centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 453F

Guía práctica de seguridad en dispositivos móviles
Android 8

Marzo 2019

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2019.04.29 13:06:18 +02'00'

© Centro Criptológico Nacional, 2019

NIPO: 083-19-016-8
Fecha de Edición: marzo de 2019
Mónica Salas y Raúl Siles (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, actualizado 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.

Marzo de 2019

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

2. OBJETO

La creciente utilización de dispositivos móviles (incluyendo teléfonos móviles, *smartphones*, *tablets* y agendas electrónicas) destinados a la gestión de información (almacenamiento, intercambio y procesamiento), tanto en el plano profesional como personal, unida al incremento en el número y tipo de amenazas que afectan a estos dispositivos, requiere poner en marcha todos los mecanismos disponibles de cara a su protección.

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 incidentes y amenazas de seguridad [Ref.- 404].

El presente documento realiza un análisis general de los mecanismos y la configuración de seguridad recomendados para el sistema operativo Android 8 de Google, también conocido como "Oreo" y "Android O", disponible tanto para los dispositivos móviles de Google (Pixel, Pixel XL, Pixel 2, Pixel 2 XL, Pixel C, Nexus 5X, Nexus 6P y Nexus Player [Ref.- 1] [Ref.- 2]) como para dispositivos móviles de otros fabricantes.

A fecha de octubre de 2018, la cuota de mercado de Android 8 sobre el total de dispositivos móviles Android era del 21,5% [1].

La presente guía proporciona detalles específicos de aplicación e implementación de las recomendaciones de seguridad y buenas prácticas necesarias para la prevención de los riesgos, amenazas, y vulnerabilidades de seguridad a las que están expuestos los dispositivos móviles basados en Android en la actualidad, y se ha redactado considerando como requisito la necesidad de encontrar un equilibrio entre seguridad y funcionalidad en relación a las capacidades 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.

Adicionalmente, se recomienda la lectura de las guías CCN-CERT 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-453C - Seguridad de dispositivos móviles: Android 5.x [Ref.- 405]
- CCN-STIC-453D - Seguridad de dispositivos móviles: Android 6.x [Ref.- 406]
- CCN-STIC-453E - Seguridad de dispositivos móviles: Android 7.x [Ref.- 407]
- CCN-STIC-454(A) - Seguridad de dispositivos móviles: iPad (iOS 7.x) [Ref.- 409]

[1] En el momento de elaboración y publicación de la presente guía, finales de febrero de 2019, la página oficial de Google de distribución de versiones de Android aún contiene las estadísticas del 26 de octubre de 2018.

- CCN-STIC-455(A) - Seguridad de dispositivos móviles: iPhone (iOS 7.x) [Ref.- 410]
- CCN-STIC-457 - Gestión de dispositivos móviles: MDM (Mobile Device Management) [Ref.- 403]
- CCN-CERT BP-03/16 - Buenas Prácticas. Dispositivos móviles [Ref.- 404]
- CCN-STIC 455C Guía Práctica de Seguridad en Dispositivos Móviles iPhone iOS 11.x [Ref.- 411]
- CCN-STIC 455D Guía Práctica de Seguridad en Dispositivos Móviles iPhone iOS 12.x [Ref.- 412]

En particular, se recomienda la lectura de la guía de seguridad para servicios y aplicaciones de Google, como complemento indispensable para proteger los aspectos relacionados con la cuenta de usuario de Google en dispositivos móviles Android, estrechamente ligada a la funcionalidad de los mismos:

- CCN-STIC-456 - Cuenta de usuario, servicios y aplicaciones de Google para dispositivos móviles Android [Ref.- 408]

3. ANDROID

Android [Ref.- 5] es un sistema operativo de código abierto (*open-source*) basado en Linux, diseñado principalmente para dispositivos móviles con pantalla táctil, que incluye: el *kernel*, los drivers responsables de gestionar el hardware específico, una capa de abstracción hardware (HAL - *Hardware Abstraction Layer*), un conjunto de librerías nativas, el entorno de ejecución (ART - *Android RunTime*), el entorno de librerías de desarrollo para las aplicaciones móviles (*Java API Framework*), y las aplicaciones móviles de sistema y/o las desarrolladas por terceros, disponibles o no por defecto. El mantenimiento de Android se lleva a cabo por parte del denominado "*Android Open Source Project*" (AOSP) [Ref.- 4].

La idea original de desarrollar un sistema operativo para plataformas móviles surgió en 2003, fundándose Android Inc., que fue adquirido por Google en el año 2005. En 2007 surgió la asociación *Open Handset Alliance* (OHA) [Ref.- 3], liderada por Google y formada por un grupo de compañías tecnológicas que se ha ido ampliando a lo largo de los años, y cuyo propósito es el desarrollo de estándares abiertos para dispositivos móviles y servicios basados en la plataforma Android.

Las diferentes versiones de Android han sido conocidas por los términos anglosajones de postres y dulces, de forma que cada nueva versión obtiene su inicial de la letra del alfabeto que sigue al del último término empleado. La versión 1.0 fue denominada "*Apple Pie*", y el primer dispositivo fue comercializado en 2008 por HTC.

Desde la aparición del primer dispositivo comercializado por Google en enero de 2010, el Nexus One, las principales versiones de Android suelen venir acompañadas de nuevos modelos de dispositivos por parte de Google. Con la versión 4.0 de 2011 (*Ice Cream Sandwich*), Android se convirtió en el sistema operativo móvil más utilizado, superando a iOS y a BlackBerry OS, alcanzando cifras de mercado cercanas al 90% en 2018 [Ref.- 6]. En la actualidad, además de en dispositivos móviles de tipo *smartphone*

o tableta, Android se ha incorporado a electrodomésticos, dispositivos IoT (*Internet of Things*), equipos multimedia como Smart TVs, relojes, equipos médicos, vehículos, etc.

A fecha de elaboración de la presente guía, algunos de los recursos oficiales relativos a la seguridad en Android son:

- *Android Security Center* [Ref.- 16] y *Android Security* [Ref.- 20]: información sobre diferentes aspectos y recursos de seguridad de Android, incluyendo la información sobre el proceso recomendado que debe seguirse para la notificación de vulnerabilidades, y los boletines de seguridad en los que se proporciona información sobre los distintos problemas reportados [Ref.- 21].
- *Security for Android developers* [Ref.- 17]: recomendaciones de seguridad para desarrolladores de aplicaciones móviles Android.
- *Android security discussions* [Ref.- 18]: foro público para tratar temas de seguridad asociados al ecosistema Android.
- Dirección de correo para notificar problemas de seguridad al equipo de seguridad oficial de Android [Ref.- 19].

Adicionalmente, existen recursos de seguridad en Android mantenidos por la comunidad. Uno de los principales es el denominado "*Android Vulnerabilities*", un repositorio no oficial mantenido por la Universidad de Cambridge [Ref.- 22].

3.1 PROYECTO TREBLE

Uno de los principales inconvenientes de Android es el modelo de actualizaciones, caracterizado por su escasa eficacia para los dispositivos móviles no comercializados por Google, ya que la publicación de una nueva versión de Android conlleva los siguientes pasos:

1. Publicación del código fuente a través del AOSP [Ref.- 4].
2. Adaptación del código fuente por parte de los fabricantes de chips (Qualcomm, MediaTek, etc.) a sus componentes para que todos los elementos mantengan la compatibilidad con la nueva versión de Android.
3. Revisión del código fuente adaptado en el paso 2 por parte de los fabricantes de dispositivos móviles (OEMs) para actualizar el software específico de sus dispositivos móviles.
4. Fase de pruebas y de integración con los operadores de telefonía móvil para el despliegue de la actualización de Android en los dispositivos que son comercializados por estos, con personalizaciones propias.
5. Publicación de la imagen OTA (ver apartado "5.1. Actualización automática del sistema operativo Android") para que esté disponible para los usuarios finales de forma progresiva.

Este modelo complejo, que requiere que el fabricante adapte la nueva versión de Android a su hardware específico, ha provocado que solo un pequeño porcentaje de los dispositivos móviles dispongan de la última versión, a diferencia de lo que sucede con la plataforma iOS de Apple. Para simplificar este proceso, con Android 8 se anunció

el proyecto *Treble* [Ref.- 7], que independiza la arquitectura del sistema operativo (*frameworks*) de los componentes de bajo nivel (como, por ejemplo, las cámaras), cuya implementación varía según el fabricante y que es, por tanto, específica del dispositivo, de forma que Android pueda actualizarse sin necesidad de que el fabricante modifique su implementación, tal como ilustra la <Figura 1>.

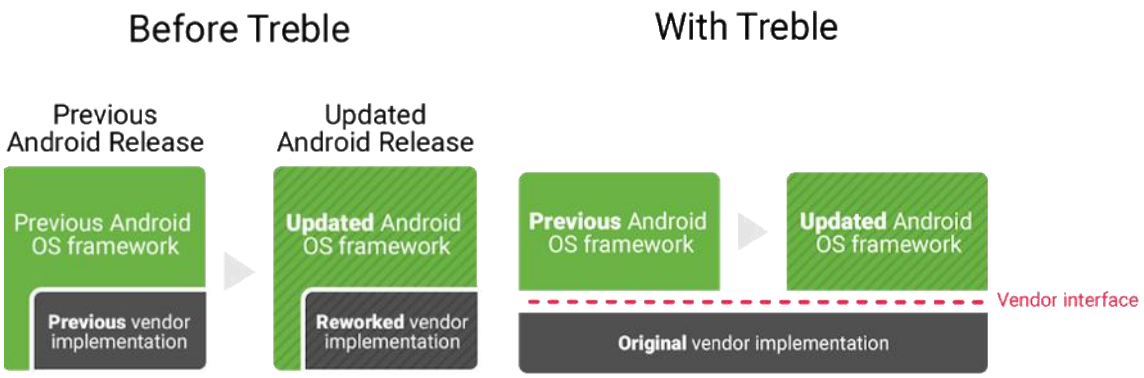

Figura 1 - Framework de Android anterior y posterior al proyecto Treble

Pese a ello, no todos los modelos de dispositivo de los diferentes fabricantes se han sumado al proyecto Treble, únicamente lo han hecho algunos (como, por ejemplo, los incluidos en la [Ref.- 8]).

El rediseño del *framework* de Android asociado al proyecto Treble proporciona un beneficio importante desde el punto de vista de seguridad. En el modelo anterior (imagen izquierda de la <Figura 1>), el diseño del HAL (*Hardware Abstraction Layer*) requería acceso directo por parte de Android a los drivers del kernel sin hacer uso de ningún interfaz estándar. Una actualización de la versión de Android requería que los fabricantes actualizasen sus personalizaciones de los drivers desarrollados para sus componentes hardware. Con la introducción de Treble (imagen derecha de la <Figura 1>), Android añade un interfaz estándar a nivel de HAL, independiente del hardware, de forma que las nuevas actualizaciones de Android puedan seguir haciendo uso de la implementación propietaria ya existente de los drivers del fabricante. Android se comunicará con el hardware a través de los drivers mediante este interfaz común, y cuya utilización no cambia entre una versión y otra de Android.

3.2 ANDROID ONE Y ANDROID GO

Android One [Ref.- 15] es una plataforma que Google anunció en 2014 para abordar la comercialización de dispositivos móviles en mercados emergentes asociados con recursos económicos más bajos, de forma que, en base a acuerdos con determinados fabricantes, se desarrollarían terminales con especificaciones y precio reducidos, pero 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 y drivers, Google liberaría las correspondientes imágenes OTA empleando un modelo similar al empleado para los dispositivos Nexus.

Para asegurar las actualizaciones de versiones de Android, que Google garantiza durante al menos dos años, 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 otros fabricantes, así como incorporar el servicio *Google Play Protect* (GPP) y el asistente de Google (*Google Assistant*). Adicionalmente, los dispositivos Android One reciben también actualizaciones de seguridad mensuales.

Desde el punto de vista de seguridad, a la hora de adquirir un dispositivo móvil, ***se recomienda sopesar la garantía de actualizaciones que ofrece el fabricante***, por lo que la pertenencia al programa Android One es un factor a considerar.

Por su parte, Android Go[2] es una versión de Android adaptada a dispositivos con menos de 1GB de memoria RAM, para los cuales las apps deberán estar diseñadas de forma más ligera y con una versión de Android optimizada para ejecutar en el hardware limitado del que disponen.

3.3 ANDROID 8

Android 8, también conocido como Android Oreo y Android O, suministrado con la API de nivel 26 (Android 8.0) y nivel 27 (Android 8.1), introduce nuevas características y capacidades de cara a los desarrolladores de apps y a los usuarios finales [Ref.- 11] [Ref.- 12]. Las directamente relacionadas con la seguridad y/o privacidad son:

- Mayor granularidad y seguridad en la instalación de apps de orígenes desconocidos (ver apartado "16.2.2. Orígenes desconocidos").
- Se introduce la opción "`Mostrar contraseñas`", que habilita/deshabilita la visualización de los caracteres asociados a una contraseña durante su introducción (ver apartado "10.1. Seguridad del dispositivo").
- La versión 2.0 de "Verified Boot" suministrada con Oreo soporta la protección denominada "*RollBack protection*", que impide al dispositivo arrancar si ha sido instalada una versión más antigua (y potencialmente más vulnerable) que la versión de Android actual (ver apartado "17. Verified Boot").
- El rediseño del framework de Android inherente al proyecto Treble (ver apartado "3.1. Proyecto Treble") conlleva mayor protección de cara a las actualizaciones para el hardware del dispositivo.
- Se elimina el soporte para SSL 3.0.
- El permiso GET_ACCOUNTS deja de ser suficiente para obtener la lista de cuentas de usuario declaradas en el dispositivo (ver apartado "11. Cuentas asociadas al dispositivo móvil"), requiriéndose invocar un método adicional para ganar acceso al interfaz de selección de cuentas.
- Se elimina el soporte para el mecanismo de "*TLS version fallback*", que permitía conectarse a servidores con implementaciones de TLS inválidas [Ref.- 45].

[2] https://www.xatakamovil.com/sistemas-operativos/android-go-una-version-mas-ligera-para-no-dejar-colgados-a-los-telefonos-menos-potentes

- Los componentes de WebView se incorporan como un proceso separado, permitiendo el manejo de contenido inseguro dentro de un *sandbox*.
- Se requiere introducir del código de acceso para habilitar las opciones de desarrollo, aun con la pantalla desbloqueada (ver apartado "15. Opciones para desarrolladores").
- "Wi-Fi Assistant" permite proteger las conexiones realizadas a través de una Wi-Fi abierta mediante una VPN establecida con los servidores de Google (ver apartado "12.2.3. Wi-Fi Assistant").
- Se modifica la implementación de la pila Wi-Fi para aleatorizar la dirección MAC del dispositivo móvil durante los escaneos de redes Wi-Fi.
- Mejora en el manejo de los identificadores del dispositivo[Ref.- 34]:
    - "Android_ID" (Settings.Secure.ANDROID_ID o SSAID): el valor de este atributo varía para cada app y para cada usuario del dispositivo (ver apartado "16. Gestión de apps").
    - "Build.SERIAL": este atributo se deja de soportar para las apps de nivel de API 26 y superior, y se reemplaza por el método Build.getSerial(), que proporcional el número de serie real si la app que lo invoca tiene permiso de acceso al teléfono (ver apartado "16.3. Permisos de las apps").
    - "Net.Hostname": representa el nombre de host del dispositivo en la red (ver apartado "14. Comunicaciones TCP/IP").
- Nuevas capacidades para el perfil AVRCP de Bluetooth, personalizaciones para el diálogo del proceso de emparejamiento y soporte para el estándar Bluetooth Low-Energy (BLE) 5.0.
- Nuevos permisos de telefonía para descolgar una llamada entrante automáticamente mediante el código de una app ("ANSWER_PHONE_CALLS") o para disponer de acceso a los números de teléfono almacenados en el dispositivo móvil ("READ_PHONE_NUMBERS").

Otras características adicionales introducidas por Android 8 (y que tienen una relación indirecta con la seguridad y/o la privacidad) son:

- "Vitals": esta iniciativa persigue mejorar la gestión de la batería del dispositivo móvil mediante los denominados "límites sabios" (*wise limits*), que limitan la actividad que una app puede desarrollar en segundo plano (por ejemplo, peticiones de localización).
- "Notification Dots": para permitir que el usuario se percate de que ha recibido notificaciones por parte de una app aún sin procesar, el icono de dicha app aparecerá en la pantalla principal con un símbolo de punto (ver apartado "8.6. Notificaciones").
- Soporte para PiP (*Picture-in-Picture*): permite al usuario la visualización de un video dentro de la ventana de otra app (por ejemplo, el marco de una vídeo llamada mientras se visualiza el contenido de otra app).

- "Auto-Enable Wi-Fi" activa el interfaz Wi-Fi en base a la localización (ver apartado "12.2. Wi-Fi"), y se suma a las capacidades de Wi-Fi Aware (ver apartado "12.2.1. Wi-Fi Aware") para comunicaciones Wi-Fi con dispositivos cercanos sin un punto de acceso Wi-Fi.
- Accesos directos y widgets en la pantalla principal (ver apartado "8.2. Pantalla de inicio (Home)").
- Autorrelleno de contraseñas: la nueva característica "*autofill*" de Android 8 (Autofill Framework[3]) permite desarrollar servicios que envíen información a un formulario de forma automática, por ejemplo, para su uso en gestores de contraseñas (ver apartado "16.4. Servicio autocompletar").
- Selección de texto: identifica secuencias de texto relacionadas con direcciones, nombres propios, etc., mediante técnicas de *machine learning*, y agrupa toda la secuencia de datos en una misma selección.
- Rediseño de la pantalla de ajustes (ver apartado "9. Configuración del dispositivo").
- Accesibilidad: la barra de navegación incluye un botón "accesibilidad" para el acceso directo a capacidades como el zoom, y se dispone de controles independientes para accesibilidad y para el volumen multimedia.

La versión concreta de Android utilizada en la elaboración de la presente guía es la 8.1.0, concretamente la publicada en diciembre de 2018[4].

En la [Ref.- 41] se pueden encontrar otras características de Android 8 más generales.

4. DISPOSITIVO MÓVIL UTILIZADO

El dispositivo móvil empleado en la elaboración de la presente guía es el Google Nexus 5x, desarrollado conjuntamente por Google y LG y comercializado en 2015 con Android 6.0 (Marshmallow). Incorpora lector de huellas y un conector USB-C, que soporta USB On-the-Go (OTG). El Nexus 5x recibió la actualización de Android 8.0 en agosto de 2017, y no se garantizan actualizaciones de seguridad para este modelo a partir de noviembre de 2018 [Ref.- 9], aunque sí recibió la de diciembre de 2018.

La mayor parte de las recomendaciones de seguridad proporcionadas son aplicables al resto de dispositivos móviles que soportan la versión 8 de Android, pero puede que algunas no sean de aplicación directa en modelos que no dispongan de los componentes hardware implicados, especialmente en dispositivos de otros fabricantes.

Salvo para los apartados en que se indique lo contrario, los aspectos de configuración descritos a lo largo de la presente guía corresponden a un dispositivo en el que no se ha dado de alta una cuenta de usuario de Google. Dado que la existencia de una cuenta de usuario de Google activa en el dispositivo es requisito indispensable

[3] https://developer.android.com/guide/topics/text/autofill

[4] https://dl.google.com/dl/android/aosp/bullhead-opm7.181205.001-factory-5f189d84.zip

para poder utilizar los servicios de la "Play Store" y actualizar las apps, la versión de todas las apps corresponde a la proporcionada con la imagen de sistema operativo existente por defecto en el dispositivo móvil.

5. ACTUALIZACIÓN DEL SISTEMA OPERATIVO ANDROID

La versión de Android que ejecuta en un dispositivo está disponible a través de "`Ajustes - [Sistema] - Información del teléfono - Versión de Android`". La versión del nivel de seguridad se proporciona en "`Ajustes - [Sistema] - Información del teléfono - Nivel de parche de seguridad de Android`".

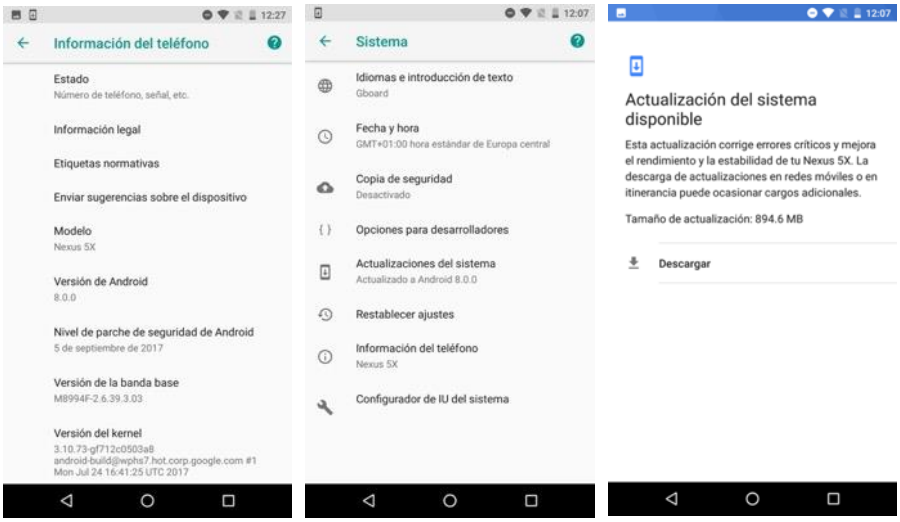

Figura 2 - Comprobación de la versión de Android y de la disponibilidad de actualizaciones

Para comprobar si existen actualizaciones de sistema operativo, se debe seleccionar la opción "`Ajustes - [Sistema] - Actualizaciones del sistema`".

Alternativamente, desde el teclado del teléfono en Android se puede forzar una búsqueda inmediata de actualizaciones y parches mediante el código USSD "`*#*#checkin#*#*`" (o "`*#*#2432546#*#*`"). La notificación "`checkin succeeded`" informará del éxito al realizar la comprobación de actualizaciones.

Figura 3 - Comprobación de actualizaciones mediante marcación de un código USSD

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 proporcionarse por cada fabricante y/o por los operadores de telefonía móvil, en base a las modificaciones y ajustes realizados sobre el proyecto AOSP para el dispositivo en cuestión por cada uno de ellos. Google únicamente proporciona actualizaciones para los dispositivos Nexus y Pixel. No existe ningún modelo estandarizado definido para la distribución de las actualizaciones de seguridad de Android, ni ninguna periodicidad definida para su implementación por los fabricantes (pese a su publicación periódica cada mes por parte de Google), salvo para los dispositivos Google Nexus y/o Pixel, por lo que cada fabricante (miembro o no de la

Open Handset Alliance) puede seguir procedimientos de actualización diferentes. Google no se compromete a actualizar indefinidamente con los parches de seguridad mensuales todas y cada una de las versiones de Android que han estado disponibles para un dispositivo móvil concreto, sino que actualizará mensualmente únicamente la última versión de Android disponible para los dispositivos Nexus y Pixel aún cubiertos por el periodo soporte de Google.

En 2018 Google ha comenzado a establecer requisitos más estrictos sobre los fabricantes de dispositivos móviles. Concretamente, estableciendo en los contratos que firman entre ambas partes que el fabricante se compromete (contractualmente) a ofrecer actualizaciones durante al menos 2 años para dispositivos "populares"[5], especificando adicionalmente que deben proporcionar al menos 4 actualizaciones de seguridad al año, es decir, trimestralmente (como mínimo). El concepto de dispositivo móvil "popular" parece que aplica a cualquier dispositivo comercializado a partir del 31 de enero de 2018 y que haya sido activado por más de 100.000 usuarios.

Una vez que se libera una nueva actualización para un modelo de dispositivo concreto, el usuario puede proceder a realizar una instalación:

- Automática: el dispositivo, en base a su configuración y a los mecanismos internos del sistema, identifica la disponibilidad de la actualización y procede a su instalación automática (con o sin intervención del usuario), a través de un mecanismo OTA (*Over-the-Air*)[6]. Android no soporta actualizaciones automáticas completas del dispositivo, sino únicamente parciales.
- Manual: descargando la imagen correspondiente al dispositivo publicada por Google [Ref.- 10] y siguiendo las instrucciones de instalación.

Las actualizaciones pueden ir encaminadas a llevar al dispositivo a:

- Una nueva versión "*major*" (por ejemplo, de la versión 7.1.2 a la 8.0.0).
- Una nueva versión "*minor*" (por ejemplo, de la versión 8.0.0 a la 8.1.0).
- Un *bundle* de parches de seguridad sobre una versión concreta (por ejemplo, la aplicación de los parches de seguridad para Android 8.1.0 de diciembre de 2018 sobre un dispositivo que ejecuta Android 8.1.0 con el nivel de parches de seguridad de octubre de 2018). Google publica mensualmente el boletín con las vulnerabilidades de seguridad corregidas en el nivel de parches correspondiente [Ref.- 14], que se suministra como actualización OTA.

Se distinguen dos tipos de paquete de actualización:

- Completa: el paquete de instalación incluye todos los componentes y contenidos propios de la versión de Android a la que pertenece. Google mantiene y publica dos tipos de imágenes, que el usuario puede descargar y aplicar:

[5] https://www.theverge.com/2018/10/24/18019356/android-security-update-mandate-google-contract

[6] El concepto de "actualización OTA" alude al proceso de servir, a través de una conexión inalámbrica (Wi-Fi o móvil, 2/3/4G), una actualización de software o firmware a un dispositivo móvil capacitado para recibirla sin procedimientos complejos, y no es propietario de Google.

- *Factory image* [Ref.- 10]: contiene todos los binarios para dejar el dispositivo móvil en la versión asociada a la imagen en cuestión. Al aplicarla, el dispositivo pierde su configuración y los datos de usuario, regresando al estado correspondiente a la versión de fábrica.
- *Full OTA image* [Ref.- 23]: contiene todos los paquetes de actualización para una versión concreta compatible con la existente en el dispositivo móvil. El dispositivo mantendrá la configuración actual tras la actualización.

- Parcial: solo incluye los cambios que se deben aplicar sobre una versión concreta para pasar a la versión objetivo. Google no libera públicamente las actualizaciones parciales para su instalación manual por parte del usuario, este proceso se lleva a cabo a través de paquetes OTA que el dispositivo descarga directamente de los servidores de Google.

En cualquier caso, antes de proceder a la actualización del dispositivo móvil, ***se recomienda realizar una copia de seguridad del mismo*** (ver apartado "21. Copias de seguridad y restauración").

El dispositivo debe cumplir los requisitos que permitan la aplicación de la actualización (por ejemplo, disponer de un mínimo porcentaje de batería, que no haya incompatibilidad con la actividad que en ese momento se esté llevando a cabo, etc.).

Desde el punto de vista de seguridad, ***se recomienda mantener el dispositivo actualizado a una versión reciente, y, específicamente, aplicar los parches de seguridad publicados para el dispositivo a la mayor brevedad posible***. En ningún caso se recomienda la instalación del sistema operativo desde una fuente no oficial.

5.1 ACTUALIZACIÓN AUTOMÁTICA DEL SISTEMA OPERATIVO ANDROID

Los dispositivos móviles Android con conectividad de datos hacia Internet pueden verificar automáticamente si existe una nueva versión o actualización parcial del sistema operativo, que se realizará mediante mecanismos OTA. La implementación OTA de Google se basa en un elemento cliente que reside en el sistema como parte del AOSP (y que, por tanto, está disponible para el resto de fabricantes) y otro elemento, también cliente, que puede variar según el fabricante (en el caso de Google, este elemento está integrado en la app Google Play Services, o GPS).

La actualización automática vía OTA de Android no requiere que el dispositivo tenga dada de alta una cuenta de usuario de Google, a diferencia de lo que sucede en la actualización de apps mediante Google Play (ver apartado "16. Gestión de apps").

En el caso del dispositivo móvil empleado en la presente guía, se parte de la versión 7.1.2 de Android, para la cual se liberó como imagen OTA la actualización correspondiente a la versión 8.0.0. Si se desea actualizar un dispositivo a una versión de Android 8 diferente a la que Google ofrece para el dispositivo en un momento concreto, se puede descargar la imagen OTA[7] completa de la versión deseada de la

[7] Un paquete OTA se denomina *payload*.

web oficial de Google [Ref.- 23] y realizar una actualización manual completa (ver apartado "5.2. Actualización manual del sistema operativo Android").

El modelo de actualizaciones depende sustancialmente de si el dispositivo soporta las denominadas "A/B *seamless updates*" (ver apartado "5.1.1. A/B seamless updates"). Cuando el dispositivo móvil detecta una nueva versión disponible para él, mostrará una notificación, que, al seleccionarse, permitirá iniciar la descarga del *payload*, y, una vez completada, proceder a su instalación.

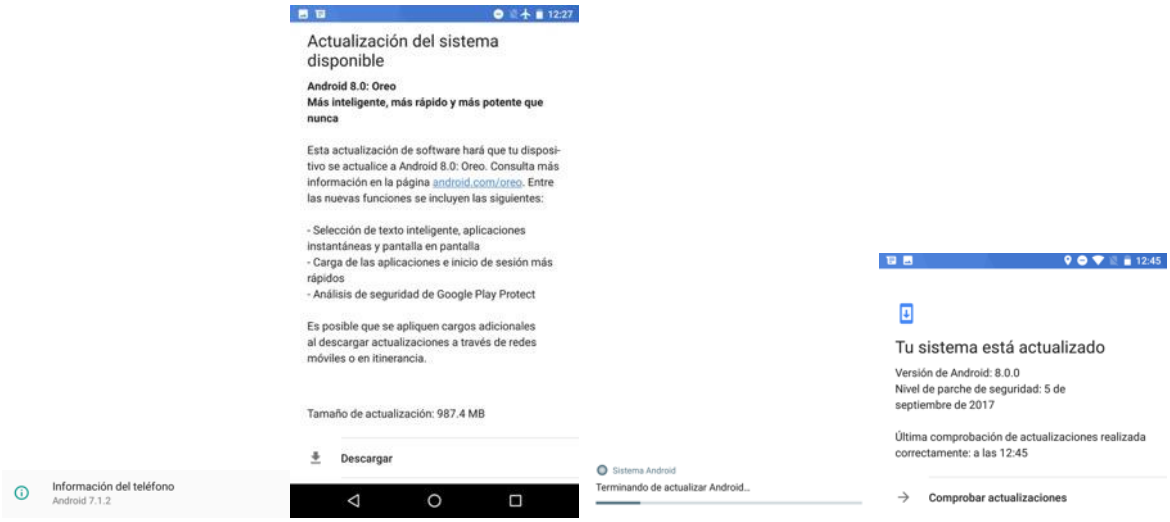

Figura 4 - Instalación automática de una actualización de Android de tipo OTA

El fichero de actualización contiene metadatos (incluyendo una lista de acciones para verificar que la nueva versión es de aplicación en el dispositivo objetivo), y los propios contenidos y binarios que forman parte de la actualización del sistema. Tras la correcta instalación del *payload* y tras el arranque, se comprueba la integridad del sistema a través de *update_verifier*.

Android 7 introdujo una opción que habilita las descargas automáticas de actualizaciones dentro de las opciones para desarrolladores denominada "`Actualizaciones del sistema automáticas`" (disponible en el menú "`Ajustes - [Sistema] Opciones para desarrolladores`", ver apartado "15. Opciones para desarrolladores"). Con esta opción (activa por defecto en los dispositivos Nexus 5x comercializados de fábrica con Android 7), el dispositivo móvil recibe de los servidores de Google (mediante un procedimiento de tipo "*push*") las nuevas versiones de OTA disponibles, y procederá a su descarga e instalación sin solicitar confirmación al usuario siempre que se cumpla la condición de estar conectado a una red Wi-Fi y que cuente al menos con un 50% de batería. Esta opción no aplica a actualizaciones hacia versiones "*major*"[8] de Android.

Pese a que ***se recomienda*** encarecidamente ***mantener el dispositivo móvil Android en la versión más reciente*** (tanto a nivel de versión consolidada o principal, como de nivel de parches de seguridad publicados para una versión de Android

[8] Las versiones "*major*" son las correspondientes a una versión principal.

concreta), en determinados escenarios puede resultar conveniente desactivar la opción "`Actualizaciones del sistema automáticas`" y proceder a la instalación de la última versión de parches de seguridad tras haber analizado su contenido, atestiguado su estabilidad, y determinado si alguna nueva opción o cambio que se haya incorporado puede provocar comportamientos no deseados en el dispositivo móvil.

La política de actualizaciones de Google persigue que sus terminales dispongan de la última versión de Android principal que haya sido liberada para ellos, por lo que, una vez se detecta que existe una versión mayor de Android disponible para un modelo de dispositivo, los parches de seguridad correspondientes a la versión actual no se aplicarán, siendo necesario instalarlos manualmente siguiendo el procedimiento descrito en el apartado "5.2. Actualización manual del sistema operativo Android".

5.1.1 A/B SEAMLESS UPDATES

Android 7 (Nougat) introdujo como una de sus principales novedades un esquema de actualizaciones de sistema operativo que recibe el nombre de "A/B *(Seamless) System Updates*" (o actualizaciones sin interrupciones), de aplicación únicamente para los modelos de dispositivo móvil comercializados con posterioridad a la publicación de Android 7.0 (en agosto de 2016) y que trajesen esta versión preinstalada de fábrica.

El primer dispositivo fabricado por Google que soportó las actualizaciones sin interrupciones fue el Pixel (y Pixel XL), pero ningún Nexus 5x (modelo empleado en la elaboración de la presente guía) lo soporta, al no disponer de doble particionado.

Este esquema de actualizaciones de sistema asegura que el dispositivo dispone de una versión de Android estable en disco durante una actualización OTA, y se asienta sobre un conjunto de particiones lógicas (denominadas *slots*) dual; un *slot* será el activo (*online*), y el otro estará en segundo plano (*offline*). Cada *slot* está integrado a su vez por el conjunto de particiones lógicas necesarias para el correcto funcionamiento del sistema: arranque (*boot_x*), sistema (*system_x*) y una específica para el fabricante (*vendor_x*). Un *slot* se denomina "`a`" y el otro "`b`" (por ejemplo, `boot_a/boot_b`), de ahí la termología "A/B *seamless updates*". Los dispositivos que no soportan este esquema A/B solo disponen de una instancia de cada partición.

La instalación de una actualización se realiza sobre la partición inactiva, en la que se copian todos los ficheros correspondientes a la nueva versión de Android. Si la instalación finaliza con éxito, la partición inactiva se marcará como "arrancable" (*bootable*). Tras reiniciarse el dispositivo, el gestor de arranque (*bootloader*) iniciará el sistema operativo desde la nueva versión de Android, marcando esa partición como activa si el arranque tiene éxito (<Figura 5>).

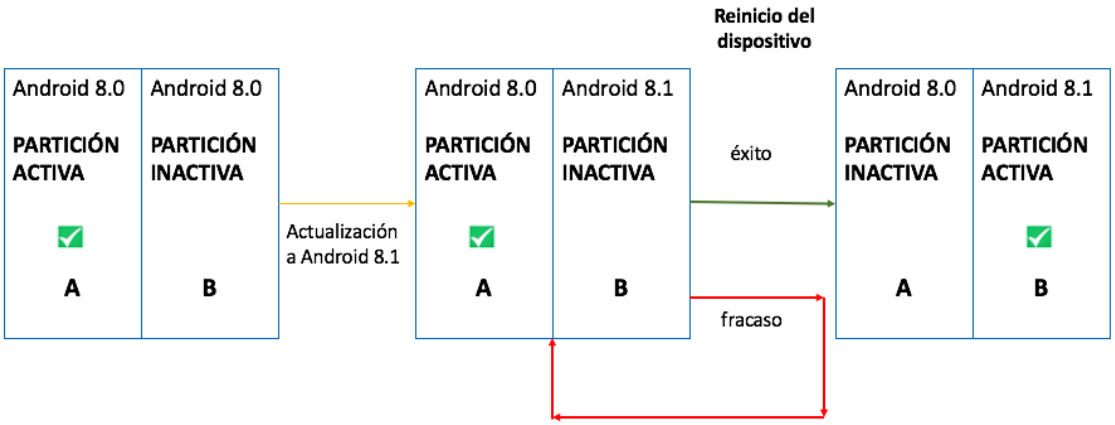

Figura 5 - Esquema de actualización "A/B seamless updates"

NOTA: por simplicidad, se omite la descripción completa de la arquitectura "*A/B seamless updates*". Si se desea profundizar en ella, se recomienda la lectura del apartado "6.5. A/B (Seamless) System Updates" de la "Guía CCN-STIC-453E – Seguridad de dispositivos móviles: Android 7.x" [Ref.- 407].

El proceso de actualizaciones "*seamless*" protege al dispositivo móvil frente a ciertas amenazas y *exploits*, ya que la partición activa de sistema se puede montar en modo de solo lectura (*read-only*), al no requerir el proceso de actualización escribir sobre ella.

Cada bloque de almacenamiento físico de la partición de sistema se firmará para garantizar su integridad, tal como se describe en el apartado "17. Verified Boot".

La descarga e instalación de una nueva versión se presenta al usuario a través de una notificación. La selección de la misma ofrece los detalles de la actualización[9].

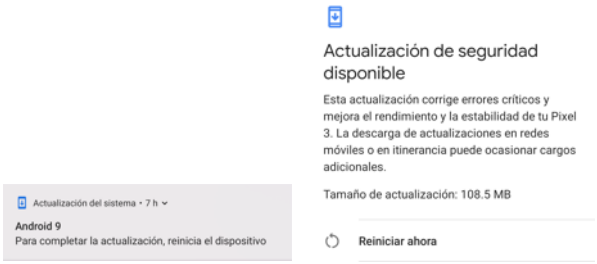

Figura 6 - Notificación de disponibilidad de una nueva versión de Android

IMPORTANTE: se ha comprobado que, si el dispositivo se resetea a fábrica tras haberse completado un proceso de actualización A/B sobre la partición inactiva, el proceso de reseteo a fábrica del terminal, tras el reinicio, arrancará de la partición actualizada (si es correcta), por lo que se habrá actualizado a la nueva versión, sin que el usuario disponga de posibilidad de evitarlo.

Adicionalmente, la opción "*Android rollback protection*" (ver apartado "17. Verified Boot") impedirá realizar una instalación manual (ver apartado "5.2. Actualización manual del

[9] Las imágenes mostradas en la <Figura 6> corresponden a un dispositivo Pixel 3, ya que, como se ha indicado, el modelo Nexus 5x no dispone de esquema de particiones dual.

sistema operativo Android") de una versión anterior de Android, por lo que, para usuarios avanzados, se recomienda mantener desactivada la opción "Actualizaciones del sistema automáticas" (disponible en el menú "Ajustes - [Sistema] Opciones de desarrollo", ver apartado "15. Opciones para desarrolladores"), y proceder a la comprobación de la estabilidad de la actualización antes de proceder a aplicarla.

Si la actualización OTA fracasa, bien durante el proceso de *flash*, bien tras el arranque que sigue a la aplicación de la actualización, el dispositivo todavía podrá arrancar de la partición no actualizada. Esto permite además reducir el tamaño de la partición de caché, que no albergará en ningún momento la actualización en los dispositivos con soporte para actualizaciones A/B.

A fecha de elaboración de la presente guía, la opción para desarrolladores "Actualizaciones del sistema automáticas" (ver apartado "15. Opciones para desarrolladores") no impide que el dispositivo se descargue la actualización de una nueva versión. Sin embargo, si está desactivada, se conseguirá que la partición de arranque siga siendo la que tiene la versión sin actualizar.

Desde el punto de vista de seguridad, ***a la hora de elegir un dispositivo móvil, se recomienda seleccionar uno que disponga de soporte para "A/B seamless updates"***, puesto que proporciona al dispositivo mayor protección frente a ataques que afecten a la partición de sistema y un proceso de actualización más fluido y sencillo para el usuario.

Los siguientes comandos "adb" permiten comprobar si un dispositivo soporta el esquema "A/B" y la partición activa:

```
$ getprop ro.build.ab_update
true
$ getprop ro.boot.slot_suffix
b
```

Figura 7 - Comandos "adb" para comprobar el esquema "A/B seamless updates"

5.2 ACTUALIZACIÓN MANUAL DEL SISTEMA OPERATIVO ANDROID

Es posible actualizar el sistema operativo Android mediante la descarga de los ficheros de actualización oficiales desde los recursos ofrecidos por el correspondiente fabricante. En condiciones normales, la actualización manual no es requerida, y debe llevarse a cabo con extrema precaución, pero es la única opción posible para ciertos fabricantes u operadores de telefonía móvil, que no proporcionan actualizaciones automáticas. Google proporciona tanto imágenes OTA de fábrica completas [Ref.- 23] como imágenes de fábrica [Ref.- 10] para los dispositivos móviles de la familia Google Nexus y/o Pixel, que se liberan mensualmente para asegurar que se dispone de imágenes con los últimos parches de seguridad [Ref.- 9].

La actualización manual requiere de conexión mediante USB entre el dispositivo móvil y un ordenador, en el que previamente se habrá descargado la imagen objetivo.

Se recomienda realizar una copia de seguridad antes de llevar a cabo cualquier proceso de actualización.

El nombre del fichero ZIP o formato correspondiente a los ficheros con las imágenes de fábrica de Ggoogle sigue el patrón descrito a continuación. Desde el punto de vista de seguridad, ***conviene comprobar el hash SHA256 del fichero descargado antes de proceder a su instalación*** para verificar que no ha sido manipulado.

- Imágenes de fábrica (*Factory images*): nombre clave del tipo de dispositivo móvil + número de compilación + "factory" + 8 primeros caracteres hexadecimales del hash SHA256 del fichero ".zip" o ".tgz".
- Imágenes OTA completas (*Full OTA images*): nombre clave del tipo de dispositivo móvil + "ota" + número de compilación + 8 primeros caracteres hexadecimales del hash SHA256 del fichero ".zip" o ".tgz".

5.2.1 INSTALACIÓN DE UNA IMAGEN OTA COMPLETA

Este proceso permite actualizar un dispositivo móvil Android conservando los datos de usuario mediante la aplicación de una "*full OTA image*". Google recomienda este tipo de actualización frente a la basada en una imagen de fábrica. Las "*full OTA images*" contienen todos los paquetes de la versión objetivo completa de Android.

IMPORTANTE: estas imágenes OTA no son equivalentes a las imágenes parciales que el dispositivo se descarga *Over-the-Air* durante una actualización automática (descrita en el apartado "5.1. Actualización automática del sistema operativo Android"), ya que estas últimas tienen en cuenta tanto la versión de Android de partida como la objetivo, y solo actualizan los componentes que han cambiado entre ambas.

La actualización de una imagen OTA completa se realiza a través del protocolo ADB (*Android Debug Bridge*) mediante el comando "`adb`", que permite acceso vía USB al dispositivo móvil como desarrollador. Por tanto, se precisa, además:

- Habilitar la opción "`Depuración por USB`" en el dispositivo móvil.
- Haber establecido una relación de confianza entre el citado ordenador (ver apartado "15.2. Opciones para desarrolladores – Depuración") y el dispositivo.

Para aplicar una imagen OTA completa, se requiere:

1. Arrancar el dispositivo móvil en modo "*Recovery*" y entrar en su menú de opciones, según se ilustra en el apartado "25. anexo b: índice de figuras
2. Figura 1 – Framework de Android anterior y posterior al proyecto Treble 11

3. Anexo c: Modos de arranque del dispositivo móvil".
4. Seleccionar la opción "`Apply update from ADB`".
5. Desde el ordenador en el que reside la imagen, ejecutar el commando "`adb sideload <fichero_ota.zip>`".

```
C:\Android\> adb sideload bullhead-ota-opm6.171019.030.k1-118c2b3a.zip
opening bullhead-ota-opm6.171019.030.k1-118c2b3a.zip'...
connecting...
serving: '8 bullhead-ota-opm6.171019.030.k1-118c2b3a.zip'  (~3%)
Total xfer: 2.00x
```

Figura 8 - Instalación de una imagen OTA completa en un dispositivo Nexus 5x

6. Cuando la instalación concluya mostrando el mensaje "*Install from ADB complete*", seleccionar la opción "`Reboot system now`" en el menú de recuperación del dispositivo móvil.
7. ***Se recomienda deshabilitar el modo*** "`Depuración por USB`" ***una vez concluido el proceso de actualización***.
8. Tras el reinicio del dispositivo móvil, realizar el proceso de configuración inicial de la nueva versión (ver apartado "6. Configuración inicial del sistema operativo Android").

En el caso mostrado durante el presente apartado, se aplicó la imagen de fábrica correspondiente a la versión 8.1.0 con parches de seguridad de diciembre de 2018:

Figura 9 - Resultado de aplicar una imagen OTA completa

5.2.2 INSTALACIÓN DE UNA IMAGEN DE FÁBRICA ("FACTORY IMAGE")

El proceso de actualización/instalación manual de Android mediante una imagen de *firmware* completa de fábrica (*factory image*) requiere que el gestor de arranque esté desbloqueado. Este proceso de carga eliminará todos los datos de usuario del terminal, a diferencia de lo que sucede con la actualización partiendo de una imagen OTA completa (ver apartado anterior). Los pasos a seguir son:

1. Descomprimir en el ordenador el fichero correspondiente a la imagen de fábrica.
2. Arrancar el dispositivo móvil desde el gestor de arranque (modo *bootloader*) según se describe en el apartado "5.2.3. Desbloqueo/bloqueo del bootloader". Si el *bootloader* no estuviese desbloqueado, proceder a desbloquearlo.
3. Invocar el script "`flash-all`" desde el directorio del ordenador en el que se encuentra la imagen descomprimida.
4. Una vez finalizado el proceso, ***se recomienda bloquear de nuevo el bootloader*** (ver apartado "5.2.3. Desbloqueo/bloqueo del bootloader").
5. Tras reiniciar el dispositivo, realizar el proceso de configuración inicial de la nueva versión (ver apartado "6. Configuración inicial del sistema operativo Android").
6. La <Figura 10> representa la aplicación de la imagen de fábrica correspondiente a la versión 8.1.0, que incluye los parches de seguridad de septiembre de 2018:

```
C:\./flash-all.bat
< waiting for any device >
target reported max download size of 536870912 bytes
sending 'bootloader' (4620 KB)...
OKAY [ 0.184s]
writing 'bootloader'...
…
Created filesystem with 11/6144 inodes and 1422/24576
blocks
-------------------------------------------
Bootloader Version...: BHZ31b
Baseband Version.....: M8994F-2.6.41.5.01
Serial Number........: 0257a9231868440f
-------------------------------------------
…
OKAY [  0.213s]
writing 'cache'...
OKAY [  0.077s]
rebooting...
finished. total time: 87.542s
Press any key to exit...
```

Figura 10 - Resultado de aplicar una imagen de fábrica (factory image)

5.2.3 DESBLOQUEO/BLOQUEO DEL BOOTLOADER

IMPORTANTE: los pasos descritos en este apartado pueden no estar soportados por todos los fabricantes o modelos de dispositivos móviles, por lo que su ejecución debe llevarse a cabo únicamente por usuarios avanzados y experimentados.

El gestor de arranque (*bootloader*) viene bloqueado de fábrica por defecto por seguridad, lo cual impide que se pueda escribir sobre las particiones de sistema. El estado del *bootloader* se puede verificar arrancando el dispositivo desde el gestor de arranque (o modo *bootloader*), detallado a continuación, mediante la entrada "`Device State [Locked | Unlocked]`".

La condición de desbloqueo/bloqueo del *bootloader* persiste aunque se borre la partición de sistema o de datos, tal como ocurre tras llevar a cabo una restauración a fábrica del dispositivo móvil.

DESBLOQUEO DEL BOOTLOADER

IMPORTANTE: El desbloqueo del gestor de arranque podría en algún caso invalidar la garantía del dispositivo móvil.

Para proceder a desbloquear el *bootloader*, se requiere:

- Activar la opción de desarrollo "`Desbloqueo de OEM`" (ver apartado "15. Opciones para desarrolladores").

Figura 11 - Activación de la opción de desarrollo "Desbloqueo de OEM"

- Reiniciar el dispositivo móvil en modo "*Bootloader*" según se ilustra en el apartado "25. anexo b: índice de figuras

- Anexo c: Modos de arranque del dispositivo móvil":
- Ejecutar el comando "`fastboot flashing unlock`" desde un ordenador conectado al dispositivo móvil por USB. Tras recibir la confirmación del usuario a través de la pantalla del dispositivo móvil (utilizando el botón de subir volumen y presionando el botón de encendido), se eliminarán todos los datos existentes en el dispositivo móvil y se desbloqueará el *bootloader*. Al reiniciar el dispositivo móvil, se mostrará el mensaje de la imagen central de la <Figura 12> (ver apartado "17. Verified Boot").

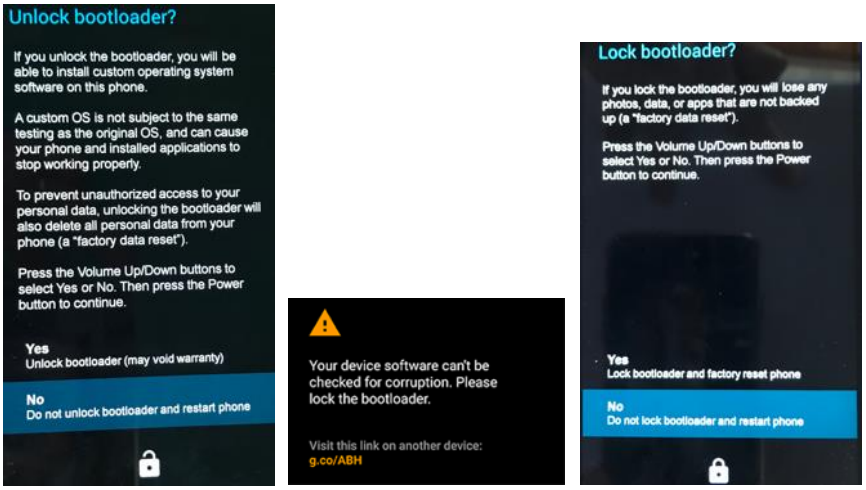

Figura 12 - Desbloqueo/bloqueo del gestor de arranque

BLOQUEO DEL BOOTLOADER

Para proceder a volver a bloquear el *bootloader*, ***opción recomendada desde el punto de vista de seguridad una vez completada la actualización,*** que fue previamente desbloqueado, se requiere:

- Reiniciar el dispositivo móvil en modo *bootloader*.
- Ejecutar el comando "`fastboot flashing lock`" desde un ordenador conectado por USB al dispositivo móvil.

Se recomienda adicionalmente ***volver a desactivar la opción de desarrollo*** "`Desbloqueo de OEM`" (ver apartado "15. Opciones para desarrolladores").

5.3 ROLLBACK PROTECTION

En versiones anteriores, Android había permitido la posibilidad de instalar una versión del sistema operativo más antigua que la presente en el dispositivo (*downgrade*). Android 8 introduce el mecanismo "*Android Rollback Protection*", que impide el *downgrade* como medida de seguridad para evitar el uso de versiones antiguas de sistema operativo con vulnerabilidades que ya han sido solucionadas, no permitiendo el arranque del dispositivo en esas circunstancias. Esta nueva medida de protección está vinculada a la versión 2.0 de *Android Verified Boot* (AVB) (ver apartado "17. Verified Boot"), y es opcional para los fabricantes para los dispositivos suministrados de fábrica con Android 8.

Aunque existen mecanismos no oficiales para realizar el *downgrade* de un dispositivo, en función del fabricante puede ocurrir que el terminal quede en un estado inconsistente que no permita su arranque[10]. Se ***desaconseja proceder a la desactivación del rollback protection,*** especialmente para usuarios no técnicos.

[10] Un ejemplo público conocido es el que afectó a los dispositivos Xiaomi Redmi Note 5: https://www.xda-developers.com/xiaomi-anti-rollback-protection-brick-phone/.

6. CONFIGURACIÓN INICIAL DEL SISTEMA OPERATIVO ANDROID

El presente apartado detalla el proceso de configuración inicial de Android 8.0.0 al restablecer los ajustes de fábrica en un dispositivo Nexus 5x. En función de la versión concreta de Android 8 preinstalada en el dispositivo, las pantallas presentadas pueden diferir en formato y/o contenido, pero las opciones de configuración serán similares.

Al arrancar el dispositivo móvil, se muestra la pantalla de bienvenida, en la que se permite seleccionar el idioma con el que se desea configurar el dispositivo móvil y que también se empleará durante el proceso de instalación (en el ejemplo, se usará "`Español (España)`"), y se dispone de la opción "`Ajustes de visión`", que permite configurar opciones de accesibilidad. El botón "◁" se puede utilizar en cualquier momento durante el proceso de configuración para retroceder a menús anteriores y cambiar la selección.

Seguidamente, se insta a la inserción de una tarjeta SIM, proceso que se puede omitir mediante el botón "`Saltar`", y se ofrece al usuario instalar el dispositivo desde cero (opción "`Configurar como nuevo`", que es la ilustrada en este apartado) o utilizar como base la configuración de otro terminal (opción "`Copiar tus datos`").

A continuación, se presenta el menú de selección de una red Wi-Fi. Desde el punto de vista de seguridad, ***se desaconseja proceder al proceso de instalación inicial del dispositivo móvil utilizando una red Wi-Fi que no sea de total confianza***. Adicionalmente, para disponer de mayor control sobre las actualizaciones automáticas que se llevarán a cabo en el dispositivo, ***se recomienda proceder a la instalación inicial sin conexión a ninguna red de datos***, y, una vez aplicados los ajustes requeridos en base a las necesidades del usuario y a las recomendaciones descritas en la presente guía, proceder a la configuración de las conexiones inalámbricas.

Desde el punto de vista de seguridad, ***se desaconseja proceder al proceso de instalación inicial del dispositivo móvil utilizando una red Wi-Fi que no sea de total confianza***. Adicionalmente, para disponer de mayor control sobre las actualizaciones automáticas que se llevarán a cabo en el dispositivo, ***se recomienda proceder a la instalación inicial sin conexión a ninguna red de datos***, y, una vez aplicados los ajustes requeridos en base a las necesidades del usuario y a las recomendaciones descritas en la presente guía, proceder a la configuración de las conexiones inalámbricas.

6.1 CONFIGURACIÓN SIN CONEXIÓN A RED WI-FI

Si no se desea utilizar una red Wi-Fi para el proceso de instalación inicial, es posible hacer uso de la opción "`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 "`Continuar`". En ese caso, aparecerá el menú de configuración de "`Fecha y hora`", seguido de la opción del "`Nombre`" del propietario.

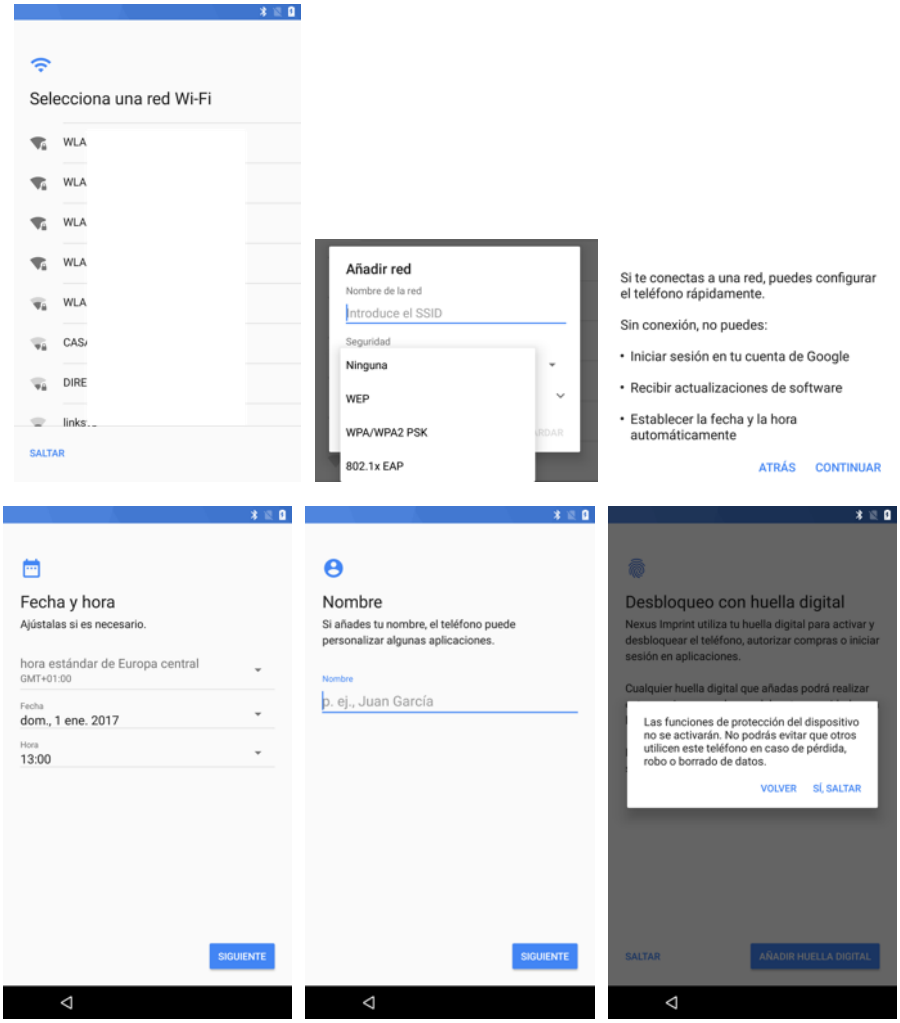

Figura 13 - Proceso de configuración inicial de Android 8: red Wi-Fi y nombre del propietario

Seguidamente se presenta el menú "`Desbloqueo con huella digital`":

- La selección del botón "`Saltar`", en función de la versión de Android 8 presente en el dispositivo, podrá proseguir con el proceso de configuración sin habilitar ningún método de acceso, o presentar la selección de un método alternativo.
- Si se opta por dar de alta una huella dactilar digital (`Nexus Imprint`), se solicitará la selección de la combinación de la misma con otro mecanismo de protección de respaldo, pudiéndose elegir entre "`Nexus Imprint + patrón`", "`Nexus Imprint + PIN`" o "`Nexus Imprint + contraseña`"[11].

[11] Se ha comprobado que, si tras configurar el PIN, el patrón o la contraseña, lo que lleva a iniciar el proceso de adición de una huella, se pulsa el botón de retroceder en la pantalla del dispositivo, el proceso de instalación volverá a la pantalla de configuración de la protección de acceso al dispositivo móvil y, pulsando el botón "Saltar", se obviará el proceso de configuración de una huella dactilar digital, pero se mantendrá el tipo de código de acceso (de respaldo) que se hubiese ya configurado.

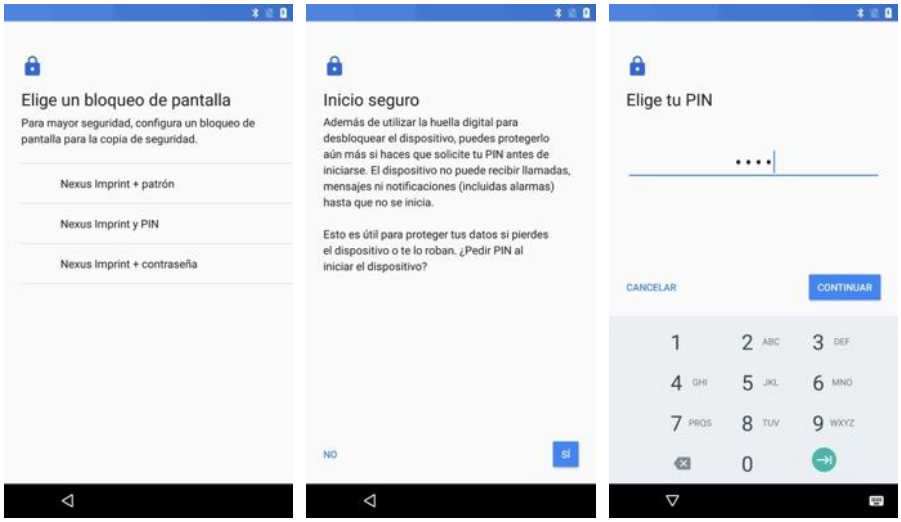

Figura 14 - Proceso de instalación inicial de Android 8: bloqueo de pantalla

La pantalla "`Inicio seguro`" permite proteger el dispositivo móvil de forma que el método de acceso se solicite en el arranque antes de poder utilizar toda la funcionalidad del dispositivo móvil (ver apartado "20.1. Inicio seguro"). Desde el punto de vista de seguridad, ***se recomienda responder "`SÍ`" para aceptar este ajuste***.

En primer lugar, se procederá a definir el método de acceso de respaldo (PIN/patrón/contraseña) que se desea utilizar si fallase el reconocimiento de huella (ver apartado "10.1. Seguridad del dispositivo" para más detalles), seguido del alta de la huella dactilar digital. Si el proceso de instalación se detuviese antes de definir la huella (por ejemplo, reiniciando el dispositivo móvil), se retomaría desde cero la configuración, pero se mantendría el código de acceso de respaldo que se hubiese definido.

Por último, se muestra el menú "`Servicios de Google`", que ofrece las siguientes opciones (activas por defecto), y que, por seguridad y privacidad, ***se recomienda desactivar inicialmente***:

- "`Permitir que las aplicaciones encuentren tu ubicación`" y "`Mejorar la precisión de la ubicación`": provocará que las apps y servicios puedan generar tráfico Wi-Fi y/o Bluetooth aunque los respectivos interfaces estén desactivados.
- "`Enviar datos del sistema`": empleado para el análisis de datos de uso del dispositivo por parte de Google.

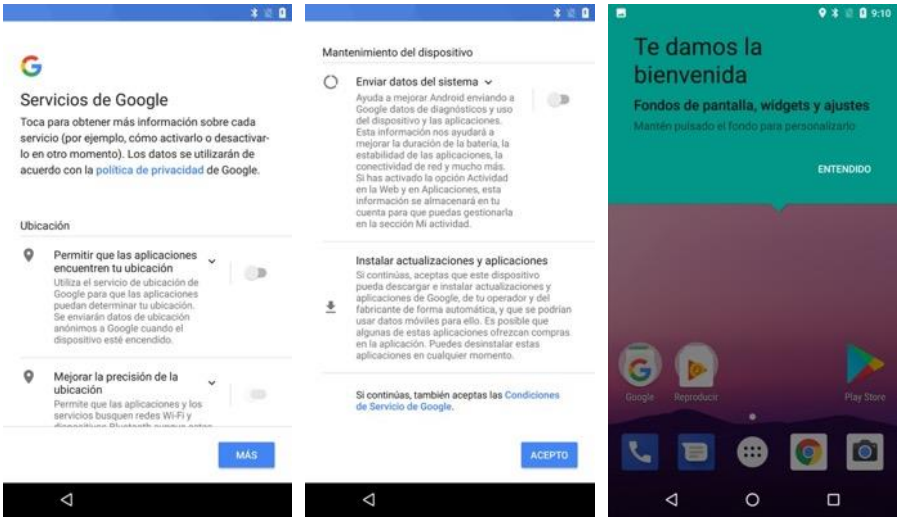

Figura 15 - Proceso de instalación inicial de Android 8: servicios de Google

La sección "¿Algo más?" permite añadir cuentas de correo y apps adicionales, lo cual requiere de conexión de datos, y definir la presentación de notificaciones en la pantalla de bloqueo (ver apartado "8.6. Notificaciones").

6.2 CONFIGURACIÓN CON CONEXIÓN A RED WI-FI

El dispositivo mostrará la lista de las cinco redes Wi-Fi cuya intensidad de señal sea superior desde la ubicación actual en la que se encuentra el dispositivo móvil, ordenadas por intensidad de señal y, a igualdad en este criterio, por orden alfabético. Si se desea utilizar una red Wi-Fi que no esté en dicha lista, pero que sea visible, se deberá seleccionar la opción "Ver todas las redes Wi-Fi", lo cual mostrará una pantalla con todas las redes Wi-Fi al alcance del dispositivo móvil, y que se actualizará dinámicamente en función de cómo varíe la recepción de la señal de cada una de ellas.

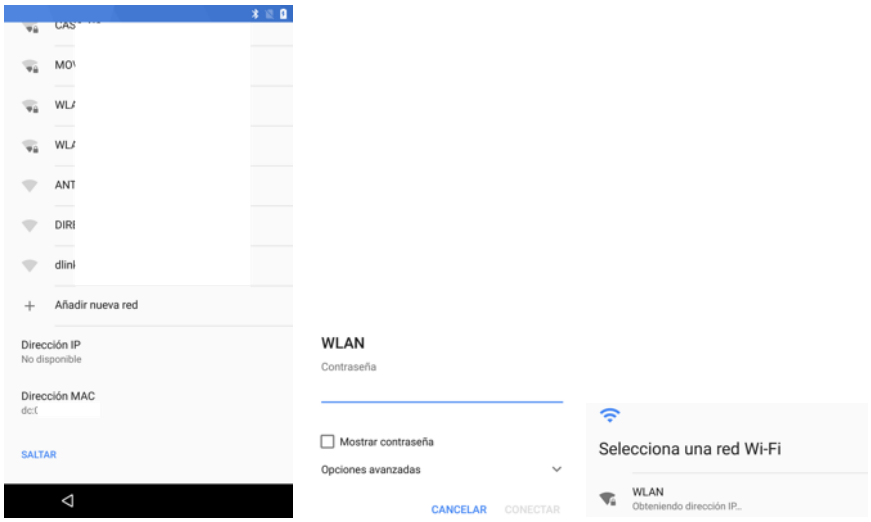

Figura 16 - Proceso de instalación inicial: selección de red Wi-Fi

El botón "`+ Añadir nueva red`" permite añadir redes Wi-Fi ocultas que hagan uso de diferentes mecanismos de seguridad: WEP, WPA/WPA2 PSK o 802.1x EAP. ***El uso de redes Wi-Fi ocultas se desaconseja desde el punto de vista de seguridad***.

Al seleccionarse una red concreta, se muestra el menú de introducción de la contraseña. Es importante realizar este paso en condiciones que impidan el acceso visual a la pantalla del dispositivo por parte de terceros, ya que los caracteres de la contraseña se muestran en claro durante unos instantes desde su introducción. Adicionalmente, se permite definir si la red es o no de uso medido.

El dispositivo se conectará a los servidores de Google y mostrará la pantalla "`Buscando actualizaciones`", aunque no mostrará información sobre si ha encontrado alguna actualización disponible.

Para disponer de un control más granular de la configuración del dispositivo, se recomienda posponer la introducción de la cuenta de Google seleccionando "`Saltar`". El proceso de instalación continúa con las secciones "`Servicios de Google`" y "`Desbloqueo con Pixel Imprint`", descritos en el subapartado anterior "6.1. Configuración sin conexión a red Wi-Fi". Por último, se ofrecerá la posibilidad de instalar aplicaciones adicionales, añadir una cuenta de correo electrónico y configurar la presentación de notificaciones. Desde el punto de vista de seguridad, ***se recomienda desmarcar todas las aplicaciones adicionales y proceder únicamente a la instalación de las que se requieran***.

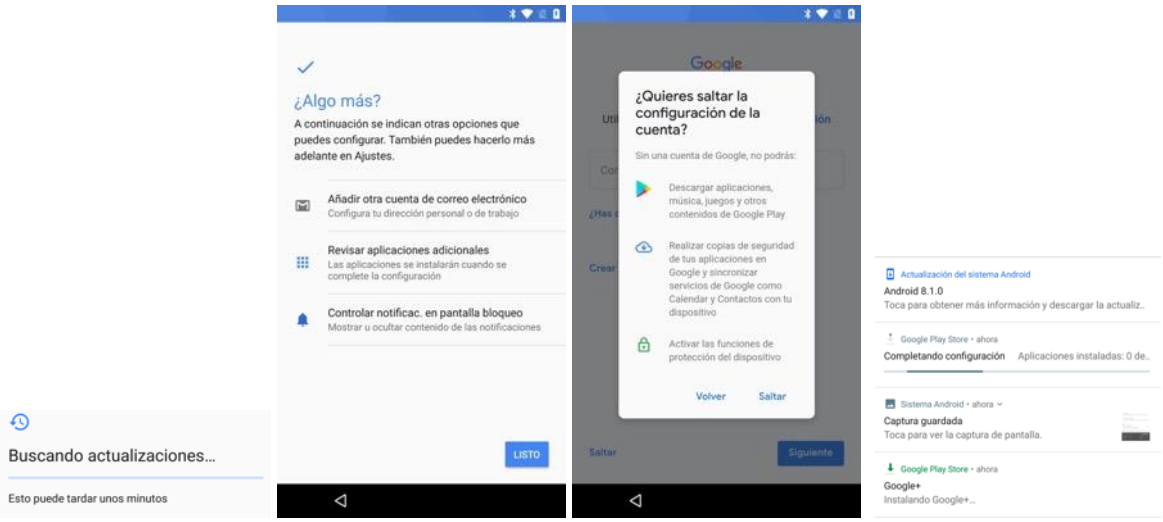

Figura 17 - Proceso de instalación inicial: copia de datos desde otro dispositivo

Finalmente, el dispositivo móvil quedará instalado y listo para su uso, presentando la pantalla principal.

NOTA: se ha constatado que, tras el proceso de instalación y configuración inicial de Android 8, el dispositivo móvil inicia automáticamente una serie de descargas (ver imagen derecha de la <Figura 17>) para instalar aplicaciones de Google que no vienen en la imagen de fábrica, como Google+ y Google Keep, y ello sin que el usuario haya dado de alta su cuenta de usuario de Google en el dispositivo móvil. Se recomienda desinstalar dichas aplicaciones salvo que se vaya a hacer uso de ellas.

La versión concreta instalada se puede obtener a través del menú "Ajustes - Sistema - Información del teléfono - Versión de Android". ***Se recomienda proceder a la aplicación de las recomendaciones de seguridad descritas en la presente guía***.

Al disponer de conexión a una red Wi-Fi, el dispositivo móvil detectará la disponibilidad de una nueva actualización, e iniciará su descarga e instalación de forma automática en base a la opción "Actualizaciones del sistema automáticas" (introducida y activa por defecto desde Android 7; ver apartado "15. Opciones para desarrolladores"). La disponibilidad de la nueva versión se mostrará al usuario a través de una notificación. Los detalles sobre el proceso de detección e instalación de nuevas versiones se pueden consultar en el apartado "5.1. Actualización automática del sistema operativo Android".

7. PRIMERAS ACCIONES PARA PROTEGER EL DISPOSITIVO MÓVIL

Las primeras recomendaciones de seguridad a aplicar una vez finalizada la instalación o configuración inicial de Android en el dispositivo móvil son:

1. Deshabilitar la opción "Mostrar contraseñas", activa por defecto, que lleva a que la introducción de caracteres de contraseñas en Android muestre brevemente cada carácter introducido (ver apartado "10. Seguridad y ubicación").
2. Establecer un código de acceso (si no se llevó a cabo este paso durante la configuración inicial) y el bloqueo automático de pantalla (ver apartado "10. Seguridad y ubicación").
3. Desactivar los interfaces inalámbricos de los que no se esté haciendo uso: Wi-Fi, Bluetooth, NFC y datos móviles, que quedan habilitados por defecto tras el proceso de instalación, aunque no se haya hecho uso de ellos (ver apartado "12. Red e Internet").
4. Desactivar la ubicación (ver apartado "10.3. Servicios de localización").
5. Configurar las notificaciones de forma que no se muestre su contenido con la pantalla bloqueada (ver apartado "8.6. Notificaciones").
6. Desinstalar todas aquellas apps de las que no se vaya a hacer uso.
7. Personalizar el menú de ajustes rápidos para eliminar elementos sensibles (ver apartado "8.3. Menú de ajustes rápidos").
8. Tan pronto finalice la aplicación de las medidas de securización y protección del dispositivo, realizar una copia de seguridad (ver apartado "21. Copias de seguridad y restauración").

8. INTERFAZ DE USUARIO

8.1 PANTALLA DE BLOQUEO

La pantalla de bloqueo (*lock screen*) se presenta tras arrancar el dispositivo móvil o tras presionar una vez el botón de encendido. Para encender/apagar el dispositivo,

se realiza una pulsación larga sobre el botón de encendido (Power), que ofrece las opciones "Apagar" y "Reiniciar".

Esta pantalla permite, sin necesidad de introducir el código de acceso, la pre-visualización de diversos elementos por defecto:

- Parte superior o barra superior de estado: nombre del operador de telecomunicaciones, los iconos de conectividad (Wi-Fi, datos móviles, Bluetooth), el nivel de batería y el usuario actual, además de iconos como el de "no molestar" si el dispositivo está en este modo (ver apartado "8.4. Barra superior de estado").
- En la zona central: fecha y hora, y el panel de notificaciones (consultar apartado "8.6. Notificaciones").
- Zona inferior: acceso al asistente de Google (se solicitará el método de desbloqueo de pantalla), estado de la batería (y si el dispositivo está conectado a la corriente), indicador del método de bloqueo vigente (ver apartado "10.1. Seguridad del dispositivo") y acceso directo a la cámara. Particularmente, el conocimiento del método de bloqueo puede favorecer que un atacante se decida a sustraer el dispositivo, especialmente si comprueba que está desbloqueado por *Smart Lock* y/o no tiene un método configurado.

Adicionalmente, es posible desplegar el menú de ajustes rápidos, que permite realizar operaciones sensibles sin necesidad de introducir el código de acceso (ver apartado "8.3. Menú de ajustes rápidos").

Para activar el bloqueo de pantalla, presionar una vez el botón de encendido.

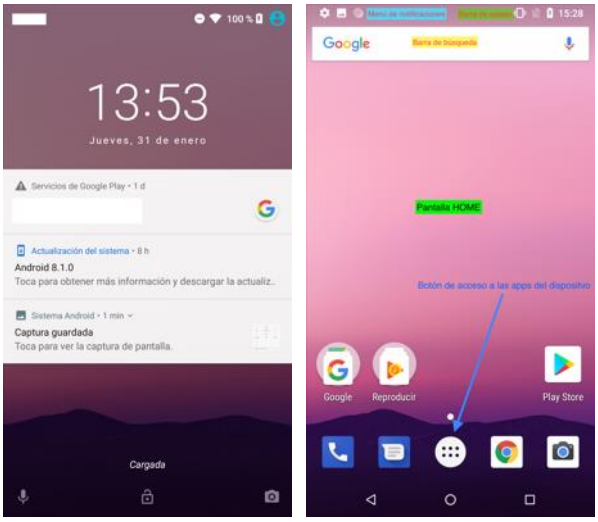

Figura 18 - Pantalla de bloqueo y de inicio ("Home") de Android 8

8.2 PANTALLA DE INICIO (HOME)

La pantalla de inicio se muestra al salir de la pantalla de bloqueo. Su apariencia en Android 8 es muy similar a la de su antecesor, Android 7.1.2, y desde ella se puede acceder a las distintas apps, ver la barra de estado, la barra de notificaciones y la barra

de búsqueda por voz, descritos a lo largo de este apartado. Los botones para navegar por el interfaz son: "  " (para volver a la pantalla de inicio desde cualquier menú), "  " (retroceso al menú padre) y "  " (lista de apps en ejecución).

El principal elemento de control y configuración del dispositivo móvil en Android es el menú de `Ajustes`, representado por el símbolo "  ".

Los iconos de apps se pueden agrupar entre sí, para lo cual se debe seleccionar mediante una pulsación larga un icono y arrastrarlo hasta el icono que representa al grupo contenedor (un grupo se crea cuando el icono de una app es arrastrado hasta el de otra app). El nombre del grupo se asigna pulsando sobre él y seleccionando el actual (que, inicialmente, es "`Carpeta sin nombre`"). Aunque desde el punto de vista práctico se suele asignar a los grupos nombres representativos del tipo de apps que contienen, desde el punto de vista de privacidad se recomienda no elegir nombres muy explícitos (como "Banca", "Salud", o "Personal"), que pueden ser fácilmente vistos por terceros que tengan acceso visual al dispositivo.

Android 8 introdujo la posibilidad de añadir accesos directos (*shortcuts*) a acciones concretas de apps y *widgets*. Al pulsar prolongadamente el icono de una app, se desplegarán:

- El icono da acceso a los *widgets* de la app (en el margen superior derecho).
- El icono de información que abre el menú "`Información de la aplicación`".
- Una lista de acciones que, si se arrastran a la pantalla de inicio, crearán un acceso directo a esa acción.

Desde el punto de vista de seguridad y privacidad, se desaconseja incluir accesos directos a acciones sensibles, pues basta con una pulsación sobre un icono para iniciar la acción.

Por su parte, los *widgets* (complementos que proporcionan una funcionalidad muy concreta de una app, disponible de forma persistente en la pantalla de inicio cuando la misma está desbloqueada) se añaden mediante el siguiente procedimiento:

- Pulsar un espacio vacío en la pantalla de inicio 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 soltarlo levantando el dedo. Si el *widget* admite alguna personalización, por ejemplo, realizar una llamada directa de teléfono, al soltarlo se abrirá el menú de opciones. En el caso del acceso para realizar una llamada directa, se mostrará un menú para elegir el contacto.
- Para eliminar un *widget* de la pantalla de inicio, se pulsará prolongadamente sobre el *widget*, y se arrastrará hacía el texto "`x Quitar`" de la parte superior de la pantalla.

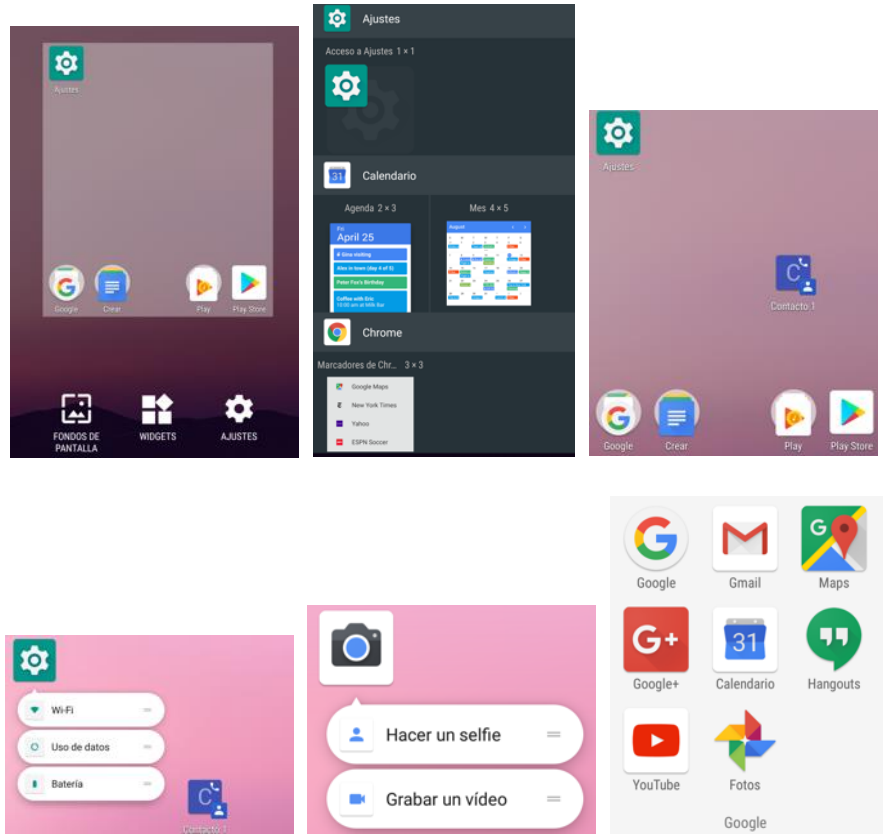

Figura 19 - Uso de grupos de apps, accesos directos y widgets

El interfaz de usuario de Android permite visualizar la pantalla en modo vertical y horizontal de forma automática mediante el ajuste rápido "`Girar automáticamente`".

8.3 MENÚ DE AJUSTES RÁPIDOS

El menú de ajustes rápidos permite realizar determinadas configuraciones desde la pantalla actual sin tener que recorrer todo el camino desde el menú principal de "`Ajustes`" y los correspondientes submenús que dan acceso a una opción determinada, de forma similar a un acceso directo. Es posible desplegarlo mediante:

- Con la pantalla bloqueada, deslizando uno o dos dedos de arriba hacia abajo.
- Con la pantalla desbloqueada:
    - Deslizando con un dedo de arriba hacia abajo (además de las notificaciones activas), aparecerá un menú con los 6 primeros iconos del menú, sombreados o en negro (según si la funcionalidad asociada a ellos está activa o no en ese momento).
    - Deslizando con dos dedos desde la parte superior de la pantalla, o con un solo dedo en dos tramos.

Para configurar los ajustes rápidos a incluir en el menú, pulsar el botón de edición "✎" y arrastrar los iconos de cada ajuste hacia arriba (para añadir la función) o hacia abajo (para eliminarla). No es posible definir elementos que únicamente estén disponibles con la pantalla desbloqueada, aunque algunos requieren de la validación

del código de acceso para lanzar su acción, como "Ubicación" y "Enviar". Desde el menú de edición, mediante "⋮ - Restablecer" es posible devolver el menú a las opciones activas por defecto.

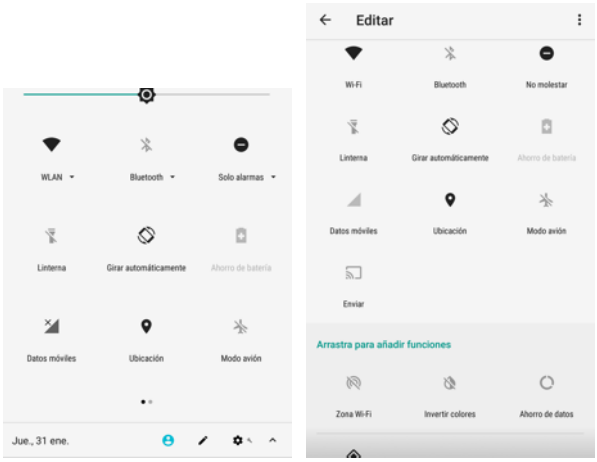

Figura 20 - Menú de ajustes rápidos

Aunque representa un elemento orientado a la facilidad de uso, el menú de ajustes rápidos tiene mucho impacto desde el punto de vista de seguridad, pues permite a cualquier tercero con acceso físico al dispositivo móvil realizar acciones críticas mediante la manipulación del correspondiente icono. Por ello, a continuación, se proporcionan recomendaciones para los iconos más relevantes. La eliminación de los elementos indicados puede ser complementada con la adición de *widgets* para las funciones correspondiente en la pantalla de inicio, lo que proporciona equilibrio entre la comodidad en el uso y la seguridad:

- "Wi-Fi, Bluetooth y datos móviles": además del estado de la conexión (en gris si no está activa) y la posibilidad de activarla/desactivarla, se representa el estado de la transmisión de datos (la flecha hacia arriba indica transmisión desde el dispositivo; hacia abajo, transmisión hacia el dispositivo). ***Se recomienda eliminar ambos ajustes*** para evitar que se manipule el estado de las comunicaciones establecidas por el usuario.
- "Ahorro de batería": ante una situación en la que se sabe de antemano que el dispositivo móvil no podrá conectarse a la corriente (por ejemplo, durante un viaje, se recomienda activar este modo para prolongar la vida de la batería).
- "No molestar": ver apartado "8.6. Notificaciones". ***Se recomienda eliminar este ajuste*** para evitar que un tercero pueda desactivar este modo y recibir en la pantalla las notificaciones de apps sensibles.
- "Linterna": encenderá el flash de la cámara del dispositivo móvil para ser usado como linterna. ***Se recomienda mantener este ajuste*** porque este modo puede ser utilizado como elemento de petición de auxilio.
- "Modo avión": ***se recomienda eliminar este ajuste***, que permitiría suprimir todas las conexiones inalámbricas de datos del dispositivo impidiendo su localización mediante el servicio de Google "Encontrar mi dispositivo".

- "Ubicación": solo admite manipulación introduciendo el código de acceso si el dispositivo está bloqueado, pero ***se recomienda eliminar este ajuste*** porque permite saber si los servicios de localización geográfica están o no activos.
- "Enviar": permite compartir la pantalla actual con otro dispositivo a través de Wi-Fi Direct (por ejemplo, con un dispositivo *ChromeCast*), es irrelevante desde el punto de vista de seguridad porque requiere introducir el código de acceso.
- "Zona Wi-Fi": ***se recomienda eliminar este ajuste*** porque permite activar o desactivar la compartición de la conexión móvil de datos del dispositivo móvil con otros dispositivos vía Wi-Fi (ver apartado "12.2. Wi-Fi").

La pulsación prolongada sobre los iconos del menú de ajustes rápidos despliega el menú principal de ajustes asociado a dicha función específica, pero esta acción, realizada desde la pantalla de bloqueo, solicita al usuario la validación del código de acceso, por lo que no tiene efectos peligrosos sobre la seguridad del dispositivo.

8.4 BARRA SUPERIOR DE ESTADO

Ubicada en la parte superior de la pantalla, proporciona información relevante sobre el estado del dispositivo, disponible incluso con la pantalla bloqueada, incluyendo por defecto los iconos de conectividad (Wi-Fi, 2/3/4G y Bluetooth), ubicación, el nivel de batería y el usuario actual (si es distinto del propietario), además de iconos como el de "No molestar" si el dispositivo está en este modo. En su parte izquierda muestra el estado del interfaz de telefonía móvil (incluyendo el nombre del operador) y los símbolos correspondientes a las apps que tienen notificaciones activas en la barra de notificaciones (ver <Figura 18 >).

Android no ofrece un método directo para personalizar el contenido de esta barra, sino que proporciona una funcionalidad "oculta" que se describe en el apartado "15.4. Configurador de IU del sistema". Pese a que esta funcionalidad debe ser utilizada con precaución, ***se recomienda su uso desde el punto de vista de seguridad para suprimir***, desactivando los interruptores correspondientes, ***todos los iconos relativos a comunicaciones***, ***modo "No molestar" y perfil de trabajo***.

8.5 BÚSQUEDA MEDIANTE TEXTO Y VOZ

La app "Google", que proporciona acceso directo al buscador de Google y a otros servicios de la compañía, está accesible desde la parte superior de la pantalla de inicio (ver <Figura 18>), permite realizar búsquedas mediante texto y voz, proporcionando sugerencias personalizadas asociadas a la actividad del usuario. Al estar vinculada a la existencia de una cuenta de usuario de Google activa en el dispositivo, queda fuera del alcance de la presente guía (los detalles de uso y configuración pueden consultarse en el apartado "8.2.1. Asistente personal Y "OK Google"" de la "Guía CCN-STIC-456 - Cuenta de usuario, servicios y aplicaciones de Google para dispositivos móviles Android" [Ref.- 408].

8.6 NOTIFICACIONES

Una notificación es un mensaje que una aplicación o app puede mostrar al usuario fuera del interfaz gráfico propio, para informarle de eventos que se consideran relevantes desde el punto de vista de la app. Las notificaciones se envían al sistema para que las procese conforme a la configuración definida por el usuario en relación con la política de interrupciones 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.

Figura 21 - Notificaciones en la pantalla de bloqueo

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 "8.6.2. Interrupciones").
    - 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 bloqueo. Se mostrarán un total de cuatro notificaciones, y, las sucesivas, se englobarán en una sola entrada que va precedida con el símbolo "`+número`", siendo "`número`" el número de notificaciones activas pendientes que no se están visualizando actualmente.
    - Con el dispositivo desbloqueado, las notificaciones se mostrarán en la barra de notificaciones (*notification drawer*) situada en el margen superior izquierdo del dispositivo móvil; para ver el detalle de la notificación, se desplegará el panel deslizando el dedo desde la parte superior hacia abajo.
- Sensibilidad de la notificación (se define a nivel de la aplicación móvil).
- Carácter de la notificación: definición de su prioridad (por parte de la app).

Las notificaciones con la pantalla bloqueada pueden revelar información muy sensible del usuario y la aplicación, por lo que ***se recomienda valorar cuidadosamente los ajustes definidos a través del menú "`Ajustes - Aplicaciones y notificaciones`"***.

MENÚ "NOTIFICACIONES"

Los ajustes definidos directamente en este menú tienen carácter global, es decir, afectan a todas las apps del dispositivo móvil. Aunque desde Android 8 se proporciona un control muy granular de las notificaciones que incorpora estos mismos ajustes a nivel de app, e incluso de categoría de notificación dentro de una app, los ajustes

globales de este menú establecen el modo más restrictivo, que ningún ajuste específico puede relajar, pero sí viceversa:

- "`En la pantalla de bloqueo`": fijar a "`No mostrar notificaciones`" (no se mostrará ninguna indicación de la llegada de una notificación, opción más segura) u "`Ocultar notificaciones sensibles`" (solo se mostrará la aplicación origen de la notificación y la parte de los contenidos que dicha app no considere sensibles). La opción "`Mostrar todo el contenido de las notificaciones`" suele desaconsejarse, al menos mientras no se haya realizado una configuración de notificaciones granular adaptada a las particularidades de uso del dispositivo, que vele por la sensibilidad de la información potencialmente expuesta.
- "`Permitir puntos de notificación`": Android incorpora este ajuste imitando el comportamiento de iOS para señalizar que una app tiene notificaciones sin procesar mediante un pequeño punto o burbuja en el icono de la app. Este ajuste no tiene impacto desde el punto de vista de seguridad.
- "`Deslizar por el sensor de huellas para abrir notificaciones`": con este ajuste activo, las notificaciones se desplegarán si se desliza el dedo hacia abajo por el sensor de huellas (gesto). No tiene impacto desde el punto de vista de seguridad.

Si bien las notificaciones asociadas a apps de mensajería suelen incluir acciones para responder de forma rápida, la invocación de estas acciones no está disponible en la pantalla de bloqueo, aunque esté activa la opción "`Mostrar todo el contenido de las notificaciones`", lo cual supone un beneficio desde el punto de vista de seguridad.

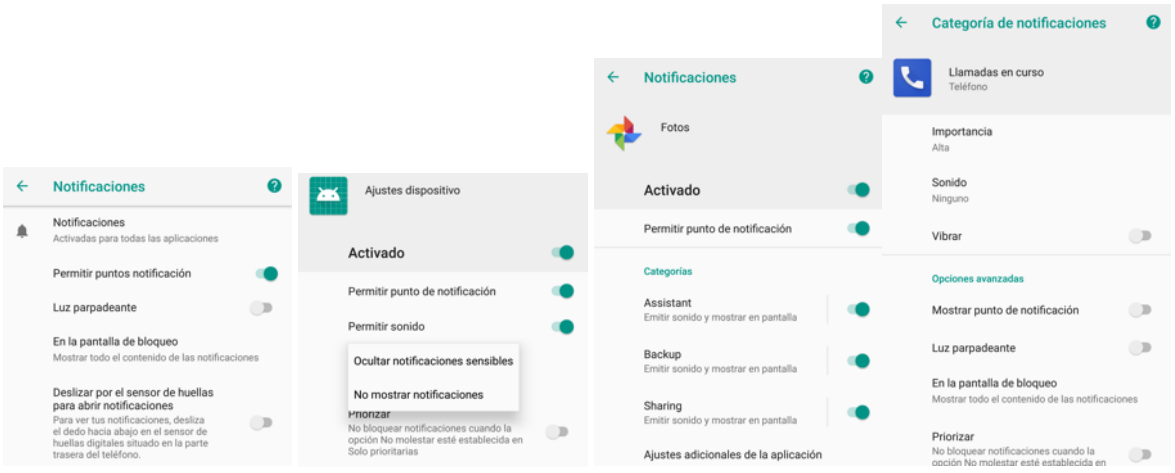

Figura 22 - Configuración de notificaciones a nivel de app y categorías de notificación

8.6.1 CONTROL DE NOTIFICACIONES A NIVEL DE APP

A través del menú "`Ajustes - Aplicaciones y notificaciones - Notificaciones`" se obtiene la lista de apps instaladas en el dispositivo. Seleccionando una app concreta, es posible definir los ajustes descritos en la sección previa MENÚ

"NOTIFICACIONES" a nivel de app y/o de categoría de notificación específica (ya que algunas apps establecen sus propias categorías de notificación, denominadas "canales" en la API 26 [Ref.- 29]), así como establecer qué tipo de comportamiento se desea en cuanto a:

- "Importancia": afecta al modo en que la notificación se mostrará en pantalla cuando ésta se encuentra desbloqueada [urgente - emite sonido y muestra en pantalla | alta - emite sonido| media - muestra en silencio| baja - muestra en silencio y minimiza].
- "Sonido".
- "Vibrar": [on|off].
- "Opciones avanzadas": la opción "Priorizar" (Android 8.0.0) / "Omitir No molestar" (Android 8.1.0) permite alterar el ajuste por defecto para el modo "No molestar" (ver apartado "8.6.2. Interrupciones").

Adicionalmente, es posible acceder a la configuración granular de las categorías (o canales) de las notificaciones de una aplicación deslizando ligeramente el dedo de izquierda a derecha sobre una notificación y presionando "⚙" - "Todas las categorías" (Android 8.0) / "Más ajustes" (Android 8.1.0). La imposibilidad de desactivar las notificaciones para las apps de sistema se indica en el texto que se despliega al realizar esta acción. Como se indicó anteriormente, el ajuste global "En la pantalla de bloqueo" determinará qué valor mínimo puede tomar este ajuste para las distintas categorías de notificación de la app, que no podrán infringirlo.

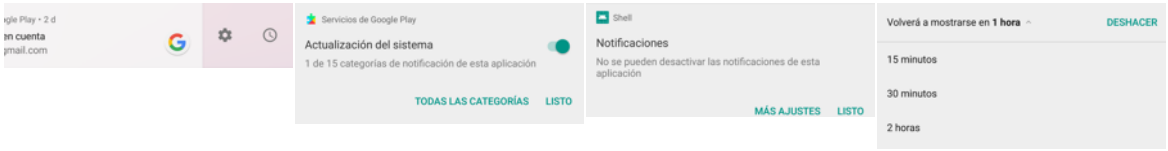

Figura 23 - Ajustes rápidos de notificaciones

La desactivación de todas las notificaciones de una app se muestra en el propio menú "Aplicaciones y notificaciones - Notificaciones" (el interruptor aparecerá "Desactivado"). Es posible saber qué apps tienen las notificaciones desactivadas desplegando el submenú "Notificaciones de aplicaciones - Aplicaciones desactivadas". A través de la opción "⋮" se puede mostrar la configuración de notificaciones para las aplicaciones del sistema.

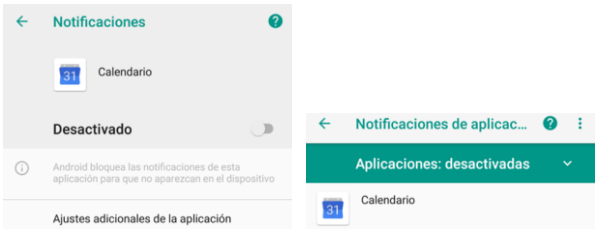

Figura 24 - Comprobación del estado de las notificaciones de una app

Adicionalmente, algunas apps permiten establecer ajustes de notificaciones desde sus menús de configuración particulares.

8.6.2 INTERRUPCIONES

Una interrupción es un evento generado por una app, que normalmente ejecuta en segundo plano, destinado a atraer la atención del usuario interfiriendo con el uso que está haciendo del dispositivo en un momento concreto. Las interrupciones emiten señales, como activación de la pantalla, de la luz de notificación, o vibración. Es la aplicación la que define el carácter de la interrupción en cuanto a su prioridad, pero es el usuario quien establece el comportamiento del dispositivo frente a la interrupción, que puede ser:

- "`Silencio total`": se bloquean todos los sonidos y vibraciones mientras esté vigente el modo "No molestar" (aunque es posible establecer un plazo "`Durante X horas`" (por defecto 1 hora, pero ampliable a las horas que especifique el usuario con los botones de "+" y "-")).
- "`Solo alarmas`".
- "`Solo prioritarias`": permite filtrar qué llamadas y mensajes se desea recibir, así como si los recordatorios y eventos podrán provocar la interrupción. Las alarmas siempre se consideran prioritarias.

El modo "`No molestar`" se configura a través de "`Ajustes - Sonido - Preferencias de No molestar`", y, alternativamente, mediante una pulsación larga al símbolo "⊖" del menú de ajustes rápidos (ver apartado "8.3. Menú de ajustes rápidos"). Las opciones de este menú son:

- "`Prioridad solo permite`" configura el comportamiento para las interrupciones consideradas "Prioritarias".
- "`Bloquear interrupciones visuales`": especifica el comportamiento de las señales de interrupción con la pantalla bloqueada y desbloqueada.
- "`Reglas automáticas`": permite establecer reglas propias (de tipo de evento de calendario o de fecha y hora).

El modo "`No molestar`" se puede activar manualmente mediante una pulsación sobre el icono "⊖" del menú de ajustes rápidos (ver apartado "8.3. Menú de ajustes rápidos") y mediante una pulsación larga sobre el botón de bajar volumen.

El menú "`Ajustes - Aplicaciones y notificaciones - [Avanzado] Alertas de emergencias`" incluye los ajustes particulares de las alertas que determinados países envían por SMS ante situaciones de riesgo para la población, como en caso de inclemencias meteorológicas extremas o el programa AMBER [Ref.- 31]. ***Desde el punto de vista de la seguridad personal, se recomienda establecer el valor*** "`Permitir alertas`" para este tipo de interrupciones.

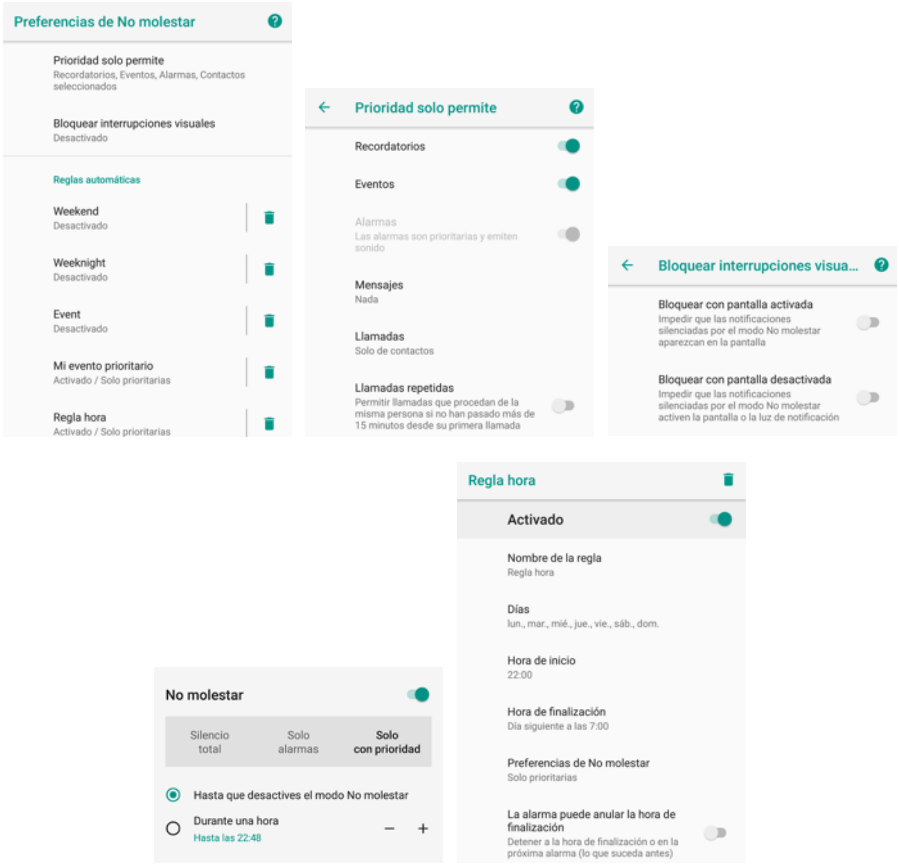

Figura 25 - Configuración del modo "No molestar"

Desde el punto de vista de seguridad, ***se recomienda eliminar el icono "`No molestar`" del menú de ajustes rápidos*** (ver apartado "8.3. Menú de ajustes rápidos") para impedir que un tercero con acceso físico al dispositivo pueda activar este modo. Se recomienda activar el modo "No molestar" en situaciones donde pueda requerirse ocultar la presencia del dispositivo, impidiendo que sea patente la existencia del mismo debido a notificaciones inoportunas.

Para más información y detalles sobre las distintas opciones de configuración del modo "`No molestar`", se recomienda consultar la [Ref.- 30].

9. CONFIGURACIÓN DEL DISPOSITIVO

La configuración del dispositivo móvil, crítica desde el punto de vista de seguridad, se realiza principalmente desde el menú "`Ajustes`", identificado por el símbolo "⚙". Android 8 prescinde de la navegación por las diferentes categorías mediante deslizamiento táctil existente en Android 7, y reorganiza el menú dividiéndolo en 4 zonas:

- Una barra de búsqueda en la parte superior (que permite buscar por el nombre de un ajuste).
- Área de sugerencias, con accesos directos a las tareas propuestas.

- Estado actual del dispositivo, con accesos directos a los ajustes para alterar dicho estado (por ejemplo, ahorro de datos activado, modo "No molestar" activo, etc.). Resulta muy útil si se han suprimido los iconos de la barra superior de estado siguiendo las recomendaciones propuestas en el apartado "8.4. Barra superior de estado".
- Sección de ajustes, organizados por categorías, que se describirán a lo largo de los diferentes apartados de la presente guía:

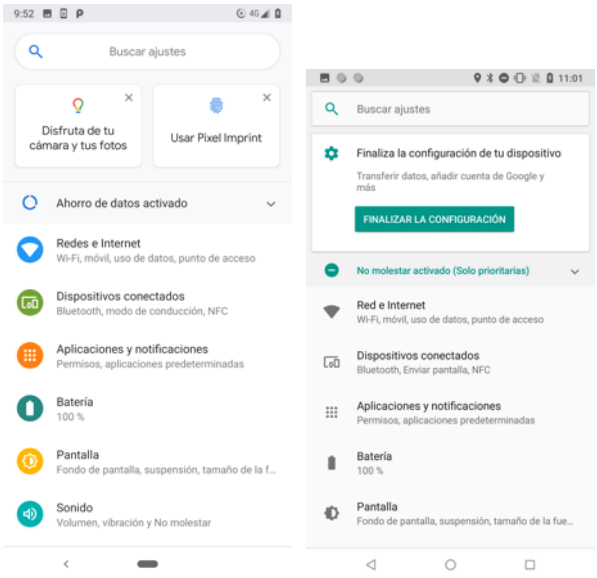

Figura 26 - Menú "Ajustes"

Como parte de este apartado se describen las categorías de ajustes "Sistema", "Batería", "Pantalla", "Sonido", "Accesibilidad" y "Almacenamiento". El resto de categorías se describirá en apartados propios donde se analiza su seguridad asociada.

Android 8 permite disponer de varias instancias del menú "Ajustes" ejecutando en paralelo, lo que posibilita realizar distintos cambios de configuración sin necesidad de volver a recorrer todos los menús de esta app. Dado que cada una de estas instancias del menú de ajustes queda activa, aunque las demás se hayan cerrado, conviene verificar que todas se cierran cuando se haya terminado de realizar todos los cambios de configuración.

9.1 SISTEMA

Esta sección incorpora información y ajustes generales del dispositivo móvil. Además de las visibles por defecto, existen funcionalidades ocultas para el usuario, que se pueden activar mediante operaciones especiales, como "Opciones para desarrolladores" y "Configurador IU del sistema" (descritas en el apartado "15. Opciones para desarrolladores").

IDIOMAS E INTRODUCCIÓN DE TEXTO

A pesar de aportar usabilidad al dispositivo móvil, desde el punto de vista de la seguridad y/o la privacidad, ***se recomienda establecer los siguientes ajustes***:

- "Teclado virtual":
  - "Dictado por voz de Google": desactivar mediante "+ Administrar teclados".
  - "Gboard - Preferencias": desactivar "[Pulsación de teclas] Sonar al pulsar tecla" para evitar que se revele la longitud de las contraseñas.
  - "Gboard - Ajustes avanzados": desactivar las opciones de "Mejorar Gboard", que envían información de la interacción con el teclado a Google, incluyendo fragmentos de texto.
  - "Gboard - Escritura deslizando el dedo": valorar la desactivación de "Mostrar recorrido del gesto", que permite seguir visualmente el rastro de los caracteres introducidos.
- "[Ajustes avanzados] Servicio autocompletar": (ver apartado "16.4. Servicio autocompletar").

GESTOS

Este menú, situado bajo "Ajustes - Sistema", incorpora ciertos ajustes relevantes desde el punto de vista de seguridad cuya recomendación se indica a continuación:

- "Acceso rápido a la cámara": permite lanzar la app cámara pulsando dos veces sobre el botón de encendido. Carece de interés desde el punto de vista de seguridad en Android 8, ya que el acceso a la cámara está también permitido en la pantalla de bloqueo a través del botón táctil situado en la parte inferior del dispositivo.

COPIA DE SEGURIDAD

Para obtener los detalles de la opción "Copia de seguridad en Google Drive", consultar el apartado "21. Copias de seguridad y restauración".

OPCIONES DE RECUPERACIÓN

Permiten devolver el dispositivo móvil a los ajustes de fábrica para:

- "Wi-Fi, red móvil y Bluetooth": se eliminarán las contraseñas de las redes Wi-Fi, así como todas las vinculaciones establecidas con dispositivos BT.
- "Ajustes de aplicaciones": todas las apps serán devueltas a sus preferencias originales, incluyendo permisos, notificaciones y estado de habilitación, pero sin pérdida de los datos propios de la app. Esta acción puede ser requerida si se observan comportamientos extraños en el dispositivo o si se ha perdido el control del mismo durante cierto tiempo.
- "Borrar todos los datos": ver apartado "22. Eliminación de datos del dispositivo móvil".

ACTUALIZACIONES DEL SISTEMA

Permite determinar la versión de Android del dispositivo móvil (incluyendo el nivel de parches de seguridad), así como iniciar la comprobación de actualizaciones.

No obstante, la disponibilidad de una nueva versión para el dispositivo se avisa mediante una notificación.

Para más información sobre las actualizaciones de sistema operativo, consultar el apartado "5. Actualización del sistema operativo Android".

INFORMACIÓN DEL TELÉFONO

En esta sección se muestran datos relevantes del hardware del dispositivo móvil y del estado del mismo, a diferentes niveles (ver <Figura 2>).

La sección "Estado" muestra el estado de la batería, de la SIM (incluyendo el IMEI, la red móvil que proporciona el servicio, la condición de itinerancia y el tipo de red móvil), la dirección MAC del interfaz Wi-Fi y Bluetooth, y el número de serie. Esta sección es meramente informativa, pero conviene conocer qué elementos incluye de cara a la detección de problemas en las conexiones establecidas por el dispositivo.

Además del "Nombre del dispositivo", existen otros tres identificadores estrechamente ligados al uso dispositivo:

- DEVICE_ID: corresponde al número de serie del terminal.
- ANDROID_ID: este identificador (de 64 bits) se genera durante el proceso inicial de instalación y configuración. En versiones anteriores a Android 8.0 (API 26), permanecía invariable mientras el terminal no fuese restablecido a fábrica. A partir de Android 8.0, el "ANDROID_ID" va asociado a una combinación única de clave de firma de la app que quiere obtenerlo, usuario y dispositivo, que prevalece desde el proceso de configuración inicial hasta que cambie la clave de firma del APK de la app o se efectúe un reseteo a fábrica [Ref.- 57], pero no si la app es desinstalada y reinstalada. Su valor también es diferentes para distintos usuarios, como si se tratara de dispositivos móviles distintos (multi-usuario). El comando que permite obtener el "ANDROID_ID" es:

```
$ settings get secure android_id
3483b1950b017ebe
```

Figura 27 - Obtención del ANDROID_ID

- GAID (*Google Advertising ID*): es un identificador único que se utiliza con fines de publicidad[12], y que el usuario puede restablecer mediante la opción "Ajustes - Google - Servicios - Anuncios - Restablecer ID de publicidad". ***Desde el punto de vista de privacidad, se recomienda activar el ajuste*** "Inhabilitar Personalización de Anuncios".

9.2 BATERÍA

Mantener un nivel de carga de batería adecuado afecta a la seguridad a la hora de garantizar la disponibilidad del dispositivo móvil en situaciones donde debe ser localizado. Para una información detallada sobre el modo de ahorro de batería, que Android empezó a potenciar desde Android 6 con el denominado proyecto "Doze", se

[12] https://support.google.com/googleplay/android-developer/answer/6048248?hl=es

recomienda la lectura del apartado "9.9. Ahorro de batería (Doze)" de la "Guía CCN-STIC-453E – Seguridad de dispositivos móviles: Android 7.x" [Ref.- 407]. Las recomendaciones generales para los ajustes que afectan al consumo de batería son:

- "Ahorro de batería": se recomienda establecer un valor de activación automática cuando se llegue al 15% de la carga para prolongar su duración, siendo conscientes de que ello limitará la actualización de datos de aplicaciones que ejecuten en segundo plano. Es posible establecer una lista de exclusión (o *whitelist*) que permite al usuario definir qué apps pueden saltarse parcialmente las políticas de ahorro de batería mediante "⋮" - "Optimización de batería", que mostrará la pantalla de "Sin optimizar"[13]. Desplegando el menú "Sin optimizar" y eligiendo "Todas las aplicaciones", aparecerán todas las apps instaladas, que se pueden seleccionar y marcar "No optimizar" para añadir la app a la lista de exclusión.
- "Porcentaje de batería": se recomienda activarlo para disponer del icono asociado al nivel de batería numérico en la barra superior de estado.
- "Brillo automático": activar para que se ajuste el nivel de brillo en función de la luz exterior.
- "Suspender después de": ***se recomienda fijar este valor*** (que apaga la pantalla del dispositivo móvil) ***a entre 1 y 2 minutos***.
- "Pantalla ambiente": permite ver una pantalla con fondo negro en la que se muestra la hora y los iconos de notificaciones al levantar el teléfono, pero sin necesidad de activar la pantalla. También incluyen el ajuste "Nuevas notificaciones", que activa la pantalla ante la recepción de una notificación.

En situaciones donde se constate que la duración de la batería es anormalmente baja, se recomienda seleccionar "Uso de la batería - "⋮" - Mostrar uso completo del dispositivo" para evaluar el comportamiento de las apps.

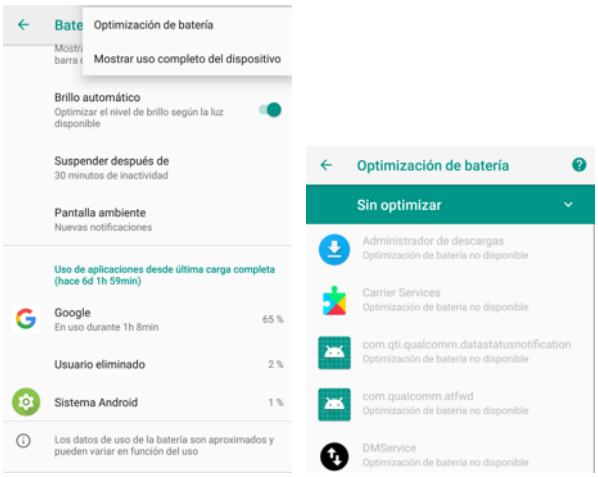

Figura 28 - Gestión y optimización de la batería

[13] En gris aparecen las apps que no pueden entrar en modo ahorro.

9.3 PANTALLA

Los ajustes de este apartado relacionados con la seguridad son:

- "`Suspender después de <X>`": este parámetro (que puede tomar valor de [15 segundos, 30 segundos, 1, 2, 5, 10 ó 30 minutos] determina cuándo se apagará la pantalla tras el tiempo de inactividad definido, y es muy relevante por influenciar directamente el ajuste "`Bloquear automáticamente`", que bloquea el dispositivo móvil hasta la introducción del código de acceso definido (ver apartado "10.1.1. Bloqueo de pantalla"). Buscando el equilibrio entre seguridad y usabilidad, ***se recomienda fijarlo a un máximo de 1 ó 2 minutos***, pero su valor dependerá de la política de seguridad de la organización y/o el usuario.
- "`[Avanzado] - Pantalla ambiente`": ver apartado ("9.2. Batería").

Android permite capturar la pantalla actual (*screenshot*) presionando simultáneamente los botones de encendido y bajar volumen.

9.4 SONIDO

Esta sección controla el volumen, los tonos, la vibración y la emisión de las señales acústicas relacionadas con el dispositivo móvil, aunque buena parte de estos ajustes pueden ser también definidos por la configuración particular de las apps. Adicionalmente, determina los parámetros relacionados con el modo "`No molestar`" (ver apartado "8.6.2. Interrupciones"). ***Se recomienda desactivar los ajustes*** "`Tonos del teclado`", "`Sonidos al tocar`" y "`Vibrar al tocar`", que provocan la emisión de un pequeño sonido y una respuesta táctil al interaccionar con el teclado, ***ya que pueden revelar la longitud de contraseñas*** (por ejemplo, del código de acceso al dispositivo).

9.5 ACCESIBILIDAD

Algunas funciones relacionadas con la accesibilidad suelen exponer más la información del dispositivo móvil desde el punto de vista de seguridad, por lo que se recomienda no habilitarlas salvo que la condición del usuario lo requiera. Se debe intentar evitar el uso del servicio "Talkback" [Ref.- 35] en la pantalla de bloqueo asegurándose de que el interruptor "`Función teclas volumen - Permitir en la pantalla de bloqueo`" está desactivado; este servicio permite interaccionar mediante voz con el dispositivo, reduciendo al mínimo la necesidad del teclado.

9.6 ALMACENAMIENTO

Proporciona información sobre el uso del almacenamiento del sistema tanto a nivel global como según diferentes categorías, incluyendo la distribución de uso del almacenamiento por parte de los demás usuarios existentes.

Pulsando sobre cada una de estas categorías se despliega la información sobre la utilización que cada app consume, y la categoría "Archivos", al seleccionarse, invoca al explorador de archivos, que permite acceder al almacenamiento a través de un sistema de navegación por carpetas, incluyendo la creación y eliminación de elementos en función de los permisos del sistema operativo (por ejemplo, la carpeta "Pictures - Screenshots" da acceso a las capturas de pantalla realizadas con el dispositivo).

La función "Almacenamiento inteligente" elimina de forma automática las fotografías y vídeos con antigüedad superior a uno, dos (opción por defecto) o tres meses y de las que se disponga de copia de seguridad a través de la app "Google Fotos". Se recomienda desactivar esta función para tener control sobre el contenido del dispositivo móvil en todo momento.

Android 8 introdujo la opción "liberar espacio", que analiza los contenidos del directorio "*Download*" (en el que se almacenan las descargas) y las apps que se usan de forma muy poco frecuente y propone al usuario el borrado y desinstalación de los mismos. Por defecto, todos los elementos detectados tras el escaneo están marcados para ser borrados una vez el usuario confirme a través de la opción "Liberar <nnn> MB".

Los dispositivos que soportan "A/B *seamless updates*" (ver apartado "5.1.1. A/B seamless updates"), al disponer de dos copias de las particiones de arranque y sistema, presentan una ocupación mayor del almacenamiento que los que no las soportan.

Para eliminar los datos de una app concreta, se ofrecen dos opciones a través del menú "Otras aplicaciones - <nombre de la app>":

- "Borrar caché": eliminación de los datos actualmente en caché pertenecientes a la app. Esta operación puede ser necesaria en ocasiones en las que el rendimiento de la app es anormalmente bajo y en las que se observa que el tamaño ocupado por la app en caché es elevado.
- "Administrar espacio" o "Borrar datos" (según la app): despliega un menú en el que, en función de la app, se puede seleccionar qué tipo de datos se desea eliminar o proceder al borrado completo, incluyendo ajustes, archivos generados durante la ejecución de la app, cuentas asociadas a ella, etc.

La correcta gestión del almacenamiento del dispositivo es importante desde el punto de vista del rendimiento, ya que un dispositivo con poco espacio libre resultará lento. Se recomienda supervisar cada cierto tiempo el uso de espacio y valorar la realización de tareas de liberación del mismo.

Aunque cada app dispone de su propio espacio de almacenamiento (dentro de su *sandbox*), una app puede solicitar permisos de lectura/escritura en el almacenamiento compartido (ver apartado "16.3. Permisos de las apps"), por lo que se recomienda ser cautelosos a la hora de otorgarlos.

10.SEGURIDAD Y UBICACIÓN

Este menú, que es accesible directamente del menú de "Ajustes", recoge los principales ajustes de seguridad y privacidad, especialmente en lo relativo al acceso tanto visual como de control de la configuración del dispositivo móvil. En los siguientes subapartados se describen las recomendaciones de seguridad asociadas a él.

La sección "[Estado de seguridad]" incluye información sobre la actualización de parches de seguridad instalados en el dispositivo, así como la configuración del servicio "Encontrar mi dispositivo", a través del cual Google permite al usuario geolocalizarlo en caso de extravío o robo. Dado que dicho servicio tiene como requisito la existencia de una cuenta de usuario de Google activa en el dispositivo, que no se contempla como parte de la presente guía, se recomienda consultar el apartado "10.4. Gestión remota de dispositivos Android por parte del usuario" de la "Guía CCN-STIC-456 - Cuenta de usuario, servicios y aplicaciones de Google para dispositivos móviles Android" [Ref.- 408], en la cual se describe dicho servicio detalladamente.

IMPORTANTE: la función "Encontrar mi dispositivo" está vinculada a la existencia del componente "Encontrar mi dispositivo" en la sección "Aplicaciones de admin. de disp." (al final de los ajustes del menú "Seguridad y ubicación"), que está asociado a un tipo de permiso especial. Las apps incluidas en esta sección tienen capacidad para gestionar el dispositivo de forma remota, independientemente de si su interruptor está o no activo, lo cual se constata viendo cómo se activa tras una operación como el intento de localización.

Por su parte, la configuración de "Google Play Protect" se describe en el capítulo "10.2. Verificación de seguridad de las apps: Google Play Protect" de la misma guía.

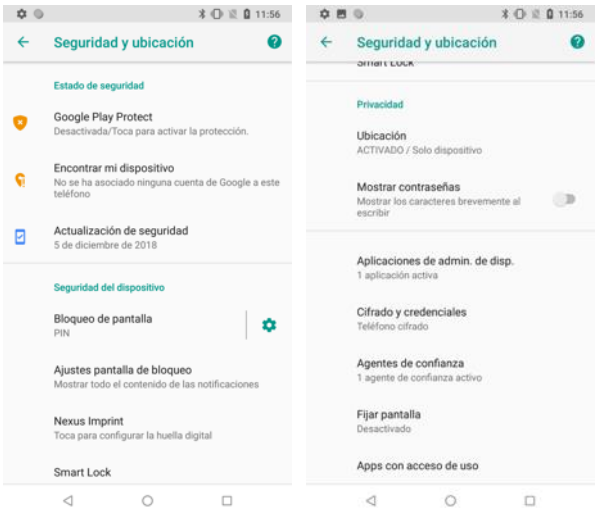

Figura 29 - Menú "Seguridad y ubicación"

10.1 SEGURIDAD DEL DISPOSITIVO

El elemento de seguridad más crítico es el acceso físico al dispositivo móvil, que permitiría a cualquier individuo controlar toda la funcionalidad y servicios disponibles. Desde el punto de vista de seguridad, ***se recomienda proteger los siguientes elementos***:

- Acceso a la tarjeta SIM, estableciendo un PIN que impida hacer uso de los servicios y capacidades de telefonía móvil del terminal. Si la tarjeta SIM está bloqueada, únicamente se permitirá la realización de llamadas de emergencia (número de teléfono 112). Aunque el dispositivo móvil permanecerá bloqueado mientras no se introduzca el PIN de la SIM, un potencial atacante podría extraerla y acceder al terminal.
- Bloqueo de pantalla: se basa en establecer un método de acceso que impida acceder directamente a las opciones de configuración del dispositivo móvil, a los datos del usuario y a las aplicaciones instaladas.

El PIN de la tarjeta SIM consiste en una secuencia numérica de mínimo 4 dígitos y máximo 8 (opción recomendada), que se puede fijar a través de "`Ajustes - Seguridad y ubicación - Bloqueo de tarjeta SIM`". ***Se recomienda activar la opción*** "`Bloquear tarjeta SIM`" ***y establecer un PIN robusto (si el actual no lo es) mediante*** "`Cambiar PIN de la tarjeta SIM`". Este PIN no debe contener dígitos fácilmente adivinables, como 0000, 1111, 1234, etc., ni ser el mismo que el PIN o código de desbloqueo de pantalla.

El PIN de la SIM solo es requerido al reiniciarse el dispositivo, ya que, una vez introducido, es almacenado en memoria, y no se solicita al salir del "`modo avión`".

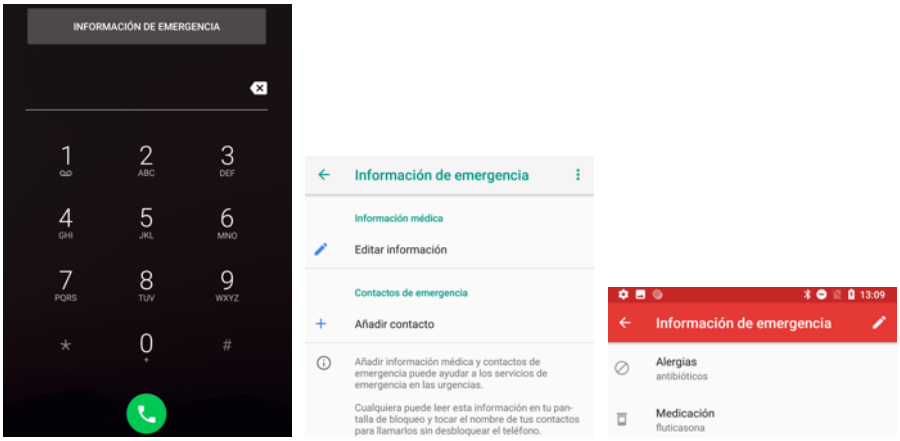

Figura 30 - Llamadas e información de emergencia

Para cursar llamadas de emergencia, se debe pulsar el texto "`Emergencia`" en la pantalla de bloqueo. Al activar esta pantalla, se mostrará el texto que se haya definido en la sección "`Ajustes - Usuarios y cuentas - Información de emergencia`", en la que también se puede añadir un contacto al que se desea se localice en caso de necesidad[14].

Android proporciona principalmente dos tipos de métodos de protección de acceso al propio dispositivo móvil: basados en el conocimiento de un código (PIN/patrón/contraseña) y basados en biometría (reconocimiento facial y/o huella dactilar digital), aunque no obliga a la existencia de uno salvo para determinadas funciones (como el almacenamiento de credenciales descrito en el apartado "19.

[14] A diferencia de lo que sucede en iOS 11.x y 12.x, en Android 8 la activación del modo de llamadas de emergencia no desactiva las capacidades de desbloqueo por biometría.

Almacén de credenciales"). Desde el punto de vista de seguridad, ***es fundamental disponer de un método o código de acceso robusto al dispositivo móvil y, en la medida de lo posible, prescindir de métodos de desbloqueo automático*** (descritos en el apartado "10.1.2. Desbloqueo mediante "Smart lock""").

Se recomienda deshabilitar la opción `"[Privacidad] - Mostrar contraseñas"` para impedir que los caracteres se muestren brevemente durante su introducción.

10.1.1 BLOQUEO DE PANTALLA

Los ajustes recomendados desde el punto de vista de seguridad para el bloqueo de la pantalla del dispositivo móvil, accesibles desde el símbolo de engranaje son:

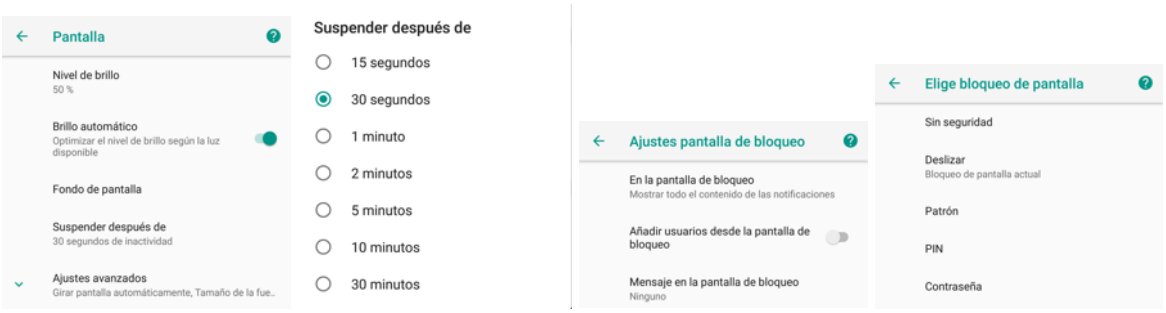

Figura 31 - Opciones de bloqueo de pantalla

- `"Bloquear automáticamente"`: este valor controla cuanto tiempo después de que se haya apagado la pantalla debido al ajuste `"Pantalla - Suspender después de…"` se activará el bloqueo de la pantalla. El rango razonable para `"Suspender después de"`, buscando el equilibrio entre seguridad y usabilidad, es de 1 ó 2 minutos, pero debe ser definido por la política de seguridad de la organización propietaria del dispositivo móvil. El valor para `"Bloquear automáticamente"` se aconseja que sea de entre 5 y 30 segundos.
- `"Bloquear al encender/apagar"`: ***se recomienda activar este interruptor*** para que, si el usuario apaga la pantalla mediante el botón de encendido, se solicite el código de acceso para desbloquearla. Esta opción no se tendrá en cuenta si se cumple alguna condición de desbloqueo definida por *Smart Lock*.
- `"Mensaje en la pantalla de bloqueo"`: este mensaje se muestra cuando la pantalla se encuentra bloqueada, que puede ser útil, por ejemplo, en caso de pérdida del dispositivo móvil. ***Se recomienda proporcionar un mensaje descriptivo*** que, sin desvelar información sensible, crítica, o que pueda ayudar a identificar detalles innecesarios del propietario, permita contactar con él. Un ejemplo sería: "*Si encuentra este teléfono, por favor, llame al número +34 987654321*".
- Si se ha optado por definir un patrón de desbloqueo, esta sección mostrará la opción `"Mostrar el patrón dibujado"`, que ***se recomienda desactivar***, a fin de impedir que el patrón se dibuje en la pantalla de bloqueo al ser introducido.

El tipo de bloqueo se muestra en la parte inferior central de la pantalla de bloqueo:

- "sin seguridad" (totalmente desaconsejado): la pantalla se muestra en negro.
- "deslizar" (totalmente desaconsejado): se representa por un candado abierto.
- "PIN, Patrón y Contraseña": se representan con un candado cerrado.
- "Huella digital": se representa con un símbolo de huella dactilar.
- "Condición de desbloqueo de Smart Lock": candado abierto encerrado en un círculo.

A fin de minimizar el éxito de los ataques de adivinación por fuerza bruta, si la introducción de un código de acceso basado en PIN, contraseña o patrón fracasa tras 5 intentos consecutivos, el dispositivo bloqueará la posibilidad de introducirlo de nuevo durante 30 segundos. Si, transcurrido este plazo, volviesen a realizarse 5 intentos de acceso fallidos, se volverá a establecer el plazo de 30 segundos en los que el dispositivo no permite la introducción del código. A partir del undécimo intento fallido, el plazo de 30 segundos se mantendrá por cada nuevo intento de desbloqueo que no tenga éxito.

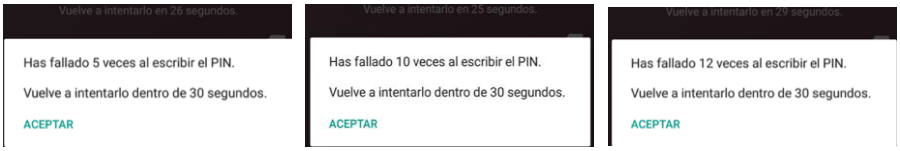

Figura 32 - Inserción de un PIN o código de acceso incorrecto

Durante la configuración del PIN/patrón/contraseña, se solicitará al usuario si desea habilitar el "Inicio seguro", que hará que se solicite el código de acceso definido para proceder a descifrar la partición de datos al reiniciarse el dispositivo, evitando que se puedan recibir llamadas, mensajes o notificaciones (ver apartado "20. Cifrado del dispositivo móvil"). ***Se recomienda aceptar esta opción para evitar la exposición de la información sensible en caso de pérdida o robo del dispositivo***. Aunque hasta Android 7 este ajuste se podía controlar de forma independiente mediante el interruptor "Ajustes - [Personal] Seguridad - Inicio seguro [Seguridad del dispositivo] Bloqueo de pantalla - [Tipo de bloqueo] - Inicio seguro", en Android 8 desaparece y solo se puede desactivar/reactivar realizando algún cambio en el método o código de acceso.

No existe ningún mecanismo para recuperar un código de acceso olvidado. Si ello ocurriera, la única opción para volver a tener acceso al terminal es restablecer los ajustes de fábrica (ver apartado "22. Eliminación de datos del dispositivo móvil") y volver a configurar el dispositivo móvil.

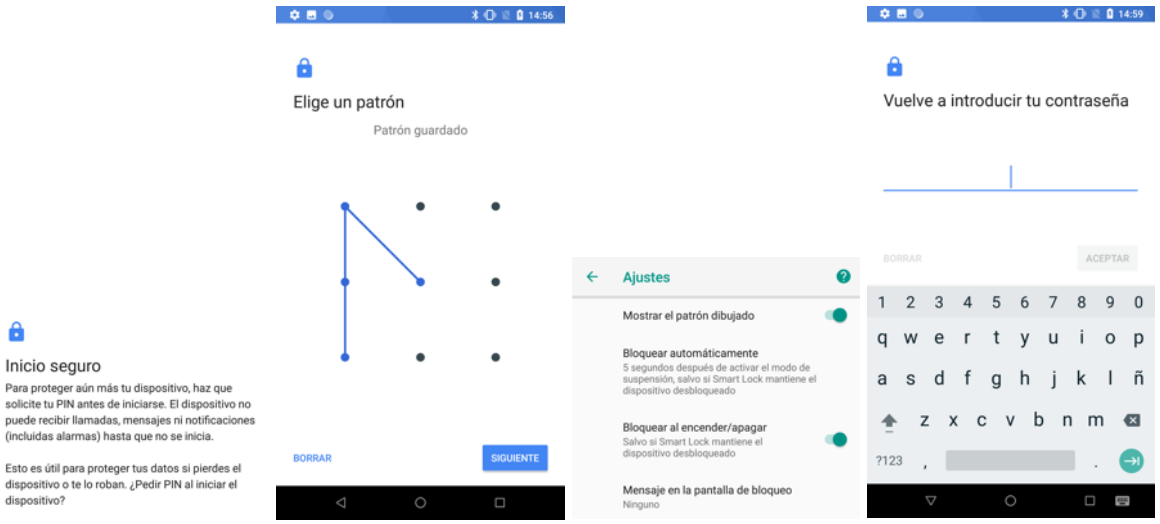

Figura 33 - Configuración del método o código de acceso

PIN

PIN o código numérico tradicional, compuesto por un mínimo de cuatro dígitos y un máximo de 16 (siendo recomendable hacer uso de al menos 8 dígitos). Su longitud no se desvela en la pantalla de bloqueo.

PATRÓN

Está formado por una secuencia de movimientos realizados sobre una matriz de 3x3 puntos, que debe de comprender un mínimo de 4 y un máximo de 9 puntos conectados o enlazados sin interrupción. El número máximo de combinaciones para el patrón de desbloqueo es 389.112[15], muy inferior a 10^8 (100.000.000) para un PIN de 8 dígitos, aunque superior a las 10.000 (10^4) de un PIN de 4 dígitos. Asimismo, se han publicado estudios que indican que, grabando con una cámara a un usuario que introduce su patrón, es posible obtenerlo en un número muy reducido de intentos[16].

En caso de elegirse el uso de un patrón, se desaconseja emplear aquéllos que correspondan con las iniciales del usuario o con letras del abecedario, práctica que resulta muy común. Asimismo, debe desactivarse la opción "`Mostrar el patrón dibujado`", descrita anteriormente. Esta opción no impide que el dispositivo emita una leve vibración acompañada de un sonido mientras el usuario dibuja el patrón en la matriz de 3x3 puntos de la pantalla de bloqueo, lo cual puede permitir a un potencial atacante saber cuántos puntos integran el patrón.

IMPORTANTE: durante el establecimiento del patrón, el mismo se muestra (y queda fijo) en pantalla, independientemente del valor de la opción "`Mostrar el patrón dibujado`". Por ello es fundamental realizar este paso sin que ningún tercero disponga de acceso visual a la pantalla.

CONTRASEÑA

[15] https://www.quora.com/Android-operating-system-How-many-combinations-does-Android-9-point-unlock-have/answer/Yoyo-Zhou

[16] http://www.lancaster.ac.uk/staff/wangz3/publications/ndss_17.pdf

Consiste en una secuencia alfanumérica de entre 4 y 16 caracteres (incluyendo, si se desea, letras minúsculas, mayúsculas, dígitos y símbolos de puntuación) por lo que ***se considera la opción más recomendada desde el punto de vista de seguridad***, siempre que se utilice una combinación robusta y de al menos 8 caracteres.

HUELLA DACTILAR DIGITAL (IMPRINT)

En los dispositivos equipados con lector de huellas, es posible registrar hasta 5 huellas dactilares digitales en el sistema de autentificación mediante huella (Imprint o Nexus Imprint). Un *Keystore* implementado por hardware es el responsable de almacenar la representación digital de las huellas, cuyos datos deben estar cifrados y firmados, y no ser accesibles fuera del TEE (*Trusted Execution Environment*) [Ref.- 27]. Las apps que hagan uso del reconocimiento de la huella para realizar acciones de validación no dispondrán en ningún caso de acceso a la representación de la huella dactilar digital del usuario, sino que lo harán a través del sistema operativo, el cual, en función de la respuesta que obtenga del TEE, proporcionará a la app un token de notificación de aceptación o de rechazo de la huella introducida por el usuario.

Los mecanismos basados en biometría se consideran menos seguros que un PIN o contraseña robustos, y requieren de la existencia de un método de acceso de respaldo que se solicitará al usuario en los siguientes escenarios [Ref.- 26]:

- Tras 5 intentos fallidos de reconocimiento de la huella.
- Al reiniciar el dispositivo móvil.
- Al cambiar de usuario en el dispositivo móvil (en escenarios multi-usuario).
- Tras 48 horas sin haber desbloqueado el dispositivo móvil con el método de respaldo.
- Para realizar cambios en la configuración del método de acceso (incluyendo la adición/eliminación de huellas): esto evita que un tercero con acceso temporal no autorizado al dispositivo móvil pueda registrar una nueva huella dactilar digital sin conocer el método de respaldo, aunque el dispositivo estuviese desbloqueado.
- Para añadir/eliminar certificados digitales a través del menú "`Cifrado y credenciales`" (ver apartado "19. Almacén de credenciales").
- Para acceder al menú de opciones "`Smart Lock`".

El menú "`Nexus Imprint`" presenta el interfaz de configuración de la huella, que guía al usuario en el proceso de alta de la misma. Cada huella dactilar digital creada se denomina "`Dedo X`" (1<X<5), puede renombrarse pulsando sobre su entrada y borrarse mediante el icono "🗑". El método de desbloqueo mediante huella quedará desactivado cuando se eliminen las entradas de todas las huellas dadas de alta. 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.

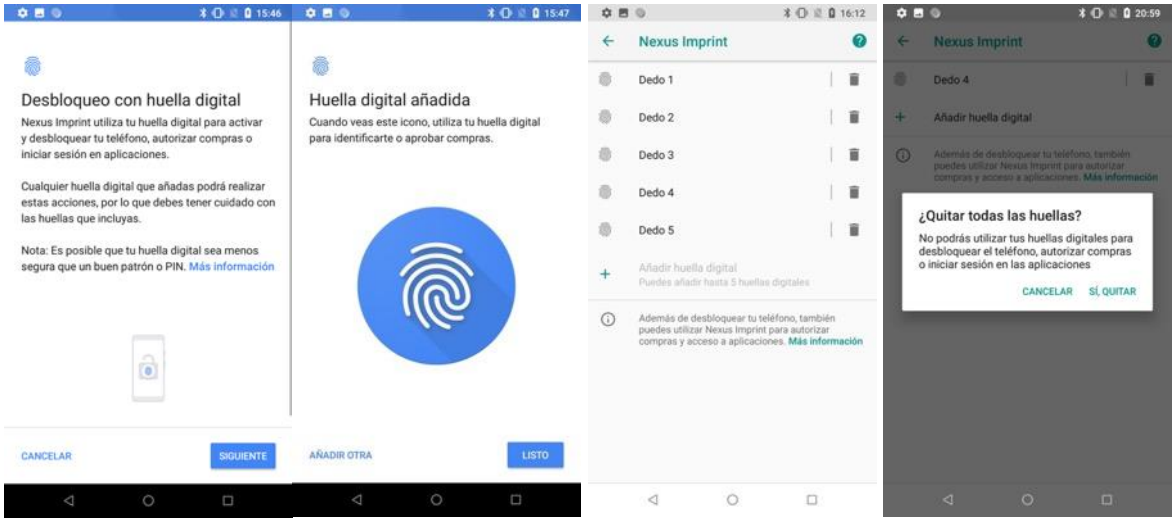

Figura 34 - Desbloqueo con huella dactilar digital

10.1.2 DESBLOQUEO MEDIANTE "SMART LOCK"

Smart Lock es una funcionalidad que permite que el dispositivo móvil se mantenga desbloqueado en determinadas circunstancias (por ejemplo, en una ubicación configurada por el usuario, o si está conectado a un dispositivo Bluetooth de confianza), a pesar de que se cumplan otras condiciones de bloqueo, como el tiempo de inactividad. 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).

Smart Lock se basa en el concepto de "Agentes de confianza", que son componentes del sistema que evalúan el entorno y, si lo consideran favorable según sus criterios, relajan la seguridad del dispositivo. Estos agentes se listan en el menú "`Ajustes - Seguridad y ubicación - Agentes de confianza`", y, por defecto, el de Google se encuentra habilitado. Desde el punto de vista de seguridad, ***se desaconseja el uso de la funcionalidad Smart Lock***, que, si bien aporta comodidad de uso, limita el control que el usuario tiene sobre la situación de bloqueo del dispositivo móvil. Para ello, lo más recomendable es desactivar el agente de confianza "`Smart Lock (Google)`".

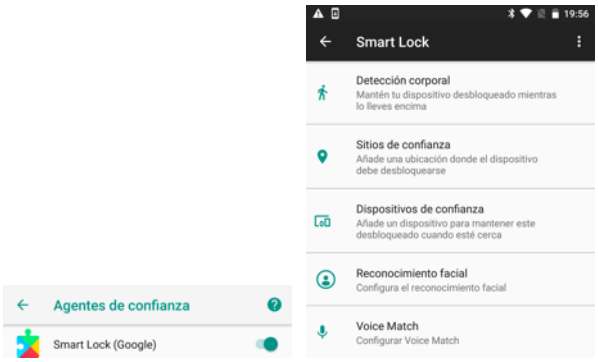

Figura 35 - Smart Lock

La configuración de Smart Lock requiere la introducción del método de acceso vigente en el dispositivo móvil, y se ofrecen diferentes opciones de desbloqueo, configurables de forma independiente:

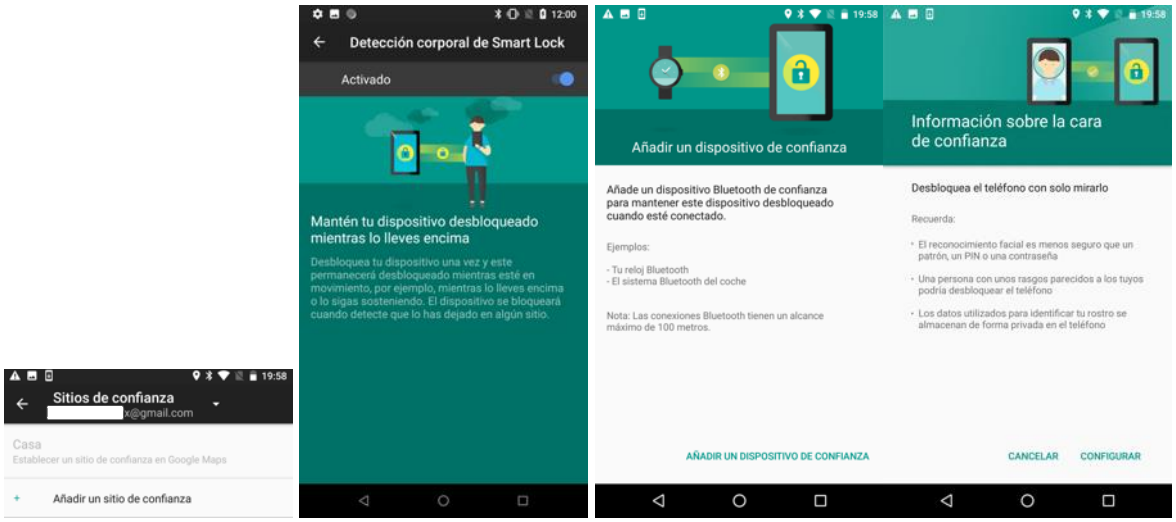

Figura 36 - Opciones de Smart Lock

- "`Detección corporal`": mantiene el dispositivo móvil desbloqueado mientras detecta movimiento del usuario, pero no puede distinguir si es él quien lo porta o un tercero; desde el punto de vista de seguridad, ***se desaconseja su uso***.
- "`Sitios de confianza`": mantiene el dispositivo móvil desbloqueado cuando detecta que se encuentra en una ubicación que el usuario ha definido como de confianza, típicamente, su domicilio o su lugar de trabajo. Este método está disponible únicamente para dispositivos móviles que cuentan con un módulo GPS integrado y requiere que la ubicación esté activada. El dispositivo no se desbloqueará al entrar en el radio de proximidad del sitio de confianza[17], sino que únicamente se mantendrá desbloqueado si lo estaba y ya se encontraba en una ubicación de confianza, y mientras permanezca dentro de ésta. Este método no puede impedir que un tercero pueda acceder al dispositivo móvil dentro del radio de confianza, por lo que ***se desaconseja su uso***, especialmente en lugares de acceso público. También se desaconseja por la viabilidad de la manipulación de las señales de ubicación mediante equipos especializados, que permiten suplantar la señal de los satélites GPS.
  El registro de un nuevo sitio no requiere que la ubicación esté activada, pero sí se precisa disponer de conectividad de datos (móviles o Wi-Fi) para permitir la introducción de las coordenadas en el mapa de Google Maps[18].

[17] 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 (aproximadamente).

[18] Si existe una cuenta de usuario de Google activa en el dispositivo móvil (ver apartado "Cuenta de usuario de Google" de la "Guía CCN-STIC-456 - Cuenta de usuario, servicios y aplicaciones de Google

- "`Dispositivos de confianza`": mantiene el dispositivo móvil desbloqueado mientras la conexión con el dispositivo Bluetooth designado de confianza esté activa. Previamente debe haberse establecido un emparejamiento entre ambos. De hecho, cualquier vinculación entre el dispositivo móvil y un dispositivo Bluetooth provocará que salte una notificación invitando al uso de la funcionalidad de desbloqueo Smart Lock. ***Se desaconseja especialmente la designación de dispositivos de confianza que acompañen al dispositivo,*** por ejemplo, auriculares que se guarden en el mismo maletín o ubicación.
- "`Reconocimiento facial`": permite desbloquear un dispositivo móvil al reconocer (mediante la cámara frontal) un rostro registrado previamente. 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. ***Se desaconseja debido a que no se puede garantizar su fiabilidad ante un tercero con rasgos similares a los del usuario, o ante el uso de una fotografía***. Adicionalmente, basta con que el usuario mire brevemente a la cámara, aun involuntariamente, para que el terminal se desbloquee.
- "`Voice Match`" (Reconocimiento de voz): permite desbloquear el dispositivo móvil en base al servicio "`Ok Google`" (requiere, al igual que los "`Sitios de confianza`", que haya una cuenta de usuario de Google activa en el dispositivo).

IMPORTANTE: la indicación de desbloqueo del dispositivo debida a una condición propia de la funcionalidad *Smart Lock* se identifica a través de un símbolo de candado abierto que parpadea en la pantalla de inicio ( ). En caso de que se desee suprimir temporalmente la condición de desbloqueo, se puede realizar una pulsación sobre el candado, lo que hará necesario hacer uso del código de acceso para desbloquear de nuevo el dispositivo móvil.

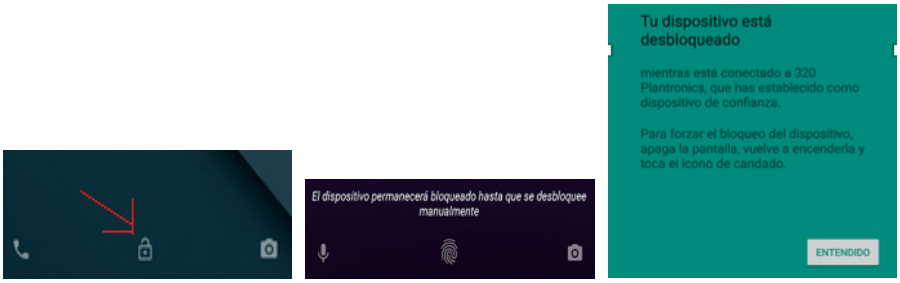

Figura 37 - Indicación de dispositivo desbloqueado por Smart Lock

El desbloqueo debido a la funcionalidad *Smart Lock* se suprime tras 4 horas o si el dispositivo es reiniciado. Dado que la indicación de dispositivo desbloqueado a causa de *Smart Lock* en la pantalla de inicio es muy sutil, puede ocurrir que el usuario no sea consciente de esa situación y se despreocupe. Al desplegar la pantalla de inicio en esa circunstancia, se mostrará un mensaje que informa de la condición que se cumple.

para dispositivos móviles Android" [Ref.- 408]), los sitios de confianza serán asociados a dicha cuenta, por lo que estarán disponibles de forma global en todos los dispositivos móviles vinculados a ella.

10.1.3 AJUSTES DE LA PANTALLA DE BLOQUEO

Este apartado establece ajustes complementarios que afectan a la funcionalidad disponible en la pantalla de bloqueo, ilustrados en la imagen derecha de la <Figura 31>. Los ajustes recomendados desde el punto de vista de seguridad son:

- "`En la pantalla de bloqueo`": determina la información relativa a las notificaciones que se mostrará con el dispositivo bloqueado (ver apartado "8.6. Notificaciones"). ***Se recomienda marcar*** "`No mostrar notificaciones`" o, cuando menos, "`Ocultar contenido sensible`".
- "`Añadir usuarios desde la pantalla de bloqueo`": ***se recomienda dejarla desmarcada*** (ver apartado "10.2. Perfiles de usuario").

Figura 38 - Ajustes del menú "Power" en la pantalla de bloqueo

10.1.4 FIJAR PANTALLA

La funcionalidad "`Fijar pantalla`" (*Screen pinnning*) permite que el usuario pueda dejar en primer plano una aplicación para ser utilizada sin que sea posible cambiar a otra app distinta, ni recibir notificaciones. Por tanto, esta funcionalidad es muy conveniente en entornos educativos y en quioscos, pero también si, puntualmente, se debe prestar el dispositivo móvil a un tercero para un uso concreto (como realizar una llamada de teléfono con urgencia, o acceder al navegador web puntualmente).

Al activarla, ***se recomienda seleccionar*** "`Solicitar PIN para desactivar`", de forma que no sea posible acceder al resto de funcionalidades sin validar el método de acceso.

Para fijar una pantalla, se debe abrir la app a fijar, pulsar el botón de aplicaciones recientes "▣", y desplazar la barra del título de la app hasta ver el símbolo "📌" en el margen inferior derecho. Al pulsarlo, la pantalla quedará fija. Para dejar de fijar la pantalla, se pulsarán simultáneamente los botones y "◁" (retroceso) y "▣".

10.2 PERFILES DE USUARIO

Los perfiles de usuario permiten la utilización del dispositivo móvil por más de un usuario. Cada usuario existente en el dispositivo puede personalizar la pantalla de inicio, los complementos (*widgets*), las aplicaciones móviles (apps) y ciertos ajustes de la configuración (como el método de desbloqueo, la red Wi-Fi, etc.), y dispone de un

entorno separado, incluyendo almacenamiento separado en la tarjeta de almacenamiento externa (o tarjeta SD, en caso de existir), mediante emulación.

La gestión de usuarios y perfiles restringidos está disponible a través del menú "`Ajustes - Usuarios y cuentas`" (el usuario activo aparece en este menú como "`Tú`"), así como desde la barra de ajustes rápidos, representado mediante el icono circular con una silueta (el usuario activo se lista en primera posición, rodeado por una línea circular).

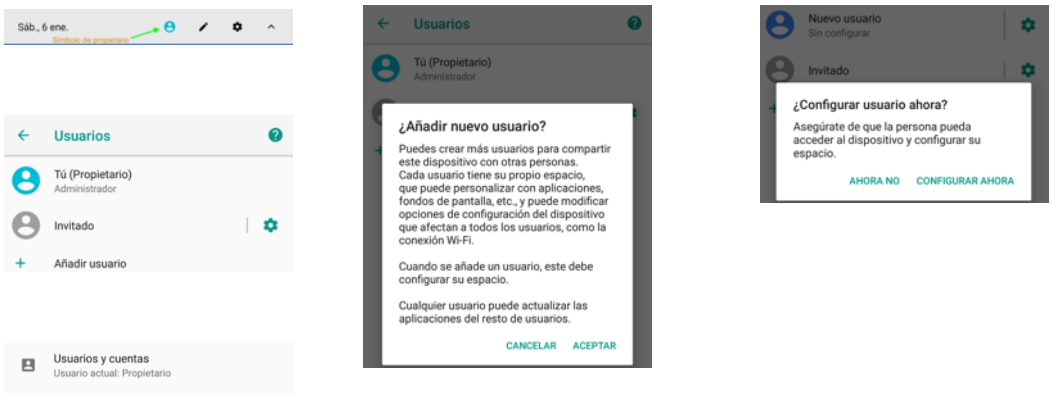

Figura 39 - Identificación del usuario activo en el dispositivo móvil

Existen tres tipos de perfil de usuario:

- "`Propietario`" (*owner*): corresponde al usuario principal, existente por defecto, con rol de administración sobre el resto de perfiles y control completo del dispositivo móvil. Se identifica con el texto correspondiente al nombre del usuario proporcionado durante la configuración inicial (si no se definió un nombre para el usuario, aparecerá el texto "`Propietario`"), pudiéndose modificar el nombre pulsando sobre su entrada. El propietario puede añadir otros usuarios mediante el botón "`+ Añadir usuario`".
- "`Usuario`": este perfil tiene la capacidad de realizar una configuración personalizada del dispositivo, incluyendo la instalación de apps y el alta de su propia cuenta de usuario de Google. Cuando accede por primera vez, el sistema le solicitará iniciar la configuración inicial de su entorno, de forma similar a la descrita para el propietario en el apartado "6. Configuración inicial del sistema operativo Android", incluyendo, si lo desea, el establecimiento de un código de acceso propio. Se puede limitar el acceso a llamadas y envío de SMS a este tipo de usuarios a través de la opción "`Activar llamadas y SMS`" del menú de configuración correspondiente al usuario, accesible mediante el icono "⚙".

  Para eliminar un usuario existente en el dispositivo, se debe acceder al menú "`Usuarios y cuentas`", pulsar el botón de engranaje y seleccionar "`Quitar usuario`".

- "`Invitado`" (*guest*): este perfil se crea tras ser accedido por primera vez por el "`Propietario`", y aparecerá en la barra de ajustes rápidos. Android no presenta al usuario invitado ninguna indicación para que configure un método de acceso propio, lo que permite que cualquier individuo que disponga de acceso físico al dispositivo pueda entrar con este perfil. Por ello, ***se recomienda al usuario propietario acceder como invitado y fijar un método de acceso específico antes de permitir a un tercero la utilización de este perfil***. El invitado no tiene permisos para añadir redes Wi-Fi, pero sí puede cambiar ajustes del sistema, algunos tan importantes como activar/desactivar la ubicación, el interfaz Bluetooth (incluyendo emparejamiento con nuevos dispositivos) y el modo avión. Algunos de estos ajustes persistirán cuando se salga del modo invitado (como el modo avión), mientras que otros se devuelven al estado definido por el usuario al que se cambie. Se puede limitar el acceso a las llamadas mediante el interruptor "`Activar llamadas`" del menú de configuración del usuario invitado.
  Para eliminar al usuario invitado, es preciso acceder a la lista de usuarios desplegando el menú de ajustes rápidos, seleccionar el icono "" y pulsar en "`Quitar invitado`".

La utilización de múltiples perfiles de usuario está desaconsejada desde el punto de vista de seguridad, si bien puede resultar preferible habilitarla momentáneamente en caso de que, por una circunstancia ineludible, sea preciso prestar el dispositivo móvil a un tercero, en vez de prestarlo utilizando el perfil del propietario. Una vez haya cesado la circunstancia que dio lugar a la necesidad de habilitar otros usuarios, ***se recomienda eliminarlos del sistema***. La eliminación de un usuario conlleva la eliminación de los datos y aplicaciones asociados.

Se recomienda mantener desactivada la opción "`Añadir usuarios desde la pantalla de bloqueo`", a fin de evitar que pueda darse acceso al terminal a terceros sin control por parte del propietario.

Un claro ejemplo del riesgo que implica disponer de usuarios adicionales es que, al igual que para el usuario principal, Android no obliga a que los demás usuarios establezcan un código de bloqueo del dispositivo móvil. Si, estando la pantalla bloqueada por el propietario, otro usuario solicita acceso mediante el menú de ajustes rápidos y este usuario no ha definido un código de acceso, podrá desbloquear el dispositivo y entrar en su perfil. Esto implicaría que cualquier persona con acceso físico al dispositivo móvil podría utilizar dicho perfil.

Android facilita la utilización de perfiles de trabajo para permitir a las organizaciones gestionar los datos y apps corporativos de forma independiente de los personales. Para ello es preciso disponer de una app que actúe de controlador de las políticas de gestión empresarial de dispositivos móviles o EMM (*Enterprise Mobility Management*) [Ref.- 33], cuyo análisis queda fuera del alcance de la presente guía.

10.3 SERVICIOS DE LOCALIZACIÓN

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), o de Bluetooth, pueden ser activadas y desactivadas por el usuario en función de su utilización. La configuración habilitada por defecto dependerá de las opciones seleccionadas en la pantalla de "Servicios de Google" durante el proceso inicial de instalación y configuración del dispositivo móvil (ver <Figura 15>). El módulo GPS estará activo únicamente cuando se está haciendo uso de una app que utilice los servicios de localización de Android, lo cual se indica en la barra superior de estado mediante el icono "", pero no se representa mediante ningún indicador el estado de activación de los servicios de ubicación salvo en ese caso, lo cual dificulta que el usuario sea consciente de cuál es ese estado.

Además de a través del interruptor "[Ubicación] Activado", en función de su configuración, es posible activar/desactivar el servicio a través del menú de ajustes rápidos (ver apartado "8.3. Menú de ajustes rápidos").

La configuración de los servicios de ubicación está bajo la sección "[Privacidad] Ubicación", entre los que se encuentran:

- "Modo": permite seleccionar los recursos que se utilizarán para obtener la ubicación, que incluyen "Alta precisión" (hace uso del módulo GPS, de las conexiones Bluetooth, 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), "Ahorro de batería" (excluye el uso del módulo GPS para el cálculo) y "Solo dispositivo" (uso exclusivo del módulo GPS). Desde el punto de vista de seguridad, ***se recomienda seleccionar "Solo en dispositivo"***, pues las demás conllevan el intercambio de información con los servicios de Google [Ref.- 36].
- "Permisos de las aplicaciones": permite otorgar/revocar el acceso a los servicios de localización a nivel de aplicación, por lo que ***conviene revisar la lista de apps que lo tienen concedido y eliminarlo de las que, por su cometido, no lo requieran***. Son muchos los servicios y apps que, sin estar dirigidos a proporcionar servicios de ubicación, tratan de acceder y utilizar la información de localización del dispositivo móvil, como "Google Fotos", el buscador de Google, o el navegador web Chrome (si se desea obtener más información al respecto, consultar el capítulo "11. Localización (o ubicación) geográfica" de la "Guía CCN-STIC-456 – Cuenta de usuario, servicios y aplicaciones de Google para dispositivos móviles Android" [Ref.- 408].

- "Búsqueda": ofrece dos opciones para permitir/denegar la búsqueda de redes Wi-Fi y Bluetooth, independientemente del estado que el usuario haya definido para los respectivos interfaces, a fin de mejorar los servicios de localización. ***Se recomienda desactivar ambas opciones***, que realizarán periódicamente escaneos Wi-Fi y/o Bluetooth, para evitar comunicaciones inalámbricas indeseadas[19].
- "Servicios de ubicación": para la funcionalidad "Compartir ubicación en Google" e "Historial de ubicaciones de Google", se requiere disponer de una cuenta de usuario de Google activa en el dispositivo, por lo que, si se desea información sobre ambas, se recomienda consultar los capítulos "11.2. Google Maps" y "11.5 Historial de ubicaciones" de la "Guía CCN-STIC-456 - Cuenta de usuario, servicios y aplicaciones de Google para dispositivos móviles Android" [Ref.- 408].

La activación del modo avión de Android deshabilitará los servicios de ubicación de Google, no permitiendo ninguna transmisión inalámbrica de datos con las redes Wi-Fi o de telefonía móvil, ni con otros dispositivos Bluetooth, pese a que el módulo GPS sí sigue activo en el dispositivo empleado para la elaboración de la presente guía (puede no ser así en otros modelos de dispositivo móvil).

11.CUENTAS ASOCIADAS AL DISPOSITIVO MÓVIL

El usuario puede añadir diferentes cuentas a través del menú "Usuarios y cuentas", que irán ligadas a su perfil (ver apartado "10.2. Perfiles de usuario"), mediante la opción "Añadir cuenta". A través de este menú, además de la configuración de las diversas cuentas, en esta sección se puede establecer:

- "Información de emergencia", incluyendo los contactos que se mostrarán cuando se acceda a una llamada de emergencia (ver <Figura 30>).
- "Sincronizar datos automáticamente": este ajuste controla que las apps puedan actualizar los datos de sus respectivas cuentas. Si se desactiva, solo se podrá realizar una sincronización manual.
- "Añadir usuarios desde la pantalla de bloqueo": ***se aconseja deshabilitar esta opción,*** que permitiría que cualquier tercero con acceso físico al dispositivo pudiera dar de alta un usuario en el sistema sin ninguna validación previa.

Se permite añadir cuentas de Microsoft Exchange, y de cualquier servicio IMAP y POP3.

[19] Existen estudios pasados que reflejan que la información de localización intercambiada entre el dispositivo móvil Android y Google no es completamente anónima (http://on.wsj.com/gDfmEV), pues, además de incluir detalles de las señales de las redes inalámbricas recibidas y la ubicación del terminal, se incluye un identificador único del dispositivo móvil, lo cual puede afectar a la privacidad del usuario.

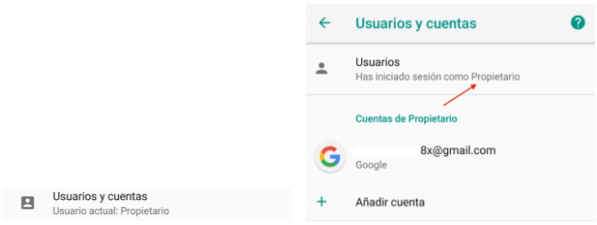

Figura 40 - Configuración de las cuentas para un usuario

11.1 CUENTA DE GOOGLE

La cuenta de usuario de Google permite (y es requerida) para acceder a todos los servicios de Google. 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 activación de dicha cuenta, determinados servicios básicos no estarán disponibles sin ella, como la instalación y actualización de apps del mercado oficial "Play Store" o la funcionalidad para localizar un dispositivo extraviado mediante el servicio "Encontrar mi dispositivo" (ver apartado "10.4. Gestión remota de dispositivos Android por parte del usuario" de la "Guía CCN-STIC-456 - Cuenta de usuario, servicios y aplicaciones de Google para dispositivos móviles Android" [Ref.- 408]). Al dar de alta la cuenta de usuario de Google en un dispositivo móvil, el mismo pasará a formar parte de los dispositivos pertenecientes al propietario de la cuenta, y podrá ser usado como segundo factor de autentificación para iniciar sesión en ella.

Un mismo dispositivo puede contar con varias cuentas de usuario de Google, y las distintas apps de Google permiten indicar en sus ajustes cuál de ellas se empleará para acceder al servicio correspondiente. Debido a la sensibilidad de la información asociada a la cuenta que Google almacena, el control no autorizado sobre ella por parte de un tercero tiene un impacto elevado, no solo de cara al propio dispositivo móvil, sino de cara a la seguridad y privacidad del propietario. Por tanto, si se opta por habilitar dicha cuenta, deben extremarse los mecanismos de protección sobre la misma.

Por su parte, desde Android 8 se mejora la seguridad impidiendo el acceso a la lista de cuentas registradas en el dispositivo por parte de las apps en base al permiso GET_ACCOUNTS, y, en su lugar, se traslada al usuario la concesión de este permiso mediante un menú de diálogo[20]. Por ello, ante una solicitud de selección de cuenta por parte de una app, se debe sopesar la necesidad de otorgarlo.

Con las diferentes versiones de Android las mejoras e incrementos de funcionalidad del dispositivo van estrechamente ligadas a los servicios de Google que, a su vez, cada vez almacenan y gestionan información más sensible del usuario. Desde el punto de vista de seguridad y privacidad, ***se recomienda prescindir de la cuenta de usuario de Google en el dispositivo***. En caso de requerirse hacer uso de ella para determinados servicios, se recomienda aplicar las recomendaciones descritas en la

[20] Alternativamente, las apps pueden usar el método "AccountManager#newChooseAccountIntent()", asociado a un intent, para obtener acceso a una cuenta de usuario.

"Guía CCN-STIC-456 - Cuenta de usuario, servicios y aplicaciones de Google para dispositivos móviles Android" [Ref.- 408] y, siempre que sea posible, especialmente si se comparte el dispositivo con otros usuarios, ***proceder a cerrar la sesión para minimizar los riesgos de que un tercero logre acceso a ella***. Para cerrar sesión, es preciso acceder a "`Ajustes - Google - Aplicaciones conectadas - Android device - Desconectar`".

En el caso de dispositivos multi-usuario (ver apartado "10.2. Perfiles de usuario"), es posible definir una cuenta para cada usuario existente en el sistema, de modo que la sesión activa sea la determinada por el usuario que actualmente use el dispositivo. En caso de utilización de un dispositivo móvil ajeno que requiera dar de alta la propia cuenta en el mismo, ***se recomienda proceder a eliminarla del sistema tan pronto se deje de usar dicho dispositivo***.

Es posible otorgar permiso a otras apps para conectarse a la cuenta de usuario de Google y hacer uso de sus servicios, por ejemplo, a clientes de correo para acceder a la cuenta de Gmail. Para saber qué aplicaciones emplean este mecanismo, se puede acceder al menú "`Ajustes - Google - Aplicaciones conectadas`". Si se detecta alguna app que no debería tener este acceso, es posible desactivarla seleccionando la app y marcando "`Desconectar`".

12. RED E INTERNET

Los dispositivos móviles basados en Android hacen uso de diferentes tecnologías inalámbricas que proporcionan la conectividad necesaria de voz y datos. En Android 8, este menú alberga la configuración de las redes Wi-Fi, datos móviles y VPN. La protección de los interfaces de red es especialmente importante, ya que la mayor parte de información gestionada por el dispositivo pasa a través suyo. De manera general, desde el punto de vista de seguridad, ***se recomienda mantener desactivados todos los interfaces de comunicaciones que no estén siendo requeridos en un momento concreto***.

12.1 MODO AVIÓN

La activación del modo avión deshabilita todos los interfaces de comunicaciones inalámbricos del dispositivo, pero deja activo el módulo GPS, por lo que sigue siendo posible usar apps de ubicación desde el propio dispositivo a través de los satélites. El modo avión es la única alternativa para inhabilitar temporalmente las capacidades de telefonía móvil de voz y SMS.

Al salir del modo avión se restaurará el estado de los interfaces Wi-Fi, Bluetooth y datos al valor de activación que tuviesen con anterioridad a entrar en dicho modo.

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; al igual que el interfaz Wi-Fi).

Para activar el modo avión, se dispone del menú "`Redes e Internet - Modo avión`" y del menú de ajustes rápidos (aunque se recomienda eliminar este acceso

directo de dicho menú, según se indica en el apartado "8.3. Menú de ajustes rápidos"). El estado de activación de este ajuste se indica mediante el icono "✈" de la barra de estado y en el menú principal del menú "Ajustes", desde el que es posible desactivarlo.

12.2 WI-FI

La principal recomendación de seguridad asociada a las comunicaciones Wi-Fi (802.11) es ***mantener desactivado el interfaz inalámbrico Wi-Fi salvo cuando 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. Tras el proceso de configuración inicial del dispositivo móvil empleado en la elaboración de la presente guía, el interfaz Wi-Fi quedará habilitado por defecto, se haya o no realizado la configuración de conexión a una red Wi-Fi, por lo que se recomienda proceder a deshabilitarlo mientras el usuario no vaya a completar la configuración de una red Wi-Fi en un entorno seguro.

Android restaura el estado del interfaz Wi-Fi a su valor de partida tras reiniciar el dispositivo móvil y al salir del modo avión, incluso con la pantalla bloqueada.

IMPORTANTE: el estado de activación del interfaz Wi-Fi no se muestra en la barra superior de estado salvo que exista actualmente una conexión a una red. Por tanto, para saber si el interfaz Wi-Fi está habilitado o no, hay que consultar el interruptor del menú "Wi-Fi" del menú "Ajustes - Red e Internet"[21], o el menú de ajustes rápidos.

El menú "Wi-Fi", a través del interruptor "Activado", y el icono "Wi-Fi" del menú de ajustes rápidos permiten modificar el estado de activación del interfaz. Si el interfaz está activo, pero no existe ninguna conexión a una red Wi-Fi actualmente, no aparecerá ninguna entrada marcada como "Conexión establecida".

La lista de redes mostrada en este menú contiene: la red a la que se está actualmente conectado ("Conexión establecida"), las redes a las que el dispositivo ha estado conectado alguna vez ("Guardado") y el resto de redes Wi-Fi no ocultas en rango. Pulsando sobre la entrada de cualquier red guardada, se iniciará la desconexión de la red actual y la conexión a la nueva[22]. Para ver los detalles de la red actual, se pulsará sobre su nombre, que incluyen la intensidad y frecuencia de la señal, el mecanismo de seguridad y la información TCP/IP de la conexión. El botón "Olvidar" permite eliminar del sistema la configuración de la red.

Las acciones de configuración de la conexión están disponibles pulsando sobre la entrada "Wi-Fi". Para añadir una nueva red, se puede:

- Elegirla a partir de la lista de redes Wi-Fi visibles mostrada.

[21] A partir de este momento, por simplificar, el menú "Ajustes - Red e Internet - Wi-Fi" se abreviará como "Wi-Fi".

[22] No existe ninguna opción para desconectarse de la red actual sin iniciar una conexión a otra red, salvo desactivar el interfaz Wi-Fi.

- Añadirla manualmente a través del botón "`+ Añadir red`". Esta opción se desaconseja desde el punto de vista de seguridad, ya que existen numerosos escenarios en los que el dispositivo móvil generará tráfico desvelando el nombre (o SSID) de la red, al considerarla oculta. Lamentablemente, esta opción, de uso habitual, permite más granularidad en la selección de opciones, como el tipo de mecanismo de seguridad (WEP, WPA/WPA2 PSK o 802.1x EAP).

Sin embargo, si, a pesar del consejo, una red es añadida como oculta, no se ha encontrado ninguna opción del interfaz que permita saber a posteriori si una red se ha configurado como tal, ni tampoco si existe alguna red definida como oculta, por lo que sigue siendo imposible para el usuario saber si el dispositivo móvil está desvelando su existencia a la hora de buscar este tipo de redes.

La opción para desarrolladores "`Habilitar registro Wi-Fi detallado`" (*"Enable Wi-Fi verbose logging"*), estando habilitada, añade información adicional a la pantalla de detección de redes Wi-Fi.

El menú "`Preferencias de Wi-Fi`" presenta las siguientes opciones [Ref.- 43]:

- "`Conectarse a redes abiertas`": permite que el dispositivo se conecte de forma automática a redes abiertas de alta calidad (siempre que el interfaz Wi-Fi esté habilitado, según se describe en la sección "*Auto connect to open networks*" de la [Ref.- 42]). ***Se aconseja mantener desactivada esta opción***.
- "`Notificaciones de redes abiertas`": estando activa, propicia que se emita una notificación informando de la disponibilidad de una red Wi-Fi abierta. Dado que el uso de redes abiertas está desaconsejado desde el punto de vista de seguridad, ***se aconseja deshabilitar esta opción***.
- "`Ajustes avanzados`": esta opción alberga, además de la dirección MAC y la dirección IP asignada al dispositivo móvil en la red concreta:
    - "`Instalar certificados`": para redes Wi-Fi corporativas (ver apartado "19. Almacén de credenciales"). Los certificados instalados mediante esta opción para Wi-Fi no se visualizan dentro de la pestaña "`Usuario`" del almacén de credenciales, sino solo a través del menú de configuración de una red Wi-Fi de tipo empresarial (o EAP/802.1x).
    - "`Proveedor de valoración de redes`": este campo permite seleccionar una de las apps existentes en el sistema que cumplan los requisitos descritos en la sección "*External network rating provider*" de la [Ref.- 42]. El objetivo de estas apps es proporcionar un criterio de valoración de la calidad de una red Wi-Fi abierta (*Slow, OK, Fast, Very fast*) de cara a la conexión automática a dichas redes. Por defecto, el valor es "Google", y, si se fija a "Ninguno", dejará de mostrarse la clasificación otorgada a la red bajo el icono del nombre de la red pública.
    - "`Wi-Fi Direct`": ver apartado "12.2.2. Wi–Fi Direct".
    - "`Botón WPS`": permite iniciar una conexión con un punto de acceso Wi-Fi con soporte para WPS (*Wi-Fi Protected Setup*) en la modalidad "WPS Push", que no precisa definir ni un nombre de red ni una clave y que

requiere pulsar un botón en el punto de acceso Wi-Fi durante la conexión (lo cual requiere proximidad física al mismo).

- "PIN WPS": este tipo de conexión se realiza a través de un código numérico o PIN (de 8 dígitos) que debe introducirse en el punto de acceso Wi-Fi para establecer la conexión WPS con el dispositivo móvil. Al pulsar esta opción, Android mostrará el PIN (que cambia con cada utilización). El uso de WPS con PIN está desaconsejado por ser vulnerable a ataques de fuerza bruta.

- "Redes guardadas": ver apartado "12.2.4. Conexión automática a redes Wi-Fi: ocultas o visibles y restricción de conexión".

Android 8 introduce restricciones relativas a la frecuencia de los escaneos Wi-Fi, de forma que una app solo puede iniciar un escaneo cada 30 minutos, y solo si dispone de al menos uno de los permisos listados en la [Ref.- 44].

El consumo de datos Wi-Fi por parte de las apps se muestra en el menú "Uso de datos", y es posible determinar el consumo por aplicación a través de "Uso de datos móviles". Se recomienda vigilar si existen apps que consumen datos de forma anormal, lo cual puede ser indicativo de algún problema de seguridad o infección del dispositivo móvil.

La inclusión del componente "Ajustes del dispositivo" en la copia de seguridad en la nube de Google (ver apartado "21.2. Copia de seguridad en la nube") provocará que se salven las contraseñas de las redes Wi-Fi conocidas en los servidores de Google.

12.2.1 WI-FI AWARE

Wi-Fi Aware (también conocido como NAN, *Network Awareness Networking*) es un estándar de la Wi-Fi Alliance, y su objetivo es proporcionar a los dispositivos que la implementan la capacidad de descubrirse, conectarse y medir el alcance entre sí, aunque no dispongan de conexión a Internet ni de acceso a redes móviles. El principal propósito es permitir la compartición de datos de gran volumen y con un buen ancho de banda entre dispositivos Wi-Fi que confían uno en el otro [Ref.- 46].

Android 8 soporta "Wi-Fi Aware" para el descubrimiento y la conexión a otros dispositivos, pero no para calcular la distancia existente entre estos y el dispositivo móvil.

No existen parámetros de configuración relativos a Wi-Fi Aware en la versión de Android 8 empleada en la elaboración de la presente guía, quedando el comportamiento de esta funcionalidad a cargo de los servicios del sistema y de las apps que proporcionen servicios basados en ella.

12.2.2 WI-FI DIRECT

La tecnología Wi-Fi Direct permite el establecimiento de conexiones Wi-Fi punto a punto ("P2P", Peer-to-Peer) directamente entre dispositivos (mínimo dos, pero

admitiéndose varios), sin hacer uso de una infraestructura, red o punto de acceso Wi-Fi. Algunos escenarios de uso son mostrar la pantalla y cualquier contenido multimedia (o juegos) del dispositivo móvil en un televisor, monitor o proyector, imprimir en una impresora inalámbrica, y compartir e intercambiar ficheros con otros dispositivos, por ejemplo, cámaras, o sincronizar datos con un ordenador.

Las capacidades de Wi-Fi Direct en Android se habilitan desde el menú "`Red e Internet - Wi-Fi - Preferencias de Wi-Fi - Ajustes Avanzados - Wi-Fi Direct`", siendo necesario que el interfaz Wi-Fi esté activo.

El nombre empleado por el dispositivo 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_bd78". Se recomienda cambiar este nombre a través de la opción "⋮" - "`Cambiar nombre del dispositivo`" por uno que no desvele detalles sobre el tipo de terminal (por ejemplo, "disp_0001").

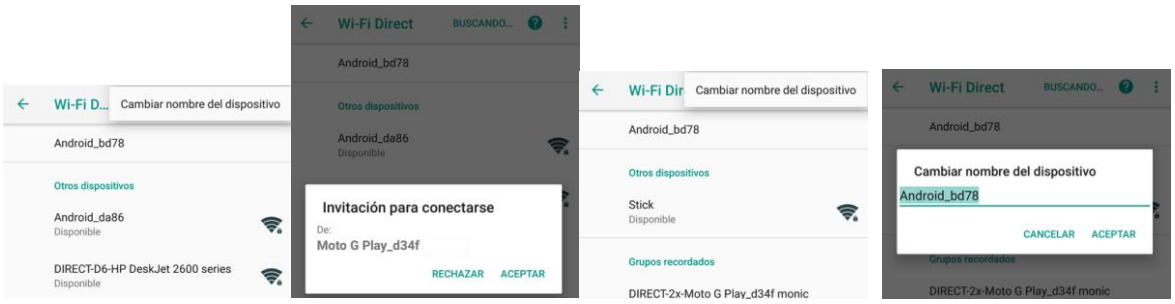

Figura 41 - Configuración de Wi-Fi Direct

La búsqueda de otros dispositivos Wi-Fi Direct se inicia al entrar en el menú y, desde éste, es posible forzar la búsqueda mediante la opción "`Buscar dispositivos`". Una vez seleccionada la entrada del dispositivo con el que se desea establecer la conexión, se enviará una invitación que, si es aceptada por su parte, establecerá un nuevo grupo de Wi-Fi Direct, y se llevará a cabo la conexión. Un dispositivo Android puede recibir invitaciones de comunicación, disponiéndose de 30 segundos para aceptarla. Para efectuar la desconexión, hay que pulsar sobre la entrada correspondiente al dispositivo remoto y aceptar la confirmación.

El establecimiento de una conexión Wi-Fi Direct hace que se cree un grupo, el cual se muestra en el campo "`Grupos recordados`". Las conexiones futuras de los grupos recordados podrán iniciarse sin necesidad de aceptar la invitación de nuevo. Por tanto, se recomienda olvidar el grupo mediante la opción "`<Nombre del grupo> Olvidar`" una vez haya finalizado la conexión.

En la implementación de Wi-Fi Direct de los dispositivos móviles de Google no se ofrece la posibilidad de crear grupos Wi-Fi Direct integrados por varios dispositivos, ni tampoco establecer parámetros como el tiempo de inactividad para dar por concluida una conexión, u opciones para establecer comunicaciones automáticas con los grupos conocidos cuando se entra en el menú `Wi-Fi Direct`[23].

[23] Fabricantes como Motorola sí proporcionan estas opciones.

Las implementaciones Wi-Fi Direct de algunos fabricantes no permiten establecer este tipo de comunicaciones y mantener simultáneamente la conexión a una red Wi-Fi mediante un punto de acceso. En Android 8 sí es posible disponer de ambas conexiones Wi-Fi simultáneamente.

12.2.3 WI-FI ASSISTANT

Las capacidades de Wi-Fi Assistant permiten securizar las conexiones a redes Wi-Fi abiertas a través de una red VPN establecida con Google, y requieren habilitar la opción "`Conectarse a redes abiertas`" descrita anteriormente, ya que actualmente no funcionan si la conexión a la red se realiza de forma manual. Wi-Fi Assistant solo está disponible en determinados países y, si el dispositivo cuenta con el servicio "Google Fi"[24] para tarificación de uso de datos, en algunos países adicionales, incluido España. Por otra parte, solo las redes públicas que Google considera de confianza permitirán el establecimiento de la VPN hacia los servidores de Google.

Tras la conexión a una red Wi-Fi abierta considerada de confianza, el túnel VPN se establecerá automáticamente, lo cual se indica a través de un icono de llave junto al icono de Wi-Fi de la barra superior de estado. Desde el punto de vista de seguridad, puede resultar interesante hacer uso de esta opción si no queda más remedio que conectarse a una red Wi-Fi abierta y no se dispone de ninguna otra solución de VPN con un servidor propio. Por el contrario, requiere que la opción "`Conectarse a redes abiertas`" esté activa, lo cual se desaconseja desde el punto de vista de seguridad.

[24] https://fi.google.com/about/

12.2.4 CONEXIÓN AUTOMÁTICA A REDES WI-FI: OCULTAS O VISIBLES Y RESTRICCIÓN DE CONEXIÓN

La sección "Redes guardadas" almacena la lista de las redes preferidas por el dispositivo (PNL, *Preferred Network List*), que son aquellas a las que se ha conectado previamente o que han sido añadidas manualmente mediante "Añadir red", y está disponible aunque el interfaz Wi-Fi no esté activo.

Cuando se habilita el interfaz Wi-Fi, el dispositivo intentará conectarse en primer lugar a la última red a la que estuvo conectado y, si no es posible, irá obteniendo e intentando conectarse a redes de esta lista hasta que tenga éxito. 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.

Android 8 permite 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, cuando el modo "Ahorro de datos" está activo. Esta opción no implica que no se realicen conexiones a dicha red, pero se avisará al usuario si se intentan descargar actualizaciones de sistema operativo o apps o ficheros de cierto tamaño a través de ella. Estas restricciones de uso se establecen en el menú "Red e Internet - Uso de datos - Restricciones de red - [Redes Wi-Fi sin uso medido | Redes Wi-Fi sin tarifa plana]" (ver apartado "12.4. Comunicaciones de datos móviles").

Se aconseja reiniciar el interfaz Wi-Fi tras aplicar las restricciones en el uso.

12.2.5 USO DE CERTIFICADOS EN REDES WI-FI EMPRESARIALES

Si la configuración de una red Wi-Fi empresarial utiliza como mecanismo de seguridad "802.1x EAP" (802.1x y *Extensión Authentication Protocol*) y un método EAP de tipo PEAP, TLS o TTLS, se recomienda indicar manualmente durante la configuración de la red en el dispositivo móvil el certificado raíz correspondiente a la CA (autoridad certificadora) que haya emitido el certificado digital del servidor RADIUS de dicha red Wi-Fi empresarial. Para ello es preciso haber importado previamente este certificado (ver apartado "19. Almacén de credenciales"), de forma que el mismo aparezca en la lista "Certificado de CA" del menú de configuración de la red Wi-Fi.

En el menú de configuración de la red Wi-Fi aparecerán tantas instancias del certificado como veces se haya importado con distinto nombre.

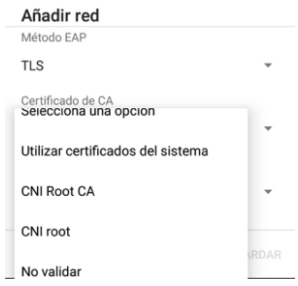

Figura 42 - Uso de certificados en redes Wi-Fi empresariales

12.3 COMUNICACIONES DE VOZ Y SMS

El interfaz de comunicaciones de voz se activa tan pronto se introduce el PIN de la tarjeta SIM insertada en el dispositivo móvil, y permanecerá habilitado, salvo si el dispositivo entra en "modo avión" o se extrae la tarjeta SIM, no existiendo ningún mecanismo que permita deshabilitarlo de forma individualizada.

Los ajustes relacionados con las comunicaciones de voz están disponibles desde el menú "`Redes e Internet - Red móvil`", bajo el que figura el nombre del operador de telefonía móvil asociado a la tarjeta SIM, y que engloba distintas opciones (a continuación, se detallan las que afectan a las comunicaciones de voz):

- "`Operadores de red`": permite seleccionar, tanto de forma automática (opción "`Seleccionar automáticamente`") como manual (opción "`Buscar redes`"), el proveedor de servicios de telefonía móvil. Esta opción no debe modificarse en el país de emisión de la tarjeta SIM, pero sí en caso de itinerancia, para seleccionar la red más conveniente para el usuario.

Adicionalmente, algunas apps que ofrecen servicios de telefonía disponen de otras capacidades y ajustes de configuración que pueden tener implicaciones desde el punto de vista de seguridad. En el caso de la app "`Teléfono`" suministrada por defecto, accesibles desde el menú "⋮" - "`Ajustes`", se identifican los siguientes (ver <Figura 43>):

- "`Respuestas rápidas`": permite configurar mensajes predeterminados que se enviarán como SMS si el usuario recibe una llamada que no puede atender. Dado que el envío de estos mensajes puede realizarse desde la pantalla de bloqueo mediante la opción "`Responder`", se recomienda ser cauteloso a la hora de seleccionar el contenido, pues un tercero con acceso físico al dispositivo durante una llamada podría enviar el mensaje como si fuera el propio usuario. Lamentablemente, la única opción identificada para impedir el uso de respuestas automáticas es eliminar el permiso "SMS" a la app teléfono.
- "`Llamadas`":
    - "`Cuentas de llamadas`": permite definir una cuenta SIP para cursar llamadas de voz sobre IP (VoIP).
    - "`Desvío de llamadas`": esta opción permite establecer las condiciones ("`siempre | cuando esté comunicando | cuando no responda | cuando esté apagado o sin cobertura`") para que las llamadas se desvíen a otro número de teléfono. En términos generales, se desaconseja desviar llamadas a números ajenos o asignados a dispositivos que puedan estar en posesión de terceros.
    - "`Ajustes adicionales`": el campo "`ID de llamada`" permite mostrar/ocultar el número propio al realizar una llamada. Este ajuste puede resultar útil en caso de que no se desee que el receptor pueda determinar el número llamante. Complementariamente, Google implementa un servicio por el cual, cuando se cursa una llamada con alguien que no está en la lista de contactos, buscará coincidencias en la

cuenta de usuario de Google y en el directorio "Google My Business"[25] para tratar de ampliar la información de los números de teléfono implicados. Aunque la configuración de la cuenta de usuario de Google queda fuera del alcance de la presente guía, por su relevancia desde el punto de vista de seguridad, se recomienda deshabilitar las opciones del menú disponible en el enlace web "https://myaccount.google.com/phone?pli=1" (ver <Figura 43>).

- "`Números bloqueados`": permite configurar los números de los cuales no se desea recibir llamadas. Esta opción es interesante para inhabilitar números registrados como fraudulentos o asociados a empresas que realizan comunicaciones comerciales no deseadas. El bloqueo de un número puede también realizarse pulsando sobre él en la lista de llamadas y seleccionando "`Bloquear/marcar como spam`".
- "`ID de llamada y spam`": esta opción utiliza el servicio "Google My Business"[25] y las cuentas de centros de trabajo y educativos para "traducir" el número llamante. Con la opción "`Filtrar llamadas de spam`", las llamadas procedentes de los números que Google identifica como no deseados no sonarán en el teléfono, pero sí se guardarán en el historial. El uso de esta opción provoca que la información sobre las llamadas cursadas sea enviada a Google, por lo que se desaconseja su utilización desde el punto de vista de privacidad.
- "`Sitios cercanos`": utilizar la ubicación del dispositivo móvil para encontrar sitios cercanos que coincidan con las búsquedas realizadas mediante la opción "`Buscar contactos y lugares`" de la app Teléfono, aunque la información proporcionada no esté disponible en la agenda o lista de contactos, actuando de guía telefónica. Requiere que la app Teléfono disponga del servicio de ubicación. Desde el punto de vista de privacidad, no se aconseja conceder este permiso ni activar esta opción.

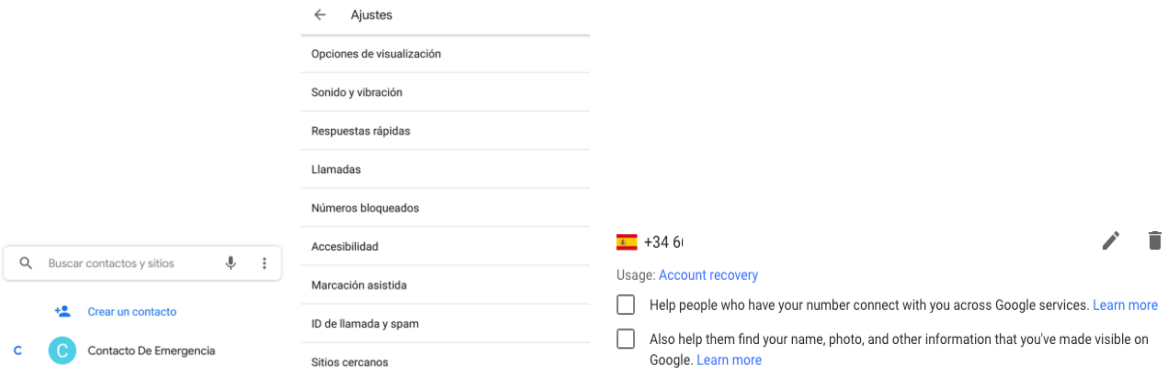

Figura 43 - Opciones de identificación del número de teléfono

[25] https://www.google.com/intl/es_es/business/

12.3.1 SMS

SMS (*Short Message Service*) es el estándar para el envío de mensajes cortos empleando la infraestructura GSM (2G), UMTS (3G) y LTE (4G).

Dado que algunas de las funcionalidades avanzadas de SMS incluyen mostrar contenidos web, gestionar datos binarios e intercambiar ficheros multimedia, ***se recomienda*** actuar con prudencia y:

- No abrir mensajes no esperados o solicitados, ni permitir la instalación de contenidos adjuntos[26].
- Proceder a borrar el mensaje directamente.
- Evitar pinchar o pulsar en los enlaces a sitios web contenidos en los SMS.

Por otra parte, de cara a la configuración de la presentación de mensajes, hay que tener en cuenta que el contenido:

- Puede revelar información sensible o confidencial.
- Puede estar asociado a mecanismos de autentificación, por ejemplo, códigos de un solo uso para autorizar operaciones bancarias críticas de banca online.
- Puede servir para validar acceso a cuentas de distintos servicios cuando el número de teléfono se emplea como segundo factor de autentificación. Para más información sobre la configuración del segundo factor de autentificación, se recomienda consultar el apartado "17.1. Inicio de sesión y seguridad" de la "Guía CCN-STIC-456 - Cuenta de usuario, servicios y aplicaciones de Google para dispositivos móviles Android" [Ref.- 408].

Por todo ello, ***se recomienda***:

- Establecer las notificaciones al valor "`No mostrar notificaciones`" para el campo "`En la pantalla de bloqueo`" (ver apartado "8.6. Notificaciones").
- En caso de permitirse mostrar notificaciones en la pantalla de bloqueo, asegurarse de que la app predeterminada para gestionar SMS ("`Mensajes`" en el caso de Android) tiene el campo "`Qué hacer`" a "`Mostrar en silencio`".
- Retirar permisos innecesarios a las apps que gestionen SMS, como "`Cámara`", "`Micrófono`" y "`Ubicación`".
- Confirmar que no existen ninguna app que haya solicitado el permiso especial "`SMS Premium`" (ver apartado "16.3. Permisos de las apps"), ya que este mecanismo se ha utilizado frecuentemente por software malicioso para el envío de SMS fraudulentos y con implicaciones económicas para el usuario.
- Dentro de los ajustes de la app "`Mensajes`" (disponible desde el menú "⋮" … - "`Ajustes`"):

[26] Durante la elaboración de la presente guía, Google publicó una vulnerabilidad de severidad crítica, que afecta a todas las versiones de Android entre la 7 y la 9, que permitiría a un atacante ejecutar código dentro del contexto de una app privilegiada utilizando un fichero de imagen en formato PNG. La información se puede consultar en https://source.android.com/security/bulletin/2019-02-01.

- Desactivar la opción "Respuesta inteligente" (ya que no es posible determinar de qué forma se realiza el análisis de contenidos de mensajes previos).
- En el menú "Vistas previas automáticas", deshabilitar todas las opciones de mostrar vistas previas.
- En la sección "Avanzados": deshabilitar "Descargar MMS automáticamente" y "Descargar MMS automáticamente en itinerancia".
- Utilizar el menú "Contactos bloqueados" para evitar que se muestren notificaciones sobre SMS recibidos de números sobre los que pueda albergarse sospecha de envío de mensajes fraudulentos o de mensajes no deseados. Esta acción es equivalente a seleccionar el mensaje dentro de la app y pulsar la opción "Marcar como spam".

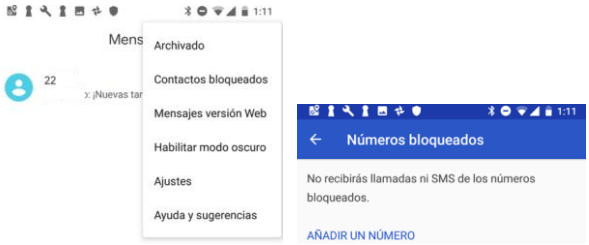

Figura 44 - Bloqueo de números en la recepción de mensajes

12.4 COMUNICACIONES DE DATOS MÓVILES

Tras la inserción de una tarjeta SIM con capacidad para datos móviles, Android habilitará el interfaz y quedará activo el servicio proporcionado por la red del operador. Al igual que con el resto de interfaces, la recomendación es desactivar el interfaz mientras no se esté haciendo uso de él (por ejemplo, mientras se esté conectado a una red Wi-Fi).

El estado del interfaz de datos móviles se muestra en la barra superior de estado con el símbolo "/", así como en el menú de ajustes rápidos. Su estado vigente se mantiene tras el reinicio del dispositivo. Para activar/desactivar el interfaz, se dispone de las siguientes opciones:

- Habilitar el modo avión: desactiva todos los interfaces de comunicaciones. No es posible habilitar individualmente el interfaz de datos en este modo.
- Utilizar el botón "Datos móviles" del menú de ajustes rápidos.
- Acceder al menú de configuración de datos móviles disponible en "Red e Internet - Uso de datos" y desactivar el interruptor "[Móviles] Datos móviles".
- Acceder al menú "Red e Internet - Red móvil" y desactivar el interruptor "[Móviles] Datos móviles".
- El menú de "Prueba", disponible mediante marcación del número *#*#4636#*#* (o *#*#info#*#*) ofrece la opción "Información sobre el teléfono - ⋮ - Habilitar conexión de datos", pero no permite inhabilitarla.

Cuando un dispositivo Android está conectado a una red Wi-Fi, cursará el tráfico hacia Internet a través de ella, aunque los datos móviles se encuentren activos. Si el sistema no detecta ninguna red Wi-Fi conocida en rango, Android registrará de nuevo el dispositivo en la red del operador automáticamente para pasar a usar los datos móviles.

- La opción para desarrolladores "`[Redes] Datos móviles siempre activos`" (*mobile data always-on while on wifi*) tiene el efecto de mantener la tarjeta SIM del dispositivo conectada a la red móvil de forma permanente, lo que acelera la transición cuando se pierde la señal Wi-Fi. En algunos terminales, se ha observado una disminución en la duración de la batería al emplear esta opción.
- La opción para desarrolladores "`[Redes] Transferencia agresiva de Wi-Fi a móvil`" (*Agressive Wifi to mobile handover*) provoca que el registro en la red de datos se realice cuando la señal Wi-Fi es débil, para impedir que las apps interrumpan sus conexiones.

El menú "`Red móvil`" controla los ajustes propios de la red, como el operador y el tipo de red preferida. El dispositivo móvil utilizará las redes más fiables disponibles a la hora de establecer las conexiones, y rebajará el nivel de exigencia si no encuentra ninguna de este tipo. Se recomienda mantener el ajuste a "`4G`" pero, en caso de encontrarse con situaciones en las que las conexiones de datos fallan, el usuario puede fijar este valor a "`3G`" o "`2G`" para favorecer el acceso a redes menos fiables.

12.4.1 CONTROLES SOBRE EL CONSUMO DE DATOS

El usuario puede establecer umbrales de consumo de datos móviles mediante el menú "`Uso de datos - [Móviles] Uso de datos móviles -` ⚙":

- "`Establecer límite de datos`": el sistema desactivará automáticamente los datos móviles cuando se alcance el umbral definido en el campo "Límite de datos", bloqueando su consumo.
  Es posible configurar una advertencia cuando se alcance un umbral próximo a este límite mediante la opción "Establecer advertencia de datos".
- El menú "`Red móvil - Itinerancia`" permite habilitar/deshabilitar el uso de comunicaciones de datos cuando se viaja al extranjero y el dispositivo móvil se conecta a la red de un operador ajeno. Se recomienda mantener el interruptor deshabilitado para evitar que se inicien comunicaciones de datos inadvertidas.

El consumo de datos móviles del sistema se muestra en el menú "`Uso de datos`", y es posible determinar el consumo por aplicación a través de "`Uso de datos móviles`". ***Se recomienda vigilar si existen apps que consumen datos de forma anormal***, lo cual puede ser indicativo de algún problema de seguridad o infección del dispositivo móvil.

Android dispone de la funcionalidad "`[Uso de datos] - Ahorro de datos`" (*Data saver*), también disponible desde el menú de ajustes rápidos, que, estando activa,

limita el consumo de datos móviles de las apps que están ejecutando en segundo plano. No obstante, mediante el menú "`Datos no restringidos`", es posible establecer una lista blanca de aplicaciones que podrán saltarse este ajuste y continuar con el consumo de datos móviles aun cuando el usuario no esté interactuando activamente con ellas. Por ejemplo, la app "Servicios de Google Play" es incluida por defecto en la lista blanca. A través del menú "⋮ - `Datos no restringidos - Mostrar aplicaciones del sistema`" se dispone de más granularidad para controlar qué servicios se desea limitar en datos o no.

A nivel de app, el menú "`Aplicaciones y notificaciones - <nombre de la app> Uso de datos`" muestra los datos de consumo del periodo mostrado, y dispone de las opciones:

- "`Datos en segundo plano`" (en Android 8.0.0 se denomina "`Conexiones automáticas`"): permite que la app consuma datos, aunque no esté ejecutando en primer plano.
- "`Uso no restringido de datos`": introduce la app en la lista blanca del modo de ahorro de datos.

Si el ahorro de datos está activo, se mostrará el icono "⊕" en la barra de estado.

La opción de establecer un límite de uso de datos resulta útil cuando se hace uso de una conexión de red compartida (zona Wi-Fi) con otro dispositivo, así como cuando existen varios usuarios en el sistema.

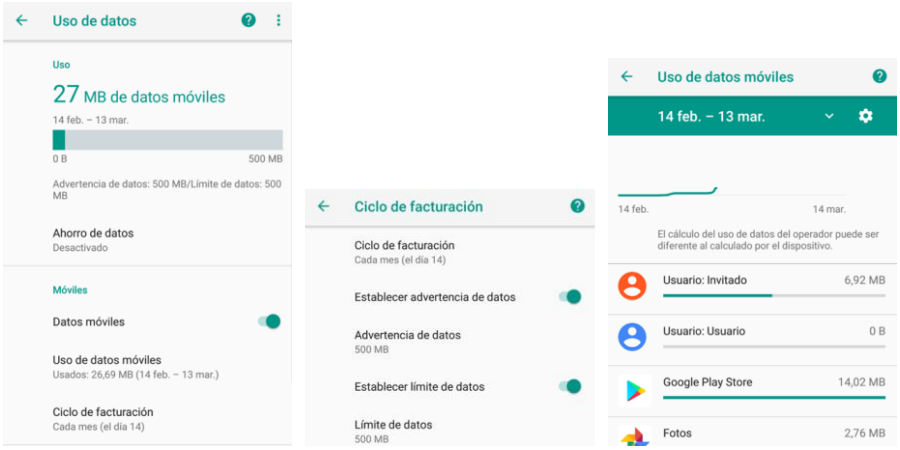

Figura 45 - Gestión del uso de datos móviles

12.5 CONEXIÓN DE RED COMPARTIDA (ZONA WI-FI)

Android proporciona capacidades nativas de *tethering* (compartición de la conexión de datos móviles con otro dispositivo), conocido de forma imprecisa como "zona Wi-Fi", a través de diversos mecanismos. El uso de conexiones a redes Wi-Fi compartidas proporcionadas por un dispositivo propio se considera más seguro que la conexión a redes Wi-Fi abiertas, por lo que constituye la mejor opción si se requiere acceder a Internet desde un equipo que carece de datos móviles.

Se recomienda deshabilitar la compartición de red tan pronto finalice la necesidad de usarla, mediante la desactivación del interruptor correspondiente al tipo de compartición (USB, Wi-Fi o Bluetooth).

Figura 46 - Configuración de una zona Wi-Fi

12.5.1 CONEXIÓN DE RED COMPARTIDA POR BLUETOOTH

Android proporciona capacidades nativas de *tethering* (compartición de la conexión de datos móviles con otro dispositivo) con un dispositivo emparejado actualmente mediante Bluetooth). Para habilitarla, es necesario acceder al menú "`Ajustes - Red e Internet - Zona Wi-Fi/Compartir conexión - Compartir conexión por Bluetooth`".

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), por ejemplo, 192.168.44.191. 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. El dispositivo móvil, con dirección IP 192.168.44.1[27], actúa de *gateway* por defecto, de servidor DHCP, y de servidor DNS, y es alcanzable mediante *ping* (ICMP).

```
$ ifconfig
…
bt-pan    Link encap:UNSPEC
          inet addr:192.168.44.1
          Bcast:192.168.44.255
          Mask:255.255.255.0
…
```

```
C:\ ipconfig
…
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
…
```

Figura 47 - Parámetros de red de zona Wi-Fi compartida mediante Bluetooth

[27] 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.

El dispositivo móvil informa de la compartición de la conexión Bluetooth a través de una notificación, que permanece en el área de notificaciones hasta que dicha conexión finalice.

12.5.2 CONEXIÓN DE RED COMPARTIDA POR WI-FI

Android proporciona capacidades nativas de *tethering* (compartición de la conexión de datos móviles con otro dispositivo), creando un punto de acceso Wi-Fi en el dispositivo móvil (conocido como *hotspot*) al que otros equipos se pueden conectar (hasta un máximo de 10). El dispositivo móvil actuará de *router* hacia Internet, compartiendo su conexión de datos de telefonía móvil (2/3/4G).

El estado de activación de una zona Wi-Fi se representa mediante el icono "", tanto en el menú de ajustes rápidos como en la barra superior de estado.

La disponibilidad de una conexión de datos móviles es un requisito para el establecimiento del *hotspot*, así como que no se encuentre habilitado el modo de "ahorro de datos" (ver apartado "12.4. Comunicaciones de datos móviles").

Las opciones de configuración de este tipo de conexión se encuentran en el menú "Red e Internet - Zona Wi-Fi/Compartir conexión" (ver <Figura 46>):

- "Punto de acceso Wi-Fi": habilita/deshabilita el *hotspot*. Esta operación también puede realizarse desde el icono "" del menú de ajustes rápidos.
- "Configurar punto de acceso Wi-Fi":
  - "Nombre de la red": se recomienda cambiarlo para que no revele detalles sobre el modelo o versión del dispositivo móvil.
  - "Seguridad": mantener el valor por defecto "WPA2 PSK".
  - "Contraseña": es un valor alfanumérico de mínimo 8 caracteres (se recomienda emplear frases de paso de al menos 20), que se aconseja cambiar periódicamente y, especialmente, si se requiere proporcionar conexión al *hotspot* a dispositivos ajenos.
  - "Seleccionar banda de AP": 2,4 ó 5 GHz, sin repercusiones para la seguridad.

Una vez configurado y activado el punto de acceso, el nombre dado al *hotspot* se mostrará en la lista de redes Wi-Fi de cualquier dispositivo que se encuentre en rango, y podrá ser seleccionada y accedida si se proporciona la contraseña correcta. El rango de direccionamiento IP es similar al empleado en el *tethering* Bluetooth, haciendo uso de la red 43 en lugar de la 44 (o de la 42 mediante USB). Tras finalizar la conexión con un *hotspot*, ***se recomienda olvidar la red Wi-Fi asociada***.

12.5.3 CONEXIÓN DE RED COMPARTIDA POR USB

La activación de la compartición de la conexión de datos móviles a través del interfaz USB requiere que exista conexión física mediante cable a través del puerto USB de los dos dispositivos implicados.

Tras habilitarse la compartición mediante USB *tethering*, se crea un interfaz de red específico para la conexión en el dispositivo móvil, "rndis0", cuyos parámetros se pueden obtener a través del comando "`adb shell ip addr`". La dirección "inet addr" es la que se utilizará para enrutar el tráfico entre el dispositivo móvil y el dispositivo remoto:

```
rndis0: …
    inet addr 192.168.42.129/24 Bcast 192.168.42.255 Mask 255.255.255.0
    …
```

Figura 48 - Interfaz para el USB tethering

Por su parte, en el ordenador (empleando Windows 10 de nuevo como ejemplo) que hace uso de la compartición de la conexión se creará un interfaz de red "Remote NDIS", que recibirá por DHCP una dirección de clase C (/24) en la subred 192.168.42.x/24. De nuevo, este direccionamiento no puede ser modificado. Se recomienda restringir la configuración de este interfaz de red para habilitar únicamente los protocolos y servicios que sean necesarios.

12.6 VPN

Android 8 proporciona soporte para las siguientes tecnologías y protocolos empleados por redes VPN (*Virtual Private Networks*):

- PPTP: se desaconseja su utilización porque es vulnerable a ataques de fuerza bruta por el uso que hace de MSCHAPv2. En caso de elegir esta opción, se debe recomienda mantener marcada la opción "Cifrado de PPP (MPPE)".
- L2TP/IPSec PSK e IPSec RSA.
- IPSec Xauth PSK, Xauth RSA y Hybrid RSA.

Para redes basadas en L2TP e IPSec, se recomienda establecer como mecanismo de autentificación certificados digitales frente a la utilización de claves precompartidas (PSK - *Preshared Key*), que, además de ser conocidas por todos los usuarios de la red, puede ser usada en ataques MitM[28]. Para obtener más detalles sobre los protocolos de VPN soportados en Android, consultar el apartado "19.6. Redes VPN" de la "Guía CCN-STIC-453E – Seguridad de dispositivos móviles: Android 7.x" [Ref.- 407].

La adición de una red VPN se puede realizar a través de la opción "`Red e Internet - VPN - +`". La opción "`Mostrar opciones avanzadas`" permite especificar los dominios de búsqueda y 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, en relación a la VPN. Tras fijarse las opciones de configuración de la red, la misma se podrá "`Guardar`" y aparecerá en la lista de redes VPN, desde la que se puede iniciar la conexión a ella pulsando sobre su nombre.

Para acceder a la configuración de la red VPN, el dispositivo debe disponer de un método de acceso vigente.

[28] http://www.cisco.com/en/US/tech/tk583/tk372/technologies_security_notice09186a0080215981.html

Si el tipo de red VPN a configurar utiliza certificados digitales, se recomienda importarlos previamente en el dispositivo (ver apartado "19. Almacén de credenciales") y seleccionarlos desde el menú, impidiendo así que un potencial atacante suplante al servidor VPN, ya que Android no verifica el certificado de CA en L2TP/IPSec-RSA.

Si se define un servidor DNS para la conexión, Android habilitará la opción "`VPN siempre activa`", que, si se activa por parte del usuario, impedirá el envío de cualquier tipo de tráfico hacia Internet hasta que la VPN se haya establecido. Esta opción ***se recomienda desde el punto de vista de seguridad***, pero deberá deshabilitarse temporalmente cuando la conexión a la red deba realizarse a través de un portal cautivo, que no permitirá el establecimiento del túnel hasta el servidor VPN.

No se recomienda **marcar la opción** "`Guardar información de la cuenta`", a fin de evitar que las credenciales de acceso a la red VPN se almacenen en el dispositivo móvil.

Android 8 permite, en dispositivos multi-usuario, que todos, incluido el invitado, añadan en su espacio privado de usuario redes VPN, pero sin permitir el acceso a las redes VPN definidas por el resto de usuarios.

13. DISPOSITIVOS CONECTADOS

La sección "`Ajustes - Dispositivos conectados`" alberga la configuración relativa a las conexiones punto a punto entre el dispositivo móvil y otros dispositivos, incluyendo las asociadas a las tecnologías Bluetooth, NFC, Impresión, Chromecast y Chromebook.

13.1 BLUETOOTH

La configuración de Bluetooth (referenciado como BT en adelante) se realiza a través del menú "`Bluetooth`". Este menú permite:

- Activar/desactivar el interfaz BT. Adicionalmente, es posible utilizar el icono BT del menú de ajustes rápidos para este propósito.
- El nombre BT del dispositivo, que, por defecto, identifica el modelo. Este nombre se puede cambiar desde el campo "`Nombre del dispositivo`".
- Verificar qué dispositivos hay conectados actualmente: la sección "`Dispositivos vinculados`" incluye la información "`Conectado`" si actualmente existe una conexión activa con el dispositivo BT en cuestión. A través del icono "⚙" se puede acceder a los detalles de cada dispositivo BT, incluyendo el nombre (modificable a través del icono "✎"), la dirección BT y los permisos concedidos, que varían según el perfil (o perfiles) BT que el otro dispositivo haya publicado. También informa de la dirección MAC (o BDADDR, *Bluetooth address*) obtenida para el dispositivo remoto. Este menú permite iniciar la conexión con el dispositivo u olvidarlo, a fin de evitar conexiones involuntarias.

- Iniciar un escaneo BT para detectar nuevos dispositivos BT en rango mediante la opción "`Vincular nuevo dispositivo`". Esta acción pondrá el dispositivo móvil en modo "Visible", y mostrará dinámicamente la lista de dispositivos BT disponibles actualmente para el emparejamiento.
- La dirección MAC del interfaz BT al final de esta pantalla: los tres primeros bytes permiten identificar al fabricante del dispositivo BT[29].

Por defecto, Android proporciona información en la barra superior de estado sobre el estado del interfaz Bluetooth mediante el icono "", esté o no conectado a otro dispositivo; si existe una conexión establecida actualmente, se mostrará con un par de pequeños puntos (uno a cada lado). Por su parte, el menú de ajustes rápidos también informará del estado del interfaz Bluetooth, desde el que se puede ver el dispositivo con el que se ha realizado la conexión en primer lugar y, al pulsar sobre la flecha situada a la derecha del nombre del dispositivo conectado, todo el resto de dispositivos con los que hay establecida una conexión.

Tras reiniciar el dispositivo móvil, se restaura el estado del interfaz Bluetooth al estado previo al reinicio, incluso aunque aún no haya sido desbloqueado, y permanece activo cuando el dispositivo móvil está en pantalla de bloqueo. Tras el reinicio, se intentará volver a establecer las conexiones Bluetooth previamente activas.

Cuando se reactiva el interfaz Bluetooth después de haber sido inhabilitado, el sistema intentará establecer la conexión con el primero de los dispositivos de su lista de emparejamiento que esté disponible y que no requiera la introducción de ningún código para el emparejamiento (por ejemplo, un dispositivo manos libres). Si se desea establecer conexiones adicionales, habrá que pulsar manualmente sobre el nombre de los demás dispositivos. Para finalizar la conexión, se puede pulsar sobre la opción "x" desde el menú de ajustes rápidos o sobre el nombre del dispositivo desde el menú "`Ajustes - Dispositivos conectados - Preferencias de conexión - Bluetooth`".

Para establecer una nueva vinculación o emparejamiento Bluetooth, se requiere seleccionar la opción "`Vincular nuevo dispositivo`". En Android 8, esta operación requiere que el interfaz BT se encuentre activado. La propia dirección BT se mostrará en esta pantalla, pero no así la del dispositivo remoto (para el cual se muestra directamente el nombre BT, a menos que carezca de él). El dispositivo móvil permanecerá en modo visible mientras dure el escaneo BT. Desde Android 8, por defecto solo los dispositivos que tienen un nombre BT asociado se muestran en la lista de dispositivos descubiertos. Para poder ver en esta lista los dispositivos que solo publican su dirección MAC BT, debe habilitarse la opción para desarrolladores "`[Redes] - Mostrar dispositivos Bluetooth sin nombre`" (ver apartado "15. Opciones para desarrolladores"). Si la vinculación requiere proporcionar o confirmar una clave, se dispondrá de 30 segundos para introducirla, y, en caso de no hacerse, la operación de vinculación será cancelada por el sistema.

[29] https://regauth.standards.ieee.org/standards-ra-web/pub/view.html#registries

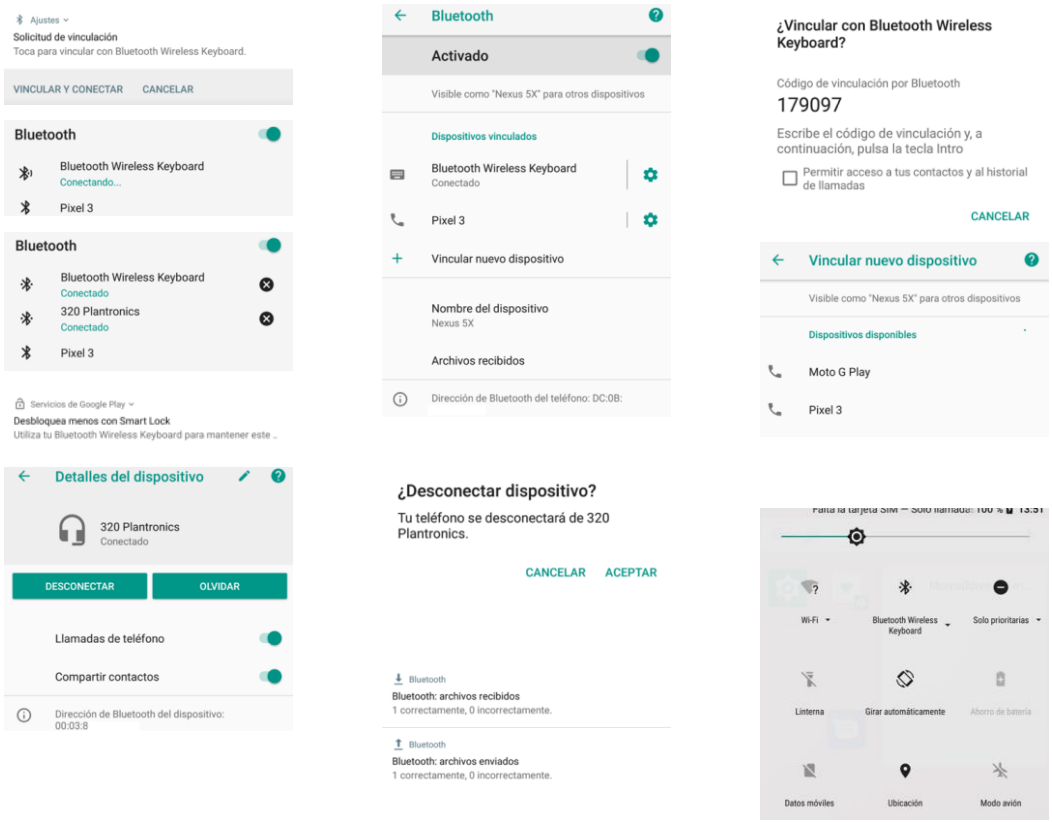

Figura 49 - Opciones de menú e información relativas a las conexiones Bluetooth

La vinculación con un dispositivo Bluetooth lanza una notificación que invita a que se utilice la funcionalidad de desbloqueo mediante un dispositivo de confianza de Smart Lock (ver apartado "10.1.2. Desbloqueo mediante "Smart lock"").

El icono a la izquierda de los dispositivos BT remotos descubiertos permite conocer su tipo (en base a su clase BT), y la selección de su nombre desde la lista iniciará el proceso de emparejamiento, que, dependiendo de la especificación BT soportada por aquel, puede requerir o no la introducción o aceptación de un código de emparejamiento, que se muestra en claro en la pantalla (para más información sobre los tipos de emparejamiento, se puede consultar la sección "15.3. Dispositivos Bluetooth emparejados" de la "Guía CCN-STIC-453E – Seguridad de dispositivos móviles: Android 7.x" [Ref.- 407]). La implementación de BT de Android incluye diferentes perfiles (especificaciones de la funcionalidad y servicios proporcionados por los dispositivos Bluetooth), que dependen de la versión de Android y del dispositivo móvil utilizados, y cuya lista completa se puede consultar en la [Ref.- 38]. Adicionalmente, se puede definir qué permisos se desea conceder.

13.1.1 OBEX PUSH - INTERCAMBIO DE OBJETOS A TRAVÉS DE BLUETOOTH

Android dispone por defecto de capacidades para el intercambio de objetos asociadas al perfil Bluetooth estándar OBEX Push, para el que no se han identificado opciones que permitan desactivarlo. Este perfil permite que otro dispositivo pueda

enviar objetos, por ejemplo, archivos, sin necesidad de que exista un emparejamiento previo entre ambos.

Cuando otro dispositivo Bluetooth se comunica con este perfil e intenta enviar un objeto, el sistema receptor emitirá las siguientes notificaciones:

- Solicitud de autorización del usuario para permitir la operación de intercambio, la cual se representa mediante el icono de Bluetooth con un par de puntos a su derecha en la parte superior izquierda de la barra de estado, y que se produce aunque ambos dispositivos estén actualmente emparejados.
- Progreso del proceso de intercambio, si éste fue autorizado.
- Resultado de la transferencia, que incluye las estadísticas de transferencias, y desde la cual es posible acceder a la lista de archivos recibidos y, pulsando sobre cualquiera de ellos, abrirlos con la app encargada de su manejo según su tipo (ver <Figura 49>).

Los objetos recibidos se almacenan por defecto en el directorio "`bluetooth`" del área de almacenamiento externo del dispositivo móvil (ej. "`/sdcard/bluetooth/`"), que se puede consultar desde la app "`Archivos`". Los detalles sobre todos los objetos relacionados con intercambios BT entrantes están disponibles en "`Ajustes - Dispositivos conectados - Bluetooth - Archivos recibidos`"

13.1.2 BLUETOOTH LOW ENERGY (BLE)

El estándar BLE (*Bluetooth Low Energy*) utiliza el mismo rango de frecuencias de transmisión que el Bluetooth clásico, pero, gracias a un sistema de modulación diferente, consume menos energía, por lo que su uso se extiende cada vez a más dispositivos periféricos, móviles, e IoT (Internet of Things).

Android 8 introduce soporte para la especificación BLE 5.0.

Cuando se establece una conexión con un dispositivo BLE, la app que actúa de pasarela entre ambos 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 *smart watch*, de forma que, si éste sale del rango de alcance, se restablezca la conexión cuando vuelva a entrar en él.

Para permitir el escaneo BLE, se requiere habilitar el servicio de ubicación y conceder a la app que lo esté iniciando permiso de localización (ver "16.3. Permisos de las apps"). Se recomienda ser muy cuidadoso con el tipo de apps utilizadas para gestionar otros dispositivos con conectividad BLE.

13.1.3 NEARBY

Google Nearby se lanzó como un servicio de búsqueda que, en función de la ubicación del dispositivo móvil, proporcionaba al usuario información de contexto sin requerir disponer de una app específica que la gestionase. Para ello, la app o sitio web

que desea hacer uso de estas notificaciones debe asociarse con un dispositivo BLE, o un *beacon* EddyStone o iBeacon. Cuando un dispositivo móvil Android con capacidades Nearby se aproxima a un dispositivo de ese tipo, se generarán mensajes en forma de notificación que permiten dirigir al usuario a la Play Store, a un sitio móvil web o directamente a una funcionalidad específica de una app instalada.

Las denominadas "*Nearby Connections*" son una API de comunicaciones extremo a extremo destinada al descubrimiento, conexión e intercambio de datos entre dispositivos en tiempo real, aunque no estén conectados a través de una red con una infraestructura determinada [Ref.- 40]. Las conexiones Nearby utilizan *hotspots* Wi-Fi, y comunicaciones BLE y Bluetooth para establecer las comunicaciones entre dispositivos con capacidad Nearby. En función de la intensidad y calidad de cada una de dichas señales inalámbricas, se cambiará de una a otra.

Aunque la configuración de este servicio, asociado al menú "`Ajustes - Google - Nearby`", queda fuera del alcance de la presente guía, hay que reseñar que tiene impacto desde el punto de vista de seguridad, ya que exige tener el interfaz BT y la ubicación activos para poder recibir las notificaciones, así como disponer de conexión a Internet (ver [Ref.- 40], 'Solución de problemas'). En las versiones más recientes de la app Google sí es posible deshabilitar las notificaciones asociadas a Nearby para evitar interrupciones no deseadas mediante el interruptor "`Recibir notificación si hay enlaces disponibles`".

Google ha anunciado la interrupción del servicio de notificaciones asociadas a NearBy, debido a que están resultando de poco interés para los usuarios y generando situaciones frecuentes de notificaciones no deseadas o spam [Ref.- 55].

13.1.4 RESUMEN DE LAS CONSIDERACIONES DE SEGURIDAD ASOCIADAS A BLUETOOTH

A continuación se facilita un listado con las recomendaciones de seguridad de BT:

- ***Desactivar el interfaz BT tras el proceso de configuración inicial del dispositivo***, que lo deja activado, incluso aunque no se haya establecido ninguna conexión.
- ***Desactivar el interfaz BT una vez haya finalizado la conexión con los dispositivos emparejados*** y hasta que vuelva a ser necesaria su utilización.
- ***Cambiar el nombre BT del dispositivo*** para evitar revelar información sobre el tipo y modelo de dispositivo a través del menú "`Ajustes - Dispositivos conectados - Bluetooth - Nombre del dispositivo`".
- ***Olvidar todo dispositivo Bluetooth con el que ya no se requiera tener conexión activa*** a través del botón "`Olvidar`" del menú "⚙ - `Dispositivos vinculados - <Nombre del dispositivo>`".
- ***Comprobar las direcciones MAC de los dispositivos con los que se ha establecido un emparejamiento*** a través del menú anterior.
- ***Activar el interfaz Bluetooth en modo oculto*** siempre que sea posible, utilizando el menú de ajustes rápidos del dispositivo móvil.

- ***Minimizar la visibilidad del dispositivo únicamente al tiempo necesario*** durante la realización de emparejamientos, no permaneciendo más tiempo del necesario en el menú "Vincular nuevo dispositivo".
- ***Limitar los permisos asociados a los perfiles BT a los mínimos requeridos***.
- ***Se desaconseja evitar el uso de dispositivos BT para el desbloqueo mediante Smart-Lock***, minimizando el riesgo si ambos son sustraídos simultáneamente.
- ***Deshabilitar la compartición de la conexión de tipo tethering mediante Bluetooth tan pronto deje de utilizarse la misma.***

La opción "`Ajustes - Sistema - Opciones de recuperación - Restablecer Wi-Fi, red móvil y Bluetooth`" permite restablecer todos los ajustes de red, incluyendo los asociados a Bluetooth.

13.2 NFC

Android dispone de capacidades de comunicación inalámbricas de corto alcance de tipo NFC (*Near Field Communication*) en aquellos dispositivos móviles que disponen de un interfaz NFC, con los siguientes modos de operación:

- Lectura (*Reader Mode*): de etiquetas NFC pasivas para apps en primer plano.
- P2P (*Point to Point*): intercambio básico de datos entre dos dispositivos, como por ejemplo aplicar la configuración de un dispositivo antiguo en uno nuevo.
- Emulación de tarjeta (*Host-based Card Emulation, HCE*): el dispositivo Android puede actuar como una tarjeta NFC de la que puede leer un dispositivo externo, como por ejemplo un TPV, para realizar pagos sin contacto (*contactless*).

El interfaz NFC se puede deshabilitar desde el menú "`Preferencias de conexión - NFC`", y no se incluye ningún icono en la barra superior de estado que informe de su estado. Tampoco se dispone de ajustes de configuración NFC más avanzados que permitan autorizar los distintos modos de operación de forma individual.

En términos generales, ***se aconseja habilitar el interfaz NFC solo en el momento de hacer uso de él, y proceder a desactivarlo seguidamente***.

13.2.1 ANDROID BEAM

Cuando el interfaz NFC se encuentra activo, el dispositivo móvil activará por defecto la opción "`Android Beam`"[30], que permite la compartición de contenidos entre dos dispositivos móviles Android utilizando el modo P2P de NFC.

Android Beam proporciona dos modos de compartición, que requieren que la pantalla se encuentre desbloqueada:

[30] El término "*beam*" se traduce por emitir, irradiar.

- "Toca para compartir": permite compartir contenido específico de una app entre dos dispositivos móviles, y depende fundamentalmente de la app que lo comparte. La app receptora actuará en función de dicho contenido. Por ejemplo, la compartición de un enlace por parte del navegador web Chrome provocará que el navegador web del dispositivo receptor abra la URL correspondiente automáticamente. Si el dispositivo receptor no dispone de la app necesaria para procesar el contenido recibido, se abrirá automáticamente la app Google Play para permitir su descarga e instalación.

  Se lleva a cabo aproximando el interfaz NFC de ambos dispositivos móviles, normalmente situado en su parte trasera. Se emitirá una señal acústica que confirma el establecimiento de la conexión NFC, la cual se inicia cuando el usuario toca la pantalla del dispositivo emisor.

- Menú " - Android Beam": permite el intercambio de ficheros entre los dos dispositivos. Una notificación informa de que el servicio NFC está a cargo de la transferencia, que tendrá una flecha apuntando hacia arriba en el dispositivo emisor y hacia abajo en el receptor.
  Los ficheros recibidos a través de este mecanismo se almacenan en el directorio "/sdcard/beam".

Si bien la compartición a través de la funcionalidad Android Beam requiere que los dos dispositivos implicados estén muy próximos (a menos de 4 ó 5 centímetros aproximadamente) y se encuentren desbloqueados, desde el punto de vista de seguridad ***se recomienda no habilitarla para evitar que contenidos sensibles puedan ser transferidos desde el dispositivo móvil del usuario a otro dispositivo***. Por ejemplo, sería posible una transferencia accidental (o intencionada) de contenidos entre usuarios que viajen en un medio de transporte como metro o autobús, cuyos dispositivos se encuentren en un bolsillo, cartera o bolso, y se acerquen suficientemente.

13.2.2 PAGOS MEDIANTE NFC

La funcionalidad encargada de emular tarjetas NFC para el pago en Android se denomina "Toca y paga", y la app proporcionada y asignada como predeterminada en los dispositivos Nexus es "Google Pay", aunque pueden utilizarse otras.

No existe ningún interruptor para la activación/desactivación de esta funcionalidad, pero es posible hacer uso del botón "Inhabilitar" asociado a esta app a través del gestor de aplicaciones. En todo caso, ***la opción más recomendable es desactivar el interfaz NFC y proceder a activarlo cuando se desee hacer uso de estas capacidades***.

La utilización de Google Pay está vinculada a la existencia de una cuenta de usuario de Google activa en el dispositivo, lo cual queda fuera del ámbito de la presente guía. Pueden consultarse todos los detalles relativos al servicio "Toca y paga" en el apartado "14.3. Pagos (y otros servicios) mediante NFC" de la "Guía CCN-STIC-453E – Seguridad de dispositivos móviles: Android 7.x" [Ref.- 407].

13.3 IMPRESIÓN

Android incorpora un servicio de impresión para imprimir de forma inalámbrica en impresoras conectadas a la misma red Wi-Fi que el dispositivo móvil. Este servicio, habilitado por defecto, dispone de un servicio de impresión predeterminado que, al seleccionarse, escanea la red en busca de impresoras. El botón "`Añadir servicio`" abre la app Google Play, desde la cual se puede instalar la app propia del fabricante de la impresora.

Se recomienda desactivar la opción de "`Servicio de impresión predeterminado`" y "`Cloud Print`", y proceder a habitarla solo cuando se requiera hacer uso de este servicio.

13.4 USB

El interfaz USB del dispositivo móvil, además de ser el mecanismo para cargar la batería, proporciona dos tipos de conexiones:

- Modo *accesory*: permite que el dispositivo móvil se comporte como una unidad de disco externa, que proporcionará acceso a su almacenamiento interno y externo (si dispone del mismo, o emulado). El menú "`USB`" permite determinar si el acceso se hará en modo "`Transferencia de archivos`" (MTP), que permite intercambiar archivos en ambas direcciones o "`Transferencia de fotos`" (PTP), proporcionando solo acceso a las carpetas "`DCIM`" y "`Pictures`", emulando una cámara digital.
  La conexión USB en modo *accesory* generará una notificación, desde la cual es posible definir el tipo de acceso que se va a permitir.
- Modo *host*: este modo posibilita la conexión MIDI (*Musical Instrument Digital Interface*), que permite conectar el dispositivo móvil a un dispositivo de tipo MIDI (como un teclado) que se controlará desde una app específica (como un sintetizador).
  Otro uso del modo *host* es la conexión a un periférico (como un ratón), pudiendo el dispositivo móvil proporcionarle carga (se mostrará un icono de batería en la barra superior de estado).

La conexión por USB posibilita la compartición de la conexión de datos móviles con el dispositivo en el otro extremo del cable USB (ver apartado "12.5.3. Conexión de red compartida por USB").

El menú de "`Opciones para desarrolladores`" proporciona diversas opciones para las conexiones USB:

- "`[Redes] Seleccionar configuración de USB `": define el tipo de conexión por defecto que se utilizará para la conexión USB si el dispositivo está desbloqueado. En caso contrario, solo se utilizará como fuente de carga de la batería (opción por defecto).
- "`Depuración por USB`": ver apartado "15.2. Opciones para desarrolladores – Depuración".

- "Revocar autorizaciones de depuración USB": ídem.
- "Inhabilitar enrutamiento de audio por USB": para controlar si el audio se dirige o no automáticamente a periféricos USB de audio conectados.
- "Verificar aplicaciones por USB": ver apartado "16.2.2. Orígenes desconocidos".

Para poder acceder a los contenidos del almacenamiento interno desde un ordenador, es necesario desbloquear el dispositivo móvil al menos en una ocasión desde que se haya conectado el cable USB. A partir de ese momento, es posible disponer de acceso a los contenidos en cualquier momento, incluso aunque el dispositivo móvil se encuentre de nuevo bloqueado, mientras el cable permanezca conectado. Transcurrido cierto tiempo sin que exista intercambio de datos entre ambos dispositivos, la conexión pasará al modo "Cargar este dispositivo".

Desde el punto de vista de seguridad, ***se recomienda mantener la opción de configuración de USB al modo de "solo carga"*** mientras no sea necesario realizar una operación que requiera disponer de acceso de datos, y volver al modo carga inmediatamente después. Debe prestarse atención a los mecanismos de auto-ejecución de Windows (*autorun* y *autoplay*), para evitar la propagación de software malicioso[31].

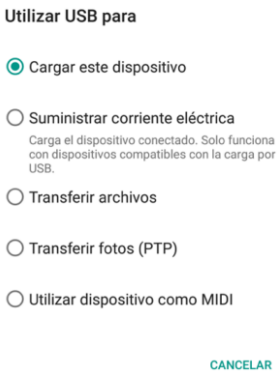

Figura 50 - Opciones para la conexión USB con otro equipo

14.COMUNICACIONES TCP/IP

La información relativa a las comunicaciones TCP/IP está disponible en "Sistema - Información del teléfono - Estado". Típicamente, los dispositivos móviles obtienen su dirección IP y el resto de parámetros asociados (puerta de enlace - o *gateway* -, longitud del prefijo de red - o máscara de subred - y servidores DNS) mediante DHCP, aunque todos estos ajustes se pueden configurar de forma estática durante el proceso de adición de la red Wi-Fi. Para cambiar los ajustes TCP/IP de una red Wi-Fi ya añadida, será necesario seleccionarla con una pulsación larga y elegir la opción "Modificar red". Para cambiar los ajustes TCP/IP de una red Wi-Fi ya añadida, será necesario seleccionarla y hacer uso del icono de edición superior.

[31] Ejemplo: troyano Ambler (https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=TrojanSpy:Win32/Ambler.D)

Android 8 mejora la seguridad de la pila TCP/IP eliminando el soporte para el mecanismo de "*TLS version fallback*", que permitía conectarse a servidores con implementaciones de TLS no estándares respecto a la negociación de la versión de TLS[32].

El identificador de dispositivo cliente "`net.hostname`" (que proporciona información sobre el nombre de red del dispositivo móvil) se envía vacío, siguiendo las recomendaciones de privacidad para DHCP del RFC 7844 [Ref.- 49]. Cuando actúa como cliente DHCP, el dispositivo no enviará tampoco el valor del DHCP *hostname* (que incluía el "ANDROID_ID" en versiones anteriores)[33].

15.OPCIONES PARA DESARROLLADORES

Las "`opciones para desarrolladores`" (denominadas "opciones de desarrollo" en versiones de Android hasta la 7 [Ref.- 407]) son capacidades normalmente empleadas por los desarrolladores de apps para Android que permiten llevar a cabo tareas de depuración y modificar el comportamiento del sistema. El menú está oculto por defecto, y se habilita pulsando 7 veces sobre la opción "`Ajustes [Sistema] - Información del teléfono - Número de compilación`". Desde la versión 8 de Android, este paso requiere la introducción del código de acceso al dispositivo móvil si existe alguno vigente (opción recomendada desde el punto de vista de seguridad), incluso aunque el dispositivo esté desbloqueado. Una vez completado el proceso, aparecerá el menú "`Opciones para desarrolladores`" bajo "`Ajustes - Sistema`":

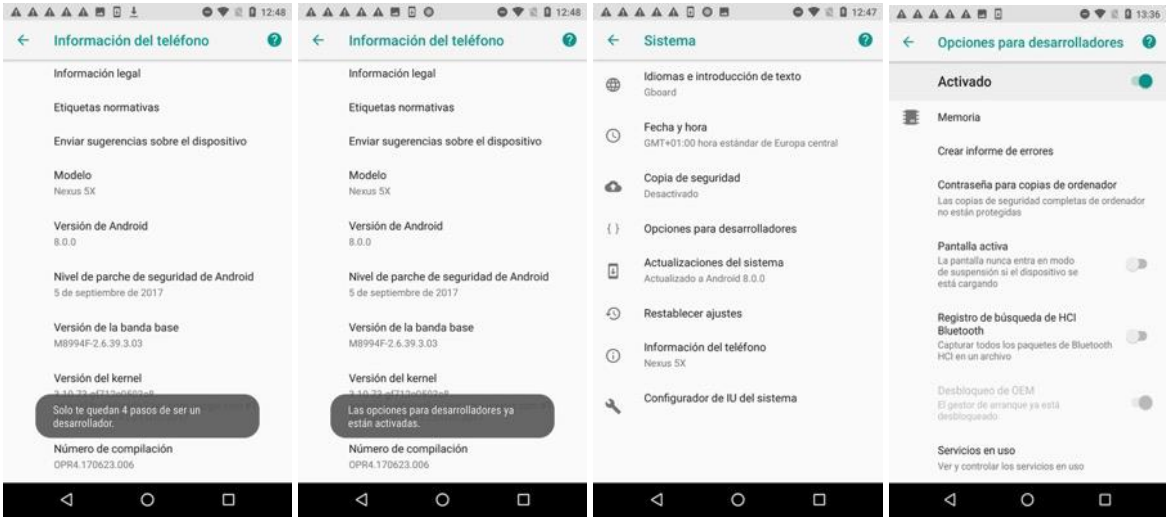

Figura 51 - Activación de las opciones de desarrollo en Android

El menú "`Opciones para desarrolladores`" alberga multitud de opciones avanzadas, que se agrupan en las secciones: `General` (aunque este término no aparece como sección en sí misma), `Depuración`, `Redes`, `Entrada`, `Dibujo`, `Renderización acelerada por hardware`, `Multimedia`, `Supervisión` y `Aplicaciones`. Aunque la recomendación es no hacer uso de este menú salvo por parte de usuarios expertos y

[32] https://android-developers.googleblog.com/2017/04/android-o-to-drop-insecure-tls-version.html
[33] https://android-developers.googleblog.com/2017/04/changes-to-device-identifiers-in.html

sólo bajo una necesidad específica, a continuación, se detallan las más relevantes (junto a su recomendación de uso) desde el punto de vista de seguridad. En la [Ref.-25] se puede consultar información adicional sobre el resto de opciones de desarrollo.

Se recomienda habilitar las opciones de desarrollo en el dispositivo móvil solo para aquellas acciones que lo requieran (por ejemplo, realizar un backup o restauración a través de ADB), y deshabilitarlas una vez realizada la acción que llevó a su activación.

15.1 OPCIONES PARA DESARROLLADORES - GENERAL

Recomendaciones de seguridad para las opciones generales de desarrollo:

- "Contraseña para copias de ordenador": permite establecer una contraseña para el uso de los comandos "adb" de backup y restauración. ***Se recomienda establecer una contraseña si se va a emplear este método de backup***.
- "Pantalla activa": evita que la pantalla se suspenda automáticamente mientras el dispositivo se está cargando. ***Se desaconseja activar esta opción, que permitiría a un potencial atacante acceder al dispositivo si este ha quedado temporalmente desatendido***.
- "Desbloqueo de OEM": permite desbloquear el gestor de arranque (*bootloader*), requerido para poder instalar imágenes de sistema de forma manual. Esta operación requiere la introducción del código de acceso, y, una vez habilitada, la opción aparecerá en gris en el menú, y solo se podrá revertir mediante la utilidad *fastboot* (ver apartado "5.2 Actualización manual del sistema operativo Android").
- "Servicios en uso": ofrece un interfaz que muestra el uso de memoria del dispositivo (incluyendo los procesos en caché) y la lista de apps activas, junto a sus procesos y servicios asociados (cuyo detalle se obtiene seleccionando una app concreta). Esta opción puede permitir investigar en detalle comportamientos anómalos del dispositivo móvil.
- "Actualizaciones del sistema automáticas": si esta opción está activa, el dispositivo móvil buscará actualizaciones y las aplicará de forma automática (ver apartado "5.1. Actualización automática del sistema operativo Android"). Esta opción controla si, tras el reinicio, se debe tratar de arrancar de la partición inactiva (completando así la actualización) o no (manteniendo la versión de Android previa al proceso de actualización).

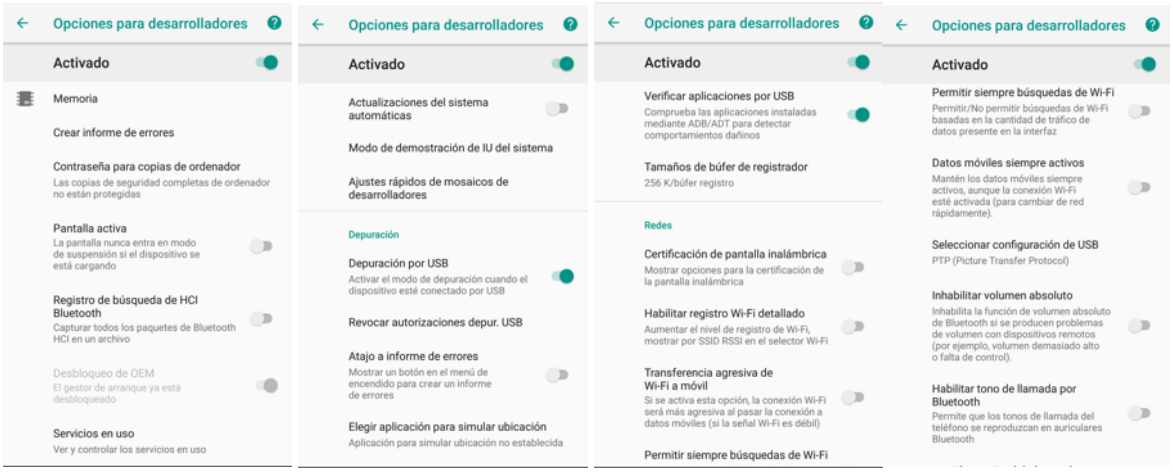

Figura 52 - Opciones generales para desarrolladores

15.2 OPCIONES PARA DESARROLLADORES - DEPURACIÓN

La opción más relevante desde el punto de vista de seguridad de este menú es la denominada "`Depuración por USB`". Si esta opción esta activa, Android proporcionará acceso a funciones avanzadas y de bajo nivel del dispositivo móvil vía USB empleando el *Android Debug Bridge* (ADB) [Ref.- 24]. Esta opción permite el acceso al dispositivo móvil desde un ordenador, instalar apps y llevar a cabo transferencia de ficheros (incluyendo backups y restauración), y el proceso de *sideload* (que actualiza la imagen del sistema).

Al habilitar la opción de "`Depuración por USB`", el dispositivo móvil mostrará un mensaje de autorización que incluye el hash MD5 de la clave pública del ordenador, y que el usuario debe aceptar para poder establecer la relación de confianza entre el dispositivo móvil y el ordenador[34]. La relación de confianza puede establecerse 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`". El comando "`adb devices`", ejecutado en el ordenador, indicará si la relación de confianza se ha establecido ("*número de serie del dispositivo móvil + device*") o no ("*número de serie del dispositivo móvil + unathorized*"). 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 de depur. USB`":

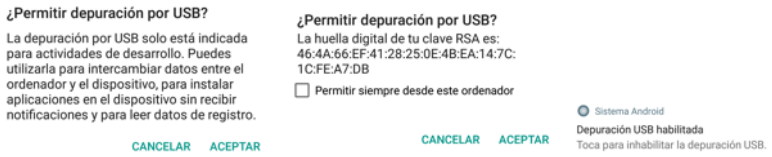

Figura 53 - Activación de las capacidades de depuración por USB

```
C:\> adb devices
List of devices attached
0257a9231868440f    unauthorized
C:\> adb devices
List of devices attached
0257a9231868440f        device
C:\> adb shell
shell@bullhead:/ $
```

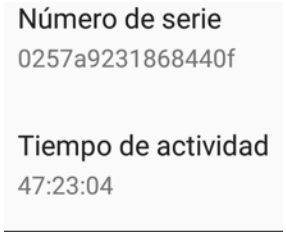

Figura 54 - Relaciones de confianza en Android a través de USB

El dispositivo móvil mostrará una notificación cuando la relación de confianza se haya establecido, y, al seleccionarla, se abrirá el menú "`Opciones para desarrolladores`".

[34] 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, y bajo "%USERPROFILE%/.android" en Windows, en los ficheros "adbkey" (clave privada, en formato PEM) y "adbkey.pub" (clave pública, en base64).

En los dispositivos móviles Android multi-usuario, únicamente el usuario propietario puede autorizar el acceso de depuración por USB a un ordenador.

Una vez finalizada la operación que haya requerido el establecimiento de una relación de confianza por USB, ***se recomienda ejecutar la opción*** **"**`Revocar autorizaciones de depuración USB`**"** para que se eliminen del dispositivo las relaciones de confianza correspondientes al ordenador conectado, especialmente si el mismo no es de uso exclusivo del usuario.

Existe bajo este menú la opción "`Verificar aplicaciones por USB`" (activa por defecto), que analiza las apps instaladas mediante ADB para detectar comportamientos sospechosos mediante la funcionalidad *Verify Apps* de Google (y Safety Net).

15.3 OPCIONES PARA DESARROLLADORES - REDES

Este apartado contiene opciones que afectan a las conexiones establecidas por el dispositivo móvil. Las más relevantes desde el punto de vista de seguridad son:

- "`Habilitar registro Wi-Fi detallado`": con esta opción activa, el menú "`Red e Internet - Wi-Fi`" proporciona detalles sobre el protocolo Wi-Fi, como detalles de la señal vía el RSSI (*Received Signal Strength Indication*), la frecuencia empleada por el canal usado por la red Wi-Fi, las direcciones MAC propia y del punto de acceso (BSSID), etc.
- "`Seleccionar configuración de USB`": ver apartado "15. Opciones para desarrolladores".
- "`Permitir siempre búsquedas Wi-Fi`": habilita que el dispositivo móvil busque en cualquier momento otros puntos de acceso (incluso de la misma red Wi-Fi utilizada actualmente) que proporcionen mejor intensidad de señal, con idea de conectarse a ellos mediante *roaming* Wi-Fi.
- "`Transferencia agresiva de Wi-Fi a móvil`": provoca que el cambio de la red Wi-Fi a la red de datos móviles se produzca cuando la señal Wi-Fi es más débil que la del umbral por defecto. Se recomienda utilizarla cuando la señal de la red Wi-Fi es inestable.
- "`Datos móviles siempre activos`": ver apartado "12.4. Comunicaciones de datos móviles".

15.4 CONFIGURADOR DE IU DEL SISTEMA

El "`Configurador de IU del sistema`" (*System UI Tuner*) otorga acceso a funcionalidades "ocultas" que permiten personalizar la barra de estado y el menú de ajustes rápidos. Para habilitarlo, se requiere:

- Tener habilitadas las opciones para desarrolladores.
- Realizar una pulsación prolongada sobre el icono del engranaje que se muestra al desplegar el menú de ajustes rápidos. Cuando este icono empiece a girar, se mantendrá la pulsación durante unos segundos.

- Con esta acción, se añadirá un nuevo menú bajo "`Ajustes - [Sistema] <Símbolo de llave inglesa> Configurador de IU del sistema`". Este símbolo de llave inglesa se añadirá también al icono de ajustes de la barra de ajustes rápidos: " ".
- Debe usarse con precaución por parte de usuarios no experimentados.
- Una vez aplicados los cambios deseados, ***se recomienda eliminar el configurador*** a través de "`Ajustes - Sistema - Configurador de IU del sistema`", seleccionando los 3 puntos de la derecha y marcando "`Quitar de ajustes`".

La opción "`Barra de estado`" permite configurar los iconos correspondientes a las opciones que se sitúan en la esquina superior derecha de la pantalla cuando se den las condiciones asociadas a ellos, y la opción "`No molestar`" permite definir cómo se activará este modo:

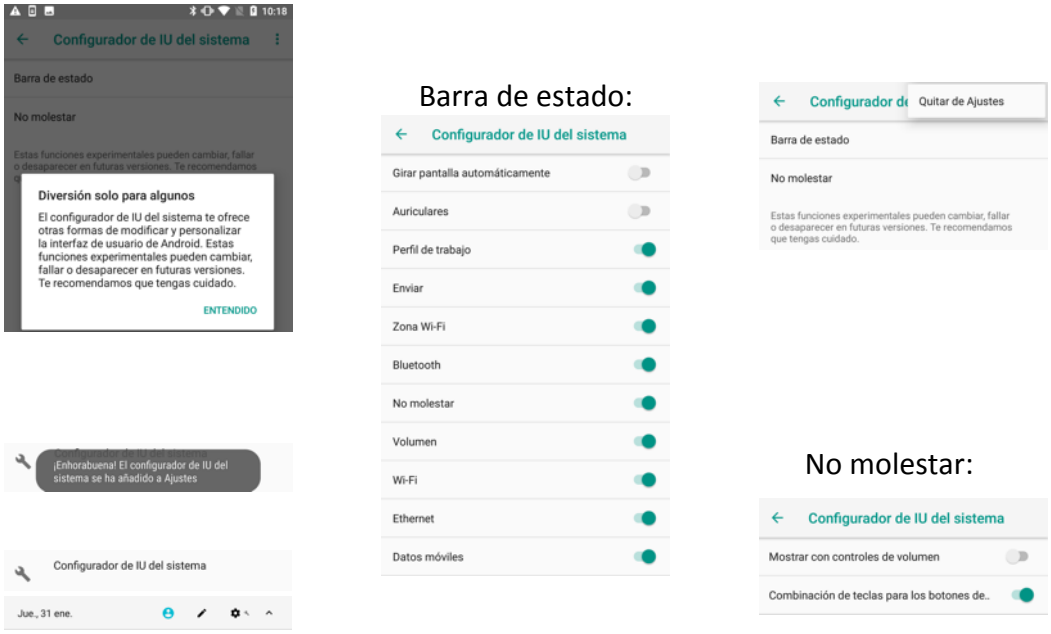

Figura 55 - Configuración de IU del sistema

16.GESTIÓN DE APPS

El término apps, o aplicaciones móviles, engloba al conjunto de aplicaciones móviles de sistema o de terceros que son compatibles con Android y que pueden ser instaladas sobre el dispositivo móvil. El mercado oficial de apps está accesible desde la app "Play Store", que requiere de la existencia de una cuenta de usuario de Google activa en el dispositivo móvil para poder instalar nuevas apps. Por su parte, la actualización de apps ya instaladas se realiza también a través de esta misma app, salvo para ciertos componentes del sistema, que se lleva a cabo mediante la app del sistema "Servicios de Google Play". La propia app "Play Store" recibe actualizaciones silenciosas que se aplican automáticamente y sin aviso para el usuario. El menú de configuración de esta app informa, a través de la opción "`Ajustes - [Información] Versión de Play Store`", sobre si existen actualizaciones de la app "Play Store"

disponibles para el dispositivo, pero dichas actualizaciones se llevarán a cabo cuando la política de Google para el dispositivo así lo autorice.

La primera recomendación de seguridad en relación con el uso de apps es mantenerlas siempre actualizadas**, **no sin antes verificar que las nuevas versiones no introducen comportamientos, o solicitan permisos, que pueden resultar indeseados. La actualización de las apps puede llevarse a cabo de diversas formas:

- Manual: el usuario decide cuándo proceder a la actualización de las apps, que puede iniciarse:
  - A través de la notificación generada por el sistema en la barra de notificaciones, si está activa la opción "`Ajustes - [General] Notificaciones - Actualizaciones`". ***Se recomienda activar esta opción***, así como la de "`Actualizaciones automáticas`", que enviará una notificación cuando los servicios de Play Store realicen una actualización automática.
  - Accediendo a la app "Play Store" y a su menú de configuración "☰" - "`Mis aplicaciones y juegos - [Actualizaciones] Actualizaciones disponibles - <nombre app> Actualizar`". Este menú ofrece también la sección "`Actualizaciones recientes`", en el que se indica cuándo tuvo lugar la actualización de cada app y, pulsando el botón "⌄", las novedades introducidas por esa versión, y "`Actualizaciones pendientes`", que muestra las apps para las que existe una versión más actual.
- Automática: a través del menú de configuración de la app "Play Store" y accediendo a su menú de "`Ajustes - [General] Actualizar aplicaciones automáticamente - En cualquier red | Solo por Wi-Fi`".
  Si se ha seleccionado la opción de actualizaciones automáticas, Android permite excluir de la misma determinadas apps. Para ello, se ha de acceder al menú "Play Store - "☰" - `Mis aplicaciones y juegos - <nombre de la app>` - ⋮" y desmarcar "`Actualizar autom.`". Este menú permite además informar a Google sobre apps cuyo contenido no se considera adecuado.

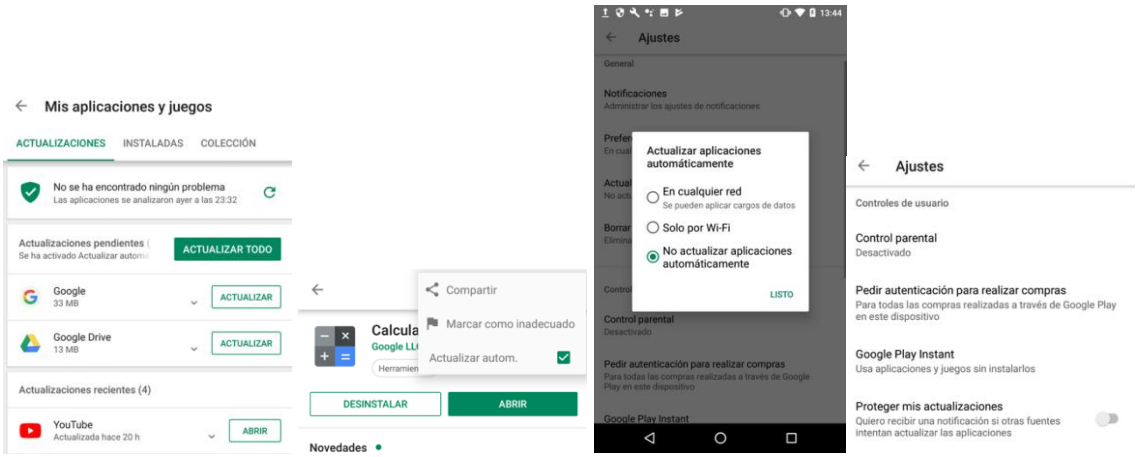

Figura 56 - Actualización de apps mediante la app "Play Store"

Android utiliza una conexión HTTPS cifrada y mecanismos de *certificate pinning* (ver apartado "19.4. Certificate pinning") para proteger las descargas y actualizaciones de las apps.

Se recomienda activar estas opciones de la sección [Controles de usuario] ***del menú de ajustes de la app "Play Store"***:

- "Pedir autenticación para realizar compras": se recomienda seleccionar "para todas las compras realizadas a través de Google Play en este dispositivo"; de este modo se solicitará al usuario sus credenciales de la cuenta de usuario de Google antes de proceder a instalar apps no gratuitas.
- "Proteger mis actualizaciones": de este modo se mostrará una notificación si una app va a ser actualizada fuera de la Play Store.
- "Google Play Instant": se desaconseja utilizar el uso de las denominadas "*Instant apps*" (ver apartado "16.5. Instant apps").

El menú para gestionar los ajustes de configuración de las diferentes apps existentes en el dispositivo móvil se encuentra en "Ajustes - Aplicaciones y notificaciones". En la parte superior se muestra la lista de apps recientes y, bajo ella, la opción "Ver todas las aplicaciones". El menú "⋮" permite:

- "Mostrar aplicaciones del sistema": incluye las apps del sistema en el listado de todas las apps.
- "Recuperar ajustes de aplicaciones": devuelve a la configuración de fábrica los ajustes de las apps relativos a notificaciones, habilitación, aplicaciones predeterminadas, restricciones de datos móviles y permisos.

Complementariamente, se incluye información sobre los siguientes parámetros:

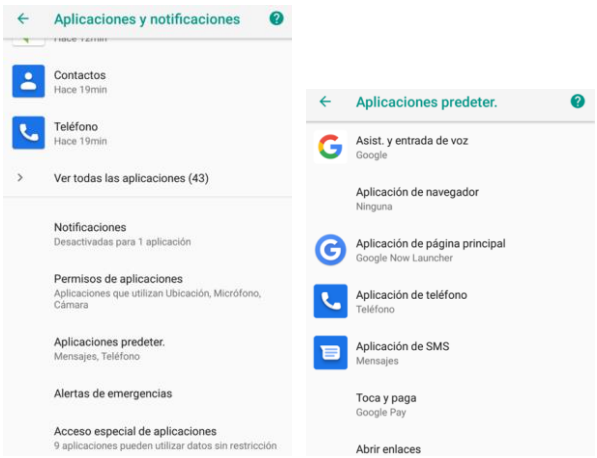

Figura 57 - Aplicaciones instaladas en el dispositivo móvil

- "Notificaciones": proporciona los ajustes globales del sistema en lo relativo a las notificaciones (ver apartado "8.6. Notificaciones").

- "Aplicaciones predeterm.": incluye la lista de aplicaciones que se abrirán por defecto cuando se invoque la acción asociada a ella. Si existe más de una app con las mismas capacidades, este menú permitirá seleccionar qué app se desea emplear de manera predeterminada. Este menú contiene una opción muy relevante desde el punto de vista de seguridad:
  - "Abrir enlaces": ***se aconseja desmarcar la opción*** "Aplicaciones instantáneas" (ver apartado "16.5. Instant apps").
  - En la sección "[Aplicaciones instaladas]", ***se aconseja examinar la lista de apps y verificar qué enlaces manejan*** y, si se detecta alguno sospechoso, seleccionar la app concreta, pulsar en la sección "Abrir enlaces compatibles" y marcar "Preguntar siempre" o "No abrir en esta aplicación". ***Esta opción se debería establecer por defecto para todas las apps que indiquen el enlace "*"*** para tener control en todo momento sobre las URLs visitadas durante la ejecución de la app.
- "Permisos de aplicaciones": ver apartado "16.3. Permisos de las apps".
- "Alertas de emergencias": ver apartado "8.6.2. Interrupciones".
- "Acceso especial de aplicaciones": ver apartado "16.3.1. Acceso especial de aplicaciones".

16.1 AJUSTES ESPECÍFICOS DE UNA APP

La selección de una app concreta a partir del menú "Ajustes - [Aplicaciones y notificaciones]" proporciona la información relativa a ella, que ofrece las siguientes opciones:

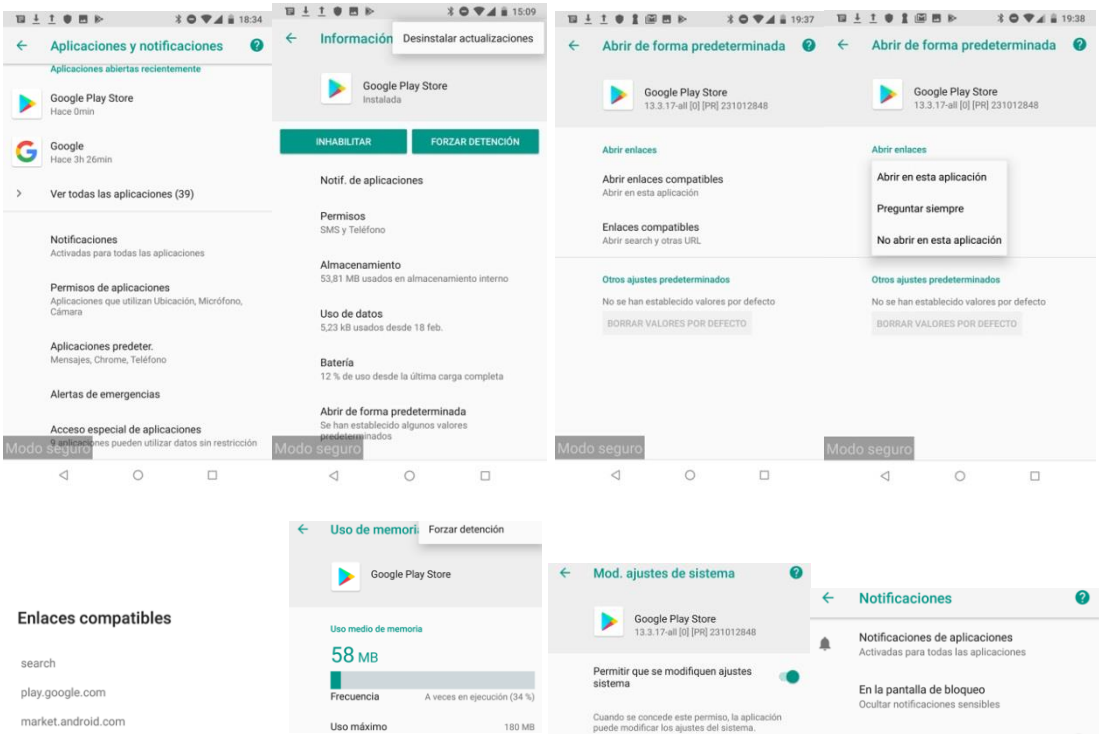

Figura 58 - Ajustes de una app concreta

- "Inhabilitar": (si no aparece sombreada). Tiene como efecto detener la app e impedir su ejecución. El icono de la app no se mostrará en la lista de apps accesible desde el menú "  " (Launcher) hasta que se seleccione "Habilitar". Esta opción resulta útil en caso de detectarse comportamientos anómalos del sistema durante la ejecución de una determinada app.
- "Forzar detención": aborta la ejecución en curso de la app hasta que vuelva a ser invocada.
- "Desinstalar": solamente disponible para las apps instaladas por el usuario.
- " - Desinstalar actualizaciones": solamente disponible para las apps proporcionadas por el paquete de instalación de Android, restaura la versión de la app suministrada de fábrica.
- "Notif. de aplicaciones": proporciona acceso a la configuración de las notificaciones de la app, descrito en el apartado "8.6. Notificaciones".
- "Permisos": ver apartado "16.3. Permisos de las apps".
- "Almacenamiento": permite consultar y gestionar el espacio consumido por la app en el almacenamiento del sistema (ver apartado "9.6. Almacenamiento").
- "Uso de datos": proporciona información sobre los datos consumidos por la app durante su ejecución desde el inicio del sistema. Los ajustes de esta sección se describen en el apartado "12.4. Comunicaciones de datos móviles".
- "Batería": informa del porcentaje de uso de batería de la app, útil para solucionar problemas de consumo excesivo de batería del dispositivo en determinadas circunstancias.
- "Memoria": permite consultar el uso que ha hecho la app de la memoria RAM del dispositivo, y "forzar detención" desde el menú "" en caso de un consumo anormalmente elevado que provoque mal funcionamiento del sistema, para liberar memoria. Si se detecta alguna app con excesivo consumo de memoria, se debería proceder a inhabilitarla temporalmente (si esta opción está disponible para ella) y, en caso de que el problema se resuelva, desinstalarla (o devolverla a los ajustes de fábrica, si la desinstalación está deshabilitada).
- "Abrir de forma predeterminada": alberga los parámetros:
    - "Abrir enlaces compatibles": establece si esta app se utilizará como app por defecto para aquellas acciones para las que esté capacitada. Para tener un control granular, ***se recomienda marcar*** "preguntar siempre".
    - "Enlaces compatibles": indica qué URLs proporcionan el mismo servicio que la app.
- "[Ajustes avanzados] - Mod. ajustes de sistema": solo disponible para las apps que tienen concedido el permiso de modificar ajustes del sistema (ver apartado "16.3. Permisos de las apps").

- "`[Tienda] Detalles de la aplicación`": permite comprobar la versión de la app, así como el mercado de aplicaciones del que se obtuvo. En términos generales, ***se recomienda instalar apps desde el mercado oficial de Google*** (Play Store) ***o del fabricante del dispositivo móvil***, por ofrecer mecanismos de control de confianza sobre la distribución e instalación de apps.

Las apps, por su parte, proporcionan en su fichero *manifest* "`AndroidManifest.xml`" toda la información sobre ellas necesaria para su correcta instalación y ejecución, incluyendo los permisos que solicitan (para acceder a componentes protegidos del sistema o de otras apps) y los que declaran (para permitir a otras apps interactuar con sus componentes).

16.1.1 SLICES Y "APP ACTIONS"

La funcionalidad "App Actions" [Ref.- 56] proporciona a las apps la capacidad de responder a acciones del usuario, proporcionando contenido dinámico e interactivo adaptado a esas acciones en el contexto de otras apps, particularmente el Launcher, la app de búsqueda de Google, el asistente de Google, la Play Store y la capacidad de "Selección de texto inteligente" (*Smart Text Selection*), sin necesidad de que el usuario esté interactuando con la app en ese momento.

La capacidad de "*Smart Text Selection*", introducida en Android 8, facilita la selección de texto en base al contexto (aplicando técnicas de *machine learning*, ML), de forma que permite el reconocimiento de direcciones, nombres propios de personas y empresas, y otros elementos, y permite seleccionar dicho texto como un único elemento con una pulsación sostenida.

A partir de un texto seleccionado mediante esta capacidad, una app que maneje el *intent* correspondiente puede mostrarse junto al menú "`Copiar | Compartir | Seleccionar todo`" y ejecutar una acción específica.

Figura 59 - Ejemplo de uso de "App Actions" (Fuente: Android Developers)

Las denominadas "*Slices*" son una mejora sobre las "App Actions", ya que permiten incorporar a la sugerencia de acción imágenes, vídeos y otros controles que se mostrarán en la app de búsqueda de Google y en el asistente de Google, superponiéndose a ambos.

El uso de las técnicas de *machine learning* (ML) pretende aprender sobre las costumbres del usuario, de forma que las sugerencias ofrecidas por las *Slices* estén encaminadas a lo que pretende hacer, anticipándose. Aunque Google manifiesta que los datos empleados para el aprendizaje no son enviados a sus servidores a día de hoy, esta situación podría cambiar en el futuro.

16.2 INSTALACIÓN DE APPS EN ANDROID

La instalación de apps en Android puede llevarse a cabo mediante dos vías: el mercado oficial Play Store y otros repositorios que Google denomina "de orígenes desconocidos".

Toda app de Android se distribuye a través de un fichero APK (*Android PacKage*), que debe estar firmado con el certificado digital del desarrollador de la app, el cual debe incluirse como parte del APK. Durante la instalación de la app, el proceso encargado de instalación de paquetes (*Package Manager*, pm) comprueba la validez de la firma, abortando la instalación si no es posible verificarla.

Para obtener los detalles sobre el esquema de firma digital de apps, se recomienda la lectura del apartado " 7.7. Firma digital de apps en Android" de la "Guía CCN-STIC-453E – Seguridad de dispositivos móviles: Android 7.x" [Ref.- 407].

16.2.1 MERCADO OFICIAL PLAY STORE

La instalación de apps a través de la tienda "Google Play Store" se describe detalladamente en el apartado "10. 2. Verificación de seguridad de las apps: Google Play Protect" de la "Guía CCN-STIC-456 - Cuenta de usuario, servicios y aplicaciones de Google para dispositivos móviles Android" [Ref.- 408], y está vinculada a la existencia de una cuenta de usuario de Google activa en el dispositivo móvil, por lo que se excluye del alcance de la presente guía.

A modo de recomendación, se recomienda consultar la información proporcionada a través de la app Play Store bajo "☰ - `[Mis aplicaciones y juegos]` - 🛡", y activar la opción "`Buscar amenazas de seguridad`". Se aconseja desactivar la opción "`Mejorar detección de aplicaciones dañinas`", ya que la información enviada a Google puede incluir datos del dispositivo, entre otros, el *DEVICE_ID* y la dirección IP.

16.2.2 ORÍGENES DESCONOCIDOS

Cualquier app instalada en el dispositivo a través de un mercado no oficial (cualquiera diferente a la Google Play Store) se considera de "orígenes desconocidos", y en esta categoría se incluyen tanto los ficheros APK descargados desde una página web, recibidos a través de adjuntos de un mensaje de correo, etc., como los obtenidos de mercados propios de otros fabricantes o proveedores de servicios. Normalmente, estos mercados alternativos no ofrecen actualizaciones automáticas, pero hay excepciones.

Desde Android 8 se modifica el mecanismo para permitir la instalación de apps de "orígenes desconocidos", que en versiones anteriores se gestionaba a través de un ajuste global, incorporando el permiso especial "`Instalar aplicaciones desconocidas`" (ver apartado "16.3.1. Acceso especial de aplicaciones") para aquellas apps que el usuario desee utilizar como canal de distribución para obtener el paquete de instalación de otras apps [Ref.- 59]. En caso contrario, el sistema mostrará el mensaje de la <Figura 62 >. Previamente, al descargarse el fichero APK se habrá

mostrado un mensaje de advertencia sobre el peligro existente, pero la descarga continuará si el usuario acepta este mensaje.

La instalación de apps también puede realizarse mediante la transferencia del paquete desde un ordenador hasta el almacenamiento del dispositivo móvil, tras lo cual se utilizará un explorador de archivos para seleccionar el fichero APK y que comience la instalación, o desde un servicio en la nube en el que se alberguen dichos ficheros.

Las apps instaladas al margen de la Play Store mostrarán en la sección "`<nombre app> [Tienda]`" el texto "`Aplicación instalada desde Instalador de paquetes`".

La opción para desarrolladores "`Verificar aplicaciones por USB`", que se recomienda habilitar si se va a hacer uso del método de instalación de apps a través de ADB (desaconsejado desde el punto de vista de seguridad), provoca que el sistema lleve a cabo ciertos mecanismos de verificación de los ficheros asociados a la app para detectar potenciales componentes maliciosos[35].

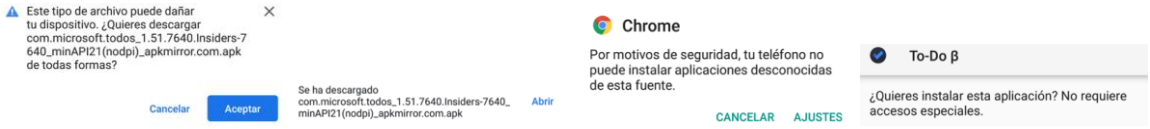

Figura 60 - Instalación de una app de orígenes desconocidos

16.3 PERMISOS DE LAS APPS

La seguridad más granular de la plataforma Android se basa en un mecanismo de permisos que impone restricciones en las operaciones que una app puede llevar a cabo sobre un recurso del sistema o los datos que caen fuera de su *sandbox* (entorno de ejecución privado de la app).

Se establece la siguiente clasificación de permisos [Ref.- 58]:

- "Normales": aquellos con escaso riesgo de compromiso sobre la privacidad del usuario o la operación del sistema (según el criterio de Google). Estos permisos se conceden por parte del sistema a la app solicitante durante el proceso de instalación, y no pueden ser revocados por el usuario. Algunos de estos permisos son el acceso al estado del interfaz Wi-Fi o poder fijar una alarma.
- "Peligrosos": los que afectan a los datos privados del usuario o a la operación de otras apps. Cuando una app ejecuta por primera vez y/o requiere acceso a un recurso controlado por un permiso peligroso del sistema que no le ha sido aún concedido por el usuario, deberá solicitar al usuario el permiso correspondiente a través de un menú de diálogo. Algunos de estos permisos son el envío/recepción/lectura de SMS, o el acceso a la cámara o la tarjeta SD.

[35] Es importante reseñar que Google recopilará datos sobre las apps de orígenes desconocidos y sobre el dispositivo móvil si esta opción está habilitada: https://support.google.com/accounts/answer/2812853.

- "De firma": son asignados por el sistema durante la instalación, pero únicamente si la app que lo solicita está firmada con el mismo certificado digital que la app que publicó el permiso.
- "Especiales": ver apartado "16.3.1. Acceso especial de aplicaciones". El sistema solo los concederá a una app instalada por el usuario tras obtener su autorización mediante un mensaje de confirmación muy detallado.

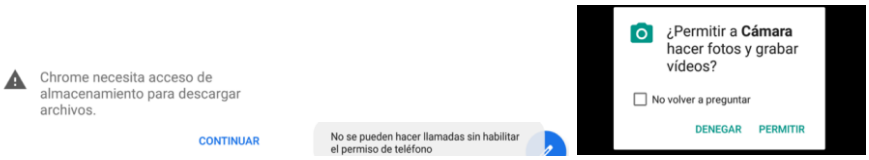

Figura 61 - Solicitud de permisos de una app

Los permisos se organizan en grupos o categorías que guardan relación entre sí. El permiso se asigna a nivel de grupo, y así se solicita su concesión al usuario. Por ejemplo, los permisos "lectura" y "escritura" sobre el almacenamiento se agrupan bajo el grupo "Almacenamiento"; si una app solicita permiso para leer del almacenamiento, el sistema solicitará al usuario confirmación para el grupo completo, pudiendo también escribir en el almacenamiento, o incluso formatearlo (destruyendo todos sus contenidos).

El comando "`adb shell pm list permissions -s`" muestra la lista de permisos y grupos de permisos disponibles en el dispositivo móvil desde línea de comandos. Por su parte, el menú "`Aplicaciones y notificaciones - Permisos de aplicaciones`" muestra los grupos de permisos junto a las estadísticas de las apps que lo tienen concedido. La selección de un grupo presenta una pantalla desde la que es posible otorgar/revocar ese grupo de permisos a nivel de app. La revocación de un permiso irá acompañada de un mensaje que informa de que la app podría no funcionar adecuadamente sin él.

Una app puede solicitar reiteradamente acceso a un grupo de permisos que le ha sido denegado en cada ejecución, aunque el usuario dispone de la opción "No volver a preguntar" para evitarlo. Si una app solicita un permiso y le es rechazado, puede optar por interrumpir su ejecución (el sistema mostrará un mensaje informativo en el margen inferior de la pantalla) o continuar con funcionalidad limitada (o con funcionalidad completa, si realmente ese permiso no es fundamental para la operación de la app).

Dado que es frecuente que las apps soliciten permisos que no requieren, y que pueden suponer un riesgo para la seguridad o la privacidad del usuario, ***se recomienda ser muy cuidadoso a la hora de aceptar permisos en tiempo de ejecución, así como revisar la lista de grupos de permisos disponibles y revocar los que una app claramente no necesite.*** Si, por alguna circunstancia especial, es necesario otorgar el permiso a la app, ***se recomienda proceder a su denegación*** tras finalizar la necesidad de uso. Un ejemplo es el permiso de ubicación para la app "`Fotos`", que Google incluye para permitir la incorporación de coordenadas geográficas en las fotografías, opción desaconsejada desde el punto de vista de privacidad.

Android 8 introduce los permisos ANSWER_PHONE_CALLS y READ_PHONE_NUMBERS con el objetivo de limitar el uso y abuso de los servicios de telefonía del dispositivo móvil por parte de apps maliciosas en la obtención del número de teléfono del usuario y del número llamante.

La existencia de vulnerabilidades en el manejo de permisos ha permitido la exposición de información no deseada (ver apartado "10. Privacidad del usuario en las plataformas móviles" del "Informe Anual 2018. Dispositivos y comunicaciones móviles. CCN-CERT" [Ref.- 413]).

16.3.1 ACCESO ESPECIAL DE APLICACIONES

El menú "`Aplicaciones y notificaciones - [Ajustes avanzados] Acceso especial de aplicaciones`" ofrece los detalles de acceso a permisos considerados "especiales". Los que se consideran más relevantes desde el punto de vista de seguridad y privacidad son:

- "`Aplicaciones de admin. de disp.`": las apps con este permiso pueden realizar acciones tan sensibles como borrado remoto del dispositivo móvil o la gestión del método de acceso y de servicios y apps. Por defecto, Android incorpora la app "`Encontrar mi dispositivo`" y "`Google Pay`". ***Se recomienda vigilar las apps con este permiso*** y consultar a personal técnico especializado en caso de duda.
- "`Mostrar sobre otras aplicaciones`": la superposición de una app sobre la ventana activa de otra es una técnica común de ataque en aplicaciones móviles, por lo que es importante desactivar esta opción para la mayoría de apps[36].
- "`Mod. ajustes de sistema`": Android clasifica los ajustes del sistema en dos grupos, comunes y globales[37]. Esta opción concede permiso para modificar los ajustes comunes, como el brillo o el sonido, que no impactan en principio sobre la seguridad.
- "`Acceso a no molestar`": dado que el modo "`No molestar`" puede deshabilitar funcionalidades como la recepción de llamadas o mensajes, se considera que este permiso no debe concederse, dejando la activación de dicho modo a la voluntad del usuario.
- "`Acceso a notificaciones`": debe evitarse su concesión, ya que las notificaciones pueden contener información confidencial, que una app maliciosa podría reenviar a servicios externos (por ejemplo, un código de autorización de una operación bancaria o de la validación de un segundo factor de autentificación).

[36] https://www.kaspersky.com/blog/cloak-and-dagger-attack/16960/

[37] https://developer.android.com/reference/android/provider/Settings.Global

- "`Imagen en imagen`": esta opción es relativa al modo "PIP" (*Picture-in-Picture*), que permite que la pantalla de una app aparezca como una pequeña ventana mostrando contenido al margen de la app en primer plano. Esta funcionalidad puede ser usada para esconder otros mensajes de advertencia de apps legítimas, de modo que se desaconseja conceder este permiso.
- "`Acceso a SMS Premium`": tradicionalmente, el envío de SMS de tipo Premium ha sido una fuente de ingresos para organizaciones fraudulentas a través de código móvil malicioso. ***Se recomienda desactivar este permiso*** si no se tiene constancia de requerir el uso de este servicio de pago.
- "`Acceso al uso`": este permiso permite obtener datos sobre el dispositivo móvil como el idioma o el uso que se hace de las apps. Aunque no afecta a datos sensibles, podría emplearse por apps maliciosas para conocer la app que está actualmente en ejecución y lanzar ataques de superposición.
- "`Datos no restringidos`": permite saltarse la restricción de uso de datos de aplicaciones en segundo plano, lo cual no suele ser necesario salvo para apps de mensajería instantánea (o similares), que deben poder actualizar su información en todo momento.
- "`Instalar aplicaciones desconocidas`": este permiso ***debe suprimirse para todas las apps***, deshabilitando el interruptor "`Autorizar descargas de esta fuente`" que se muestra al seleccionarlas, especialmente para los navegadores web y los clientes de correo, evitando así que se descarguen apps de sitios comprometidos. En caso de requerir instalar una app a través de alguno de estos canales, se recomienda deshabilitar este permiso tan pronto finalice dicha necesidad.

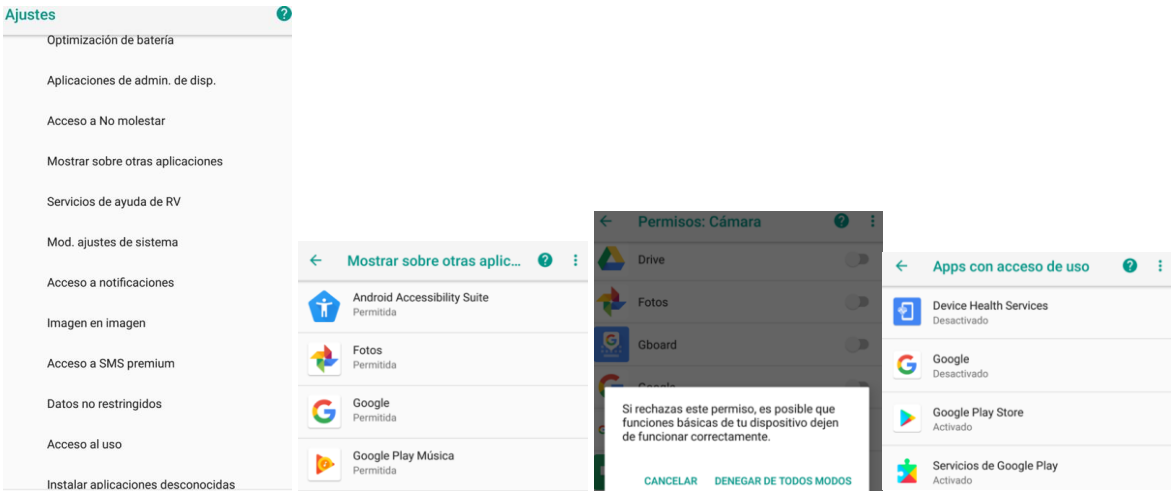

Figura 62 - Permisos especiales

16.4 SERVICIO AUTOCOMPLETAR

La característica denominada "*Autofill Service*" (Servicio Autocompletar o servicio de autorrelleno) está pensada para detectar (durante la utilización habitual del dispositivo) datos de *login* (autentificación en servicios y/o apps) y almacenarlos en una base de datos (local o remota) y permitir al usuario que sean introducidos de

forma automática al acceder a estos servicios en ocasiones sucesivas. Hasta Android 8, Google proporcionaba su propio servicio de almacenamiento de contraseñas en la nube, principalmente para sitios web, pero también para apps que utilizasen WebViews.

Android 8 añade un *framework* para permitir que apps de terceros, en concreto gestores de contraseñas reconocidos (por ejemplo, 1Password, Dashlane o Lastpass), soliciten al usuario almacenar la información de login cuando se accede por primera vez a una app o a un sitio web que requiere el uso de credenciales [Ref.- 47].

Android establece por defecto una app para el servicio de autorrelleno (asociada al propio servicio de Google, si existe una cuenta de usuario activa en el dispositivo móvil). La app por defecto se puede modificar mediante la opción "`Ajustes - Sistema - Idiomas e introducción de texto - Ajustes avanzados - Servicio Autocompletar`". El servicio se desactiva si se elige la opción "`Ninguna`". Al pulsar "`+ Añadir servicio`", se abrirá la app "Play Store" con la lista de gestores de contraseñas admitidos por este servicio.

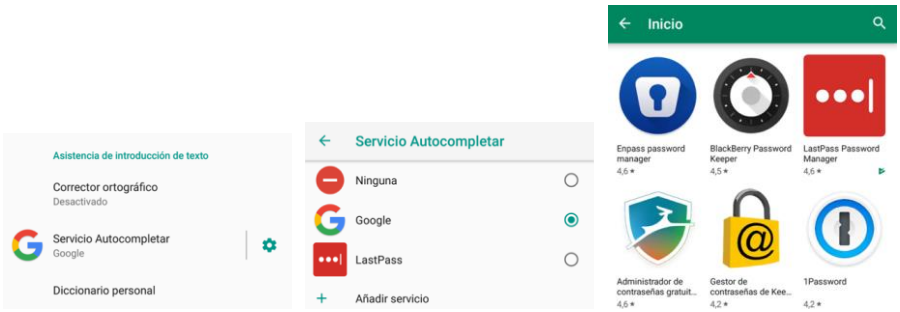

Figura 63 - Servicio Autocompletar

Desde el punto de vista de seguridad, el uso de gestores de contraseñas permite al usuario la utilización de contraseñas más robustas y menos repetitivas, por lo que se recomienda frente a opciones como la reutilización de contraseñas, o su anotación en ficheros en claro. Respecto al uso del servicio Autocompletar, dado que recientemente se han descubierto vulnerabilidades que afectan a los mecanismos de autorrelleno de los gestores (ver apartado "9. Código dañino para plataformas móviles" del "Informe Anual 2018. Dispositivos y comunicaciones móviles" [Ref.- 413]), ***se desaconseja utilizarlo***, especialmente para las contraseñas más sensibles, que deberían ser introducidas manualmente por el usuario (y, de ser posible, recordadas por él).

16.5 INSTANT APPS

Las "*Instant Apps*" son aplicaciones nativas de Android que se ejecutan de forma instantánea sin requerir su instalación previa en el dispositivo móvil. Al acceder a un servicio (por ejemplo, servidor web) que proporcione aplicaciones instantáneas, se descargará - bajo demanda - el segmento de código de la app correspondiente a una determinada acción. Si la app completa ya está instalada en el dispositivo, será ella quien se abra en lugar de la aplicación instantánea.

Aunque las *Instant Apps* se ejecutan dentro de un *sandbox* propio y no se han detectado operaciones de distribución de malware a través de ellas, pueden propiciar ataques de *phishing* en combinación con el uso de gestores de contraseñas (ver apartado "9. Código dañino para plataformas móviles" del "Informe Anual 2018. Dispositivos y comunicaciones móviles. CCN-CERT" [Ref.- 413]).

Ante la incertidumbre sobre la confianza en este tipo de apps (ligada a la confianza en el sitio web que las ofrece), la recomendación más conservadora es desactivar su uso a través de la opción "`Ajustes - Google - Google Play Instant - [Cuenta de Aplicaciones Instantáneas] Ninguna`".

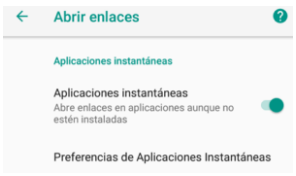

Figura 64 - Menú de activación de Instant apps

17.VERIFIED BOOT

"*Verified Boot*" es un mecanismo destinado a verificar la integridad del sistema durante el proceso de arranque, para detectar posibles modificaciones que pudieran haberse llevado a cabo por parte de software malicioso (*malware*) o un tercero.

Desde Android 8 se incorporó una implementación de "*Verified Boot*" denominada "*Android Verified Boot*" (AVB)[38], o "*Verified Boot* 2.0", que soporta la arquitectura del proyecto Treble (ver apartado "3.1. Proyecto Treble").

```
C:\> adb shell
getprop | grep "avb"
1
```

Figura 65 - Comandos adb para verificar la versión de Verified Boot

La verificación de la partición de sistema durante el proceso de arranque (cuyo flujo puede consultarse en la [Ref.- 50]) puede emitir tres mensajes de aviso (o estados del proceso de arranque); se recomienda la lectura del capítulo "7.9. Proceso de arranque seguro: Verified Boot" de la "Guía CCN-STIC-453E – Seguridad de dispositivos móviles: Android 7.x" [Ref.- 407] para obtener todos los detalles sobre este mecanismo:

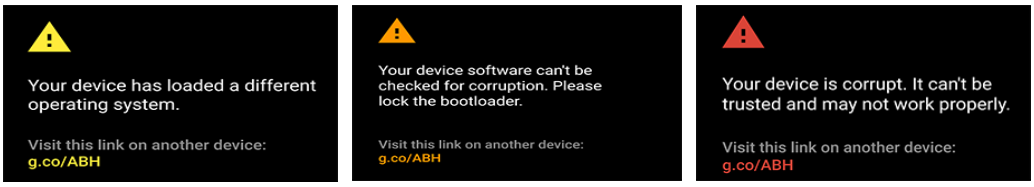

Figura 66 - Mensajes de condiciones anormales de arranque de Verified Boot

[38] https://android.googlesource.com/platform/external/avb/+/refs/heads/oreo-cts-release/libavb/avb_version.h

Si el usuario no es consciente de haber realizado ningún cambio en el sistema relativo al desbloqueo del gestor de arranque, ***debería evitar el uso del dispositivo y consultar con su soporte técnico*** (ver apartado "5.2.3. Desbloqueo/bloqueo del bootloader").

El siguiente comando permite conocer el estado del análisis realizado por el mecanismo *Android Verified Boot* durante el arranque:

```
bullhead:/ $ getprop ro.boot.verifiedbootstate
green
```

Figura 67 - Verificación del estado de arranque mediante AVB

AVB incorpora adicionalmente la funcionalidad "*Android Rollback Protection*" (ver apartado "5.3. Rollback Protection") para evitar la instalación de una versión de Android más antigua que la actual.

17.1 MODO DE ARRANQUE SEGURO

Android dispone de un modo especial de arranque, conocido como "*Safe Mode*", que el usuario puede invocar si detecta condiciones anómalas de funcionamiento del dispositivo (como consumo excepcional de batería, ralentización en el uso, temperatura elevada, etc.) o ante la sospecha de que alguna app no fiable haya sido instalada.

Para reiniciar el dispositivo en modo seguro, hay que pulsar el botón de encendido hasta que aparezca el menú de apagado, y mantener pulsada la opción "`Apagar`" hasta que se muestre el mensaje de confirmación de reinicio en este modo[39]. También es posible arrancar en modo seguro manteniendo pulsado el botón de bajar el volumen durante el reinicio del dispositivo una vez aparece el logotipo de Google y se inicia su animación en la pantalla de arranque o inicio [Ref.- 28].

El mensaje "Modo seguro" en el margen inferior izquierdo del dispositivo confirma que el sistema ha arrancado en este modo, en el cual las apps que no son de sistema mostrarán sus iconos sombreados y no podrán ejecutarse.

En caso de que el motivo para utilizar este modo sea haber observado un comportamiento anormal del sistema, ***se recomienda proceder a desinstalar una a una las apps más recientes*** (en orden inverso a como se instalaron) y reiniciar el dispositivo móvil en modo normal (a través de la opción "`Reiniciar`" del botón de apagado) ***para comprobar si el problema persiste***.

18. NAVEGADOR WEB MOBILE CHROME

El análisis del navegador web Chrome, suministrado por defecto con Android, queda fuera del alcance de la presente guía, pero se aborda en detalle en los

[39] Este mecanismo es válido para dispositivos móviles Nexus y Pixel, pero puede variar su disponibilidad para otros fabricantes, por lo que se recomienda consultar la documentación específica.

siguientes apartados de la "Guía CCN-STIC-456 - Cuenta de usuario, servicios y aplicaciones de Google para dispositivos móviles Android" [Ref.- 408], cuya lectura y aplicación de recomendaciones de seguridad se aconseja, ya que el navegador web es un elemento fundamental desde el punto de vista de la seguridad y privacidad del usuario:

- 14.1. Navegación web: navegador Chrome
- 9.2. Servicio de "Alerta de contraseña" para Chrome
- 9.3. Navegación privada
- 11.9. Navegador web

Se recomienda comprobar los ajustes del servicio "`Smart Lock para contraseñas`" (descrito en el apartado "12.2. Servicio de contraseñas de Google Smart Lock"), ya que, si está activado en la cuenta de usuario de Google (activo por defecto), Chrome hará uso de él para guardar las credenciales de los sitios web para los que el usuario acepte esta acción, lo cual se desaconseja desde el punto de vista de seguridad y privacidad, pues, si un tercero consiguiera control de la cuenta de usuario de Google, dispondría de todas las contraseñas aquí almacenadas y, por tanto, de acceso a todos esos sitios web.

19.ALMACÉN DE CREDENCIALES

Android dispone de un almacén de credenciales (denominado *Keystore*) a nivel de sistema en el que se guarda el material criptográfico (certificados digitales, claves privadas, *tokens*, etc.) que requiere el sistema operativo. El subsistema encargado de la gestión de este material se conoce como "*Android Keystore System*" (AKS), tanto a nivel de sistema como de apps. El AKS está diseñado de forma que el material criptográfico no puede ser extraído del dispositivo móvil, ni siquiera por las apps que lo utilizan.

Android 8 actualiza los certificados raíz de las CAs ofrecidos por defecto, eliminando buena parte de los obsoletos, así como los de WoSign y StartCom [Ref.-32].

Android permite al usuario añadir nuevos certificados digitales al sistema, que se incorporarán al almacenamiento de credenciales, accesible para el usuario a través del menú "`Seguridad y ubicación - [Privacidad] Avanzado - Cifrado y credenciales - [Almacenamiento de credenciales]`". El menú ofrece las siguientes opciones:

- "Tipo de almacenamiento": referencia al tipo de implementación del almacén de credenciales que, en los dispositivos Nexus, hace uso de un almacén seguro implementado en el propio hardware del dispositivo móvil.
- "Credenciales de confianza": ver apartado "19.1. Certificados raíz".
- "Credenciales de usuario": permite ver qué certificados han sido importados por el usuario, tanto de tipo raíz (ver apartado "19.1. Certificados raíz") como de tipo hoja o cliente (ver apartado "19.2. Certificados hoja").

- "Instalar desde almacenamiento": permite añadir un nuevo certificado a partir de los ficheros asociados al mismo. Este mecanismo se explicará más adelante.
- "Eliminar certificados": permite el restablecimiento a valores de fábrica del almacén de credenciales, eliminando las personalizaciones realizadas.

Para poder añadir certificados al almacén de claves, el dispositivo móvil debe disponer de un método de acceso vigente, al igual que para eliminar certificados, que será solicitado al realizar estas operaciones.

Para instalar un certificado basta con transferir el fichero que lo contiene al dispositivo móvil mediante correo electrónico, la tarjeta de almacenamiento externa, compartición por Android Beam desde otro dispositivo, etc. También es posible descargarlo desde un servidor web (se recomienda que sea un servidor propio, frente a servidores públicos de terceros), e incluso instalarlo directamente desde el navegador web Chrome proporcionado por defecto con Android. El certificado debe estar en formato DER (X.509) y tener extensión ".crt" o ".cer", aunque también son válidos los certificados contenidos en un almacén de claves PKCS#12 (extensión ".p12" o ".pfx"). Los archivos reconocidos como contenedores de certificados se representan con el icono de una huella dactilar en la app "Archivos".

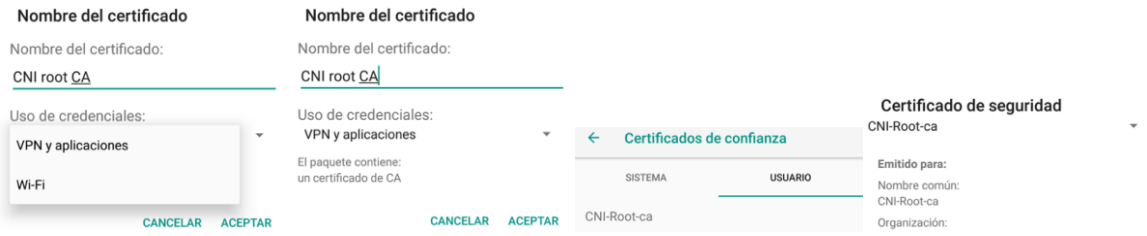

Figura 68 - Instalación de certificados de CA

19.1 CERTIFICADOS RAÍZ

Los certificados raíz corresponden a las autoridades certificadoras (*Certificate Authorities o* CAs), ya sean CAs raíz o intermedias.

A nivel de aplicación, además de disponerse de acceso a los certificados de las CAs incluidos en el AOSP, la app puede añadir anclajes de confianza (*trust anchors*) propios en su fichero "network-security-config.xml", para el acceso a dominios específicos.

Para poder añadir un nuevo certificado raíz al repositorio de credenciales, el dispositivo debe estar protegido por un método de acceso, cuya introducción se solicitará antes de proceder a la instalación del nuevo certificado.

Durante la importación del certificado debe indicarse:

- El nombre que se le quiere dar al certificado (servirá como identificador).
- El propósito de uso: "`VPN y aplicaciones`" o "`Wi-Fi`". Si un mismo certificado se va a emplear con ambos propósitos, deberá importarse dos veces.

Los certificados raíz o de CA añadidos por el usuario se pueden encontrar en la pestaña "Certificados de confianza - Usuario", mientras que los proporcionados por el sistema operativo están en "Certificados de confianza - Sistema". El nombre que se visualiza en esta pestaña para una CA raíz será el "*Common Name*" (CN) definido en el propio certificado, y no el nombre introducido por el usuario durante su importación. Mediante la selección del certificado digital es posible ver todos sus detalles.

El directorio "/system/etc/security/cacerts" contiene un fichero por cada uno de los certificados digitales asociados a las CAs de sistema suministradas por Android.

Por su parte, en el menú "Credenciales de usuario" se muestra el nombre proporcionado por el usuario durante la importación de:

- Los certificados raíz añadidos para uso de "VPN y aplicaciones". Estos certificados se pueden eliminar de forma individual desde el menú, seleccionando su nombre y pulsando "Quitar".
- Los certificados raíz añadidos para uso "Wi-Fi" pueden visualizarse desde este menú, pero no se permite eliminarlos desde él. El único modo conocido para eliminar los certificados para su uso en redes Wi-Fi es reseteando el almacén de credenciales completo mediante el menú "Eliminar certificados".
- Los certificados de usuario o cliente (ver apartado "19.2. Certificados hoja").

Desde la sección "Credenciales de usuario" no es posible visualizar los detalles de los certificados digitales que han sido importados en el dispositivo móvil.

Un certificado de CA se puede eliminar de la lista "Certificados de confianza - Usuario" seleccionándolo o pulsado el botón "Quitar".

También es posible instalar un certificado de CA para su uso en redes Wi-Fi corporativas desde el menú "+ Añadir red" (ver apartado "12.2.5. Uso de certificados en redes Wi-Fi empresariales").

Los certificados de CA importados por el usuario no se consideran de confianza por defecto, es decir, no serán aceptados por las apps debido al mecanismo de seguridad de tipo *certificate pinning*, implementado a través del fichero de la configuración de seguridad de red de las apps ("network_security_config.xml") vigente desde Android 7.

19.2 CERTIFICADOS HOJA

Se distinguen dos tipos de certificados digitales hoja o finales, debiendo ambos estar firmados por una CA que atestigüe su autenticidad:

- Servidor: tienen como finalidad proporcionar confianza en el servicio de cara a los clientes, por ejemplo, el servidor RADIUS de una red Wi-Fi corporativa o un servidor web.
- Usuario: destinados a autentificar al cliente de cara al uso de un servicio, por ejemplo, una app y su servidor o aplicación web asociados, una red Wi-Fi corporativa o un servidor VPN.

Si el fichero que contiene un certificado digital cliente es un almacén de claves, por ejemplo en formato PKCS#12, se solicitará al usuario la contraseña que fue empleada para proteger el fichero que contiene el certificado digital y la clave privada, y poder así extraer los contenidos del mismo. Al visualizar este tipo de certificados mediante el menú "`Credenciales de usuario`", se mostrará el texto "`una clave de usuario`" (clave privada) y "`un certificado de usuario`" (certificado con la clave pública). Si el fichero correspondiente al certificado también contiene el certificado de la CA que firmó dicho certificado, Android mostrará el texto "`un certificado de CA`" y "`un certificado de usuario`".

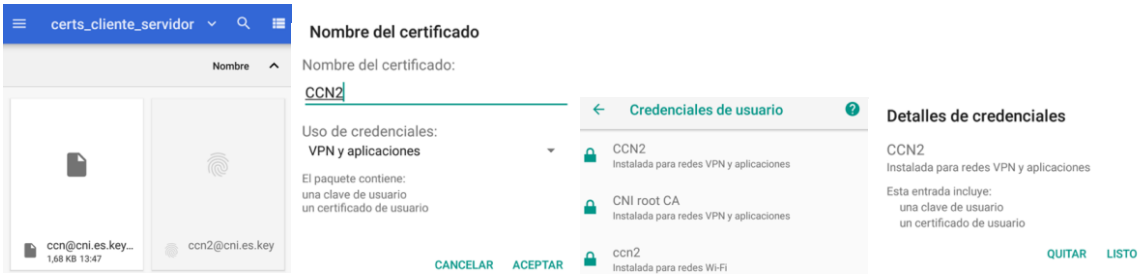

Figura 69 - Instalación de certificados de usuario

Durante la importación de un certificado cliente y su clave privada asociada, se solicitará al usuario un identificador para dicho certificado (por defecto se proporciona el valor del campo "*localKeyID*" del mismo). Se recomienda proporcionar un nombre de certificado que permita su selección de forma sencilla en las apps que hagan uso del certificado cliente (por ejemplo, para su selección en el navegador web de cara a un servicio web que requiera disponer de un certificado digital de usuario).

19.3 GESTIÓN DE CERTIFICADOS EN CHROME

Al acceder a un sitio web mediante HTTPS utilizando el navegador web Chrome existente en Android por defecto, el dispositivo móvil intentará verificar el certificado digital asociado y su cadena de confianza hasta la autoridad certificadora (CA) raíz correspondiente. Si la validación falla, Chrome generará un mensaje de advertencia, a través del cual, mediante la opción "`Opciones avanzadas`", se ofrecerá más información.

Para ver los datos de un certificado, se puede pulsar sobre el icono de la barra de navegación de Chrome y seleccionar "🔒" o "⚠") - `Detalles - Datos del certificado`".

Es importante tener en cuenta que, si se acepta un certificado, éste se almacenará en caché y se considerará válido mientras no se cierre la instancia de Chrome.

Desde el punto de vista de seguridad, ***se desaconseja aceptar certificados no válidos***. ***En caso de ser necesario hacerlo puntualmente, se debe cerrar el navegador web tan pronto haya finalizado la conexión al sitio web, y limpiar su caché***.

Chrome permite la instalación de certificados desde un servidor web, sin más que seleccionar el fichero que contiene el certificado y aceptar su importación.

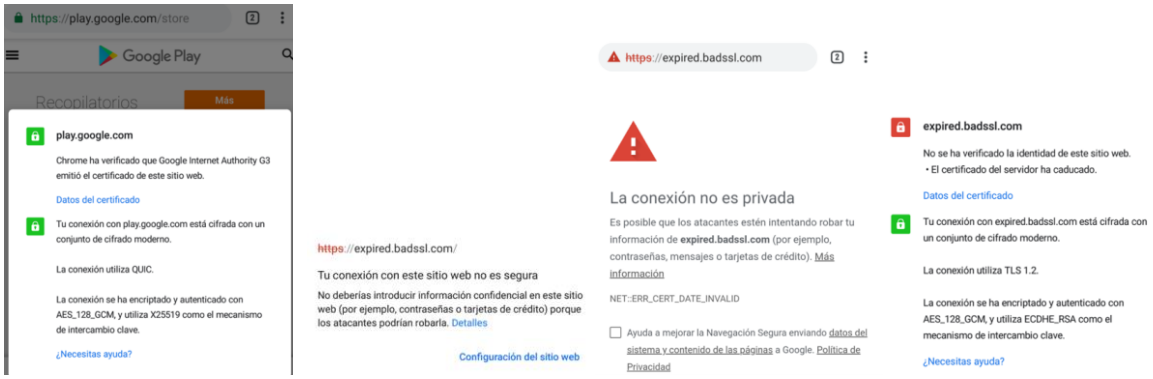

Figura 70 - Visualización de certificados digitales en Chrome

Por otra parte, los certificados cliente añadidos al almacén de credenciales están disponibles para su utilización en Chrome, permitiendo conectarse a sitios web que soliciten acceso mediante certificado digital cliente, ya que Chrome mostrará al usuario la lista de certificados disponibles, de la que podrá seleccionar el que corresponda.

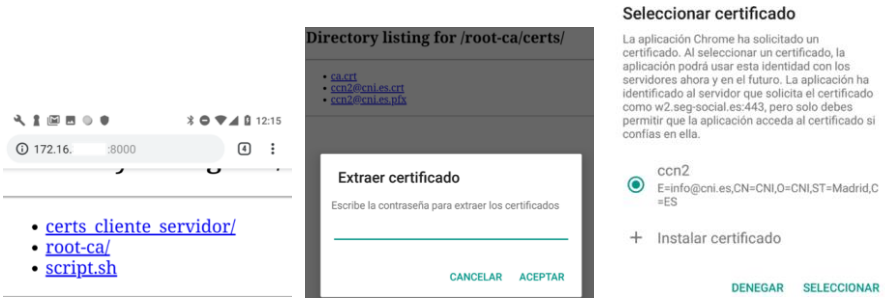

Figura 71 - Gestión de certificados digitales instalados en el sistema en Chrome

19.4 CERTIFICATE PINNING

Los mecanismos de *certificate pinning* (CP) proporcionan validación y protección de las comunicaciones autentificadas y cifradas mediante HTTPS (TLS), por ejemplo, durante la descarga de apps de la Play Store.

El CP consiste en una validación del certificado proporcionado por el servicio en el lado cliente, sin hacer uso de la infraestructura pública de certificados asociada a las CAs. Para que esta verificación sea posible, la app debe conocer previamente el certificado del servidor esperado (o su *fingerprint* criptográfico), es decir, debe disponer del pin. De este modo, cuando se establezca la conexión con el servidor, la app podrá comparar el *fingerprint* (o pin conocido) con el certificado recibido desde el servidor remoto. Si son idénticos, la conexión se considerará válida y la transferencia de datos se iniciará. Si no lo son, la app deberá interrumpir la negociación TLS y rechazar la conexión.

La característica "*Network Security Configuration*" (NSC) [Ref.- 51], introducida en Android 7, permite declarar en los ficheros de configuración XML de una app los *fingerprints* o pines que reconoce, adoptando así fácilmente el mecanismo de CP sin

ser necesarias modificaciones en el código de la app. De este modo, se dificulta mucho la ejecución de ataques basados en técnicas MitM (Man-in-the-Middle).

20.CIFRADO DEL DISPOSITIVO MÓVIL

Android dispone de capacidades para el cifrado de los datos almacenados en la memoria interna del dispositivo móvil de manera nativa, de forma que los mismos sólo se puedan acceder cuando el dispositivo está desbloqueado. El proceso de cifrado es irreversible y no es posible devolver el terminal a un estado sin cifrar, a menos que el dispositivo partiese desde fábrica de una versión de Android que no obligase al cifrado, en cuyo caso podría resetearse el terminal a los ajustes de fábrica.

Los dispositivos móviles pueden venir cifrados de fábrica o ser cifrados a posteriori. El estado de cifrado del dispositivo se comprueba a través del menú "`Seguridad y ubicación - Cifrado y credenciales`".

Los documentos de compatibilidad de Android 8 [Ref.- 52] establecen como requisito que los dispositivos que soporten AES (*Advanced Encrytion Standard*) con un rendimiento superior a 50MiB/segundo deben proporcionar cifrado de la partición de datos por defecto. Este es el caso del dispositivo Nexus 5x utilizado para la elaboración de la presente guía, que viene cifrado por defecto, por lo que no es posible ilustrar el proceso de cifrado[40]. Sin embargo, dispositivos de gama más baja comercializados bajo el programa "Android Go" (ver apartado "3.2. Android One y Android Go") no son capaces de ofrecer un rendimiento aceptable con el terminal cifrado, por lo que no están obligados a ofrecer mecanismos de cifrado "*out-of-the-box*".

En versiones de Android anteriores a 7, el mecanismo de cifrado de la partición de datos era el denominado "FDE" (*Full disk encryption*), que utilizaba una clave única protegida por el código de acceso del usuario para descifrar de forma global todos los contenidos de la partición de datos (ver apartado "20.1. Inicio seguro"). Con Android 7 se introdujo el mecanismo "FBE" (*File based encrytion*), que permite que el sistema pueda descifrar en el arranque solo los ficheros asociados a características básicas del sistema operativo y de ciertas apps (como, por ejemplo, alarmas, notificaciones y recepción de llamadas), lo cual permite un acceso limitado al sistema inmediatamente después de arrancar, sin la intervención del usuario, para pasar a descifrar el resto de datos más sensibles cuando el usuario valida el método de acceso (ver apartado "20.2. Direct Boot").

Para pasar de FDE a FBE es necesario acceder a las opciones de desarrollo "`Ajustes - [Sistema] {} Opciones para desarrolladores - Convertir a cifrado de archivo`". Es muy importante reseñar que esta operación implica un reseteo a fábrica y todos los datos del dispositivo móvil se perderán, como ilustra el mensaje de confirmación (se solicitará introducir el código de acceso antes de proceder a la conversión del tipo de cifrado). ***Se recomienda utilizar FBE desde el punto de vista de***

[40] Para obtener todos los detalles sobre el proceso de cifrado de un dispositivo móvil que parte sin cifrar desde fábrica, se recomienda consultar este mismo apartado en la "Guía CCN-STIC-453D - Seguridad de dispositivos móviles: Android 6.x" del CCN-CERT [Ref.- 406].

***seguridad*,** dado que aporta más granularidad y protección en el acceso a los datos, y dado que es el modelo de cifrado de referencia aplicado a las últimas versiones de Android, así como a versiones futuras.

Figura 72 - Conversión a cifrado de tipo FBE

En los dispositivos que soportan FBE, los datos pueden almacenarse en dos ubicaciones:

- *Credential encrypted* (CE) *storage*: almacenamiento basado en credenciales, disponible una vez el dispositivo móvil ha sido desbloqueado mediante el código de acceso, y que es el empleado por defecto por las apps. Este es el almacenamiento recomendado para los datos más sensibles.
- *Device Encrypted* (DE) *storage:* almacenamiento disponible tanto durante el arranque con "Direct Boot" como tras el desbloqueo del dispositivo móvil. Este almacenamiento es el recomendado para datos menos sensibles.

La utilización de FBE permite, en dispositivos multi-usuario, que cada usuario disponga de dos claves (una para cada tipo de almacenamiento) asociadas a su código de acceso, e independientes de las del resto de usuarios.

Para profundizar en los detalles de los cifrados FBE y FDE, se recomienda consultar el apartado "10. Cifrado de datos en Android" de la "Guía CCN-STIC-453E – Seguridad de dispositivos móviles: Android 7.x" [Ref.- 407].

20.1 INICIO SEGURO

El mecanismo de cifrado FDE impide acceder a cualquier contenido en claro del dispositivo móvil durante su arranque mientras no se haya validado el método de acceso, necesario para descifrar la partición de datos de usuario que almacena dichos contenidos. Esto impide tanto el uso de servicios de accesibilidad como de alarmas, llamadas y recepción de notificaciones si el dispositivo se reinicia de forma inesperada.

Como medio para evitar estos inconvenientes al hacer uso de FDE, se permite deshabilitar la opción "Inicio seguro" durante la configuración del código de acceso mediante PIN, patrón o contraseña. Si se selecciona la opción "No, gracias", Android utilizará la contraseña "default_password" (conocida e idéntica para todos los dispositivos Android) como contraseña para proteger la clave de cifrado AES maestra, utilizada para descifrar y montar la partición de datos ("/data") durante el proceso de arranque, y permitir la recepción de notificaciones, alarmas y llamadas. Con este modelo, una vez iniciado el sistema operativo Android, para poder acceder al dispositivo móvil seguirá siendo necesario introducir el código de acceso en la pantalla de bloqueo. Si se acepta el uso de "Inicio seguro", por el contrario, la clave de cifrado utilizada para

desbloquear el acceso a la funcionalidad básica del dispositivo estará protegida por el PIN, patrón o contraseña definidos por el usuario (y no por una contraseña por defecto). La forma para saber si un dispositivo utiliza FDE es precisamente ver que se presenta el menú "Requerir <código> para iniciar dispositivo" durante la configuración del código de acceso.

Los dispositivos Nexus 5x no incorporan Android 8 de fábrica, por lo que siguen utilizando un modelo de cifrado de tipo FDE, y pueden hacer uso del mecanismo de "Inicio seguro", aunque también pueden convertirse a FBE según lo descrito anteriormente.

20.2 DIRECT BOOT

El modelo de arranque "Direct Boot" surge a la par que el cifrado FBE para permitir que un dispositivo móvil pueda ofrecer parte de su funcionalidad sin que el usuario haya validado aún el método de acceso, empleado para el cifrado de la partición de datos, durante el proceso de arranque.

El acceso a datos en modo "Direct Boot" es restringido: así por ejemplo, aunque se permite recibir llamadas, no se mostrará la información del contacto que la realiza; en el caso de la recepción de SMS, se recibirá la notificación de su llegada, pero no se mostrarán los detalles hasta que el dispositivo sea desbloqueado.

Las aplicaciones que no son de sistema pueden marcar determinados datos con un atributo que permite que estos estén disponibles durante el arranque (Direct Boot).

21. COPIAS DE SEGURIDAD Y RESTAURACIÓN

Un elemento fundamental para la protección del dispositivo móvil y sus datos es mantener una política de copias de seguridad (*backups*) adecuada, especialmente antes de proceder a la actualización del sistema operativo, o si se requiere instalar nuevas apps de mercados no oficiales (opción desaconsejada). Las dos alternativas para albergar las copias de seguridad son el uso de un ordenador personal localmente y el uso servicios en la nube, como Google Drive, suministrados por defecto con Android.

En el caso de dispositivos móviles Android multi-usuario, únicamente el usuario propietario puede gestionar las opciones de copia de seguridad y restauración.

21.1 COPIA DE SEGURIDAD LOCAL

Estas copias se realizan a través del mecanismo ADB invocado desde un ordenador al que se conecta el dispositivo móvil mediante un cable USB, por lo que requieren que las capacidades de depuración estén habilitadas (ver apartado "15.2. Opciones para desarrolladores – Depuración"), aunque la recomendación es

deshabilitarlas una vez completado el proceso de *backup*. Asimismo, se recomienda que la versión de las "*Platform Tools*" empleada en el ordenador esté actualizada[41].

Las apps que incluyan en su fichero *manifest* que no desean ser incluidas en la copia de seguridad quedarán excluidas del proceso de copia.

El comando "`adb`" recomendado para realizar un backup manual es:

```
C:\> adb backup -f Android_8x_backup.ab -all -system -shared -apk
Now unlock your device and confirm the backup operation...
```

Figura 73 - Comando adb para copia de seguridad local

El dispositivo móvil mostrará una pantalla de confirmación para autorizar la realización de la copia de seguridad, en la que se solicitará la introducción (opcional) de una contraseña para proceder a cifrar los contenidos del backup. ***Se recomienda proteger el backup con una contraseña de al menos 8 caracteres***, ya que, en caso contrario, el fichero resultante (que emplea un formato "`tar`" propietario) podría ser leído en claro con herramientas disponibles públicamente.

La opción de desarrollo "`Contraseña para copias de ordenador`" permite establecer un código alfanumérico para proteger las copias realizadas con "`adb backup`" por defecto. Si no se desea especificar una contraseña cada vez, ***se recomienda configurarlo***.

Para restaurar una copia de seguridad local, se dispone del comando "`adb restore`", que solicitará que el dispositivo esté desbloqueado, así como la confirmación de la contraseña empleada para el cifrado del backup, si el usuario o la opción "`Contraseña para copias de ordenador`" lo establecieron al realizar la copia de seguridad.

21.2 COPIA DE SEGURIDAD EN LA NUBE

El proceso de backup de Android también permite realizar las copias de seguridad en la nube de Google, empleando las capacidades de almacenamiento de Google Drive.

Para habilitar la copia de seguridad en Google Drive, se dispone del menú "`Ajustes - Sistema - Avanzado - Copia de seguridad - Copia de seguridad en Google Drive`", que requiere de la existencia de una cuenta de usuario de Google activa en el dispositivo. Si hay varias cuentas de usuario de Google configuradas en el dispositivo móvil, será necesario elegir aquella sobre la que se realizará la copia de seguridad mediante la opción "`Cuenta`". Pulsando sobre cada componente de la sección "[`Copias de seguridad activas`]" se mostrará información sobre los datos que se salvan como parte del *backup* de dicho componente. En algunos casos, como el de "`Fotos y vídeos`", se ofrecen también opciones de selección de carpetas, realización de copias en itinerancia, o utilización en redes de datos móviles.

[41] https://developer.android.com/studio/releases/platform-tools#downloads

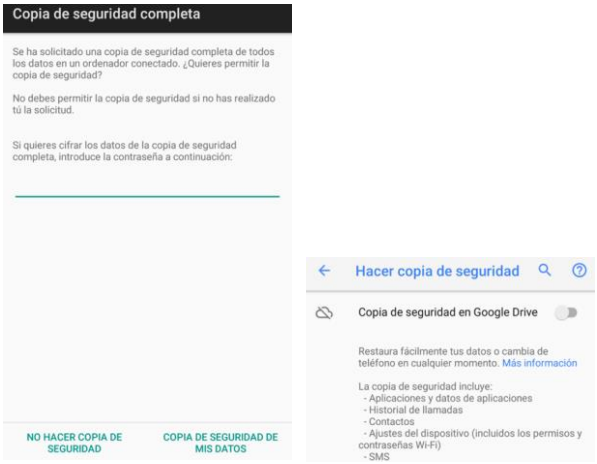

Figura 74 - Copia de seguridad local (izquierda) y en la nube (derecha)

Los datos que se incluirán en la copia de seguridad de la nube de Google se describen en [Ref.- 60]. Para saber qué apps están salvando actualmente sus datos mediante este procedimiento, se puede acceder al menú "`Datos de aplicaciones - Datos de aplicaciones con copia de seguridad`".

La gestión de las copias de seguridad en el dispositivo móvil se realiza a través de la app `Drive`, mediante la opción de menú "`Copias de seguridad`", en la cual se incluyen las copias realizadas sobre todos los dispositivos asociados a la cuenta de Google.

La restauración parcial de los datos guardados en una copia de seguridad de `Drive` se puede realizar cuando se reinstala una app cuyos datos se almacenaron en ella, para lo cual es preciso que el ajuste "`Datos de aplicaciones - Restauración automática`" esté activo. La restauración total de la copia se realiza durante la configuración inicial del propio dispositivo tras un reseteo a fábrica, o sobre un nuevo dispositivo al que se asocia la misma cuenta de Google que la empleada para hacer la copia de seguridad.

Para obtener información más detallada sobre el proceso de copias de seguridad en la nube de Google, se recomienda consultar el apartado "13. Copias de Seguridad" de la "Guía CCN-STIC-456 – Cuenta de usuario, servicios y aplicaciones de Google para dispositivos móviles Android" [Ref.- 408].

22.ELIMINACIÓN DE DATOS DEL DISPOSITIVO MÓVIL

Para eliminar completamente todos los datos del dispositivo móvil, incluyendo las cuentas de usuario de Google, la configuración y datos de las apps y del sistema (incluyendo las tarjetas de almacenamiento externas), así como las apps de terceros previamente descargadas e instaladas, se requiere llevar a cabo un proceso de restablecimiento a fábrica, que se desencadena mediante el menú "`Ajustes - Sistema - Opciones de recuperación - Borrar todos los datos`", y que requiere introducir el código de acceso. Tras la restauración, únicamente permanecerá el software del sistema operativo y las actualizaciones de sistema ya aplicadas.

El borrado completo del dispositivo móvil también puede iniciarse de forma remota desde una aplicación de tipo "administrador de dispositivos" (ver apartado "10. Seguridad y ubicación"), como "`Encontrar mi dispositivo`". Los detalles de uso de esta funcionalidad se pueden consultar en el apartado "10.4. Gestión remota de dispositivos Android por parte del usuario" de la "Guía CCN-STIC-456 – Cuenta de usuario, servicios y aplicaciones de Google para dispositivos móviles Android" [Ref.-408], en la cual se describe dicho servicio detalladamente.

Además del borrado completo (restablecimiento a fábrica), se dispone de varias opciones para restablecer ajustes parciales del dispositivo móvil:

- La opción "`Ajustes - Sistema - Opciones de recuperación - Restablecer Wi-Fi, red móvil y Bluetooth`" permite restablecer todos los ajustes de red, incluyendo los asociados a redes Wi-Fi, redes móviles y Bluetooth.
- La opción "`Ajustes - Aplicaciones y notificaciones - Recuperar ajustes de aplicaciones`" devuelve a la configuración de fábrica los ajustes de las apps relativos a notificaciones, habilitación, aplicaciones predeterminadas, restricciones de datos móviles y permisos.
- La opción "`Borrar todos los datos`" resetea el dispositivo móvil a la configuración de fábrica, eliminando todos los datos. Solicita validación del método de acceso y confirmación adicional.

En caso de olvido del código de acceso, el usuario deberá restablecer los ajustes de fábrica desde el menú de recuperación (*Recovery*) del terminal (según se ilustra en el apartado "25. anexo b: índice de figuras

Anexo c: Modos de arranque del dispositivo móvil"), y seleccionar la opción "**`Wipe data/Factory reset`**". Se eliminarán todos los datos del dispositivo móvil, y, al reiniciar el terminal, se iniciará el proceso de configuración desde cero.

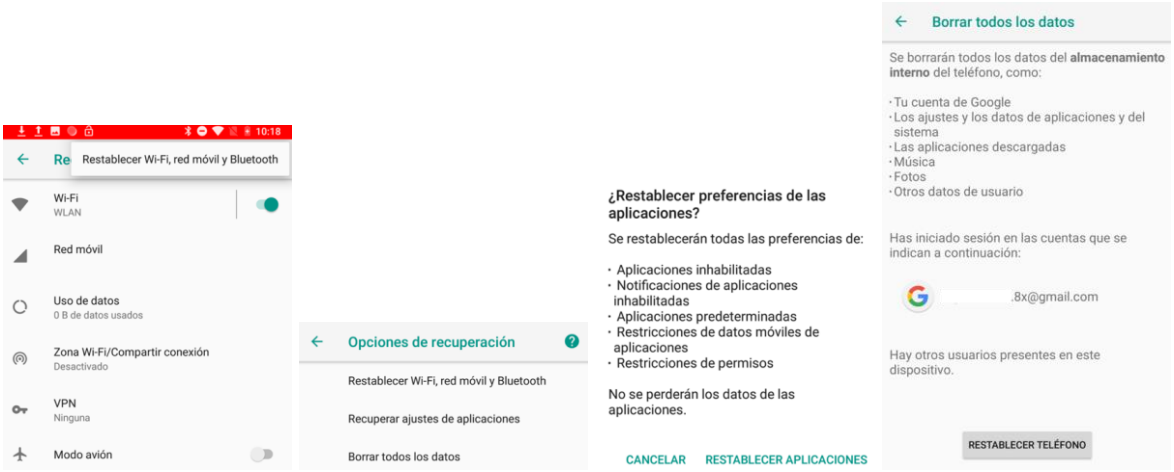

Figura 75 - Mecanismos de eliminación de datos del dispositivo móvil

23. RESUMEN DE LAS RECOMENDACIONES DE SEGURIDAD DE ANDROID 8

	Decálogo Básico de Seguridad
1	Proteger el acceso al dispositivo móvil mediante un código de acceso robusto, preferiblemente una contraseña alfanumérica, de al menos 8 caracteres, y que no esté directamente relacionado con información del usuario. La opción "Mostrar contraseñas" debe desactivarse, así como la de "Mostrar el patrón dibujado" (si se utiliza un patrón). Se debe configurar un bloqueo de pantalla automático que se active a la mayor brevedad posible desde que el usuario deje de interaccionar con el dispositivo, y habilitar la opción para que el código de acceso se solicite inmediatamente tras bloquearse la pantalla.
2	Mantener el dispositivo móvil actualizado, preferiblemente sin activar la opción de "Actualizaciones del sistema automáticas", y realizando una copia de seguridad previa a la actualización. La copia de seguridad debe estar protegida mediante una contraseña, y, de ser posible, realizarse en un ordenador de confianza, frente a las copias en Google Drive.
3	Cifrar el contenido del dispositivo móvil, si éste no viene cifrado de fábrica. Primar el modelo de cifrado FBE frente a FDE y, en caso de hacer uso de FDE, debe activarse el inicio seguro.
4	Eliminar del menú de ajustes rápidos las opciones más sensibles, en especial, "Modo avión", "No molestar", "Zona Wi-Fi", "Wi-Fi", "Bluetooth" y "Datos móviles". En su lugar, se pueden crear los correspondientes "Widgets" para minimizar el impacto en la usabilidad.
5	Evitar la conexión a redes Wi-Fi abiertas y ocultas, prefiriendo establecer conexiones de datos a través de un *hotspot* Wi-Fi de uso personal (el cual debe desactivarse tan pronto finalice la necesidad de uso). Desactivar los interfaces Wi-Fi y Bluetooth cuando no se estén utilizando, pero mantener activa la conexión de datos móviles para permitir (si se usan los servicios asociados a la cuenta de usuario de Google) la localización del dispositivo móvil a través del servicio "Encontrar mi dispositivo". Desactivar el interfaz NFC y el servicio "Android Beam".
6	Limitar los permisos concedidos a las apps, especialmente los de "acceso especial", los asociados a la ubicación y todos aquellos que no estén relacionados con la funcionalidad que las apps tienen por objeto. Evitar la presentación del contenido de las notificaciones en la pantalla de bloqueo, especialmente para las apps más sensibles. Desinstalar todas aquellas apps que no se usen expresamente.
7	Utilizar un gestor de contraseñas de confianza para evitar la reutilización de contraseñas o la selección de contraseñas débiles, pero sin emplearlo para las contraseñas más sensibles. Evitar el uso de los servicios "autocompletar" para relleno de contraseñas y "Smart Lock para contraseñas".
8	Utilizar las "Opciones para desarrolladores" para añadir las opciones de seguridad recomendadas, y desactivarlas una vez se haya completado la configuración.
9	Dado que la existencia de una cuenta de usuario de Google es requerida para poder instalar y actualizar apps, se recomienda aplicar las recomendaciones de seguridad de la "Guía CCN-STIC-456 - Cuenta de usuario, servicios y aplicaciones de Google para dispositivos móviles Android" [Ref.- 408] y, preferiblemente proceder a cerrar la sesión en cuanto se hayan instalado o actualizado las apps.
10	El dispositivo móvil no debe dejarse desatendido, menos aun estando la pantalla desbloqueada. Si, a pesar de estar desaconsejado, fuese necesario prestarlo temporalmente a un tercero, utilizar la funcionalidad "Fijar pantalla" (con solicitud de PIN activa) con la app que se requiera compartir o, en caso de precisarse un uso del terminal más amplio, crear un perfil de usuario específico y borrarlo tan pronto cese la necesidad de compartición. En ningún caso se debe habilitar la opción "Añadir usuarios desde la pantalla de bloqueo".

24.ANEXO A. REFERENCIAS

Referencia	Título, autor y ubicación
[Ref.- 1]	Nexus. Google. URL: https://www.google.com/intl/es_es/nexus/
[Ref.- 2]	Pixel. Google. URL: https://store.google.com/product/pixel_3 URL: https://store.google.com/product/pixel_2_xl
[Ref.- 3]	Open Handset Alliance (OHA). URL: https://www.openhandsetalliance.com
[Ref.- 4]	Source. Android. URL: http://source.android.com
[Ref.- 5]	Android. Open Handset Alliance. URL: https://www.openhandsetalliance.com/android_overview.html
[Ref.- 6]	Smartphone Market Share. IDC. URL: https://www.idc.com/promo/smartphone-market-share/os
[Ref.- 7]	Here comes Treble: A modular base for Android. Android Developers Blog. URL: https://android-developers.googleblog.com/2017/05/here-comes-treble-modular-base-for.html
[Ref.- 8]	Treble experimentations. Thomas Maier. URL: https://github.com/phhusson/treble_experimentations/wiki
[Ref.- 9]	Plazos de las actualizaciones de Android en teléfonos Pixel y dispositivos Nexus. Google. URL: https://support.google.com/nexus/answer/4457705#nexus_devices
[Ref.- 10]	Factory Images for Nexus and Pixel Devices. Android developers. URL: https://developers.google.com/android/images
[Ref.- 11]	Android 8.0 Features and APIs. Android developers. URL: https://developer.android.com/about/versions/oreo/android-8.0
[Ref.- 12]	Android 8.0 Behavior Changes. Android developers. URL: https://developer.android.com/about/versions/oreo/android-8.0-changes.html
[Ref.- 13]	A/B (Seamless) System Updates. Android source. URL: https://source.android.com/devices/tech/ota/ab
[Ref.- 14]	Android Security Bulletins. Android source. URL: https://source.android.com/security/bulletin
[Ref.- 15]	Android One. Google. URL: https://www.android.com/one/
[Ref.- 16]	Android Security Center. Android. URL: https://www.android.com/security-center/
[Ref.- 17]	Security for Android Developers. Android developers. URL: https://developer.android.com/topic/security/
[Ref.- 18]	Android security discussions. Google. URL: https://groups.google.com/forum/#!forum/android-security-discuss
[Ref.- 19]	e-mail: security@android.com
[Ref.- 20]	Security. Android source. URL: https://source.android.com/security URL: https://source.android.com/security/overview/updates-resources
[Ref.- 21]	Android Security Bulletins. Android source. URL: https://source.android.com/security/bulletin
[Ref.- 22]	Android Vulnerabilities. Universidad de Cambridge. URL: http://androidvulnerabilities.org
[Ref.- 23]	Full OTA Images for Nexus and Pixel Devices. Google. URL: https://developers.google.com/android/ota

Referencia	Título, autor y ubicación
[Ref.- 24]	Android Debug Bridge (ADB). Android Developers. URL: http://developer.android.com/guide/developing/tools/adb.html
[Ref.- 25]	Configure on-device developer options. Android Developers. URL: https://developer.android.com/studio/debug/dev-options
[Ref.- 26]	Unlock with your fingerprint. Google. URL: https://support.google.com/nexus/answer/6285273
[Ref.- 27]	Android 8 Compatibility Definition. Google. URL: https://source.android.com/compatibility/8.1/android-8.1-cdd.html
[Ref.- 28]	Reiniciar dispositivos en modo seguro para detectar aplicaciones problemáticas en Android. Google. URL: https://support.google.com/nexus/answer/2852139?hl=es
[Ref.- 29]	Create and Manage Notification Channels. Android developers. URL: https://developer.android.com/training/notify-user/channels
[Ref.- 30]	Limitar las interrupciones con el modo No molestar en Android. Google. URL: https://support.google.com/android/answer/9069335?hl=es
[Ref.- 31]	Amber alert. Wikipedia. URL: https://en.wikipedia.org/wiki/Amber_alert
[Ref.- 32]	Final removal of trust in WoSign and StartCom Certificates. Google Security Blog. URL: https://security.googleblog.com/2017/07/final-removal-of-trust-in-wosign-and.html
[Ref.- 33]	Perfiles de trabajo. Google. URL: https://support.google.com/work/android/answer/6191949?hl=es
[Ref.- 34]	Changes to Device Identifiers in Android O. Android Developers Blog. URL: https://android-developers.googleblog.com/2017/04/changes-to-device-identifiers-in.html
[Ref.- 35]	Android Accesibility Help. Google. URL: https://support.google.com/accessibility/android#topic=6007234
[Ref.- 36]	Gestionar los ajustes de ubicación de tu dispositivo. Google. URL: https://support.google.com/accounts/answer/3467281?hl=es
[Ref.- 37]	Google Duo. Play Store. URL: https://play.google.com/store/apps/details?id=com.google.android.apps.tachyon&hl=en
[Ref.- 38]	Bluetooth Services. Android Source. URL: https://source.android.com/devices/bluetooth/services
[Ref.- 39]	Cómo interactuar con lo que está a tu alrededor. Google. URL: https://support.google.com/accounts/answer/6260286?hl=es-419
[Ref.- 40]	Nearby. Android Developers. URL: https://developers.google.com/nearby/
[Ref.- 41]	Android 8.0 - Oreo. Android.com. URL: https://www.android.com/versions/oreo-8-0/
[Ref.- 42]	Wi-Fi Infrastructure Features. Android developers. URL: https://source.android.com/devices/tech/connect/wifi-infrastructure
[Ref.- 43]	Conectarse a redes Wi-Fi en un teléfono Pixel. Google. URL: https://support.google.com/pixelphone/answer/2819519?hl=es
[Ref.- 44]	Wi-Fi scanning overview. Android Developers. URL: https://developer.android.com/guide/topics/connectivity/wifi-scan#wifi-scan-restrictions
[Ref.- 45]	Android O to drop insecure TLS version fallback in HttpsURLConnection. Android Developers Blog. URL: https://android-developers.googleblog.com/2017/04/android-o-to-drop-insecure-tls-version.html
[Ref.- 46]	Wi-Fi Aware. WiFi Alliance. URL: https://www.wi-fi.org/discover-wi-fi/wi-fi-aware
[Ref.- 47]	"Use your favorite password manager with Android Oreo". Google Blog. URL: https://www.blog.google/products/android/use-your-favorite-password-manager-android-oreo/
[Ref.- 48]	RFC 7858: Specification for DNS over Transport Layer Security (TLS). IETF. URL: https://tools.ietf.org/html/rfc7858

Referencia	Título, autor y ubicación
[Ref.- 49]	RFC 7844: Anonymity Profiles for DHCP Clients. IETF. URL: https://tools.ietf.org/html/rfc7844
[Ref.- 50]	Verified Boot - Boot Flow. Android Source. URL: https://source.android.com/security/verifiedboot/boot-flow
[Ref.- 51]	Network security configuration. Android developers. URL: https://developer.android.com/training/articles/security-config
[Ref.- 52]	Android 8 Compatibility Definition. Android Source. URL: https://source.android.com/compatibility/8.0/android-8.0-cdd
[Ref.- 53]	Enabling Adiantum. Android Source. URL: https://source.android.com/security/encryption/adiantum
[Ref.- 54]	Introducing Adiantum: Encryption for the Next Billion Users. Google Security Blog. URL: https://security.googleblog.com/2019/02/introducing-adiantum-encryption-for.html
[Ref.- 55]	Discontinuing support for Android Nearby Notifications. Android developers blog. URL: https://android-developers.googleblog.com/2018/10/discontinuing-support-for-android.html
[Ref.- 56]	App Actions. Android developers. URL: https://developer.android.com/guide/actions/ Slices. Android developers. URL: https://developer.android.com/guide/slices/
[Ref.- 57]	Settings.Secure. Android developers. URL: https://developer.android.com/reference/android/provider/Settings.Secure
[Ref.- 58]	Permissions overview. Android developers. URL: https://developer.android.com/guide/topics/permissions/overview#normal-dangerous
[Ref.- 59]	Making it safer to get apps on Android O. Android Developers Blog. URL: https://android-developers.googleblog.com/2017/08/making-it-safer-to-get-apps-on-android-o.html
[Ref.- 60]	Gestionar y restaurar las copias de seguridad de un dispositivo en Google Drive. Google. URL: https://support.google.com/drive/answer/6305834?co=GENIE.Platform%3DAndroid&hl=es

Referencia	Título, autor y ubicación
[Ref.- 400]	"Guía CCN-STIC-450 - Seguridad de dispositivos móviles". CCN-CERT. Marzo 2013. URL: 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
[Ref.- 401]	"Guía CCN-STIC-453(A) - Seguridad de dispositivos móviles: Android 2.x". CCN-CERT. Mayo 2013. URL: https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/11-ccn-stic-453-seguridad-en-android/file.html
[Ref.- 402]	"Guía CCN-STIC-453B - Seguridad de dispositivos móviles: Android 4.x". CCN-CERT. Abril 2015. URL: 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
[Ref.- 403]	"Guía CCN-STIC-457 - Gestión de dispositivos móviles: MDM (Mobile Device Management)". CCN-CERT. Noviembre 2013. URL: 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
[Ref.- 404]	"Buenas Prácticas. CCN-CERT BP-03/16. Dispositivos móviles". CCN-CERT. Octubre 2016. URL: https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/1757-ccn-cert-bp-03-16-dispositivos-moviles/file.html
[Ref.- 405]	"Guía CCN-STIC-453C - Seguridad de dispositivos móviles: Android 5.x". CCN-CERT. Marzo 2018. URL: https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2733-ccn-stic-453c-seguridad-en-android-5-x/file.html

Referencia	Título, autor y ubicación
[Ref.- 406]	"Guía CCN-STIC-453D - Seguridad de dispositivos móviles: Android 6.x". CCN-CERT. Junio 2018. URL: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2901-ccn-stic-453d-seguridad-de-dispositivos-moviles-android-6-x/file.html
[Ref.- 407]	"Guía CCN-STIC-453E - Seguridad de dispositivos móviles: Android 7.x". CCN-CERT. Septiembre 2018. URL: https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3040-ccn-stic-453e-seguridad-de-dispositivos-moviles-android-7-x.html
[Ref.- 408]	"Guía CCN-STIC-456 - Cuenta de usuario, servicios y aplicaciones de Google para dispositivos móviles Android". CCN-CERT. Septiembre 2018. URL: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3043-ccn-stic-456-cuenta-de-usuario-servicios-aplicaciones-google-para-dispositivos-moviles-android/file.html
[Ref.- 409]	"Guía CCN-STIC-454 - Seguridad en iPad". CCN-CERT. Agosto 2014. URL: https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/12-ccn-stic-454-seguridad-en-ipad.html
[Ref.- 410]	"Guía CCN-STIC-455 - Seguridad en iPhone". CCN-CERT. Agosto 2014. URL: https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/13-ccn-stic-455-seguridad-en-iphone.html
[Ref.- 411]	"Guía CCN-STIC-455C - Guía Práctica de Seguridad en Dispositivos Móviles iPhone (iOS 11.x)". URL: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3161-ccn-stic-455c-guia-practica-de-seguridad-en-dispositivos-moviles-iphone-ios-11x-1/file.html
[Ref.- 412]	"Guía CCN-STIC-455D - Guía Práctica de Seguridad en Dispositivos Móviles iPhone (iOS 12.x)". URL: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3158-ccn-stic-455d-guia-practica-de-seguridad-en-dispostivos-moviles-iphone-ios-12/file.html
[Ref.- 413]	"Informe Anual 2018. Dispositivos y comunicaciones móviles". CCN-CERT. Febrero 2019. URL: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3464-ccn-cert-ia-04-19-informe-anual-2018-dispositivos-moviles/file.html

25.ANEXO B: ÍNDICE DE FIGURAS

26.ANEXO C: MODOS DE ARRANQUE DEL DISPOSITIVO MÓVIL

Los dispositivos móviles Nexus 5x tienen 3 modos de arranque, que pueden seleccionarse encendiendo el dispositivo mediante la combinación de teclas "`Power + bajar volumen`": `Start` (Normal, modo por defecto), `Recovery` (Recuperación) y `Bootloader` (Gestor de arranque).

Para reiniciar el dispositivo móvil en un modo concreto, se requiere emplear uno de estos dos métodos:

a) El comando "`adb reboot <modo>`". Por ejemplo, "`adb reboot bootloader`" para entrar en el menú del gestor de arranque, o "`adb reboot recovery`" para entrar en el menú de recuperación.
b) Con el dispositivo apagado, utilizar la combinación de teclas "`Power + bajar volumen`", y desplazarse con las teclas de bajar/subir volumen por los diferentes modos.

Una vez se muestre el modo deseado, presionar el botón "`Power`" para entrar en él. Cada modo ofrece diferentes opciones. Las principales para la operación del terminal son:

- Menú "*Recovery*": este modo se identifica por el símbolo de un androide tumbado con un triángulo que contiene una admiración de color rojo (/!\) y el texto "*No command*". Para acceder a las opciones del menú "*Recovery*", hay que presionar el botón de "`Power`" y seguidamente el de "`Subir volumen`" de forma sostenida. Desde este menú se permite realizar actualizaciones manuales y resetear el dispositivo a los ajustes de fábrica.
- Menú "*Bootloader*": permite bloquear/desbloquear el gestor de arranque.

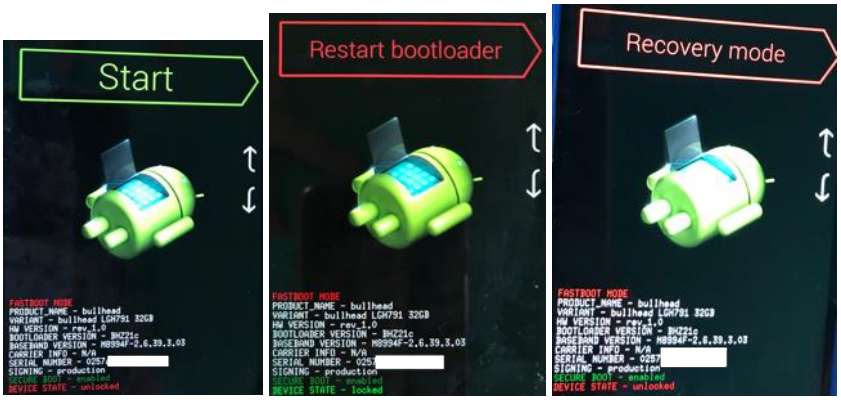

Figura 76 - Gestor de arranque

Figura 77 - Menú de recuperación del Nexus 5x