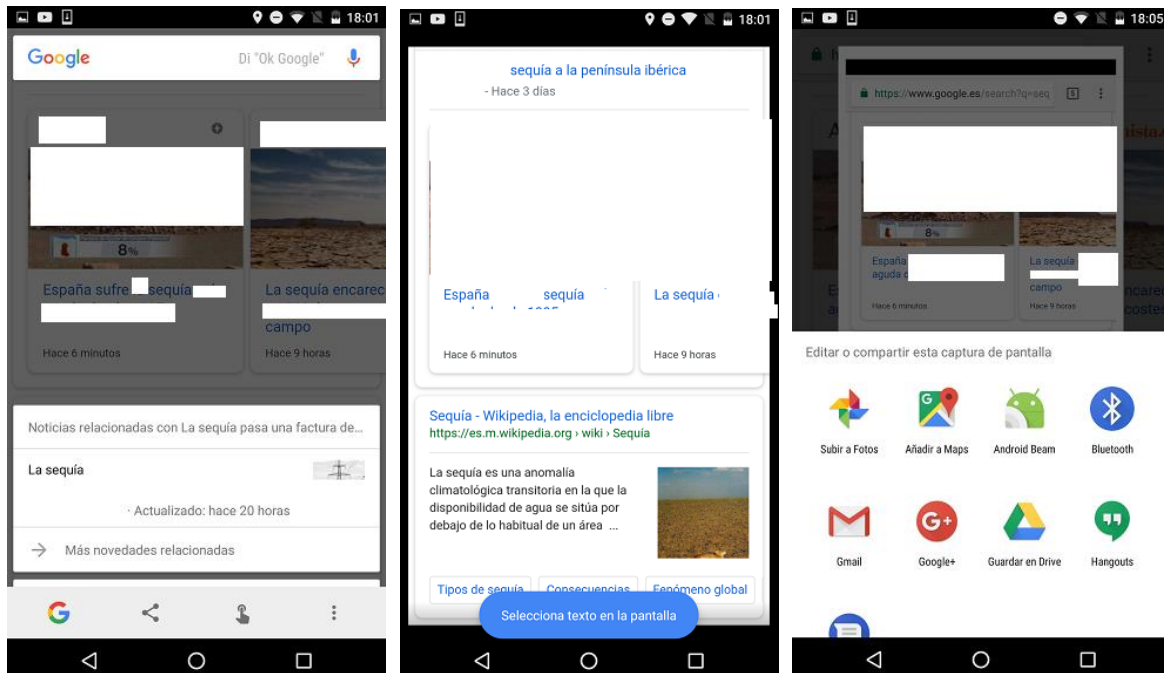
1832. Android 6.0 (Marshmallow) introdujo la funcionalidad “Now on Tap” o “Búsqueda directa”, concebida como un asistente para proporcionar información contextualizada referente a los contenidos de la aplicación que esté ejecutando en primer plano cuando se invoca la ayuda de “Now on Tap”.

1833. El propósito de esta nueva funcionalidad es facilitar al usuario a través de una sola pulsación la búsqueda en Google sobre elementos que se referencian en las aplicaciones basándose en el contexto de la información concreta que se muestre. Así, por ejemplo, si se tiene abierta la aplicación Google Maps, al invocar “Now on Tap” se lanzará una búsqueda sobre los puntos de interés que allí aparezcan. Si se está mencionando un personaje público en una ventana del navegador web, se mostrará una tarjeta con la información básica de dicha persona.

1834. Con la versión inicial de Android 6.0, la función “Now on Tap” requería que el dispositivo móvil estuviese configurado con idioma inglés para poder ser utilizada. Posteriormente, se incluyeron otros idiomas, entre ellos el español, como configuraciones válidas para acceder a esta funcionalidad.
1835. “Now on Tap” está inhabilitada por defecto, y se requiere seguir una serie de pasos para poder utilizarla, los cuales se detallan a continuación.
1836. En primer lugar, ha de habilitarse el servicio “Mi Tablón”, también conocido como *feed* o, en versiones anteriores, como “Google Now”, siguiendo los pasos detallados en el apartado “22. App Google: Asistente de Google, Mi Tablón y Servicios de Búsqueda de Google”.
1837. En segundo lugar, dentro de los ajustes de la app Google, hay que entrar en el apartado “Búsqueda directa” y activar el botón que aparece en la parte superior de la siguiente imagen:



1838. A partir de ese momento, desde cualquier pantalla de la aplicación que esté en primer plano y pulsando prolongadamente el botón de inicio del dispositivo móvil, será posible buscar información contextualizada o lanzar acciones asociadas al tipo de búsqueda que se esté realizando, por ejemplo:
- Seleccionar texto para obtener detalles: tras pulsar el botón de inicio, aparecerá un menú en la parte inferior de la pantalla que ofrece la posibilidad de seleccionar texto (tocando sobre el icono de una mano con un dedo elevado y marcando el texto sobre el que se desea obtener más detalles).



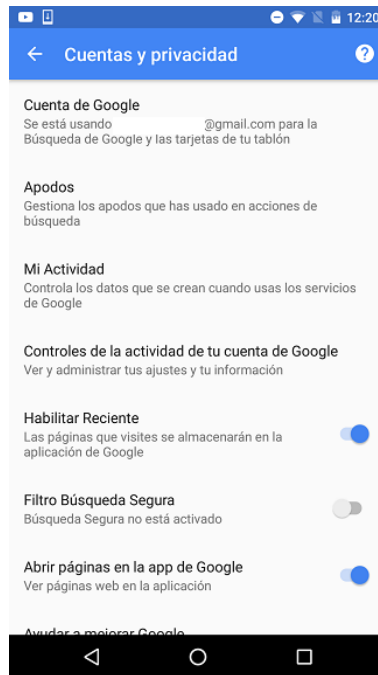
- Compartir la pantalla activa a través de otras aplicaciones (icono correspondiente a un grafo de tres puntos).
- Traducir: seleccionando el icono de tres puntos alineados en vertical (disponible solo para ciertos idiomas).
- Buscar por imagen: al pulsar prolongadamente sobre el botón de inicio cuando haya una imagen en pantalla, Google proporcionará información sobre dicha imagen.
- Buscar con la cámara: si, tras enfocar una imagen con la app “Cámara” se pulsa sobre el botón de inicio, Google proporcionará información sobre dicha imagen.

1839. El apartado “Búsqueda directa” incluye también una opción, deshabilitada por defecto, que permite que se almacenen y revisen las imágenes sobre las que se emplea “Now on Tap” no sólo en la cuenta del usuario, sino en los servidores de Google, a fin de mejorar la funcionalidad del servicio.

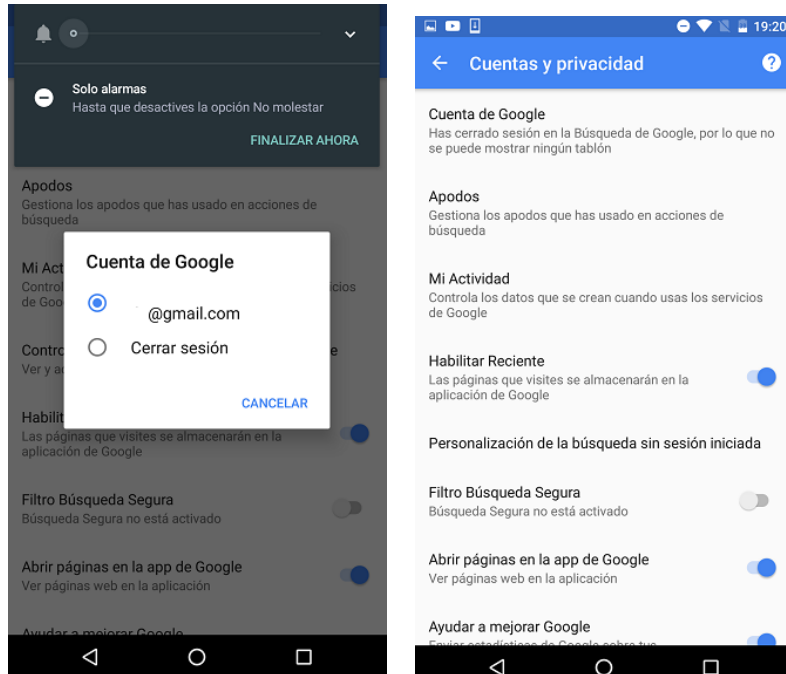
1840. De nuevo, toda la actividad relativa a las búsquedas de “Now on Tap” se envía a los servidores de Google y se almacena en la cuenta del usuario, por lo que, desde el punto de vista de la privacidad, se desaconseja hacer uso de ella.

## 22.2. CUENTAS Y PRIVACIDAD

1841. Bajo este apartado se encuentran las opciones relativas a las búsquedas en Google y del asistente “Mi Tablón” asociadas a la cuenta de Google activa en el dispositivo. Los diferentes campos se describen a continuación. Los marcados con “G” entre paréntesis sólo se muestran si hay una cuenta de Google activa en el dispositivo.



1842. “Cuenta de Google”: además de mostrar la dirección activa, ofrece al pinchar sobre él la posibilidad de cambiar de cuenta y de cerrar la sesión. Si la sesión se cierra, no se mostrarán tarjetas asociadas a “Mi Tablón”, como ilustra la imagen inferior derecha. Si, tras cerrar una sesión, se vuelve a seleccionar este campo, se presentarán las cuentas de Google que se hayan configurado en el dispositivo móvil y además habrá una opción “Añadir cuenta” por si se desea emplear una cuenta diferente.

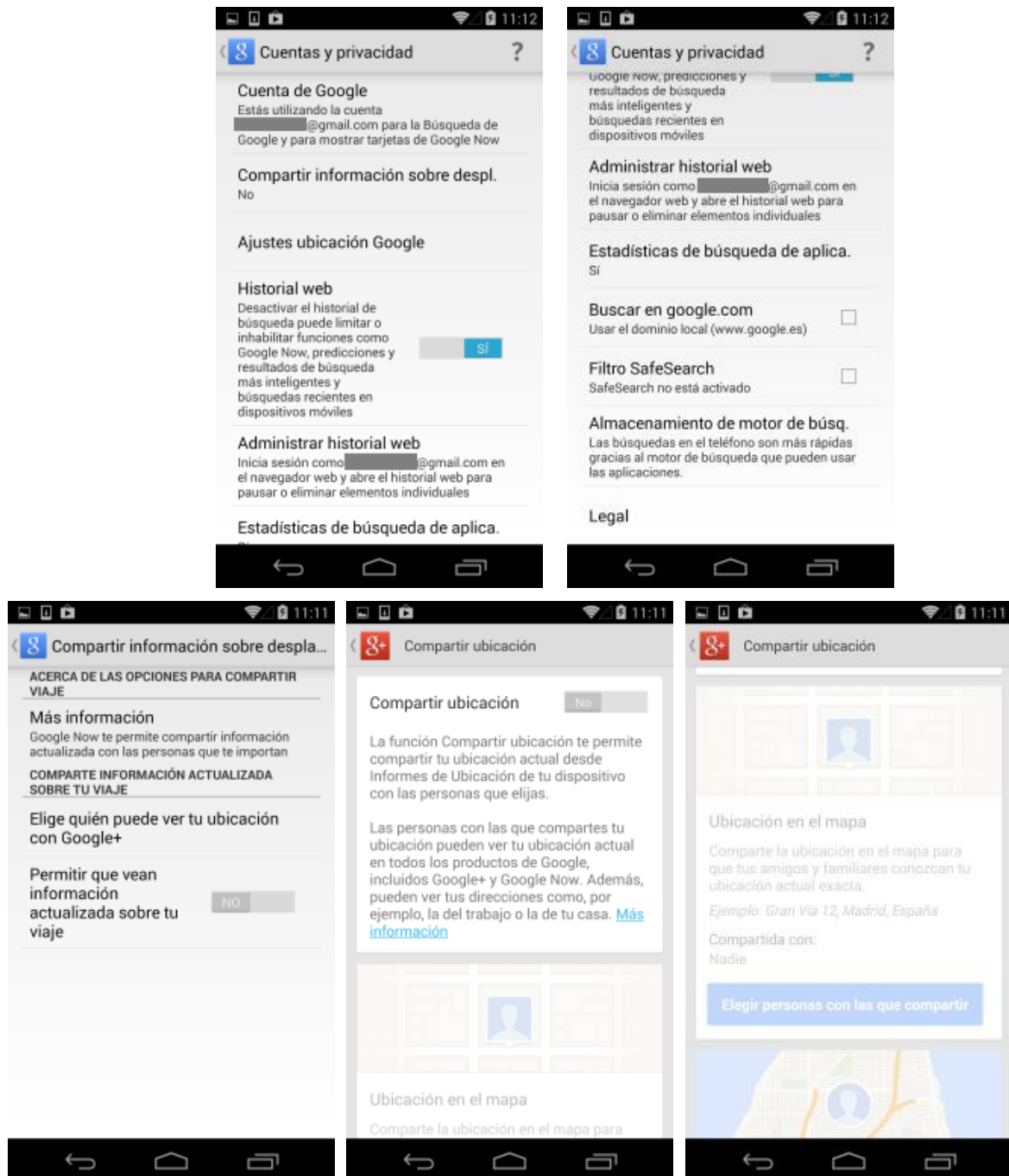


1843. Controles de la actividad de tu cuenta de Google (en versiones más antiguas de la app de Google, se denominaba “Historial de cuenta de Google”) (G): incluye diversas opciones que controlan lo que se envía o no a Google. Todas permiten “administrar actividad”, que establece una conexión con el servidor “myaccount.google.com” usando las credenciales de la cuenta de Google del usuario y da opción de consultar, eliminar y modificar la actividad de las aplicaciones que han enviado datos, e incluso cambiar los

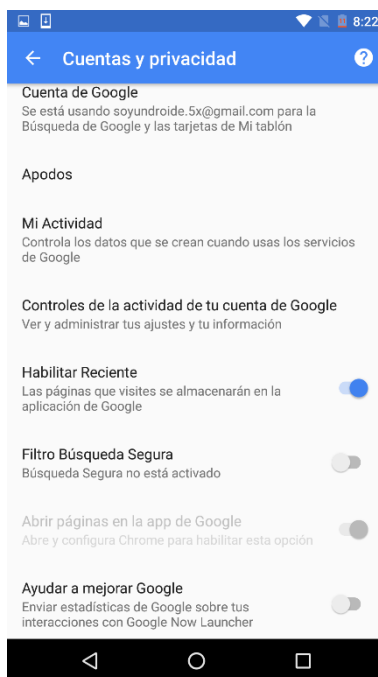
ajustes actuales de envío de datos de la cuenta de usuario en el servidor. Desde el punto de vista de seguridad y privacidad, se recomienda desactivar todas estas opciones:

- Actividad en la web y en aplicaciones [Ref.- 175]: guarda la actividad de búsqueda en aplicaciones móviles y navegadores web. Además de activar y desactivar esta funcionalidad, dispone de una opción para incluir el historial de navegación de Chrome y de aplicaciones que usen servicios de Google, un apartado “Datos de este dispositivo” que, si se selecciona, almacenará en la cuenta de Google del usuario la actividad de aplicaciones que parten del propio dispositivo móvil, y “administrar historial”, que inicia sesión en los servidores de Google y permite ver en detalle qué aplicaciones se han utilizado, pudiendo filtrarse incluso por fecha y producto de Google.
- Información de los dispositivos: envía a Google (para que sean guardados) información sobre contactos, datos del dispositivo móvil, calendarios, aplicaciones y música, con objeto (según indica la ayuda) de obtener sugerencias y resultados más precisos en las búsquedas. Para consultar el detalle de los datos guardados, se puede pulsar en “Administrar actividad”. Ello abre el menú “Información del dispositivo”, con tres puntos a la derecha que dan opción de “eliminar todo”, ver la actividad registrada (“mi actividad”), y acceder a los “controles de actividad de la cuenta”, que se conecta a “myaccount.google.com” con la cuenta del usuario y da opción de modificar los ajustes de envío de datos de la cuenta en el servidor.
- Actividad de voz y audio: almacena las búsquedas de voz (por ejemplo, a través de “Ok Google”).
- Historial de búsquedas de YouTube.
- Historial de reproducciones de YouTube.
- Historial de ubicaciones de Google: si está activa, Google obtendrá datos de la ubicación del dispositivo. Además de poderla desactivar, se ofrece la opción “Eliminar historial de ubicaciones”, que advierte de que algunas aplicaciones pueden dejar de funcionar y obliga a marcar activamente que se quiere eliminar el historial, antes de poder proceder a eliminarlo realmente.

1844. En versiones más antiguas de la app de Google que la analizada en la presente guía, el menú de configuración de “Cuentas y privacidad” ofrecía la opción “Compartir información sobre desplazamiento (G)”, deshabilitada por defecto, que posibilitaba la compartición de información actualizada con otros usuarios de Google sobre viajes y desplazamientos, permitiendo elegir qué contactos pueden ver la ubicación a través de Google+. Esta opción (que se ilustra en las imágenes ofrecidas a continuación) ya no se encuentra disponible en la app Google, sino que se traslada a la app Maps (ver apartado “12. Localización (o ubicación) geográfica”):



1845. En las últimas versiones de la aplicación Google, el apartado “Cuentas y privacidad” ofrece las siguientes opciones adicionalmente:



**Nota:** En función de la versión concreta de Android 6.x, los ajustes aquí mencionados pueden aparecer como parte de la app Google o dentro del capítulo “Ajustes - [Personal] Google”.

- “Mi Actividad”: redirige al portal “<https://myactivity.google.com/myactivity>” iniciando sesión con la cuenta del usuario activa en el dispositivo, sin solicitar de nuevo las credenciales. Desde dicho portal es posible consultar y gestionar tanto los controles de la cuenta (historial de actividad en la web y en aplicaciones, historial de ubicaciones, información de los dispositivos vinculados a la cuenta de Google del usuario, de reproducciones de YouTube...).
- Filtro Búsqueda Segura (SafeSearch): si está activado, permite bloquear imágenes, videos y sitios web explícitos (por ejemplo, con contenido pornográfico) de las búsquedas de Google, evitando la mayor parte del contenido para adultos [Ref.-166]. Concretamente, el filtro SafeSearch permite bloquear imágenes y vídeos con contenido sexual explícito, así como resultados que puedan dirigir a contenido explícito, de los resultados de las búsquedas de Google. Es importante reseñar que lo que se bloquea no son las páginas de contenido explícito en sí, sino su aparición en las búsquedas.

1846. La opción “Configuración de búsqueda” contiene parámetros como la activación de “Safe Search” (navegación segura), el funcionamiento de “Google Instant” (que presenta sugerencias para completar las búsquedas en Google), la síntesis de voz o el historial de búsquedas.

- Abrir páginas en la app de Google: si se selecciona esta opción, las búsquedas web se abrirán dentro del contexto de la app de Google, en lugar de lanzar un navegador.
- Ayudar a mejorar Google: envía estadísticas de uso de la actividad de Google Now Launcher. Se recomienda reducir el envío de información y/o estadísticas adicionales a los servidores de Google.
- Habilitar Reciente: almacena información sobre las páginas visitadas.



## Configuración de las búsquedas

## Resultados de búsqueda

Idiomas

Ayuda

## Filtros SafeSearch

**SafeSearch** te permite bloquear imágenes inapropiadas o explícitas en los resultados de la Búsqueda de Google. El filtro SafeSearch no es 100% preciso, pero ayuda a evitar la mayor parte del contenido violento o para adultos.

☐ Activar Búsqueda Segura [Bloquear SafeSearch](#)

## Predicciones de Google Instant

¿Bajo qué circunstancias debemos mostrarte **resultados a medida que escribes**?

- ☒ Solo cuando mi ordenador sea lo suficientemente rápido  
Google Instant está activado actualmente para la búsqueda web. Cambia esta opción de forma manual a continuación.
- ☐ Mostrar siempre los resultados de Google Instant
- ☐ No mostrar nunca los resultados de Google Instant

## Resultados por página

- ☐ No mostrar nunca los resultados de Google Instant

## Resultados por página



## Resultados privados

Los **resultados privados** te permiten encontrar contenido más relevante, como contenido y conexiones que solo tú puedes ver.

- ☒ Usar resultados privados
- ☐ No usar resultados privados

## Respuestas con síntesis de voz

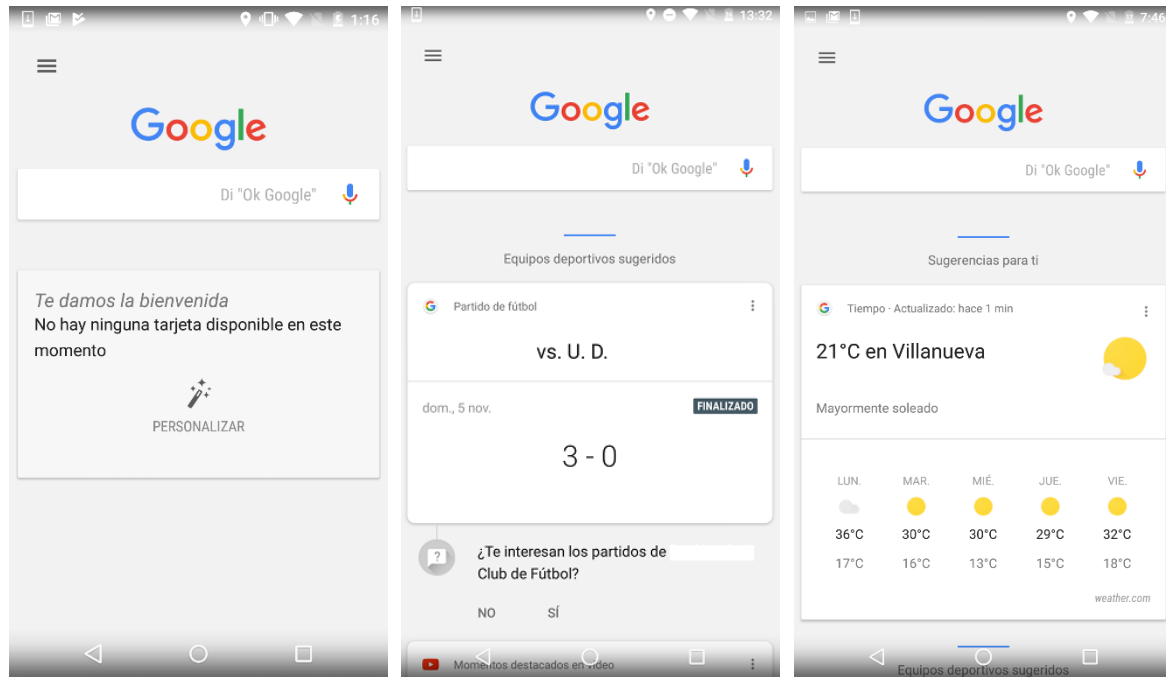
Al hacer **búsquedas por voz**, ¿es necesario decir las respuestas en voz alta?

- ☒ Decir respuestas para búsqueda por voz
- ☐ Solo mostrar texto

## 22.3. ASISTENTE PERSONAL Y “OK GOOGLE”

1847. El servicio de búsqueda de Google se concibió como un servicio o app que, actuando como asistente, permite al usuario interactuar con el dispositivo móvil Android, por ejemplo, para realizar búsquedas de información a través del buscador de Google; el buscador de Google se encuentra actualmente integrado en el denominado “*feed*” o “Google Feed”, sustituto de Google Now y dentro de la app “Google”. La versión de la app “Google” utilizada para elaborar el presente apartado de la guía es la 7.21.23.1, disponible en Google Play.

1848. Adicionalmente, si se ha activado la configuración de “Mi Tablón” del servicio *feed*, el buscador de Google se integrará en lo que se denomina “Google Now” (o “Google Now Launcher”), que está disponible como escritorio o panel individual:

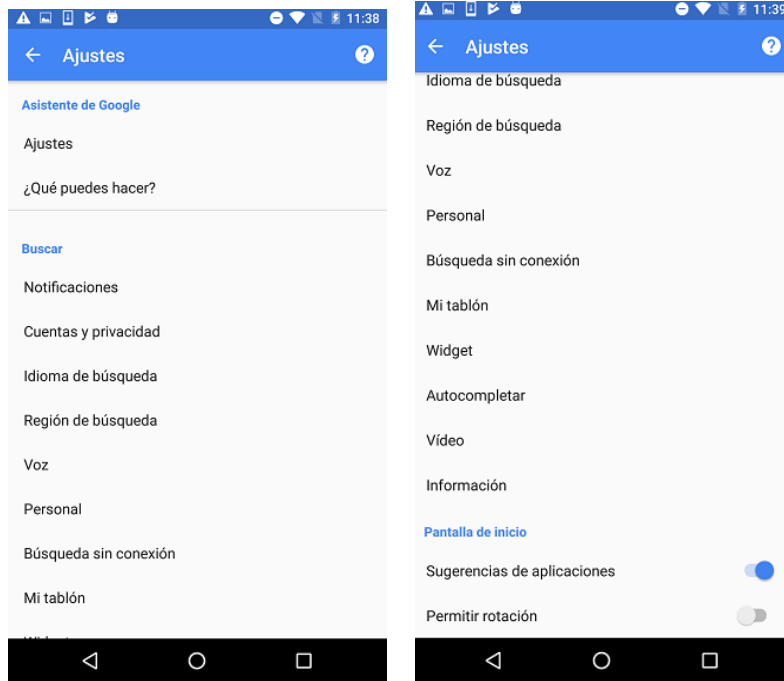


1849. Es importante no confundir el “Google Now Launcher” con el Launcher de Android, que es la aplicación que permite a su vez la ejecución de otras aplicaciones y las agrupa en el escritorio. El Launcher se invoca tocando el botón central con seis puntos en el margen inferior central de cada escritorio. Como aplicación individual, el “Google Now Launcher” dejará de estar disponible en Google Play durante el año 2017<sup>103</sup>.
1850. Por su parte, el servicio de búsqueda de Google se incorpora a la parte superior de las pantallas principales, o escritorios o pantallas de inicio (en adelante referidas como pantallas de inicio), representado por un campo de búsqueda y un icono con forma de micrófono. Al incluir entre sus funciones no una búsqueda literal, sino una búsqueda adaptada al perfil del usuario creado en base a sus interacciones con otras aplicaciones de Google, se convirtió en un “asistente personal” (Google Assistant o Asistente de Google):

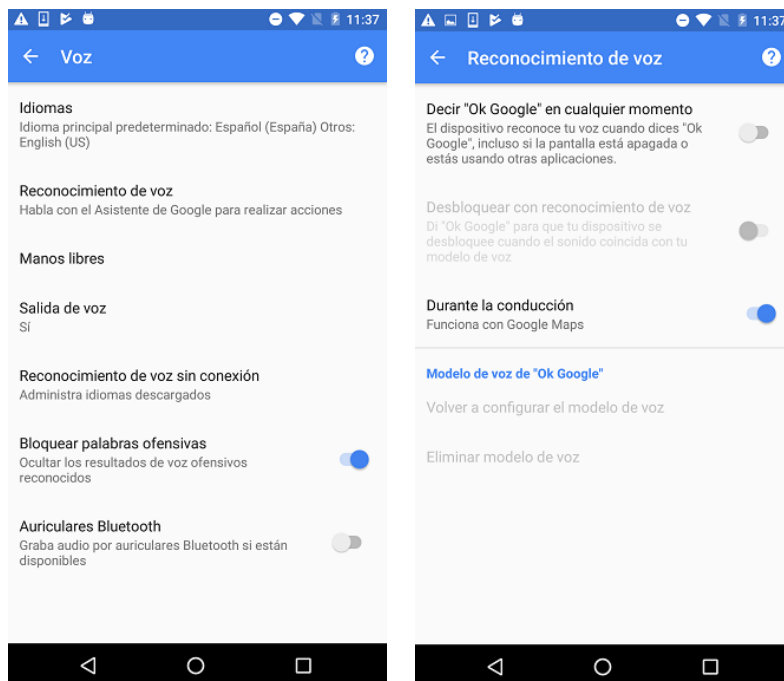
<sup>103</sup> <http://www.androidpolice.com/2017/02/03/google-will-discontinue-google-now-launcher-coming-weeks/>



1851. En el caso de estar habilitada la búsqueda por voz, al lado del icono con forma de micrófono aparecerá el texto “Di 'Ok Google'”, que permite al usuario comenzar a interactuar con esta funcionalidad mediante la voz y la pronunciación de esa frase (“Ok Google”).
1852. El asistente personal o Google Assistant (en adelante, “Ok Google”), está permanentemente activo, siempre que el usuario se encuentre con el dispositivo móvil desbloqueado y en las pantallas de inicio, escuchando al usuario a través del micrófono del dispositivo móvil, y esperando a que se pronuncie la frase de activación (“Ok Google”).
1853. Teóricamente, el dispositivo móvil no enviará ningún dato a Google mientras permanece en el modo de escucha pasiva, teniendo lugar todo el procesamiento de voz localmente en el dispositivo móvil. Tan pronto el usuario pronuncia la frase de activación, se establece una conexión mediante HTTPS con los servidores de Google para interpretar las indicaciones de voz del usuario al realizar una búsqueda o ejecutar una acción, y obtener los resultados desde los servidores de Google.
1854. Esta funcionalidad puede ser deshabilitada desde la app “Google”, y en concreto, desde el botón de menú, a través de la opción “Ajustes”, desde donde es posible acceder a los ajustes del feed (y de la app “Google”).



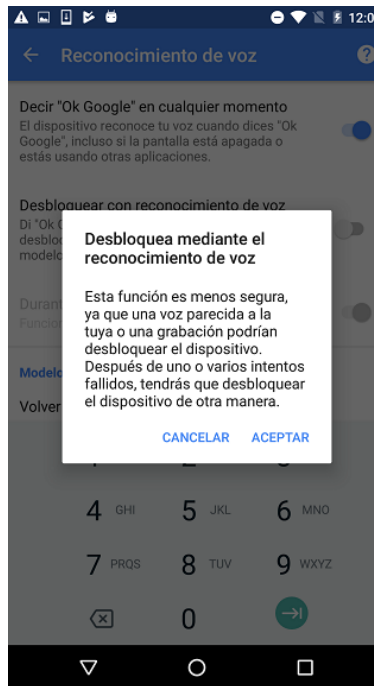
1855. La sección “Voz” alberga, bajo el apartado “Reconocimiento de voz” (en versiones anteriores de la app Google el apartado se denomina “Detección de 'Ok Google'”) las opciones de configuración disponibles, listadas a continuación. Es muy importante reseñar que, a diferencia de otros ajustes, no se requiere que el dispositivo móvil tenga configurado un código de acceso para habilitar esta funcionalidad. Ahora bien, si lo tiene, se solicitará introducirlo para cambiar las opciones:



- “Decir ‘Ok Google’ en cualquier momento” (en otras versiones de la app Google, puede mostrarse como “Siempre activa”): al pronunciar “Ok Google”, se inicia una búsqueda por voz que sólo es posible desde la app “Google” o desde cualquier pantalla de inicio del “Google Now Launcher”. Si no está habilitada la opción “Desbloquear con reconocimiento de voz” y la pantalla se encuentra bloqueada por un método de acceso, la invocación de “Ok Google” no activará el servicio, sino que emitirá un mensaje de voz informando de que no puede

realizarse la acción hasta que no se desbloquee el dispositivo, o bien mostrará la pantalla de bloqueo para que se introduzca el método de acceso.

- “Desbloquear con reconocimiento de voz” (o “Desbloqueo por voz” en versiones menos recientes): es la opción que corresponde a la función “Smart Lock - Desbloqueo por voz”, la cual posibilita desbloquear el terminal al reconocer el patrón de voz del usuario al pronunciar “Ok Google” en la pantalla de bloqueo. El dispositivo informará de la repercusión que esta opción tiene desde el punto de vista de seguridad mediante el siguiente mensaje:



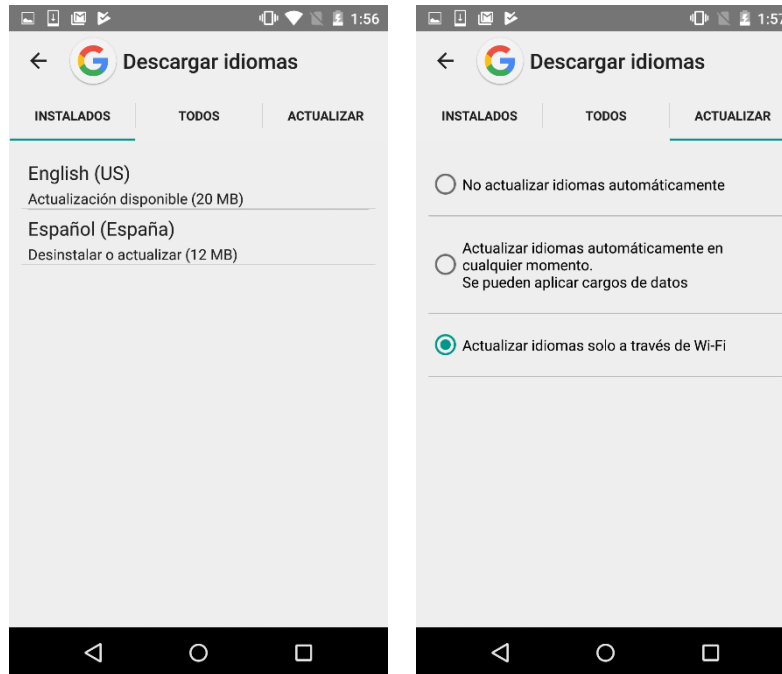
- “Durante la conducción”: permite el envío de indicaciones de voz al dispositivo al hacer uso de Google Maps, excepcionalmente y adicionalmente a desde la app “Google”. Esta opción, habilitada por defecto, será deshabilitada si se activa la opción “Decir ‘Ok Google’ en cualquier momento”, ya que se extiende su utilización a cualquier pantalla, incluida Google Maps.
- Sección “Modelo de voz de ‘Ok Google’”: de nuevo, esta opción aparece sombreada (deshabilitada) hasta que se activa la opción “Siempre activa” y se procede a registrar el modelo de voz del usuario. La opción permite volver a configurar o eliminar el modelo de voz existente (esta última opción deshabilita la opción “Decir ‘Ok Google’ en cualquier momento” y requiere que se vuelva a activar manualmente para poder usar de nuevo el modelo de voz).

1856. Al apartado de configuración “Detección de “Ok Google”” se puede llegar también desde las opciones de Smart Lock: “Ajustes - [Personal] Seguridad - [Seguridad del dispositivo] Smart Lock - Desbloqueo por voz”.

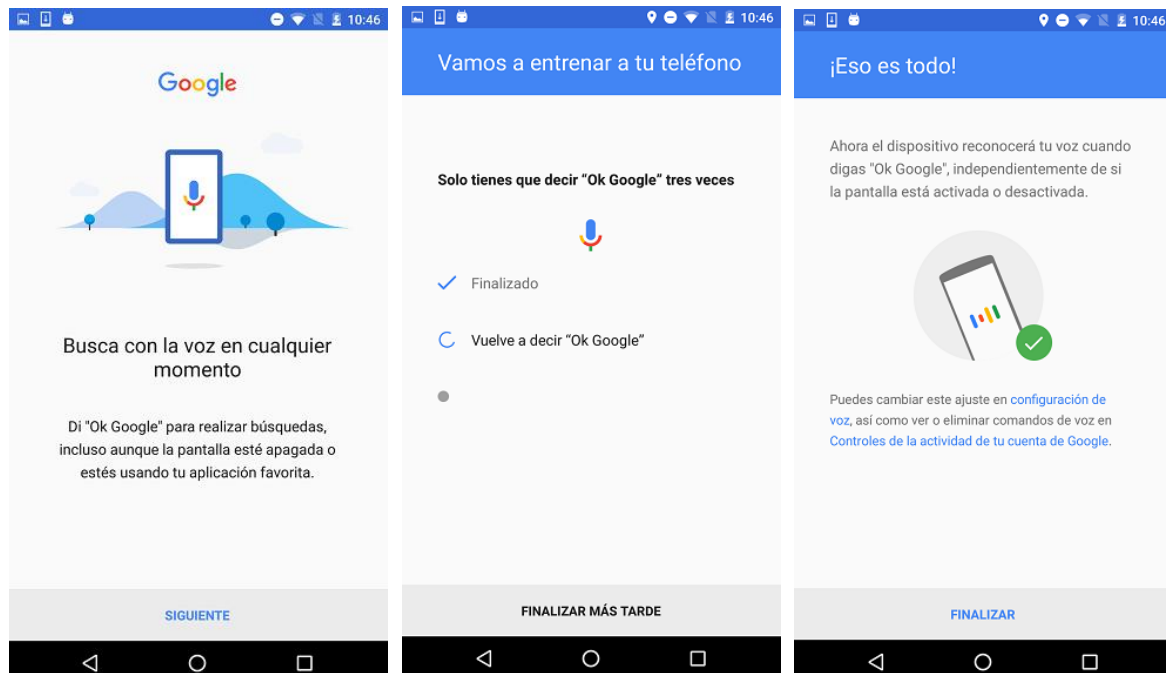
1857. Si se deshabilita la opción “Decir ‘Ok Google’ en cualquier momento”, aún es posible hacer uso de esta funcionalidad de búsqueda mediante la voz pulsando manualmente el icono del micrófono para iniciar una búsqueda desde cualquiera de las pantallas de inicio.

1858. Adicionalmente, mediante la modificación de los ajustes de la app “Google” también es posible deshabilitar de forma efectiva su utilización.

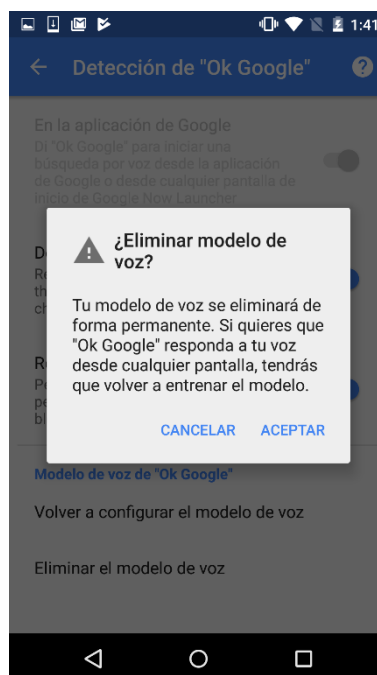
1859. Por defecto, la app “Google” dispone del idioma “English (US)” preinstalado. Desde el botón de menú, y la opción “Ajustes” de la app “Google”, es posible cambiar la configuración. Por ejemplo, la sección “Voz” permite seleccionar el idioma a emplear (opción “Idiomas”), mientras que la opción “Reconocimiento de voz sin conexión” permite administrar los idiomas descargados:



1860. Desde la opción “Reconocimiento de voz sin conexión - Descargar idiomas” es posible configurar si se desea que se descarguen y actualicen los ficheros de reconocimiento de idiomas, a través de la pestaña “Actualizar”. Por defecto, la opción seleccionada es “Actualizar idiomas solo a través de Wi-Fi”, pudiéndose actualizar los idiomas en cualquier momento (a través de la conexión e datos móviles 2/3/4G), o bloquear la actualización automática por completo.
1861. La opción “Salida de voz” permite configurar si se recibirá una respuesta audible para todas las búsquedas realizadas o sólo si el dispositivo está en modo manos libres.
1862. La opción “Manos libres” permite determinar si se aceptarán conexiones con el dispositivo bloqueado, y proporciona un botón de activación “Auriculares Bluetooth” (habilitado por defecto). En versiones anteriores a la empleada para la elaboración de la presente guía, se disponía de la opción “Para auriculares con cable” (deshabilitado por defecto). Esta opción de auriculares con cable, de estar disponible, no debe marcarse, pues posibilitaría que alguien con acceso físico al dispositivo móvil pudiera utilizar comandos de voz con solo conectar unos auriculares. La opción de Bluetooth, al haber requerido un emparejamiento previo entre los dispositivos, proporciona algo más de seguridad, pero también se aconseja deshabilitarla ya que podrían presentarse escenarios de ataque desde una cierta distancia (sin acceso físico al dispositivo) mediante la suplantación de los dispositivos Bluetooth, de tipo manos libres, emparejados con el dispositivo móvil.
1863. Para registrar el modelo de voz que será reconocido por el dispositivo, es necesario seleccionar “Modelo de voz de 'Ok Google'” y seguir los pasos que se indican, diciendo el texto “OK Google” tres veces hasta que el dispositivo reconozca el comando:

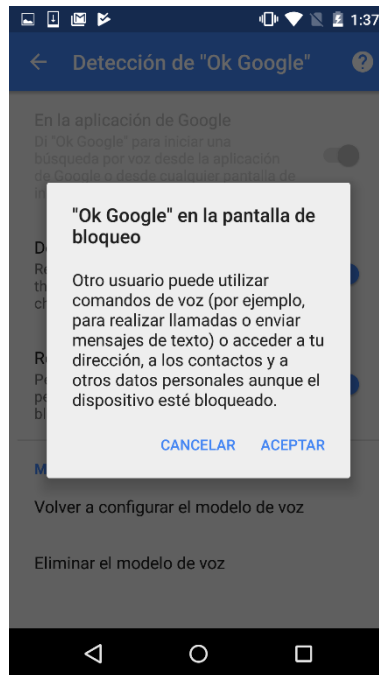


1864. El modelo de voz puede ser modificado (opción “Volver a configurar el modelo de voz”) o eliminado para desactivar la funcionalidad “Ok Google” (opción “Eliminar modelo de voz”) del menú “Ajustes de la app Google - Voz - Detección de ‘Ok Google’”.

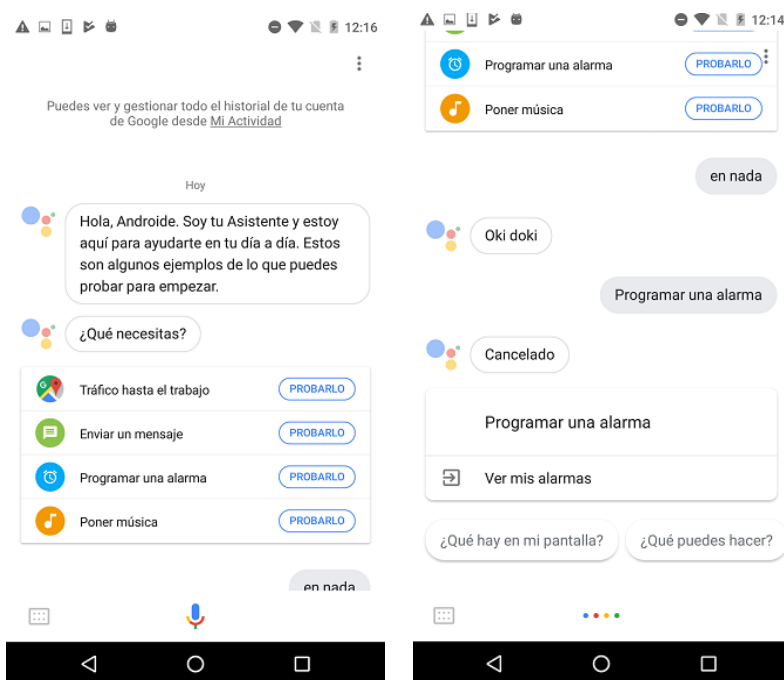


1865. La opción “Ajustes de la app Google - Voz - Detección de ‘Ok Google’ - Resultados personalizados”, existente en versiones más antiguas de la app Google, y que permite que otros usuarios (cuyo modelo de voz no está registrado) puedan realizar determinadas acciones mediante comandos de voz aun con el dispositivo bloqueado, desaparece en versiones más recientes, incluida la analizada en la presente guía. Su desaparición es ventajosa desde el punto de vista de seguridad, pues permitía acciones como las descritas en el mensaje informativo:





1866. Una vez habilitado el servicio “Ok Google”, se podrán realizar búsquedas por voz precedidas de la frase “Ok Google”, que dará paso a la pantalla del asistente de Google y pondrá al dispositivo en modo de escucha y reconocimiento de voz, y presentará varias opciones a modo de ejemplo:



1867. Desde el punto de vista de seguridad se recomienda no habilitar la funcionalidad de “Ok Google”, salvo que se valoren los riesgos existentes frente a los beneficios obtenidos.

## 23. APLICACIONES MÓVILES (APPS) EN ANDROID

1868. Los siguientes apartados proporcionan breves recomendaciones de seguridad asociadas a las aplicaciones más comunes y relevantes existentes por defecto en

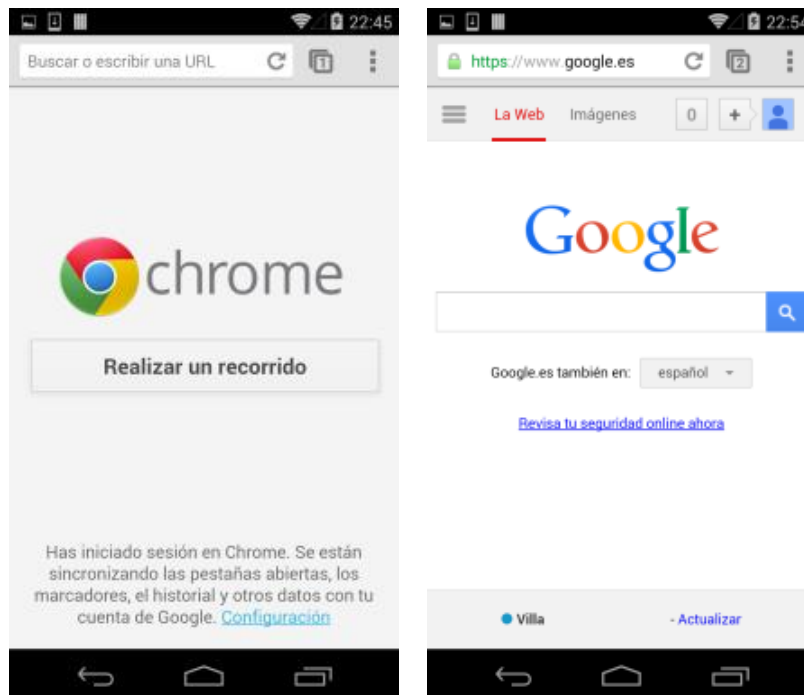
Android. Queda fuera del ámbito de esta guía el análisis de seguridad exhaustivo del funcionamiento y de todas las opciones de configuración disponibles en cada app.

**Nota:** El número de aplicaciones móviles instaladas por defecto en Android por Google, el fabricante del dispositivo móvil o el operador de telefonía móvil, así como la variedad de apps de otras compañías que pueden ser instaladas posteriormente manualmente o desde Google Play, hace inviable su análisis de seguridad dentro del alcance de la presente guía.

Para todas las apps instaladas o a instalar en el dispositivo móvil, se recomienda realizar una análisis detallado, identificando la versión actualmente instalada, evaluando la gestión de credenciales de acceso (almacenamiento y utilización), así como los protocolos empleados durante el proceso de autenticación y durante el resto de la sesión, y las capacidades de cifrado, tanto para el envío y recepción de datos, como para el almacenamiento de los mismos localmente, junto a cualquier otra característica de seguridad ofrecida por la app, especialmente los permisos que solicita de cara al dispositivo móvil y los que verdaderamente necesita para funcionar.

### 23.1. NAVEGACIÓN WEB: NAVEGADOR CHROME

1869. Una de las tareas más comunes realizadas desde los dispositivos móviles es la de navegación web por Internet. Android, a partir de la versión 4.3, incluye por defecto el navegador web Chrome, disponible desde el *Launcher*. Chrome está basado en el proyecto de código abierto Chromium [Ref.- 214].

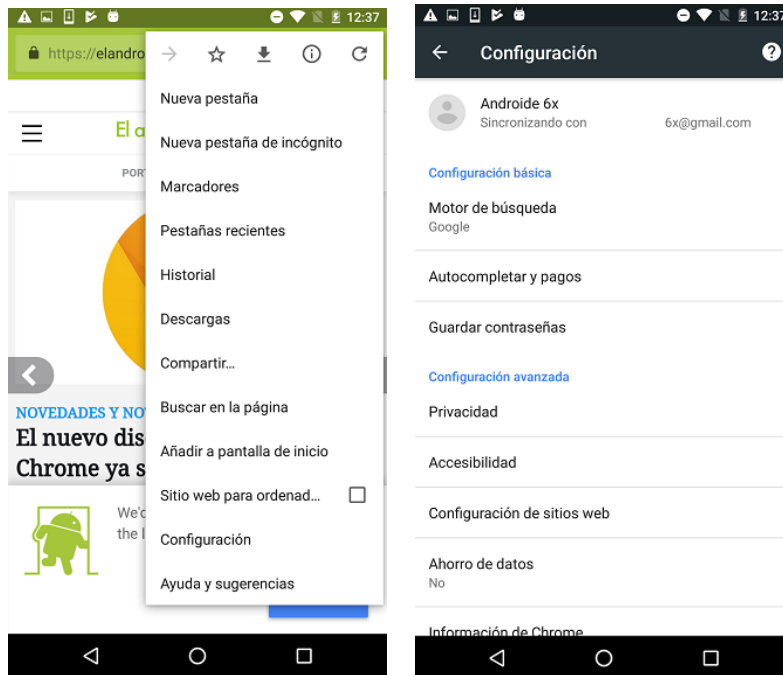


1870. Chrome sustituye al navegador web existente previamente por defecto en versiones anteriores de Android, que presentaba carencias de seguridad significativas, tal y como se describe en la versión previa de la presente guía para Android 2.x [Ref.- 401] y con algunas referencias breves en los siguientes apartados (como por ejemplo “23.1.5. Android WebViews”).

1871. Cuando se accede a Chrome por primera vez (esto es válido para todos los usuarios que se den de alta en el dispositivo móvil), Chrome solicitará permiso para “Ayudar a mejorar Chrome enviando estadísticas de uso e informes sobre fallos”. También

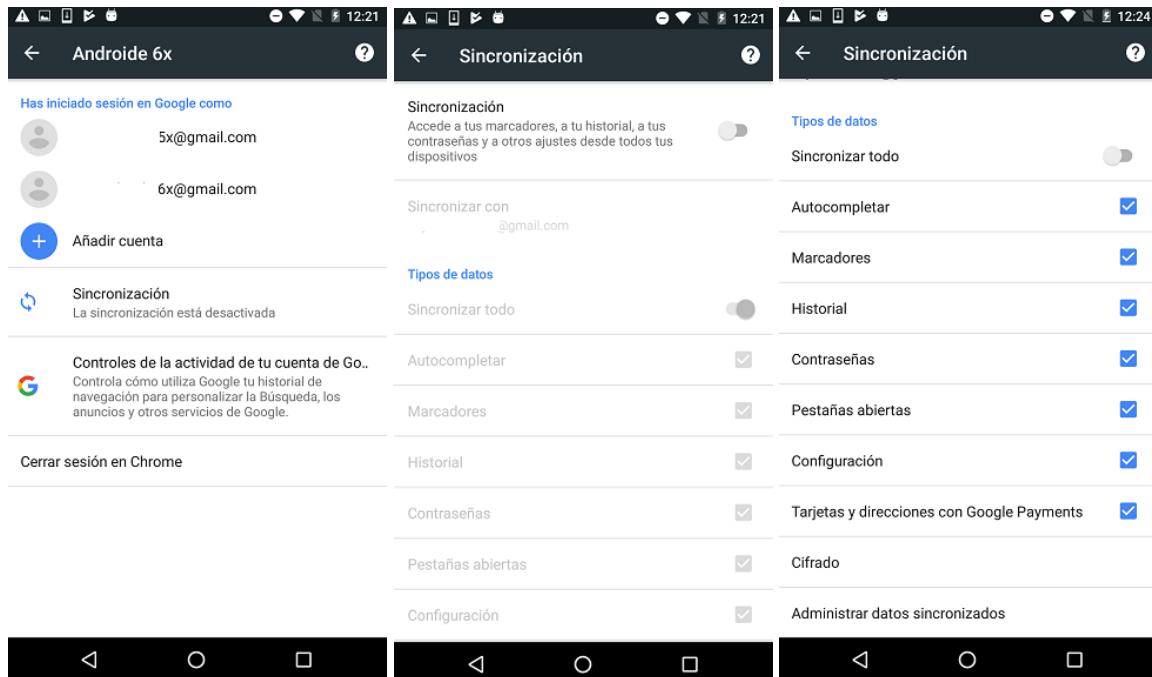
solicitará (si no se ha aceptado previamente), permiso de ayuda a mejorar el teclado (que enviará a Google fragmentos tecleados en aplicaciones de Google). Se recomienda desmarcar estas opciones, por no disponer de control sobre la información que se enviará a Google.

1872. A través del botón “Menú” (representado por tres puntos alineados verticalmente) cuando la app de Chrome está siendo ejecutada, es posible acceder mediante la opción “Ajustes” al menú de configuración de Chrome, desde donde se pueden (entre otros) gestionar múltiples ajustes, tanto “[Básicos]” como “[Avanzados]”:



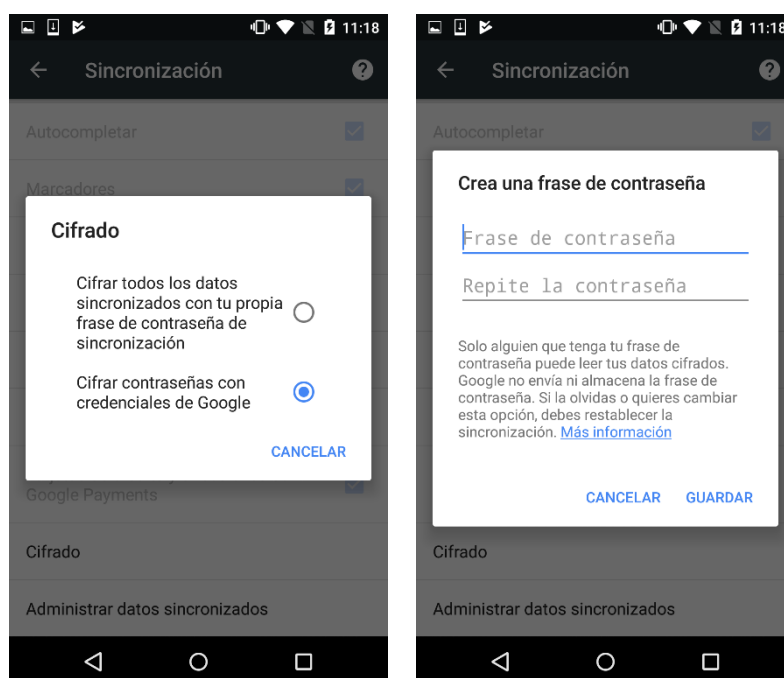
1873. La versión de Chrome, que (se obtiene al seleccionar la opción “Información sobre Chrome” en su menú de “Configuración” utilizada en la elaboración de la presente guía) es la 64.0.3282.137.
1874. Dado que cada actualización puede añadir, eliminar, renombrar y modificar opciones, puede que algunos de los puntos referenciados a continuación no se correspondan totalmente con los disponibles en otros dispositivos móviles que ejecuten Android 6.x.
1875. Chrome soluciona algunas de las limitaciones de seguridad relevantes existentes en el navegador web de Android disponible por defecto en versiones previas del sistema operativo, como por ejemplo contar con soporte para cookies “HttpOnly”, empleadas para proteger la sesión de un usuario frente a ataques de Cross-Site Scripting (XSS) [Ref.-123].
1876. Mediante la selección de la cuenta de usuario de Google es posible definir si se hará uso del servicio de sincronización de datos de Chrome que permite sincronizar las pestañas abiertas en el navegador, los favoritos o marcadores, el historial de navegación, la información para autocompletar formularios, e incluso las contraseñas, entre el dispositivo móvil y un ordenador [Ref.- 63].
1877. Para configurar las opciones de sincronización, dentro de los ajustes de Chrome se debe seleccionar la cuenta y “[Nombre asociado a la cuenta] - Sincronización”. Se presentará entonces la pantalla con la opción para activar/desactivar toda la sincronización o marcar de forma selectiva qué se desea sincronizar:

- Sincronizar todo: si se desmarca, se activarán el resto de opciones de sincronización para seleccionarlas/deseleccionarlas individualmente. En caso de requerir hacer uso de esta funcionalidad, se recomienda restringir y minimizar el tipo de datos que serán sincronizados, especialmente, las contraseñas.



1878. Una opción crítica desde el punto de vista de seguridad y la sincronización de Chrome es la asociada a la opción “Cifrado”. Ésta permite dos opciones:

- “Cifrar contraseñas con credenciales de Google” (habilitada por defecto), cifrándose las contraseñas con las credenciales de la cuenta de usuario de Google.
- “Cifrar todos los datos sincronizados con tu propia frase de contraseña de sincronización”, opción que permite al usuario establecer una contraseña para acceder a los datos sincronizados:

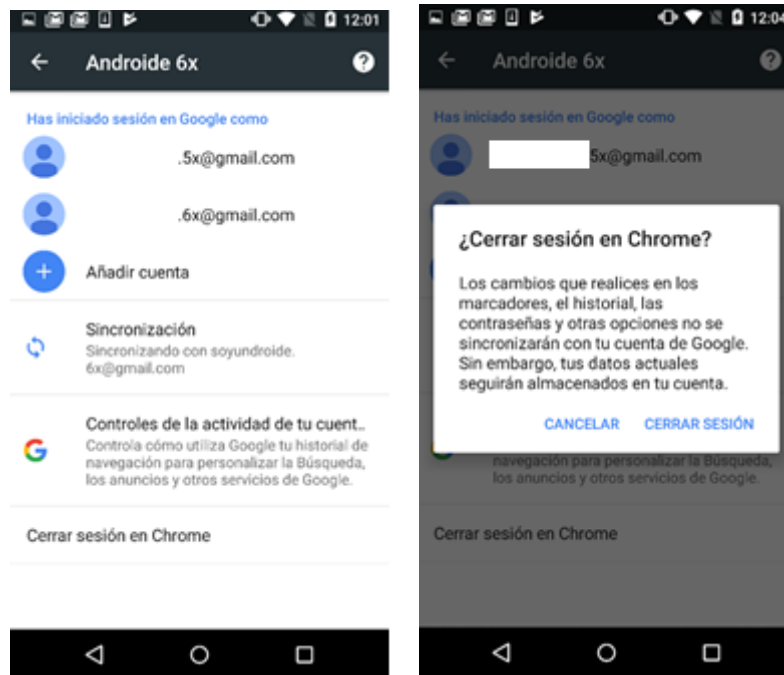


1879. La opción recomendada desde el punto de vista de seguridad es no sincronizar las contraseñas mediante este servicio. En caso de hacerlo, se debe hacer uso de la opción de cifrado con la propia contraseña, empleando una contraseña independiente y diferente de la asociada a las credenciales de la cuenta de usuario de Google, y , especialmente haciendo uso de una frase de paso o *passphrase*, es decir, una contraseña suficientemente larga y robusta [Ref.- 63].
1880. Con anterioridad a marzo de 2016, existía un servicio “Chrome to Phone” (de Chrome al móvil”, habilitado por defecto) que permitía enviar páginas web desde un ordenador que usara Chrome al dispositivo móvil. Chrome to Phone era un sistema formado por una app para Android y una extensión para el navegador Chrome de escritorio, pero Google dejó de ofrecerlo sin ofrecer ningún sustituto directo. Por tanto, la opción “De Chrome al móvil” que existía en versiones anteriores de Chrome deja de estar disponible.
1881. La opción “[Básica] Guardar contraseñas” alberga dos subopciones:
- Guardar contraseñas: la gestión de contraseñas se lleva a cabo mediante el servicio “Google Smart Lock” si este servicio está activo (ver apartado “23.14. Servicio de contraseñas de Google Smart Lock”), que almacena los campos en *passwords.google.com*. Salvo que se especifique lo contrario, no se almacenarán las contraseñas correspondientes a las cuentas de Google. Se recomienda deshabilitar esta opción y no recordar las contraseñas, debiendo eliminar las que están almacenadas actualmente. Para eliminar las contraseñas que se hayan almacenado, se ha de buscar la entrada en la lista “Contraseñas” y pulsar “Eliminar”.
    - Si el servicio “Smart Lock para contraseñas” no está activo pero el usuario ha iniciado sesión en su cuenta de Google, Chrome solicitará confirmación para almacenar las credenciales la primera vez que se visite un sitio web que las requiera y también las almacenará en *passwords.google.com*.
    - Si no se ha iniciado sesión en la cuenta de Google y el servicio Smart Lock está deshabilitado, Chrome solicitará almacenamiento de credenciales y, en caso de recibir aprobación del usuario, las almacenará localmente en el perfil de Chrome del dispositivo.
  - Iniciar sesión automáticamente: utiliza las credenciales almacenadas para iniciar sesión en los sitios web para los que estén disponibles.
1882. En versiones anteriores de la app Chrome, se ofrecía como opción de configuración el “Inicio de sesión automático”, que, de activarse, provocaba que se iniciase sesión con las credenciales de la cuenta Google del usuario en los sitios web de Google, de forma automática y sin que se solicitase la intervención del usuario [Ref.- 232]. Esta opción dejó de tener sentido en Android 6.x, ya que la sesión de la cuenta de Google no se cierra salvo que explícitamente se solicite esta acción a través de la opción “Cerrar sesión en Chrome”.
1883. El propósito de esta funcionalidad es que el usuario pueda sincronizar marcadores, historial de navegación, contraseñas, etc., cuando utilice el navegador web en dispositivos diferentes.
1884. Desde el punto de vista de seguridad, se recomienda deshabilitar todas las opciones que implican un inicio de sesión automático, salvo que se requiera hacer un uso

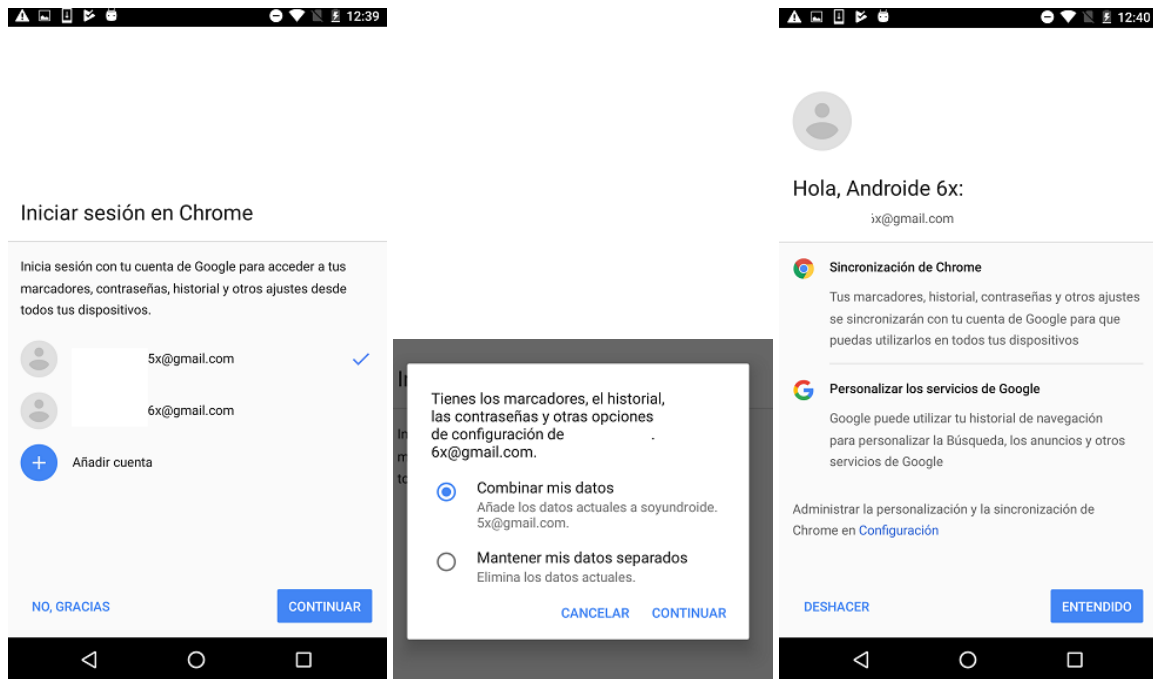
explícito de esta funcionalidad, y que se tenga plena consciencia de cuándo tiene lugar una autenticación tanto en los servicios de Google como en otros servicios.

1885. Asimismo, se recomienda no almacenar contraseñas automáticamente en Chrome.

1886. Para dejar de utilizar la cuenta de Google en Chrome, en versiones anteriores existía el botón “Desvincular cuenta de Google” (situado en la parte inferior), que permitía al usuario hacer uso de Chrome al margen de la cuenta de usuario de Google, es decir, de manera más anónima e independiente. Con las últimas versiones de Chrome, esta opción explícita desaparece y se incorpora en los ajustes de Chrome relativos a la cuenta y el botón “Cerrar sesión en Chrome”. Los datos se dejarán de sincronizar, pero no se borrarán los ya existentes.



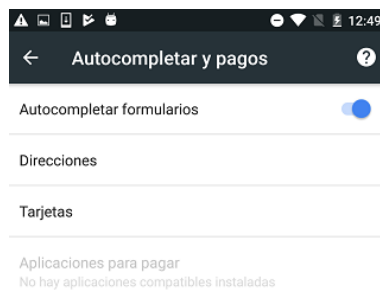
1887. Al “Cerrar sesión en Chrome”, los ajustes de Chrome pasarán a incorporar como primer campo “Iniciar sesión en Chrome”, y, al acceder, se presentarán las cuentas de Google disponibles en el dispositivo móvil para que el usuario seleccione una de ellas. En caso de que exista más de una cuenta con datos ya almacenados por Chrome, se presentará la opción de combinar los datos de ambas cuentas o de mantenerlos separados. Si se opta por mantenerlos separados, los datos actuales se eliminarán ya que, en Android, sólo existe un perfil de Chrome para un usuario concreto (por ejemplo, no es posible tener un perfil de trabajo y otro personal, a diferencia de lo que ocurre en versiones de Chrome para ordenador).



1888. Si, aunque está desaconsejado, fuese preciso compartir el dispositivo móvil con otro usuario, se deberá crear un usuario independiente en el dispositivo, y que dicho usuario acceda con su cuenta de Google a Chrome. Para más información sobre cómo crear usuarios, consultar el apartado “9.19. Múltiples perfiles de usuario”.

- Además, al iniciar sesión se activará el menú “Controles de la actividad de tu cuenta”, que redirige a la opción “Actividad en la Web y en Aplicaciones” descrita en el apartado “22. App Google: Asistente de Google, Mi Tablón y Servicios de Búsqueda de Google”.

1889. La opción “[Básica] Autocompletar y pagos” presenta 3 apartados:



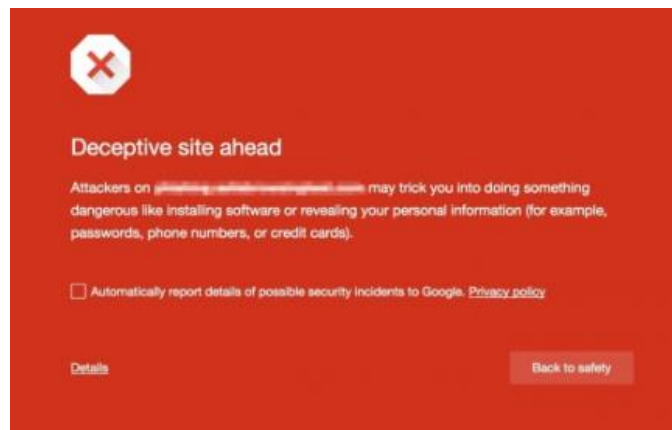
- Autocompletar formularios (habilitada por defecto): permite a Chrome autocompletar formularios con la información del perfil de usuario especificada (por defecto no se dispone de ningún perfil, y éste debe ser añadido con los datos de contacto del usuario).
- Direcciones: añade una dirección al perfil que se usará dentro de la función de autocompletar formularios.



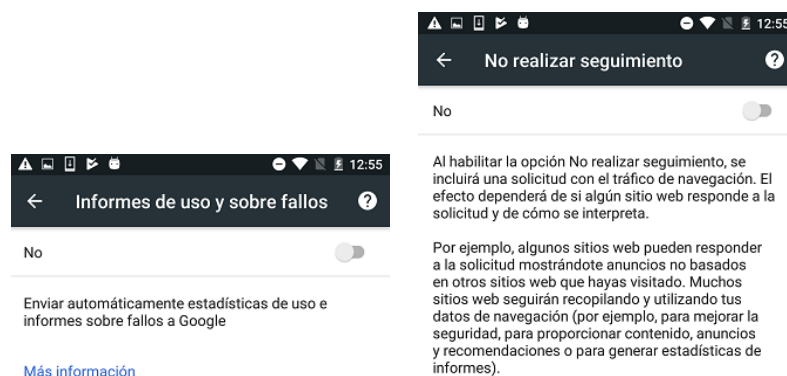
- Tarjetas de crédito: contiene los campos necesarios para poder llevar a cabo la autocompleción de tarjetas de crédito en sitios web que soliciten pagos. Por defecto no se dispone de ninguna tarjeta de crédito, y ésta debe ser añadida manualmente:

1890. Se recomienda deshabilitar la opción “Autocompletar formularios”, y no recordar los datos introducidos en formularios. En caso de existir información sobre el perfil del usuario o tarjetas de crédito, se recomienda borrar los datos almacenados actualmente.
1891. Desde la sección “[Configuración avanzada] Privacidad”, se pueden obtener sugerencias al presentarse errores de navegación, sugerencias de URLs y búsquedas, y mejorar la carga de páginas web mediante las predicciones de acciones de red. Además, en versiones recientes se ha incorporado la opción “Navegación segura”, que se apoya en la tecnología “Navegación segura” (Google *Safe Browsing*) [Ref.- 234] [Ref.- 215].

1892. Entre otras funcionalidades, la *navegación segura*, la cual analiza millones de URL todos los días, realiza la búsqueda de sitios web no seguros para mostrar advertencias en la Búsqueda de Google y en los navegadores web. Todas estas opciones están habilitadas por defecto. Para deshabilitarlas, hay que desmarcar la opción “Ajustes de Chrome - [Opciones avanzadas] Privacidad - Navegación Segura” [Ref.- 216].
1893. Además, la navegación segura pretende prevenir al usuario cuando una página web lanza una ventana en la que se insta a descargar o reproducir algún tipo de malware, o proporcionar información sensible. Chrome mostrará una ventana como la siguiente:

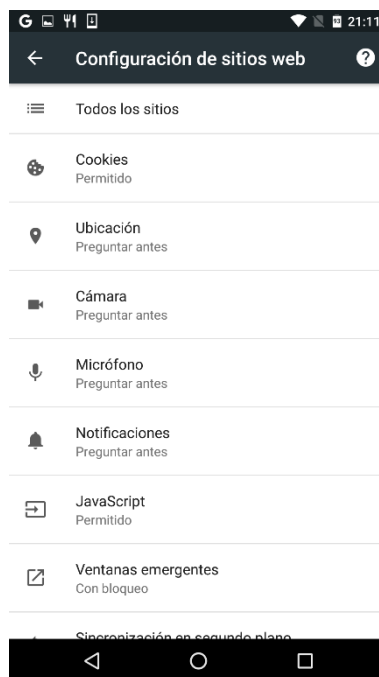


1894. Existe también (desmarcada por defecto) la opción “Informes de seguridad”, que envía a Google el contenido de las páginas web visitadas para que las incluya potencialmente en sus análisis de sitios no seguros.
1895. Adicionalmente se dispone de opciones para el envío de informes de uso y fallos y de solicitudes de no seguimiento (deshabilitada por defecto):



1896. Desde el punto de vista de la privacidad del usuario, se recomienda deshabilitar todas las opciones de sugerencias y predicciones descritas.
1897. Asimismo, se recomienda no enviar nunca informes de uso y errores, y habilitar las solicitudes de no seguimiento, para que el navegador web añada en sus peticiones la cabecera HTTP “DNT: 1” (Do Not Track, DNT) indicando a los sitios web visitados que no quiere ser monitorizado (el resultado de este ajuste de configuración depende únicamente del comportamiento de los sitios web visitados, que pueden tener en cuenta dicha cabecera, o hacer caso omiso de la misma).
1898. La opción avanzada “Accesibilidad” no deberían tener un impacto directo en la seguridad del dispositivo móvil.

1899. La opción avanzada “Configuración de sitios web” [Ref.- 217] permite realizar ajustes sobre el contenido de los sitios web visitados, como el uso de “cookies” (permitido por defecto), “JavaScript” (permitido por defecto), bloquear pop-ups o “ventanas emergentes” (bloqueadas por defecto), funcionalidad para la que los sitios web soliciten autorización para acceder al “micrófono” y la “cámara” del dispositivo móvil (configurados como “preguntar antes” por defecto), “notificaciones” (se solicitará autorización al usuario para que dé su aprobación a la petición de enviar notificaciones por parte de un sitio web), la opción “sincronización en segundo plano” (para retomar en segundo plano acciones que pueden haber quedado pendientes por haberse perdido la conexión a Internet temporalmente, como la descarga de un archivo), la opción “multimedia”, que activa la protección de contenido necesaria para la reproducción de música y vídeos *premium* y/o protegidos por *copyright* (configurado como “preguntar antes” por defecto), el *traductor de Google* (configurado a “preguntar antes” por defecto) para que Chrome ofrezca la posibilidad de traducir páginas escritas en otros idiomas, acceso a los ajustes de “ubicación” (ver apartado “12. Localización (o ubicación) geográfica”), “almacenamiento” (muestra el almacenamiento local del dispositivo que ha utilizado un sitio web) y “USB” (permite a un sitio web controlar y registrar información en un dispositivo USB conectado al terminal) [Ref.- 218]:

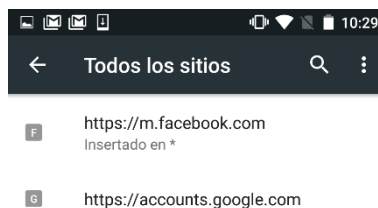


- Para una navegación web más segura, pero muy restringida desde el punto de vista de su funcionalidad, se recomienda deshabilitar la ejecución de scripts (JavaScript), mediante la opción “Habilitar JavaScript”, y el uso de cookies en el navegador web, mediante la opción “Aceptar cookies”, con el objetivo de mitigar los ataques asociados a la ejecución de scripts maliciosos en el navegador web y a la privacidad del usuario a través de las cookies. Adicionalmente, el bloqueo de pop-ups es una opción que debe estar habilitada. Esta configuración podría dificultar la visualización de páginas web que utilizan scripts y cookies en sus contenidos web y para su funcionamiento (la mayoría de páginas web en Internet), por lo que puede ser necesario tener que dejar habilitadas ambas opciones.

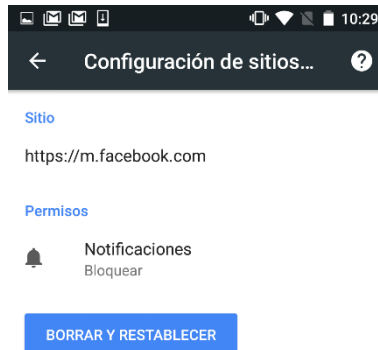
- Se recomienda deshabilitar las opciones “micrófono” y “cámara” para evitar que sitios web puedan realizar llamadas de voz y vídeo no autorizadas o registrar imágenes y sonido sin permiso del usuario.
- La opción “Multimedia - Contenido protegido” permite a sitios web como Netflix o Google Play autenticar al dispositivo móvil para confirmar si dispone de permisos para acceder a contenidos protegidos por *copyright*. Salvo que se haga un uso explícito de este tipo de contenido, se recomienda deshabilitar esta opción.
- La opción “Multimedia - Reproducción automática” controla que se pueda reproducir un vídeo que forma parte de una página web. Se recomienda deshabilitar esta opción, especialmente cuando no se está conectado a una red Wi-Fi, pues la descarga de vídeos supone un importante consumo de datos móviles.

1900. La opción avanzada “Ahorro de datos” hace que Chrome comprima las páginas antes de descargarlas. No se aplica a conexiones HTTPS o en el modo incógnito (que permite evitar que Chrome registre datos sobre la navegación) [Ref.- 219]. Se desaconseja habilitarla, pues implica que los datos de navegación serán enviados a los servidores de Google para que estos compriman los contenidos antes de descargarlos. Es decir, Google podría disponer de todos los detalles sobre las páginas web visitadas por el usuario, excepto para las páginas web accedidas mediante HTTPS o desde una pestaña de incógnito. Aunque esta funcionalidad también ofrece otros mecanismos de protección, como por ejemplo la detección de páginas con contenido malicioso, o involucradas en esquemas de suplantación de identidad, se desaconseja su utilización ya que el impacto sobre la privacidad del usuario al habilitarla es muy elevado.

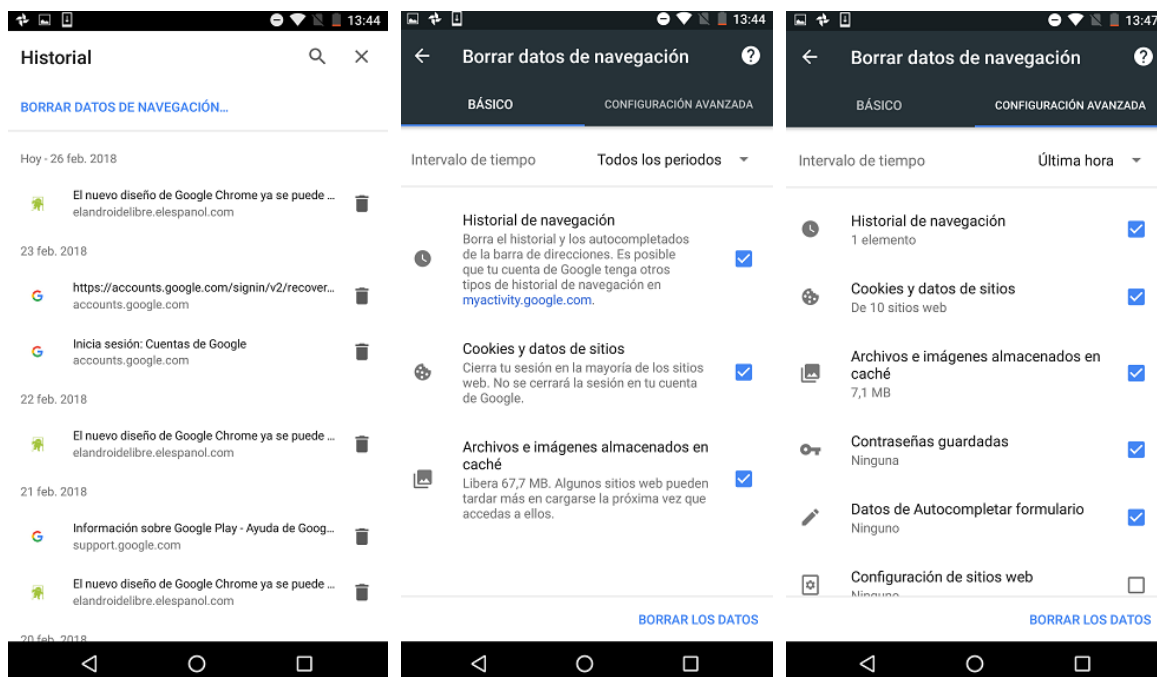
1901. El menú de Chrome “Configuración - [Configuración avanzada] Configuración de sitios web - Todos los sitios” permite obtener una lista de sitios web visitados que han accedido al almacenamiento local y/o a la ubicación, y ver los permisos otorgados a cada uno de ellos individualmente. Cada uno de estos elementos puede ser gestionado de forma particular:



1902. Accediendo a cada entrada específica de un sitio web, se puede consultar si se le han permitido notificaciones, pop-ups, si se ha aplicado algún ajuste de configuración por defecto (identificado con el carácter comodín “\*”), o la posibilidad de borrar los datos almacenados en caché para un sitio web concreto, aparte de las capacidades de habilitar o deshabilitar el acceso a la ubicación (ver apartado “12.6.5. Navegador web”):



1903. Por otro lado, y en lugar de hacerlo de forma individual por cada sitio web, desde el menú “Historial” de Chrome (fuera del menú de “Configuración”) es posible borrar los datos de navegación de manera global, mediante la opción “Borrar datos de navegación” (que incluye un apartado de “Configuración avanzada”):



1904. Estos datos incluyen el historial de navegación, la caché, las cookies y otros datos almacenados por los sitios web, las contraseñas y los datos para autocompletar formularios, almacenados actualmente.

1905. Desde el punto de vista de seguridad y privacidad del usuario, se sugiere aplicar las recomendaciones descritas previamente para cada sección con el objetivo de limitar la exposición del dispositivo móvil durante las actividades de navegación web.
1906. Se recomienda borrar de forma frecuente (tanto globalmente, como de forma individual para ciertos sitios web específicos, según las necesidades del usuario) tanto la caché como el historial de navegación web, así como el almacenamiento de cookies, y datos de formularios y contraseñas, con el objetivo de proteger la privacidad del usuario.
1907. La versión de Chrome utilizada en la elaboración de la presente guía no permite el uso de perfiles compartidos en Chrome, lo cual resulta muy conveniente desde el punto de vista de la seguridad y la privacidad [Ref.- 233].
1908. La opción “[Básica] Motor de búsqueda” determina qué motor se utilizará cuando se introduce un término en la barra de navegación del navegador que no corresponde con un servidor web (por ejemplo, una búsqueda por palabras). Por defecto, se realiza una búsqueda de dicho término a través del buscador de Google (“www.google.com”) <sup>104</sup>, pero es posible cambiarlo por Yahoo! o Bing.
1909. Este comportamiento tiene implicaciones de seguridad relevantes al revelar (potencialmente) en Internet la información introducida en la barra de navegación, como por ejemplo el nombre de servidores internos de una organización.
1910. Adicionalmente, la información del dispositivo móvil se desvela en los parámetros de la URL de “www.google.com” empleada para las búsquedas, incluyendo referencias a Chrome para Android, es decir, del navegador web y del tipo de plataforma móvil:

```
GET /search?q=raul+siles&oq=raul+siles&aqs=chrome..69i57.4923j0j4&client=ms-
android-google&sourceid=chrome-mobile&ie=UTF-8 HTTP/1.1
Host: www.google.es
```

1911. Cuando el navegador web accede a Internet, por ejemplo al buscador de Google, la cadena de caracteres que identifica al navegador web o agente de usuario (User-Agent) tiene el siguiente valor, revelando excesivos detalles sobre la versión del navegador web y la plataforma:

```
User-Agent: Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X Build/MTC20K; wv)
AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/64.0.3282.137 Mobile
Safari/537.36 MinuteMaid
```

1912. Los detalles del dispositivo móvil incluyen la plataforma (“Android”), la versión de Android (“6.0.1”), el modelo de terminal (“Nexus 5”), la versión de compilación de Android (“LMY48B”), o los detalles del navegador web (incluyendo su versión exacta y múltiples versiones de sus componentes: “64.0.3282.137 Mobile Safari/537.36 MinuteMaid”).
1913. Se recomienda modificar el valor del agente de usuario para que no desvele información adicional. Desde el botón de menú, es posible hacer uso de la opción “Sitio web para ordenad...” para forzar a Chrome a usar un agente de usuario distinto, similar al empleado por un ordenador. Este agente de usuario emula la utilización del

<sup>104</sup> También puede emplearse la versión localizada del buscador de Google según el país. Ej. “www.google.es”.

navegador web Chrome sobre un ordenador Linux genérico, aunque incluye de nuevo los detalles del navegador web (como, por ejemplo, su versión exacta):

```
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.137 Mobile Safari/537.36 MinuteMaid
```

1914. Se recomienda evaluar si habitualmente se desea realizar la navegación web como un ordenador o equipo de sobremesa (opción recomendada desde el punto de vista de seguridad para no desvelar los detalles reales del dispositivo móvil), más expuesto a ataques genéricos sobre todas las versiones del navegador web pero que probablemente no tengan éxito en el dispositivo móvil, o como dispositivo móvil, más expuesto a ataques dirigidos a este tipo de terminales y con posibilidad mayor de éxito.
1915. Debe tenerse en cuenta que la modificación del agente de usuario, y especialmente el valor de la plataforma (tradicional o móvil), podría afectar a la presentación de los contenidos web de ciertos servidores y aplicaciones web que personalizan las respuestas en función de si el cliente es un dispositivo móvil o un ordenador (de sobremesa o portátil).

**Nota:** La modificación o eliminación de información de las cabeceras HTTP puede afectar a la funcionalidad de servidores y aplicaciones web que hacen uso de dichos datos para procesar y mostrar contenidos web personalizados para el tipo de dispositivo cliente. Estas implicaciones se han mencionado igualmente a lo largo de la presente sección al deshabilitar otras funcionalidades disponibles habitualmente en los navegadores web.

Las recomendaciones de seguridad descritas a lo largo de toda la sección pretenden incrementar el nivel de seguridad y privacidad del dispositivo móvil y de su usuario, pudiendo afectar por tanto a la funcionalidad, por lo que deben ser aplicadas únicamente si no es necesario hacer uso de la funcionalidad asociada.

1916. En la versión de Chrome utilizada para la elaboración de la presente guía, las búsquedas en Google han introducido un nuevo procesamiento de las búsquedas que emplea el protocolo QUIC [Ref.- 220]. Cuando el navegador envía una búsqueda al motor de Google, como parte de la petición se devuelve que se puede utilizar QUIC en adelante, por lo que las siguientes peticiones de búsqueda se enviarán a través de este protocolo, que combina UDP, HTTP2 y TLS:

```
Alt-Svc: quic=":443"; ma=2592000; v="38,37,36,35"
```

1917. Algunos módulos de navegación web de Android, como el asociado a la información del GPS y gpsOneXTRA (ver apartado “12.4. gpsOneXTRA”), añaden la siguiente cabecera WAP que permite identificar el tipo de terminal (fabricante y modelo):

```
x-wap-profile:
http://www.openmobilealliance.org/tech/profiles/UAPROF/ccppschema-20021212#
```

1918. El UAProf (*User-Agent Profile*) es un documento XML que contiene información sobre las características y capacidades de un dispositivo móvil, estándar definido por OMA, Open Mobile Alliance. El documento está especificado en la cabecera HTTP “x-wap-profile” (o “Profile”), apuntando normalmente a una web del fabricante del terminal (repositorio de perfiles).



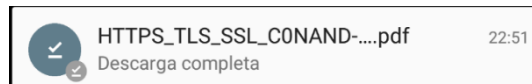
1919. El perfil puede contener información muy detallada del dispositivo móvil, incluyendo los perfiles Bluetooth, los tipos y formatos de datos soportados, protocolos de seguridad y de transferencia de datos soportados, capacidades push, WAP, MMS y de *streaming*.
1920. En el caso de Android, el perfil referenciado está asociado a una plantilla genérica para dispositivos móviles definida por la OMA, sin desvelar detalles particulares del terminal.

### 23.1.1. CONTENIDOS ADOBE FLASH

1921. Adobe anunció en noviembre de 2011 que no soportaría Adobe Flash en dispositivos móviles [Ref.- 108], en favor de las tecnologías basadas en HTML 5.
1922. Por este motivo, Adobe Flash no está soportado en el navegador web Chrome para Android [Ref.- 112]. disponible por defecto en esta plataforma móvil.
1923. Pese a que otros navegadores web para Android sí pueden disponer de soporte para Flash, como por ejemplo Firefox<sup>105</sup>, Boat o Dolphin, desde el punto de vista de seguridad no se recomienda su instalación, ya que la misma se basa en la instalación de versiones antiguas del reproductor de Flash para dispositivos móviles (Adobe Flash Player), para el que con una muy alta probabilidad se conocerán vulnerabilidades existentes públicamente.
1924. Debe tenerse en cuenta que las mejoras de seguridad incorporadas en las últimas versiones de Flash Player para los equipos de escritorio, ya no están disponibles en Flash Player para Android.

### 23.1.2. CONTENIDOS ADOBE PDF

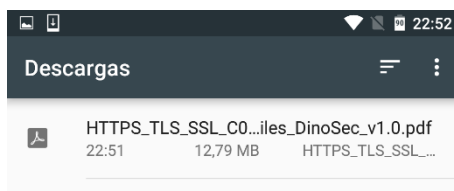
1925. Hasta Android 4.4.4, se incluía por defecto una app para la lectura de ficheros PDF denominada Quickoffice, siendo también posible instalar el cliente oficial Adobe Reader desde Google Play. Con Android 5.x (Lollipop) se introdujo un *framework* denominado *PdfRenderer* que permite que la aplicación que lo invoque pueda abrir en su contexto ficheros PDF [Ref.- 221].
1926. Se permite también al acceder a contenidos PDF desde el navegador web. Chrome descargará el fichero PDF automáticamente (a la carpeta general de “Descargas”, o “Download”, del almacenamiento interno del dispositivo móvil; ver imágenes siguientes) y el mismo podrá ser accedido también a través de la notificación del navegador web de que el fichero ha sido descargado:



1927. Al seleccionar el fichero PDF, éste será abierto automáticamente mediante la actividad “PdfViewerActivity”, según se puede ver a través de “adb logcat”:

```
I ActivityManager: Displayed
com.google.android.apps.docs/com.google.android.apps.viewer.PdfViewerActivity:
+322ms
```

<sup>105</sup> <https://support.mozilla.org/es/kb/firefox-para-moviles-no-admite-flash>

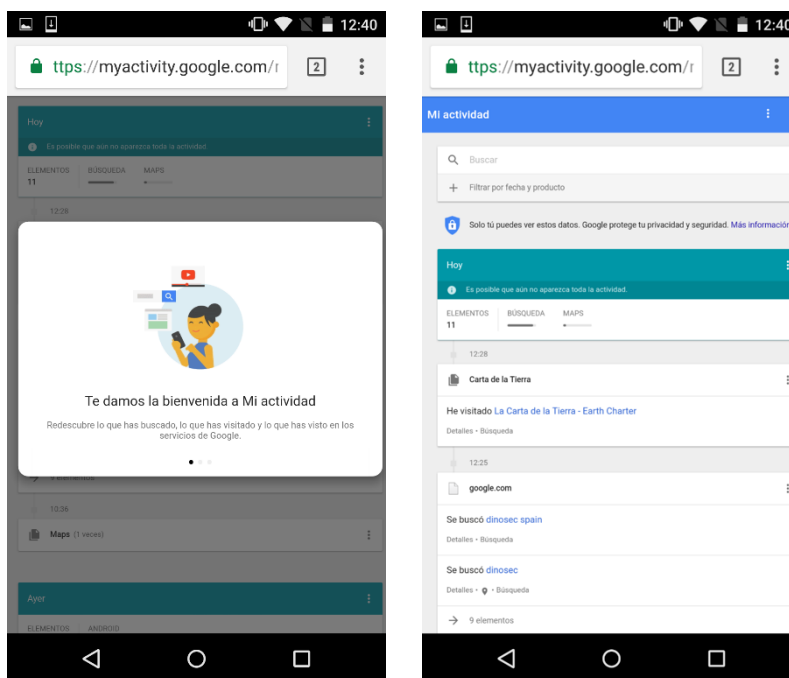


1928. En Android 6.x, el servicio de lectura de ficheros PDF se realiza a través de la app “Drive”, la cual invoca internamente la actividad “PdfViewerActivity”). Adicionalmente, se puede instalar la app “Visor de PDF de Google” (o cualquier otro visor de un desarrollador de confianza, como Adobe Acrobat, Adobe Reader, Foxit, etc.) si no se desea que la visualización de PDFs se realice a través de “Drive”.

1929. Debido a las numerosas vulnerabilidades de seguridad en las aplicaciones cliente de visualización de ficheros PDF durante los últimos años, se recomienda siempre mantener actualizada la app de visualización de ficheros PDF a la última versión.

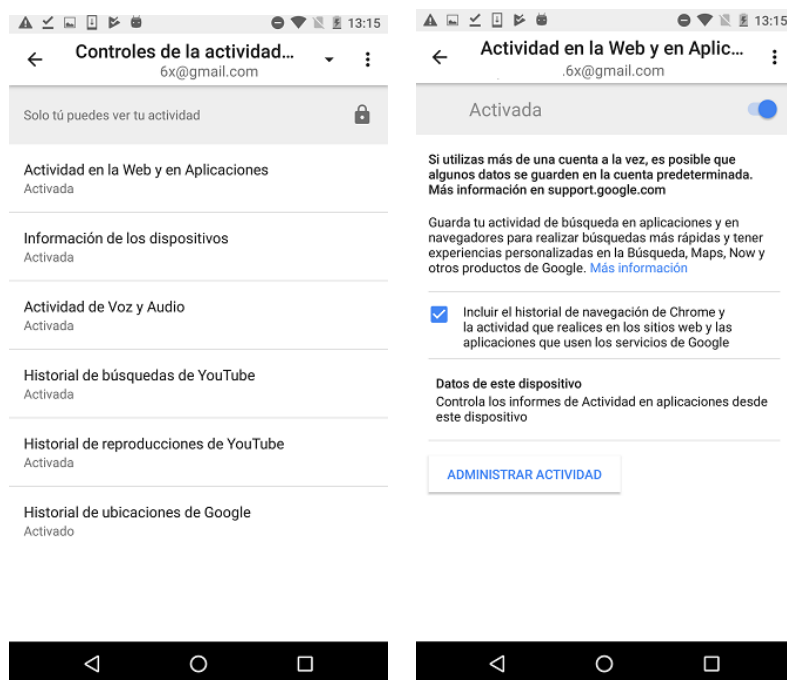
### 23.1.3. HISTORIAL DE ACTIVIDAD WEB Y DE APLICACIONES

1930. Las búsquedas realizadas por el usuario a través de Google, así como la actividad de navegación web y de otras apps, es almacenada en el portal “Mi actividad” de la cuenta de usuario de Google, disponible a través de la siguiente URL: “https://myactivity.google.com/ myactivity”.

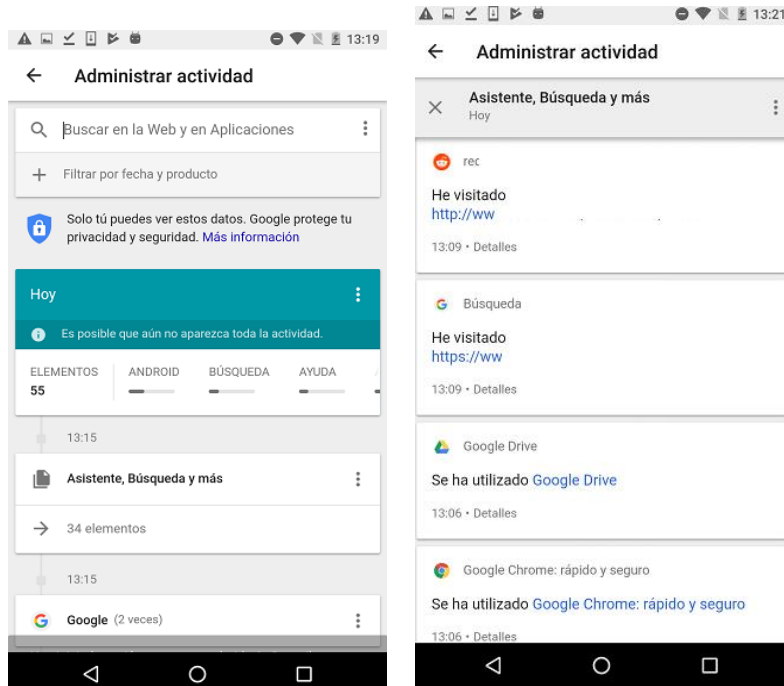


1931. Supuestamente, esta información es utilizada para proporcionarle al usuario mejores resultados y recomendaciones (más relevantes) al usar los productos y servicios de Google, como por ejemplo los servicios de búsqueda web y de mapas (con predicciones de búsqueda más precisas), conocer los resultados de las búsquedas en los que el usuario pulsa, conocer los anuncios visualizados por el usuario, poder acceder rápidamente a páginas web que ya se han visitado (disponiendo del historial de búsquedas recientes realizadas en cualquier dispositivo móvil u ordenador con la misma cuenta de usuario), la dirección IP del usuario, el tipo de navegador web empleado y su idioma, etc [Ref.- 176].

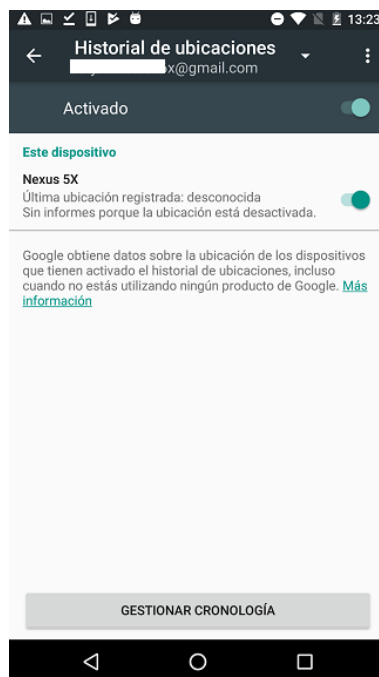
1932. El historial de actividad web y de aplicaciones puede estar desactivado si la cuenta de usuario de Google no ha sido vinculada a ningún dispositivo móvil Android, pero en caso de haberse llevado a cabo esta vinculación, y dado que esta funcionalidad está habilitada por defecto, el servicio estará activo.
1933. Si se activa desde la página web, es posible especificar si se desea incluir en el historial la actividad de Chrome a través de la siguiente URL, “<https://myactivity.google.com/item>”, y de la opción “Controles de la actividad de tu cuenta”. Asimismo, también es posible controlar los permisos y actividad de otras aplicaciones a través de la página “<https://myaccount.google.com/permissions>”.
1934. Para ello, a través de los ajustes de la app Google, hay que activar la opción “[Buscar] Cuentas y privacidad - [Controles de la actividad de tu cuenta de Google] Actividad en la Web y en Aplicaciones”:



1935. Se recomienda no activar la funcionalidad de historial de actividad web y de aplicaciones, incluyendo estas capacidades adicionales que permiten incluir en el historial la actividad de Chrome y de otras aplicaciones, salvo que se desee hacer un uso explícito de las mismas.
1936. La página “Mi Actividad” permite acceder y administrar el historial de actividad web y de aplicaciones, y dispone de detalles sobre las búsquedas y otras actividades clasificadas por servicios de Google e incluso clasificadas por fechas y horas, y obtener información detallada de todas las búsquedas realizadas:



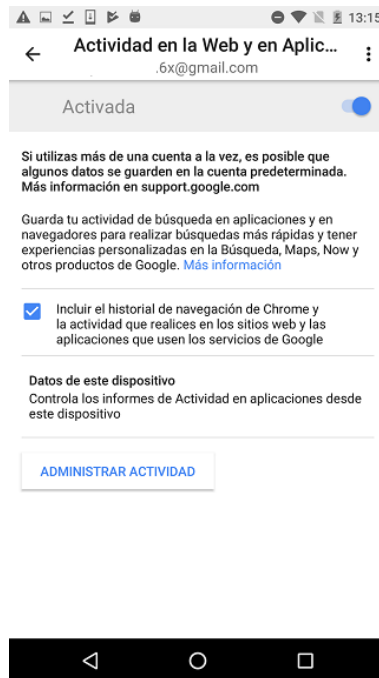
1937. El menú “Controles de la actividad de tu cuenta” contiene también la opción “Historial de ubicaciones”, que determina si se almacenará un mapa con las ubicaciones en las que algún dispositivo vinculado a la cuenta de Google ha sido localizado. Se recomienda mantenerlo sin activar por motivos de privacidad.



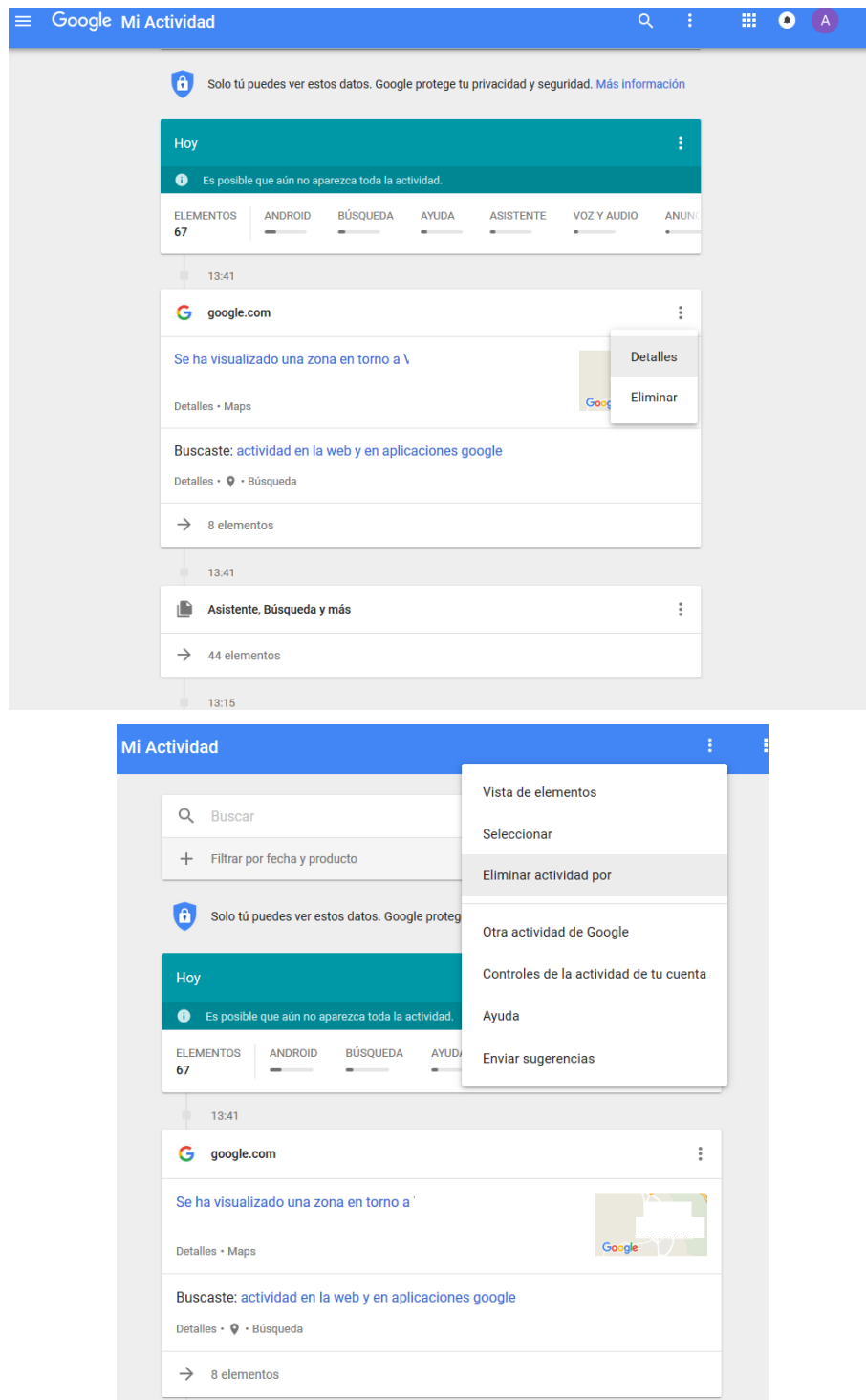
1938. Desde la página web es posible eliminar los registros del historial individualmente. Para ello, se deben seguir las indicaciones expuestas en “Eliminar la actividad guardada en Mi Actividad” [Ref.- 176].

- El historial web puede ser desactivado en cualquier momento desde la página web y desde Android, y en concreto desde la app “Ajustes de Google”, menú “Cuentas y privacidad - Controles de la actividad de tu cuenta de G. - Actividad en la web y en aplicaciones”, deshabilitando la opción “Activada” (para más

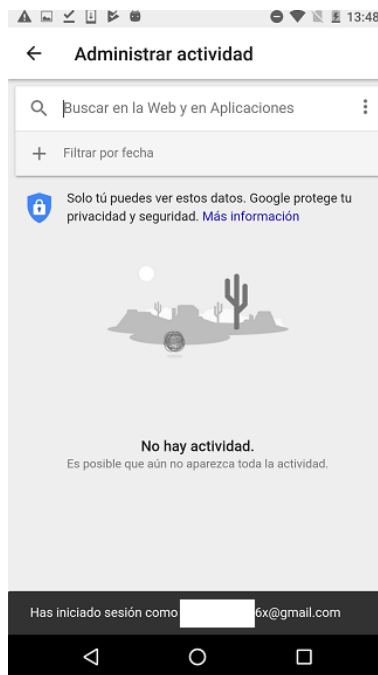
información, consultar el apartado “22. App Google: Asistente de Google, Mi Tablón y Servicios de Búsqueda de Google”):



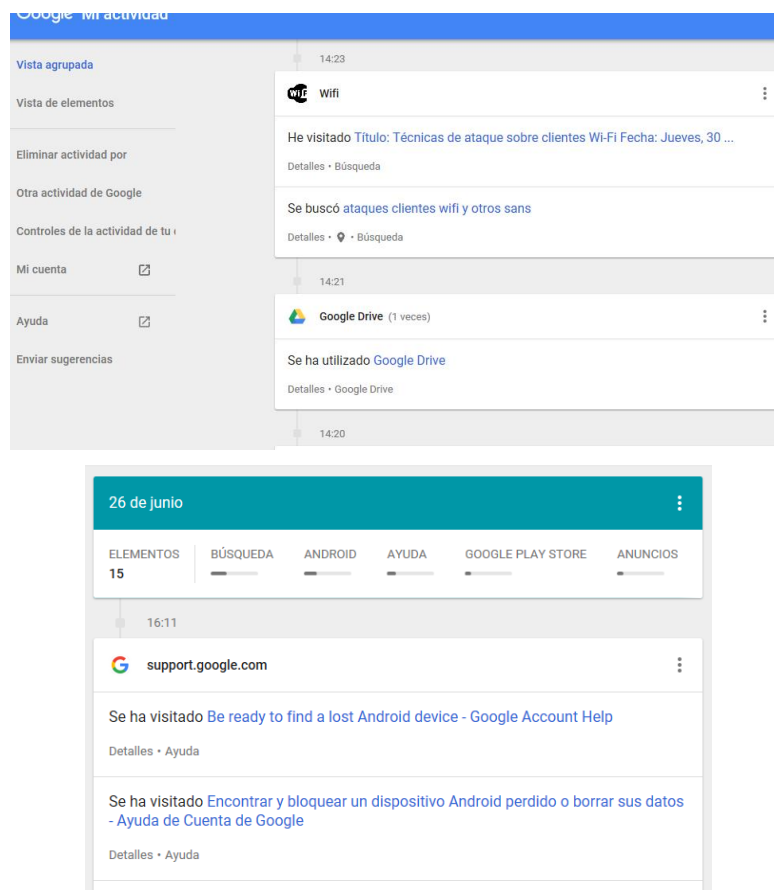
1939. Adicionalmente, se dispone de capacidades de administración del historial web desde Android mediante la opción “Administrar historial”. En versiones anteriores a Android 5.x, este botón abría un navegador web con una sesión asociada a la cuenta del usuario de Google empleando la URL “https://history.google.com/history/edit”. A partir de Android 5.x, el botón se conecta a la cuenta de Google del usuario y la app “Google” del dispositivo muestra de forma embebida la información correspondiente a “Mi actividad” (“https://myactivity.google.com/myactivity”). Desde ésta, es igualmente posible eliminar elementos del historial web selectivamente o en función del periodo temporal. Para eliminar el historial completo, en lugar de existir un botón específico es necesario ir a la barra “Mi Actividad - puntos de ajuste - Eliminar actividad por”. Debajo de “Eliminar por fecha”, se puede seleccionar la flecha hacia abajo y a continuación se marca “Todo el periodo” y se hace uso del botón “Eliminar”.



1940. Cuando el historial ha sido eliminado, desde el dispositivo móvil o desde la página web, no se dispone de datos asociados a esta funcionalidad:

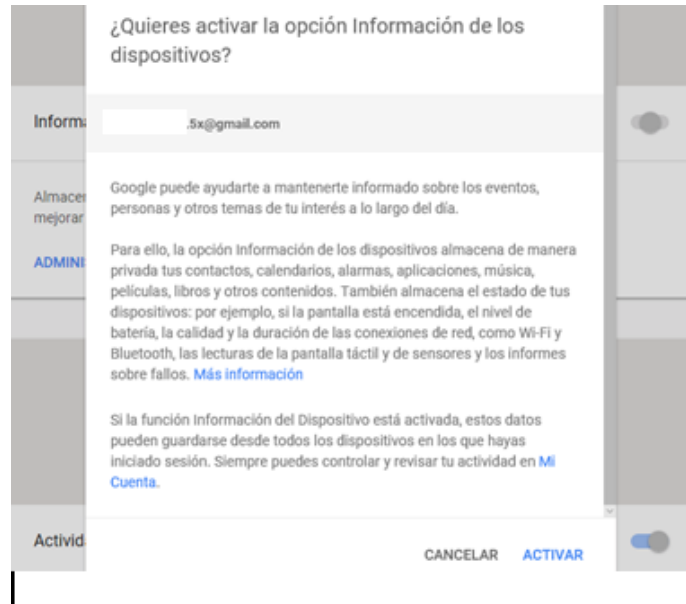


1941. En el caso de haber incluido en el historial la actividad de Chrome y de otras aplicaciones, que estará disponible en la página “Mi actividad” (descrita previamente), mediante el botón “+ Filtrar por fecha y producto” también es posible eliminar elementos selectivamente en función del periodo temporal.
1942. Los elementos del historial web incluyen términos de búsqueda, tanto en el buscador web general de Google como, por ejemplo, en las búsquedas por apps en Google Play, YouTube, etc., incluyendo el día y hora en que se utilizaron dichos términos, durante los últimos años:





1943. Adicionalmente, es posible almacenar información sobre los dispositivos, que guardará datos sobre todos los dispositivos desde los que se haya iniciado sesión en la cuenta de usuario de Google. Esta opción está deshabilitada por defecto (recomendado), y se puede activar mediante “Controles de la actividad de tu cuenta - Información de los dispositivos”.



1944. En caso de haberse activado esta opción y quererse eliminar, hay que acceder al menú “Control de tu Actividad - Información de los dispositivos - Administrar actividad”, seleccionar “Detalles del/los elementos a eliminar - Más - Eliminar”.
1945. En resumen, desde el punto de vista de seguridad, y de la privacidad el usuario, no se recomienda hacer uso del historial de actividad web y de aplicaciones. Adicionalmente, se recomienda borrar el historial de actividad web y de aplicaciones actualmente existente en la cuenta de usuario de Google.
1946. Cuando se detecta el acceso a la cuenta de Google de un usuario desde otro dispositivo diferente al que ya la tiene activa, el sistema Android mostrará una notificación indicando este hecho e invitando a revisar la configuración de la cuenta. Si se selecciona, se mostrará una ventana “Revisa el dispositivo” con información sobre el tipo de equipo, la versión de navegador, la ubicación y la hora del acceso. En ese punto, se puede seleccionar la opción “No, no fui yo” o confirmar que el acceso se llevó a cabo por parte del usuario.

#### 23.1.4. CERTIFICATE PINNING Y CERTIFICATE BLACKLISTING

1947. Android, desde la versión 4.2 (API 17), dispone de capacidades adicionales para el uso de mecanismos de validación y protección de las comunicaciones autenticadas y cifradas mediante HTTPS (TLS), basados en *certificate pinning* [Ref.- 79].
1948. El mecanismo de *certificate pinning* implica que la clave pública (o certificado) digital que se espera para un servidor o servicio sea fija y conocida, de modo que si, durante una conexión con dicho servidor se recibe un certificado digital que no concuerda con el esperado (o *pin*), la negociación TLS será interrumpida y no se establecerá la conexión.
1949. Para ello se establece una lista de *pins*, cada uno de ellos asociado al nombre (en DNS) de un *host* o servidor específico, y se permite a nivel global del sistema que tanto

el navegador web como las apps verifiquen la lista de *pins* (en caso de existir) y validen las conexiones mediante HTTPS. La lista de *pins* es almacenada en el fichero “pins” bajo “/data/misc/keychain”. Por defecto el fichero “pins” sí existe desde Android 5.x. En las pruebas realizadas, para esa versión de Android, este fichero contiene por defecto 43 entradas correspondientes a diferentes servidores y servicios de Google, y los *pins* correspondientes a sus certificados digitales, como por ejemplo: \*.spreadsheets.google.com, \*.google-analytics.com, \*.chrome.google.com, etc.

```
PIN list: /data/misc/keychain/pins
```

1950. El mecanismo de *blacklisting* (lista negra) se emplea para proteger al sistema tanto de CAs que puedan haber sido comprometidas, como de certificados digitales o claves públicas que pueden haberse revocado o comprometido.
1951. En el pasado, ya habido casos de gran impacto que revelan que, aunque comprometer una CA no es habitual, sí demuestran que es posible [Ref.- 267].
1952. Para mitigar el riesgo, Android permite añadir a una lista negra tanto certificados como claves públicas, incluso asociados a una CA. Desde Android 4.2 esta lista, que se compone de dos ficheros, puede ser actualizada de forma remota para añadir nuevas entradas:

```
/data/misc/keychain/pubkey_blacklist.txt → Contiene claves públicas o
certificados hoja (que no son de CA) revocados o comprometidos.

/data/misc/keychain/serial_blacklist.txt → Contiene los hashes o los
números de certificados de CAs comprometidas.
```

### 23.1.5. ANDROID WEBVIEWS

1953. Una WebView<sup>106</sup> es un componente del sistema basado en tecnología Chrome que permite a las apps mostrar contenidos web, como si se tratase de un navegador web personalizado, embebido y simplificado. Este contenido web puede incluir tanto páginas HTML como código JavaScript, que puede ser ejecutado por la app, por lo que las WebViews constituyen un componente crítico desde el punto de vista de seguridad en Android [Ref.- 129].
1954. Por ejemplo, mediante ataques de Cross-Site Scripting (XSS) e inyección de código JavaScript (por ejemplo en ataques MitM, Man-in-the-Middle, especialmente cuando no se hace uso de técnicas de cifrado del tráfico mediante HTTPS ni de una correcta y estricta verificación de los certificados digitales), es posible forzar a una app a ejecutar el código de un potencial atacante.
1955. Los componentes WebView son ampliamente utilizados por las apps para mostrar información, actuando de clientes web (en lugar de desarrollarse una app real completa), y por tanto, permiten obtener y mostrar contenidos o páginas web proporcionadas por los servidores y aplicaciones web asociados a la app.

<sup>106</sup> <http://developer.android.com/reference/android/webkit/WebView.html>

1956. Existen dos métodos críticos asociados a los componentes WebView. Por un lado, el método “setJavaScriptEnabled()”, que indica si se permite la ejecución de código JavaScript dentro de la WebView<sup>107</sup>.
1957. Pese a que por defecto este método no está habilitado, es decir, los componentes WebView no ejecutan código JavaScript por defecto, esta funcionalidad suele ser habilitada por los desarrolladores de apps a través del método “setJavaScriptEnabled()”.
1958. Por otro lado, el método “addJavascriptInterface()” proporciona elevadas capacidades al motor (y código) de JavaScript para invocar e interactuar con otros componentes y métodos (código) de Android. Por tanto, se recomienda sólo hacer uso del mismo por parte de las apps cuando se tenga plena confianza en el código HTML y JavaScript a ejecutar.
1959. Las versiones de Android 4.1 (API 16) e inferiores son vulnerables frente a la posibilidad de inyección de código JavaScript que permita la ejecución de comandos de sistema operativo, ya que se permite el uso de esta funcionalidad de manera generalizada y por defecto (CVE- 2012-6636).
1960. Durante los años 2011, 2012 y 2013 [Ref.- 62] se publicaron los detalles del impacto y las vulnerabilidades asociadas al método “addJavascriptInterface()” de WebView en dispositivos Android <= 4.1 (API <= 16), incluyendo la posibilidad de ejecución remota de código (RCE, *Remote Code Execution*). Un potencial código JavaScript malicioso puede hacer uso de las capacidades de interacción entre JavaScript y Java (reflexión, Java Reflection APIs), y al ser procesado por un componente WebView, ejecutar comandos de sistema operativo y código nativo a través de una shell (mediante el método “exec()” de Java y la invocación de, por ejemplo, “/system/bin/sh”).
1961. Esta vulnerabilidad no sólo afectaba a los componentes WebView de las apps de terceros de Android, sino también a apps nativas como el navegador web existente por defecto, por ejemplo en Android 4.1.2, al disponer del método “addJavascriptInterface()” habilitado por defecto (CVE-2013-4710) [Ref.- 151], o incluso en Android 4.2 y 4.3 (Jelly Bean) (CVE-2014-1939)<sup>108</sup>.
1962. La criticidad de esta vulnerabilidad es muy elevada, debido al número de componentes y apps que pueden verse afectados, y a la existencia de exploits disponibles públicamente (por ejemplo, en entornos ofensivos como Metasploit<sup>109</sup>).
1963. Versiones posteriores de Android, como Android 4.2 o superiores, también pueden ser vulnerables si las apps hacen uso de WebView y del método “addJavascriptInterface()” con compatibilidad para versiones anteriores de Android (4.1 o previas), o si por ejemplo, las apps emplean librerías de servicios y redes de publicidad y anuncios (Ads) que hacen uso de estas mismas capacidades dentro de la app. El impacto de un potencial ataque depende de los permisos y capacidades de cada app.
1964. Por defecto, desde la versión 4.2 de Android (API 17), y en concreto en el caso de las apps específicamente compiladas para esa versión (y/o versiones superiores) de Android (mediante la directiva “targetSdkVersion”), la vulnerabilidad ha sido mitigada. Para evitar este tipo de ataques, los componentes WebView, aunque dispongan del

<sup>107</sup> <http://developer.android.com/reference/android/webkit/WebSettings.html>

<sup>108</sup> <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1939>

<sup>109</sup> [http://www.rapid7.com/db/modules/exploit/android/browser/webview\\_addjavascriptinterface](http://www.rapid7.com/db/modules/exploit/android/browser/webview_addjavascriptinterface)

método “addJavascriptInterface()” habilitado, deben declarar específicamente la anotación “@JavascriptInterface”<sup>110</sup> para cada método que desean pueda ser invocado desde código JavaScript, y además esos métodos deben ser declarados como públicos.

1965. La implementación de WebView en Android estaba basada en WebKit<sup>111</sup> (motor utilizado por el navegador web por defecto de Android, Android Browser) hasta la versión Android 4.4, donde se empezó a hacer uso por defecto de Chromium<sup>112</sup> (motor utilizado por el nuevo navegador web existente por defecto en Android 4.4 o posterior, Chrome).
1966. Numerosas otras vulnerabilidades de seguridad que afectan a los componentes WebView han sido descubiertas y publicadas en los últimos años, afectando a versiones de Android inferiores a 4.4 (KitKat) [Ref.- 152] [Ref.- 61], tanto en su integración con JavaScript, como facilitando la utilización de técnicas de ataque para evitar la aplicación de la Same Origin Policy (SOP) en WebViews o el navegador web [Ref.- 118] [Ref.- 100], habiéndose publicado numerosas vulnerabilidades sobre la SOP (también conocidas como UXSS, Universal Cross-Site Scripting) para Android 4.3 [Ref.- 61].
1967. Google confirmó en enero de 2015 que no proporcionará actualizaciones y parches de seguridad para WebView en versiones de Android previas a 4.4 [Ref.- 119].
1968. Por tanto, se recomienda actualizar como mínimo a la versión 4.4 de Android (KitKat), o en su defecto, hacer uso de navegadores web que disponen de su propio motor de renderización (capacidad de procesar y mostrar contenidos web), como por ejemplo Chrome (disponible para Android 4.0 o superior) o Firefox (disponible para Android 2.3 o superior) para Android.
1969. Android 5.0 incluyó una nueva versión de Chromium para las WebViews con soporte para WebRTC, WebAudio y WebGL, junto al resto de especificaciones de Web Components. A través de una nueva clase (PermissionRequest) las apps pueden dar permiso a las WebViews para acceder a otros componentes o recursos, como la cámara o el micrófono.
1970. Aunque Chromium es el motor empleado para las WebViews desde Android 4.4, a partir de Android 5.0 se distribuyó como un fichero APK independiente y puede ser actualizado desde Google Play, con el objetivo de agilizar la distribución de actualizaciones que resuelvan problemas de seguridad (entre otros) que afecten al navegador web por defecto y a las apps que hacen uso de WebViews.
1971. El comportamiento por defecto de las WebViews para las apps cambió en Android 5.x, bloqueándose los contenidos mezclados (es decir, cuando una misma página web hace uso de contenidos HTTPS y HTTP<sup>113</sup>) y las cookies de terceros si la app especifica una versión obetivo del nivel de API 21 o superior [Ref.- 503].

<sup>110</sup> <http://developer.android.com/guide/webapps/webview.html>

<sup>111</sup> <https://www.webkit.org>

<sup>112</sup> <http://www.chromium.org>

<sup>113</sup> [https://developer.mozilla.org/en-US/docs/Web/Security/Mixed\\_content](https://developer.mozilla.org/en-US/docs/Web/Security/Mixed_content)

## 23.2. CORREO ELECTRÓNICO (E-MAIL) Y GMAIL

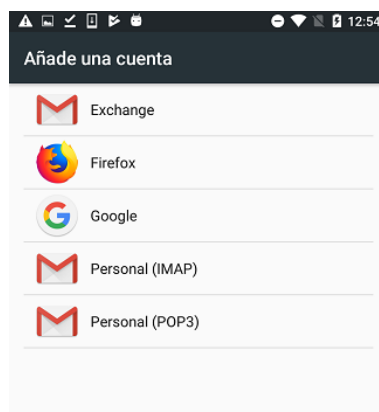
1972. Android proporciona múltiples capacidades para la gestión de correos electrónicos (e-mails) desde el dispositivo móvil, disponibles a través del icono o app “Correo” (app genérica de correo) desde el *Launcher* (como por ejemplo cuentas de correo de Exchange, IMAP o POP3, cuyo análisis detallado queda fuera del alcance de la presente guía), o desde el icono o app de “Gmail” (app específica de acceso a Gmail), desde los cuales es posible configurar una o varias cuentas de correo electrónico.

1973. Asimismo, existe una relación muy estrecha entre las cuentas de correo electrónico registradas, y las cuentas vinculadas al dispositivo móvil (ver apartado “20. Cuenta de usuario de Google”).

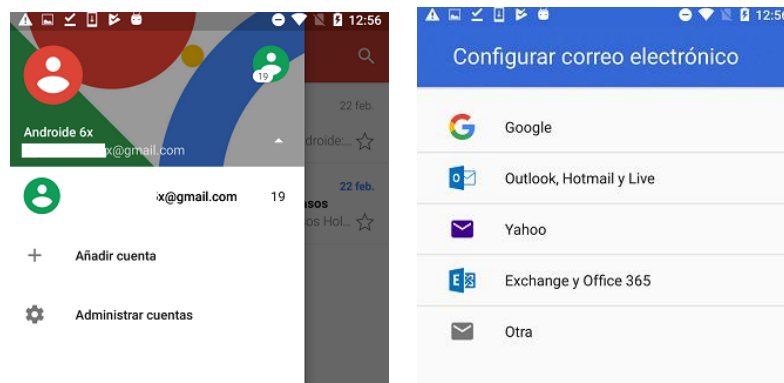
1974. Si se lleva a cabo la configuración de cuentas de correo electrónico mediante Exchange, POP3, o IMAP, incluyendo el envío de e-mails mediante SMTP, se recomienda siempre habilitar la opción de seguridad para hacer uso de conexiones cifradas (TLS), y deshabilitar cualquier opción que permita aceptar todos los certificados TLS (como aquellos no válidos, que no son de confianza o que están autofirmados).

1975. Para configurar una cuenta de correo en el dispositivo, las opciones son:

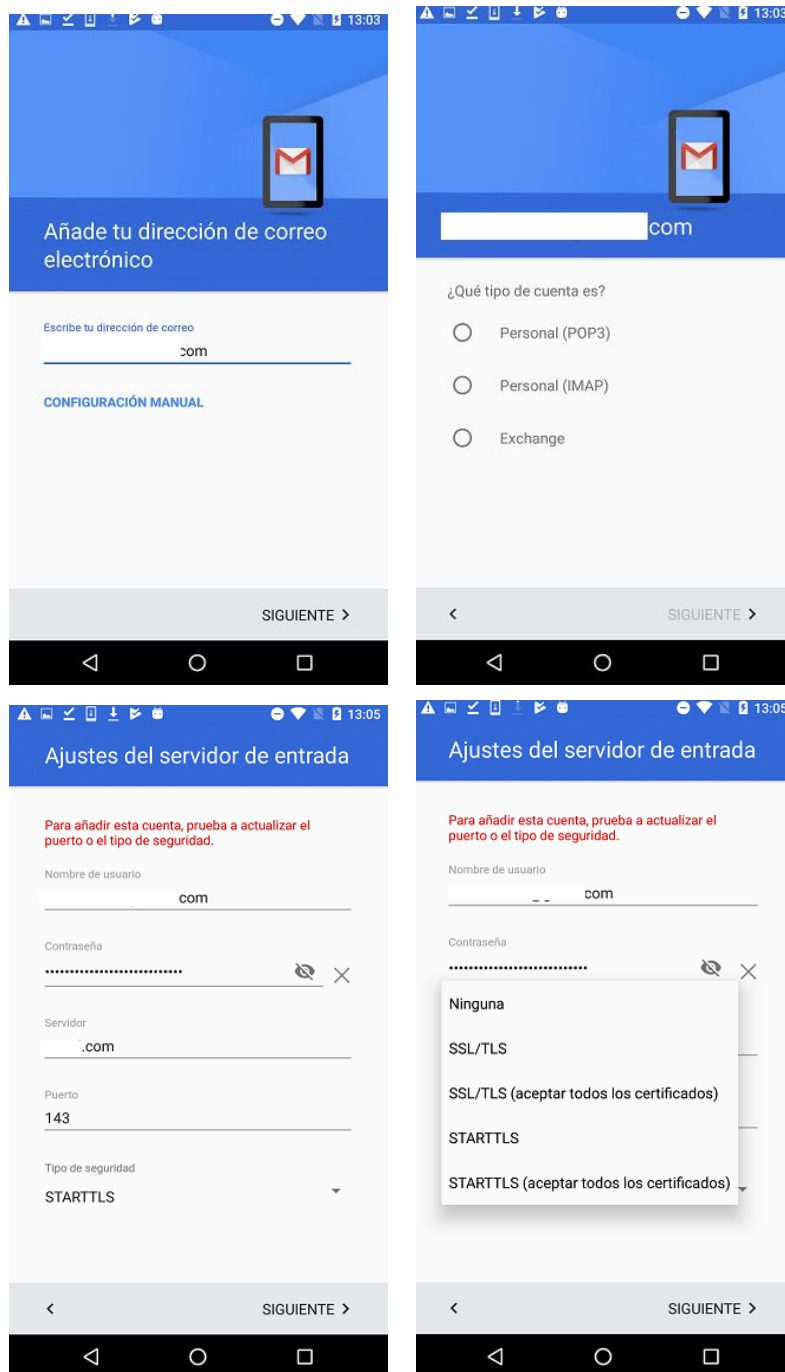
- “Ajustes - [Personal] Cuentas - + Añadir cuenta [Añade una cuenta]”.



- Aplicación Gmail: “Ajustes - seleccionar a la derecha de una cuenta sobre el símbolo de desplegar - Añadir cuenta”. Esta opción permite añadir los siguientes tipos de cuenta:



1976. Desde Android 5.x, la opción de tipo de seguridad disponible por defecto para IMAP y POP3 al añadir una nueva cuenta de correo electrónico mediante configuración manual es “STARTTLS” (en Android 4.x y anteriores era “Ninguna”):



1977. En el caso de Exchange, la opción por defecto es “SSL/TLS”, disponiéndose adicionalmente de la posibilidad de seleccionar un certificado digital cliente de usuario para llevar a cabo la autenticación con el servidor de correo electrónico.
1978. En cualquier caso, debe siempre seleccionarse “SSL/TLS” o “STARTTLS”, haciendo énfasis en que en ningún caso debe seleccionarse ninguna de las opciones con el texto “(acceptar todos los certificados)”.
1979. Debido a que la vinculación del dispositivo móvil con una cuenta de usuario de Google es prácticamente obligatoria, y a la relación existente entre esta cuenta y el servicio de correo de Google, Gmail, esta funcionalidad estará habilitada normalmente.
1980. Desde el punto de vista de seguridad, no se disponen de opciones avanzadas de configuración asociadas a Gmail desde el dispositivo móvil Android, ni siquiera a través del menú “Ajustes”, haciendo por defecto uso de cifrado mediante TLS.

1981. Aunque desde la versión 4 de Android se podría utilizar las capacidades de *certificate pinning*<sup>114</sup>, no aceptándose cualquier certificado digital como válido al establecerse una conexión cifrada mediante TLS con los servidores de Google [Ref.- 79], los servicios de Google desde Android, por ejemplo Gmail, YouTube o Google Play (entre otros), no hacen uso de mecanismos de protección propios basados en *certificate pinning*, y aceptan cualquier certificado digital de confianza que haya sido importado previamente por el usuario. Esto permite analizar las conexiones TLS con los servidores de Google y averiguar, por ejemplo, que el User-Agent de la app se identifica en la petición, así como el tipo de terminal (hammerhead) y el número de compilación.

```
User-Agent: Android-GmailProvider/60087425 (sw411dp; 420dpi) (bullhead MTC20K); gzip
```

1982. Respecto a la gestión de las credenciales de acceso a Gmail, se recomienda seguir las recomendaciones descritas en el apartado “20. Cuenta de usuario de Google”.

1983. Es de reseñar que la comunicación entre las aplicaciones de Google y los servidores Google utilizan el protocolo QUIC [Ref.- 220].

1984. Los ajustes de la aplicación de correo son accesibles desde la propia aplicación, mediante el botón de menú y “Ajustes”. Además de los “ajustes generales”, comunes a todas las cuentas de correo gestionadas desde la aplicación Gmail, los ajustes específicos para la cuenta se acceden seleccionando la cuenta.

1985. Los ajustes de la aplicación Gmail quedan fuera del alcance de la presente guía, por lo que, si se desea utilizar esta app, se recomienda al usuario revisarlos de forma detallada. Sin embargo, como carácter informativo, se expondrán algunos ajustes importantes desde el punto de vista de la seguridad y la privacidad.

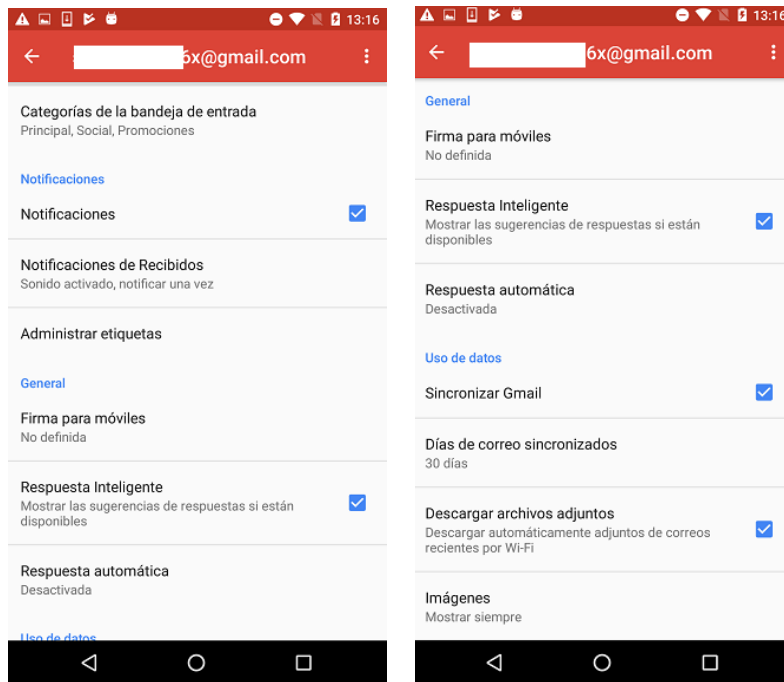
1986. Por defecto, al escribir un nuevo mensaje o e-mail desde la app de Gmail, el dispositivo móvil no añade ninguna firma, opción recomendada desde el punto de vista de seguridad para evitar indicar desde donde se realiza el envío, como por ejemplo “Enviado desde un dispositivo móvil”.

1987. Se recomienda mantener la configuración por defecto, con el valor de firma puesto a “No definida”, para no revelar información del fabricante o tipo de dispositivo móvil. En caso de querer añadir una firma, en ningún caso debería incluir detalles del terminal.

1988. La gestión de las firmas se puede realizar desde el botón de menú de la app de Gmail, mediante la opción “Ajustes - <cuenta de usuario de Google> - Firma para móviles” (por defecto “No definida”):

<sup>114</sup> <https://developer.android.com/training/articles/security-ssl.html>





1989. Por defecto, el ajuste “Descargar archivos adjuntos” está habilitado, de forma que los adjuntos a los correos se descargarán automáticamente si se detecta la utilización de una conexión Wi-Fi. Se recomienda deshabilitar esta opción y dejar que el usuario decida cuándo descargar y abrir un adjunto en función de la confianza que se tenga en el mismo.

### 23.3. REDES SOCIALES

1990. Android 6.x no incluye por defecto apps para el acceso a diferentes redes sociales disponibles en Internet, qué si estaban incluidas en versiones previas de Android (2.x). La existencia de estas apps por defecto es siempre dependiente del fabricante u operador de telefonía móvil que comercializa el dispositivo móvil, como por ejemplo Facebook o Twitter para Android.

**Nota:** Otros dispositivos móviles basados en Android, así como otras versiones de Android, incluyen adicionalmente apps de acceso a otras redes sociales y servicios web.

1991. En el caso de Android 6.x sólo se dispone de acceso a las apps para las redes sociales propias de Google, como por ejemplo YouTube, Hangouts y Google+.

1992. Siempre se recomienda, antes de hacer uso de cualquiera de las apps disponibles por defecto en el dispositivo móvil, o de las apps instaladas posteriormente, realizar un análisis de seguridad en profundidad para identificar posibles comportamientos vulnerables. En caso de no querer utilizarlas, se sugiere proceder a su desinstalación.

### 23.4. APPS DE TERCEROS: GOOGLE PLAY

1993. Google Play (anteriormente denominado Android Market), es empleado por Google para la distribución y venta de apps y software para la plataforma Android, es decir, constituye el mercado oficial de aplicaciones móviles (apps) de Google.

1994. Android incluye una app, denominada “Play Store”, disponible desde el *Launcher*, para el acceso a este servicio directamente desde el dispositivo móvil:



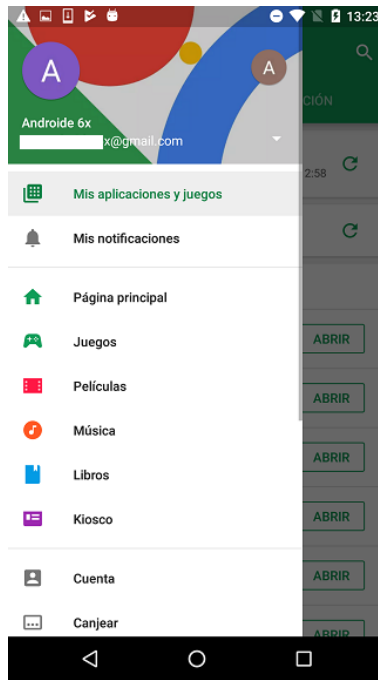
1995. La primera vez que se utiliza Play, la app solicita al usuario disponer de una cuenta de usuario de Google (si no se ha configurado una todavía en el dispositivo móvil), y le permite darla de alta o crear una nueva (ver apartado “20. Cuenta de usuario de Google”), tras aceptar los términos del servicio.

1996. La conexión de autenticación empleando la cuenta de usuario de Google, y el acceso a Google Play, se realiza a través de HTTPS hacia los servidores “www.google.com”, “android.clients.google.com”, “\*.googleusercontent.com”, y hacia otros servicios de Google.

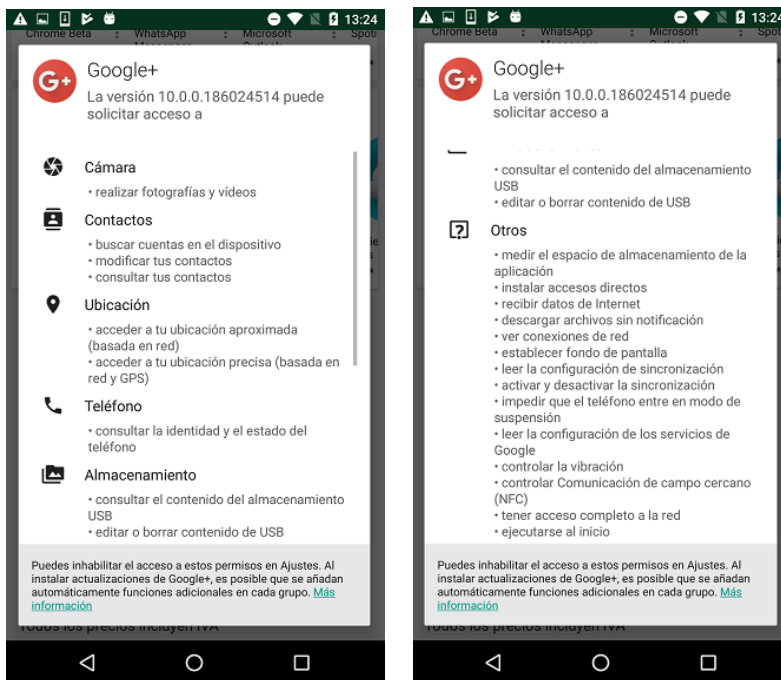
1997. Teóricamente, la integridad de las apps de Android se verifica a través de una firma digital asociada al fichero binario (.apk) descargado, pero una posible ausencia de cifrado en el tráfico empleado para descargar las apps (mediante HTTP), no así en el tráfico de acceso a Google Play que emplea HTTPS, abre potencialmente la puerta a la manipulación de este intercambio de datos, por ejemplo, mediante la sustitución de apps válidas firmadas digitalmente.

1998. Se recomienda actualizar a la última versión de las apps ya instaladas en el dispositivo móvil (ver apartado “23.9.1. Actualización de apps en Android”), ya que éstas proporcionarán posibles soluciones frente a vulnerabilidades de seguridad públicamente conocidas.

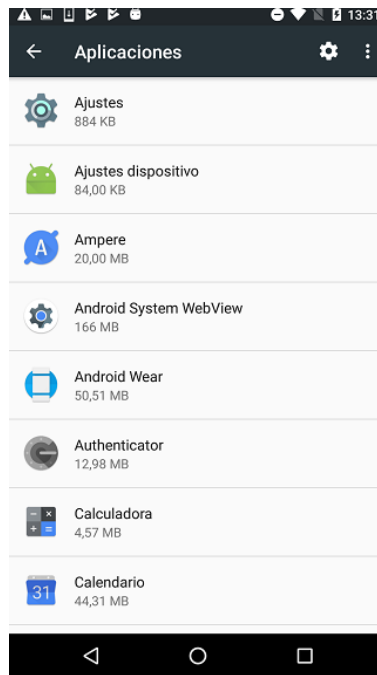
1999. La lista de programas o apps instaladas desde Google Play es accesible desde la propia app “Play Store”, mediante el icono del menú, “Mis aplicaciones y juegos” de Google Play, disponiéndose de tres pestañas para clasificar las apps: “Instaladas” (las instaladas en el dispositivo móvil), “Actualizaciones” (apps instaladas en el dispositivo móvil para las que existe alguna actualización) y “Colección” (apps instaladas en otro dispositivo, pero no en éste, con la cuenta de Google del usuario y/o apps que estuvieron instaladas en el dispositivo móvil anteriormente pero que se eliminaron):



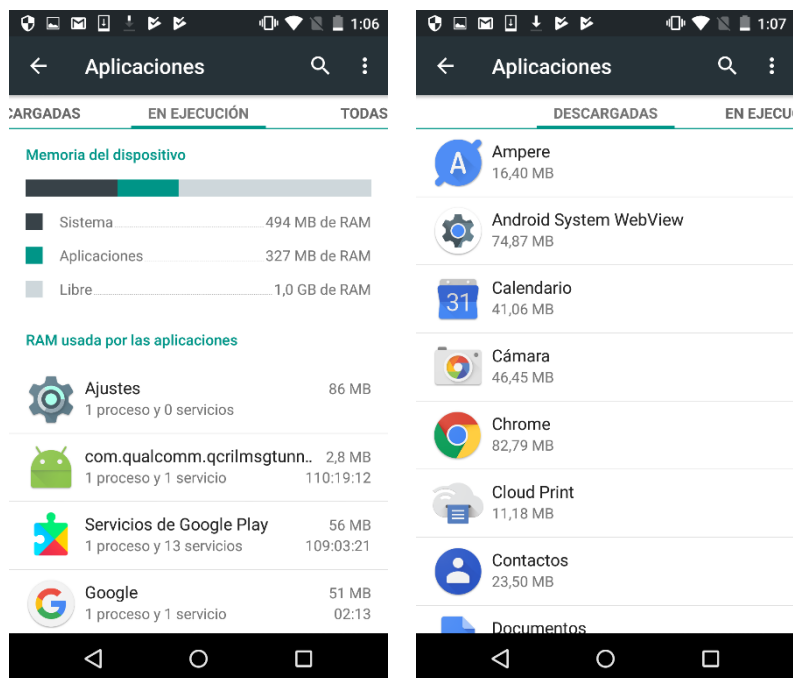
2000. Desde la app “Play Store” es posible, una vez se ha seleccionado una app, ver todos sus detalles (al igual que desde la web de Google Play), como por ejemplo su descripción, las novedades, el número de descargas, las valoraciones y comentarios de otros usuarios (siendo posible emitir una valoración), las categorías o tipo de app, enlaces a apps similares, la clasificación de su contenido, la versión (o si existen múltiples versiones según el tipo de dispositivo móvil y la versión de Android) y fecha de la última actualización, el tamaño, la información de contacto del desarrollador, su política de privacidad, u obtener información sobre los permisos solicitados por la app, entre otros. Adicionalmente, es posible abrirla, actualizarla, e instalarla (si todavía no está disponible en el dispositivo móvil):



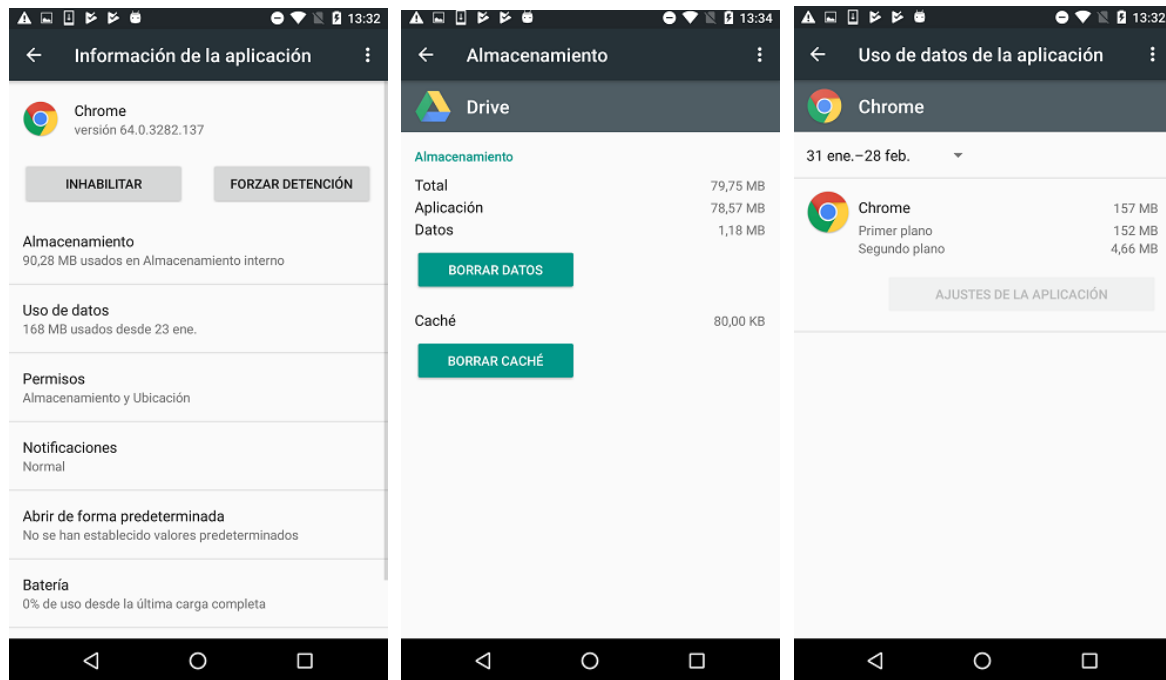
2001. Adicionalmente, el listado de apps está disponible también desde el propio Android a través del menú “Ajustes [Dispositivo] - Aplicaciones”.



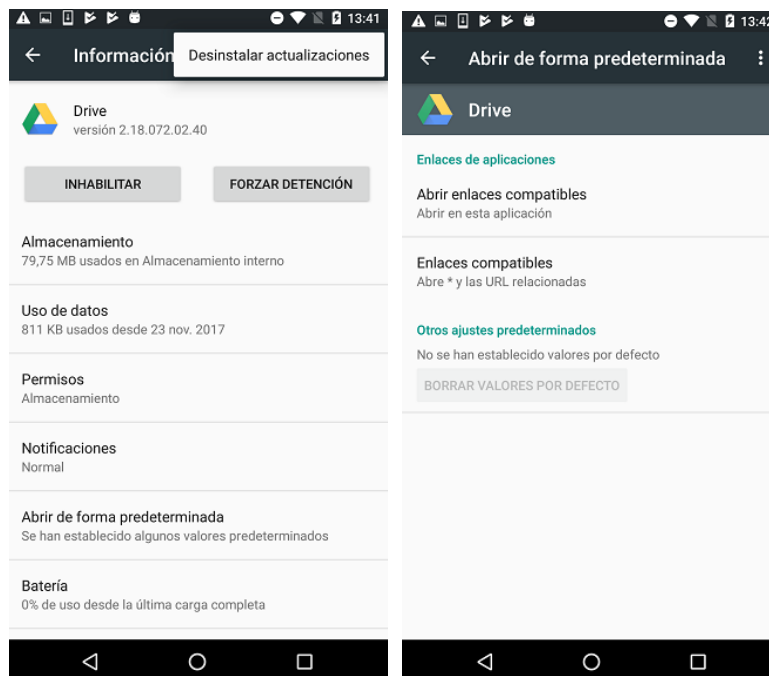
2002. Hasta Android 5.x, las aplicaciones se clasificaban en tres pestañas: “Descargadas”, “En Ejecución”, o “Todas”, para clasificar las apps que han sido instaladas alguna vez en el dispositivo móvil, que están ejecutando actualmente, o todas las apps. Sin embargo, esta clasificación no está disponible en Android 6.x:



2003. Desde el menú “Ajustes [Dispositivo] - Aplicaciones” es posible, una vez se ha seleccionado una app, acceder a sus detalles técnicos, como por ejemplo la versión, el tamaño que ocupa en el almacenamiento (total, y dividido por la app y por sus datos), el tamaño ocupado en caché, determinar si se mostrarán notificaciones generadas por la app, el uso de datos móviles en un período concreto, tanto en primer como en segundo plano, u obtener información sobre los permisos solicitados por la app, entre otros.



2004. Mediante la selección de cualquier permiso es posible obtener una descripción general del mismo. Adicionalmente, es posible forzar la detención de la app si no responde, desinstalar actualizaciones (a través del menú “[...]” de la esquina superior derecha, lo cual permite la sustitución de la app por su versión de fábrica), inhabilitarla, borrar sus datos o su caché, y borrar los valores predeterminados, que indican para qué acciones se iniciará esta app:



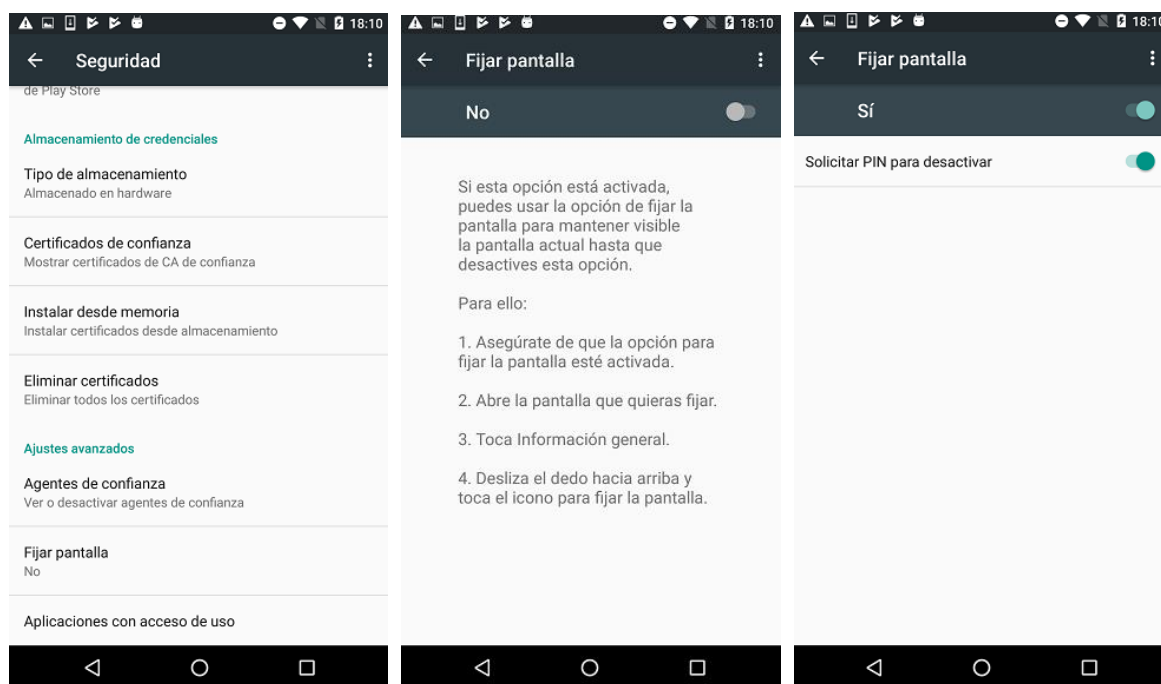
2005. La opción “Abrir de forma predeterminada” está relacionada con lo que en Android se denomina “(Android) App Links” (ver apartado “23.12. Enlaces y referencias web desde las apps”).

2006. Debe tenerse en cuenta que la disponibilidad de una app en Google Play no asegura que la misma no sea maliciosa y pueda llevar a cabo acciones desde el dispositivo móvil en el que ha sido instalada que afecten a la seguridad y privacidad del usuario [Ref.-400].

2007. Se recomienda analizar en detalle el contenido y procedencia de una app de terceros antes de instalarla desde Google Play en el dispositivo móvil, por ejemplo, identificando a su desarrollador, el tiempo que lleva la app publicada en Google Play, su valoración y reputación por parte de otros usuarios, etc.
2008. Una vez se ha configurado una cuenta de usuario de Google en el dispositivo móvil y ambos han sido vinculados (ver apartado “20. Cuenta de usuario de Google”), desde la sección de “Ajustes” de la aplicación web de Google Play (“https://play.google.com/store/account”) también será posible gestionar las apps disponibles, como también lo será a través del “Administrador de dispositivos Android” (ver apartado “8.1. Gestión remota de dispositivos Android por parte del usuario”), el o los dispositivos móviles asociados a la cuenta del usuario.

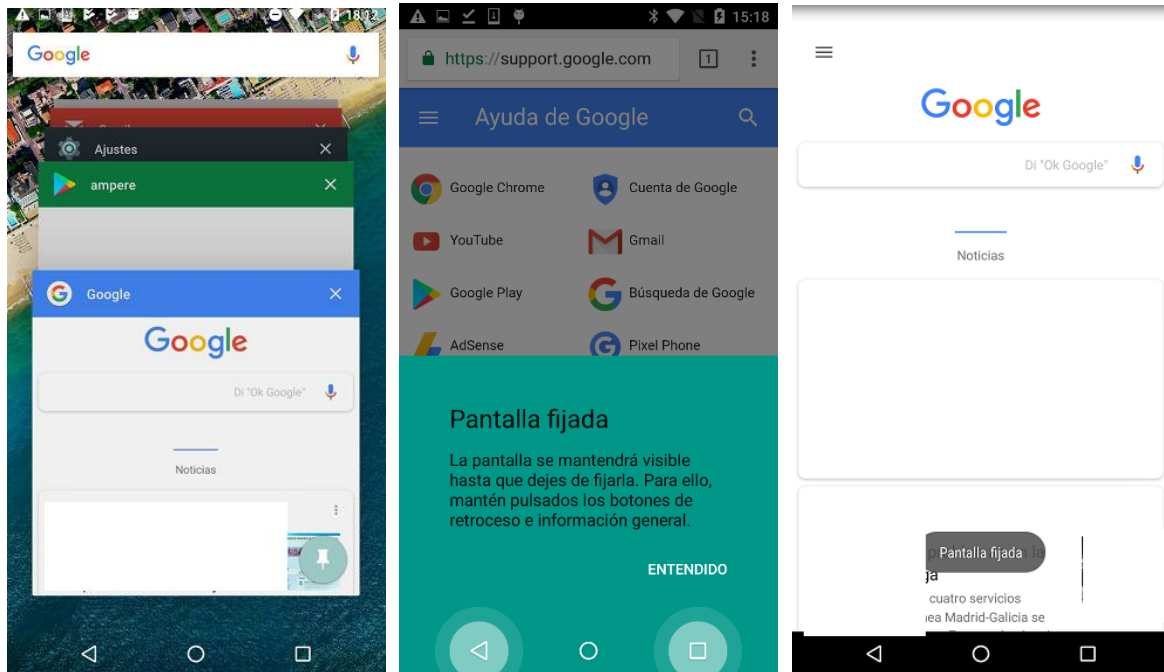
### 23.5. SCREEN PINNING

2009. Una de las características que introdujo Android 5.x es el denominado “*screen pinning*” (o fijación de pantalla) [Ref.- 515], que permite que el usuario pueda dejar en primer plano una aplicación para que pueda ser utilizada, y sin que sea posible cambiar a otra app distinta.
2010. Las capacidades de *screen pinning* restringen que el usuario pueda salir de la actividad o app mostrada actualmente (o que su ejecución sea interrumpida por las notificaciones), funcionalidad muy conveniente en entornos educativos o kioscos con un único propósito.
2011. Para hacer uso de esta funcionalidad, es necesario activarla desde el menú “Ajustes - [Personal] Seguridad - [Avanzado] Fijar pantalla”. Se recomienda marcar la opción “Solicitar PIN para desactivar” para que, una vez se salga de la pantalla o app que se había fijado, el dispositivo móvil muestre la pantalla de bloqueo y sea necesario introducir el código de acceso para desbloquear y acceder al dispositivo.

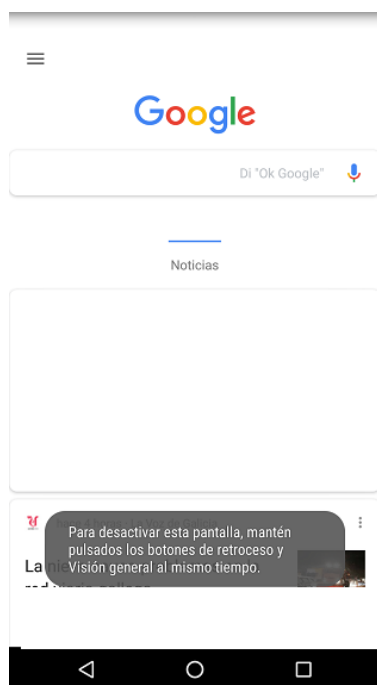


2012. Para fijar una pantalla o app concreta, se ha de pulsar el botón de actividades o apps en ejecución, también denominado “Recientes” (correspondiente a un icono cuadrado situado en la parte inferior derecha de la pantalla) y arrastrar la barra de título de la app

a fijar. Aparecerá un símbolo de *pin* en un círculo azul que, al tocarse, fijará la pantalla o app seleccionada.



2013. Para dejar de fijar una pantalla o app concreta, si esta funcionalidad fue activada manualmente por el usuario, éste deberá presionar simultáneamente los botones de “retroceso” (icono con un triángulo o flecha hacia la izquierda situado en la parte inferior izquierda de la pantalla) y (de nuevo) el botón de “Recientes”, del dispositivo móvil [Ref.- 236].



2014. El usuario no podrá acceder a la pantalla principal, ejecutar otras apps, visualizar las apps recientes o recibir notificaciones en este modo hasta que se finalice la ejecución de la app sobre la que se ha activado el *screen pinning*, independientemente de si se ha activado manualmente por parte del usuario (tal como se ha descrito previamente) o



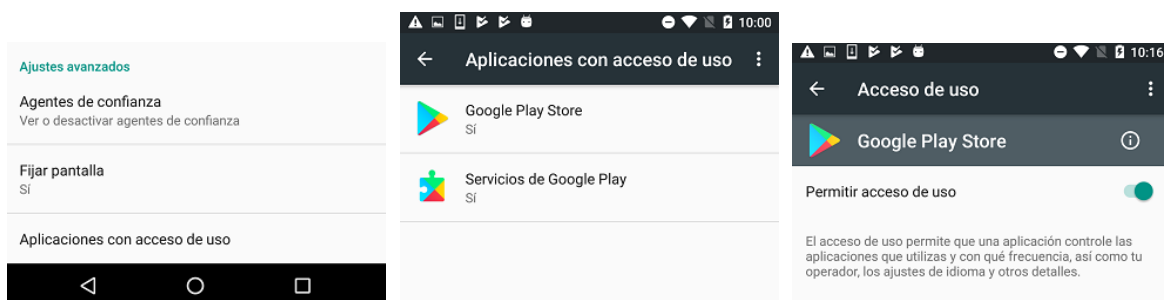
desde el código en ejecución de la propia app<sup>115</sup> (que debe ser una app con capacidades propietarias del dispositivo para poder hacer uso de *screen pinning*; en caso contrario se solicitará autorización por parte del usuario antes de proceder a fijar la pantalla).

2015. Se recomienda también hacer uso de esta funcionalidad si, por cualquier razón, se ha de prestar temporalmente el dispositivo móvil a un tercero, pero sólo se desea que acceda a una aplicación concreta.

### 23.6. ESTADÍSTICAS DETALLADAS DE USO DE LAS APPS

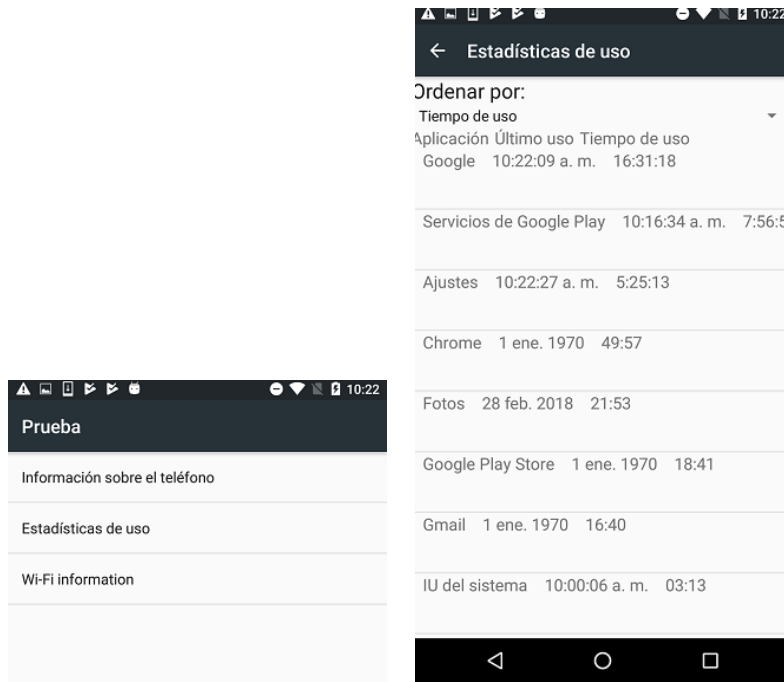
2016. Tradicionalmente, una de las técnicas de ataque a aplicaciones móviles (especialmente de banca on-line) es la que se conoce como “overlay attack” (ataque de superposición). Este ataque consiste en suplantar la ventana activa de una app superponiendo una ventana maliciosa para recabar datos sensibles del usuario (credenciales, tarjetas de crédito, etc.). Para implementar este tipo de ataque, un elemento clave es poder determinar qué aplicación está ejecutando en primer plano.

2017. Android 5.0 Lollipop afrontó esta amenaza introduciendo la API *UsageStatsManager* en sustitución de la API *getRunningTasks()*. La API *UsageStatsManager* introdujo un permiso de sistema, denominado `PACKAGE_USAGE_STATS`, sin el cual las apps no dispondrán de capacidad para recabar estadísticas detalladas de uso de todas las apps disponibles en el dispositivo móvil. Para otorgar o revocar este permiso, el usuario puede acceder a “Ajustes - [Personal] Seguridad - [Avanzado] Aplicaciones con acceso de uso”:



2018. Para recabar estadísticas de uso de las apps, Android dispone de la función experimental “Estadísticas de uso”, accesible mediante la marcación en la app “Teléfono” del código “\*`##4636##`”:

<sup>115</sup> Mediante una llamada al método “startLockTask()” o “setLockTaskPackages()”.



2019. La ventana que se despliega contiene el nombre de la app, la fecha de último uso y el tiempo de uso.

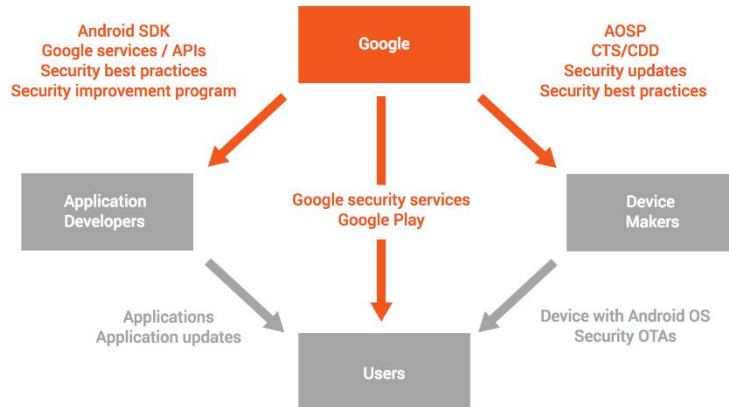
2020. Aunque existen diversas apps que permiten obtener estadísticas más detalladas sobre el uso de otras apps, no se recomienda hacer uso de ellas.

### 23.7. SAFETYNET

2021. SafetyNet es una plataforma desarrollada por Google en 2013 para analizar la configuración de los dispositivos móviles Android, incluyendo un conjunto de servicios de seguridad, tanto en el propio dispositivo móvil como “en la nube”, a través de Google Mobile Services (GMS)<sup>116</sup> y Google Play Services (GPS).

2022. SafetyNet tiene implicaciones muy relevantes desde el punto de vista de seguridad y la integridad del dispositivo móvil, ya que es empleada por el equipo de seguridad de Android para monitorizar, junto a la funcionalidad de verificación de apps (“Verify Apps”, ver apartado “23.8. Verificación de seguridad de las apps: Google Play Protect”), la existencia de ataques y código dañino o, como se han sido referenciados más recientemente, PHAs (*Potentially Harmful Applications*) [Ref.- 24], dentro del ecosistema de seguridad de Android.

<sup>116</sup> <https://www.android.com/gms/>



2023. Verify Apps se centra más en la detección y protección frente a PHAs (*potential harmful application*), mientras que SafetyNet se centraba (al menos inicialmente) en ataques a través de la red, aunque las capacidades de ambos sistemas se han ido integrando y combinando a lo largo del tiempo.
2024. Los dispositivos móviles Android pueden remitir a Google, a través de los servicios “en la nube” de SafetyNet, información de seguridad como eventos, logs, o información de configuración [Ref.- 24].
2025. Desde 2013, Google comenzó a introducir mecanismos en el código de la plataforma Android y/o de las apps para detectar intentos de explotación de vulnerabilidades y generar eventos de log asociados, con el objetivo de poder identificar tendencias de ataque (así como estadísticas de amenazas según la localización geográfica) y evaluar la efectividad de los mecanismos de protección existentes. En 2015, se añadieron capacidades de detección para nuevas vulnerabilidades, como Stagefright.
2026. En Android 4.2 se introdujeron capacidades de *certificate pinning* y de listas negras de certificados asociadas a la gestión de las autoridades certificadoras (CAs) en Android. Desde Android 4.4, Android genera un aviso al usuario indicando que se ha instalado localmente un certificado digital que podría permitir la intercepción del tráfico SSL/TLS. Desde octubre de 2014, SafetyNet hace uso de pruebas activas asociadas al tráfico de red para identificar escenarios en los que se haya podido manipular el almacén de CAs local.
2027. Asimismo, SafetyNet ha sido empleada desde 2014 para identificar apps que intentan engañar al usuario a la hora de enviar mensajes SMS *premium* en campañas de fraude a través de SMS. La información obtenida es empleada para bloquear las apps dañinas a través de Verify Apps, o eliminarlas de Google Play.
2028. En 2015 las capacidades de SafetyNet, y de envío de datos (supuestamente) anónimos a Google, se comenzaron a emplear para detectar PHAs y complementar la funcionalidad de Verify Apps, a través de un motor de correlación de anomalías (*Anomaly Correlation Engine*, ACE).
2029. En 2015 también se ampliaron sus capacidades para realizar chequeos de integridad del dispositivo móvil (cuando éste está ocioso) a través de un servicio “en la nube” denominado *System Integrity Check* (SIC), pudiendo detectar modificaciones de la partición de sistema, como las realizadas por ROMs, versiones o *firmwares* de Android personalizados, por apps dañinas que realicen modificaciones del sistema y (potencialmente) detectar apps que podían permitir aplicar el proceso de *root* sobre el

dispositivo móvil. Este tipo de apps no están permitidas en Google Play por política de Google, y Verify Apps avisa al usuario cuando intenta instalar una app con estas capacidades, o (de nuevo) una app dañina que intenta explotar alguna vulnerabilidad de escalada de privilegios.

2030. Asimismo, las capacidades de SafetyNet han sido ampliadas para detectar si el dispositivo móvil se encuentra *rootado*. Gracias a la funcionalidad y capacidades de detección de SafetyNet, algunas apps como Android Pay no ejecutarán en dispositivos móviles *rootados*.

2031. Se introduce lo que se denomina “*SafetyNet attestation*” (testimonio de SafetyNet) como característica de los Google Play Services (GPS), que Google otorga a una aplicación (o a un dispositivo móvil) tras someterla a unos test de compatibilidad, o CTS (*Compatibility Test Suite*), antes de admitirla para su inclusión en los servicios de Google Play.

2032. Además, el contexto de SafetyNet se extiende a que las aplicaciones no puedan ejecutar si un dispositivo se considera que este se encuentra en estado “*tampered*” (alterado), como en el caso de que haya sido *rootado*, infectado con malware, monitorizado, etc.

2033. Google emplea el término “CTS compatible” para los dispositivos que se consideran “no alterados”, lo cual no significa que estén libres de vulnerabilidades o actualizados a las últimas versiones de las apps o de parches de seguridad del propio sistema operativo Android.

2034. En este sentido, SafetyNet resulta útil para los desarrolladores y no tanto para el usuario final, pues asegura a los primeros que su aplicación solo ejecutará en dispositivos que se encuentren en el estado para el que la aplicación ha sido diseñada.

2035. Para hacer uso de las capacidades de “SafetyNet Attestation” la aplicación debe invocar el método `SafetyNetApi.attest()` del SDK de Google Play Services incluyendo un timestamp, que se envía a los servidores de Google a través de `GoogleApiClient` [Ref.- 25].

2036. Google responderá en formato “JSON Web Signature (JWS)” incluyendo el parámetro “*ctsProfileMatch*” con valor verdadero o falso.

2037. La aplicación verificará este valor, con lo cual podrá determinar si el dispositivo es “CTS compatible” y, en consecuencia, permitir o denegar su ejecución en el dispositivo. Esta verificación se puede realizar también en el servidor designado por la aplicación, logrando así que se pueda impedir acceso a los servicios de una aplicación de forma centralizada, y no en la parte cliente, que podría ser fácil de manipular. Este es el caso de AndroidPay.

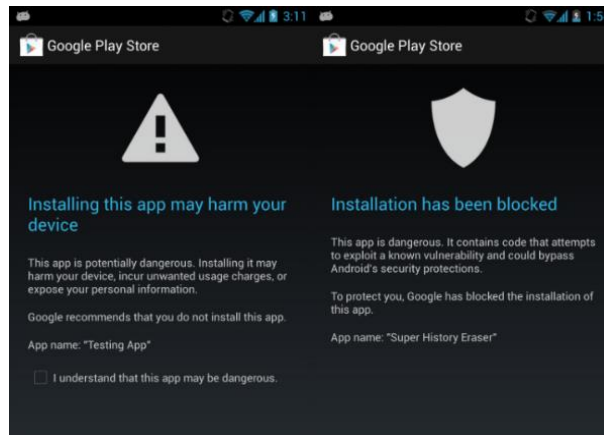
2038. El uso de estas características y capacidades de SafetyNet pueden consultarse en la página oficial de Google [Ref.- 98].

2039. Con el objetivo de ocultar que se ha realizado el proceso de root en el dispositivo móvil Android, existen herramientas como Magisk (Manager) [Ref.- 103] (u otras herramientas que ocultan la presencia del binario “su” y sus componentes), que modifican el comportamiento del sistema de cara a ocultarlo en SafetyNet, en un proceso constante de actualización de los mecanismos de detección por parte de Google (dentro de SafetyNet) y de ocultación por parte de la comunidad (con nuevas herramientas).

2040. Mediante apps como SafetyNet Helper Sample [Ref.- 12] y SafetyNet Playground [Ref.- 35] es posible consultar el estado del dispositivo móvil en SafetyNet y conocer los detalles de la evaluación actual según este servicio de Google.
2041. Por otro lado, SafetyNet puede ser utilizada por parte de las apps (a través de una API vinculada a *Google Play Services*, GPS) para evaluar las capacidades, tanto hardware como software, de un dispositivo móvil y analizar la compatibilidad del mismo con la app (empleando perfiles de compatibilidad y en base a la CTS, *Compatibility Test Suite* [Ref.- 87]), intentando asegurar que la app funcionará correctamente en el dispositivo y mejorar la experiencia del usuario [Ref.- 90].

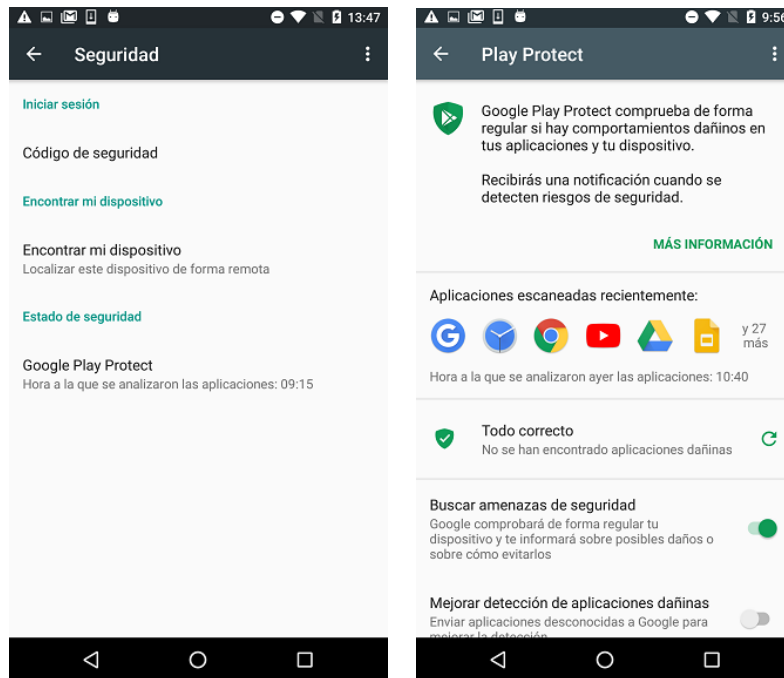
### 23.8. VERIFICACIÓN DE SEGURIDAD DE LAS APPS: GOOGLE PLAY PROTECT

2042. A lo largo del tiempo, Android ha incorporado diferentes mecanismos para analizar las aplicaciones publicadas por los desarrolladores a través del mercado oficial Google Play, llevando a cabo un proceso de escaneo o verificación de seguridad automático sobre dichas apps.
2043. Para ello, hace uso de un sistema de análisis denominado Google Bouncer, cuyo principal propósito es identificar apps que contienen software malicioso (*malware*).
2044. Google Bouncer [Ref.- 169] compara cada app con otras muestras de software malicioso conocidas, y también ejecuta las apps en un entorno virtual, simulando su ejecución en un dispositivo móvil Android, para analizar su comportamiento antes de proceder a su publicación oficial, e intentando identificar comportamientos maliciosos o anómalos normalmente asociados al *malware*.
2045. El sistema Google Bouncer analiza nuevas apps, apps existentes previamente en Google Play, reanaliza apps ya analizadas previamente una vez se incorporan nuevas capacidades al sistema, y también analiza cuentas de desarrolladores de Android (especialmente las de los nuevos desarrolladores, para evitar que agentes que distribuyen *malware* para Android lo hagan empleando la identidad de otros supuestos nuevos desarrolladores).
2046. Por otro lado, desde la versión 4.2 de Android en el año 2012, Android dispuso de capacidades para el escaneo o verificación de seguridad de las apps durante el proceso de instalación, con el objetivo de identificar y detectar la existencia de software malicioso (*malware*) en las mismas, característica conocida (en inglés) como “Verify Apps” [Ref.- 171].
2047. Inicialmente (desde Android 4.2), las capacidades de verificación de apps comparaban la app a instalar con una base de datos de apps existente en Google, con el objetivo de identificar si correspondía a un app ya conocida con comportamiento malicioso o dañino. El proceso de verificación envía a Google información sobre el nombre de la app, su tamaño, su *hash* SHA1, la versión y la URL asociada [Ref.- 173].
2048. En caso de identificarse la app como dañina, en función del nivel de peligrosidad asociado a la app, Android podía recomendar al usuario que no instalase la app (en el caso de apps potencialmente dañinas), o incluso llegar a bloquearla (en el caso de apps confirmadas como dañinas), no siendo posible proceder con su instalación [Ref.- 170]. Las siguientes imágenes muestran un ejemplo de cómo se notificaba al usuario sobre la potencial peligrosidad de una app:

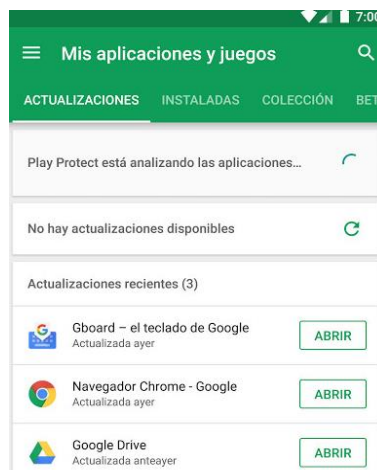


2049. Esta verificación se lleva a cabo para las apps que son instaladas manualmente por el usuario, por ejemplo desde una página web, un mercado de apps de Android no oficial, o a través de ADB (proceso conocido como *sideload*).
2050. Para que sea posible instalar una app a través de un medio distinto a Google Play, es necesario habilitar previamente la instalación de apps de fuentes que no son de confianza, mediante la opción “Orígenes desconocidos” (ver apartado “7.5. Instalación de apps (de orígenes desconocidos) en Android”).
2051. Este matiz es fundamental ya que, si la opción de “Orígenes desconocidos” no está activada, es aún posible instalar apps vía ADB (si se han permitido las opciones de desarrollo y la depuración vía USB) sin que se active la funcionalidad de verificación de apps.
2052. Para las apps instaladas desde Google Play se confía fundamentalmente en la verificación realizada por el servicio Google Play Protect.
2053. El framework “Verify Apps” se encargaba inicialmente de escanear las apps durante su instalación. A partir de 2014, se le añadió la capacidad de escanear (como servicio en segundo plano) las apps instaladas en el dispositivo móvil durante su ejecución, para identificar comportamientos inesperados que no fueron detectados durante la instalación [Ref.- 172] por si resultaban maliciosos. Así se extendió la funcionalidad a las apps que ya estaban instaladas en el dispositivo móvil.
2054. En el año 2015 la funcionalidad de “Verify Apps” fue extendida para poder eliminar apps que se registran como Administradores del Dispositivo, y para deshabilitar apps que han sido instaladas en la partición de sistema tras comprometer el modelo de seguridad de Android.
2055. Asimismo, se añadieron mejoras en el interfaz gráfico de usuario para evitar la instalación de PHAs por descuido o desconocimiento por parte del usuario, y la posibilidad de que el usuario pueda remitir una app a Google desde el propio dispositivo móvil para su revisión.
2056. A partir de febrero de 2017, se añadió al interfaz gráfico de Android un menú que mostraba información sobre la funcionalidad “Verify Apps”, al que se accedía desde “Ajustes - [Personal] Google - [Servicios] Seguridad - [Verificar aplicaciones] Verificar aplicaciones”. En este menú se puede ver tanto el registro de las aplicaciones escaneadas como activar la opción “Buscar amenazas de seguridad en tu dispositivo”.

2057. En la conferencia Google I/O de julio de 2017, Google presentó el servicio “Google Play Protect”, que integraba y extendía la funcionalidad “Verify Apps”. Este servicio se empezó a distribuir como una actualización de los “Servicios de Google Play” a partir de su versión 11 y superiores, y, desde el punto de vista de configuración, se integra bajo “Ajustes - [Personal] Google - [Servicios] Seguridad - Google Play Protect”:



2058. El servicio Google Play Protect analiza automáticamente las apps del dispositivo cuando éste no está siendo utilizado y cuando está conectado a un cargador de corriente, a fin de afectar lo menos posible a su rendimiento. Desde la app “Play Store”, y seleccionando el menú “Mis aplicaciones y juegos”, es posible determinar cuándo se ha ejecutado el servicio Google Play Protect por última vez, así como lanzarlo en ese momento a través de la pulsación en la flecha circular situada a la derecha:

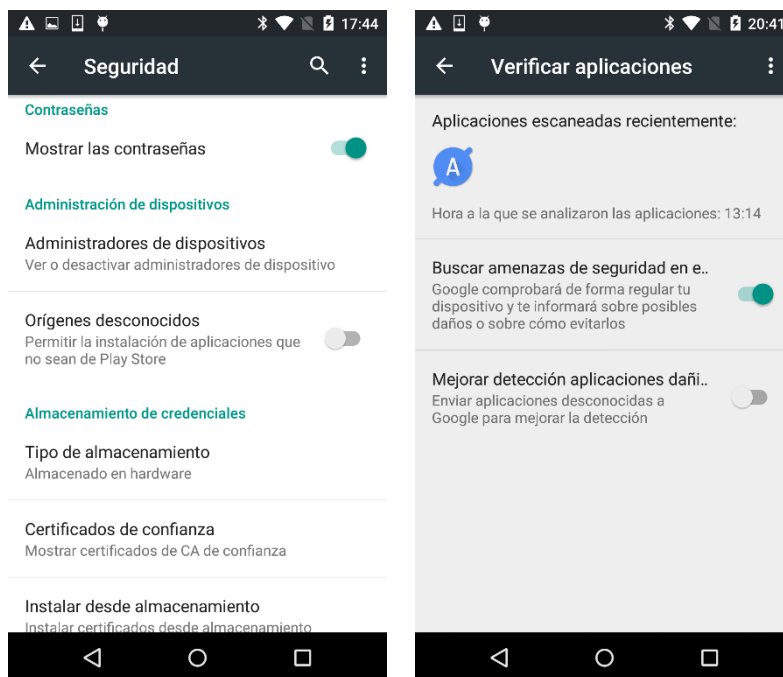


2059. Como parte de la integración entre el servicio Google Play Protect y el mercado oficial de apps de Google, Google Play, mediante la app “Play Store”, cuando se inicia la instalación de una app se mostrará el mensaje “Verificado por Play Protect” si la app ha sido ya analizada a través de dicho mecanismo:



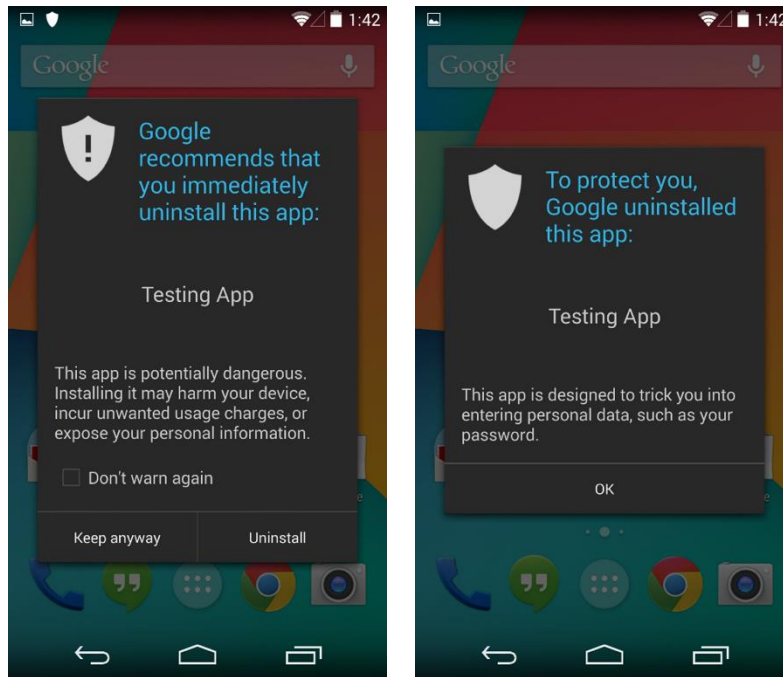


2060. Adicionalmente, en el menú “Play Protect”, se añaden las opciones “Mejorar detección de aplicaciones dañinas”, que enviará a Google información sobre las aplicaciones que se han instalado fuera de Google Play para que las analice en busca de malware, y “Buscar amenazas de seguridad”, que es la opción para habilitar/deshabilitar el servicio “Play Protect”.
2061. A pesar de que a fecha de elaboración de la presente guía existen estudios que no demuestran aún la efectividad de detección de este servicio, probablemente debido a su corta vida [Ref.- 271], se recomienda mantenerlo habilitado desde el punto de vista de seguridad.
2062. La primera vez que se instala una app desde una fuente que no es de confianza, Android mostrará una pantalla solicitando al usuario la capacidad para enviar a Google, como parte de la funcionalidad “Verify Apps”, información sobre el dispositivo móvil (como por ejemplo URLs asociadas a la app, el identificador del dispositivo móvil, la versión de Android, la dirección IP, cookies, etc.):



2063. Adicionalmente, al activar la verificación de apps, Google recopilará información (supuestamente) anónima sobre las apps que son instaladas desde fuera de Google Play, con el objetivo de mejorar la detección de apps dañinas [Ref.- 173].
2064. En caso de identificarse la app como dañina, Android puede recomendar al usuario que desinstale la app o incluso llegar a eliminar la app del dispositivo móvil<sup>117</sup>:

<sup>117</sup> Imágenes: <http://www.businessinsider.com/google-verify-apps-for-android-phones-2014-4>



2065. Las capacidades de verificación de apps se encuentran habilitadas por defecto en Android 6.x (no necesariamente en versiones previas de Android 4.2.x o superior).
2066. En el caso de dispositivos móviles Android multi-usuario, únicamente el usuario propietario podrá activar o desactivar la verificación de apps.
2067. Desde el punto de vista de seguridad se recomienda dejar habilitada la opción de “Buscar amenazas de seguridad en el dispositivo”, para disponer de una verificación más regular y continua, y activar únicamente la opción “Mejorar detección de aplicaciones dañinas” si se desea colaborar con Google en el proceso de detección de *malware*.
2068. Pese a que estas capacidades fueron introducidas en Android 4.2, actualmente están también disponibles para dispositivos móviles incluso basados en Android 2.3 (o superior) a través de la actualización de los servicios de Google Play. Por tanto, otros dispositivos móviles Android más antiguos, incluso aunque no dispongan de la versión Android 6.x, pueden disponer de estas capacidades de escaneo o verificación de apps, ya que las mismas fueron introducidas por Google en una de las actualizaciones del componente (y app) asociado a los servicios de Google Play<sup>118</sup> (sin ser necesario realizar una actualización de la versión del sistema operativo).
2069. Debe tenerse en cuenta que tanto las capacidades introducidas por Google Bouncer [Ref.- 174], como las asociadas a “Verify Apps” [Ref.- 174] y a “Play Protect”, añaden niveles de seguridad adicionales al ecosistema de Android, bajo el paradigma de seguridad en profundidad (es decir, añadir varios niveles o capas de protección), pero no proporcionan una protección completa (no son efectivas al 100%), pudiendo existir técnicas para evadir estos mecanismos de verificación de seguridad (tal como ya han demostrado en el pasado los estudios referenciados).

<sup>118</sup> <http://www.howtogeek.com/179638/not-getting-android-os-updates-heres-how-google-is-updating-your-device-anyway/>

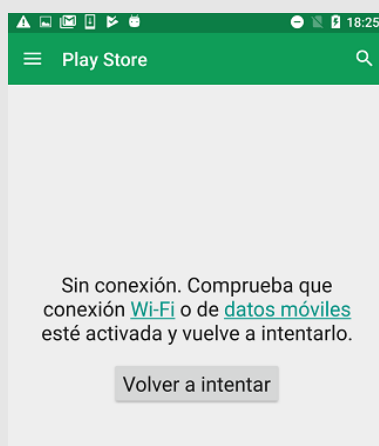
## 23.9. GESTIÓN DE APPS EN ANDROID

### 23.9.1. ACTUALIZACIÓN DE APPS EN ANDROID

2070. El término apps o aplicaciones móviles engloba en el presente apartado al conjunto de aplicaciones móviles de sistema o de terceros que son compatibles con Android y que pueden ser instaladas sobre este sistema operativo.

**Nota:** Pese a que Android permite la instalación de apps de terceros desde fuentes no oficiales (ver apartado “7.5. Instalación de apps (de orígenes desconocidos) en Android”), el análisis de las actualizaciones de apps en Android se centra en las aplicaciones móviles disponibles a través del mercado oficial de Google, denominado Google Play.

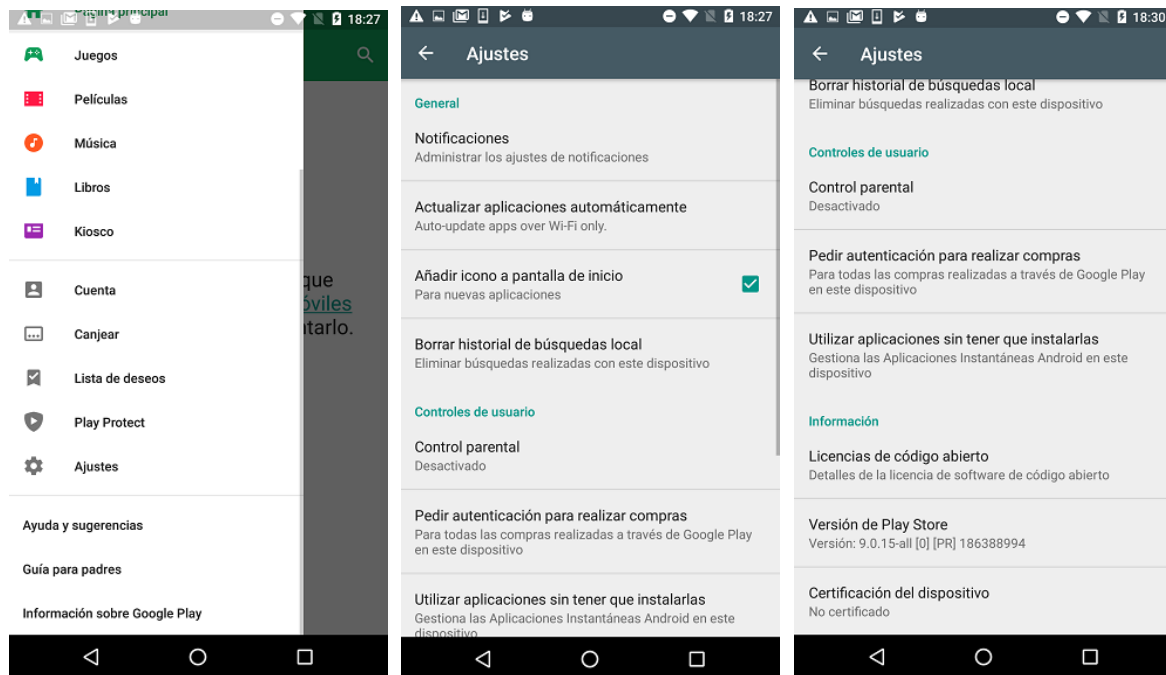
La app “Play Store” no puede ser ejecutada si no se dispone de conectividad de datos (autenticada y cifrada) hacia Google Play en Internet (Wi-Fi o 2/3/4G), mostrándose el siguiente mensaje: “Comprueba tu conexión y vuelve a intentarlo. [Reintentar]”:



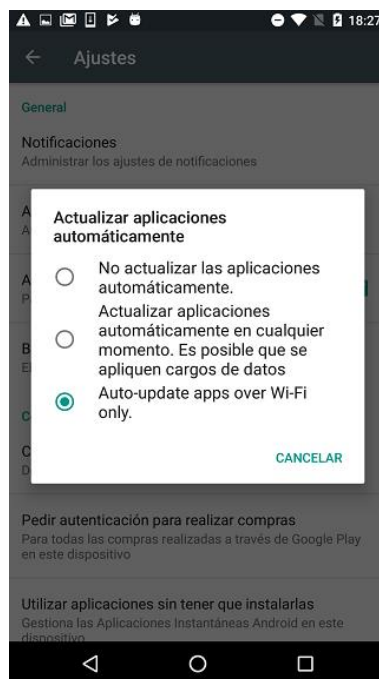
No obstante, es posible que este mensaje no se muestre si la app “Play Store” guardó en cache el resultado de su última invocación exitosa. En este caso, se verá una pantalla con los nombres de las apps pero sin los iconos.

2071. La presente guía se basa en la versión de la app (Google) “Play Store” 9.0.15, si bien alguna referencia a versiones anteriores puede estar presente para aspectos concretos.

2072. Desde la app de Google Play, denominada “Play Store”, y mediante el icono de menú es posible acceder a la sección de “Ajustes”. En el apartado “General” es posible configurar como se desea que se produzca el proceso de actualización de las apps instaladas desde Google Play mediante la opción “Actualizar automáticamente”. Se dispone de la opción de que no se actualicen las apps automáticamente, que se actualicen las apps automáticamente en cualquier momento, o sólo a través de redes Wi-Fi (opción por defecto):



2073. En caso de estar interesados en actualizar las apps tan pronto estén disponibles, tanto a través de redes Wi-Fi como de redes de datos móviles 2/3/4G, se recomienda no activar la opción “Actualizar las aplicaciones automáticamente solo a través de Wi-Fi” (habilitada por defecto):



2074. En Android 6.x, el acceso a Google Play (incluyendo el proceso de verificación de actualizaciones de las apps) se realiza a través de una comunicación HTTPS cifrada, pero no se emplean mecanismos de protección basados en *certificate pinning*, y, al igual que ocurría con otras aplicaciones de Google como Gmail, se acepta cualquier certificado digital de confianza que importado por el usuario al establecerse una conexión cifrada mediante TLS con los servidores de Google Play [Ref.- 79].

2075. Este hecho permite identificar fácilmente<sup>119</sup> que la descarga de la actualización se intenta realizar desde el servidor “android.clients.google.com”, mediante HTTPS. La respuesta redirige a la app “Play Store” hacia los servidores bajo el dominio “\*.gvt1.com”, también empleando HTTPS, para que ésta lleve a cabo una segunda petición solicitando el binario correspondiente a la app a actualizar.
2076. El proceso de descarga e instalación de una nueva actualización solicita el paquete o app a descargar y desvela numerosos detalles del dispositivo móvil y del software involucrado, como los números de versiones, identificadores, cookies, agente de usuario, incluso la cuenta de usuario de Google con la que se realiza la petición:

```
Set-Cookie: PLAY_ACTIVE_ACCOUNT=ICrt_XL6lNBE_S0rhk8RpG0j78e0XwQ23DlvB6kxiQ8=
<usuario>@gmail.com; Path=/; Secure
GET /play-apps-download-default/download/by-id/AF3DWBexsd0viV96e5U9-
SkM_V5zXTpNqxmJ1sSV1lVjT4gYxn2GQhg_euHKyADbtejmDtpbuVsS4BSCkCicQJ8G6QLXCrRnCEjQ
chlu45EMGR2Eso66efY?cpn=1LAU9LZZziqjfQq6&ctier=L&initcwndbps=7280&mm=31&mn=sn-
8vq54voxn25po-
h5q6&ms=au&mt=1520445713&mv=m&pl=24&expire=1520618655&ip=77.230.118.79&ipbits=0
&sparams=expire,ipbits,ip,q:,initcwndbps,mm,mn,ms,mv,pl,ctier&signature=673EFC6
625C2ECC91BEF6DED37A6E53FF4AEA15D.68C2FAE270BE0FD7D0ED455D1F25121DCA4CD2BB&key=
am3 HTTP/1.1
User-Agent: AndroidDownloadManager/6.0.1 (Linux; U; Android 6.0.1; Nexus 5X
Build/MTC20K)
Host: r2---sn-8vq54voxn25po-h5q6.gvt1.com
```

2077. Además, durante el intercambio de las peticiones asociadas al proceso de actualización, también se desvela la versión de la app “Play Store” del dispositivo:

```
User-Agent: Android-Finsky/9.0.15-all%20%5B0%5D%20%5BPR%5D%20186388994
```

2078. Cuando el dispositivo móvil es reiniciado, se establece una conexión con el servidor “www.googleapis.com” con el que, a través del recurso POST “/androidantiabuse/v1/x/create?alt=PROTO&key=<...>”, el dispositivo envía en formato ProtoBuffer información completa sobre sí mismo, incluido su número de serie, fabricante, modelo, versión de Android y número de compilación, entre muchos otros:

```
User-Agent: DroidGuard/11975440
Host: www.googleapis.com
...

#
Devicekey com.google.android.gms
BOARD bullhead
BOOTLOADER BHZ10r
BRAND google
CPU_ABI arm64-v8a
CPU_ABI2
SUPPORTED_ABIS arm64-v8a,armeabi-v7a,armeabi
DEVICE bullhead
DISPLAY MTC20KN
FINGERPRINT google/bullhead/bullhead:6.0.1/MTC20K/3142008:user/release-keys
HARDWARE bullhead
HOST vpba12.mtv.corp.google.com
ID MTC20K
MANUFACTURER LGE
MODEL Nexus 5X
PRODUCT bullhead
RADIO unknown
SERIAL 0111fb177f64...
TAGS release-keys
TIME 1470965993000
```

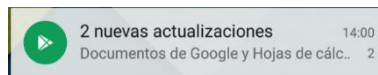
<sup>119</sup> Mediante la utilización de una CA privada propia.

```

TYPE user
USER android-build
VERSION.CODENAME REL
VERSION.INCREMENTAL 3142008
VERSION.RELEASE 6.0.1
VERSION.SDK 23
VERSION.SDK_INT 23 11.9.75 (440-8... aarch64)

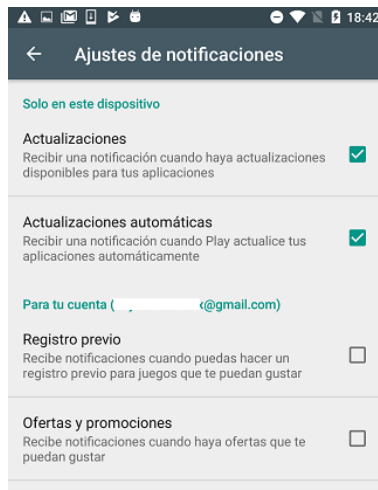
```

2079. Por defecto, la barra de notificaciones de Android mostrará un aviso sobre la disponibilidad de actualizaciones para las apps, en caso de no haber seleccionado la opción de actualización automática, ya que en ese caso las actualizaciones podrían ser llevadas a cabo sin la intervención del usuario, en concreto, si éstas no solicitan nuevos (grupos de) permisos:



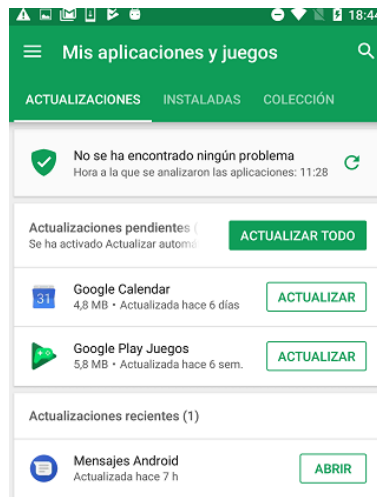
2080. Mediante la selección de dicha notificación, el usuario puede identificar para qué apps se dispone de actualización y los detalles asociados.

2081. La configuración de las notificaciones está disponible desde la app “Play Store”, a través del icono de menú, de la sección de “Ajustes”, y mediante la opción “Notificaciones”. Las notificaciones se pueden configurar a nivel de dispositivo (para informar sobre las actualizaciones que se detecten o realicen sobre el terminal) y de cuenta de Google (para que, en base a las recomendaciones de Google resultantes del análisis que se hace del perfil de la cuenta de usuario, se envíen notificaciones sobre aplicaciones y promociones que puedan interesar al usuario). Estas últimas están desactivadas por defecto, y se recomienda mantenerlas así en aras de la privacidad.

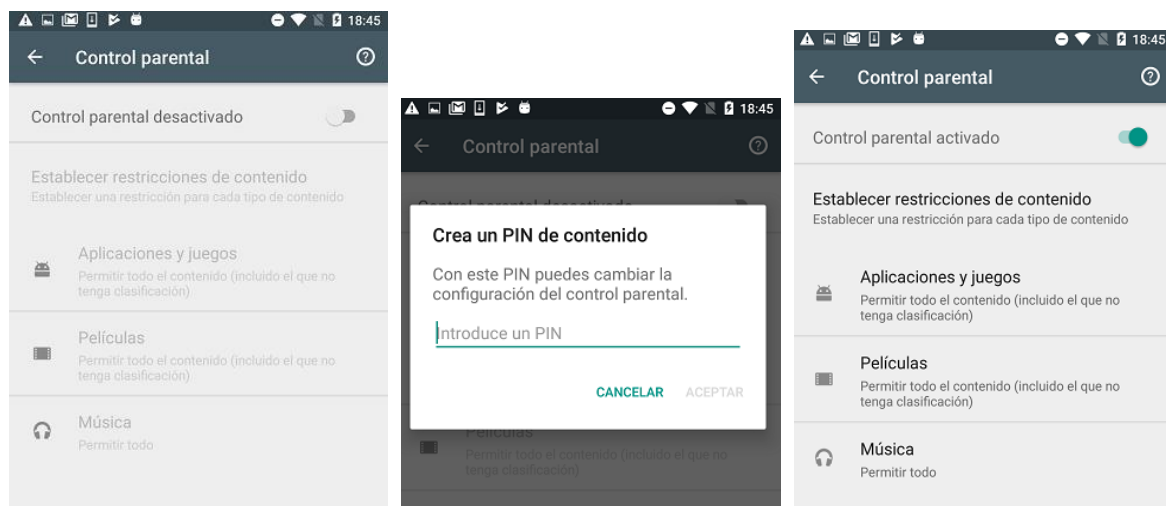


2082. La pantalla de actualizaciones está disponible desde la propia app “Play Store”, mediante el icono de menú, accediendo a la sección “Mis aplicaciones y juegos” y a la pestaña “Actualizaciones”. En ella se mostrarán por un lado las actualizaciones pendientes (si las hay) y, debajo, las “Actualizaciones recientes”.

2083. En la pestaña “Instaladas” de “Mis aplicaciones y juegos” se puede ver también qué aplicaciones tienen actualización disponible, que además tendrán a su derecha el botón “Actualizar”.

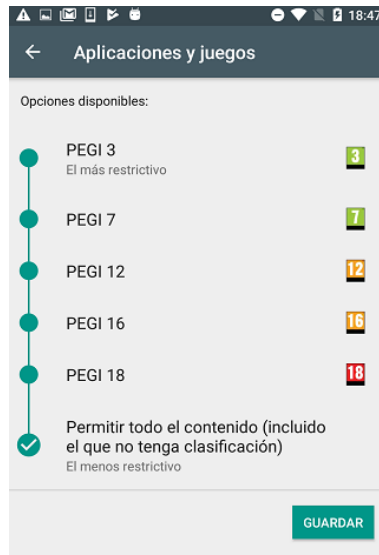


2084. Desde la misma se proporcionan detalles sobre las actualizaciones disponibles para las apps descargadas e instaladas en el dispositivo móvil, así como del resto de apps instaladas para las que no existe actualmente una actualización.
2085. Desde esta pantalla el usuario puede actualizar manualmente cada una de las apps, o todas ellas simultáneamente (botón “Actualizar Todo”).
2086. Adicionalmente, Android permite establecer restricciones de contenido desde la sección “Ajustes [Controles de Usuario] Control parental” de la app “Play Store”, de forma que sólo se puedan instalar las aplicaciones que cumplan con el nivel de filtro establecido. El control parental requiere de la creación de un PIN para acceder a su configuración y así evitar cambios en los controles de usuario y filtros de contenido por parte de otros usuarios del dispositivo móvil (como por ejemplo menores de edad). Se recomienda que este PIN sea distinto del PIN de acceso al dispositivo si lo hubiere:



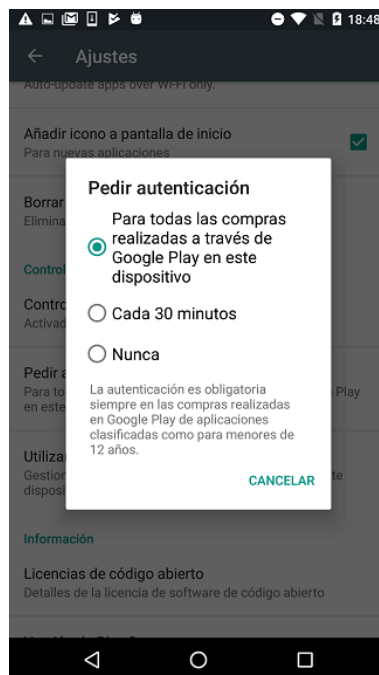
2087. Las restricciones de contenido se pueden establecer según tres categorías: películas, música y aplicaciones y juegos. Por defecto, se encuentran activadas las opciones que no restringen contenido.





2088. Todos los detalles sobre la clasificación y configuración del control parental se pueden consultar en [Ref.- 107].

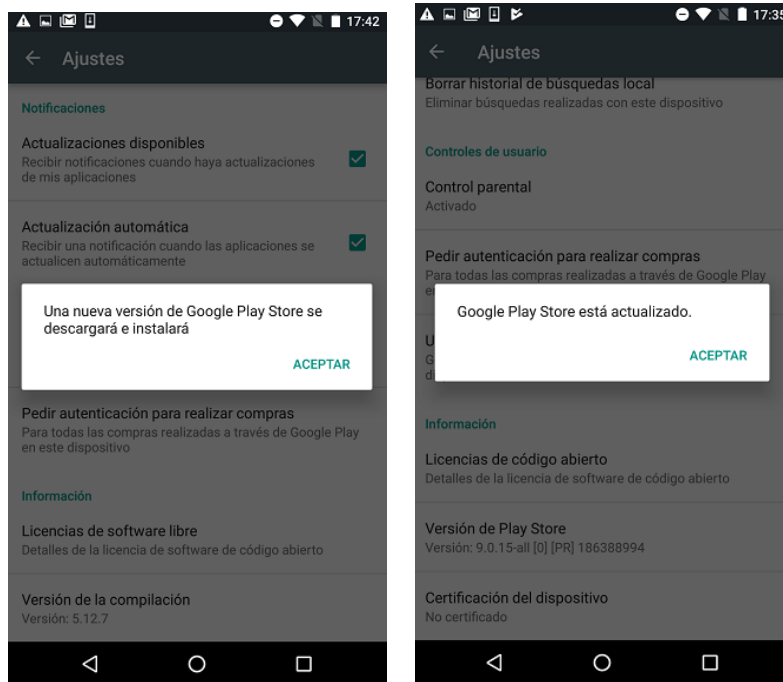
2089. Asimismo, la opción “Pedir autenticación para realizar compras” (habilitada por defecto y opción recomendada desde el punto de vista de seguridad) permite establecer controles para que, a la hora de instalar una nueva app de pago desde Google Play, se solicite autorización al usuario, junto a sus credenciales:



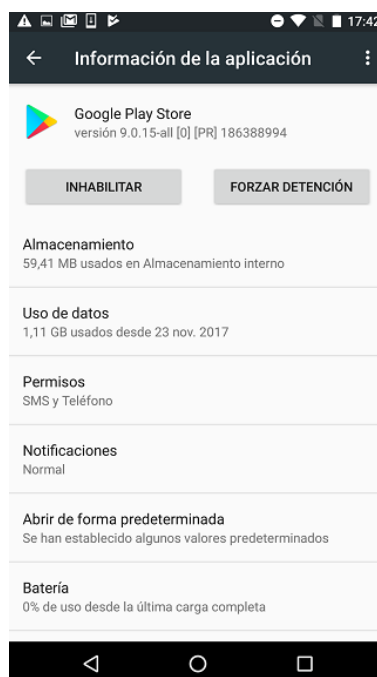
2090. Esta solicitud puede hacerse válida para los siguientes 30 minutos, con el objetivo de facilitar la realización de múltiples compras sin que sea necesario autenticarse para cada una de ellas, o nunca (opción desaconsejada).

2091. La app “Play Store” recibe actualizaciones silenciosas que se llevan a cabo automáticamente y sin aviso para el usuario. Se puede comprobar si hay alguna una actualización de la app “Play Store” disponible para el dispositivo entrando en los ajustes de la app “Play Store”, “Ajustes - [Información] Versión de la compilación “. Al seleccionar ese campo, si hay actualizaciones disponibles, se mostrará un mensaje informativo “Una nueva versión de Google Play Store se descargará e instalará”, pero

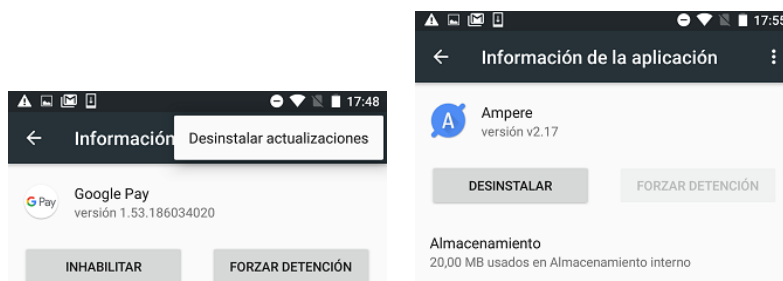
ello no provoca que la descarga de la actualización se lleve a cabo inmediatamente. La única forma de forzar una actualización automática de la app “Play Store” (si se requiere una funcionalidad precisa no disponible en la versión actual) es llevar a cabo una actualización manual del fichero APK correspondiente a la app “Play Store” de un sitio web de confianza (no existe ningún sitio oficial desde el que se puedan descargar las versiones de la app “Play Store”). Cuando la versión está actualizada, se mostrará un mensaje informativo de ello.



2092. La versión de la app “Play Store”, al igual que de cualquier otra app instalada en Android, puede obtenerse tanto desde la propia app (menú “Ajustes [Información] - Versión de Play Store”, como desde el menú “Ajustes [Dispositivo] - Aplicaciones”, por ejemplo, desde la pestaña “Todas”, seleccionando la app (en el ejemplo inferior, “Google Play Store”) de la lista de todas las apps disponibles (por ejemplo, versión 9.0.15...):



2093. La pantalla de información de una app permite tanto desinstalar la app (para aplicaciones de terceros), mediante el botón “Desinstalar”, como desinstalar todas las actualizaciones disponibles (para aplicaciones nativas del sistema y disponibles por defecto en Android), mediante el botón “[...] Desinstalar actualizaciones”. Las apps nativas no pueden ser desinstaladas completamente, sino que, al desinstalar actualizaciones, se devolverá la app a la versión que traía de fábrica.



2094. Con el objetivo de disfrutar del mayor nivel de seguridad posible en el dispositivo móvil y de manera general, se recomienda disponer siempre de la última versión de todas las apps instaladas, independientemente del desarrollador. La última versión debería solucionar todas las vulnerabilidades de seguridad públicamente conocidas.

2095. Las versiones recientes de la app “Play Store” incluyen un campo “Certificación del dispositivo” cuyo propósito es determinar si el dispositivo cumple los requisitos de compatibilidad de Android [Ref.- 271]. Las pruebas realizadas durante la elaboración de la presente guía ponen de manifiesto que un dispositivo móvil puede marcarse como “No certificado” si tiene desbloqueado el gestor de arranque (*bootloader*). A fecha de redacción de la presente guía, este estado no implica que no puedan ejecutarse instalaciones o actualizaciones del sistema operativo o de apps desde Google Play, pese a que esta posibilidad se enumera entre las consecuencias posibles que pueden aplicar en el futuro a dispositivos móviles no certificados.

2096. La información respecto a las actualizaciones de software y descargas disponibles para las apps de Android está disponible en Google Play y/o en la página web de su desarrollador.

2097. La instalación de actualizaciones de software y apps en Android, si todas las apps se han obtenido a través de Google Play, tiene asociado un proceso homogéneo, facilitando el proceso de actualización para usuarios no experimentados y aumentando el nivel de seguridad de los dispositivos móviles, al agilizarse el proceso de sustitución de software vulnerable.

### 23.9.2. ACTUALIZACIÓN AUTOMÁTICA DE APPS

2098. Android proporciona capacidades para actualizar automáticamente las apps instaladas en el dispositivo móvil tan pronto se detecte que hay disponible una nueva versión de las mismas en Google Play.

2099. Desde la app “Play Store”, mediante el icono de menú es posible acceder a los “Ajustes” de Google Play. Desde la sección “General”, es posible seleccionar la opción “Actualizar aplicaciones automáticamente”.

2100. La versión por defecto de la app “Play Store” en Android 6.0.1 es la 5.12.7, que se actualizada automáticamente (y sin la intervención del usuario) a la última versión disponible (9.0.15 a fecha de elaboración de la presente guía).

2101. Por defecto la funcionalidad de actualización automática de las apps en Google Play está habilitada sólo para llevarse a cabo mediante conexiones de datos a través de redes Wi-Fi. Adicionalmente, es posible definir si también es posible realizar las actualizaciones automáticas de las apps a través de la conexión de telefonía móvil (2/3/4G) del dispositivo móvil, ya que esta última puede tener costes asociados.
2102. Finalmente, también es posible deshabilitar las actualizaciones automáticas de las apps por completo, siendo necesaria la intervención manual del usuario para completar la actualización de cualquier app. Se sugiere aplicar una configuración específica en base a las recomendaciones descritas posteriormente.
2103. Para ello debe modificarse la opción “Actualizar las aplicaciones automáticamente solo a través de Wi-Fi” (opción habilitada por defecto) disponible en la app “Play Store”, desde el icono de menú, accediendo a los “Ajustes” de Google Play y, en concreto, a la sección “General” (mostrada en las imágenes previas).
2104. Aunque en versiones de Android anteriores a la 5 no existía la posibilidad de desactivar las actualizaciones automáticas para apps específicas (actualizaciones selectivas), desde Android 5 es posible seleccionar de manera individual qué aplicaciones se desea actualizar automáticamente [Ref.- 222]. Desde la app “Play Store”, mediante el icono de menú es posible acceder a “Mis aplicaciones y juegos”, seleccionar una app concreta de las ya instaladas, pinchar en los puntos representativos del icono de menú y habilitar o deshabilitar la opción “Actualizar autom.”. El valor de esta opción por defecto es el que aplique de la política general de actualizaciones descrita previamente.

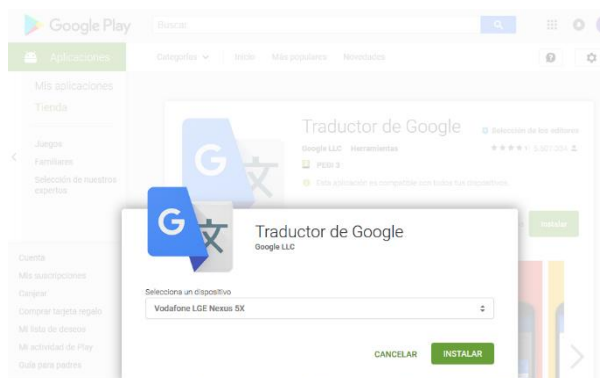


2105. Si la funcionalidad de actualizaciones automáticas ha sido habilitada, las nuevas actualizaciones serán aplicadas sin la intervención del usuario si la actualización no modifica los permisos requeridos por la app o, más recientemente, incluso si la actualización requiere disponer de nuevos permisos pero estos están englobados en un grupo de permisos previamente aprobado por el usuario para dicha app (ver apartado “7.1.4. Permisos simplificados y grupos de permisos de Google Play”).
2106. Por tanto, pese a que para un usuario no avanzado sería recomendable dejar activadas las actualizaciones automáticas con el objetivo de disponer siempre de la última versión de cada app, que supuestamente solucionará las vulnerabilidades conocidas públicamente, debido al nuevo modelo de permisos simplificados de Android, es preferible llevar a cabo las actualizaciones de las apps manualmente.
2107. Se recomienda por tanto no dejar habilitada la opción de actualizaciones automáticas, e independientemente del perfil del usuario del dispositivo móvil, forzar al usuario a revisar manualmente los nuevos permisos solicitados por cada una de las actualizaciones recibidas para todas y cada una de las diferentes apps instaladas en el terminal.

2108. Especialmente, los usuarios avanzados deben estar interesados en no habilitar esta opción para poder revisar y analizar minuciosamente las actualizaciones disponibles, y sus “nuevos” permisos, antes de que éstas sean instaladas.
2109. En caso de que los permisos de la app hayan cambiado con la actualización, el proceso de actualización manual mostrará los nuevos permisos requeridos por la nueva versión de la app que deberán ser aprobados por el usuario durante la instalación de la actualización de la app. Sin embargo, recientemente, si los nuevos permisos requeridos por la app están englobados en un grupo de permisos previamente aprobado por el usuario para dicha app, la actualización podrá ser instalada automáticamente sin la intervención del usuario.

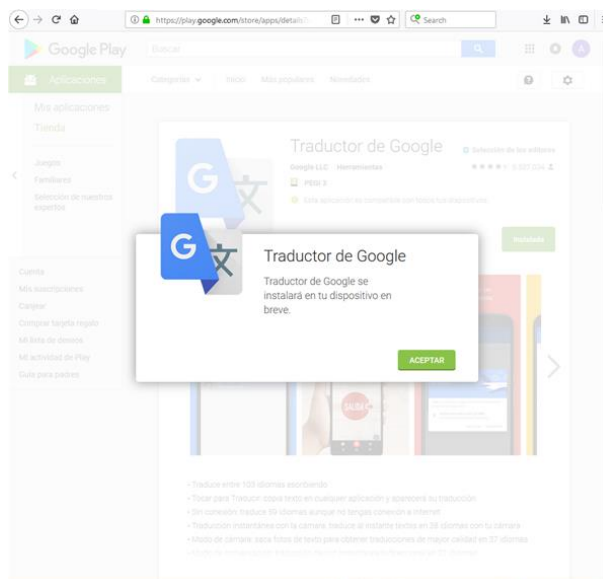
### 23.9.3. INSTALACIÓN REMOTA DE APPS

2110. En mayo de 2010 Google presentó la versión web de Google Play [Ref.- 4], que permite la consulta e instalación de apps en los dispositivos móviles Android desde otros ordenadores mediante un navegador web, en lugar de emplear la app de acceso al mercado oficial (“Play Store”) desde los propios dispositivos móviles.
2111. Una vez se adquiere una app a través de la versión web de Google Play desde el mercado oficial de apps, Google se encarga de instalarla en el dispositivo móvil a través de una conexión persistente disponible en los dispositivos móviles basados en Android a través de Internet (ver apartado “23.9.5. Conexión GTalkService”).
2112. La conexión permanente a través de Internet disponible entre los dispositivos móviles Android y Google se basa en el GTalkService [Ref.- 80]. Para la instalación remota de apps se emplea un mecanismo de envío de mensajes propio de Google y Android, y en concreto en este caso, el mensaje denominado INSTALL\_ASSET [Ref.- 81].
2113. Antes de llevar a cabo la instalación de cualquier nueva app, se recomienda revisar y analizar exhaustivamente los permisos solicitados por la misma sobre el dispositivo móvil.
2114. El acceso a Google Play se realiza mediante la cuenta de usuario de Google, por lo que el acceso no autorizado por parte de un atacante a dicha cuenta permitiría la instalación de apps en el dispositivo móvil asociado del usuario [Ref.- 8].
2115. Tras seleccionar la app en la web de Google Play, el usuario puede seleccionar en cuál de los diferentes dispositivos móviles vinculados a la cuenta de usuario de Google se desea realizar su instalación:



2116. Tras confirmar su instalación en el dispositivo móvil seleccionado, se obtiene la confirmación a través de la página web de Google Play, y en el dispositivo móvil el

proceso de instalación se lleva a cabo automáticamente, conllevando únicamente un aviso en la barra de notificaciones del dispositivo (y la aparición del icono de la app en alguna de las pantallas de inicio y/o en el *Launcher*):



2117. Es importante reseñar que, aunque la instalación no pueda llevarse a cabo en el preciso momento en que se solicita, tan pronto se pulse el botón “Aceptar” el interfaz de Google Play mostrará esa app como “Instalada”. Esto ocurre incluso aunque en el momento de solicitarse la instalación el dispositivo móvil no tenga conexión a los servidores de Google. La petición queda encolada en la cuenta de Google del usuario y, tan pronto se restablezca la conexión con los servidores, se iniciará la descarga e instalación de la app.

2118. En el pasado, la instalación remota de apps desde la web de Google Play de forma no autorizada podía suceder si un potencial atacante obtenía los identificadores de sesión empleados en el acceso web a Google Play del usuario [Ref.- 78]. Google resolvió el problema modificando la cookie “androidmarket” para que incluyese el flag *HttpOnly*, con lo cual el identificador de sesión solo es enviado por el navegador cuando hace una petición, por lo que no está disponible para ataques de XSS.

#### 23.9.4. ELIMINACIÓN REMOTA DE APPS

2119. Los dispositivos móviles basados en Android disponen también de capacidades por parte del vendedor, Google/Android, para eliminar apps de los mismos de forma remota.

2120. Este mecanismo fue diseñado como medida de seguridad en situaciones de emergencia para poder proteger a los usuarios en caso de que se produzca una distribución masiva de apps dañinas o maliciosas concretas.

2121. En junio de 2010 Google empleó estas capacidades por primera vez [Ref.- 5] [Ref.- 81] para eliminar una app creada como prueba de concepto que pretendía demostrar la facilidad para introducir apps maliciosas en los mercados de aplicaciones de varios fabricantes de dispositivos móviles, incluyendo Android Market (nombre empleado para Google Play en aquel momento).

2122. Posteriormente, Google ha hecho uso de esta funcionalidad en (al menos) otra ocasión para eliminar otras apps maliciosas introducidas en Android Market. Por ejemplo, en marzo de 2011, se vieron afectadas unas 50 aplicaciones infectadas con

malware bajo el nombre de DroidDream que fueron instaladas en más de 200.000 dispositivos móviles (cifras no oficiales). Estas apps hacían uso de vulnerabilidades conocidas en versiones de Android previas a la versión 2.2.2, y específicamente, técnicas empleadas habitualmente para conseguir acceso como root a dispositivos móviles Android (proceso conocido como *root*, *rooted* o *rooting* del dispositivo Android).

2123. Esas capacidades permiten a Google no sólo eliminar las apps maliciosas de Google Play y suspender las cuentas de los desarrolladores sospechosos, sino también eliminar las apps de los dispositivos móviles de los usuarios donde han sido instaladas, notificando al usuario sobre las acciones realizadas. Tal y como se indica en [Ref.- 6], *“Nota: Si Google determina que la actualización de una aplicación permite solucionar una vulnerabilidad de seguridad crítica, es posible que actualicemos ciertas aplicaciones independientemente de la configuración de actualización establecida en la aplicación o en tu dispositivo. Para obtener más información, consulta las Condiciones de Servicio de Google Play.”*
2124. La conexión persistente entre Google y los dispositivos móviles basados en Android también podría permitir la instalación remota de apps, y se emplea en la instalación de apps adquiridas desde el interfaz web de Google Play (detallada en el apartado previo).

### 23.9.5. CONEXIÓN GTALKSERVICE

2125. La conexión GTalkService [Ref.- 80] [Ref.- 81], comunicación permanente a través de Internet disponible entre los dispositivos móviles Android y Google, emplea los protocolos TCP/SSL/XMPP para comunicarse periódicamente con los servidores de Google (mtalk.google.com) en el puerto TCP/5228 haciendo uso de las conexiones de datos del terminal, telefonía móvil (2/3/4G) o Wi-Fi.
2126. El servicio GTalkService es empleado para el envío de mensajes desde Google a los dispositivos móviles Android, o para la instalación o eliminación remota de apps.
2127. El protocolo empleado por GTalkService no hace uso de mecanismos adicionales de seguridad (por ejemplo, firmas criptográficas de los mensajes intercambiados) aparte del uso de HTTPS (SSL/TLS), por lo que un ataque sobre este protocolo permitiría potencialmente modificar el tráfico intercambiado y, por ejemplo, eliminar o instalar nuevas apps en el dispositivo móvil.
2128. En Android 5.x y 6.x, el código USSD `*##*8255*##*` (o `*##*talk*##*`) del teclado del teléfono en Android, que ejecutaba el GTalk Service Monitor en Android 4.x y anteriores, deja de estar disponible, por lo que ya no es posible obtener todos los detalles de ejecución de GTalkService.
2129. Por defecto, en Android 4.4.4, los detalles de este servicio estaban ocultos<sup>120</sup>, y ni siquiera se pueden obtener los detalles de este servicio a través del botón de menú, y de la opción “Verbose logging”. Para más información, consultar la versión para Android 4.x de la presente guía [Ref.- 402].
2130. En versiones previas de Android, como 2.x, el *Gtalk Service Monitor* disponía de múltiples pantallas con información del servidor y puerto al que se encuentra conectado el dispositivo móvil, el identificador de usuario (Google JID) y de dispositivo móvil (Device ID), el intervalo de comprobación de la conexión (15 minutos), el estado de la

<sup>120</sup> A diferencia de como ocurría en versiones previas de Android, 2.x (ver la versión previa de la presente guía).

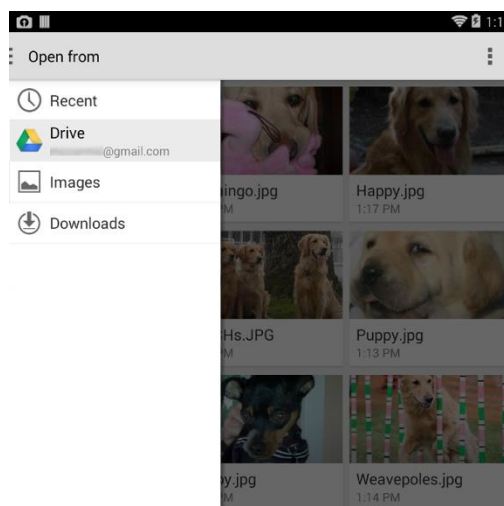


conexión, un histórico de conexiones, o estadísticas de la transmisión de datos y las comunicaciones.

**Nota:** Los valores del “JID” (ejemplo, “usuario@gmail.com/android<CODIGO>”, dónde <CODIGO> es un string de 12 valores hexadecimales) y del “Device ID” (ejemplo, “android-<CODIGO>”, dónde <CODIGO> es un string de 16 valores hexadecimales) no están relacionados con el valor del “ANDROID\_ID” (ver apartado “7.10. Configuración por defecto del dispositivo móvil”).

## 23.10. ACCESO Y ALMACENAMIENTO DE DATOS DESDE APPS

2131. Android 4.4 introdujo el *Storage Access Framework* (SAF), un entorno que simplifica el acceso, edición y almacenamiento de documentos, imágenes, vídeos y otros ficheros por parte de las apps de Android, con la capacidad de emplear múltiples proveedores de almacenamiento o proveedores de documentos (*Document Providers*) [Ref.- 165].
2132. Con Android 5.x (Lollipop), una nueva API (nivel 21) permite acceso total a los directorios y ficheros de las tarjetas SD, otorgando acceso completo, almacenamiento automático y mejorando la seguridad. Las apps pueden seleccionar un subárbol de directorio entero y proporcionar acceso de lectura y escritura a todos los documentos contenidos en él, sin requerir la confirmación del usuario para cada uno de ellos.
2133. Android 5.x añadió el *intent* (elemento o mensaje de comunicación entre componentes de una aplicación o de aplicaciones distintas) ACTION\_OPEN\_DOCUMENT\_TREE, que puede ser declarado por una app para recibir un directorio de cualquier componente “DocumentProvider”, incluyendo el almacenamiento compartido del dispositivo. La app podrá entonces crear, modificar y borrar ficheros y subdirectorios bajo el árbol recibido, incluso de forma persistente entre reinicios del dispositivo móvil.
2134. Los servicios o proveedores de almacenamiento pueden ser tanto locales (memoria interna del dispositivo) como pertenecer a servicios de almacenamiento “en la nube” (como por ejemplo Google Drive, One Drive, Dropbox, Box, etc.), y las apps pueden obtener, modificar, borrar, crear y guardar ficheros o documentos en ellos de manera homogénea a través de un interfaz estándar y unificado, así como acceder y compartir documentos proporcionados por otras apps existentes en el dispositivo móvil a través de SAF:



2135. Estas nuevas capacidades influyen principalmente en las capacidades disponibles para los desarrolladores de apps para Android, permitiéndoles gestionar múltiples documentos o hacerlo individualmente, establecer permisos sobre estos, y gestionar la autenticación del usuario en los servicios de almacenamiento en la nube antes de realizar operaciones con los datos a guardar o gestionar.

2136. Para el usuario del dispositivo móvil, los detalles de dónde y cómo se almacenan los documentos por parte de las apps son prácticamente transparentes, por lo que únicamente debe prestar especial atención desde el punto de vista de seguridad a si desea almacenar los documentos solo localmente, o en algún servicio “en la nube”.

### 23.11. ALMACENAMIENTO DE CREDENCIALES E INFORMACIÓN SENSIBLE EN APPS

2137. El almacenamiento de credenciales e información sensible en Android es uno de los elementos críticos que debería ser tenido en cuenta por los desarrolladores de apps.

2138. Las apps pueden almacenar los datos:

- En el almacenamiento interno (o *sandbox*) asociado a la app, al cual sólo esa aplicación tiene acceso salvo que se haya realizado el proceso de *rooting* al dispositivo móvil (o que se explote una vulnerabilidad). Toda aplicación que se instala en Android 6.x recibe acceso a su directorio “/data/data/appname” (donde *appname* es el nombre del paquete asociado a la app). Para controlar el acceso al directorio de la app, se emplea el mecanismo estándar de permisos de ficheros y directorios de Linux, ya que cada app que se instala recibe un identificador de usuario (UID) y de grupo (GID) únicos.
- En el almacenamiento compartido (o externo): para ello, con el nuevo modelo de permisos introducido por Android 6.x (ver apartado “7.1. Modelo de permisos de Android”), la app deberá solicitar al usuario permiso sobre el almacenamiento compartido (o tarjeta SD externa). Si se le concede, la app dispondrá de permisos globales de lectura y escritura en el mismo.

2139. Adicionalmente, por defecto el almacenamiento de datos se lleva a cabo sin cifrar, es decir, las credenciales de acceso a diferentes servicios y otra información sensible será almacenadas en ficheros o bases de datos (SQLite) en claro [Ref.- 109], por ejemplo, dentro del *sandbox* de la app bajo el directorio “/data/data/appname”, o alguno de sus subdirectorios.

2140. Si un atacante obtiene acceso físico al dispositivo móvil, podría seguir el proceso de *rooting* (o explotar una vulnerabilidad) y disponer potencialmente de acceso a las credenciales almacenadas sin cifrar.

2141. Se recomienda por tanto que los desarrolladores de apps almacenen los datos cifrados empleando una clave que no sea accesible directamente por la app, por ejemplo, almacenándola en un KeyStore (ver apartado “11.1. Android Keystore System: Almacenamiento de credenciales”) protegido por una contraseña que debe ser proporcionada por el usuario y que nunca es almacenada en el dispositivo móvil [Ref.- 184].

2142. Adicionalmente, se recomienda hacer uso de los mecanismos de cifrado del dispositivo móvil disponibles por defecto desde Android 3.0 (ver apartado “10.1. Cifrado del dispositivo móvil”).

### 23.12. ENLACES Y REFERENCIAS WEB DESDE LAS APPS

2143. En relación directa con las apps, Android 6.x añade capacidades de gestión sobre los enlaces (URLs o *links*) asociados o registrados para cada app, y que se denominan “(Android) App Links”.

2144. Es decir, los “App Links” son un tipo de enlace que las apps pueden incluir en su configuración para que, ante una solicitud de apertura de un enlace de ese tipo, se ejecute una actividad específica de la app en lugar de que se abra el enlace dentro de un navegador web. Esta funcionalidad permite que ciertos enlaces (o URLs) sean gestionados directamente por una app instalada en el dispositivo móvil, en lugar de por el servidor web asociado, en su versión para móviles, a través del navegador web [Ref.- 604]. La funcionalidad aplica a enlaces web asociados a los protocolos HTTP y HTTPS.

2145. La gestión automática de enlaces requiere que tanto el desarrollador de la app como el administrador del sitio, servidor o aplicación web trabajen conjuntamente. La app debe indicar que ella es la encargada de gestionar ese tipo de enlaces a través de su fichero *manifest* (mediante los filtros de *intents*), y la aplicación web debe indicar qué app gestionará sus enlaces mediante un fichero de enlaces a contenidos digitales (Digital Asset Links [Ref.- 269], “.well-known/assetlinks.json”) en formato JSON, verificando así la asociación entre ambas.

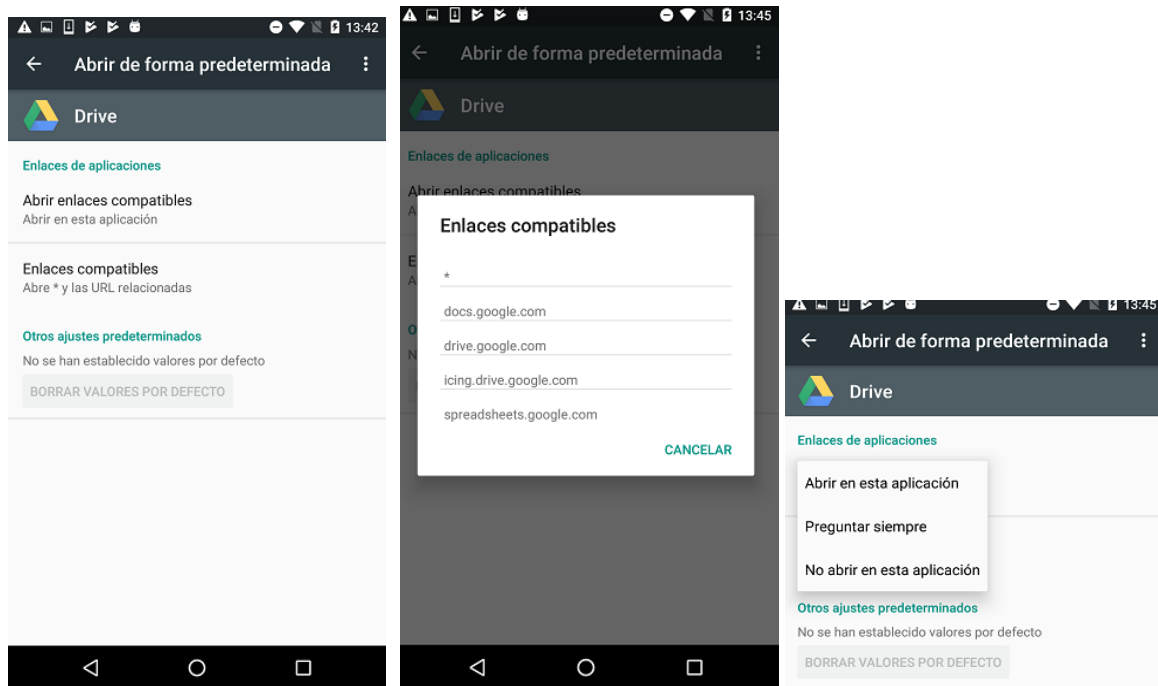
2146. Los “Digital Asset Links” establecen pues qué enlaces o URLs serán abiertos por qué app, en función del servidor web o dominio destino, y definiendo el proceso de autorización requerido por parte del usuario cuando se abre un enlace registrado.

2147. El objetivo de la nueva funcionalidad es que se pueda establecer una app por defecto encargada de gestionar un tipo de enlace HTTP o HTTPS determinado, evitando así que cada vez que el usuario pulse en un enlace de ese tipo, aparezca una ventana de diálogo preguntando cómo desea abrir dicho enlace: navegador web, app, etc.

2148. Desde “Ajustes - [Dispositivo] Aplicaciones - [<Nombre de la App>] Abrir de forma predeterminada” el usuario dispone de la capacidad de gestionar qué apps serán las asociadas por defecto a manejar qué enlaces. La app encargada por defecto de un tipo de enlaces también se puede seleccionar por parte del usuario mediante la opción “Siempre”, al ser consultado a través de la ventana de diálogo correspondiente, la primera vez que se abrió un enlace de ese tipo.

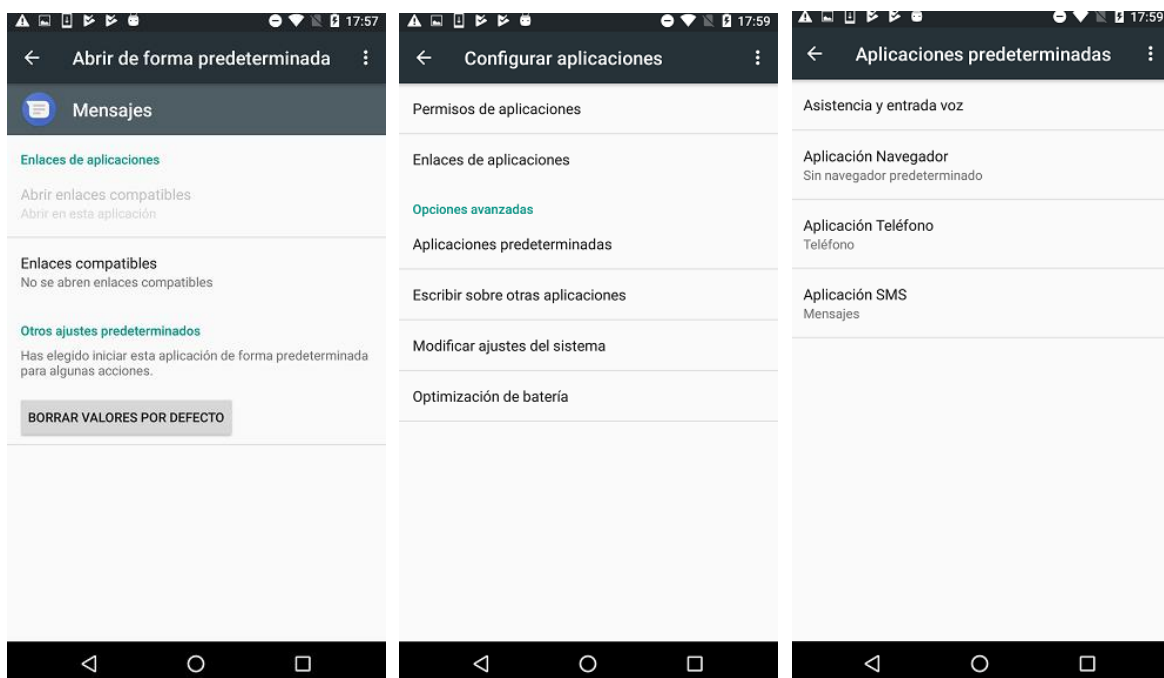
**Nota:** Los desarrolladores interesados en la creación de apps para Android disponen de todos los detalles e información en el portal para desarrolladores *Google Play Developer Console* (<https://play.google.com/apps/publish>) [Ref.- 7].

2149. La opción “Abrir enlaces compatibles” permite definir si las URLs que la app declaró como “Enlaces compatibles” se abrirán automáticamente, no se abrirán o se consultará al usuario:



2150. La opción “Enlaces compatibles” son los sitios web que la app declaró en su fichero *manifest* (y en el fichero *assetlinks.json* asociado al dominio) como propios para lanzar una actividad concreta dentro de ella.

2151. La opción “Otros ajustes predeterminados” informa de si la app se ha seleccionado como aplicación para ejecutarse ante un determinado evento. Sin embargo, este campo sólo indica si la app tiene algún ajuste de ese tipo, pero no concretamente cuál. Para consultarlo, se debe acceder a “Ajustes - [Dispositivo] Aplicaciones - [rueda de configuración] [Opciones avanzadas] Aplicaciones predeterminadas” y examinar la lista de apps.



2152. En caso de haberse seleccionado como predeterminada una app para una acción, si se desea cambiarla, se deberá seleccionar el botón “Borrar valores por defecto” y lanzar

la acción correspondiente para que el sistema pregunte de nuevo al usuario que app desea que se emplee de forma predeterminada.

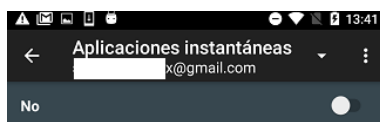
2153. El modelo empleado por Android para determinar quién se encargará de manejar un enlace se basa en los siguientes tres criterios o escenarios: si el usuario ha designado una app por defecto para dicho enlace, Android se lo enviará, y ésta se encargará de abrirlo. Si no hay establecida ninguna preferencia o asociación para ese tipo de enlace, y solo hay una app instalada para gestionar ese enlace, dicha app recibirá la petición. Si no hay establecida ninguna preferencia o asociación para ese tipo de enlace, y hay varias apps instaladas que pueden gestionar ese enlace, Android mostrará una ventana de diálogo preguntando al usuario qué app debe recibir la petición.

### 23.13. INSTANT APPS

2154. Las “Android Instant Apps” son aplicaciones nativas Android que se ejecutan de forma instantánea sin requerir instalación en el dispositivo móvil. En lugar de ello, el portal web que distribuye la app proporcionará una URL que, bajo demanda, cargará sólo la parte de una app necesaria para ejecutar una determinada acción.
2155. Uno de los principales beneficios de las Instant Apps es no tener que instalar aplicaciones sólo para realizar una tarea específica desde una web (por ejemplo, realizar un pago, pedir un taxi, etc.), sino aprovechar una app propia disponible a través de un enlace web al portal que proporciona el servicio, desde el que se cargará la app requerida.
2156. Al evitar la instalación/desinstalación de apps que sólo se requieren puntualmente, se ahorra espacio en el dispositivo móvil.
2157. Las Instant Apps permiten a los desarrolladores segmentar su app en módulos que pueden ejecutarse independientemente dentro de un sandbox, de forma que sólo se descargará el código necesario para una determinada acción, con el consiguiente ahorro de RAM en el dispositivo móvil. Por ejemplo, un usuario está de viaje en el extranjero y necesita pedir comida rápida. En lugar de instalar la aplicación de una cadena de restauración, el portal web puede ofrecer un enlace que lance la funcionalidad de búsqueda de menú (en lugar de toda la app); además, se puede integrar con Android Pay para que el usuario pueda completar el pago sin requerir más acción por su parte.
2158. Según Google, el esfuerzo a nivel de desarrollo para transformar una app tradicional en una Instant App es mínimo, pues no requiere rediseñar la app.
2159. Aunque las Instant Apps se presentaron en el Google I/O de 2016 [Ref.- 240], estas son compatibles con dispositivos desde Android 4.1 (nivel de API 16) y Google Play Services [Ref.- 239].
2160. Son varios los propósitos de las Instant Apps: por un lado, pretenden mejorar la experiencia del usuario aprovechando su integración con las funciones de Google Play Services (como la ubicación, la identidad, los pagos, etc.); por otro, permitir a los desarrolladores de apps que las mismas sean usadas sin necesidad de instalarse físicamente en el dispositivo móvil.
2161. Desde el punto de vista de seguridad, surgen varias cuestiones a tener en cuenta: cuál será la gestión de permisos de las Instant Apps (especialmente en dispositivos anteriores a Android 6.x), cómo saber si se puede confiar en una Instant App que se abre desde un determinado enlace web, cómo saber si una Instant App cumple con

políticas de seguridad corporativas, qué potenciales riesgos introduce la propia traducción de un enlace web a código ejecutable... [Ref.- 241] [Ref.- 242]. Por el momento, Google no ha elaborado ningún documento técnico abordando estas cuestiones, por lo que se recomienda tener prudencia a la hora de hacer uso de esta funcionalidad.

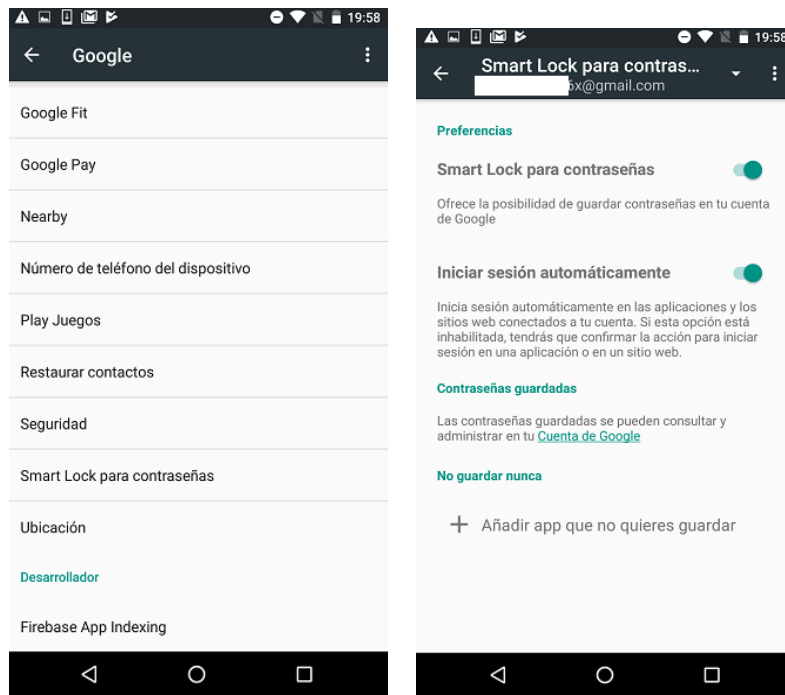
2162. Si no se desea hacer uso de este tipo de aplicaciones, se puede deshabilitar su uso a través de “Ajustes - [Personal] Google - [Servicios] Aplicaciones instantáneas” y mover el interruptor a la posición “No”.



Activa las Aplicaciones Instantáneas para iniciar aplicaciones al instante sin tener que instalarlas. [Más información](#)

## 23.14. SERVICIO DE CONTRASEÑAS DE GOOGLE SMART LOCK

2163. Además del servicio Smart Lock para mantener dispositivos Android desbloqueados (ver apartado “9.5. Desbloqueo mediante Smart Lock”), Google incorporó con la actualización a la versión 7.5 de Google Play Services (GPS) un gestor de contraseñas referenciado como “Smart Lock para contraseñas”, destinado a almacenar y sincronizar las contraseñas de sitios web accedidos con Chrome y otras aplicaciones desde los dispositivos móviles.
2164. Smart Lock para contraseñas forma parte del ecosistema “Google Identity Platform” [Ref.- 244], cuyo objetivo es la gestión segura de la identidad de los usuarios.
2165. La sincronización de datos se realiza a través de la cuenta de Google del usuario, por lo que las contraseñas almacenadas a través del gestor Smart Lock estarán disponibles en todos los dispositivos en los que se haya iniciado sesión con dicha cuenta de usuario [Ref.- 243].
2166. Cuando se visita por primera vez un sitio web o se utiliza una app que emplea esta funcionalidad y que requiere introducir credenciales, si Smart Lock para contraseñas está activo, se mostrará una ventana solicitando permiso para almacenar las credenciales. Si se acepta, la próxima vez que se visite el sitio web o se ejecute la app desde cualquier otro dispositivo que haya iniciado sesión en la cuenta de Google del usuario, no se solicitará identificación, sino que Smart Lock proporcionará automáticamente las credenciales para ingresar en dicha web o app.
2167. A nivel de app, los desarrolladores pueden integrar Smart Lock en su aplicación móvil utilizando la API “Credentials” [Ref.- 245].
2168. La activación del servicio “Smart lock para contraseñas” se realiza a través de “Ajustes - [Personal] Google - [Servicios] Smart lock para contraseñas” [Ref.- 238]. Las opciones disponibles son las siguientes:



- [Preferencias] Smart Lock para contraseñas: esta opción habilita/deshabilita el servicio.
- [Preferencias] Iniciar sesión automáticamente: si se deshabilita, se solicitará al usuario confirmación para iniciar sesión; si se habilita, el inicio de sesión tendrá lugar sin intervención del usuario.
- [Contraseñas guardadas]: redirige a la cuenta del usuario actualmente activa en el dispositivo móvil para poder consultar la información de credenciales guardada.
- [No guardar nunca]: permite elegir qué apps de las instaladas por el usuario no podrán hacer uso del servicio y, por tanto, no verán sus credenciales almacenadas.

2169. Si Smart Lock para contraseñas está activado (es el modo por defecto), Chrome hará uso de él para guardar las credenciales de los sitios web para los que el usuario acepte esta acción.

2170. Si Smart Lock para contraseñas está desactivado, pero se ha iniciado sesión en la cuenta de Google del usuario, Chrome también almacenará las credenciales de los sitios web en "https://passwords.google.com".

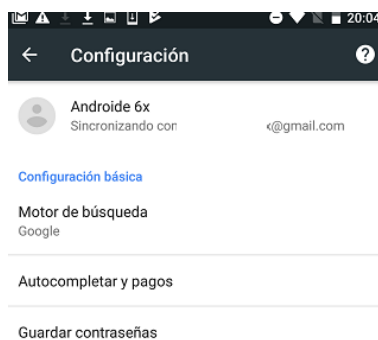
2171. Las contraseñas de páginas web y aplicaciones Android guardadas en este gestor, así como las opciones de configuración actual asociadas a él, se pueden consultar desde "https://passwords.google.com".

2172. A través de este sitio web, se pueden eliminar entradas, pero también visualizar las contraseñas e identificadores de usuario de los sitios webs para los que se aceptó el almacenamiento:





2173. La sección “Contraseñas guardadas” sólo contendrá información sobre las credenciales de sitios web si la configuración del navegador Chrome tiene habilitada la opción de “Guardar contraseñas” dentro de su configuración:

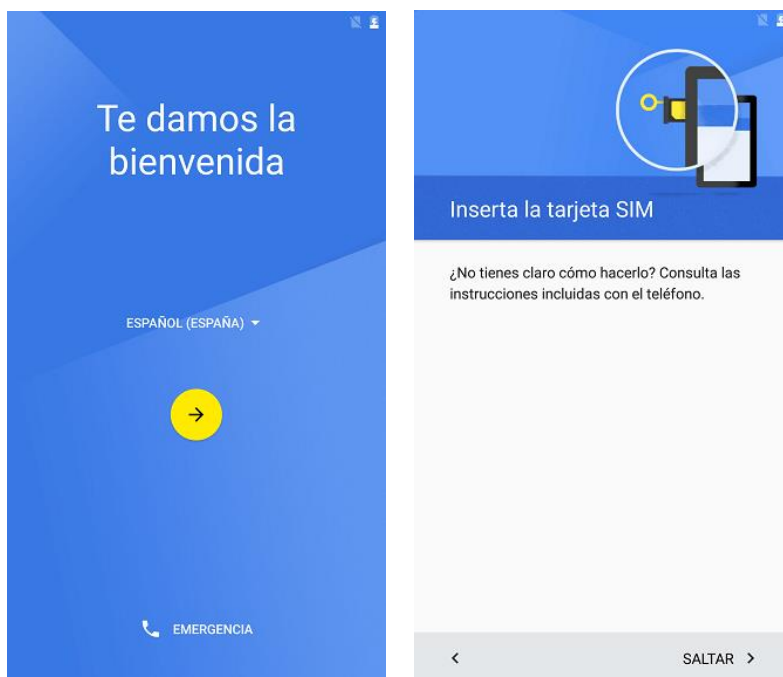


2174. Desde el punto de vista de seguridad, se recomienda deshabilitar el uso de Smart Lock para contraseñas o, cuando menos, las opciones que implican llevar a cabo un inicio de sesión automático.

## 24. APÉNDICE A: PROCESO DE INSTALACIÓN Y CONFIGURACIÓN INICIAL

2175. El presente apartado detalla el proceso de instalación y configuración inicial de Android 6.x al encender por primera vez el dispositivo móvil tras su adquisición (o tras restablecer los ajustes de fábrica). En función de la versión concreta de Android 6.x de la que se parta, las pantallas presentadas pueden diferir en formato y/o contenido, pero las opciones de configuración serán similares.

2176. Al arrancar el dispositivo móvil, se muestra una pantalla de bienvenida, “Welcome” (“Te damos la bienvenida”), donde se debe seleccionar el idioma con el que se desea configurar el dispositivo móvil y que también se empleará durante el proceso de instalación (por ejemplo, “Español (España)”). Tseleccionar el idioma se pulsará en el botón amarillo con la flecha para continuar.



2177. Seguidamente, se muestra la pantalla que sugiere al usuario que inserte la tarjeta SIM siguiendo las instrucciones que acompañan al dispositivo móvil, “Inserta una tarjeta SIM”, proceso opcional que puede ser evitado mediante el botón “Saltar” si no se desea hacer uso de las redes de telefonía móvil en este momento.

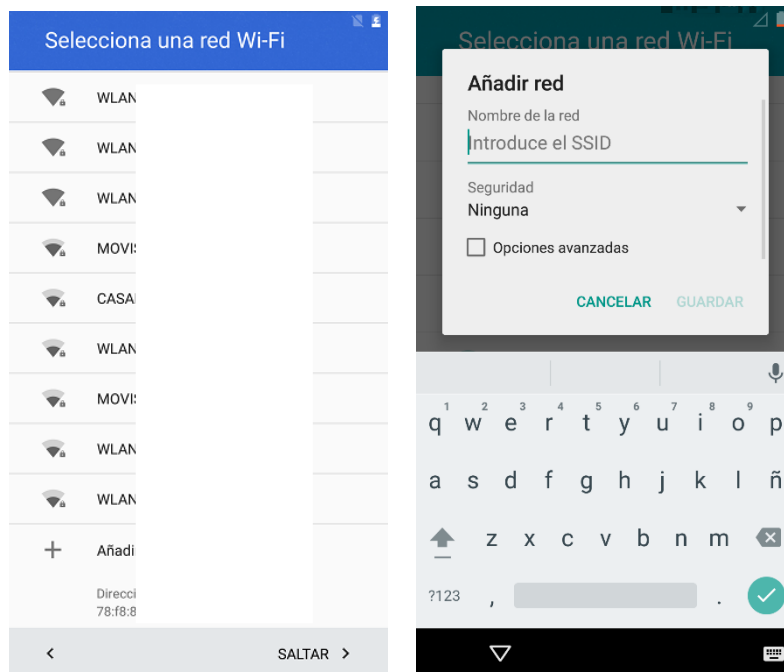
2178. Para configurar algunas de las opciones y ajustes de configuración del dispositivo móvil, es necesario disponer de conectividad a Internet mediante la selección de una red Wi-Fi, “Selecciona una red Wi-Fi”. Este paso también es opcional, mostrándose de nuevo el botón “Saltar”.

2179. Si se configura la conexión a una red Wi-Fi, se solicitará al usuario la contraseña de la red Wi-Fi.

2180. En Android 6.x, el proceso de selección de redes Wi-Fi muestra todas las redes Wi-Fi visibles y que están al alcance del dispositivo móvil, ordenadas según la intensidad con que se recibe la señal Wi-Fi, por lo que esta lista es dinámica y se actualiza si varía la intensidad de la señal de cada una de las redes.

2181. Al final de la lista de redes Wi-Fi se ofrece la opción de “Añadir otra red”, lo que permite añadir redes Wi-Fi ocultas que no aparecen en la lista actual de redes visibles.

bajo el alcance del dispositivo móvil, y que pueden hacer uso de diferentes mecanismos de seguridad: abiertas, WEP, WPA/WPA2 PSK o 802.1x EAP. Desde el punto de vista de seguridad, se desaconseja el uso de redes Wi-Fi ocultas. En Android 6.0.1, el campo para “Añadir otra red” mostrará la dirección MAC del dispositivo móvil, por si la configuración se realizase en una red Wi-Fi que filtra los clientes Wi-Fi en base a su dirección MAC.



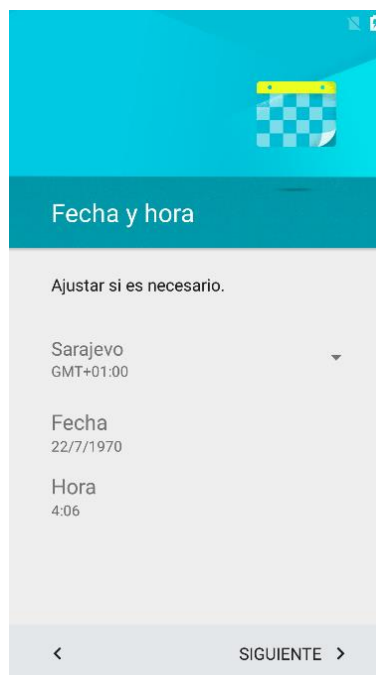
**Nota:** Desde Android 5.x las opciones de configuración avanzada del interfaz Wi-Fi, accesibles a través del botón superior derecho con tres puntos (“...”), que existían en la versión 4.x (y que permitía configurar una red Wi-Fi que hiciera uso de WPS) no están disponibles.

2182. Si se introduce incorrectamente la contraseña de la red Wi-Fi, será necesario pulsar sobre dicha red Wi-Fi hasta que aparezca el menú correspondiente, para poder seleccionar la opción “Olvidar”. En tal caso, habrá que retroceder al paso anterior para que las redes Wi-Fi sean redescubiertas y volver a seleccionar la red deseada.
2183. Si no se desea utilizar una red Wi-Fi para el proceso de instalación inicial, es posible hacer uso del botón “Saltar”, en cuyo caso se mostrará un mensaje de aviso que informará al usuario de que, si se omite la conexión a una red Wi-Fi, el dispositivo móvil no podrá realizar descargas ni llevar a cabo las actualizaciones iniciales de software. Para continuar sin conexión, se pulsará la opción “Saltar de todas formas”.

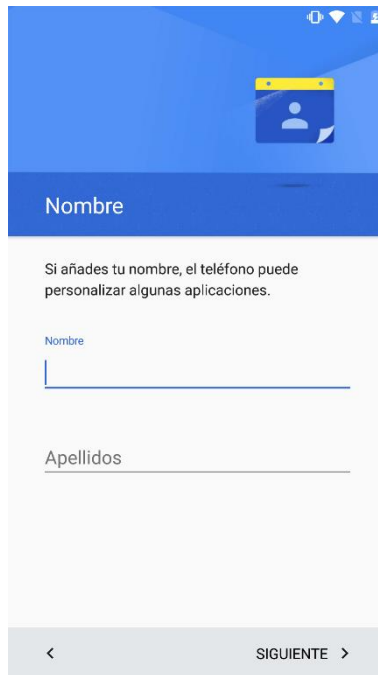


2184. Si no se ha configurado la conexión a una red Wi-Fi:

- Se presentará la pantalla de configuración de “Fecha y hora”, que parte por defecto del año 1970.



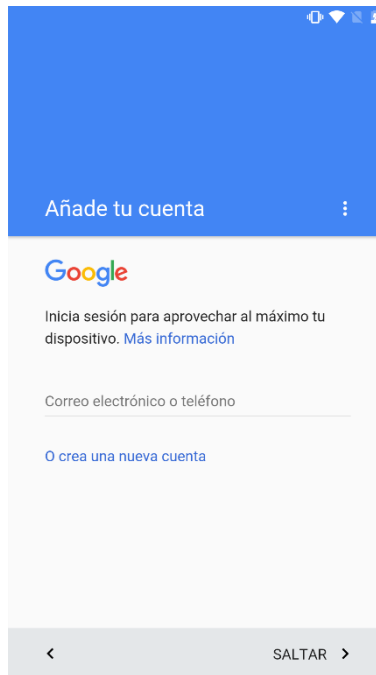
- Se invitará al usuario a añadir un nombre para la personalización de algunas aplicaciones. Este proceso puede omitirse sin más que dejar los campos vacíos y seleccionar la opción “Siguiente”.



2185. Si se establece la conexión con una red Wi-Fi, el dispositivo móvil comprueba la disponibilidad de conectividad hacia Internet. Inicialmente establece conexiones HTTP con “www.google.com”, “android.clients.google.com”, servidores del dominio “gpsnextra.net” y “clients3.google.com”, y conexiones HTTPS con “www.gstatic.com”.
2186. Si se introduce la configuración de una red Wi-Fi, nada más validar la existencia de una conexión hacia Internet, el dispositivo móvil muestra una pantalla que indica que se están “Buscando actualizaciones” (del sistema operativo Android).
2187. La versión 5.x de Android ofrecía el menú “Tocar y listo”, por el cual era posible copiar la configuración de otro dispositivo Android mediante NFC. El uso de NFC para este propósito está desaconsejado desde el punto de vista de seguridad. Sin embargo, en Android 6.x, al concluir la instalación, el interfaz NFC quedará en estado activo, por lo que se recomienda proceder a desactivarlo a través de “Ajustes - Conexiones inalámbricas y redes - ...Más - NFC”.
2188. Una vez comprobada la conexión, se presentará la pantalla “¿Tienes otro dispositivo?” que permitiría copiar las cuentas, aplicaciones y datos desde otro dispositivo móvil. El alcance de esta guía se centra en llevar a cabo la instalación inicial completa, por lo que se seleccionará la opción “No, gracias”. A diferencia de Android 5.x, el proceso de instalación no ofrece la posibilidad de copiar la configuración de otro dispositivo Android próximo utilizando NFC.

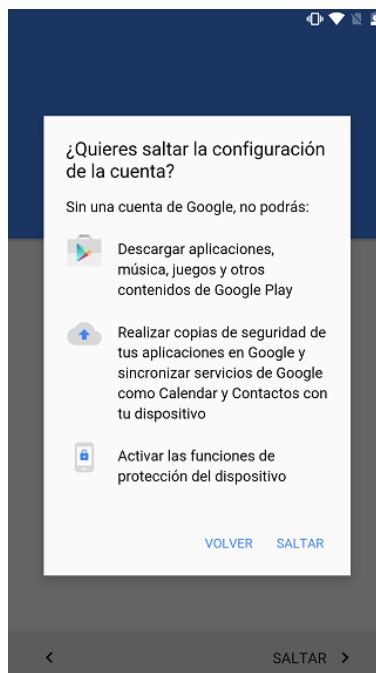


2189. Aunque en el paso anterior se opte por seleccionar la opción “No, gracias”, el dispositivo móvil intentará efectuar conexiones con los servidores de Google y, si falla la conexión de red, el proceso de instalación mostrará el mensaje “Error al iniciar sesión” (concretamente, con “https://accounts.google.com”).
2190. Debe tenerse en cuenta que tanto si se omite el proceso de conexión a una red Wi-Fi, como si se establece una conexión con una red Wi-Fi (incluso aunque posteriormente se interrumpa el proceso de configuración inicial), el interfaz Wi-Fi será habilitado y permanecerá en ese estado tras el proceso de instalación y configuración inicial de Android 6.x. Se recomienda por tanto deshabilitar el interfaz Wi-Fi lo antes posible y proceder a su configuración siguiendo las recomendaciones del apartado “16. Comunicaciones Wi-Fi”.
2191. En el caso de seleccionar una red Wi-Fi, establecer una conexión con la misma y obtener conectividad a Internet, se verifica la existencia de la conexión y se ofrece al usuario la posibilidad de configurar su cuenta de usuario de Google en el dispositivo móvil:



2192. Desde el punto de vista de seguridad se recomienda omitir la vinculación inicial entre el dispositivo móvil y una cuenta de usuario de Google y realizar el proceso de configuración inicial de la cuenta posteriormente, salvo que el usuario se encuentre en un entorno seguro y de confianza para poder establecer una conexión segura a una red Wi-Fi o 2/3/4G.

2193. Es posible omitir el uso inicial de una cuenta de usuario de Google mediante la opción “Saltar” u “Omitir”, acción que presentará una pantalla de confirmación que informa al usuario de qué implicaciones tiene no dar de alta la configuración de la cuenta de usuario de Google.



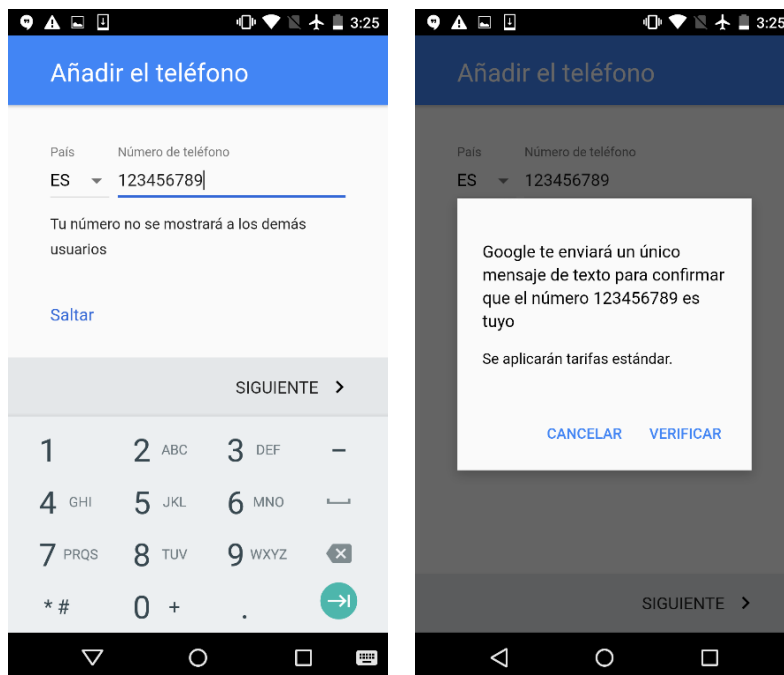
2194. Si el usuario no dispone de una cuenta de usuario de Google, se le ofrece la opción de integrar los servicios de Google en el dispositivo móvil mediante la creación de una cuenta.



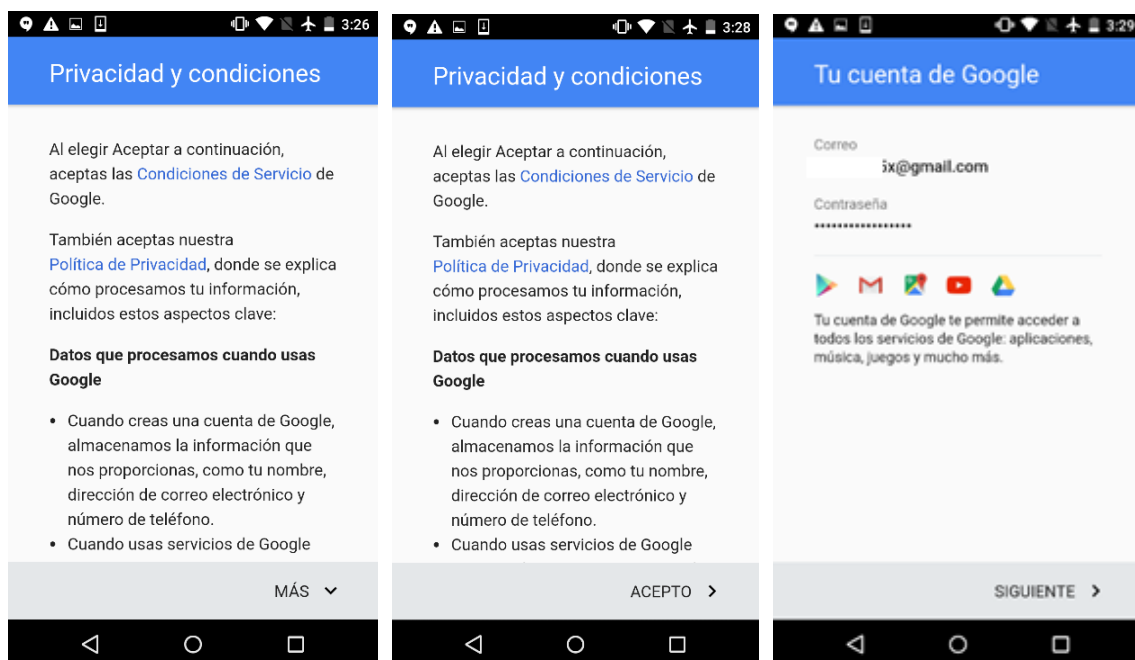
2195. Al crear una nueva cuenta de usuario de Google, se solicita el nombre y apellidos del usuario, seguido de lo que se denomina “Información Básica” y que consta de la fecha de nacimiento y el sexo del usuario (pudiéndose omitir éste). Estos campos deben rellenarse antes de proceder, si bien se permite la opción “Prefiero no decirlo” para el campo “sexo”.

2196. Tras introducir la información anterior, se debe de elegir el nombre de la cuenta de usuario de Google, asociado a la cuenta de Gmail (nombredeusuario@gmail.com). Hay ciertos nombres de usuarios no permitidos, por ejemplo, los que contengan la palabra “android”. Una vez se elige un nombre de usuario válido (que no incumpla ningún criterio no permitido, ni se encuentre ya en uso), se podrá seleccionar la contraseña asociada:

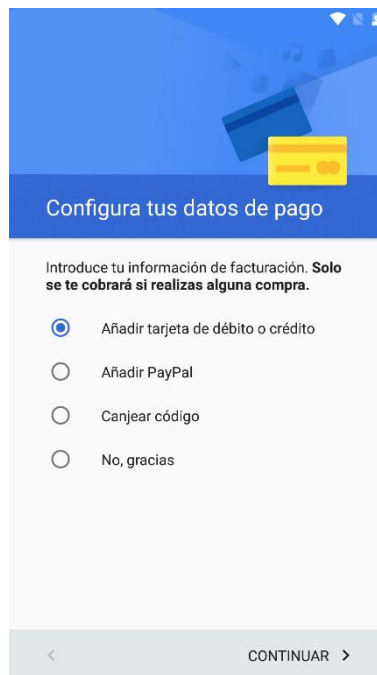
2197. Tras la selección de la contraseña, se solicitará al usuario introducir su número de teléfono. Si no se desea introducirlo, se seleccionará la opción “Saltar”. En caso de introducirse, Google enviará un SMS único de confirmación al número proporcionado.



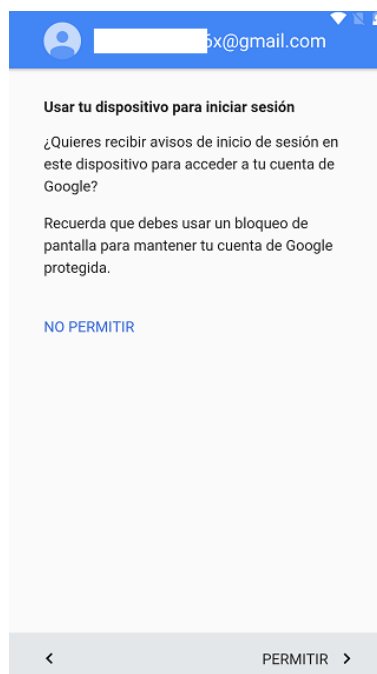
2198. El último paso antes de proceder a la creación de la cuenta de usuario es la aceptación de las condiciones de servicio y la política de privacidad de Google. Es necesario desplazarse mediante la barra lateral para que la opción “Más” se transforme en la opción “Acepto” y se proceda a la creación efectiva de la cuenta.



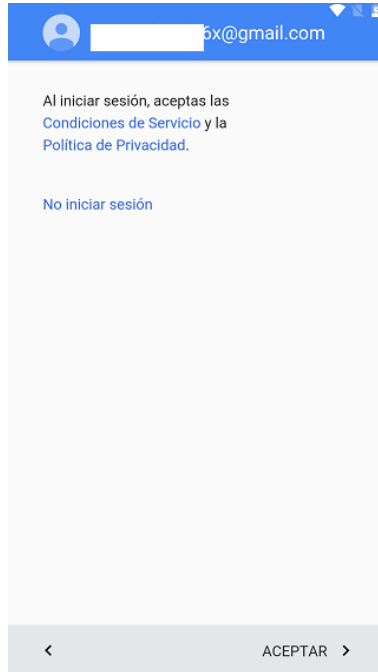
2199. Una vez llevadas a cabo por parte de Google las comprobaciones necesarias, se mostrará el menú que permite configurar los datos de pago que se utilizarán por parte del servicio o app “Play Store”. Las opciones disponibles son tarjeta de crédito, cuenta de PayPal y “No, gracias”. Esta última opción es la recomendada desde el punto de vista de seguridad, al menos durante el proceso de configuración inicial.



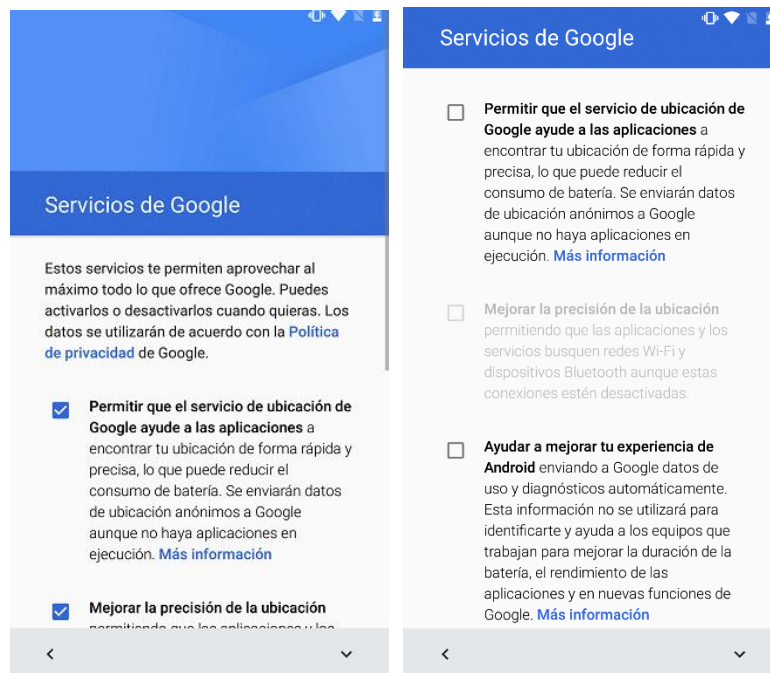
2200. Si ya se dispone de cuenta de usuario de Google y se desea utilizarla en el dispositivo móvil, se debe introducir el nombre de usuario y la contraseña asociados a la cuenta de Gmail (nombredeusuario@gmail.com). El menú de instalación presentará un mensaje preguntando si se desea recibir mensajes de inicio de sesión en el dispositivo móvil actual, en lugar de hacerlo en el dispositivo en el que se estén recibiendo actualmente. Si se desea que el dispositivo móvil reemplace al actual destinatario de los mensajes de inicio de sesión, se seleccionará “Permitir”. En caso contrario, se seleccionará “No Permitir”.



2201. El proceso de instalación proseguirá indicando que el inicio de sesión en la cuenta de Google del usuario implica la aceptación de las condiciones de servicio y la política de privacidad de Google, que pueden consultarse seleccionando el enlace (en color azul) correspondiente, y, al aceptarse, proseguirá con la configuración de datos de pago descrita anteriormente:



2202. Como resultado, se inicia sesión con la cuenta de usuario de Google, empleando una conexión cifrada mediante HTTPS, y se presentan al usuario los distintos servicios de Google disponibles (todos ellos marcados por defecto):



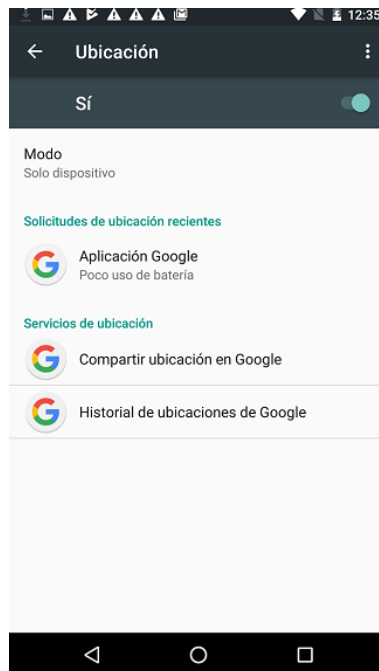
2203. Entre los servicios de Google disponibles para seleccionar, se incluye el servicio de realización de copias de seguridad y su posterior restauración, la ayuda para mejorar los servicios de ubicación (descritos posteriormente) y la ayuda para mejorar la experiencia del usuario con Android.

2204. Las capacidades relativas a las copias de seguridad se corresponden con la opción de configuración disponible posteriormente desde el menú “Ajustes [Personal] - Copia de seguridad”. En concreto, todas las opciones serán habilitadas por defecto, es decir, se llevará a cabo la copia de datos, y se restaurarán automáticamente la configuración y datos asociados al reinstalar de nuevo una app (ver apartado “21. Copias de seguridad”). Se incluirán también los datos del usuario en la cuenta de usuario de Google, las contraseñas de redes Wi-Fi, y otros ajustes de configuración.

2205. Respecto a los servicios de ubicación (o localización), se dispone de dos opciones:

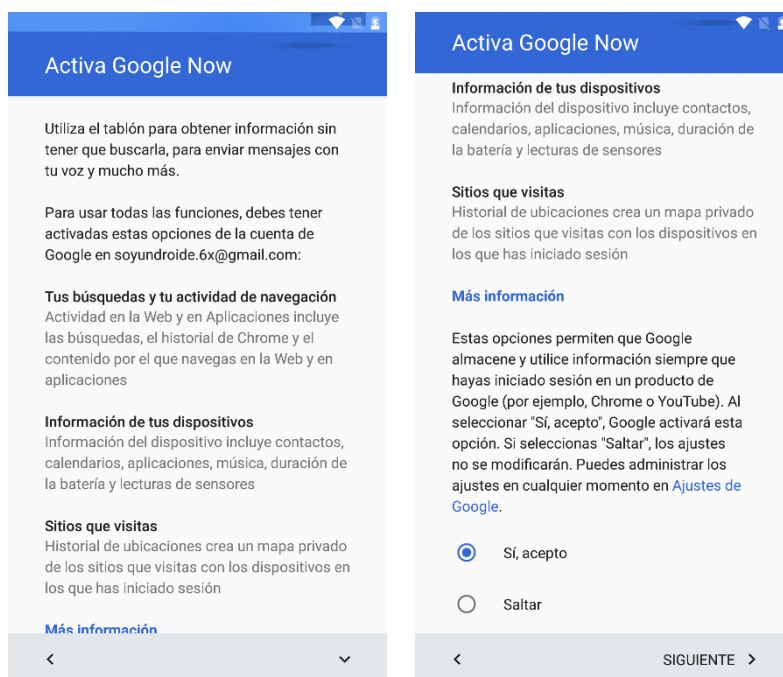
- Usar el servicio de ubicación de Google: es necesario para que las aplicaciones puedan determinar la ubicación del dispositivo móvil, pudiendo éstas remitir datos de ubicación anónimos a Google aunque no estén siendo utilizadas (teóricamente del módulo GPS, de redes Wi-Fi y de las torres de telefonía móvil).
- Ayudar a mejorar los servicios de ubicación: las apps y servicios pueden identificar las redes Wi-Fi próximas (aunque el interfaz Wi-Fi del dispositivo móvil esté deshabilitado) y proporcionar dicha información a Google para mejorar la precisión de los servicios de ubicación.

2206. Se ha constatado que, aunque se hayan desmarcado todas las opciones correspondientes a los servicios de ubicación descritas previamente, el botón de activación del menú “Ajustes - [Personal] Ubicación” se quedará activo en modo “Solo dispositivo”, comprobándose que los informes de ubicación de Google acceden a los servicios de ubicación (aunque en los pasos correspondientes del proceso de instalación se hubieran desmarcado las opciones de ubicación). Por tanto, se recomienda revisar de nuevo minuciosamente los ajustes de ubicación tras completar el proceso de instalación. La siguiente pantalla atestigua esta situación nada más finalizar el proceso de instalación:

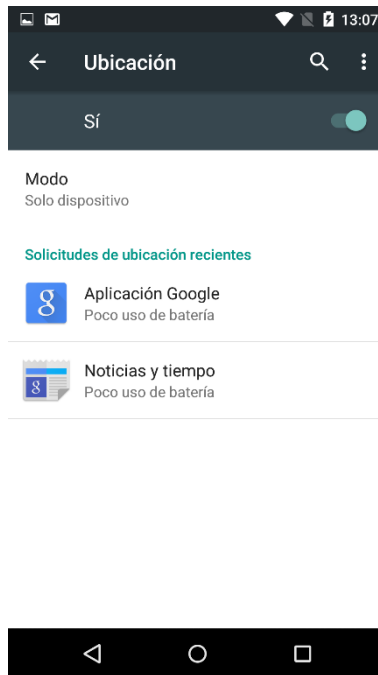


2207. También aparece marcada por defecto la opción “Ayuda a mejorar tu experiencia Android”, que será empleada para enviar datos de uso y diagnósticos a Google.

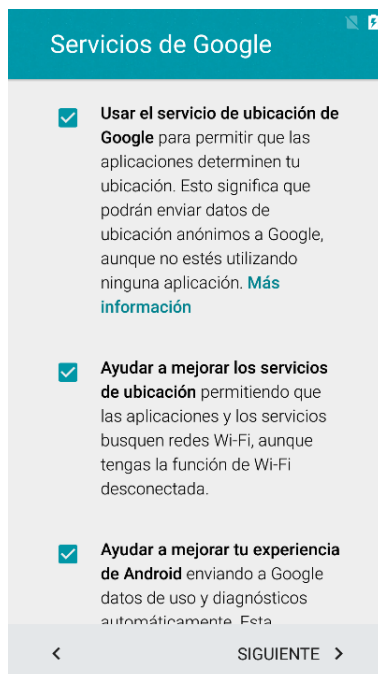
2208. Desde el punto de vista de seguridad y privacidad, salvo que se disponga de plena confianza en el tratamiento que Google hará de estos datos del usuario, es necesario evaluar en detalle si se desea activar esta funcionalidad.
2209. Si se vinculó el dispositivo móvil a una cuenta de usuario de Google, el proceso de instalación ofrecerá activar el servicio “Google Now” (actualmente denominado “Mi Tablón”), que proporciona información en tiempo real al usuario (este servicio también es referenciado como “feed”). Será necesario recorrer todas las páginas del menú utilizando el botón “Más” antes de poder elegir entre las opciones “Sí, acepto” o “Saltar”.
2210. Se recomienda omitir este paso mediante el botón “Saltar” y, una vez finalizada la configuración inicial y en función de las necesidades del usuario, revisarlo siguiendo las recomendaciones del apartado “22. App Google: Asistente de Google, Mi Tablón y Servicios de Búsqueda de Google”.



2211. En caso de haberse aceptado el uso de “Google Now”, se activarán y usarán los servicios de ubicación en modo “Solo dispositivo” (aunque en los pasos correspondientes del proceso de instalación se hubieran desmarcado las opciones de ubicación), incluyendo el envío de estadísticas a Google sobre las interacciones con “Google Now Launcher” y el historial de ubicaciones de Google (ver apartado “12.5. Historial de ubicaciones”), y se accederá a los datos del calendario del usuario, sus búsquedas web, incluyendo el historial web (ver apartado “23.1.3. Historial de actividad web”) y otros datos del usuario disponibles en los productos y servicios de Google (y/o de terceros):



2212. En el caso de no haber vinculado una cuenta de usuario de Google (ni haberse conectado a una red Wi-Fi), se ofrecerán igualmente las opciones que permiten activar ciertas capacidades asociadas a los servicios de ubicación de Google (equivalentes a las descritas anteriormente, a la hora de vincular una cuenta de usuario) para agilizar la localización del dispositivo por parte de las apps. Las dos opciones (habilitadas por defecto), permiten de nuevo recopilar datos de ubicación por parte de las apps y hacer uso de las capacidades de búsqueda de redes Wi-Fi para mejorar los servicios de ubicación de Google, incluso cuando el interfaz Wi-Fi esté deshabilitado:



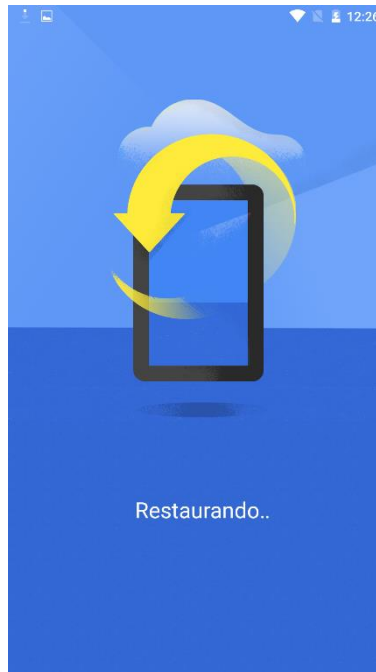
2213. Se recomienda deshabilitar ambas opciones de ubicación y habilitarlas, si se desea, posteriormente a través del menú de “Ajustes” correspondiente. En concreto, estas dos opciones corresponden a “Ajustes [Personal] - Ubicación - Modo: Alta precisión” (Determinar ubicación con GPS, redes Wi-Fi y redes móviles) y a la activación de la



opción disponible desde “Ajustes [Conexiones Inalámbricas y Redes] - Wi-Fi - [...] - Ajustes avanzados - Buscar redes siempre”, respectivamente.

2214. En caso de deshabilitar ambas opciones, la configuración de los servicios de ubicación disponible bajo el menú “Ajustes [Personal] - Ubicación - Modo” corresponderá a la opción “Solo en dispositivo”.

2215. Si se ha seleccionado la cuenta de usuario de Google, el dispositivo recibirá de los servidores de Google las apps que estuviesen vinculadas a la cuenta como “instaladas”:

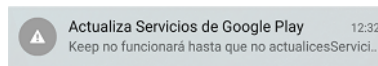


2216. La instalación finaliza con un mensaje sobre cómo personalizar el dispositivo móvil. Una vez se presione el botón “Entendido”, se podrá comenzar a utilizar el dispositivo.

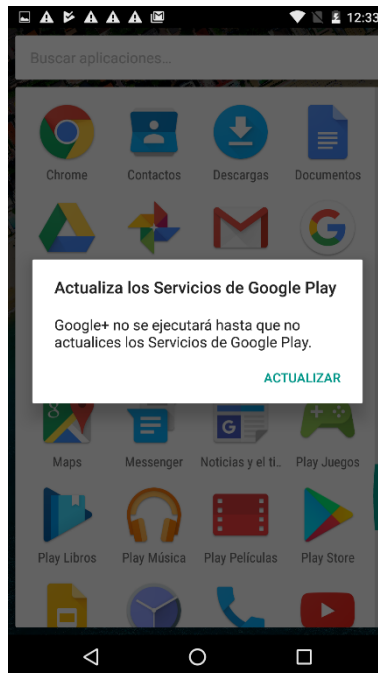


2217. Inicialmente el dispositivo da la bienvenida al usuario y le sugiere personalizar la pantalla de inicio, los *widgets* y los ajustes, pero se ha eliminado el asistente presente en versiones previas de Android (4.x y versiones anteriores).

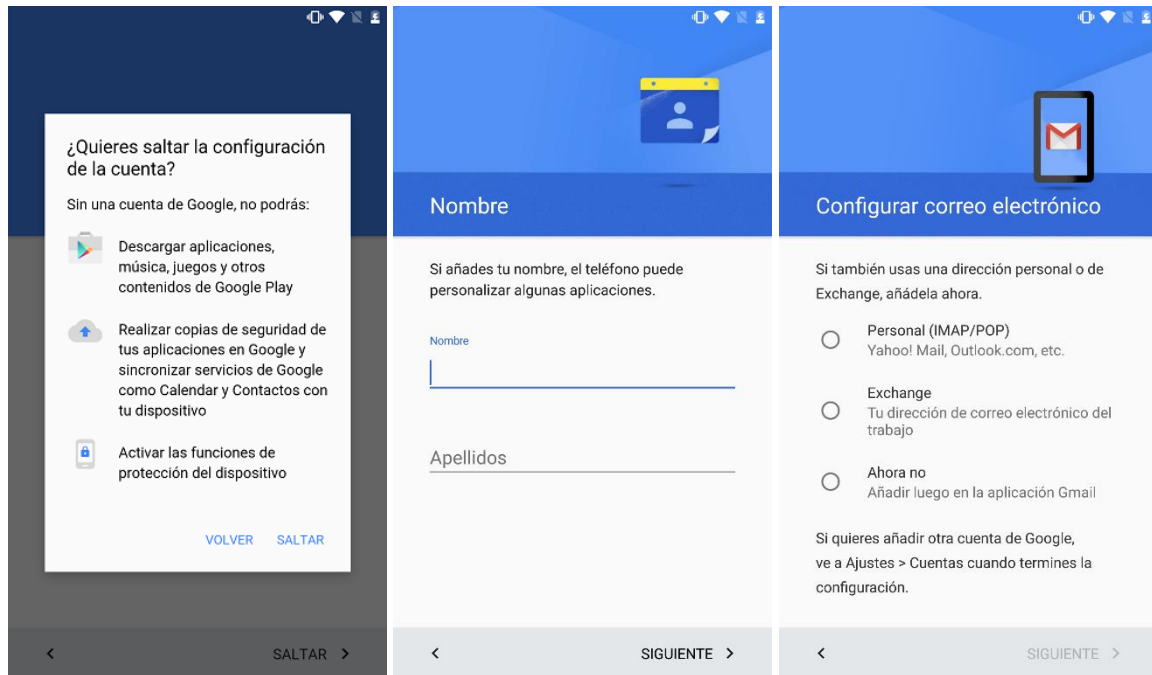
2218. Mientras se completa la instalación, el dispositivo móvil se conecta a servidores de Google por HTTP y HTTPS para comprobar si existen actualizaciones del sistema operativo (ver apartado “6. Actualización del sistema operativo Android”).
2219. Una vez completado el proceso de de instalación y configuración inicial de Android 6.x, se recomienda la aplicación de las recomendaciones reflejadas en la presente guía.
2220. En Android 6.0.1, se recibirá una notificación informando de la necesidad de actualizar los servicios de Google Play para el correcto funcionamiento de diversos servicios y aplicaciones. Esto se debe a los cambios introducidos en los diversos servicios de Google descritos a lo largo de la presente guía como, por ejemplo, “Google Play Protect”.



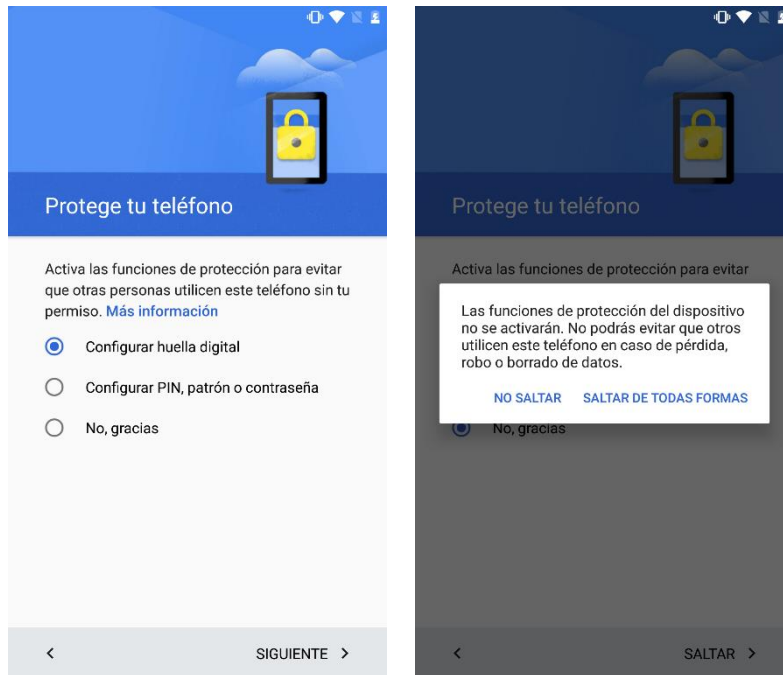
2221. Si se selecciona la notificación, se permitirá actualizar la versión de los “Google Play Services”, algo que no es posible forzar posteriormente, pues la actualización de ese componente se lleva a cabo por parte de Google automáticamente y según sus propios criterios y consideraciones.



2222. Si se opta por no vincular el dispositivo móvil a una cuenta de usuario de Google, se mostrará la pantalla que permite agregar un nombre. Si no se desea realizar este paso, se seleccionará la opción “Siguiente”. Si el proceso de instalación se realiza con conexión a una red Wi-Fi, se presentará una pantalla que permite configurar un correo electrónico de otro servicio (diferente a Google y GMail), o alternatively se puede optar por la opción “Ahora no”. Además, se muestra la información de cómo agregar una cuenta de usuario de Google con posterioridad a la instalación. Si no se está completando el proceso de instalación con conexión a una red Wi-Fi, se pasará directamente al siguiente paso de configuración.

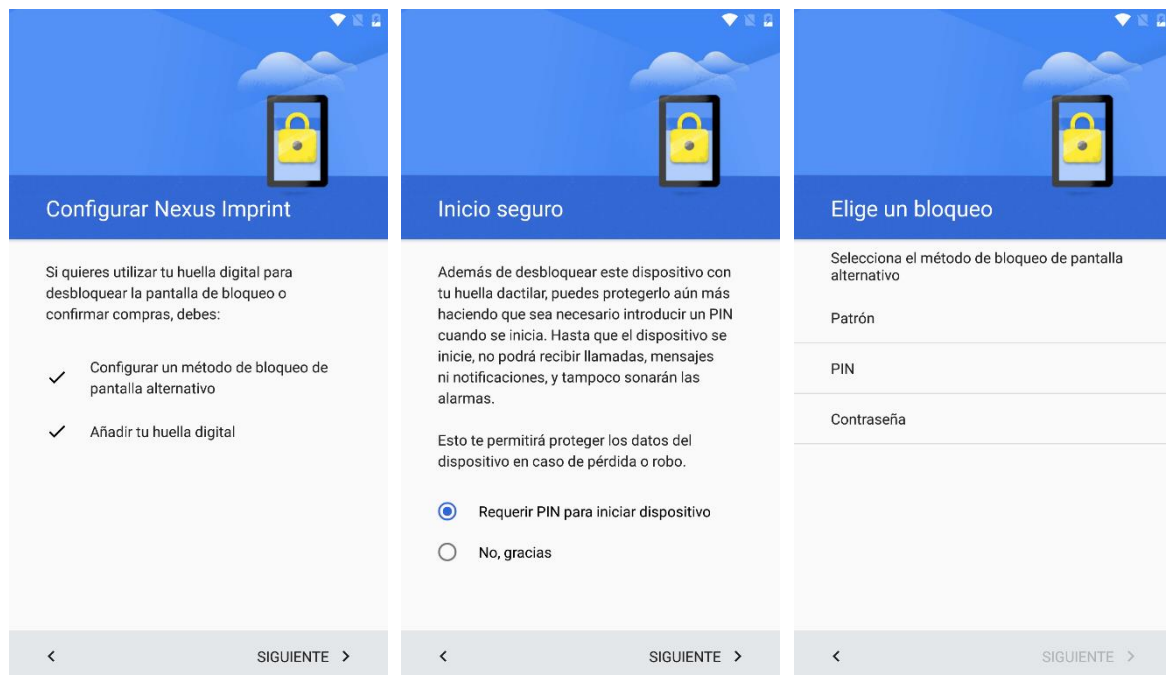


2223. En caso de no configurarse la conexión a una red Wi-Fi durante la instalación, se mostrará al usuario la pantalla de configuración del código de acceso (“Protege tu teléfono”), que permite tanto dar de alta una huella dactilar digital, como definir únicamente un código de acceso: un PIN, un patrón o una contraseña. Si no se desea configurar un código de acceso, se puede seleccionar la opción “Siguiente”. Tras activar el código de acceso seleccionado, no será posible retroceder a pasos previos del proceso de instalación, y el mecanismo de protección configurado permanecerá vigente aunque el terminal se apague antes de finalizar el proceso inicial de configuración.
2224. A continuación, se inicia la configuración de la protección de acceso al dispositivo móvil, pudiendo elegir entre “Configurar huella digital”, “Configurar PIN, patrón o contraseña” o ninguna (mediante la opción “No, gracias”). Este paso de configuración es novedad en Android 6.x respecto a versiones anteriores, como Android 5.x, en la cual no se solicitaba dar de alta ningún mecanismo de protección del dispositivo móvil basado en un código de acceso durante el proceso de instalación inicial.



2225. Si se selecciona la opción “No, gracias” (opción absolutamente desaconsejada desde el punto de vista de seguridad), se informa del riesgo de uso no autorizado, y se solicita confirmación al usuario mediante la opción “Omitir de todos modos” o “Saltar de todas formas”, o la posibilidad de revisar la respuesta mediante “No omitir” o “No saltar”.

2226. Si se selecciona la opción de huella dactilar digital, se muestra una pantalla que informa sobre el proceso de desbloqueo con huella. Si se selecciona la opción “Siguiente”, se informa al usuario de que, para poder usar la huella dactilar digital como método de acceso, es necesario configurar además un método o código de acceso alternativo. Al seleccionar la opción “Siguiente”, se muestra una pantalla para seleccionar el método de acceso alternativo: PIN, patrón o contraseña.

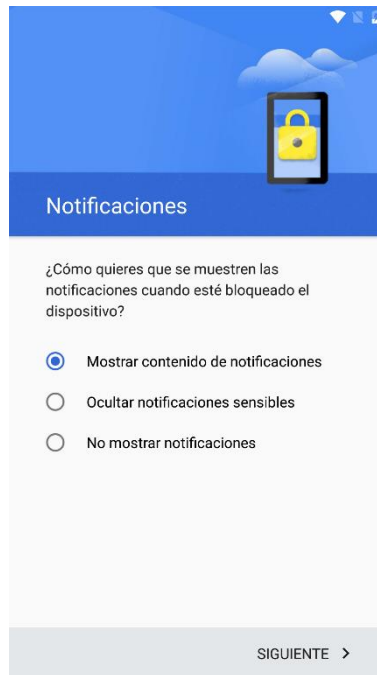


2227. Sea cual sea el método de acceso alternativo elegido, aparecerá el menú de configuración de dicho tipo de código de acceso y, aunque se seleccione la opción “No, gracias”, el dispositivo móvil pasará a configurar el método de acceso correspondiente,

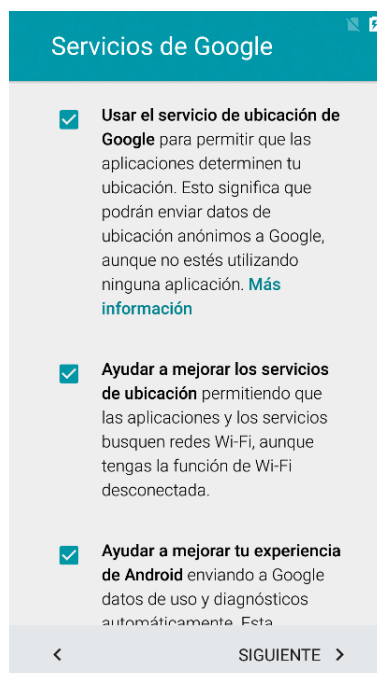
siendo necesario emplear el botón del triángulo inferior seguido del botón de retroceso para volver a la pantalla de selección de un tipo concreto de código de acceso.

2228. Si, en lugar de pedir utilizar huella digital, se selecciona “PIN, patrón o contraseña”, aparece una pantalla que permite establecer cuál de las tres medidas de protección quedará habilitada tras la instalación.

2229. El siguiente paso es relativo al servicio de notificaciones, permitiendo configurar si se desea que se muestren éstas y en qué medida. Para omitir las notificaciones, se puede seleccionar “No mostrar notificaciones”.



2230. El último paso de la instalación consiste en seleccionar qué servicios de Google se desea activar inicialmente. Se recomienda desactivarlos todos y elegir, con posterioridad al proceso de instalación, cuáles se desea activar:



2231. Una vez se haya dado de alta un PIN, contraseña o patrón, si el dispositivo permanece inactivo un tiempo durante este último paso de configuración, se solicitará desbloquear el terminal mediante la opción elegida (no se incluye la huella digital). Una vez registradas todas las huellas que se desee, se puede seleccionar el botón “Listo”.

## 25. APÉNDICE B: CAPTURA DE LA PANTALLA EN ANDROID

2232. En versiones previas de Android hasta la versión 4.x no existía ninguna aplicación nativa para capturar la pantalla del dispositivo móvil (*screenshot*), y era necesario emplear aplicaciones de terceros que, en su mayor parte, requerían efectuar el proceso de *root* del dispositivo móvil (dependiendo del modelo de terminal).
2233. Sin embargo, también era posible realizar capturas de la pantalla del dispositivo móvil Android mediante un ordenador a través del puerto USB haciendo uso de las capacidades de depuración del kit de desarrollo de software (SDK, *Software Development Kit*) de Android.
2234. Desde Android 4.0, Ice Cream Sandwich (ICS), es posible obtener una captura de la pantalla del dispositivo móvil manteniendo pulsados el botón de encendido/apagado y el botón de bajar el volumen simultáneamente, hasta que se oiga un sonido de confirmación, o se reciba una confirmación mediante una animación visual en pantalla.
2235. Adicionalmente se puede recibir una notificación asociada a dicha captura en el centro de notificaciones disponible en la parte superior.
2236. La captura de pantalla será almacenada en la galería de fotos (o fotografías), dentro de la carpeta “Screenshots”, y está disponible a través de USB mediante la carpeta “Pictures/Screenshots” de la memoria interna del dispositivo móvil o de la tarjeta externa de almacenamiento.
2237. Adicionalmente sigue siendo posible realizar una captura de la pantalla del dispositivo mediante ADB (Android Debug Bridge)<sup>121</sup>, empleando los siguientes comandos:

```
C:\> adb shell screencap -p /sdcard/screen.png
C:\> adb pull /sdcard/screen.png
C:\> adb shell rm /sdcard/screen.png
```

2238. Por otro lado, desde Android 4.4, KitKat (nivel de API 19), es posible realizar una grabación en vídeo (en formato MPEG-4, sin audio) de la pantalla del dispositivo móvil a través de ADB. El siguiente comando permite realizar una grabación a 8 Mbps de resolución (en lugar de los 4 Mbps empleados por defecto), durante 45 segundos como máximo (en lugar de emplear la duración por defecto y máxima de 3 minutos, 180 segundos), y se almacenará el vídeo en la tarjeta SD del dispositivo móvil:

```
C:\> adb shell screenrecord --bit-rate 8000000 --time-limit 45 /sdcard/kitkat-
video.mp4 (pulsar ctrl+c para parar la grabación antes de tiempo)
```

2239. Se dispone de más información sobre las diferentes opciones de grabación de la pantalla de Android en el sitio web para desarrolladores de Android y, en concreto, de ADB<sup>122</sup>.
2240. Si una app muestra vídeos o contenidos protegidos que no desea que sean grabados a través de esta funcionalidad, puede hacer uso del método “SurfaceView.setSecure()” para marcar el contenido como protegido.

<sup>121</sup> <http://developer.android.com/tools/help/adb.html>

<sup>122</sup> <http://developer.android.com/tools/help/adb.html#screenrecord>



## 26. REFERENCIAS

La siguiente tabla muestra las fuentes de información a las que se hace referencia a lo largo de la presente guía<sup>123</sup>:

Referencia	Título, autor y ubicación
[Ref.- 1]	Android. Google. URL: <a href="http://www.android.com">http://www.android.com</a>
[Ref.- 2]	Google Nexus 5. Google. URL: <a href="http://www.google.com/nexus/5/">http://www.google.com/nexus/5/</a>
[Ref.- 3]	Google Nexus 5X. Google. URL: <a href="https://www.google.com/nexus/5x/">https://www.google.com/nexus/5x/</a>
[Ref.- 4]	Google Play. URL: <a href="https://play.google.com">https://play.google.com</a>
[Ref.- 5]	"Exercising Our Remote Application Removal Feature". Rich Cannings. Android. June 2010. URL: <a href="http://android-developers.blogspot.com/2010/06/exercising-our-remote-application.html">http://android-developers.blogspot.com/2010/06/exercising-our-remote-application.html</a>
[Ref.- 6]	"Actualizar las aplicaciones Android". Google. URL: <a href="https://support.google.com/googleplay/answer/113412?hl=es">https://support.google.com/googleplay/answer/113412?hl=es</a>
[Ref.- 7]	Android Developers. Google. URL: <a href="http://developer.android.com">http://developer.android.com</a>
[Ref.- 8]	"The dark side of the new Google Play". Denis. Kaspersky Lab Expert. February 2011. URL: <a href="http://www.securelist.com/en/blog/11153/The_dark_side_of_the_new_Android_Play">http://www.securelist.com/en/blog/11153/The_dark_side_of_the_new_Android_Play</a>
[Ref.- 9]	"Android 2.3 Platform and Updated SDK Tools". December 2010. Google. URL: <a href="http://android-developers.blogspot.com/2010/12/android-23-platform-and-updated-sdk.html">http://android-developers.blogspot.com/2010/12/android-23-platform-and-updated-sdk.html</a>
[Ref.- 10]	"Android 2.3.3 Platform, New NFC Capabilities". February 2011. Google. URL: <a href="http://android-developers.blogspot.com/2011/02/android-233-platform-new-nfc.html">http://android-developers.blogspot.com/2011/02/android-233-platform-new-nfc.html</a>
[Ref.- 11]	"Android Architecture Components". Google. URL: <a href="https://developer.android.com/develop/index.html">https://developer.android.com/develop/index.html</a>
[Ref.- 12]	"SafetyNet Helper Sample". Google Play. URL: <a href="https://play.google.com/store/apps/details?id=com.scottyab.safetynet.sample">https://play.google.com/store/apps/details?id=com.scottyab.safetynet.sample</a>
[Ref.- 13]	"Google Apps Device Policy". Google. URL: <a href="https://play.google.com/store/apps/details?id=com.google.android.apps.enterprise.dmagent">https://play.google.com/store/apps/details?id=com.google.android.apps.enterprise.dmagent</a> URL: <a href="https://www.google.com/support/mobile/bin/answer.py?hl=en&amp;answer=190930">https://www.google.com/support/mobile/bin/answer.py?hl=en&amp;answer=190930</a>
[Ref.- 14]	"Google Authenticator". Google. Google Play. URL: <a href="https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2">https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2</a> URL: <a href="https://www.google.com/support/accounts/bin/answer.py?answer=1066447">https://www.google.com/support/accounts/bin/answer.py?answer=1066447</a>

<sup>123</sup> El texto "[old]" indica que se tiene constancia de que el enlace pudiera no estar operativo, o estar desactualizado, en la actualidad, pero se mantiene debido a su relevancia y por motivos históricos. En algunos casos se acompaña de una referencia actualizada, indicada por el texto "[actualizada]".

Referencia	Título, autor y ubicación
[Ref.- 15]	“About 2-step verification”. Google.   URL: <a href="https://support.google.com/accounts/answer/180744">https://support.google.com/accounts/answer/180744</a>
[Ref.- 16]	“Application Fundamentals”. Android Developers. Google.   URL: <a href="http://developer.android.com/guide/components/fundamentals.html">http://developer.android.com/guide/components/fundamentals.html</a>
[Ref.- 17]	Android Developers - Direct Share. Google.   URL: <a href="https://developer.android.com/samples/DirectShare/index.html">https://developer.android.com/samples/DirectShare/index.html</a>
[Ref.- 18]	“Mobile Application Security”. Himanshu Dwivedi, Chris Clark, David Thiel. McGraw-Hill. ISBN: 0071633561. 2010.   URL: <a href="http://www.mhprofessional.com/product.php?isbn=0071633561">http://www.mhprofessional.com/product.php?isbn=0071633561</a>
[Ref.- 19]	“API Levels”. Android Developers. Google.   URL: <a href="http://developer.android.com/guide/appendix/api-levels.html">http://developer.android.com/guide/appendix/api-levels.html</a>
[Ref.- 20]	“Verificación en dos pasos (two-step verification)”. Google.   URL: <a href="https://www.google.com/landing/2step/">https://www.google.com/landing/2step/</a>   URL: <a href="https://www.google.com/landing/2step/features.html">https://www.google.com/landing/2step/features.html</a>
[Ref.- 21]	“Android VPN Connectivity”. pfSense.   URL: <a href="https://doc.pfsense.org/index.php/Android_VPN_Connectivity">https://doc.pfsense.org/index.php/Android_VPN_Connectivity</a>
[Ref.- 22]	Android Studio &amp; SDK (Software Development Kit). Google.   URL: <a href="http://developer.android.com/sdk/index.html">http://developer.android.com/sdk/index.html</a>
[Ref.- 23]	Manifest Permission (Since API Level 1). Google.   URL: <a href="http://developer.android.com/reference/android/Manifest.permission.html">http://developer.android.com/reference/android/Manifest.permission.html</a>
[Ref.- 24]	“Android Security 2015 Year in Review”. Google Report. Android security Center. April 2016.   URL: <a href="http://static.googleusercontent.com/media/source.android.com/en//security/reports/Google_Android_Security_2015_Report_Final.pdf">http://static.googleusercontent.com/media/source.android.com/en//security/reports/Google_Android_Security_2015_Report_Final.pdf</a>
[Ref.- 25]	“SafetyNet: Google's tamper detection for Android”. John Kozyrakis.   URL: <a href="https://koz.io/inside-safetynet/">https://koz.io/inside-safetynet/</a>
[Ref.- 26]	“Code signing in Android's security model”. Nikolay Elenkov. May 2013.   URL: <a href="http://nelenkov.blogspot.com.es/2013/05/code-signing-in-androids-security-model.html">http://nelenkov.blogspot.com.es/2013/05/code-signing-in-androids-security-model.html</a>
[Ref.- 27]	“BouncyCastle Key Store (BKS) library”. The Legion of the Bouncy Castle.   URL: <a href="http://bouncycastle.org/download/bcprov-jdk16-141.jar">http://bouncycastle.org/download/bcprov-jdk16-141.jar</a>
[Ref.- 28]	“Signing Your Applications”. Android Developers.   URL: <a href="http://developer.android.com/guide/publishing/app-signing.html">http://developer.android.com/guide/publishing/app-signing.html</a>
[Ref.- 29]	RedPhone. Open WhisperSystems. 2015.   URL: <a href="https://whispersystems.org">https://whispersystems.org</a>   URL: <a href="https://play.google.com/store/apps/details?id=org.thoughtcrime.redphone">https://play.google.com/store/apps/details?id=org.thoughtcrime.redphone</a>
[Ref.- 30]	“Getting Your SMS Apps Ready for KitKat”. Android Developers Blog. October 2013.   URL: <a href="http://android-developers.blogspot.com.es/2013/10/getting-your-sms-apps-ready-for-kitkat.html">http://android-developers.blogspot.com.es/2013/10/getting-your-sms-apps-ready-for-kitkat.html</a>
[Ref.- 31]	“Android 3.0 Platform Highlights”. Google. 2011.   URL: <a href="http://developer.android.com/sdk/android-3.0-highlights.html#enterprise">http://developer.android.com/sdk/android-3.0-highlights.html#enterprise</a>

Referencia	Título, autor y ubicación
[Ref.- 32]	Signal (Private Messenger). Open Whisper Systems. URL: <a href="https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms">https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms</a> URL: <a href="https://github.com/WhisperSystems/Signal-Android">https://github.com/WhisperSystems/Signal-Android</a>
[Ref.- 33]	TextSecure. Open Whisper Systems. 2015. URL: <a href="https://whispersystems.org">https://whispersystems.org</a> URL: <a href="https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms">https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms</a>
[Ref.- 34]	"Using KitKat verified boot". Nikolai Elenkov. May 2014. URL: <a href="https://nelenkov.blogspot.com/2014/05/using-kitkat-verified-boot.html">https://nelenkov.blogspot.com/2014/05/using-kitkat-verified-boot.html</a>
[Ref.- 35]	"SafetyNet Playground". Google Play. URL: <a href="https://play.google.com/store/apps/details?id=com.cigital.safetynetplayground">https://play.google.com/store/apps/details?id=com.cigital.safetynetplayground</a>
[Ref.- 36]	"Understanding Exchange ActiveSync Mailbox Policies". MS Exchange 2010 SP2 & SP3. Microsoft Technet. 2014. URL: <a href="https://technet.microsoft.com/en-us/library/bb123484.aspx">https://technet.microsoft.com/en-us/library/bb123484.aspx</a>
[Ref.- 37]	"View or Configure Exchange ActiveSync Mailbox Policy Properties" (Microsoft Exchange 2010). Microsoft Technet. 2010. URL: <a href="http://technet.microsoft.com/en-us/library/bb123994.aspx">http://technet.microsoft.com/en-us/library/bb123994.aspx</a>
[Ref.- 38]	"Android support for Microsoft Exchange in pure Google devices". Google. 2013. URL: <a href="http://static.googleusercontent.com/media/www.google.com/es//help/hc/images/android/MicrosoftExchangePoliciesinAndroid.pdf">http://static.googleusercontent.com/media/www.google.com/es//help/hc/images/android/MicrosoftExchangePoliciesinAndroid.pdf</a>
[Ref.- 39]	"Issue 82: wifi - support ad hoc networking". Android Google Code. 2008. URL: <a href="https://code.google.com/p/android/issues/detail?id=82">https://code.google.com/p/android/issues/detail?id=82</a>
[Ref.- 40]	"Ad-Hoc (IBSS) mode support for Android 4.2.2 / 4.3 / 4.4". Thinktube. March 2014. URL: <a href="http://www.thinktube.com/tech-en/android/wifi-ibss">http://www.thinktube.com/tech-en/android/wifi-ibss</a>
[Ref.- 41]	"Why Wi-Fi Direct cannot replace Ad-hoc mode". szym. Thinktube. 2014. URL: <a href="http://www.thinktube.com/tech-en/android/wifi-direct">http://www.thinktube.com/tech-en/android/wifi-direct</a>
[Ref.- 42]	"Issue 1041: Hidden SSID Fails to Connect". Android Google Code. 2008. URL: <a href="https://code.google.com/p/android/issues/detail?id=1041">https://code.google.com/p/android/issues/detail?id=1041</a>
[Ref.- 43]	"How can I trust CAcert's root certificate?". CAcert Wiki. URL: <a href="http://wiki.cacert.org/ImportRootCert#Android_Phones">http://wiki.cacert.org/ImportRootCert#Android_Phones</a>
[Ref.- 44]	"Android code signing". Nikolay Elenkov. April 2013. URL: <a href="http://nelenkov.blogspot.com.es/2013/04/android-code-signing.html">http://nelenkov.blogspot.com.es/2013/04/android-code-signing.html</a>
[Ref.- 45]	"RealmB's Android Certificate Installer". RealmB. URL: <a href="http://www.realmmb.com/droidCert/">http://www.realmmb.com/droidCert/</a>
[Ref.- 46]	"Settings-Secure". Android Developers. URL: <a href="http://developer.android.com/reference/android/provider/Settings.Secure.html">http://developer.android.com/reference/android/provider/Settings.Secure.html</a>
[Ref.- 47]	dhcpcd. Roy Marples. URL: <a href="https://roy.marples.name/projects/dhcpcd">https://roy.marples.name/projects/dhcpcd</a>

Referencia	Título, autor y ubicación
[Ref.- 48]	“Guía CCN-STIC-406: Seguridad en redes inalámbricas”. CCN-CERT.   URL: <a href="https://www.ccn-cert.cni.es">https://www.ccn-cert.cni.es</a> (Guías)
[Ref.- 49]	“Description of the Wireless Client Update for Windows XP with Service Pack 2”. Microsoft. 2010.   URL: <a href="http://support.microsoft.com/kb/917021">http://support.microsoft.com/kb/917021</a>
[Ref.- 50]	“Guía CCN-STIC-418: Seguridad en Bluetooth”. CCN-CERT.   URL: <a href="https://www.ccn-cert.cni.es">https://www.ccn-cert.cni.es</a> (Guías)
[Ref.- 51]	“ConnectivityManager”. Android Developers.   URL: <a href="https://developer.android.com/reference/android/net/ConnectivityManager.html">https://developer.android.com/reference/android/net/ConnectivityManager.html</a>
[Ref.- 52]	“Wi-Fi Direct (“P2P”)”. Wi-Fi Alliance. 2013.   URL: <a href="http://www.wi-fi.org/discover-and-learn/wi-fi-direct">http://www.wi-fi.org/discover-and-learn/wi-fi-direct</a>
[Ref.- 53]	“Issue 3389: Full IPv6 Android support”. Android Google Code. 2009.   URL: <a href="https://code.google.com/p/android/issues/detail?id=3389">https://code.google.com/p/android/issues/detail?id=3389</a>   URL: <a href="https://code.google.com/p/android/issues/detail?id=3389#c107">https://code.google.com/p/android/issues/detail?id=3389#c107</a>
[Ref.- 54]	“Issue 14013: Enable IPv6 Privacy Extensions”. Android Google Code. 2011.   URL: <a href="https://code.google.com/p/android/issues/detail?id=14013">https://code.google.com/p/android/issues/detail?id=14013</a>   URL: <a href="http://www.h-online.com/security/news/item/IPv6-Smartphones-compromise-users-privacy-1169708.html">http://www.h-online.com/security/news/item/IPv6-Smartphones-compromise-users-privacy-1169708.html</a>
[Ref.- 55]	“These aren’t the permissions you’re looking for”. A. Lineberry, D. Richardson, T. Wyatt”. Defcon 18. 2010.   URL: <a href="https://media.defcon.org/DEF%20CON%2018/DEF%20CON%2018%20slides/DEF%20CON%2018%20Hacking%20Conference%20Presentation%20By%20-%20Lineberry%20Richardson%20and%20Wyatt%20-%20These%20Aren%27t%20the%20Permissions%20-%20Slides.m4v">https://media.defcon.org/DEF%20CON%2018/DEF%20CON%2018%20slides/DEF%20CON%2018%20Hacking%20Conference%20Presentation%20By%20-%20Lineberry%20Richardson%20and%20Wyatt%20-%20These%20Aren%27t%20the%20Permissions%20-%20Slides.m4v</a>
[Ref.- 56]	“Support connecting to IPv6-only wireless networks”. Android Google Code. June 2012.   URL: <a href="https://code.google.com/p/android/issues/detail?id=32630">https://code.google.com/p/android/issues/detail?id=32630</a>
[Ref.- 57]	“Best Practices for Security &amp; Privacy”. Android Developers.   URL: <a href="https://developer.android.com/training/best-security.html">https://developer.android.com/training/best-security.html</a>
[Ref.- 58]	“Use of IPv6 privacy extensions should be configurable “. Android Google Code. May 2012.   URL: <a href="https://code.google.com/p/android/issues/detail?id=31102">https://code.google.com/p/android/issues/detail?id=31102</a>
[Ref.- 59]	“2 big points critics always miss about Android upgrades”. Computer World. June 2015.   URL: <a href="http://www.computerworld.com/article/2476391/android/2-big-points-critics-always-miss-about-android-upgrades.html">http://www.computerworld.com/article/2476391/android/2-big-points-critics-always-miss-about-android-upgrades.html</a>
[Ref.- 60]	“Encontrar un dispositivo Android que has perdido”. Google.   URL: <a href="https://support.google.com/accounts/answer/3265955?hl=es">https://support.google.com/accounts/answer/3265955?hl=es</a>
[Ref.- 61]	“12 Days of HaXmas: A year of Metasploit Android exploits”. Rapid 7. January 2015.   URL: <a href="https://community.rapid7.com/community/metasploit/blog/2015/01/02/2014-a-year-of-android-exploits-in-metasploit">https://community.rapid7.com/community/metasploit/blog/2015/01/02/2014-a-year-of-android-exploits-in-metasploit</a>

Referencia	Título, autor y ubicación
[Ref.- 62]	“WebView addJavascriptInterface Remote Code Execution”. MRW Labs. September 2013.   URL: <a href="https://labs.mwrinfosecurity.com/blog/2013/09/24/webview-addjavascriptinterface-remote-code-execution/">https://labs.mwrinfosecurity.com/blog/2013/09/24/webview-addjavascriptinterface-remote-code-execution/</a>   URL: <a href="https://labs.mwrinfosecurity.com/blog/2012/04/23/adventures-with-android-webviews/">https://labs.mwrinfosecurity.com/blog/2012/04/23/adventures-with-android-webviews/</a>
[Ref.- 63]	“Por qué se debe iniciar sesión en Chrome”. Google.   URL: <a href="https://support.google.com/chrome/answer/165139?hl=es">https://support.google.com/chrome/answer/165139?hl=es</a>   URL: <a href="https://support.google.com/chrome/answer/1181035">https://support.google.com/chrome/answer/1181035</a>   URL: <a href="https://support.google.com/chrome/answer/2591582?hl=es">https://support.google.com/chrome/answer/2591582?hl=es</a>
[Ref.- 64]	Android Vulnerabilities. 2015.   URL: <a href="http://androidvulnerabilities.org">http://androidvulnerabilities.org</a>
[Ref.- 65]	“No puedes desbloquear el dispositivo Android”. Google.   URL: <a href="https://support.google.com/nexus/answer/3388218?hl=es">https://support.google.com/nexus/answer/3388218?hl=es</a>
[Ref.- 66]	“Android Security Announcements”. Google Groups. 2008.   URL: <a href="https://groups.google.com/group/android-security-announce">https://groups.google.com/group/android-security-announce</a>
[Ref.- 67]	“Android Security Discussions”. Google Groups. 2008.   URL: <a href="http://groups.google.com/group/android-security-discuss">http://groups.google.com/group/android-security-discuss</a>
[Ref.- 68]	[old] “Android Security FAQ”. Android Developers.   URL: <a href="http://developer.android.com/resources/faq/security.html">http://developer.android.com/resources/faq/security.html</a>   URL [actualizada]: <a href="https://developer.android.com/training/best-security.html">https://developer.android.com/training/best-security.html</a>
[Ref.- 69]	“Android Security Bulletines (or Updates)”. Google. August 2015.   URL: <a href="https://source.android.com/security/bulletin/">https://source.android.com/security/bulletin/</a>   URL: <a href="https://groups.google.com/forum/#!forum/android-security-updates">https://groups.google.com/forum/#!forum/android-security-updates</a>
[Ref.- 70]	“LG Security Bulletins”. LG.   URL: <a href="https://lgsecurity.lge.com/security_updates.html">https://lgsecurity.lge.com/security_updates.html</a>
[Ref.- 71]	“Google Play Devices”. Google.   URL: <a href="https://play.google.com/store/devices">https://play.google.com/store/devices</a>
[Ref.- 72]	“Google Experience Devices”. DanKor. 2012.   URL: <a href="http://about.me/googleexperiencedevice">http://about.me/googleexperiencedevice</a>   URL: <a href="http://googleexperiencedevice.blogspot.com">http://googleexperiencedevice.blogspot.com</a>
[Ref.- 73]	“Factory Images for Nexus and Pixel Devices”. Google.   URL: <a href="https://developers.google.com/android/images">https://developers.google.com/android/images</a>
[Ref.- 74]	“Nexus help. Check &amp; update your Android version”. Google.   URL: <a href="https://support.google.com/nexus/answer/4457705">https://support.google.com/nexus/answer/4457705</a>
[Ref.- 75]	“History of the Nexus family”. Android Authority.   URL: <a href="http://www.androidauthority.com/history-nexus-smartphone-line-536352/">http://www.androidauthority.com/history-nexus-smartphone-line-536352/</a>
[Ref.- 76]	“Android WiFi-Direct Denial of Service”. Core Security. January 2015.   URL: <a href="http://www.coresecurity.com/advisories/android-wifi-direct-denial-service">http://www.coresecurity.com/advisories/android-wifi-direct-denial-service</a>

Referencia	Título, autor y ubicación
[Ref.- 77]	“Android Screen Lock Bypass”. Thomas Cannon. 2011.   URL: <a href="http://thomascannon.net/blog/2011/02/android-lock-screen-bypass/">http://thomascannon.net/blog/2011/02/android-lock-screen-bypass/</a>
[Ref.- 78]	“Android Market Security”. Thomas Cannon. 2011.   URL: <a href="http://thomascannon.net/blog/2011/02/android-market-security/">http://thomascannon.net/blog/2011/02/android-market-security/</a>
[Ref.- 79]	“Certificate pinning in Android 4.2”. Nikolay Elenkov. December 2012.   URL: <a href="http://nelenkov.blogspot.com/2012/12/certificate-pinning-in-android-42.html">http://nelenkov.blogspot.com/2012/12/certificate-pinning-in-android-42.html</a>
[Ref.- 80]	“A Peek Inside the GTalkService Connection”. Jon Oberheide. 2010.   URL: <a href="http://jon.oberheide.org/blog/2010/06/28/a-peek-inside-the-gtalkservice-connection/">http://jon.oberheide.org/blog/2010/06/28/a-peek-inside-the-gtalkservice-connection/</a>
[Ref.- 81]	“Remote Kill and Install on Google Android”. Jon Oberheide. 2010.   URL: <a href="http://jon.oberheide.org/blog/2010/06/25/remote-kill-and-install-on-google-android/">http://jon.oberheide.org/blog/2010/06/25/remote-kill-and-install-on-google-android/</a>
[Ref.- 82]	“Apple. Google Collect User Data”. Wall Street Journal. 2011.   URL: <a href="http://on.wsj.com/gDfmEV">http://on.wsj.com/gDfmEV</a>
[Ref.- 83]	“Android Map”. Samy Kamkar. 2011.   URL: <a href="http://samy.pl/androidmap/">http://samy.pl/androidmap/</a>
[Ref.- 84]	Android Open Source Project (AOSP).   URL: <a href="http://source.android.com">http://source.android.com</a>
[Ref.- 85]	“Android Encryption”. Android.   URL: <a href="https://source.android.com/security/encryption/">https://source.android.com/security/encryption/</a>
[Ref.- 86]	“Android X.Y Platform Highlights” &amp; “Welcome to Android 4.x” &amp; “Android &lt;version&gt;”. Android Developers.   URL (2.2): <a href="http://developer.android.com/about/versions/android-2.2-highlights.html">http://developer.android.com/about/versions/android-2.2-highlights.html</a>   URL (2.3): <a href="http://developer.android.com/about/versions/android-2.3-highlights.html">http://developer.android.com/about/versions/android-2.3-highlights.html</a>   URL (3.0): <a href="http://developer.android.com/about/versions/android-3.0-highlights.html">http://developer.android.com/about/versions/android-3.0-highlights.html</a>   URL (4.0): <a href="http://developer.android.com/about/versions/android-4.0-highlights.html">http://developer.android.com/about/versions/android-4.0-highlights.html</a>   URL (4.1): <a href="http://developer.android.com/about/versions/jelly-bean.html#android-41">http://developer.android.com/about/versions/jelly-bean.html#android-41</a>   URL (4.2): <a href="http://developer.android.com/about/versions/jelly-bean.html#android-42">http://developer.android.com/about/versions/jelly-bean.html#android-42</a>   URL (4.3): <a href="http://developer.android.com/about/versions/jelly-bean.html#android-43">http://developer.android.com/about/versions/jelly-bean.html#android-43</a>   URL (4.4): <a href="https://developer.android.com/about/versions/kitkat.html">https://developer.android.com/about/versions/kitkat.html</a>   URL (5.0): <a href="https://developer.android.com/about/versions/lollipop.html">https://developer.android.com/about/versions/lollipop.html</a>   URL (6.0): <a href="https://developer.android.com/about/versions/marshmallow/index.html">https://developer.android.com/about/versions/marshmallow/index.html</a>
[Ref.- 87]	“Compatibility Test Suite (CTS)”. Google.   URL: <a href="http://source.android.com/compatibility/cts/index.html">http://source.android.com/compatibility/cts/index.html</a>
[Ref.- 88]	“Malware-Infected Apps Yanked From Android Market”. Thread post.   URL: <a href="https://threatpost.com/malware-infected-apps-yanked-android-market-030211/74985/">https://threatpost.com/malware-infected-apps-yanked-android-market-030211/74985/</a>
[Ref.- 89]	CTS (Compatibility Test Suite). AOSP.   URL: <a href="http://source.android.com/compatibility/cts-intro.html">http://source.android.com/compatibility/cts-intro.html</a>
[Ref.- 90]	“Checking Device Compatibility with SafetyNet”. Android Developers.   URL: <a href="https://developer.android.com/training/safetynet/index.html">https://developer.android.com/training/safetynet/index.html</a>

Referencia	Título, autor y ubicación
[Ref.- 91]	“Device Policy for Android” &amp; “Device Policy Administration for Android” &amp; “Google Apps Mobile Management: Overview”. Google Mobile.   URL: <a href="https://support.google.com/mobile/bin/answer.py?hl=en&amp;answer=190930">https://support.google.com/mobile/bin/answer.py?hl=en&amp;answer=190930</a>   URL: <a href="http://support.google.com/a/bin/answer.py?hl=en&amp;answer=1056433">http://support.google.com/a/bin/answer.py?hl=en&amp;answer=1056433</a>   URL: <a href="https://support.google.com/a/bin/answer.py?hl=en&amp;answer=1734200">https://support.google.com/a/bin/answer.py?hl=en&amp;answer=1734200</a>
[Ref.- 92]	“Issue 6111: Allow a hostname to be specified”. Android Google Code. January 2010.   URL: <a href="https://code.google.com/p/android/issues/detail?id=6111">https://code.google.com/p/android/issues/detail?id=6111</a>
[Ref.- 93]	“Unpacking Android backups”. Nikolay Elenkov. June 2012.   URL: <a href="http://nelenkov.blogspot.com.es/2012/06/unpacking-android-backups.html">http://nelenkov.blogspot.com.es/2012/06/unpacking-android-backups.html</a>   URL: <a href="https://github.com/nelenkov/android-backup-extractor">https://github.com/nelenkov/android-backup-extractor</a>
[Ref.- 94]	“Establecer conexión mediante zona Wi-Fi, Bluetooth o USB”. Google Mobile.   URL: <a href="https://support.google.com/nexus/answer/2812516?hl=es">https://support.google.com/nexus/answer/2812516?hl=es</a>
[Ref.- 95]	“[TAD-2011-003] Vulnerability in Android: To add, or not to add (a Wi-Fi network), that is the question”. Raúl Siles. Taddong. Mayo 2010.   URL: <a href="http://blog.taddong.com/2011/05/vulnerability-in-android-to-add-or-not.html">http://blog.taddong.com/2011/05/vulnerability-in-android-to-add-or-not.html</a>
[Ref.- 96]	“Issue 1215: IP settings for WiFi networks”. Android Android Google Code. November 2008.   URL: <a href="https://code.google.com/p/android/issues/detail?id=1215">https://code.google.com/p/android/issues/detail?id=1215</a>
[Ref.- 97]	“Putting Android to work for your business”. Official Google Enterprise Blog. April 2011.   URL: <a href="http://googleenterprise.blogspot.com/2011/04/putting-android-to-work-for-your.html">http://googleenterprise.blogspot.com/2011/04/putting-android-to-work-for-your.html</a>
[Ref.- 98]	“SafetyNet”. Google.   URL: <a href="https://developer.android.com/training/safetynet/index.html">https://developer.android.com/training/safetynet/index.html</a>
[Ref.- 99]	“Issue 11855: Support settings change in Android WIFI/USB Tether”. Android Google Code. October 2010. URL: <a href="https://code.google.com/p/android/issues/detail?id=11855">https://code.google.com/p/android/issues/detail?id=11855</a>
[Ref.- 100]	“A Tale Of Another SOP Bypass In Android Browser &lt; 4.4”. Rafay Baloch . October 2014.   URL: <a href="http://www.rafayhackingarticles.net/2014/10/a-tale-of-another-sop-bypass-in-android.html">http://www.rafayhackingarticles.net/2014/10/a-tale-of-another-sop-bypass-in-android.html</a>   URL: <a href="https://community.rapid7.com/community/metasploit/blog/2014/11/06/metasploit-weekly-wrapup">https://community.rapid7.com/community/metasploit/blog/2014/11/06/metasploit-weekly-wrapup</a>
[Ref.- 101]	“Android Fake ID bug exposes smartphones and tablets”. BBC.   URL: <a href="http://www.bbc.com/news/technology-28544443">http://www.bbc.com/news/technology-28544443</a>
[Ref.- 102]	“Package javax.net.ssl”. Android Developers.   URL: <a href="http://developer.android.com/reference/javax/net/ssl/package-summary.html">http://developer.android.com/reference/javax/net/ssl/package-summary.html</a>
[Ref.- 103]	“Magisk (Manager)”. XDA Developers.   URL: <a href="http://forum.xda-developers.com/apps/magisk/official-magisk-v7-universal-systemless-t3473445">http://forum.xda-developers.com/apps/magisk/official-magisk-v7-universal-systemless-t3473445</a>
[Ref.- 104]	“Copia de seguridad y restauración de datos del dispositivo”. Google.   URL: <a href="https://support.google.com/nexus/answer/2819582?hl=es">https://support.google.com/nexus/answer/2819582?hl=es</a>
[Ref.- 105]	“The AndroidManifest.xml File: &lt;permission&gt;”. Android Developers.   URL: <a href="http://developer.android.com/guide/topics/manifest/permission-element.html#plevel">http://developer.android.com/guide/topics/manifest/permission-element.html#plevel</a>



Referencia	Título, autor y ubicación
[Ref.- 106]	“SE Android”. SE Linux Project. 2012.   URL: <a href="https://seandroid.bitbucket.io/">https://seandroid.bitbucket.io/</a>   URL: <a href="http://selinuxproject.org/~jmorris/lss2011_slides/caseforseandroid.pdf">http://selinuxproject.org/~jmorris/lss2011_slides/caseforseandroid.pdf</a>
[Ref.- 107]	“Configurar el control parental”. Google Play.   URL: <a href="https://support.google.com/googleplay/answer/1075738?hl=es">https://support.google.com/googleplay/answer/1075738?hl=es</a>
[Ref.- 108]	“Flash to Focus on PC Browsing and Mobile Apps; Adobe to More Aggressively Contribute to HTML5”. Adobe. Noviembre 2011.   URL: <a href="http://blogs.adobe.com/conversations/2011/11/flash-focus.html">http://blogs.adobe.com/conversations/2011/11/flash-focus.html</a>
[Ref.- 109]	“Issue 10809: Password is stored on disk in plain text”. Android Google Code. August 2010.   URL: <a href="https://code.google.com/p/android/issues/detail?id=10809">https://code.google.com/p/android/issues/detail?id=10809</a>
[Ref.- 110]	“Android Debug Bridge (ADB)”. Android Developers.   URL: <a href="http://developer.android.com/guide/developing/tools/adb.html">http://developer.android.com/guide/developing/tools/adb.html</a>
[Ref.- 111]	“Catching AuthTokens in the Wild - The Insecurity of Google's ClientLogin Protocol”. Bastian Könings, Jens Nickels, and Florian Schaub. Mayo 2011.   URL: <a href="http://www.uni-ulm.de/en/in/mi/staff/koenings/catching-authtokens.html">http://www.uni-ulm.de/en/in/mi/staff/koenings/catching-authtokens.html</a>   URL: <a href="https://freedom-to-tinker.com/blog/dwallach/things-overheard-wifi-my-android-smartphone">https://freedom-to-tinker.com/blog/dwallach/things-overheard-wifi-my-android-smartphone</a>   URL: <a href="http://android.stackexchange.com/questions/3129/what-android-syncd-data-is-encrypted">http://android.stackexchange.com/questions/3129/what-android-syncd-data-is-encrypted</a>
[Ref.- 112]	“Chrome for Android”. Google.   URL: <a href="https://developer.chrome.com/multidevice/faq">https://developer.chrome.com/multidevice/faq</a>
[Ref.- 113]	“Google Data Protocol - FAQ”. Google Code.   URL: <a href="https://code.google.com/apis/gdata/faq.html#clientlogin_expire">https://code.google.com/apis/gdata/faq.html#clientlogin_expire</a>
[Ref.- 114]	“Authentication and Authorization for Google APIs - ClientLogin for Installed Applications”. Google Code.   URL: <a href="https://code.google.com/apis/accounts/docs/AuthForInstalledApps.html">https://code.google.com/apis/accounts/docs/AuthForInstalledApps.html</a>
[Ref.- 115]	“Using OAuth 2.0 to Access Google APIs”. Google.   URL: <a href="https://developers.google.com/accounts/docs/OAuth2">https://developers.google.com/accounts/docs/OAuth2</a>
[Ref.- 116]	“LOOK-10-007 - TapJacking”. Lookout. December 2010.   URL: <a href="http://blog.mylookout.com/look-10-007-tapjacking/">http://blog.mylookout.com/look-10-007-tapjacking/</a>   URL: <a href="http://blog.mylookout.com/blog/2010/12/09/android-touch-event-hijacking/">http://blog.mylookout.com/blog/2010/12/09/android-touch-event-hijacking/</a>
[Ref.- 117]	[old] “Android Master Key Exploit - Uncovering Android Master Key That Makes 99% of Devices Vulnerable”. BlueBox. July 2013.   URL: <a href="https://bluebox.com/technical/uncovering-android-master-key-that-makes-99-of-devices-vulnerable/">https://bluebox.com/technical/uncovering-android-master-key-that-makes-99-of-devices-vulnerable/</a>
[Ref.- 118]	“Android Browser Same Origin Policy Bypass &lt; 4.4 - CVE-2014-6041”. Rafay Baloch . September 2014. URL: <a href="http://www.rafayhackingarticles.net/2014/08/android-browser-same-origin-policy.html">http://www.rafayhackingarticles.net/2014/08/android-browser-same-origin-policy.html</a>   URL: <a href="https://community.rapid7.com/community/metasploit/blog/2014/09/15/major-android-bug-is-a-privacy-disaster-cve-2014-6041">https://community.rapid7.com/community/metasploit/blog/2014/09/15/major-android-bug-is-a-privacy-disaster-cve-2014-6041</a>

Referencia	Título, autor y ubicación
[Ref.- 119]	“Android WebView fixes”. Adrian Ludwig. January 2015.   URL: <a href="https://plus.google.com/+AdrianLudwig/posts/1md7ruEwBLF">https://plus.google.com/+AdrianLudwig/posts/1md7ruEwBLF</a>   URL: <a href="https://community.rapid7.com/community/metasploit/blog/2015/01/11/google-no-longer-provides-patches-for-webview-jelly-bean-and-prior">https://community.rapid7.com/community/metasploit/blog/2015/01/11/google-no-longer-provides-patches-for-webview-jelly-bean-and-prior</a>   URL: <a href="https://community.rapid7.com/community/metasploit/blog/2015/01/16/weekly-metasploit-wrapup">https://community.rapid7.com/community/metasploit/blog/2015/01/16/weekly-metasploit-wrapup</a>
[Ref.- 120]	“Issue 8196: Enhancement: Client Certificate Authentication in Browser”. Android Google Code. May 2010.   URL: <a href="https://code.google.com/p/android/issues/detail?id=8196">https://code.google.com/p/android/issues/detail?id=8196</a>
[Ref.- 121]	“Issue 11231: Provide support for managing CA and client certificates”. Android Google Code. September 2010.   URL: <a href="https://code.google.com/p/android/issues/detail?id=11231">https://code.google.com/p/android/issues/detail?id=11231</a>
[Ref.- 122]	“KeyChain”. Android Developers.   URL: <a href="http://developer.android.com/reference/android/security/KeyChain.html">http://developer.android.com/reference/android/security/KeyChain.html</a>
[Ref.- 123]	“Browser Security Handbook, part 2”. Michal Zalewski. Marzo 2011 (actualizado).   URL: <a href="https://code.google.com/p/browsersec/wiki/Part2#Same-origin_policy_for_cookies">https://code.google.com/p/browsersec/wiki/Part2#Same-origin_policy_for_cookies</a>
[Ref.- 124]	“Uso del ID de publicidad de Android”: Google Play.   URL: <a href="https://play.google.com/intl/es/about/monetization-ads/ads/ad-id/">https://play.google.com/intl/es/about/monetization-ads/ads/ad-id/</a>
[Ref.- 125]	“Issue 6348: Bluetooth should have the option to be constantly discoverable and not just have a set time limit”. Android Google Code. January 2010.   URL: <a href="https://code.google.com/p/android/issues/detail?id=6348">https://code.google.com/p/android/issues/detail?id=6348</a>
[Ref.- 126]	“Malicious Android Applications: Risks and Exploitation”. Joany Boutet. SANS Reading Room. Marzo 2010.   URL: <a href="https://www.sans.org/reading_room/whitepapers/malicious/malicious-android-applications-risks-exploitation_33578">https://www.sans.org/reading_room/whitepapers/malicious/malicious-android-applications-risks-exploitation_33578</a>
[Ref.- 127]	“App Ops Brings Granular Permissions Control to Android 4.3”. Will Verduzco. Julio 2013. URL: <a href="http://www.xda-developers.com/app-ops-brings-granular-permissions-control-to-android-4-3/">http://www.xda-developers.com/app-ops-brings-granular-permissions-control-to-android-4-3/</a>   URL: <a href="http://www.androidpolice.com/2013/07/25/app-ops-android-4-3s-hidden-app-permission-manager-control-permissions-for-individual-apps/">http://www.androidpolice.com/2013/07/25/app-ops-android-4-3s-hidden-app-permission-manager-control-permissions-for-individual-apps/</a>
[Ref.- 128]	“App Ops Lives On In Android 4.4, Can Now Deny Even More Permissions”. Android Police. November 2013.   URL: <a href="http://www.androidpolice.com/2013/11/25/new-app-app-ops-lives-on-in-android-4-4-can-be-unleashed-with-app-ops-from-color-tiger-and-enhanced-with-root/">http://www.androidpolice.com/2013/11/25/new-app-app-ops-lives-on-in-android-4-4-can-be-unleashed-with-app-ops-from-color-tiger-and-enhanced-with-root/</a>
[Ref.- 129]	“Using WebView - Security Tips”. Google. 2015.   URL: <a href="http://developer.android.com/training/articles/security-tips.html#WebView">http://developer.android.com/training/articles/security-tips.html#WebView</a>
[Ref.- 130]	“Android Version History”. Wikipedia.   URL: <a href="https://en.wikipedia.org/wiki/Android_version_history">https://en.wikipedia.org/wiki/Android_version_history</a>
[Ref.- 131]	“AppOps”. Sylvain Galand.   URL: <a href="https://play.google.com/store/apps/details?id=fr.slvn.appops&amp;hl=en">https://play.google.com/store/apps/details?id=fr.slvn.appops&amp;hl=en</a>   URL: <a href="https://github.com/slvn/android-appops-launcher">https://github.com/slvn/android-appops-launcher</a>
[Ref.- 132]	“Security”. Android.   URL: <a href="https://www.android.com/security-center/">https://www.android.com/security-center/</a>

Referencia	Título, autor y ubicación
[Ref.- 133]	"Security". Android Open Source.   URL: <a href="https://source.android.com/security/index.html">https://source.android.com/security/index.html</a>
[Ref.- 134]	"Revisiting Android disk encryption". Nikolay Elenkov. Octubre 2014.   URL: <a href="http://nelenkov.blogspot.com.es/2014/10/revisiting-android-disk-encryption.html">http://nelenkov.blogspot.com.es/2014/10/revisiting-android-disk-encryption.html</a>
[Ref.- 135]	"DevBytes: Android L Developer Preview". Google Developers. Julio 2014.   URL: <a href="https://www.youtube.com/watch?v=s7JLYYkJuNs#t=90">https://www.youtube.com/watch?v=s7JLYYkJuNs#t=90</a>
[Ref.- 136]	"Sharing what's up our sleeve: Android coming to wearables". Official Android Blog. Julio 2014.   URL: <a href="https://android.googleblog.com/2014/03/sharing-whats-up-our-sleeve-android.html">https://android.googleblog.com/2014/03/sharing-whats-up-our-sleeve-android.html</a>
[Ref.- 137]	"DevBytes: Restricted Profiles in Android 4.3". Google Developers. Julio 2014.   URL: <a href="https://www.youtube.com/watch?v=pdUcANNm72o">https://www.youtube.com/watch?v=pdUcANNm72o</a>
[Ref.- 138]	"CCS Injection Vulnerability". Lepidum. June 2014.   URL: <a href="http://ccsinjection.lepidum.co.jp">http://ccsinjection.lepidum.co.jp</a>   URL: <a href="http://ccsinjection.lepidum.co.jp/blog/2014-06-05/CCS-Injection-en/index.html">http://ccsinjection.lepidum.co.jp/blog/2014-06-05/CCS-Injection-en/index.html</a>
[Ref.- 139]	"Early ChangeCipherSpec Attack". Imperial Violet - Adam Langley. Junio 2014.   URL: <a href="https://www.imperialviolet.org/2014/06/05/earlyccs.html">https://www.imperialviolet.org/2014/06/05/earlyccs.html</a>
[Ref.- 140]	"Security Enhancements in Android x.y". Android Source.   URL: <a href="https://source.android.com/security/enhancements/index.html">https://source.android.com/security/enhancements/index.html</a>   URL: <a href="https://source.android.com/security/enhancements/enhancements41.html">https://source.android.com/security/enhancements/enhancements41.html</a>   URL: <a href="https://source.android.com/security/enhancements/enhancements42.html">https://source.android.com/security/enhancements/enhancements42.html</a>   URL: <a href="https://source.android.com/security/enhancements/enhancements43.html">https://source.android.com/security/enhancements/enhancements43.html</a>   URL: <a href="https://source.android.com/security/enhancements/enhancements44.html">https://source.android.com/security/enhancements/enhancements44.html</a>   URL: <a href="https://source.android.com/security/enhancements/enhancements50.html">https://source.android.com/security/enhancements/enhancements50.html</a>   URL: <a href="https://source.android.com/security/enhancements/enhancements60.html">https://source.android.com/security/enhancements/enhancements60.html</a>
[Ref.- 141]	"Android Hacker's Handbook". Wiley. 2014.
[Ref.- 142]	"Security-Enhanced Linux in Android". Android Source.   URL: <a href="http://source.android.com/devices/tech/security/se-linux.html">http://source.android.com/devices/tech/security/se-linux.html</a>
[Ref.- 143]	Google Cloud Messaging (GCM) for Android. Google.   URL: <a href="http://developer.android.com/google/gcm/index.html">http://developer.android.com/google/gcm/index.html</a>
[Ref.- 144]	"Credential storage enhancements in Android 4.3". Nikolay Elenkov. August 2013.   URL: <a href="http://nelenkov.blogspot.com.es/2013/08/credential-storage-enhancements-android-43.html">http://nelenkov.blogspot.com.es/2013/08/credential-storage-enhancements-android-43.html</a>
[Ref.- 145]	"Android's 5.x Lock Screen may be bypassed by attackers". Martin Brinkmann. Ghacks.net   URL: <a href="https://www.ghacks.net/2015/09/16/androids-5-x-lock-screen-may-be-bypassed-by-attackers/">https://www.ghacks.net/2015/09/16/androids-5-x-lock-screen-may-be-bypassed-by-attackers/</a>
[Ref.- 146]	"Secure USB debugging in Android 4.2.2". Nikolay Elenkov. Febrero 2013.   URL: <a href="http://nelenkov.blogspot.com.es/2013/02/secure-usb-debugging-in-android-422.html">http://nelenkov.blogspot.com.es/2013/02/secure-usb-debugging-in-android-422.html</a>   URL: <a href="http://android-developers.blogspot.jp/2013/02/security-enhancements-in-jelly-bean.html">http://android-developers.blogspot.jp/2013/02/security-enhancements-in-jelly-bean.html</a>
[Ref.- 147]	"Utilizar el identificador de llamada de Google". Google. 2014.   URL: <a href="https://support.google.com/nexus/answer/3459196?hl=es">https://support.google.com/nexus/answer/3459196?hl=es</a>

Referencia	Título, autor y ubicación
[Ref.- 148]	“Android 4.4 - KitKat”. Google.   URL: <a href="http://www.android.com/versions/kit-kat-4-4/">http://www.android.com/versions/kit-kat-4-4/</a>   URL: <a href="https://www.youtube.com/watch?v=sONcojECWxs">https://www.youtube.com/watch?v=sONcojECWxs</a>
[Ref.- 149]	“Administrar la ubicación de tu dispositivo”. Google.   URL: <a href="https://support.google.com/nexus/answer/3467281?hl=es">https://support.google.com/nexus/answer/3467281?hl=es</a>
[Ref.- 150]	Google Play Services. Google.   URL: <a href="https://developer.android.com/google/play-services/index.html">https://developer.android.com/google/play-services/index.html</a>
[Ref.- 151]	“On the WebView addJavascriptInterface Saga”. DroidSec. February 2014.   URL: <a href="http://www.droidsec.org/news/2014/02/26/on-the-webview-addjsif-saga.html">http://www.droidsec.org/news/2014/02/26/on-the-webview-addjsif-saga.html</a>
[Ref.- 152]	“Updating Your Security Provider to Protect Against SSL Exploits”. Android.   URL: <a href="http://developer.android.com/training/articles/security-gms-provider.html">http://developer.android.com/training/articles/security-gms-provider.html</a>
[Ref.- 153]	“Issue 52314: unlock password is limited to 16 characters”. Android Google Code. February 2013.   URL: <a href="https://code.google.com/p/android/issues/detail?id=52314">https://code.google.com/p/android/issues/detail?id=52314</a>
[Ref.- 154]	“Issue 29468: Different passwords for encryption and screen lock”. Android Google Code. April 2012.   URL: <a href="https://code.google.com/p/android/issues/detail?id=29468">https://code.google.com/p/android/issues/detail?id=29468</a>
[Ref.- 155]	“EncPassChanger”. Kibab. December 2012.   URL: <a href="https://github.com/kibab/encpasschanger">https://github.com/kibab/encpasschanger</a>   URL: <a href="https://play.google.com/store/apps/details?id=com.kibab.android.EncPassChanger">https://play.google.com/store/apps/details?id=com.kibab.android.EncPassChanger</a>
[Ref.- 156]	“Cryptfs Password”. Nikolay Elenkov. August 2013.   URL: <a href="https://play.google.com/store/apps/details?id=org.nick.cryptfs.passwdmanager">https://play.google.com/store/apps/details?id=org.nick.cryptfs.passwdmanager</a>   URL: <a href="https://github.com/nelenkov/cryptfs-password-manager">https://github.com/nelenkov/cryptfs-password-manager</a>
[Ref.- 157]	“Changing Android's disk encryption password”. Nikolay Elenkov. August 2012.   URL: <a href="http://nelenkov.blogspot.com/2012/08/changing-androids-disk-encryption.html">http://nelenkov.blogspot.com/2012/08/changing-androids-disk-encryption.html</a>
[Ref.- 158]	“Android encryption switched to scrypt in 4.4.2”. AOSP.   URL: <a href="https://android.googlesource.com/platform/system/vold/+android-4.4_r1/cryptfs.c">https://android.googlesource.com/platform/system/vold/+android-4.4_r1/cryptfs.c</a>   URL: <a href="https://android.googlesource.com/platform/system/vold/+log/android-4.4_r1/cryptfs.c">https://android.googlesource.com/platform/system/vold/+log/android-4.4_r1/cryptfs.c</a> (commit c4c70f1)   URL: <a href="https://android.googlesource.com/platform/system/vold/+c4c70f15bb8845b02f9ec1d624794757badd6933">https://android.googlesource.com/platform/system/vold/+c4c70f15bb8845b02f9ec1d624794757badd6933</a>
[Ref.- 159]	“Android Security Internals”. Nikolay Elenkov. No Starch Press. October 2014.   URL: <a href="http://www.nostarch.com/androidsecurity">http://www.nostarch.com/androidsecurity</a>
[Ref.- 160]	“Android's Permissions System Is Broken and Google Just Made It Worse”. Chris Hoffman. December 2013.   URL: <a href="http://www.howtogeek.com/177904/androids-permissions-system-is-broken-and-google-just-made-it-worse/">http://www.howtogeek.com/177904/androids-permissions-system-is-broken-and-google-just-made-it-worse/</a>
[Ref.- 161]	“Android's App Permissions Were Just Simplified - Now They're Much Less Secure”. Chris Hoffman. June 2014.   URL: <a href="http://www.howtogeek.com/190863/androids-app-permissions-were-just-simplified-now-theyre-much-less-secure/">http://www.howtogeek.com/190863/androids-app-permissions-were-just-simplified-now-theyre-much-less-secure/</a>

Referencia	Título, autor y ubicación
[Ref.- 162]	“Revisar los permisos de aplicaciones en Android 5.1.1 o anteriores “. Google. 2015.   URL: <a href="https://support.google.com/googleplay/answer/6014972?hl=es">https://support.google.com/googleplay/answer/6014972?hl=es</a>
[Ref.- 163]	“Android 5.x Lockscreen Bypass (CVE-2015-3860)”. Austin University of Texas.   <a href="http://sites.utexas.edu/iso/2015/09/15/android-5-lockscreen-bypass/">http://sites.utexas.edu/iso/2015/09/15/android-5-lockscreen-bypass/</a>
[Ref.- 164]	“Añadir aplicaciones, accesos directos y widgets a las pantallas de inicio “. Google.   URL: <a href="https://support.google.com/nexus/answer/2781850?hl=es">https://support.google.com/nexus/answer/2781850?hl=es</a>
[Ref.- 165]	“Storage Access Framework”. Google.   URL: <a href="https://developer.android.com/guide/topics/providers/document-provider.html">https://developer.android.com/guide/topics/providers/document-provider.html</a>   URL: <a href="https://www.youtube.com/watch?v=zxHVeXbk1P4">https://www.youtube.com/watch?v=zxHVeXbk1P4</a>   URL: <a href="https://www.youtube.com/watch?v=UFj9AEz0DHQ">https://www.youtube.com/watch?v=UFj9AEz0DHQ</a>
[Ref.- 166]	“Activar o desactivar SafeSearch”. Google.   URL: <a href="https://support.google.com/websearch/answer/510?hl=es">https://support.google.com/websearch/answer/510?hl=es</a>
[Ref.- 167]	“Ubicación en Ajustes de Google”. Google.   URL: <a href="https://support.google.com/accounts/answer/3118687?hl=es">https://support.google.com/accounts/answer/3118687?hl=es</a>
[Ref.- 168]	“ART (Android RunTime)”. Google.   URL: <a href="http://source.android.com/devices/tech/dalvik/">http://source.android.com/devices/tech/dalvik/</a>
[Ref.- 169]	“Android and Security” (Google Bouncer). Google Mobile Blog. February 2012.   URL: <a href="http://googlemobile.blogspot.com/2012/02/android-and-security.html">http://googlemobile.blogspot.com/2012/02/android-and-security.html</a>
[Ref.- 170]	“Android 4.2 ‘Verify apps’ security feature explained by Google”. Android Authority. November 2012.   URL: <a href="http://www.androidauthority.com/android-4-2-verify-apps-security-feature-explained-by-google-131514/">http://www.androidauthority.com/android-4-2-verify-apps-security-feature-explained-by-google-131514/</a>
[Ref.- 171]	“Expanding Google’s security services for Android”. Android Official Blog. April 2014.   URL: <a href="http://officialandroid.blogspot.com.es/2014/04/expanding-googles-security-services-for.html">http://officialandroid.blogspot.com.es/2014/04/expanding-googles-security-services-for.html</a>
[Ref.- 172]	“Protegerse frente a aplicaciones dañinas”. Google.   URL: <a href="https://support.google.com/accounts/answer/2812853?hl=es">https://support.google.com/accounts/answer/2812853?hl=es</a>   URL: <a href="https://plus.google.com/+MichaelMorrissey/posts/dutcnbu72pv">https://plus.google.com/+MichaelMorrissey/posts/dutcnbu72pv</a>
[Ref.- 173]	“An Evaluation of the Application (“App”) Verification Service in Android 4.2”. Xuxian Jiang. December 2012.   URL: <a href="http://www.cs.ncsu.edu/faculty/jiang/appverify/">http://www.cs.ncsu.edu/faculty/jiang/appverify/</a>
[Ref.- 174]	“Dissecting the Android Bouncer”. Jon Oberheide. 2012.   URL: <a href="https://jon.oberheide.org/files/summercon12-bouncer.pdf">https://jon.oberheide.org/files/summercon12-bouncer.pdf</a>
[Ref.- 175]	“Actividad web y de aplicaciones”. Google.   URL: <a href="https://support.google.com/accounts/answer/54068?hl=es">https://support.google.com/accounts/answer/54068?hl=es</a>
[Ref.- 176]	“Eliminar búsquedas y actividad de navegación”. Google.   URL: <a href="https://support.google.com/accounts/answer/465?hl=es">https://support.google.com/accounts/answer/465?hl=es</a>
[Ref.- 177]	“Crear una copia de seguridad de tus fotos y vídeos automáticamente”. Google.   URL: <a href="https://support.google.com/plus/answer/1647509">https://support.google.com/plus/answer/1647509</a>

Referencia	Título, autor y ubicación
[Ref.- 178]	“Función Reconócame en fotos y vídeos”. Google.   URL: <a href="https://support.google.com/plus/answer/2370300?hl=es">https://support.google.com/plus/answer/2370300?hl=es</a>
[Ref.- 179]	“Ver fotos en las que te hayan etiquetado”. Google.   URL: <a href="https://support.google.com/plus/answer/1254833?hl=es">https://support.google.com/plus/answer/1254833?hl=es</a>
[Ref.- 180]	“Bloquear o desbloquear cuentas de otras personas”. Google.   URL: <a href="https://support.google.com/accounts/answer/6388749?visit_id=1-636343239744150110-383769448&amp;p=block_list&amp;hl=es&amp;rd=1">https://support.google.com/accounts/answer/6388749?visit_id=1-636343239744150110-383769448&amp;p=block_list&amp;hl=es&amp;rd=1</a>
[Ref.- 181]	“New NFC capabilities through Host Card Emulation”. Google.   URL: <a href="http://developer.android.com/about/versions/kitkat.html#44-hce">http://developer.android.com/about/versions/kitkat.html#44-hce</a>
[Ref.- 182]	“Cómo compartir contenido con Android Beam”. Google.   URL: <a href="https://support.google.com/nexus/answer/2781895?hl=es">https://support.google.com/nexus/answer/2781895?hl=es</a>
[Ref.- 183]	“Utilizar la función Tocar y pagar con tu dispositivo”. Google.   URL: <a href="https://support.google.com/nexus/answer/3470787?hl=es">https://support.google.com/nexus/answer/3470787?hl=es</a>
[Ref.- 184]	“Security Tips”. Google. 2015.   URL: <a href="http://developer.android.com/training/articles/security-tips.html">http://developer.android.com/training/articles/security-tips.html</a>
[Ref.- 185]	“Utilizar certificados”. Google.   URL: <a href="https://support.google.com/nexus/answer/2844832?hl=es">https://support.google.com/nexus/answer/2844832?hl=es</a>
[Ref.- 186]	“ID de publicidad”. Google.   URL: <a href="https://support.google.com/googleplay/android-developer/answer/6048248?hl=es">https://support.google.com/googleplay/android-developer/answer/6048248?hl=es</a>
[Ref.- 187]	“Nexus 5 Stock OTA URLs”. XDA Developers.   URL: <a href="http://forum.xda-developers.com/google-nexus-5/general/ref-nexus-5-stock-ota-urls-t2475327">http://forum.xda-developers.com/google-nexus-5/general/ref-nexus-5-stock-ota-urls-t2475327</a>
[Ref.- 188]	“Using the ICS KeyChain API” (4.0, ICS). Nikolay Elenkov. November 2011.   URL: <a href="http://nelenkov.blogspot.com.es/2011/11/using-ics-keychain-api.html">http://nelenkov.blogspot.com.es/2011/11/using-ics-keychain-api.html</a>   “ICS Credential Storage Implementation”. Part 1 &amp; 2. November/December 2011.   URL: <a href="http://nelenkov.blogspot.com.es/2011/11/ics-credential-storage-implementation.html">http://nelenkov.blogspot.com.es/2011/11/ics-credential-storage-implementation.html</a>   URL: <a href="http://nelenkov.blogspot.com.es/2011/12/ics-credential-storage-implementation.html">http://nelenkov.blogspot.com.es/2011/12/ics-credential-storage-implementation.html</a>
[Ref.- 189]	“ICS Trust Store Implementation” (4.0, ICS). Nikolay Elenkov. December 2011.   URL: <a href="http://nelenkov.blogspot.com.es/2011/12/ics-trust-store-implementation.html">http://nelenkov.blogspot.com.es/2011/12/ics-trust-store-implementation.html</a>
[Ref.- 190]	“Certificate blacklisting in Jelly Bean” (4.1, JB). Nikolay Elenkov. July 2012.   URL: <a href="http://nelenkov.blogspot.com.es/2012/07/certificate-blacklisting-in-jelly-bean.html">http://nelenkov.blogspot.com.es/2012/07/certificate-blacklisting-in-jelly-bean.html</a>
[Ref.- 191]	“Jelly Bean hardware-backed credential storage” (4.1, JB). Nikolay Elenkov. July 2012.   URL: <a href="http://nelenkov.blogspot.jp/2012/07/jelly-bean-hardware-backed-credential.html">http://nelenkov.blogspot.jp/2012/07/jelly-bean-hardware-backed-credential.html</a>
[Ref.- 192]	“Questioning the chain of trust: investigations into the root certificates on mobile devices”. Andrew Blach. Bluebox. October 2014.   URL: <a href="https://bluebox.com/blog/technical/questioning-the-chain-of-trust-investigations-into-the-root-certificates-on-mobile-devices/">https://bluebox.com/blog/technical/questioning-the-chain-of-trust-investigations-into-the-root-certificates-on-mobile-devices/</a>
[Ref.- 193]	“Iniciar sesión con tu teléfono en lugar de usar una contraseña”. Google.   URL: <a href="https://support.google.com/accounts/answer/6361026?hl=es">https://support.google.com/accounts/answer/6361026?hl=es</a>

Referencia	Título, autor y ubicación
[Ref.- 194]	"Why Do Wi-Fi Clients Disclose their PNL for Free Still Today?". Raúl Siles. DinoSec. February 2015.   URL: <a href="http://blog.dinosec.com/2015/02/why-do-wi-fi-clients-disclose-their-pnl.html">http://blog.dinosec.com/2015/02/why-do-wi-fi-clients-disclose-their-pnl.html</a>
[Ref.- 195]	"A Systematic Security Evaluation of Android's Multi-User Framework". 2014.   URL: <a href="http://www.cis.syr.edu/~wedu/Research/paper/multi_user_most2014.pdf">http://www.cis.syr.edu/~wedu/Research/paper/multi_user_most2014.pdf</a>
[Ref.- 196]	"Android Internals: A Confectioner's Cookbook". Jonathan Levin. 2015.   URL: <a href="http://newandroidbook.com">http://newandroidbook.com</a>   URL: <a href="http://newandroidbook.com/files/Andevcon-ART.pdf">http://newandroidbook.com/files/Andevcon-ART.pdf</a> ("ART (&amp; OAT) Internals")
[Ref.- 197]	"Android for Work". Android.   URL: <a href="https://www.android.com/work/">https://www.android.com/work/</a>   URL: <a href="https://enterprise.google.com/android">https://enterprise.google.com/android</a>
[Ref.- 198]	"Samsung Android Security Updates". Samsung. October 2015.   URL: <a href="http://security.samsungmobile.com/smrupdate.html">http://security.samsungmobile.com/smrupdate.html</a>
[Ref.- 199]	"Full OTA Images for Nexus and Pixel Devices". Google.   URL: <a href="https://developers.google.com/android/ota">https://developers.google.com/android/ota</a>
[Ref.- 200]	"Application Signing". Android Source.   URL: <a href="https://source.android.com/security/apksigning/">https://source.android.com/security/apksigning/</a>
[Ref.- 201]	"Encontrar un dispositivo Android que has perdido". Google.   <a href="https://support.google.com/accounts/answer/3265955?hl=es">https://support.google.com/accounts/answer/3265955?hl=es</a>
[Ref.- 202]	"Android History". Android.   URL: <a href="https://www.android.com/history/">https://www.android.com/history/</a>
[Ref.- 203]	"Android Security Center". Android.   URL: <a href="https://www.android.com/intl/es_es/security-center/monthly-security-updates/">https://www.android.com/intl/es_es/security-center/monthly-security-updates/</a>
[Ref.- 204]	"Security Updates and Resources". Android.   URL: <a href="https://source.android.com/security/overview/updates-resources">https://source.android.com/security/overview/updates-resources</a>
[Ref.- 205]	"All together now. Introducing G Suite.". Google Cloud Official blog. September 2016.   URL: <a href="https://cloud.googleblog.com/2016/09/all-together-now-introducing-G-Suite.html">https://cloud.googleblog.com/2016/09/all-together-now-introducing-G-Suite.html</a>
[Ref.- 206]	"Dissecting Lollipop's Smart Lock". Nelenkov. December 2014.   URL: <a href="https://nelenkov.blogspot.com.es/2014/12/dissecting-lollipops-smart-lock.html">https://nelenkov.blogspot.com.es/2014/12/dissecting-lollipops-smart-lock.html</a>
[Ref.- 207]	Android Security Bulletin. Google.   URL: <a href="https://source.android.com/security/bulletin/2016-12-01">https://source.android.com/security/bulletin/2016-12-01</a>
[Ref.- 208]	"How many combinations does Android 9 point unlock have?". Quora. February 2011.   URL: <a href="https://www.quora.com/Android-operating-system-How-many-combinations-does-Android-9-point-unlock-have/answer/Yoyo-Zhou">https://www.quora.com/Android-operating-system-How-many-combinations-does-Android-9-point-unlock-have/answer/Yoyo-Zhou</a>   URL: <a href="http://beust.com/weblog2/archives/000497.html">http://beust.com/weblog2/archives/000497.html</a>
[Ref.- 209]	"Password storage in Android M". Nikolay Elenkov. June 2015.   URL: <a href="https://nelenkov.blogspot.com.es/2015/06/password-storage-in-android-m.html">https://nelenkov.blogspot.com.es/2015/06/password-storage-in-android-m.html</a>
[Ref.- 210]	"Añadir aplicaciones, accesos directos y widgets a las pantallas de inicio". Google.   URL: <a href="https://support.google.com/nexus/answer/2781850?hl=es">https://support.google.com/nexus/answer/2781850?hl=es</a>



Referencia	Título, autor y ubicación
[Ref.- 211]	“Administrar invitados y usuarios”. Google.   URL: <a href="https://support.google.com/nexus/answer/2865944?hl=es">https://support.google.com/nexus/answer/2865944?hl=es</a>
[Ref.- 212]	“Utilizar perfiles restringidos en tablets”. Ayuda de Nexus.   URL: <a href="https://support.google.com/nexus/answer/3175031">https://support.google.com/nexus/answer/3175031</a>
[Ref.- 213]	“Configurar la gestión de dispositivos móviles”. Ayuda de G-Suite. Google.   URL: <a href="https://support.google.com/a/answer/6328699?hl=es">https://support.google.com/a/answer/6328699?hl=es</a>
[Ref.- 214]	“The Chromium Projects”.   URL: <a href="https://www.chromium.org/">https://www.chromium.org/</a>
[Ref.- 215]	“Informe de transparencia”. Google.   URL: <a href="https://www.google.com/transparencyreport/safebrowsing/?hl=es-419">https://www.google.com/transparencyreport/safebrowsing/?hl=es-419</a>
[Ref.- 216]	“Administrar advertencias sobre sitios web no seguros”. Google.   URL: <a href="https://support.google.com/chrome/answer/99020?co=GENIE.Platform%3DAndroid">https://support.google.com/chrome/answer/99020?co=GENIE.Platform%3DAndroid</a>
[Ref.- 217]	“Modificar la configuración de contenido de los sitios web”. Google.   URL: <a href="https://support.google.com/chrome/answer/114662?co=GENIE.Platform%3DAndroid&amp;hl=es">https://support.google.com/chrome/answer/114662?co=GENIE.Platform%3DAndroid&amp;hl=es</a>
[Ref.- 218]	“Conectar un sitio web a un dispositivo Bluetooth o USB”. Google.   URL: <a href="https://support.google.com/chrome/answer/6362090">https://support.google.com/chrome/answer/6362090</a>
[Ref.- 219]	“Navegar en privado con el modo incógnito”. Google.   URL: <a href="https://support.google.com/chrome/answer/95464?co=GENIE.Platform%3DAndroid&amp;hl=es">https://support.google.com/chrome/answer/95464?co=GENIE.Platform%3DAndroid&amp;hl=es</a>
[Ref.- 220]	“QUIC, a multiplexed stream transport over UDP”. “The Chromium project”.   URL: <a href="https://www.chromium.org/quic">https://www.chromium.org/quic</a>
[Ref.- 221]	“PdfRenderer”. Android Developers.   URL: <a href="https://developer.android.com/reference/android/graphics/pdf/PdfRenderer.html">https://developer.android.com/reference/android/graphics/pdf/PdfRenderer.html</a>
[Ref.- 222]	“Actualizar las aplicaciones Android”. Ayuda de Google Play.   URL: <a href="https://support.google.com/googleplay/answer/113412?hl=es">https://support.google.com/googleplay/answer/113412?hl=es</a>
[Ref.- 223]	“Advisory: Crashing Android devices with large Assisted-GPS Data Files [CVE-2016-5348]”. Nightwatch Cybersecurity. October 2016.   URL: <a href="https://www.nightwatchcybersecurity.com/2016/10/04/advisory-cve-2016-5348-2/">https://www.nightwatchcybersecurity.com/2016/10/04/advisory-cve-2016-5348-2/</a>
[Ref.- 224]	“USB Host and Accessory”. Android developers.   URL: <a href="https://developer.android.com/guide/topics/connectivity/usb/index.html">https://developer.android.com/guide/topics/connectivity/usb/index.html</a>
[Ref.- 225]	“Android HAX”. Jon Oberheide.   URL: <a href="https://jon.oberheide.org/files/summercon10-androidhax-jonoberheide.pdf">https://jon.oberheide.org/files/summercon10-androidhax-jonoberheide.pdf</a>
[Ref.- 226]	“Android Device Manager has a new name: Find My Device”. Engadget.   URL: <a href="https://www.engadget.com/2017/05/18/google-lost-android-find-my-device/">https://www.engadget.com/2017/05/18/google-lost-android-find-my-device/</a>
[Ref.- 227]	“Descargar zonas y navegar sin conexión”. Google.   URL: <a href="https://support.google.com/maps/answer/6291838?co=GENIE.Platform%3DAndroid&amp;hl=es">https://support.google.com/maps/answer/6291838?co=GENIE.Platform%3DAndroid&amp;hl=es</a>
[Ref.- 228]	“Ver o editar tu cronología”. Google.   URL: <a href="https://support.google.com/maps/answer/6258979?hl=es&amp;ref_topic=3092425&amp;co=GENIE.Platform%3DAndroid&amp;oco=1">https://support.google.com/maps/answer/6258979?hl=es&amp;ref_topic=3092425&amp;co=GENIE.Platform%3DAndroid&amp;oco=1</a>

Referencia	Título, autor y ubicación
[Ref.- 229]	“Ayuda de Google Maps”. Google.   URL: <a href="https://support.google.com/maps#topic=3092425">https://support.google.com/maps#topic=3092425</a>
[Ref.- 230]	“Share your trips and real-time location from Google Maps”. Google blog.   URL: <a href="https://www.blog.google/products/maps/share-your-trips-and-real-time-location-google-maps/">https://www.blog.google/products/maps/share-your-trips-and-real-time-location-google-maps/</a>
[Ref.- 231]	“Compartir tu ubicación en tiempo real con otros usuarios”. Ayuda de Google Maps. URL: <a href="https://support.google.com/maps/answer/7326816?hl=es&amp;ref_topic=3092425&amp;co=GENIE.Platform%3DAndroid&amp;oco=1">https://support.google.com/maps/answer/7326816?hl=es&amp;ref_topic=3092425&amp;co=GENIE.Platform%3DAndroid&amp;oco=1</a>
[Ref.- 232]	“Iniciar sesión en Chrome”. Google.   URL: <a href="https://support.google.com/chrome/answer/185277?co=GENIE.Platform%3DDesktop&amp;hl=es">https://support.google.com/chrome/answer/185277?co=GENIE.Platform%3DDesktop&amp;hl=es</a>
[Ref.- 233]	“Compartir Chrome con otros usuarios o añadir un perfil”. Google.   URL: <a href="https://support.google.com/chrome/answer/2364824?co=GENIE.Platform%3DAndroid&amp;oco=1">https://support.google.com/chrome/answer/2364824?co=GENIE.Platform%3DAndroid&amp;oco=1</a>
[Ref.- 234]	“Protecting hundreds of millions more mobile users”. Google Security Blog.   URL: <a href="https://security.googleblog.com/2015/12/protecting-hundreds-of-millions-more.html">https://security.googleblog.com/2015/12/protecting-hundreds-of-millions-more.html</a>
[Ref.- 235]	“Gestionar la opción Información de los dispositivos”. Google.   URL: <a href="https://support.google.com/accounts/answer/6135999?p=account_device_info&amp;hl=es&amp;authuser=0&amp;visit_id=1-636342504159902489-3147238312&amp;rd=1">https://support.google.com/accounts/answer/6135999?p=account_device_info&amp;hl=es&amp;authuser=0&amp;visit_id=1-636342504159902489-3147238312&amp;rd=1</a>
[Ref.- 236]	“Cómo fijar y dejar de fijar pantallas”. Google.   URL: <a href="https://support.google.com/nexus/answer/6118421?hl=es-419">https://support.google.com/nexus/answer/6118421?hl=es-419</a>
[Ref.- 237]	“Hardware-accelerated disk encryption in Android 5.1”. Nikolay Elenkov. May 2015.   URL: <a href="https://nelenkov.blogspot.com.es/2015/05/hardware-accelerated-disk-encryption-in.html">https://nelenkov.blogspot.com.es/2015/05/hardware-accelerated-disk-encryption-in.html</a>
[Ref.- 238]	“Sincronizar contraseñas en tus dispositivos”. Google.   URL: <a href="https://support.google.com/accounts/answer/6197437?co=GENIE.Platform%3DAndroid">https://support.google.com/accounts/answer/6197437?co=GENIE.Platform%3DAndroid</a>
[Ref.- 239]	“Android Instant Apps”. Google Developer.   URL: <a href="https://developer.android.com/topic/instant-apps/index.html">https://developer.android.com/topic/instant-apps/index.html</a>
[Ref.- 240]	“Presentación de las Instant Apps en Google I/O 2016”. Google.   URL: <a href="https://youtu.be/cosqlfqrpFA">https://youtu.be/cosqlfqrpFA</a>
[Ref.- 241]	“Android Instant Apps: The security jury is out”. NowSecure.   URL: <a href="https://www.nowsecure.com/blog/2016/05/19/android-instant-apps-the-security-jury-is-out/">https://www.nowsecure.com/blog/2016/05/19/android-instant-apps-the-security-jury-is-out/</a>
[Ref.- 242]	“Will Google’s Instant Apps Undermine Enterprise Security?”. Appthority.   URL: <a href="https://www.appthority.com/mobile-threat-center/blog/will-googles-instant-apps-undermine-enterprise-security/">https://www.appthority.com/mobile-threat-center/blog/will-googles-instant-apps-undermine-enterprise-security/</a>
[Ref.- 243]	“Sincronizar contraseñas en tus dispositivos”. Google.   URL: <a href="https://support.google.com/accounts/answer/6197437?co=GENIE.Platform%3DAndroid&amp;oco=1">https://support.google.com/accounts/answer/6197437?co=GENIE.Platform%3DAndroid&amp;oco=1</a>
[Ref.- 244]	“Introducing the Google Identity Platform”. Google developers blog.   URL: <a href="https://developers.googleblog.com/2015/05/introducing-google-identity-platform.html">https://developers.googleblog.com/2015/05/introducing-google-identity-platform.html</a>

Referencia	Título, autor y ubicación
[Ref.- 245]	“Smart Lock for Passwords on Android”. Google developers.  URL: <a href="https://developers.google.com/identity/smartlock-passwords/android/">https://developers.google.com/identity/smartlock-passwords/android/</a>
[Ref.- 246]	“Android One”. Google.  URL: <a href="https://www.android.com/one/">https://www.android.com/one/</a>
[Ref.- 247]	“Taking the next step with Android One”. Google.  URL: <a href="https://www.blog.google/products/android/taking-next-step-android-one/">https://www.blog.google/products/android/taking-next-step-android-one/</a>
[Ref.- 248]	“Cómo administrar tus claves de firma de apps”. Google.  URL: <a href="https://support.google.com/googleplay/android-developer/answer/7384423?hl=es-419">https://support.google.com/googleplay/android-developer/answer/7384423?hl=es-419</a>
[Ref.- 249]	“Security-Enhanced Linux in Android”. Google.  URL: <a href="https://source.android.com/security/selinux/">https://source.android.com/security/selinux/</a>
[Ref.- 250]	“KeyChain”. Android Developers.  URL: <a href="https://developer.android.com/reference/android/security/KeyChain.html">https://developer.android.com/reference/android/security/KeyChain.html</a>
[Ref.- 251]	“Google collects Android users’ locations even when location services are disabled”. Quartz.  URL: <a href="https://qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled/">https://qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled/</a>
[Ref.- 252]	“Google Privacy Policy”. Google.  URL: <a href="https://www.google.com/policies/privacy/">https://www.google.com/policies/privacy/</a>
[Ref.- 253]	“iBeacon”. Apple.  URL: <a href="https://developer.apple.com/ibeacon/">https://developer.apple.com/ibeacon/</a>
[Ref.- 254]	“Platform Overview”. Google Beacon Platform.  URL: <a href="https://developers.google.com/beacons/">https://developers.google.com/beacons/</a>
[Ref.- 255]	“G Pay”. Google.  URL: <a href="https://www.blog.google/topics/shopping-payments/announcing-google-pay/">https://www.blog.google/topics/shopping-payments/announcing-google-pay/</a>
[Ref.- 256]	“Legacy Core Specifications”. Bluetooth SIG.  URL: <a href="https://www.bluetooth.com/specifications/bluetooth-core-specification/legacy-specifications">https://www.bluetooth.com/specifications/bluetooth-core-specification/legacy-specifications</a>
[Ref.- 257]	“Wireshark”. Wireshark.org.  URL: <a href="https://www.wireshark.org/">https://www.wireshark.org/</a>
[Ref.- 258]	“Firebase”. Google.  URL: <a href="https://firebase.google.com/docs">https://firebase.google.com/docs</a>
[Ref.- 259]	“OAuth 2.0”. OAuth.net.  URL: <a href="http://oauth.net/2/">http://oauth.net/2/</a>
[Ref.- 260]	“Instalar Google Authenticator”. Google.  URL: <a href="https://support.google.com/accounts/answer/1066447">https://support.google.com/accounts/answer/1066447</a>
[Ref.- 261]	“Utilizar la llave de seguridad para la verificación en dos pasos”. Google.  URL: <a href="https://support.google.com/accounts/answer/6103523?hl=es">https://support.google.com/accounts/answer/6103523?hl=es</a>
[Ref.- 262]	¿Qué es el centro de pagos de Google?. Google.  URL: <a href="https://support.google.com/payments/answer/7500996">https://support.google.com/payments/answer/7500996</a>

Referencia	Título, autor y ubicación
[Ref.- 263]	"Add Google Sign-In to Your Android App". Google.   URL: <a href="https://developers.google.com/identity/sign-in/android/">https://developers.google.com/identity/sign-in/android/</a>
[Ref.- 264]	"Files that are backed up". Google.   URL: <a href="https://developer.android.com/guide/topics/data/autobackup.html#Files">https://developer.android.com/guide/topics/data/autobackup.html#Files</a>
[Ref.- 265]	"Back Up Key-Value Pairs with Android Backup Service". Google.   URL: <a href="https://developer.android.com/guide/topics/data/keyvaluebackup.html">https://developer.android.com/guide/topics/data/keyvaluebackup.html</a>
[Ref.- 266]	"Inhabilitar el inicio de sesión automático". Google.   URL: <a href="https://support.google.com/accounts/answer/39273?hl=es">https://support.google.com/accounts/answer/39273?hl=es</a>
[Ref.- 267]	"DigiNotar Certificate Authority Breach Crashes e-Government in the Netherlands". IEEE Spectrum.   URL: <a href="https://spectrum.ieee.org/riskfactor/telecom/security/diginotar-certificate-authority-breach-crashes-egovernment-in-the-netherlands">https://spectrum.ieee.org/riskfactor/telecom/security/diginotar-certificate-authority-breach-crashes-egovernment-in-the-netherlands</a>
[Ref.- 268]	"Device Administration". Android Developers.   URL: <a href="https://developer.android.com/guide/topics/admin/device-admin.html">https://developer.android.com/guide/topics/admin/device-admin.html</a>
[Ref.- 269]	"Google Digital Asset Links". Google Developers.   URL: <a href="https://developers.google.com/digital-asset-links/v1/getting-started">https://developers.google.com/digital-asset-links/v1/getting-started</a>
[Ref.- 270]	"The Android Trojan Svpeng now capable of Mobile Phishing". SecureList.   URL: <a href="https://securelist.com/the-android-trojan-svpeng-now-capable-of-mobile-phishing/57301/">https://securelist.com/the-android-trojan-svpeng-now-capable-of-mobile-phishing/57301/</a>   "The evolution of Acecard". SecureList.   URL: <a href="https://securelist.com/the-evolution-of-acecard/73777/">https://securelist.com/the-evolution-of-acecard/73777/</a>
[Ref.- 271]	"The best antivirus software for Android". The Independent IT-Security Institute.   URL: <a href="https://www.av-test.org/en/antivirus/mobile-devices/android/september-2017/?_ga=2.224379036.604887240.1508931778-1860796072.1508931778">https://www.av-test.org/en/antivirus/mobile-devices/android/september-2017/?_ga=2.224379036.604887240.1508931778-1860796072.1508931778</a>
[Ref.- 272]	"android.app.admin overview". Android developers.   URL: <a href="https://developer.android.com/reference/android/app/admin/package-summary.html">https://developer.android.com/reference/android/app/admin/package-summary.html</a>

La siguiente tabla muestra las fuentes de información a las que se hace referencia a lo largo de la presente guía, en concreto las referencias asociadas directamente al CCN-CERT:

Referencia	Título, autor y ubicación
[Ref.- 400]	“Guía CCN-STIC-450: Seguridad de dispositivos móviles”. CCN-CERT. Marzo 2013.   URL: <a href="https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/6-ccn-stic-450-seguridad-en-dispositivos-moviles/file.html">https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/6-ccn-stic-450-seguridad-en-dispositivos-moviles/file.html</a>
[Ref.- 401]	“Guía CCN-STIC-453(A) - Seguridad de dispositivos móviles: Android 2.x”. CCN-CERT. Mayo 2013.   URL: <a href="https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/11-ccn-stic-453-seguridad-en-android/file.html">https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/11-ccn-stic-453-seguridad-en-android/file.html</a>
[Ref.- 402]	“Guía CCN-STIC-453B - Seguridad de dispositivos móviles: Android 4.x”. CCN-CERT. Abril 2015.   URL: <a href="https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/827-ccn-stic-453b-seguridad-en-android-4-x/file.html">https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/827-ccn-stic-453b-seguridad-en-android-4-x/file.html</a>
[Ref.- 403]	“CCN-STIC-457: Gestión de dispositivos móviles: MDM (Mobile Device Management)”. CCN-CERT. Noviembre 2013. URL: <a href="https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/14-ccn-stic-457-herramienta-de-gestion-de-dispositivos-moviles-mdm/file.html">https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/14-ccn-stic-457-herramienta-de-gestion-de-dispositivos-moviles-mdm/file.html</a>
[Ref.- 404]	“Buenas Prácticas. CCN-CERT BP-03/16. Dispositivos móviles”. CCN-CERT. Octubre 2016.   URL: <a href="https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/1757-ccn-cert-bp-03-16-dispositivos-moviles/file.html">https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/1757-ccn-cert-bp-03-16-dispositivos-moviles/file.html</a>
[Ref.- 405]	“Guía CCN-STIC-453C - Seguridad de dispositivos móviles: Android 5.x”. CCN-CERT. Enero 2018.   URL: <i>&lt;enlace correspondiente a la versión previa de la presente guía&gt;</i>

La siguiente tabla muestra las fuentes de información a las que se hace referencia a lo largo de la presente guía relacionadas específicamente con la versión 5.x (Lollipop) de Android:

Referencia	Título, autor y ubicación
[Ref.- 500]	“Android 5.0 Lollipop”. Android.   URL: <a href="https://www.android.com/versions/lollipop-5-0/">https://www.android.com/versions/lollipop-5-0/</a>
[Ref.- 501]	“Android Lollipop”. Android Developers.   URL: <a href="https://developer.android.com/about/versions/lollipop.html">https://developer.android.com/about/versions/lollipop.html</a>
[Ref.- 502]	“Android 5.0 APIs”. Android Developers.   URL: <a href="https://developer.android.com/about/versions/android-5.0.html">https://developer.android.com/about/versions/android-5.0.html</a>
[Ref.- 503]	“Android 5.0 Behavior Changes”. Android Developers.   URL: <a href="https://developer.android.com/about/versions/android-5.0-changes.html">https://developer.android.com/about/versions/android-5.0-changes.html</a>
[Ref.- 504]	“Android 5.1 APIs”. Android Developers.   URL: <a href="https://developer.android.com/about/versions/android-5.1.html">https://developer.android.com/about/versions/android-5.1.html</a>
[Ref.- 505]	“Android in the Workplace and in Education”. Android 5.0 Developers.   URL: <a href="https://developer.android.com/about/versions/android-5.0.html#Enterprise">https://developer.android.com/about/versions/android-5.0.html#Enterprise</a>
[Ref.- 506]	“Android Platform Tools r20”.   URL: <a href="http://dl-ssl.google.com/android/repository/platform-tools_r20-macosx.zip">http://dl-ssl.google.com/android/repository/platform-tools_r20-macosx.zip</a>   URL: <a href="http://dl-ssl.google.com/android/repository/platform-tools_r20-windows.zip">http://dl-ssl.google.com/android/repository/platform-tools_r20-windows.zip</a>   URL: <a href="http://dl-ssl.google.com/android/repository/platform-tools_r20-linux.zip">http://dl-ssl.google.com/android/repository/platform-tools_r20-linux.zip</a>
[Ref.- 507]	“Notifications”. Android Developers - Google.   URL: <a href="https://developer.android.com/guide/topics/ui/notifiers/notifications.html">https://developer.android.com/guide/topics/ui/notifiers/notifications.html</a>

Referencia	Título, autor y ubicación
[Ref.- 508]	“Android developers”. Google.   URL: <a href="https://developer.android.com/about/versions/android-5.0-changes.html#BehaviorNotifications">https://developer.android.com/about/versions/android-5.0-changes.html#BehaviorNotifications</a>
[Ref.- 509]	“Android Official Blog”. Google.   URL: <a href="https://android.googleblog.com/2015/03/android-51-unwrapping-new-lollipop.html">https://android.googleblog.com/2015/03/android-51-unwrapping-new-lollipop.html</a>
[Ref.- 510]	“Memory Leak on Lollipop crashing Apps” - Google issue tracker.   <a href="https://issuetracker.google.com/issues/37010796">https://issuetracker.google.com/issues/37010796</a>
[Ref.- 511]	“UICC Carrier Privileges”. Android Source.   URL: <a href="https://source.android.com/devices/tech/config/uicc">https://source.android.com/devices/tech/config/uicc</a>
[Ref.- 512]	“Verified Boot”. Android.   URL: <a href="https://source.android.com/security/verifiedboot/">https://source.android.com/security/verifiedboot/</a>   URL: <a href="https://source.android.com/security/verifiedboot/verified-boot.html">https://source.android.com/security/verifiedboot/verified-boot.html</a>
[Ref.- 513]	“Reiniciar en modo seguro para detectar aplicaciones con problemas”. Soporte de Google.   URL: <a href="https://support.google.com/nexus/answer/2852139?hl=es">https://support.google.com/nexus/answer/2852139?hl=es</a>
[Ref.- 514]	“Cambio de nombre de Android for Work a Android y de Google Play for Work a Google Play”. Google. URL: <a href="https://support.google.com/work/android/answer/7218437">https://support.google.com/work/android/answer/7218437</a>   URL: <a href="https://blog.google/topics/connected-workspaces/update-android-and-google-plays-progress-enterprise/">https://blog.google/topics/connected-workspaces/update-android-and-google-plays-progress-enterprise/</a>
[Ref.- 515]	“Screen Pinning (Fijación de pantalla)”. Android Developers.   URL: <a href="https://developer.android.com/about/versions/android-5.0.html#ScreenPinning">https://developer.android.com/about/versions/android-5.0.html#ScreenPinning</a>
[Ref.- 516]	“¿Qué es un perfil de trabajo?”. Google.   URL: <a href="https://support.google.com/work/android/answer/6191949">https://support.google.com/work/android/answer/6191949</a>
[Ref.- 517]	“Tricking Android Smart Lock with Bluetooth”. Martin Herfurt. May 2015.   URL: <a href="https://mherfurt.wordpress.com/2015/05/08/tricking-android-smart-lock-with-bluetooth/">https://mherfurt.wordpress.com/2015/05/08/tricking-android-smart-lock-with-bluetooth/</a>   URL: <a href="https://youtu.be/Xb0YG6EpY48">https://youtu.be/Xb0YG6EpY48</a>
[Ref.- 518]	“Set up your device for automatic unlock”. Google. Nexus Help.   URL: <a href="https://support.google.com/nexus/answer/6093922?hl=en">https://support.google.com/nexus/answer/6093922?hl=en</a>
[Ref.- 519]	“Consultar el estado de certificación del dispositivo”. Ayuda de Google Play.   URL: <a href="https://support.google.com/googleplay/answer/7165974?hl=es">https://support.google.com/googleplay/answer/7165974?hl=es</a>

La siguiente tabla muestra las fuentes de información a las que se hace referencia a lo largo de la presente guía relacionadas específicamente con la versión 6.x (Marshmallow) de Android:

Referencia	Título, autor y ubicación
[Ref.- 600]	“Android 6.0 Marshmallow”. Android.   URL: <a href="https://www.android.com/versions/marshmallow-6-0/">https://www.android.com/versions/marshmallow-6-0/</a>
[Ref.- 601]	“Android 6.0 Marshmallow”. Android Developers.   URL: <a href="https://developer.android.com/about/versions/marshmallow/index.html">https://developer.android.com/about/versions/marshmallow/index.html</a>

Referencia	Título, autor y ubicación
[Ref.- 602]	“Android 6.0 Changes”. Android Developers.   URL: <a href="https://developer.android.com/about/versions/marshmallow/android-6.0-changes.html">https://developer.android.com/about/versions/marshmallow/android-6.0-changes.html</a>
[Ref.- 603]	“Android 6.0 APIs”. Android Developers.   URL: <a href="https://developer.android.com/about/versions/marshmallow/android-6.0.html">https://developer.android.com/about/versions/marshmallow/android-6.0.html</a>
[Ref.- 604]	“Handling App Links”. Android Developers.   URL: <a href="https://developer.android.com/training/app-links/index.html">https://developer.android.com/training/app-links/index.html</a>
[Ref.- 605]	“BoringSSL”. Google.   URL: <a href="https://boringssl.googlesource.com/boringssl/">https://boringssl.googlesource.com/boringssl/</a>
[Ref.- 606]	“Android (Marshmallow) Compatibility Definition Document (CDD)” (7.3.10. Fingerprint Sensor). Google. URL: <a href="https://source.android.com/compatibility/6.0/android-6.0-cdd">https://source.android.com/compatibility/6.0/android-6.0-cdd</a>
[Ref.- 607]	“Fingerprint and payments APIs (100 Days of Google Dev)”. Google Developers. May 2015.   URL: <a href="https://www.youtube.com/watch?v=VOn7VrTRIA4">https://www.youtube.com/watch?v=VOn7VrTRIA4</a>
[Ref.- 608]	“Fingerprint security on Nexus devices”. Google Support.   URL: <a href="https://support.google.com/nexus/answer/6300638">https://support.google.com/nexus/answer/6300638</a>
[Ref.- 609]	“Desbloqueo mediante huella dactilar digital”. Google Support.   URL: <a href="https://support.google.com/nexus/answer/6285273">https://support.google.com/nexus/answer/6285273</a>
[Ref.- 610]	“Fingerprint Unlock Security: iOS vs. Google Android (Part I &amp; II)”. Elcomsoft. June 2016.   URL: <a href="http://blog.elcomsoft.com/2016/06/ios-fingerprint-unlock-security/">http://blog.elcomsoft.com/2016/06/ios-fingerprint-unlock-security/</a>   URL: <a href="http://blog.elcomsoft.com/2016/06/fingerprint-unlock-security-ios-vs-google-android-part-ii/">http://blog.elcomsoft.com/2016/06/fingerprint-unlock-security-ios-vs-google-android-part-ii/</a>
[Ref.- 611]	“Fingerprints On Mobile Devices: Abusing and Leaking”. FireEye Labs. BH USA 2015.   URL: <a href="https://www.blackhat.com/docs/us-15/materials/us-15-Zhang-Fingerprints-On-Mobile-Devices-Abusing-And-Leaking-wp.pdf">https://www.blackhat.com/docs/us-15/materials/us-15-Zhang-Fingerprints-On-Mobile-Devices-Abusing-And-Leaking-wp.pdf</a>
[Ref.- 612]	“App Install Location”. Android Developers.   URL: <a href="https://developer.android.com/guide/topics/data/install-location.html">https://developer.android.com/guide/topics/data/install-location.html</a>
[Ref.- 613]	“Apps on SD Card: The Details”. Android Developers Blog. July 2010.   URL: <a href="http://android-developers.blogspot.com/2010/07/apps-on-sd-card-details.html">http://android-developers.blogspot.com/2010/07/apps-on-sd-card-details.html</a>
[Ref.- 614]	“Decrypting Android M adopted storage”. Nikolay Elenkov. Android Explorations. June 2015.   URL: <a href="https://nelenkov.blogspot.com.es/2015/06/decrypting-android-m-adopted-storage.html">https://nelenkov.blogspot.com.es/2015/06/decrypting-android-m-adopted-storage.html</a>
[Ref.- 615]	“Fingerprint HAL”. Android Source.   URL: <a href="https://source.android.com/security/authentication/fingerprint-hal.html">https://source.android.com/security/authentication/fingerprint-hal.html</a>
[Ref.- 616]	“Optimizing for Doze and App Standby”. Android Developers.   URL: <a href="https://developer.android.com/training/monitoring-device-state/doze-standby.html">https://developer.android.com/training/monitoring-device-state/doze-standby.html</a>
[Ref.- 617]	“Requesting Permissions at Run Time”. Android Developers.   URL: <a href="https://developer.android.com/training/permissions/requesting.html">https://developer.android.com/training/permissions/requesting.html</a>
[Ref.- 618]	“Cómo trabajar con permisos del sistema”. Android Developers.   URL: <a href="https://developer.android.com/training/permissions/index.html">https://developer.android.com/training/permissions/index.html</a>   URL: <a href="https://developer.android.com/training/permissions/best-practices.html#testing">https://developer.android.com/training/permissions/best-practices.html#testing</a>



Referencia	Título, autor y ubicación
[Ref.- 619]	“Warning about operating system safety”. Nexus.   URL: <a href="http://g.co/ABH">http://g.co/ABH</a>   URL: <a href="https://support.google.com/nexus/answer/6185381?p=verified_boot">https://support.google.com/nexus/answer/6185381?p=verified_boot</a>
[Ref.- 620]	“Password storage in Android M”. Nikolay Elenkov. Android Explorations. June 2015.   URL: <a href="https://nelenkov.blogspot.com.es/2015/06/password-storage-in-android-m.html">https://nelenkov.blogspot.com.es/2015/06/password-storage-in-android-m.html</a>
[Ref.- 621]	“Hardware-backed Keystore”. Google.   URL: <a href="https://source.android.com/security/keystore/">https://source.android.com/security/keystore/</a>
[Ref.- 622]	“BoringSSL”. Google.   URL: <a href="https://boringssl.googlesource.com/boringssl/">https://boringssl.googlesource.com/boringssl/</a> &amp; <a href="https://github.com/google/boringssl">https://github.com/google/boringssl</a>   URL: <a href="https://www.imperialviolet.org/2015/10/17/boringssl.html">https://www.imperialviolet.org/2015/10/17/boringssl.html</a>   URL: <a href="https://developer.android.com/about/versions/marshmallow/android-6.0-changes.html#boringSSL">https://developer.android.com/about/versions/marshmallow/android-6.0-changes.html#boringSSL</a>
[Ref.- 623]	“Controlar los permisos de una aplicación en Android 6.0 y versiones superiores”. Ayuda de Google Play.   URL: <a href="https://support.google.com/googleplay/answer/6270602">https://support.google.com/googleplay/answer/6270602</a>
[Ref.- 624]	“Cómo activar o desactivar tu feed”. Google.   URL: <a href="https://support.google.com/websearch/answer/2824784?hl=es-419&amp;co=GENIE.Platform=Android">https://support.google.com/websearch/answer/2824784?hl=es-419&amp;co=GENIE.Platform=Android</a>
[Ref.- 625]	“Usar Mi tablón en la aplicación de Google”. Google.   URL: <a href="https://support.google.com/websearch/answer/2819496?hl=es">https://support.google.com/websearch/answer/2819496?hl=es</a>
[Ref.- 626]	“Personalizar el Tablón de la aplicación de Google”. Google.   URL: <a href="https://support.google.com/websearch/answer/6237870?&amp;co=GENIE.Platform%3DAndroid">https://support.google.com/websearch/answer/6237870?&amp;co=GENIE.Platform%3DAndroid</a>
[Ref.- 627]	“Requesting Permissions”. Google developers.   URL: <a href="https://developer.android.com/guide/topics/permissions/requesting.html#normal-dangerous">https://developer.android.com/guide/topics/permissions/requesting.html#normal-dangerous</a>
[Ref.- 628]	“Lock screen notifications”. Android developers.   URL: <a href="https://developer.android.com/guide/topics/ui/notifiers/notifications.html#lockscreenNotification">https://developer.android.com/guide/topics/ui/notifiers/notifications.html#lockscreenNotification</a>
[Ref.- 629]	“Keystore redesign in Android M”. Nelenkov. June 2015.   URL: <a href="https://nelenkov.blogspot.com.es/2015/06/keystore-redesign-in-android-m.html">https://nelenkov.blogspot.com.es/2015/06/keystore-redesign-in-android-m.html</a>
[Ref.- 630]	“Android Keystore System”. Android developers.   URL: <a href="https://developer.android.com/training/articles/keystore.html">https://developer.android.com/training/articles/keystore.html</a>
[Ref.- 631]	GateKeeper. “Android Source”.   URL: <a href="https://source.android.com/security/authentication/gatekeeper">https://source.android.com/security/authentication/gatekeeper</a>
[Ref.- 632]	“Bluetooth Services”. Android Source.   URL: <a href="https://source.android.com/devices/bluetooth/services">https://source.android.com/devices/bluetooth/services</a>
[Ref.- 633]	“Find people, things, &amp; places in your photos”. Google.   URL: <a href="https://support.google.com/photos/answer/6128838">https://support.google.com/photos/answer/6128838</a>

Referencia	Título, autor y ubicación
[Ref.- 634]	“Back Up User Data with Auto Backup”. Android Developers. URL: <a href="https://developer.android.com/guide/topics/data/autobackup.html">https://developer.android.com/guide/topics/data/autobackup.html</a>
[Ref.- 635]	“Auto Backup for Apps made simple”. Android developers blog. URL: <a href="https://android-developers.googleblog.com/2015/07/auto-backup-for-apps-made-simple.html">https://android-developers.googleblog.com/2015/07/auto-backup-for-apps-made-simple.html</a>