GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

CCN
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 456

Cuenta de usuario, servicios y aplicaciones de Google para dispositivos móviles Android

Septiembre 2018

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2018.09.17 18:47:53 +02'00'

NIPO: 083-19-017-3

Fecha de Edición: septiembre de 2018

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

PRÓLOGO

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

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

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

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

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

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

Septiembre de 2018

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN

1. El desarrollo de los dispositivos y comunicaciones móviles, y de las tecnologías inalámbricas, en los últimos años ha revolucionado la forma de trabajar y comunicarse. El uso creciente de estas tecnologías sitúa a los dispositivos móviles como uno de los objetivos principales de las ciberamenazas.

2. La proliferación de dispositivos móviles en los últimos años, junto al aumento de las capacidades, prestaciones y posibilidades de utilización de los mismos, hace necesario evaluar en profundidad la seguridad ofrecida por este tipo de dispositivos respecto a la información que gestionan, profundizando en los mecanismos de protección que ofrecen, dentro de los entornos de Tecnologías de la Información y las Comunicaciones (TIC).

3. Se considera dispositivo móvil aquel dispositivo electrónico de uso personal o profesional y reducido tamaño que permite la gestión de información (almacenamiento, intercambio y procesamiento de información) y el acceso a redes de comunicaciones y servicios remotos, tanto de voz como de datos, y que habitualmente dispone de capacidades de telefonía, como por ejemplo teléfonos móviles, *smartphones* (teléfonos móviles avanzados o inteligentes), *tablets* (o tabletas) y agendas electrónicas (PDAs, Personal Digital Assistants), independientemente de sí disponen de teclado físico o pantalla táctil.

4. Pese a que los dispositivos móviles se utilizan para establecer comunicaciones personales y profesionales, privadas y relevantes, y para el almacenamiento e intercambio de información sensible, el nivel de percepción de la amenaza de seguridad real existente no ha tenido la suficiente trascendencia en los usuarios finales y las organizaciones.

5. La concienciación, el sentido común y las buenas prácticas en la configuración y el uso de los dispositivos móviles constituyen una de las mejores defensas para prevenir y detectar este tipo de incidentes y amenazas [Ref.- 404].

6. En paralelo con la creciente utilización de este tipo de dispositivos, se han desarrollado servicios complementarios "en la nube", los cuales pretenden proporcionar al usuario una experiencia común a los diversos dispositivos (móviles y tradicionales) que emplee, independientemente de sus plataformas, sistemas operativos y fabricantes, y que tenga continuidad de forma inmediata, aunque migre o incorpore un nuevo dispositivo.

7. Este tipo de servicios, sin embargo, llevan implícita la transferencia de datos personales y empresariales, de mayor o menor sensibilidad, a servidores externos, gestionados por organizaciones ajenas a la propia, con el consiguiente interrogante de cómo el responsable de dichos servicios custodia dichos datos y de qué uso puede estar haciendo de ellos.

8. El presente documento realiza un análisis detallado de los mecanismos y la configuración de seguridad recomendados para uno de los principales elementos vinculados al uso de dispositivos móviles Android: la cuenta de usuario de Google y sus servicios asociados.

9. Esta guía se ha elaborado utilizando un dispositivo móvil Google Nexus 5X con versión 7.x de Android (en concreto, 7.1.2), con el objetivo de reducir su superficie de exposición frente a ataques de seguridad y/o privacidad.
10. La versión de la app "Google" empleada para la elaboración de la presente guía es concretamente la 8.13.15.21, que estuvo disponible a finales de julio y principios de agosto de 2018.
11. Dado que la mayor parte de las opciones de configuración asociadas a la cuenta de usuario de Google son específicas de la app "Google" y no tanto de la versión concreta de Android, esta guía es de aplicación para diversas versiones de Android, siempre que soporten la app "Google" (desde Android 6.x en adelante) o "Ajustes de Google" (para Android 5.x).
12. Adicionalmente, es importante reseñar que la mayor parte de las recomendaciones descritas asociadas al interfaz web de gestión de la cuenta de usuario de Google a lo largo de la presente guía son de aplicación no solo para dispositivos móviles con otras versiones de Android, sino también para dispositivos móviles basados en plataformas de otros fabricantes, como Apple y Microsoft.

2. OBJETO

13. El propósito del presente documento es definir una lista de recomendaciones de seguridad y privacidad asociadas al uso de una cuenta de usuario de Google como parte de la configuración de dispositivos móviles basados en el sistema operativo Android (en adelante, Android) [Ref.- 1], cuyo objetivo es proteger tanto el propio dispositivo móvil y sus comunicaciones como la información y datos que gestiona y almacena en servidores externos de Google y, muy en particular, la información de carácter más sensible y confidencial.
14. La presente guía proporciona los detalles específicos (asociados a los servicios de Google), complementando a los detalles de aplicación e implementación de las recomendaciones de seguridad generales descritas en la guía inicial de esta misma serie [Ref.- 400], que presenta la información necesaria para la evaluación y análisis de los riesgos, amenazas, y vulnerabilidades de seguridad a las que están expuestos los dispositivos móviles en la actualidad, y a la guía específica de "Seguridad de dispositivos móviles: Android 7.x" [Ref.- 407], publicada en 2018.
15. La serie CCN-STIC-450, "Seguridad de dispositivos móviles", se ha estructurado en dos niveles: una guía genérica inicial centrada en al análisis de seguridad de dispositivos móviles (CCN-STIC-450) [Ref.- 400], complementada por guías específicas para los principales sistemas operativos empleados por los dispositivos móviles hoy en día (o en el pasado). Por este motivo, antes de la lectura y aplicación de la presente guía, asociada a la cuenta de usuarios y servicios de Google, se recomienda la lectura de la guía general de seguridad, CCN-STIC-450.
16. Adicionalmente, se recomienda la lectura de las guías de la serie CCN-STIC-450 asociadas a otros sistemas operativos y versiones de plataformas móviles, en caso de ser necesaria su aplicación en otros terminales, y a la gestión empresarial de dispositivos móviles (MDM):

- CCN-STIC-450 - Seguridad de dispositivos móviles [Ref.- 400]
- CCN-STIC-451 - Seguridad de dispositivos móviles: Windows Mobile 6.1
- CCN-STIC-452 - Seguridad de dispositivos móviles: Windows Mobile 6.5
- CCN-STIC-453(A) - Seguridad de dispositivos móviles: Android 2.x [Ref.- 401]
- CCN-STIC-453B - Seguridad de dispositivos móviles: Android 4.x [Ref.- 402]
- CCN-STIC-453C - Seguridad de dispositivos móviles: Android 5.x [Ref.- 405]
- CCN-STIC-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)
- CCN-STIC-455(A) - Seguridad de dispositivos móviles: iPhone (iOS 7.x)
- CCN-STIC-457 - Gestión de dispositivos móviles: MDM (Mobile Device Management) [Ref.- 403]

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

3. ALCANCE

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

4. HISTORIA DE ANDROID: VERSIONES Y CARACTERÍSTICAS

18. La historia detallada de la plataforma para dispositivos móviles Android, de Google, así como su evolución a través de múltiples versiones durante los últimos años está disponible, con un enfoque específico desde el punto de vista de seguridad, en la guía de "Seguridad de dispositivos móviles: Android 7.x" [Ref.- 407].

5. ENTORNO DE APLICACIÓN DE ESTA GUÍA

19. Los contenidos de esta guía aplican a dispositivos móviles basados en Android en castellano: "Español (España)". El idioma puede ser seleccionado desde el menú "Ajustes [Personal] - Idioma e introducción de texto - [Preferencias de idioma]" y pulsando sobre el idioma de preferencia a la vez que se desplaza el dedo hacia la parte superior.

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

20. La guía ha sido probada y verificada con la versión 7.1.2 del sistema operativo Android, empleando las versiones de las apps y servicios de Google disponibles en el momento de su elaboración, potencialmente comunes a todos los dispositivos móviles y tradicionales independientemente de su versión.

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

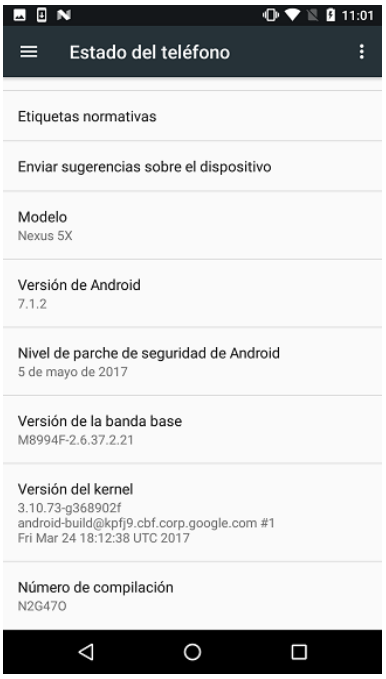
21. Las operaciones que requieren del uso de un ordenador han sido llevadas a cabo mediante Windows 10 Home Premium 64-bits en castellano.

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

22. El hardware sobre el que se ha verificado la presente guía tiene las siguientes características: [Ref.- 3]

    - Dispositivo móvil Google Nexus 5X (fabricado por LG, modelo LG-H791):
        - Versión de Android: 7.1.2.
        - Versión de banda base: (ver imagen inferior): M8994F-2.6.37.2.21.
        - Versión de kernel: (ver imagen inferior): 3.10.73-g368902f... 2017.
        - Número de compilación: N2G470.

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



Nota: La guía ha sido diseñada (y aplicada) para dispositivos móviles estándar basados en Android en los que no se ha llevado a cabo el proceso de *rooting* o root. Este proceso

permite al usuario disponer de control completo del dispositivo móvil y acceder al mismo como root, superusuario, o usuario privilegiado, y en concreto, al subsistema Linux subyacente en Android, eliminando así los controles y/o restricciones establecidos por la plataforma Android estándar, los fabricantes y/o los operadores de telefonía móvil asociados al dispositivo móvil.

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

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

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

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

23. La versión 7.x de Android ("Nougat", N) fue liberada por Google a finales de agosto de 2016[1], con soporte para los dispositivos móviles Nexus 6, 9, 5X y 6P, y significativos cambios ofrecidos a través de su API, de nivel 24 [Ref.- 703].
24. Se recomienda siempre recabar e inventariar la información de versiones, tanto hardware como software, de los dispositivos móviles a proteger, con el objetivo de disponer de toda la información necesaria a la hora de tomar decisiones relativas a la aplicación de nuevas actualizaciones y medidas de seguridad.
25. Dado que el interfaz web de administración de la cuenta de usuario de Google, "https://myaccount.google.com", es accesible desde cualquier plataforma (móvil o

[1] https://android-developers.blogspot.com.es/2016/08/taking-final-wrapper-off-of-nougat.html

tradicional), las opciones asociadas al mismo son válidas independientemente de la versión de Android que ejecute el dispositivo móvil. Para facilitar la lectura de los diferentes apartados, algunas capturas de pantalla se realizarán accediendo al interfaz web de los servicios de Google desde un ordenador.

26. Antes de aplicar esta guía en un entorno de producción debe confirmarse su adecuación a la organización objetivo, siendo probada previamente en un entorno aislado y controlado donde se puedan realizar las pruebas necesarias y aplicar cambios en la configuración para que los mismos se ajusten a los criterios y requisitos específicos de cada organización.

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

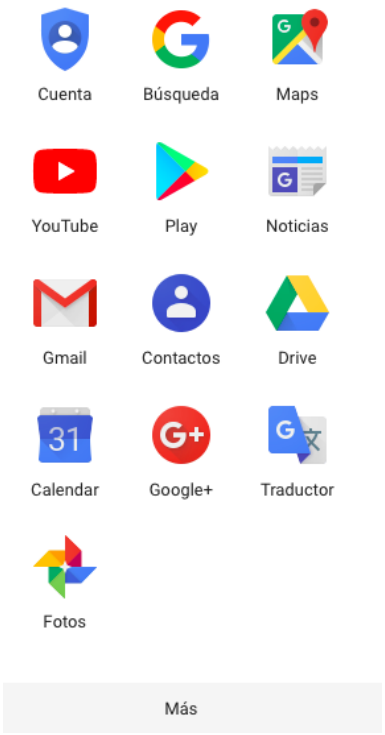
6. CUENTA DE USUARIO DE GOOGLE

27. Aunque de cara a la utilización de las capacidades de telefonía y conexiones de datos de un dispositivo móvil basado en Android se puede prescindir de la configuración de una cuenta de usuario de Google, si se pretende hacer uso de las apps de Google en Android, y de otros servicios adicionales de Google, es preciso dar de alta dicha cuenta en el dispositivo móvil.

28. La cuenta de usuario de Google permite acceder a todos los servicios de Google.

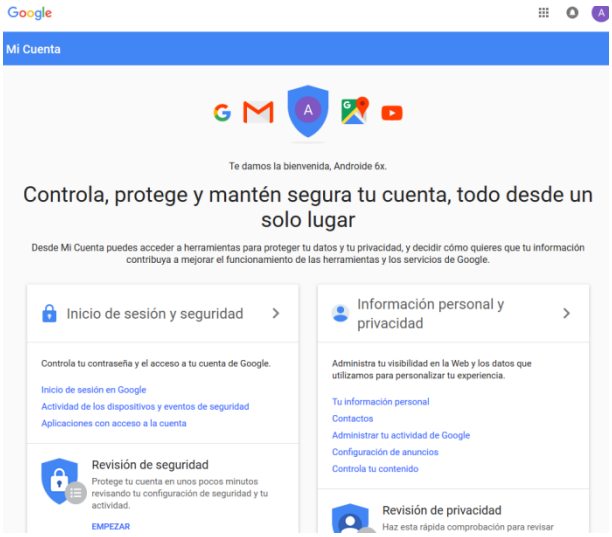
29. Por ejemplo, para descargar aplicaciones de Google Play [Ref.- 4] (ver apartado "10. Servicios de Google Play"), hacer copias de seguridad de los datos y la configuración en los servidores de Google (ver apartado "13.1. Copia de seguridad en los servidores de Google") y otros servicios de Google como Gmail, Maps, Contactos, Calendario, Drive, etc., desde el dispositivo móvil es necesario iniciar sesión en la cuenta de usuario de Google.

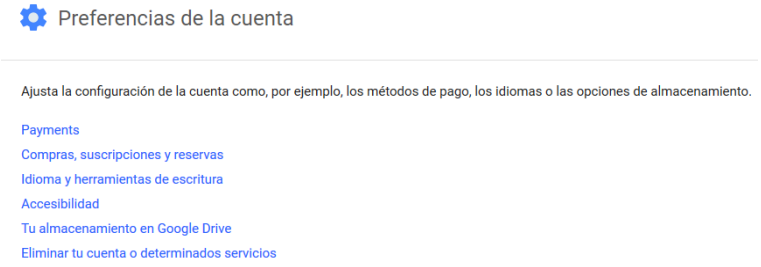
30. Los dispositivos Nexus 5X que vienen de fábrica con Android 7.x traerán integrados, entre otros, los siguientes servicios de Google: Gmail, Google+, Fotos, Maps, Contactos, Calendario, Keep, Drive, YouTube, Hangouts, etc.



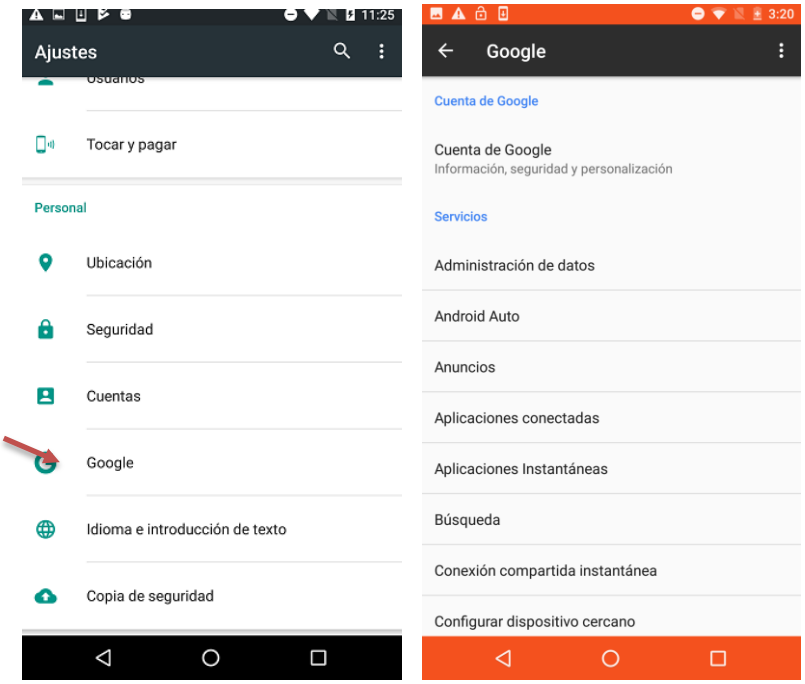
31. La configuración de las opciones de la cuenta de usuario de Google puede realizarse a través de dos mecanismos:

    - A través del portal web de Google "Mi cuenta" (https://myaccount.google.com), que presenta esta apariencia a fecha de elaboración de la presente guía:





- A través de los ajustes del propio dispositivo móvil: en versiones anteriores de Android (hasta la 5.x), la gestión de la cuenta de usuario de Google se llevaba a cabo a través de una app denominada "Ajustes de Google"; a partir de Android 6.x, los ajustes de Google dejaron de existir como una app independiente y se integraron en los ajustes generales del sistema, bajo el apartado "[Personal] - Google", a los que también se accede desde la app "Google" (descrita en el apartado "7. App "Google""). No obstante, algunos de estos ajustes finalmente acceden al interfaz web "Mi cuenta", requiriendo para su modificación acceso a Internet:

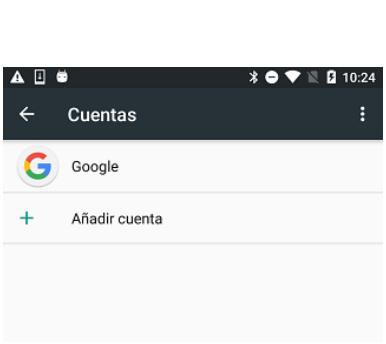


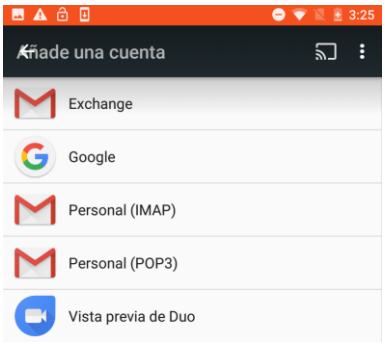
6.1. ASIGNACIÓN DE UNA CUENTA DE USUARIO DE GOOGLE AL DISPOSITIVO

32. La configuración de una cuenta de usuario de Google ya existente y su vinculación al dispositivo móvil Android, o la creación de una nueva cuenta, puede llevarse a cabo mediante el proceso de instalación y configuración inicial de Android 7.x (ver apartado "16. Proceso de instalación y configuración inicial").

33. Asimismo, una vez el dispositivo móvil ha sido configurado, puede vincularse a una o varias cuentas de usuario de Google desde el menú "Ajustes - [Personal] Cuentas".

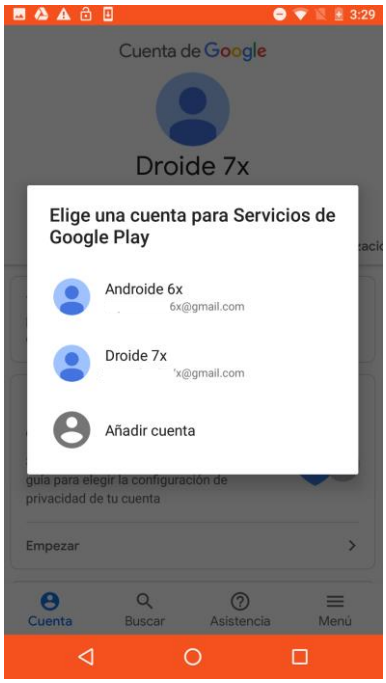
34. El botón "+ Añadir cuenta" permite por defecto añadir tanto una cuenta de usuario de Google como cuentas de usuario de distintos tipos, por ejemplo, de Microsoft Exchange, y cuentas de correo electrónico IMAP y POP3, siendo necesario proporcionar las credenciales de la cuenta existente, es decir, la dirección de correo electrónico del usuario y la contraseña (ver apartado "14.2. Correo electrónico (e-mail) y Gmail"):





35. La sincronización de las cuentas de Google es bidireccional, es decir, los cambios del dispositivo móvil se reflejarán en los servicios web de Google, y viceversa.

36. Adicionalmente, una vez vinculada una cuenta de usuario de Google aparecerá en el menú "Ajustes - [Cuentas]" una nueva entrada denominada "Google", que permite el acceso a los detalles de las cuentas de usuario de Google vinculadas al dispositivo:



37. En el caso de las cuentas de usuario de Google, es posible seleccionar si se añadirá una cuenta ya existente (para lo que se solicitarán las credenciales de acceso) o se creará una nueva cuenta.

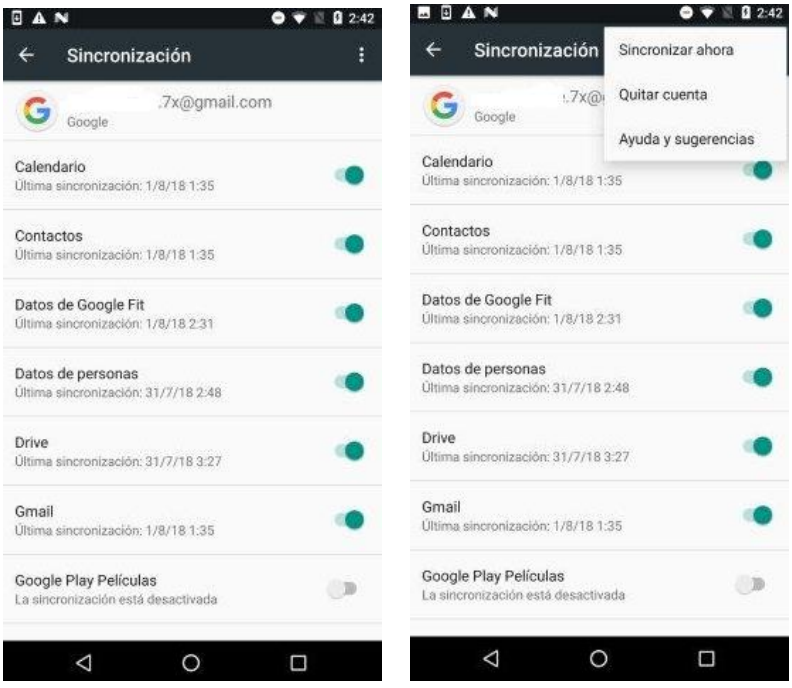
38. En versiones anteriores a Android 5.x, tanto el botón "Google", como el botón "Añadir cuenta", redirigían al usuario a la configuración del interfaz Wi-Fi y lo activaban (incluso aunque estuviera apagado previamente), con el objetivo de disponer de conexión a Internet y poder hacer uso de la cuenta de usuario de Google ya existente, o permitir la creación de una cuenta nueva. A partir de Android 5.x, si no hay conexión a Internet (independientemente del motivo), se mostrará un mensaje informativo, pero no se activará ninguna conexión de datos de forma automática.

39. Adicionalmente, para configurar y poder hacer uso de otros servicios críticos y relevantes en Android, como por ejemplo el acceso a Google Play y la instalación de apps de terceros (ver apartado "10. Servicios de Google Play"), es también necesario disponer de una cuenta de usuario de Google.

40. El proceso de vinculación de una cuenta de usuario de Google existente se lleva a cabo mediante una conexión HTTPS inicial con el servidor "www.googleapis.com" (entre otros). Durante el mismo se solicita confirmación por parte del usuario de los términos de uso y de configuración de datos de pago (paso que se puede omitir y que queda fuera del alcance de la presente guía).

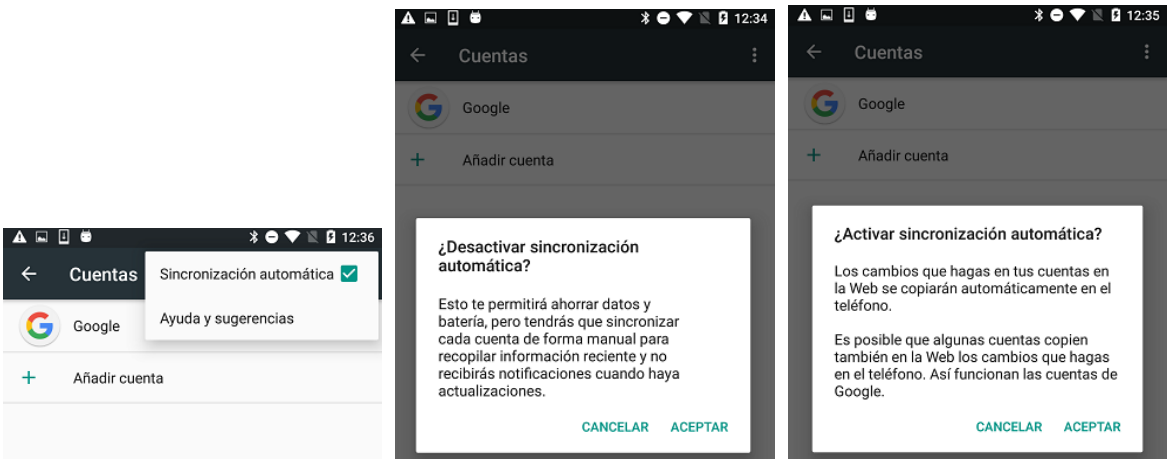
41. Desde el menú "Ajustes - [Personal] Cuentas - [Entrada asociada a la cuenta]" se puede definir qué servicios se sincronizarán con los servicios disponibles en la nube de Google y, por tanto, qué información y datos se enviarán a los servidores de Google. Desde el menú "[…]" de esa ventana, se puede asimismo lanzar una sincronización de datos o eliminar la cuenta del dispositivo móvil.

42. El resto de opciones de configuración de cada servicio se definen dentro de los ajustes de las apps que los proporcionan:



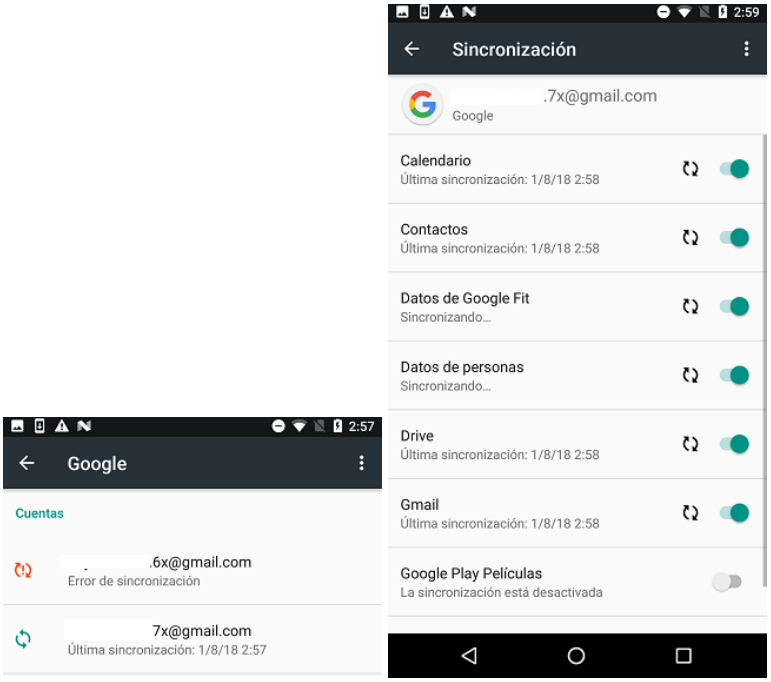
43. Una vez se ha vinculado una cuenta de usuario de Google con el dispositivo móvil, se realizará la sincronización de los servicios seleccionados de manera automática.

44. Para desactivar completamente la sincronización automática, se debe marcar la opción "Ajustes - [Personal] Cuentas […] Sincronización automática". Si se desea volver a activar la sincronización, bastará con volver a marcar la opción correspondiente:



45. También es posible desactivar la sincronización automática servicio a servicio, desmarcando uno a uno todos los interruptores de aquellos servicios que no se desee sincronizar.

46. El icono compuesto por dos flechas circulares junto al nombre de la cuenta en la pantalla de cuentas de usuario informa sobre el estado de la sincronización automática. Si la sincronización está completamente desactivada, se mostrará en gris y tachado, y bajo el nombre de cuenta de usuario de Google aparecerá el mensaje "La sincronización está desactivada". Si algún servicio tiene habilitada la sincronización, el icono asociado a la cuenta se mostrará con las flechas circulares en verde (indicando que tiene lugar algún tipo de sincronización de datos):



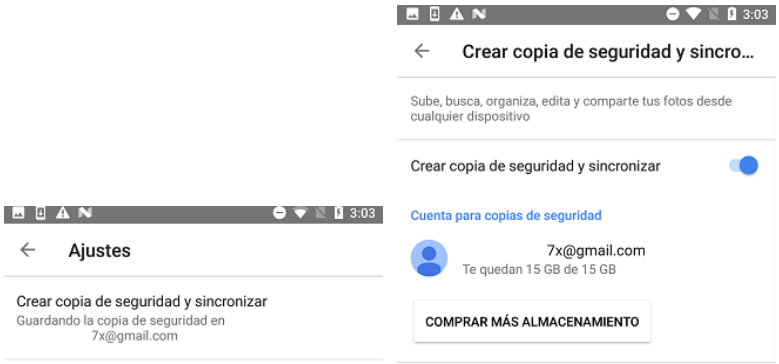
47. A través del botón de menú […] es posible forzar la sincronización de todos los servicios, o elementos marcados para sincronizar en la cuenta, mediante la opción "Sincronizar ahora". Se mostrará una pareja de flechas en los elementos cuya sincronización se esté produciendo en ese momento (ver imagen superior derecha).

48. A través del botón de menú superior es posible eliminar la cuenta de usuario del dispositivo móvil, mediante la opción "Quitar cuenta".

49. La sincronización de la información de los diferentes servicios de Google en Android 7.x se realiza mediante conexiones HTTPS cifradas[2] [Ref.- 112].

50. Los servicios incluidos para su sincronización en Android 7.x incluyen el calendario, el navegador web Chrome, los contactos, los datos de las apps, datos de Google Fit, Drive, Gmail, Google Play (incluyendo los libros, el kiosco, la música, y las películas) e información sobre las personas (entre otros).

51. Adicionalmente, otros servicios de Google (como "Fotos") ofrecen sus propias opciones de sincronización dentro de sus respectivos menús de "Ajustes". Por ejemplo, para la app Fotos, se dispone de la siguiente opción de sincronización y copia de seguridad:



52. Desde el punto de vista de seguridad se recomienda deshabilitar todos y cada uno de los servicios de los que el usuario no esté haciendo uso y/o para los que no se desea hacer un uso explícito de la sincronización, situando a "off" el interruptor correspondiente.

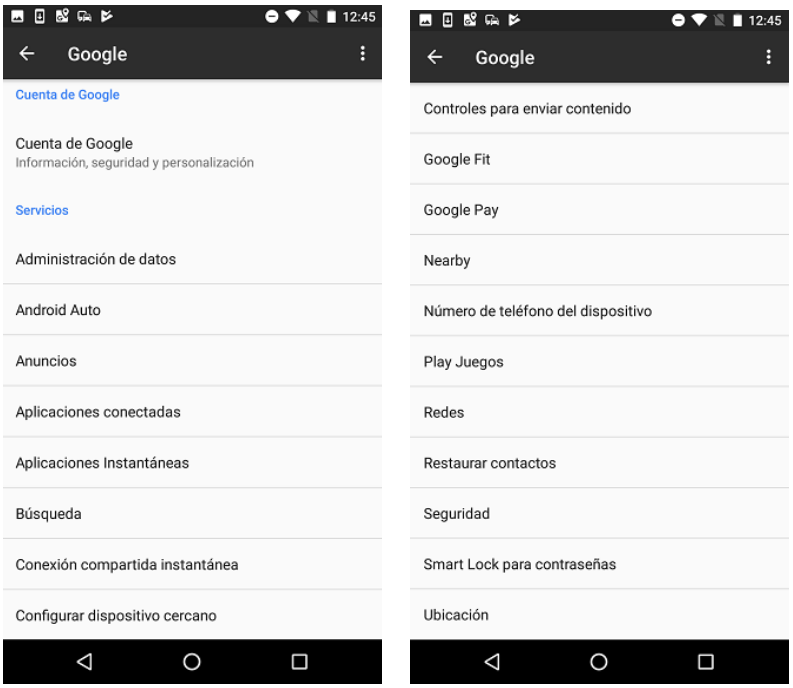
53. Al deshabilitar la sincronización de cada opción o servicio, los datos asociados no serán eliminados del dispositivo móvil. Los datos sólo pueden borrarse eliminando la cuenta.

6.2. AJUSTES "GOOGLE"

54. Los denominados "Ajustes "Google"" permiten definir desde el dispositivo móvil multitud de parámetros asociados a la cuenta del usuario y a los diferentes servicios de Google.

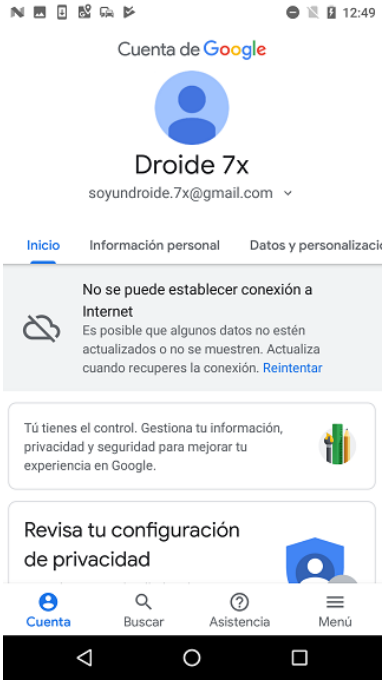
55. Se acceden a través del menú "Ajustes - [Personal] Google", en el que se presentan dos secciones principales: [Cuenta de Google] y [Servicios]".

[2] En versiones previas de Android, 2.x, algunos servicios de Google empleaban tráfico HTTP sin cifrar.



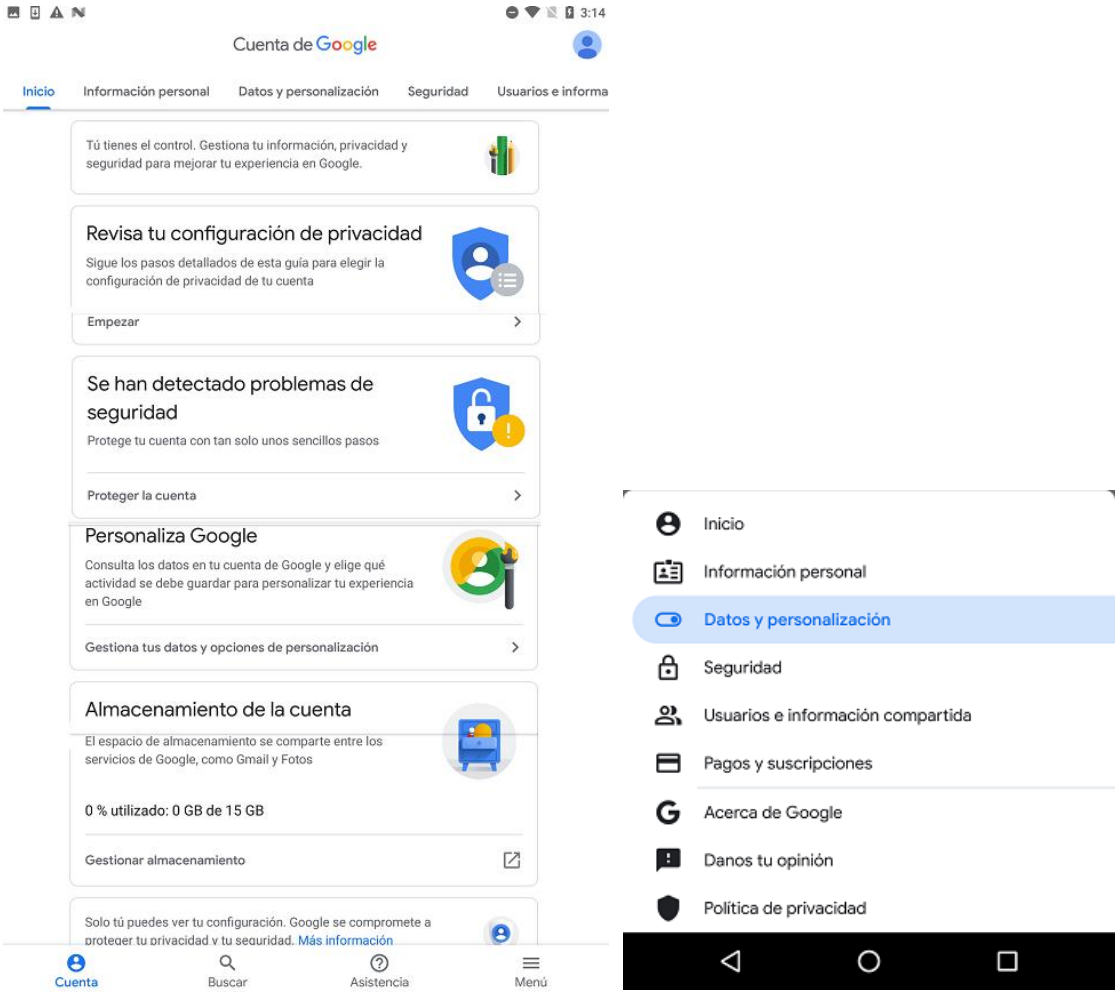
6.2.1. SECCIÓN "CUENTA DE GOOGLE"

56. La sección "Cuenta de Google" (o cuenta de usuario de Google) proporciona un interfaz de administración desde el dispositivo móvil para consultar y modificar los parámetros asociados a la cuenta de usuario de Google; en caso de que no se disponga de conexión a Internet cuando se trate de acceder a este apartado, se presentará un mensaje en el que se indica que los datos mostrados pueden no estar actualizados:



57. Este interfaz de administración dispone de varias pantallas, organizadas por secciones en la parte superior (Inicio, Información personal, Seguridad, etc.), y de accesos a ajustes particulares (que se presentan en pantalla y se recorren deslizando el dedo de abajo hacia arriba de la pantalla del terminal). Adicionalmente, a través

del botón situado en la parte inferior derecha de la pantalla (representado por tres líneas horizontales paralelas), se presenta un menú con las mismas secciones que las mostradas en la parte superior.

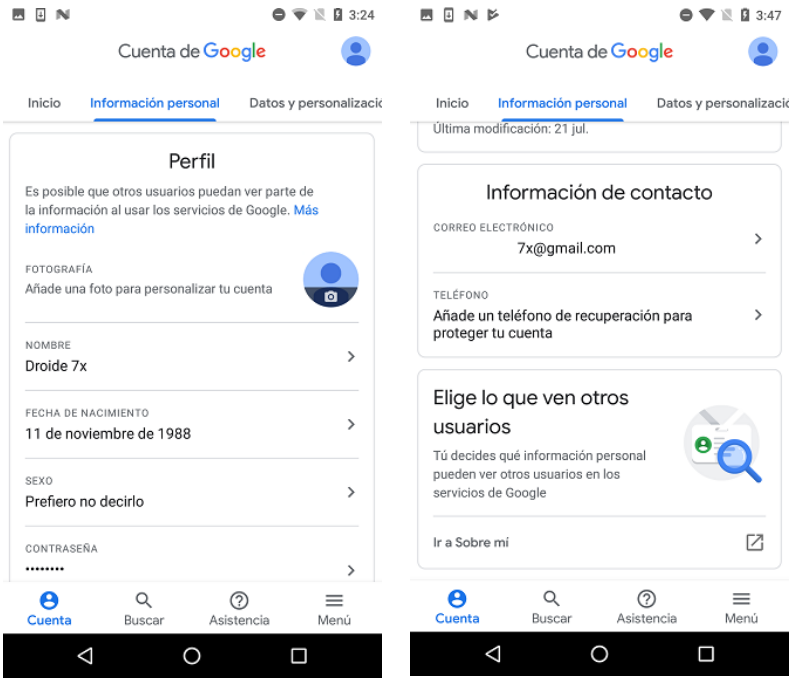


58. A continuación se describen las opciones presentes dentro de cada categoría.

6.2.1.1. INFORMACIÓN PERSONAL

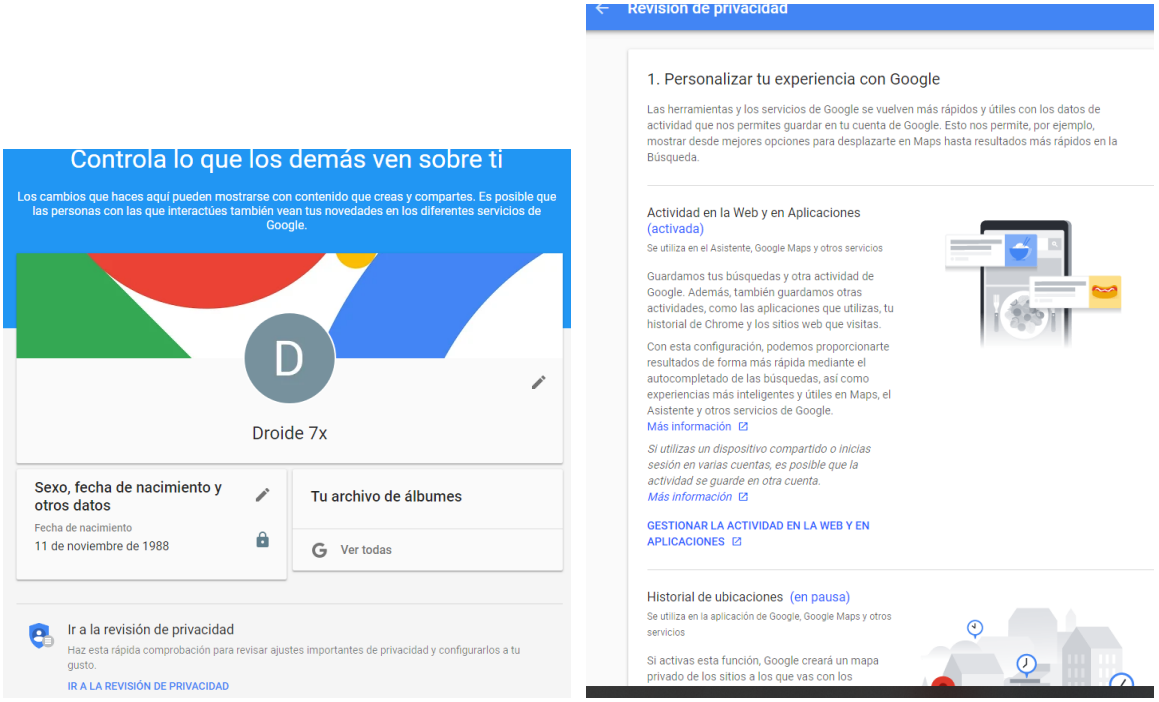
59. Bajo esta sección de configuración se pueden consultar y modificar elementos como los datos personales (el nombre, correo electrónico y número de teléfono) que se utilizan por los productos y servicios de Google, como Hangouts, Gmail y Maps para que otros usuarios puedan consultarlos, así como administrar la actividad de la cuenta de usuario de Google y controlar su contenido.

60. Desde el dispositivo móvil, el acceso a esta configuración está en "Ajustes - [Personal] Google - [Cuenta de Google] Cuenta de Google - Información personal", que lanza el correspondiente menú del interfaz "Cuenta de Google".

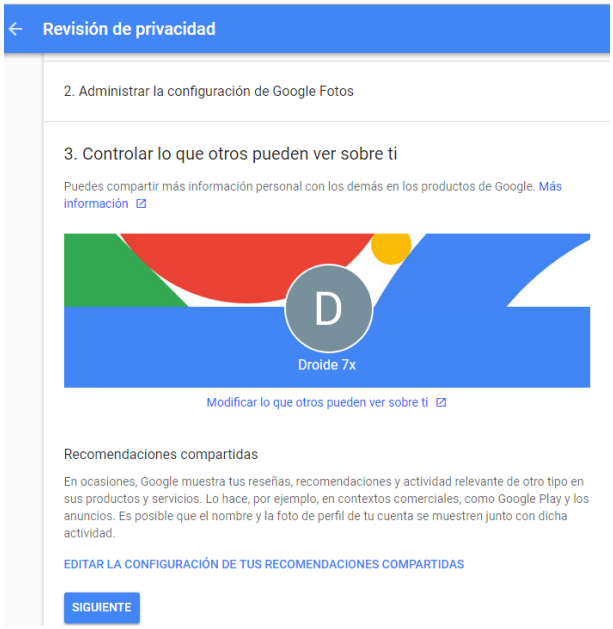


61. Para modificar algunos de estos valores, como el nombre o la contraseña, se solicitará la contraseña actual de la cuenta de usuario de Google.

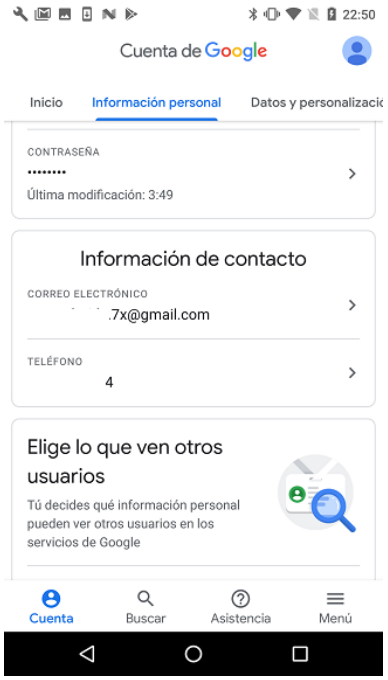
62. La opción "Ir a Sobre mí" proporciona acceso al portal "https://aboutme.google.com", desde el que se gestiona la información propia visible para otros usuarios de productos de Google. Concretamente, la opción "Ir a la revisión de privacidad" despliega un menú con múltiples detalles personales, todos ellos editables:



63. Dentro de la "Revisión de privacidad", se pueden modificar los datos personales que se comparten con otros usuarios de servicios de Google. Debido a la extrema sensibilidad de estos datos, se recomienda no proporcionarlos (en caso de ser posible) o elegir valores que no necesariamente se correspondan con la realidad.



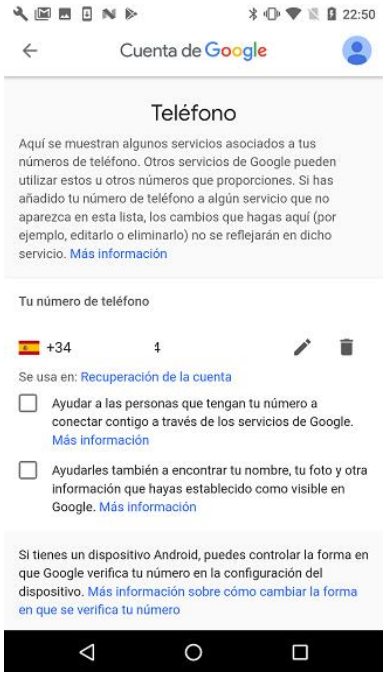
64. En la sección "Información personal" se dispone de la dirección de correo asociada a la cuenta de usuario de Google y el número de teléfono configurado para ella:



65. Desde la versión Android 4.4 (KitKat), Google ha implementado la identificación de llamadas inteligente, también denominada identificación de llamada de Google [Ref.- 148]. Cuando se recibe (o se realiza) una llamada de alguien que no está en la agenda o lista de contactos, el teléfono buscará coincidencias para las personas en base a la información disponible en su cuenta de usuario de Google (desde el año 2014) y para las empresas que tengan una ficha local en Google My Business.

66. En el caso de compañías y organizaciones que hagan uso de cuentas de trabajo, o de centros educativos, el servicio tratará de buscar coincidencias en los directorios propios para ver si contienen información sobre dichos contactos.

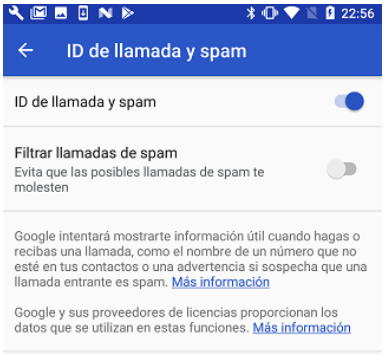
67. La visibilidad del número de teléfono propio para otras personas puede ser modificada a través de los ajustes de la cuenta de usuario de Google (sección "Información personal - Información de contacto"):



68. La modificación del número de teléfono asociado a la cuenta de usuario de Google afecta a los servicios de Google listados en la página web anterior. Debe tenerse en cuenta que existen numerosos servicios que pueden hacer uso del número de teléfono del usuario.

69. Se recomienda deshabilitar la visibilidad del número de teléfono en la cuenta de usuario de Google (a menos que existan razones para compartir el número de teléfono propio con otros usuarios). Si se habilita su visibilidad, otros usuarios podrán enviar un mensaje (no sólo a través de aplicaciones como Hangouts que usan el número de teléfono, sino también mensajes de correo electrónico), o consultar el nombre o la foto del perfil del usuario al establecer una llamada.

70. Adicionalmente, existe una opción que permite que, al recibir o cursar una llamada asociada a un número que no forma parte de la lista de contactos, se intente ofrecer información sobre el otro interlocutor. Esta funcionalidad está disponible en Android desde la app del teléfono, mediante el menú de opciones avanzadas disponible en la parte superior derecha, a través del menú "… - Ajustes - ID de llamada y spam" (opción que por defecto está habilitada) [Ref.- 148]:

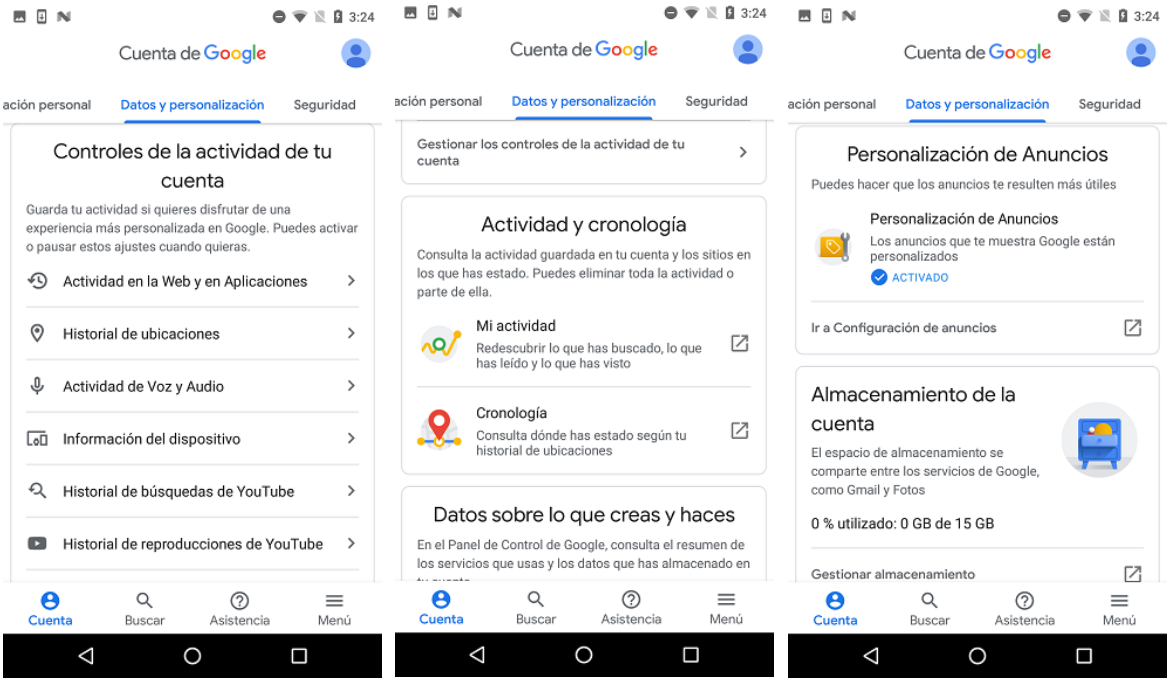


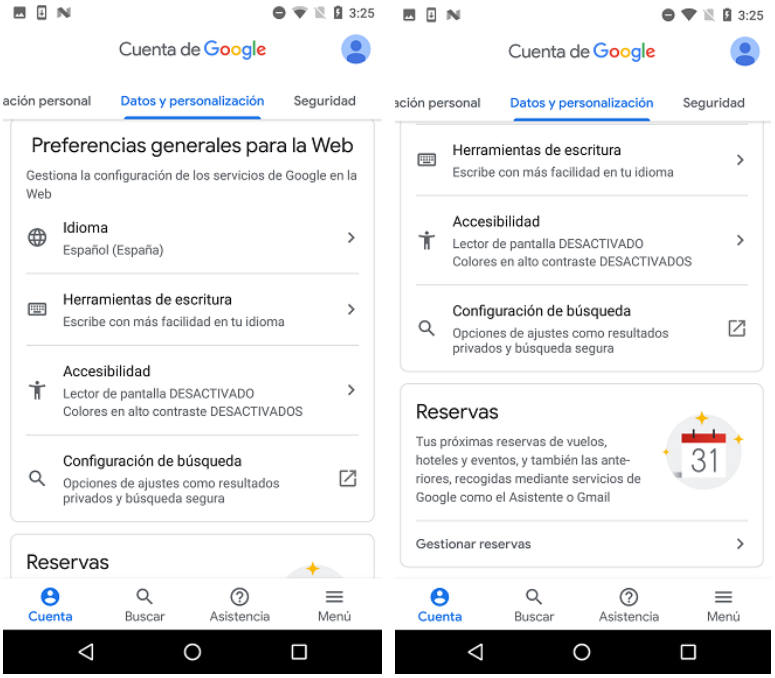
71. Los identificadores de llamada de Google no se añaden automáticamente a la lista de contactos. Desde el punto de vista de seguridad, si no se desea hacer uso de esta funcionalidad, se recomienda deshabilitarla.

72. En resumen: por un lado, desde la configuración del número de teléfono de la cuenta de usuario de Google, el propietario del dispositivo móvil puede definir si desea que otros usuarios tengan capacidad para localizarle en base al número de teléfono propio; por otro lado, desde los ajustes de la app "Teléfono" en Android es posible configurar si se desea localizar a otros usuarios (que lo permitan) a través de la funcionalidad del identificador de llamada de Google.

6.2.1.2. DATOS Y PERSONALIZACIÓN

73. Bajo este apartado se encuentran la mayor parte de las opciones estrechamente relacionadas con la privacidad del usuario. Si bien los mensajes ofrecidos en los diferentes menús invitan al usuario a activarlas para mejorar su experiencia y que ésta sea más personalizada, se recomienda valorar cuidadosamente cuáles se desea utilizar, ya que, algunas, de ser accedidas por un tercero que tome control (aunque sea temporalmente) de la cuenta del usuario, pueden revelar información sensible:

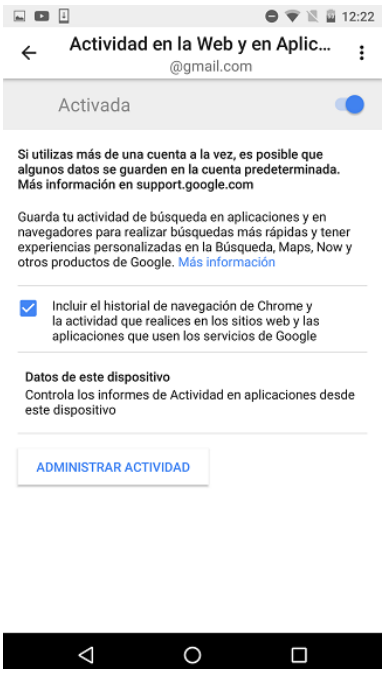




74. Las opciones que se presentan en esta sección tienen su equivalente en el interfaz web bajo "Información personal y privacidad".

75. **Controles de la actividad de tu cuenta**: incluye diversas opciones que controlan lo que se envía o no a Google. Todas permiten administrar la actividad del usuario (mediante el botón "Administrar actividad"), que establece una conexión HTTPS con el servidor "myaccount.google.com" usando las credenciales de la cuenta de Google del usuario y da opción a consultar, eliminar y modificar la actividad de las aplicaciones que han enviado datos, e incluso cambiar los ajustes actuales de envío de datos de la cuenta de usuario en el servidor. En versiones más antiguas de la app de Google, se denominaba "Historial de cuenta de Google". Desde el punto de vista de seguridad y privacidad, se recomienda valorar cuidadosamente cuáles de estas opciones se desea tener activas:

    - Actividad en la Web y en Aplicaciones [Ref.- 176]: guarda la actividad de búsqueda en aplicaciones móviles y navegadores web. Además de activar y desactivar esta funcionalidad, dispone de una opción para incluir el historial de navegación de Chrome y de aplicaciones que usen servicios de Google, un apartado "Datos de este dispositivo" que, si se selecciona, almacenará en la cuenta de Google del usuario la actividad de aplicaciones que parten del propio dispositivo móvil, y la opción "Administrar historial", que inicia sesión en los servidores de Google y permite ver en detalle qué aplicaciones se han utilizado, pudiendo filtrar incluso por fecha y producto de Google.

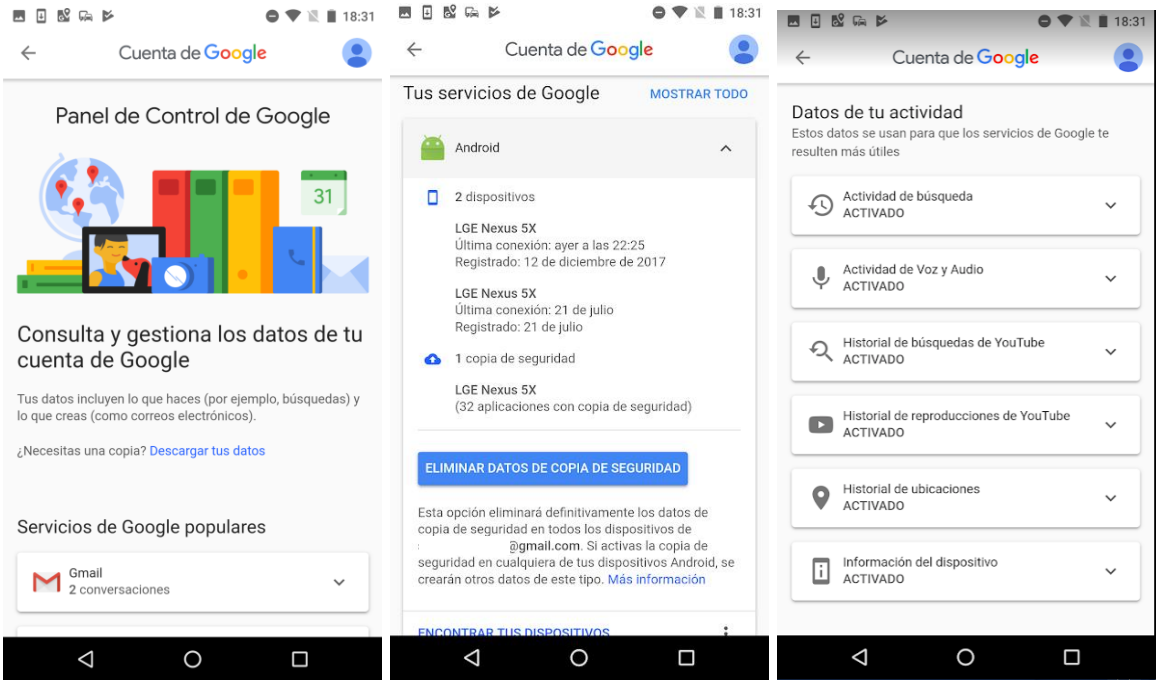


- Historial de ubicaciones (de Google): si está activa, Google obtendrá datos de la ubicación del dispositivo móvil. En versiones anteriores de Android, además de poderse desactivar esta opción, se ofrecía un botón de "Eliminar historial de ubicaciones", que permitía eliminar de forma sencilla todo el historial. A fecha de elaboración de la presente guía, solo se dispone de la opción "Eliminar día". Para eliminar por completo el historial de ubicaciones, es preciso acceder al menú de ajustes de la app "Maps" y acceder a "Contenido personal - Ajustes de ubicación - Eliminar todo el historial de ubicaciones" (ver apartado "11.5. Historial de ubicaciones" para más información).
- Actividad de Voz y Audio: almacena las búsquedas de voz (por ejemplo, a través de "Ok Google"), supuestamente para mejorar el reconocimiento de voz de dicho servicio [Ref.- 753].
- Información del dispositivo: envía a Google (para que sean almacenados) información sobre los contactos, datos del dispositivo móvil, calendarios, aplicaciones y música, con objeto (según indica la ayuda) de obtener sugerencias y resultados más precisos en las búsquedas. Para consultar el detalle de los datos guardados, se puede pulsar en "Administrar actividad". Ello abre el menú "Información del dispositivo", con tres puntos a la derecha que dan opción para "Eliminar todo", ver la actividad registrada ("Mi actividad"), y acceder a los "Controles de actividad de la cuenta", que se conecta de nuevo a "myaccount.google.com" con la cuenta del usuario de Google y da opción de modificar los ajustes de envío de datos de la cuenta en el servidor.
- Historial de búsquedas de YouTube.
- Historial de reproducciones de YouTube.

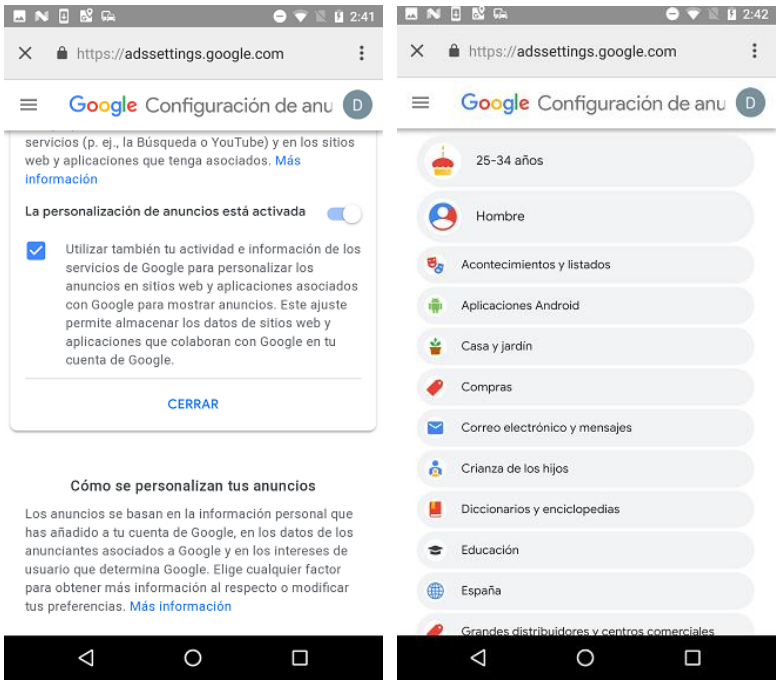
76. **Actividad y cronología**: en este apartado se puede consultar toda la actividad del usuario en relación con la cuenta de usuario de Google, no solo desde el propio dispositivo móvil, sino desde cualquier otro dispositivo en el que se haya accedido con dicha cuenta de usuario.

- Mi actividad: redirige al portal "https://myactivity.google.com/myactivity" iniciando sesión con la cuenta del usuario activa en el dispositivo móvil, sin solicitar de nuevo las credenciales. Desde dicho portal es posible consultar y gestionar tanto los controles de la cuenta (historial de actividad en la web y en aplicaciones, historial de ubicaciones, información de los dispositivos vinculados a la cuenta de Google del usuario, historial de reproducciones de YouTube, etc.).
- (Mi) Cronología: ofrece un historial de ubicaciones clasificadas por fecha, integrándose con Google Maps.

77. **Datos sobre lo que creas o haces**: al seleccionar esta opción, se abre el denominado "Panel de Control de Google", en el que se indexa diversa información sobre el uso que se hace de la cuenta de Google del usuario, desde las aplicaciones utilizadas (incluyendo qué funcionalidad concreta ha sido empleada), los dispositivos asociados a la cuenta, los historiales de actividad, etc.



78. **Personalización de Anuncios**: establece una conexión con "accounts.google.com" cifrada mediante HTTPS que redirige a "adssettings.google.com", en el que se puede acceder a la configuración de los anuncios que se presentarán al usuario durante la navegación web, en base a la información que ha rellenado en su perfil y a datos que Google extrae de la actividad de la cuenta.



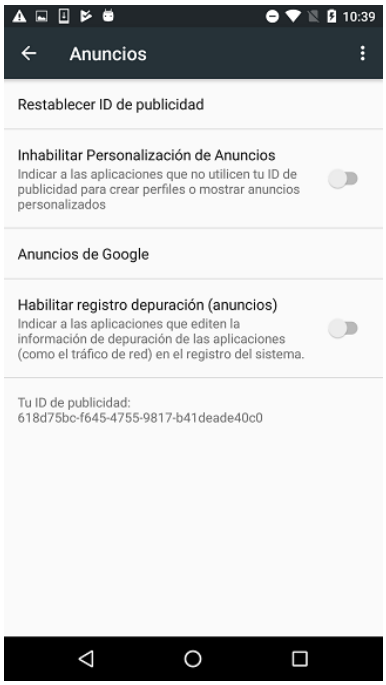
79. Hay que recalcar que no es posible inhabilitar la presentación de anuncios, tal y como refleja la política de Google[3], y que todos los parámetros que se definan afectarán únicamente al tipo de anuncio que se mostrará.

80. En el caso de la configuración de anuncios, el usuario puede filtrar por temas, utilizar la actividad y la información de la cuenta de usuario de Google para personalizar los anuncios que se muestran en diversos sitios web y aplicaciones, y guardar estos datos en la cuenta de Google del usuario. Esta opción (habilitada por defecto) no está recomendada desde el punto de vista de la privacidad, pues, aunque deshabilitarla hará que los anuncios mostrados sean más genéricos, y muy probablemente de menor interés para el usuario, evita que se haga un seguimiento del usuario en este tipo de servicios.

81. La versión 4.x de los servicios de Google Play introdujo lo que se denomina "ID de publicidad", un número aleatorio y único (supuestamente anónimo) que se generaba en el momento de la instalación inicial del dispositivo móvil, o cada vez que éste es restaurado a fábrica, y que se emplea por los servicios de anuncios, asociados a Google Play y a las apps de terceros, para hacer un seguimiento "anónimo" del usuario [Ref.- 187].

82. La configuración del identificador (o ID) de publicidad se encuentra disponible en "Ajustes - [Personal] Google - [Servicios] Anuncios":

[3] https://support.google.com/ads/answer/2662922?hl=es



83. Desde agosto de 2014, y con el objetivo de proteger la privacidad del usuario, Google Play Services (y sus servicios de anuncios) obligó a todas las apps de terceros a hacer uso del ID de publicidad (funcionalidad disponible desde octubre de 2013 mediante la versión 4.0 de los servicios y app de Google Play Services, GPS) para llevar a cabo cualquier tarea de seguimiento del usuario con fines publicitarios, en lugar de emplear (tal como hacían numerosas apps en el pasado) otros identificadores persistentes vinculados al usuario o al dispositivo móvil, como por ejemplo el identificador de la cuenta de usuario de Google, el IMEI del terminal, el IMSI de la tarjeta SIM, las direcciones MAC de los interfaces inalámbricos Wi-Fi y/o Bluetooth, etc. [Ref.- 125].

84. Conviene activar la opción "Inhabilitar Personalización de Anuncios" (deshabilitada por defecto), impidiendo así que las apps usen el ID de publicidad del usuario para mostrar anuncios en base a sus intereses, pero salvaguardando su privacidad.

85. La opción "Habilitar registro depuración (anuncios)", si se habilita, hará que las apps registren en el log del sistema de Android (logcat) información relativa a los anuncios. Esta actividad, que no tiene interés desde el punto de vista del usuario final, se puede consultar mediante el comando "adb logcat":

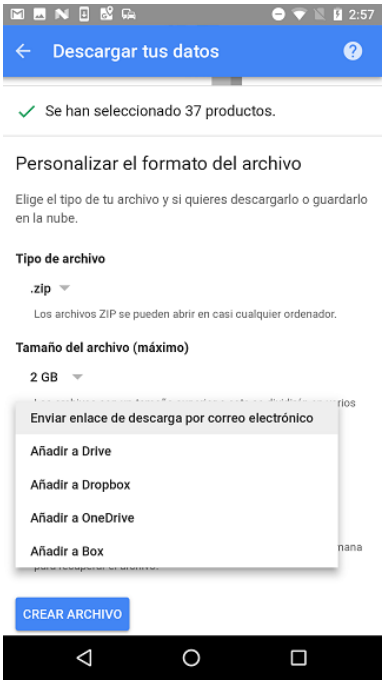
```
03-02 10:53:38.240  4412  4412 D AdvertisingIdNS: Notifying advertising info
update event for package com.google.android.youtube
```

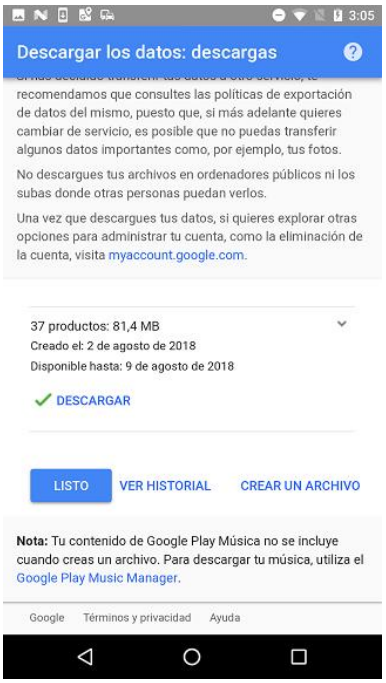
86. Por último, la opción "Anuncios de Google" redirige al usuario a la página web de Google que informa de los servicios de anuncios y publicidad.

87. **Almacenamiento de la cuenta**: redirige mediante una conexión cifrada con HTTPS hacia "drive.google.com", en la que se informa del espacio utilizado en el servicio Google Drive y los distintos paquetes de almacenamiento disponibles para el usuario.

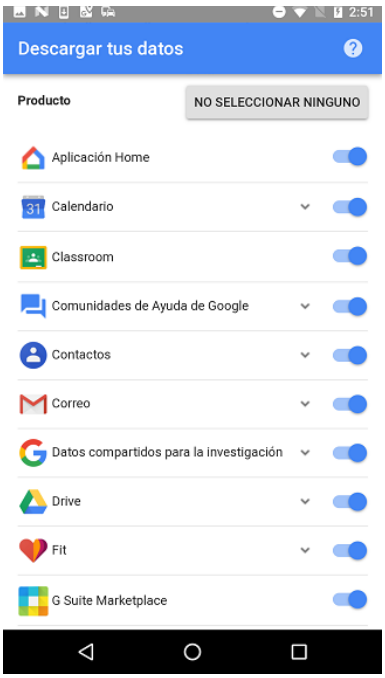
88. **Descargar, eliminar o crear un plan para los datos**: a través de esta sección se ofrece al usuario realizar una copia de los datos generados por las aplicaciones y servicios de Google, establecer un plan de acción si la cuenta permanece inactiva durante cierto tiempo o eliminar un servicio de la cuenta. A continuación se describen las diferentes opciones disponibles en esta sección.

89. *Descargar tus datos*: esta opción permite realizar una copia de la configuración y los datos de las apps y servicios de Google vinculados a la cuenta del usuario, pudiéndose seleccionar cuáles se desean incluir en el archivo generado como resultado.





90. Al seleccionar "Crear archivo", se ofrece un menú que permite elegir qué datos se salvarán y transmitirán al archivo (por defecto en formato ZIP) con la copia de los datos.

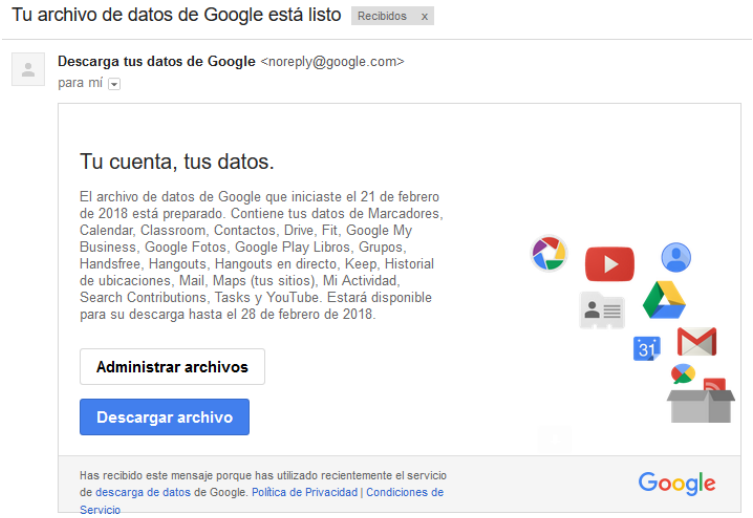


91. El formato del archivo puede ser ".zip" o ".tgz" (en versiones anteriores se ofrecía también el formato ".tbz"), y el tamaño máximo es de 50 GB.

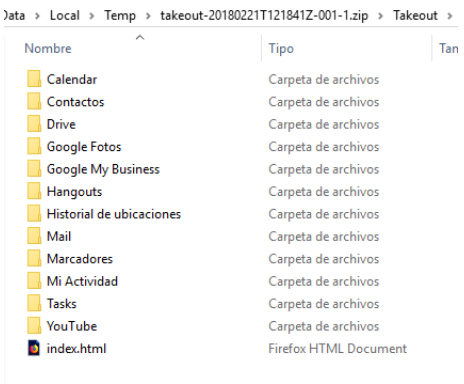
92. Como métodos para obtener el archivo, se puede seleccionar el correo electrónico, Google Drive, Dropbox o Microsoft OneDrive (en cuyo caso el archivo se guardará en el servicio en la nube especificado y el enlace a su ubicación se enviará por correo

electrónico a la cuenta de usuario de Google). El detalle de estos servicios queda fuera del alcance de la presente guía.

93. Cuando el archivo se encuentre disponible, se recibirá un e-mail en la cuenta de usuario y se podrá descargar el mismo:



94. El archivo emplea la nomenclatura "takeout-fecha-ID.extensión_designada". Por ejemplo, "takeout-20180221T115317Z-001.zip. El contenido del archivo sigue una estructura de subdirectorios, uno por cada aplicación seleccionada, y un fichero index que muestra lo que se ha salvado. Al seleccionar el icono de cada aplicación, es posible identificar el formato empleado para cada app (MBOX para el mail, JSON para las búsquedas y Hangouts, ICS para el calendario, HTML para los marcadores, etc.):

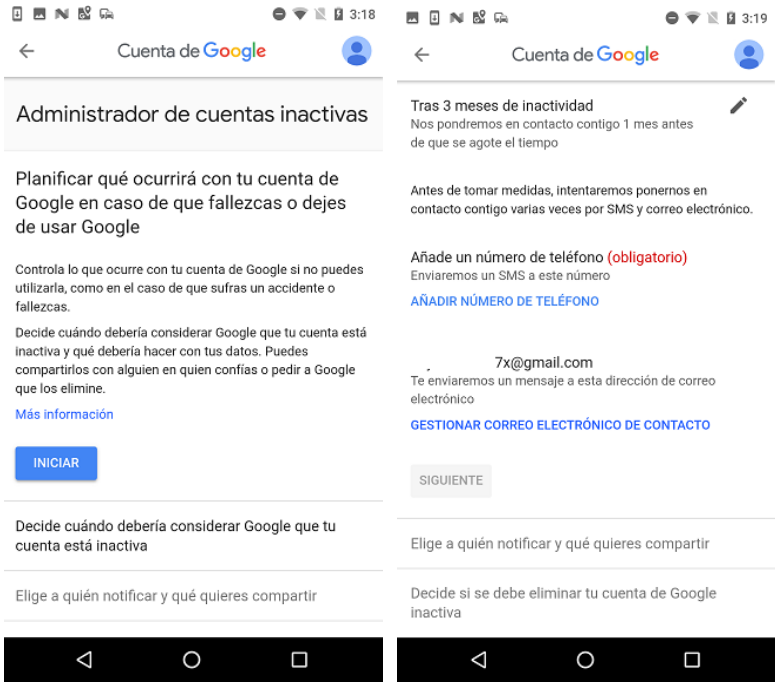


95. La creación de un archivo de descarga no elimina ninguna parte o contenido de la información almacenada en la cuenta de Google del usuario.

96. Una vez creado un archivo, estará disponible durante una semana para su descarga pero, a fecha de elaboración de la presente guía, no se dispone de ninguna opción para eliminar el archivo de los servidores de Google por parte del usuario.

97. Este método se puede utilizar si se desea exportar los datos a otro tipo de servicio, y también como una alternativa para realizar una copia de seguridad de los datos.

98. *Crea un plan para tu cuenta*: redirige a la una sección denominada "Administrador de cuentas inactivas", en el que se pueden configurar diversas opciones de actuación sobre cuentas de usuario que permanecen inactivas durante el periodo definido (mínimo 3 meses), independientemente del motivo.



99. Por defecto, se establece un periodo mínimo de espera de tres meses tras el cual la cuenta se considerará inactiva (el máximo configurable es 18 meses) y a quién se enviarán las alertas antes de que se cumpla el tiempo para que la cuenta se marque como inactiva; además, se puede configurar un máximo de 10 personas a quienes se notificará sobre la designación de la cuenta como inactiva, e incluso darles acceso a los datos que el propietario de la cuenta considere oportunos.

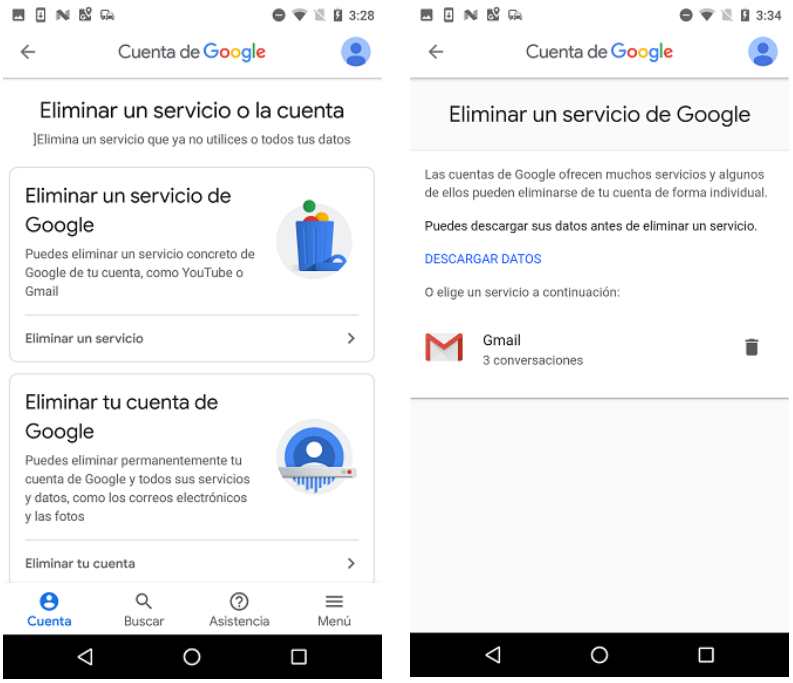
100. Además, se puede configurar la opción de eliminar por completo la cuenta en caso de que se declare inactiva según los parámetros definidos anteriormente.

101. Una vez finalizada la configuración, se ofrece revisar el plan y, en caso de ser el adecuado, confirmar su aplicación.

102. Si se añade un contacto de confianza mediante la opción "Elige a quién notificar y qué quieres compartir", se ofrecerá la posibilidad de seleccionar qué datos pueden ser accedidos por dicho contacto. Además de su dirección de correo electrónico, se puede proporcionar un número de teléfono del contacto para comprobar su identidad e impedir accesos no autorizados a los datos. Los contactos de confianza recibirán dicho código de verificación después de que la cuenta se marque como inactiva.

103. Desde el punto de vista de seguridad y privacidad, se debe sopesar cuidadosamente si se hace uso de la funcionalidad "Administrador de cuentas inactivas", pues pueden ser múltiples las circunstancias que provoquen que una cuenta deje de ser utilizada y no en todas ellas el propietario podrá revocar una autorización de acceso a sus datos por parte de otros usuarios, habilitada previamente.

104. *Eliminar un servicio o la cuenta*: ofrece la posibilidad de eliminar algunos servicios de Google, incluso de eliminar la propia cuenta de usuario. A diferencia de otras secciones descritas anteriormente, en ésta se solicita confirmar la contraseña de la cuenta de usuario de Google.

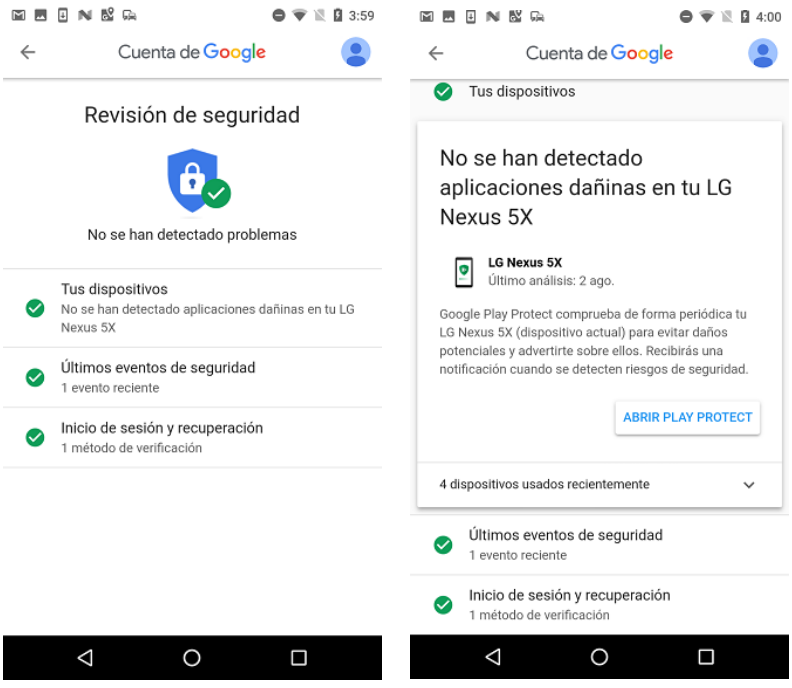


105. Aunque la descripción de la sección parece indicar que se podría eliminar cualquier servicio, solo es posible eliminar los presentados en el menú, que, a fecha de elaboración de la presente guía, se reducen a Gmail, como ilustra la imagen superior derecha.

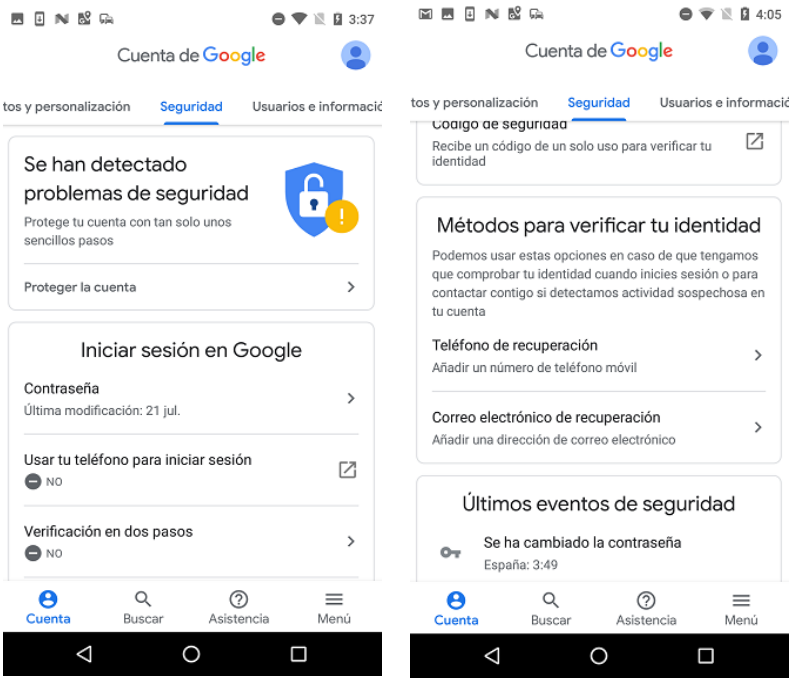
6.2.1.3. SEGURIDAD

106. En esta sección se resumen (y configuran) diversos aspectos relacionados con la seguridad de la cuenta de usuario de Google, que, por su enorme importancia y criticidad, se deben analizar cuidadosamente.

107. En la cabecera de esta sección, se ofrece la revisión de seguridad, que informa de si se han detectado problemas o incidentes de seguridad y permite actuar respecto a los mismos, si el usuario así lo desea.

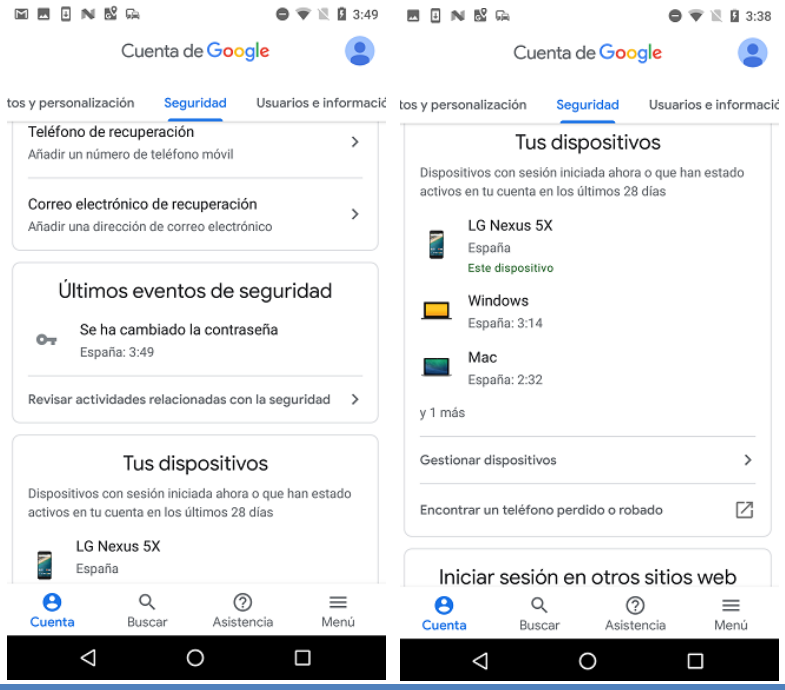


108. **Iniciar sesión en Google**: presenta los mecanismos configurados para el inicio de sesión en la cuenta de usuario de Google (ver apartado "9.4. Inicio de sesión y seguridad"):



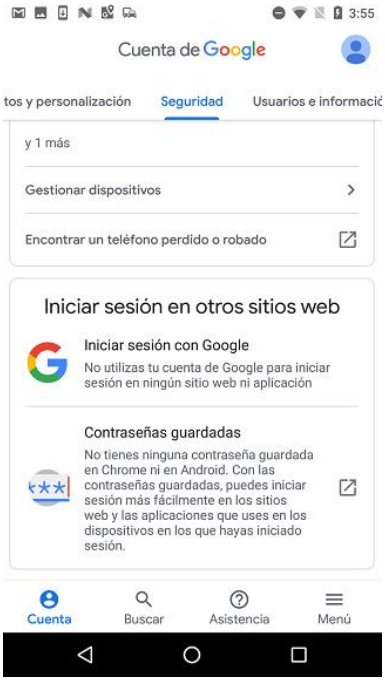
109. **Métodos para verificar tu identidad**: refleja los métodos vigentes para la verificación de identidad (teléfono de recuperación y correo electrónico de recuperación), que se emplearán en caso de que se bloquee el acceso temporalmente a la cuenta por cualquier causa, entre ellas, la detección de actividad inusual o anómala en la cuenta (ver imagen superior derecha).

110. **Últimos eventos de seguridad**: este apartado registra la actividad asociada a la cuenta de Google del usuario que tiene relación directa con la seguridad de la misma, como por ejemplo un cambio de contraseña o un inicio de sesión desde un nuevo dispositivo, o desde una ubicación (por ejemplo, país), desde el que no se había efectuado un inicio de sesión nunca.



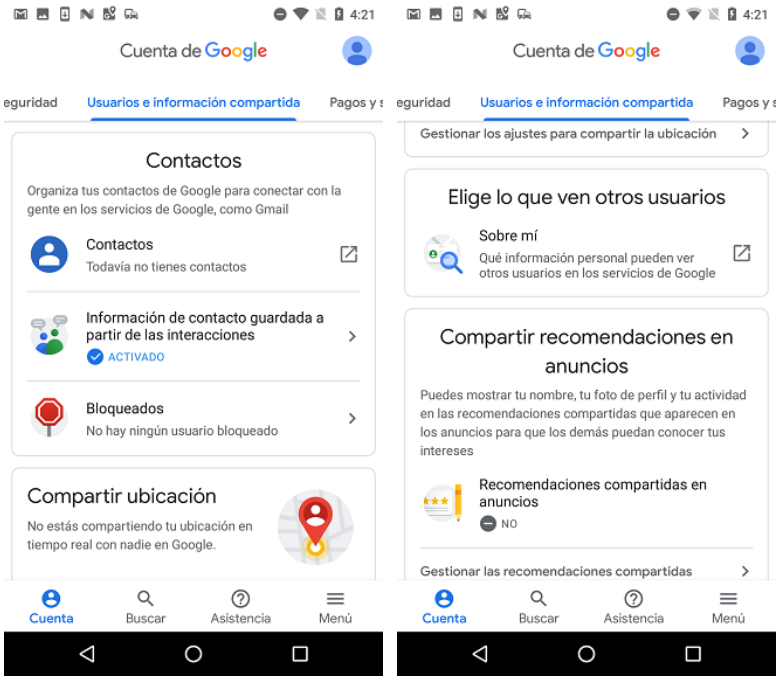
111. **Tus dispositivos**: (ver imagen superior derecha) además de mostrar los dispositivos desde los que se ha iniciado sesión en la cuenta de usuario de Google en los últimos 28 días (incluyendo la fecha concreta y la ubicación de los mismos de estar activa en el momento del acceso), ofrece la opción "Encontrar un teléfono perdido o robado", la cual proporciona acceso a "Encontrar tu móvil", desde donde es posible realizar una serie de acciones encaminadas a localizar y/o proteger un dispositivo móvil extraviado (ver apartado "10.4. Gestión remota de dispositivos Android por parte del usuario").

112. **Iniciar sesión en otros sitios web**: informa de si la cuenta de usuario de Google se ha utilizado para iniciar sesión en otras apps o sitios web (por ejemplo, en redes sociales de terceros), así como si se está haciendo uso del almacenamiento de credenciales de otras apps o sitios web en la cuenta de usuario de Google (ver apartado "12.2. Servicio de contraseñas de Google Smart Lock").



6.2.1.4. USUARIOS E INFORMACIÓN COMPARTIDA

113. Desde esta sección se puede consultar y configurar información relativa a interacción con otros usuarios, por lo que su configuración afecta directamente a la privacidad:



114. **Contactos**: además de visualizar y añadir contactos, se dispone de la opción "Información de contacto guardada a partir de las interacciones" (activa por defecto), que hará que se almacenen en la cuenta de usuario de Google nombres y direcciones de otros usuarios con los que se ha mantenido alguna relación en el contexto de algún servicio de Google (a excepción de Gmail, en el que esta posibilidad se controla de forma independiente). Adicionalmente, se puede consultar la lista de usuarios bloqueados (y añadir elementos a ella).

115. **Compartir ubicación**: permite consultar si se está haciendo uso de la función de compartir la ubicación en tiempo real con otros usuarios de Google. Esta opción se configura a través de la app "Google Maps" (ver apartado "11.2. Google Maps").

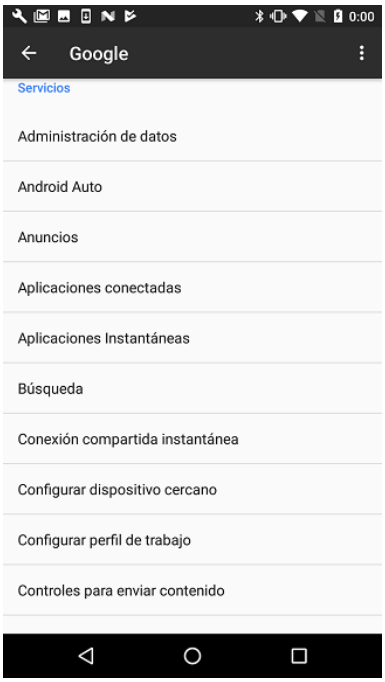
6.2.1.5. PAGOS Y SUSCRIPCIONES

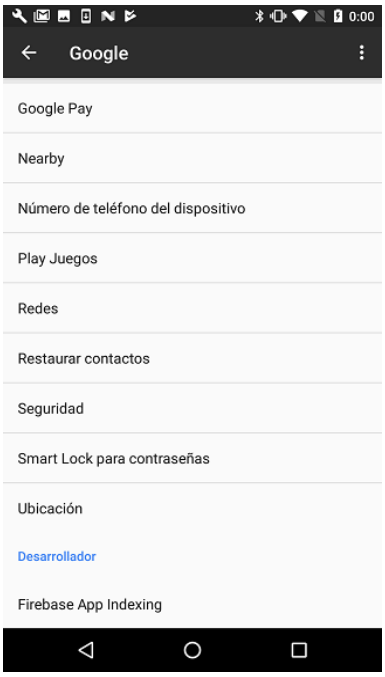
116. Permite consultar y gestionar los métodos de pago configurados en "Google Pay" (GPay), las compras realizadas, las suscripciones y reservas de viajes o eventos realizadas mediante servicios de Google.

117. El análisis detallado de estos elementos queda fuera del alcance de la presente guía.

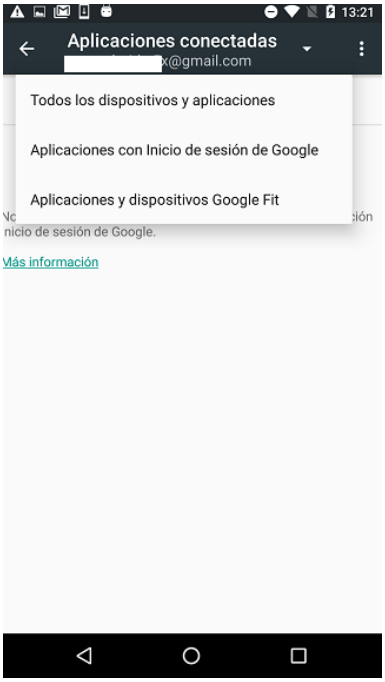
6.2.2. SERVICIOS

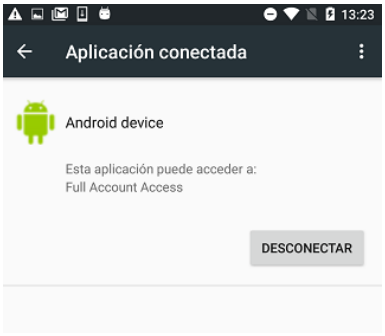
118. En esta sección se ofrecen diversos parámetros generales asociados a los distintos servicios de Google; se describen a continuación los más relevantes desde el punto de vista de seguridad y privacidad:





119. **Aplicaciones conectadas**: permite ver qué apps (además de las propias de Google) se han conectado a la cuenta de usuario seleccionada, con inicio de sesión o con dispositivos Google Fit. De hecho, a fecha de elaboración de la presente guía, la única opción que se conoce para cerrar la sesión en la cuenta de usuario de Google en el dispositivo es proceder a la desconexión de la app que se muestra como "Android device":





120. **Aplicaciones instantáneas**: esta funcionalidad se describe en el apartado "14.3. Instant Apps".

121. **Búsqueda**: contiene todas las opciones de configuración relativas a la interacción con el asistente de Google (ver apartado "8. Asistente de Google, Mi Tablón y Servicios de búsqueda de Google"), por ejemplo, el idioma y región de búsqueda, las notificaciones, así como los parámetros que se engloban en el apartado "6.2.3. Cuentas y privacidad".

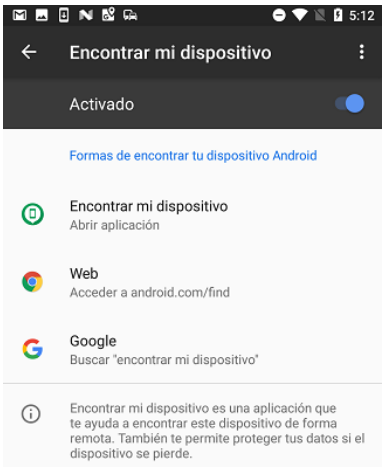
122. **Configurar dispositivo cercano**: permite configurar un dispositivo personal en base a la configuración del dispositivo móvil actual a través de una conexión Wi-Fi y/o Bluetooth. Esta opción está desaconsejada desde el punto de vista de seguridad a menos que el entorno en el que se lleve a cabo la conexión esté controlado.

123. **Configurar perfil de trabajo**: para dispositivos de uso corporativo.

124. **Nearby**: esta funcionalidad se describe en el apartado "15. Google Nearby".

125. **Redes**: este ajuste está relacionado con el denominado "Proyecto Fi", lanzado por Google en 2015 [Ref.- 750], y que, de forma resumida, ofrece servicios de operador de telefonía a través de una tarjeta SIM especial para dispositivos Android específicos, proporcionando servicios de datos móviles prepagados. El dispositivo móvil se conectará a la red más favorable, y usará Wi-Fi para realizar llamadas y envío de mensajes. A través del parámetro "Asistente de Wi-Fi" que se encuentra dentro de esta sección, el dispositivo móvil se conectará automáticamente a redes Wi-Fi abiertas que Google considere fiables [Ref.- 749]. Desde el punto de vista de seguridad, no se recomienda el uso de esta funcionalidad, pues requiere que el interfaz Wi-Fi se encuentre permanentemente activo.

126. **Seguridad**: ofrece acceso a configuración relativa a la funcionalidad "Encontrar mi dispositivo" (ver apartado "10.4. Gestión remota de dispositivos Android por parte del usuario").



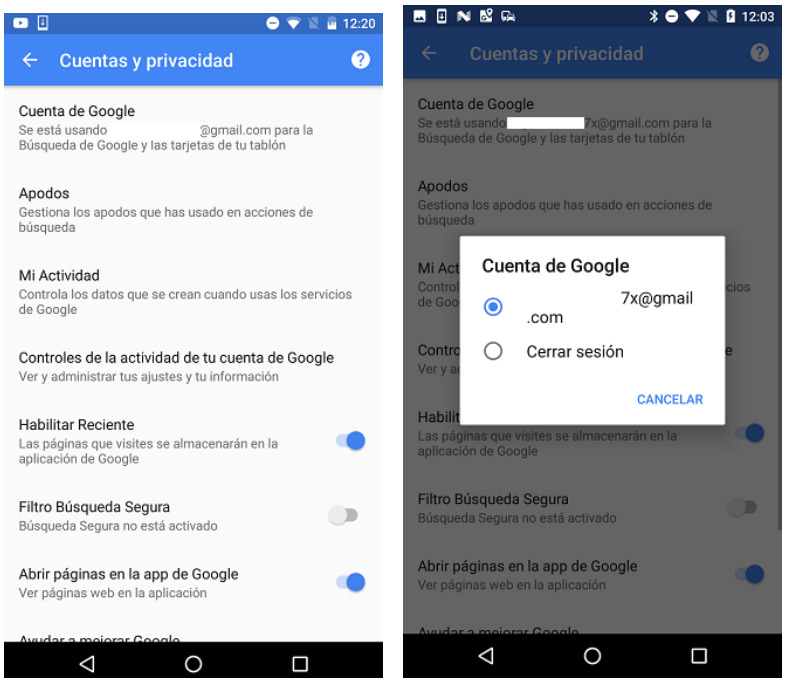
127. **Smart Lock para contraseñas**: esta funcionalidad se describe en el apartado "12.2. Servicio de contraseñas de Google Smart Lock".

128. **Ubicación**: esta funcionalidad se describe en el apartado "11. Localización (o ubicación) geográfica".

6.2.3. CUENTAS Y PRIVACIDAD

129. El apartado "Cuentas y privacidad", disponible bajo "Ajustes - [Personal] Google - [Servicios] Búsqueda - [Buscar]" contiene las opciones que se aplicarán en las búsquedas de Google y en lo relativo al servicio "Mi tablón", descritos en el apartado "8. Asistente de Google, Mi Tablón y Servicios de búsqueda de Google".

130. Algunas de estas opciones tienen su correspondencia en el interfaz web descrito en el apartado "6.2.1.2. Datos y personalización", y modifican los parámetros de la cuenta de Google del usuario, requiriendo acceso a una red de datos. A continuación, solo se describirán las opciones que no se incluyen en dicho apartado.



131. **Cuenta de Google**: además de permitir cambiar qué cuenta de usuario de Google está utilizándose para las búsquedas de Google en el dispositivo móvil de entre todas las que se hayan dado de alta, permite cerrar sesión. Este cierre de sesión solo se aplicará a las búsquedas "Búsqueda de Google" (ver apartado "7. App "Google""), pero el resto de apps y servicios disponibles bajo "Ajustes - [Personal] Google - [Servicios]" seguirán utilizando la cuenta de usuario de Google.

132. **Filtro Búsqueda Segura (SafeSearch)**: si está activado, permite bloquear imágenes, videos y sitios web explícitos (por ejemplo, con contenido pornográfico) de las búsquedas de Google, evitando la mayor parte del contenido para adultos. Concretamente, el filtro SafeSearch permite bloquear imágenes y vídeos con contenido sexual explícito, así como resultados que puedan dirigir a contenido explícito, de los resultados de las búsquedas de Google (si se desea obtener información sobre cómo configurarlo, se recomienda consultar la referencia [Ref.-755]). Es importante reseñar que lo que se bloquea no son las páginas de contenido explícito en sí, sino la aparición de referencias a ellas en las búsquedas.

133. **Abrir páginas en la app de Google**: si se selecciona esta opción, las búsquedas web se abrirán dentro del contexto de la app de Google, en lugar de lanzar un navegador web.

134. **Ayudar a mejorar Google**: envía estadísticas de uso de la actividad de Google Now Launcher. Se recomienda reducir el envío de información y/o estadísticas adicionales a los servidores de Google.

135. **Editar y compartir capturas de pantalla**: permite a la "Búsqueda de Google" analizar la información contenida en las capturas de pantalla que realice el usuario, para incorporarla al resto de elementos que influencian las búsquedas.

136. En versiones más antiguas de la app de Google que la analizada en la presente guía, el menú de configuración de "Cuentas y privacidad" ofrecía la opción "Compartir información sobre desplazamiento", deshabilitada por defecto, que posibilitaba la compartición de información actualizada con otros usuarios de Google sobre viajes y desplazamientos, permitiendo elegir qué contactos podían ver la ubicación del

usuario a través de Google+. Esta opción ya no se encuentra disponible en la app "Google", sino que se traslada a la app Maps (ver apartado "11. Localización (o ubicación) geográfica").

6.3. GESTIÓN DE LAS CREDENCIALES DE LA CUENTA DE USUARIO DE GOOGLE

137. Desde el punto de vista de seguridad, la opción ideal sería no almacenar la contraseña de la cuenta del usuario de Google en el dispositivo móvil, mitigando así el riesgo de que un potencial atacante obtenga acceso al mismo, y como consecuencia, a la cuenta del usuario, junto a todos sus servicios asociados, como por ejemplo Google Play o Gmail.

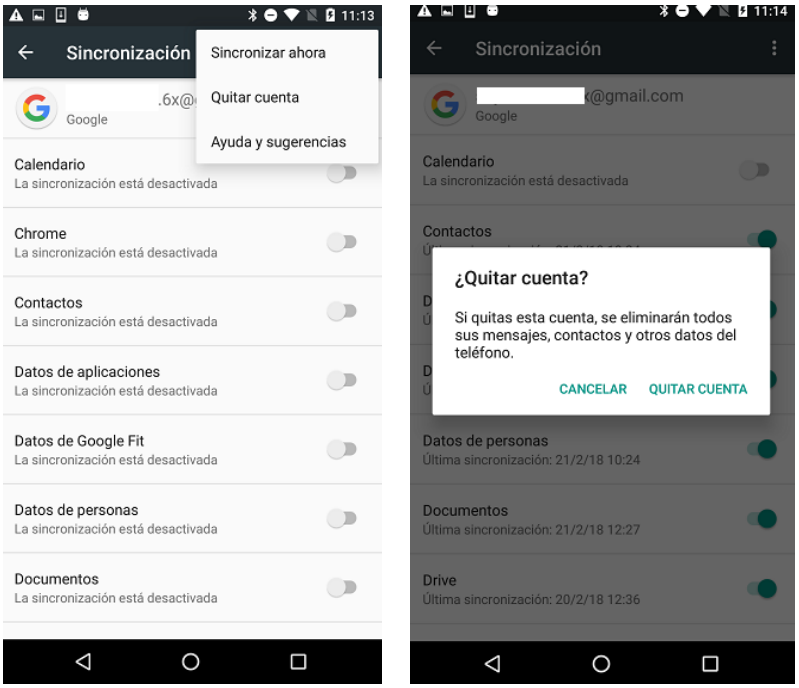
138. Sin embargo, no se ha identificado ninguna opción de configuración en el dispositivo móvil, a través de "Ajustes [Cuentas]" o "Ajustes [Personal] - Seguridad" (o en la configuración de la app "Play Store" o "Gmail"), para evitar el almacenamiento de la contraseña (o de los *tokens* de autentificación) de la cuenta de usuario de Google.

139. Es decir, la contraseña (o *token* de autentificación) asociada a la cuenta del usuario queda almacenada automáticamente en el dispositivo móvil, no siendo posible evitar su almacenamiento. Como resultado, tras encender el dispositivo móvil, se dispone de acceso directo y completo a la cuenta del usuario y a todos los servicios asociados.

140. Este escenario de gestión y almacenamiento automático de contraseñas para las cuentas del usuario es similar para las cuentas de otros servicios, por ejemplo redes sociales como Facebook o Twitter, en los cuales la contraseña (o token) queda almacenada en la app y, por tanto, en el dispositivo móvil, no siendo posible evitarlo.

141. Las alternativas identificadas para evitar esta asociación entre cuenta/contraseña de Google y el dispositivo móvil son:

- Eliminar la cuenta asociada cada vez que se termina de hacer uso de la misma a través de la pantalla de "Ajustes - [Personal] Cuentas - Google - <nombre de cuenta> … - Quitar cuenta". Esta opción presenta el inconveniente de que todos los datos y personalización de las apps de Google se eliminarían del dispositivo móvil.



- Desconectar la app "Android device" de la cuenta (según se describe en el apartado "6.2.2. Servicios") a través de "Ajustes - [Personal] Google - [Servicios] Aplicaciones conectadas - Android device - Desconectar". Mediante este método, todas las apps de Google dejarán de tener acceso a la cuenta de usuario. Desde cualquiera de ellas, a través del mensaje de la app relativo a que no se ha podido iniciar sesión en la cuenta (cuyo contenido concreto es dependiente de cada app; en algunas de ellas este estado se refleja mediante errores de sincronización con los servicios asociados), se ofrece al usuario la posibilidad de volver a iniciar sesión en la cuenta.

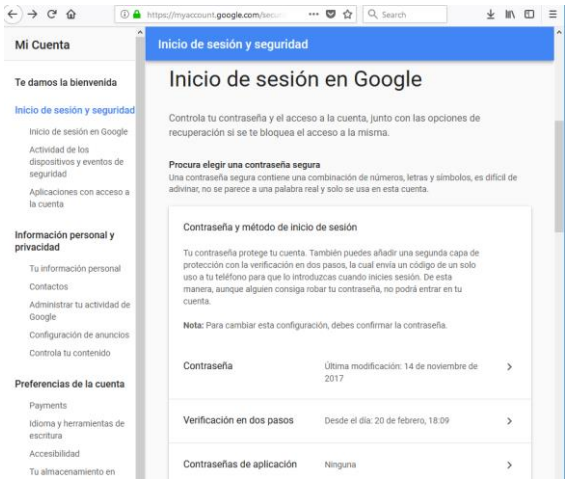
142. En cualquiera de los dos métodos descritos anteriormente, la situación se mantiene aunque se reinicie el dispositivo móvil.

143. Si se hace uso del dispositivo móvil como segundo factor de autentificación, la desconexión de la cuenta de usuario de Google por cualquiera de los dos métodos impediría poder utilizarlo para validar el uso de la cuenta de Google del usuario en otros dispositivos.

144. Android no proporciona capacidades para modificar la contraseña de la cuenta principal de Google asociada al dispositivo móvil, ni para modificar las contraseñas de otros servicios de Google disponibles en Android.

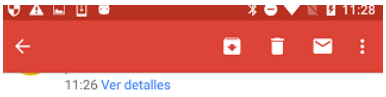
145. Las siguientes recomendaciones aplican tanto a la cuenta principal de Google como a las cuentas de otros servicios, como Twitter o Facebook. Para otros servicios será necesario evaluar la secuencia de acciones a seguir independientemente (pero de manera similar a como se describe a continuación), y en todo caso, hacer uso del acceso web estándar a los mismos.

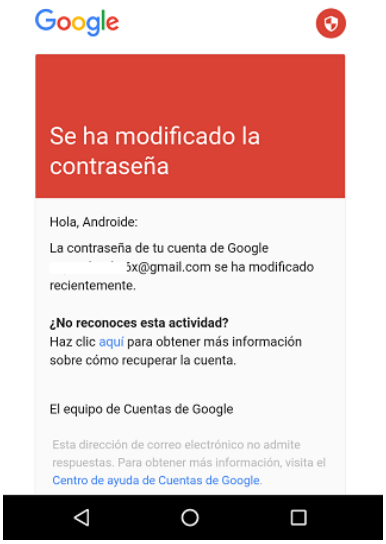
146. Para invalidar la contraseña almacenada para la cuenta principal de Google asociada al dispositivo móvil, el método más directo pasa por modificar la contraseña a través de la página web estándar del servicio "https://myaccount.google.com - Inicio de sesión y seguridad - Inicio de sesión en Google - Contraseña", desde otro ordenador o desde el propio navegador web del dispositivo móvil Android.

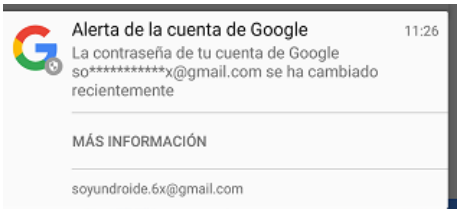


147. Una vez se accede al menú de cambio de contraseña, se distinguen dos escenarios:

- Cuando el mecanismo de verificación en dos pasos está desactivado y se cambia la contraseña de la cuenta de usuario de Google, se cerrará la sesión en el dispositivo móvil y se enviará un mensaje informativo al buzón de Gmail del usuario:

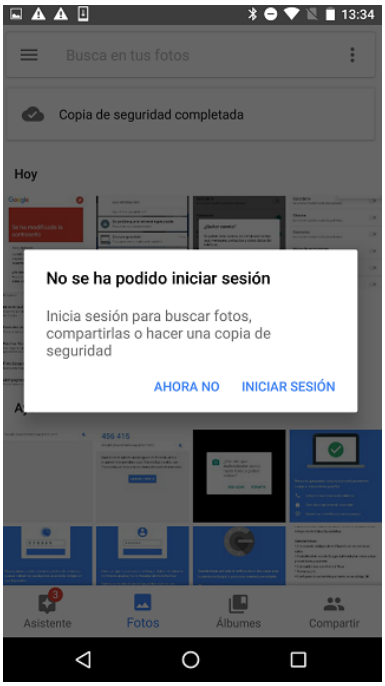


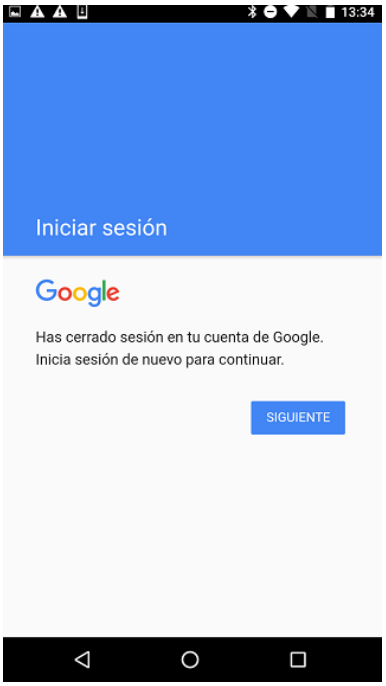




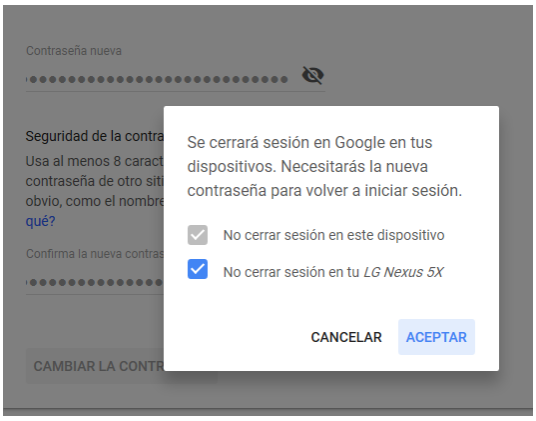
Tan pronto una app que utilice los servicios de Google trate de conectarse a ellos, se producirá un error (en versiones de Android hasta la 5.1.1 inclusive se generaba una notificación de error de sincronización y se instaba al usuario a introducir la nueva contraseña), el cual dependerá de la app concreta, y se llevará al usuario a la pantalla de configuración de la cuenta[4]. Las siguientes imágenes muestran el error de las apps "Gmail" y "Fotos" y la ventana que se muestra cuando se selecciona el mensaje que invita a iniciar sesión:

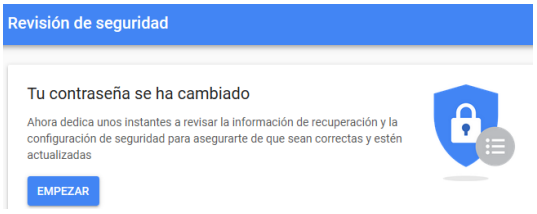
[4] Algunas apps o servicios concretos de Google también pueden generar sus notificaciones, como Google Drive.



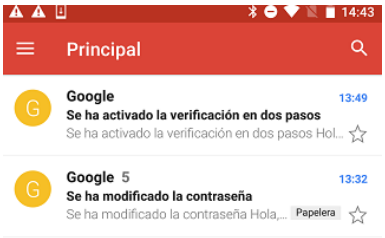


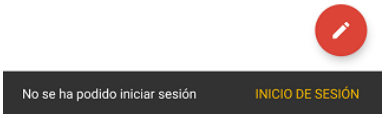
- Si el mecanismo de verificación en dos pasos se encuentra activo, el interfaz web de Google presentará la siguiente ventana:

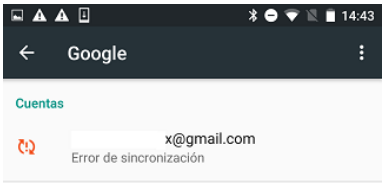




  - Si al cambiar la contraseña se deja marcada (configuración por defecto) la opción "No cerrar sesión en tu <dispositivo>", la sesión correspondiente a la cuenta de usuario de Google del dispositivo móvil no se cerrará, por lo que todos los servicios y apps de Google seguirán funcionando con normalidad, incluso aunque se reinicie el dispositivo móvil.
  - Si se desmarca la opción, la situación será similar a la que se presenta cuando la verificación en dos pasos está desactivada, por lo que las apps que se conecten a servicios de Google mostrarán errores y ofrecerán una opción para iniciar sesión de nuevo. Si se consulta la cuenta de usuario de Google a través de "Ajustes - [Personal] Cuentas - Google", se observará un error de sincronización:







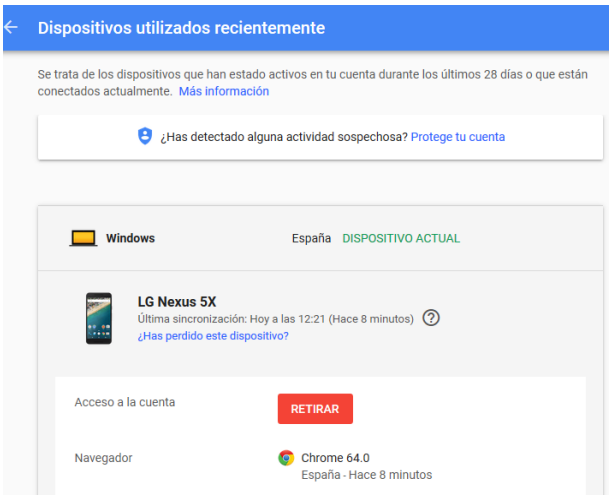
148. La siguiente tabla muestra la petición de la app Gmail para acceder a la cuenta y sincronizar los mensajes, y la respuesta fallida procedente del servidor, denegando la autorización:

```
POST /mail/g/?version=25&clientVersion=25 HTTP/1.1
Authorization: Bearer ya29.Go4BagV6K1YvWV3dax-r9emD3w_ <...> 55MQQ
Content-Encoding: gzip
Host: mail.google.com
User-Agent: Android-GmailProvider/60087425 (sw411dp; 420dpi) (bullhead MTC20K);
gzip
Cookie: COMPASS=gmail=CokBAAlriVeYO_TatyWzl0vWZqmlDPo6GEqx_ <...> kJ7g
Cookie2: $Version=1

HTTP/1.1 401 Unauthorized
Content-Type: text/html; charset=UTF-8
WWW-Authenticate: Bearer realm="https://accounts.google.com/"
Server: GSE
<HTML>
<HEAD>
<TITLE>Unauthorized</TITLE>
</HEAD>
<BODY BGCOLOR="#FFFFFF" TEXT="#000000">
<H1>Unauthorized</H1>
<H2>Error 401</H2>
</BODY>
</HTML>
```

149. Es importante reseñar que no se recibe ninguna notificación que informe al usuario de que el error es debido a un cambio en la contraseña.

150. Si el cambio de contraseña se debe a que el usuario ha perdido el dispositivo móvil, se deberá desmarcar la opción "No cerrar sesión en tu <nombre_dispositivo>"para asegurarse de que no se mantendrá abierta la sesión y que un tercero no autorizado con acceso físico al dispositivo móvil pueda tener acceso a toda la funcionalidad de la cuenta de Google del usuario.



Nota: La solicitud de la contraseña asociada a la cuenta del usuario también se puede presentar al cambiar la tarjeta SIM del dispositivo móvil, según la versión de Android y el modelo de dispositivo móvil empleado.

151. En caso de sustracción o pérdida del dispositivo móvil, este cambio de contraseña a través de la web debería ser una de las primeras tareas a realizar por el usuario.

152. Por otro lado, debido a que Android está diseñado para trabajar con una cuenta de usuario de Google que esté siempre activa, tampoco proporciona capacidades para desconectarse (o cerrar la sesión actual) de la cuenta de usuario de Google, de forma que la próxima vez que se utilice cualquiera de los servicios asociados, y se establezca una sesión con estos, se solicite de nuevo al usuario la contraseña de la cuenta.

153. El método disponible para forzar esta desconexión, sin tener que eliminar la cuenta del dispositivo móvil y/o resetear el mismo, pasa por cambiar la contraseña desde la web (como se ha descrito previamente) o utilizar apps de terceros con este propósito.

154. En versiones previas de Android, 1.x, era posible forzar esta desconexión borrando la caché y los datos asociados a algunos de los servicios críticos de conexión y sincronización con Google (Gmail, Google Apps y Gmail Storage). Los botones "Borrar datos" y "Borrar caché" estaban disponibles a través del menú de "Ajustes - Aplicaciones - Administrar aplicaciones", desde la pestaña "Todas", seleccionando una por una estas aplicaciones (o servicios). Esta recomendación no aplica desde Android 2.x.

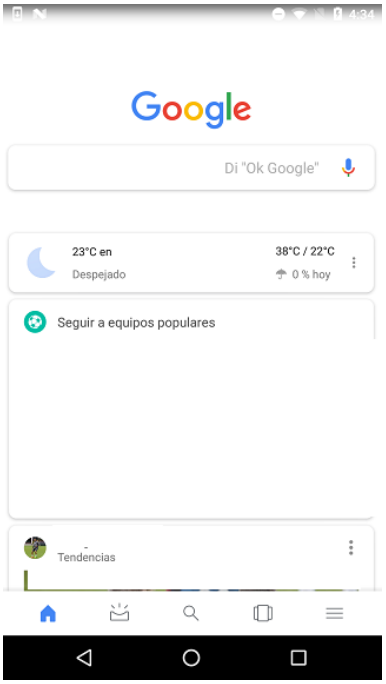
7. APP "GOOGLE"

155. La app "Google" controla, además de los servicios descritos en el apartado "8. Asistente de Google, Mi Tablón y Servicios de búsqueda de Google", multitud de ajustes relacionados con la cuenta de usuario de Google, y, particularmente, los correspondientes al apartado "6.2.1.2. Datos y personalización".

156. La última versión de la app "Google" disponible a fecha de elaboración de la presente guía y empleada en el presente apartado está detallada en al apartado "1.

Introducción". Se representa mediante un símbolo "G" multicolor (a diferencia de versiones anteriores, en las que se empleaba una letra "g" de color azul).

157. La app "Google" se puede invocar en Android desde su icono (círculo con la letra "G" multicolor) desde las pantallas de inicio, desde el *Launcher*, o realizando una pulsación prolongada sobre el botón de inicio, que despliega el menú que se muestra en la zona inferior de la siguiente imagen (en lugar de deslizando la pantalla desde la parte inferior hacia arriba, como ocurría en la versión 5.1.1 de Android) y permite ver las tarjetas existentes, siempre que se disponga de conexión de datos (Wi-Fi o 2/3/4G):



158. La app "Google" es el interfaz que permite gestionar las búsquedas (de texto, voz, contenido multimedia, etc.) y otras actividades diversas asociadas a la cuenta de usuario de Google activa en el dispositivo móvil y relativas a las aplicaciones de Google. Esta app ha evolucionado desde sus orígenes, y sigue en constante evolución, de forma que su interfaz gráfico de usuario (GUI), su funcionalidad y las opciones de configuración que proporcionan pueden cambiar significativamente entre distintas versiones de la propia app y/o de Android.

159. El icono con el símbolo de una casa (en el margen inferior izquierdo) es el correspondiente al inicio, en el que se encuentra el campo principal de búsqueda y el acceso a la funcionalidad "Ok Google" (ambos descritos a continuación).

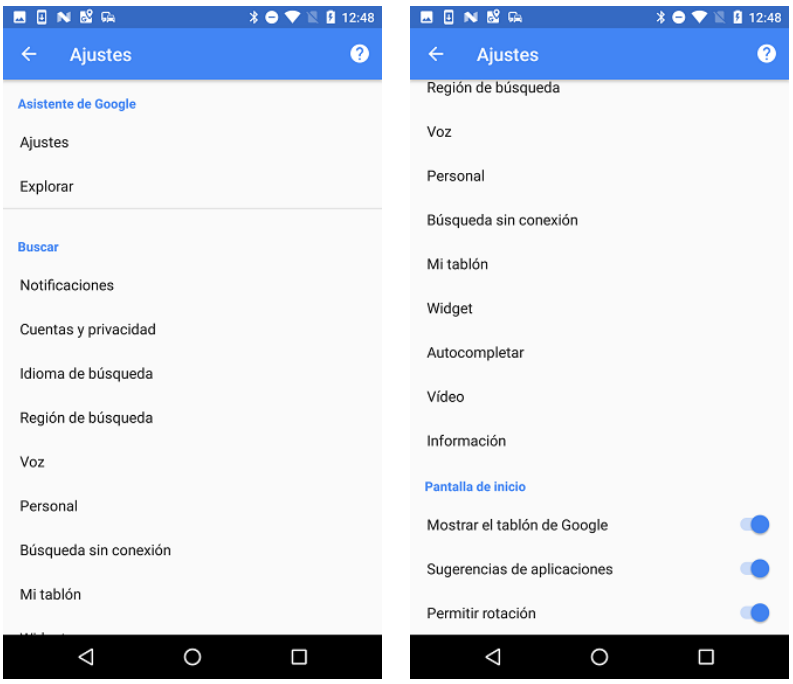
160. El icono situado en segunda posición por la izquierda (con forma de mensaje de correo electrónico) invoca al asistente de Google, el cual requiere que la "Actividad en la Web y en Aplicaciones" descrita en el capítulo "6. Cuenta de usuario de Google" se encuentre activa, pues el asistente ofrece sugerencias en base a los datos que Google almacena en relación a la interacción del usuario con los distintos servicios, apps y webs a los que accede.

161. El icono central, correspondiente a la lupa, permite realizar búsquedas en Internet dentro del contexto de la app "Google", en lugar de tener que utilizar un navegador web.

162. El icono situado en segunda posición por la derecha (con forma de ventana) se denomina "Recientes", y muestra las búsquedas realizadas desde la app "Google" (con la referencia al momento del tiempo en que tuvieron lugar), así como sugerencias para usar esta funcionalidad.

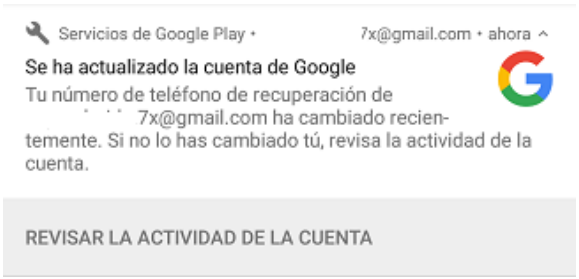
163. Por último, el menú situado en la parte más a la derecha de la pantalla (representado por tres líneas horizontales paralelas), proporciona las opciones de configuración de la app "Google", concretamente, mediante la opción "Ajustes". En versiones más antiguas de la app "Google", las opciones de configuración se localizaban en el margen superior derecho.

164. Estos ajustes son los mismos a los que se accede desde "Ajustes - [Personal] Google - [Servicios] Búsqueda", que se organizan en tres secciones: Asistente de Google, Buscar y Pantalla de inicio:



165. Los detalles sobre estos ajustes se describen en el apartado "8. Asistente de Google, Mi Tablón y Servicios de búsqueda de Google".

166. La app "Google" genera notificaciones relativas a cambios en la cuenta de Google del usuario, por lo que se recomienda estar pendiente de ellas:



8. ASISTENTE DE GOOGLE, MI TABLÓN Y SERVICIOS DE BÚSQUEDA DE GOOGLE

167. Android 4.1 ("Jelly Bean") introdujo en 2012 "Google Now", un asistente personal que se incluyó como un servicio de la aplicación "Google Search". Éste hacía uso de una interfaz de usuario de lenguaje natural para responder preguntas, hacer recomendaciones y realizar acciones transmitiendo la petición del usuario a los servicios web correspondientes. Además de responder a consultas del usuario, Google Now ofrecía información al usuario, de forma pasiva, sobre aspectos que podían ser de su interés en función de los hábitos de búsqueda recopilados por las aplicaciones y servicios.

168. Google Now fue evolucionando a lo largo de los años, ampliando su funcionalidad y adaptándose a las aplicaciones del ámbito y ecosistema de Google.

169. Con las versiones recientes de la aplicación "Google" (incluyendo la versión 8.13.15.21 empleada en la elaboración de la presente guía), los servicios anteriormente conocidos como "Google Now" se englobaron en lo que pasó a denominarse "*feed*" o "Google Feed", y se configuran en la nueva versión de la app a través del menú "Mi tablón" de la aplicación "Google". Para más información, se recomienda consultar la documentación oficial de usuario de Google [Ref.- 624] [Ref.- 625].

Nota: Las opciones de configuración de la aplicación "Google" son extremadamente dependientes de la versión de la app, por lo que algunos de los puntos descritos en el presente apartado pueden no corresponder con los existentes en otros dispositivos móviles con versiones de la aplicación "Google" diferentes.

8.1. MI TABLÓN

170. El presente apartado utilizará la nomenclatura empleada por Google a fecha de la elaboración de la presente guía para a los servicios relativos al "*feed*" (o "Google Feed"), es decir "Mi Tablón" (o, simplemente, "tablón"), en lugar del término "Google Now" de versiones anteriores de Android.

171. El "tablón" ofrece su información dentro de la app "Google", pudiendo incorporarse a la pantalla de inicio si se activa el ajuste "[Pantalla de inicio] Mostrar el tablón de Google". Este ajuste, al activarse, hará que el tablón se pueda acceder deslizando el dedo de izquierda a derecha desde la pantalla de inicio.

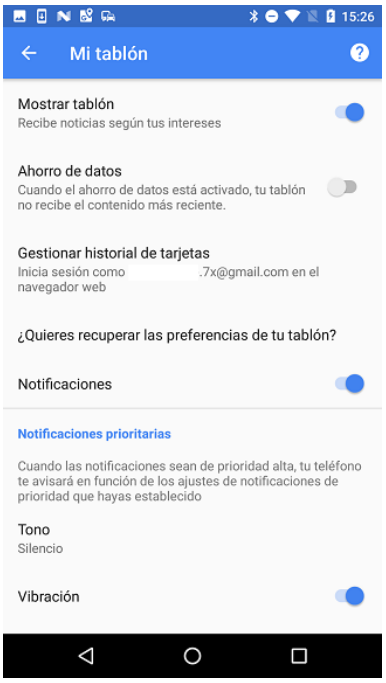
172. Los servicios asociados a "Mi Tablón" ejecutan en segundo plano, analizando los datos de la actividad diaria del usuario, su ubicación (e histórico de ubicaciones) y mostrando las tarjetas de información (anteriormente conocidas como tarjetas "Google Now" o tarjetas Now) o notificaciones en función de los eventos que ocurren en tiempo real, y proporcionan su información principalmente a través de la app "Google", disponible para la realización de búsquedas a través del buscador de Google.

173. Es importante reseñar que las opciones de configuración concretas son dependientes de la versión de la app "Google" que esté instalada. La documentación descrita en la presente guía corresponde a las opciones de la versión de la app "Google" de agosto de 2018, disponible para Android 7.1.2. Por tanto, en función de

la versión de esta aplicación, los menús y opciones pueden variar y no corresponder con los aquí expuestos. Para conocer la versión de la app instalada, se puede consultar desde el menú "Ajustes - Información" de la app "Google", o desde el menú general "Ajustes - [Dispositivo] Aplicaciones - Google".

174. La activación de "Mi Tablón" se puede llevar a cabo durante el proceso de instalación y configuración inicial de Android (ver apartado "16. Proceso de instalación y configuración inicial"), cuando se da de alta una cuenta de usuario de Google en el dispositivo móvil (si no se hizo durante la instalación), o posteriormente a través de los ajustes de la aplicación "Google".

175. Si este servicio no se activó en tiempo de instalación, se dispone del interruptor "Ajustes - [Personal] Google - [Servicios] Búsqueda - [Buscar] Mostrar tablón":

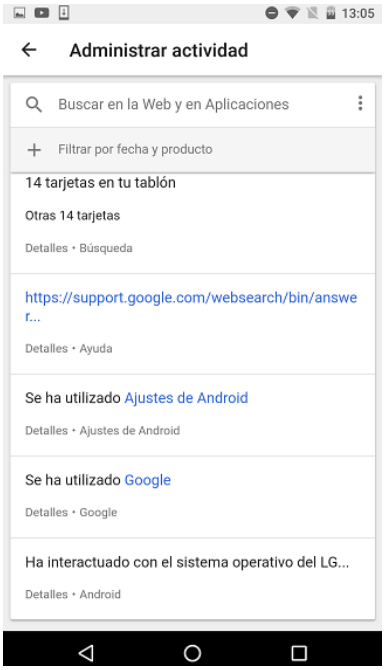


176. El servicio "Mi tablón" hace uso de los servicios de ubicación (incluyendo el historial de ubicaciones; ver apartado"11.5. Historial de ubicaciones"), datos del calendario del usuario, sus búsquedas en la web y aplicaciones (incluyendo el historial web; ver apartado "14.1.3. Historial de actividad web") y otros datos del usuario disponibles en los productos y servicios de Google (y/o de terceros). En caso de que la "Actividad en la Web y en Aplicaciones" esté desactivada, el tablón mostrará información genérica; en caso contrario, se proporcionará información acorde al perfil del usuario que Google genera en base a su actividad.

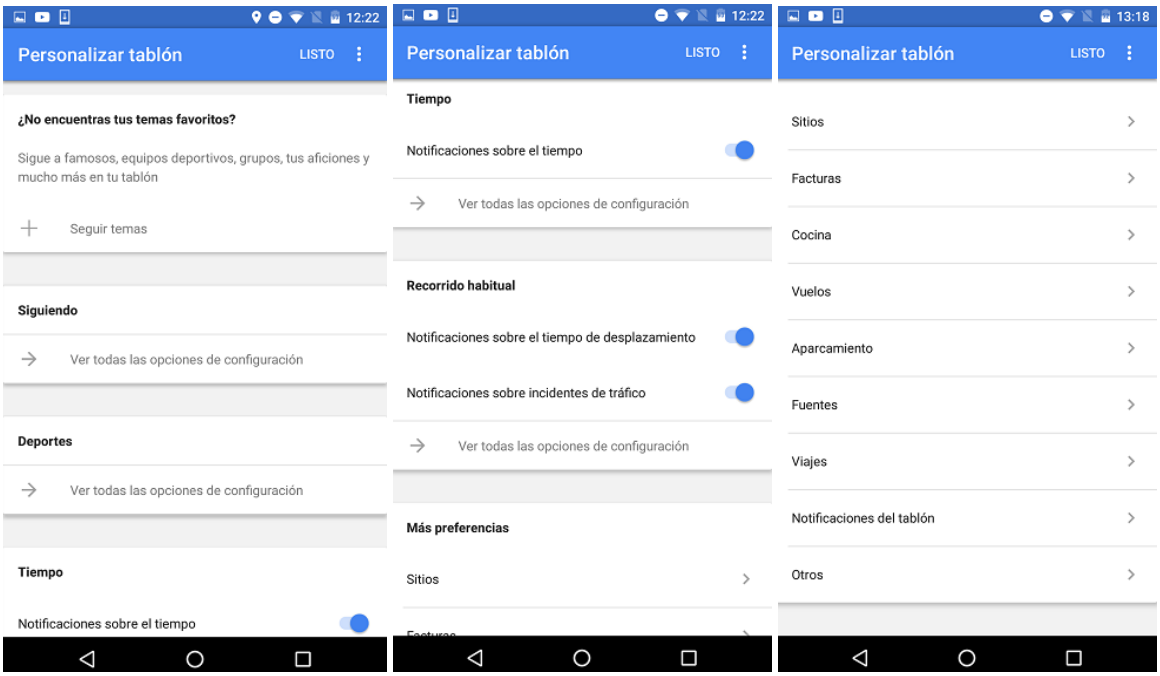
177. Desde el punto de vista de seguridad y privacidad, salvo que se desee hacer uso de la funcionalidad ofrecida por el *feed* (o tablón), se recomienda no activar estas capacidades, debido a que conllevan un uso y análisis intensivo, y muy detallado, de los datos y actividades diarias del usuario y su cesión a Google.

178. Entre los ajustes de "Mi Tablón", se puede seleccionar "Ahorro de datos" (para evitar un consumo de datos móviles indeseado) y la recepción de "Notificaciones" asociadas a él.

179. Una vez activado el botón "Actividad en la Web y en Aplicaciones", Google comenzará a recabar múltiples datos sobre toda la actividad del usuario, como se ilustra en la siguiente imagen:



180. Para configurar las tarjetas que se desee recibir, hay que elegir la opción "Personalizar" en el menú de opciones (identificado por tres líneas horizontales) de la app "Google":



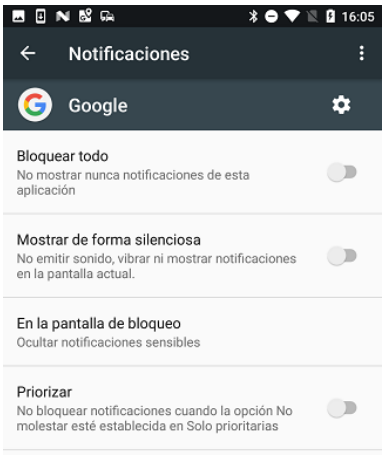
181. La información del tablón relativa a la ubicación se muestra en función de la ubicación que el usuario haya definido como "casa". Si ésta no está disponible, podrá utilizarse la definida como "trabajo", o la correspondiente a la ubicación actual del dispositivo.

182. Dada la ingente cantidad de datos personales y potencialmente sensibles que recopila la funcionalidad "Mi Tablón", desde el punto de vista de seguridad y

privacidad se desaconseja vehementemente deshabilitar completamente dicha funcionalidad.

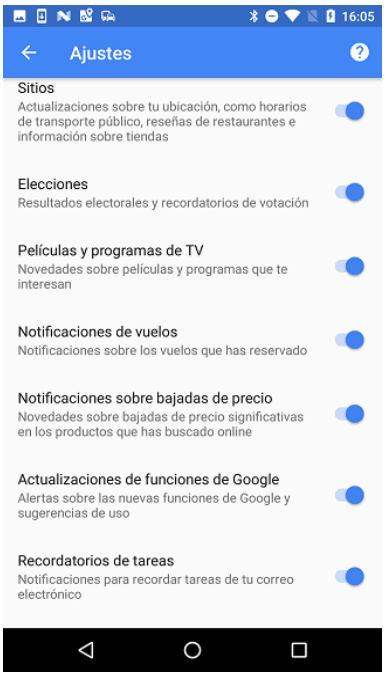
Nota: La aplicación "Google" se representa como una circunferencia con una G de varios colores (multicolor) desde sus últimas versiones, pero, en versiones más antiguas, como en la versión que se instala por defecto con la versión 6.0 de Android, se representaba como una letra "g" de color azul rodeada de un círculo blanco.

183. Además de con la opción "Notificaciones" propia del tablón, para dejar de recibir notificaciones del feed de forma puntual, se puede acceder al menú "Ajustes - [Dispositivo] Notificaciones - (Todas las aplicaciones) - (Aplicación) Google" (en versiones previas a Android 7.x el acceso era a través de "Ajustes - [Dispositivo] Sonido y notificaciones - Notificaciones de aplicaciones - (Aplicación) Google"). Para eliminar cualquier tipo de notificación basta con mover a la posición de activación del botón "Bloquear todo":



184. El icono de engranaje situado en la parte superior derecha da acceso al menú de ajustes de la app "Google".

185. Para activar o desactivar sólo ciertas categorías de notificación, se debe acceder al apartado de ajustes de "Mi Tablón" a través de la app "Google", menú de opciones y "Personalizar" (funcionalidad que se modifica frecuentemente por parte de Google), y deslizar el dedo para recorrer la pantalla hasta llegar a las opciones deseadas:



186. Con el servicio "Mi Tablón" activo, se recibirán las notificaciones correspondientes a las categorías habilitadas en el menú anterior de igual forma que el resto de notificaciones del sistema Android.

8.2. ASISTENTE DE GOOGLE

187. Además de configurar el servicio de *feed* mediante "Mi tablón", los ajustes de la sección "[Buscar]" de la aplicación "Google" incluyen otros apartados, entre los cuales figuran:

- Cuentas y privacidad: se detalla en el apartado "6.2.3. Cuentas y privacidad".
- Idioma de búsqueda: por defecto, se usa el idioma definido en la instalación, pero se puede cambiar por otro (no es posible tener varios idiomas simultáneos).
- Voz: configurar el idioma y otras capacidades asociadas a las búsquedas por voz, e incluye la "Detección de OK Google", descrito en el subapartado "8.2.1. Asistente personal y "Ok Google"".
- Vídeo: controla si los vídeos se empezarán a reproducir automáticamente y si lo harán sólo con conexión Wi-Fi o también con conexión a redes de datos móviles.
- Búsqueda sin conexión: si está activo, las búsquedas realizadas anteriormente que hayan fallado por no disponerse de conexión de datos se reintentarán, informando mediante una notificación al usuario cuando los resultados estén disponibles.

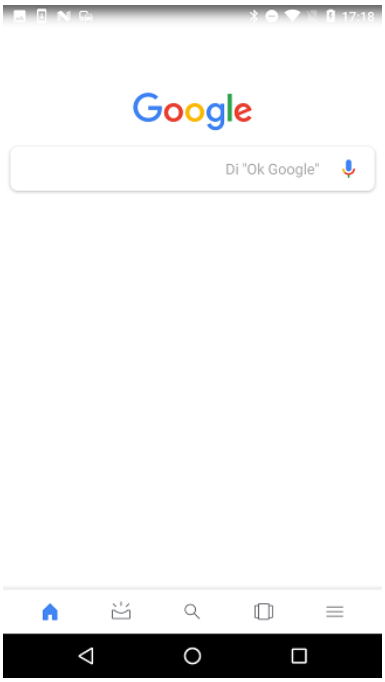
188. En versiones anteriores de la app "Google", existía un campo denominado "Búsqueda directa", que corresponde a la funcionalidad denominada "Now on Tap" (consultar el apartado "8.2.2. ¿Qué hay en mi pantalla?" para más información). Esta funcionalidad consistía permitía al usuario obtener información contextualizada referente a los contenidos de la aplicación que estuviese ejecutando en primer plano

cuando se invoca la ayuda de "Now on Tap". Esta información era también transferida al *feed*.

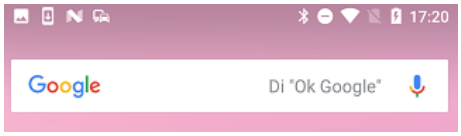
8.2.1. ASISTENTE PERSONAL Y "OK GOOGLE"

189. El servicio de búsqueda de Google se concibió como un servicio o app que, actuando como asistente, permite al usuario interactuar con el dispositivo móvil Android, por ejemplo, para realizar búsquedas de información a través del buscador de Google; el buscador de Google se encuentra actualmente integrado en el denominado "*feed*" o "Google Feed", sustituto de Google Now y dentro de la app "Google".

190. Adicionalmente, si se ha activado la configuración de "Mi Tablón" del servicio *feed*, el buscador de Google se integrará como parte de él; en caso de que no se haga uso del tablón, estará disponible como escritorio o panel individual al invocar la app "Google":



191. Adicionalmente, el servicio de búsqueda de Google se incorpora a la parte superior de las pantallas principales, o escritorios o pantallas de inicio (en adelante referidas como pantallas de inicio), representado por un campo de búsqueda y un icono con forma de micrófono. Al incluir entre sus funciones, no una búsqueda literal, sino una búsqueda adaptada al perfil del usuario creado en base a sus interacciones con otras aplicaciones de Google, se convirtió en un "asistente personal" (Google Assistant, Asistente de Google o Asistente personal de Google):



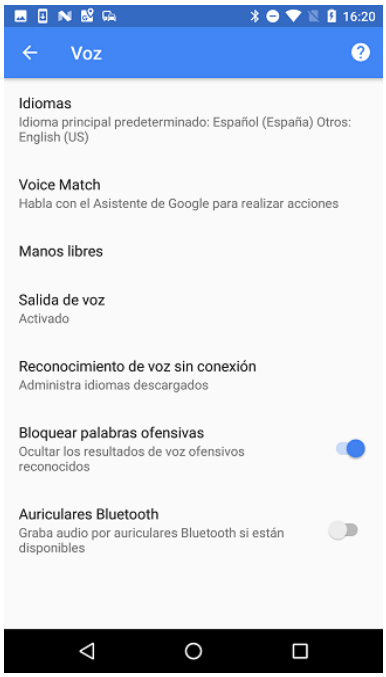
192. En el caso de estar habilitada la búsqueda por voz, al lado del icono con forma de micrófono aparecerá el texto "Di 'Ok Google'", que permite al usuario comenzar a interactuar con esta funcionalidad mediante la voz y la pronunciación de esa frase ("Ok Google").

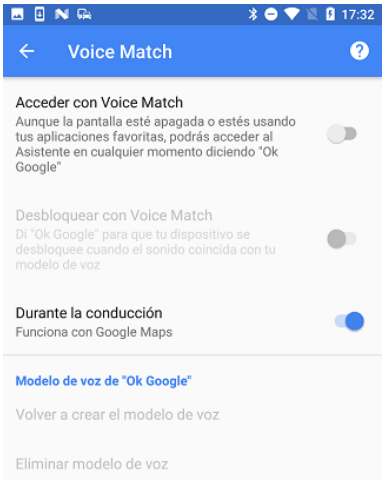
193. El Asistente (personal) de Google o Google Assistant (en adelante, "Ok Google"), está permanentemente activo, siempre que el usuario se encuentre con el dispositivo móvil desbloqueado y en las pantallas de inicio, escuchando al usuario a través del micrófono del dispositivo móvil, y esperando a que se pronuncie la frase de activación ("Ok Google").

194. Teóricamente, el dispositivo móvil no enviará ningún dato a Google mientras permanece en el modo de escucha pasiva, teniendo lugar todo el procesamiento de voz localmente en el dispositivo móvil. Tan pronto el usuario pronuncia la frase de activación, se establece una conexión mediante HTTPS con los servidores de Google para interpretar las indicaciones de voz del usuario al realizar una búsqueda o ejecutar una acción, y obtener los resultados desde los servidores de Google.

195. A fecha de elaboración de la presente guía, el servicio "Ok Google" (asociado al Asistente de Google) se ha integrado con un nuevo servicio denominado "Voice Match", concebido para dispositivos Google Home [Ref.- 754].

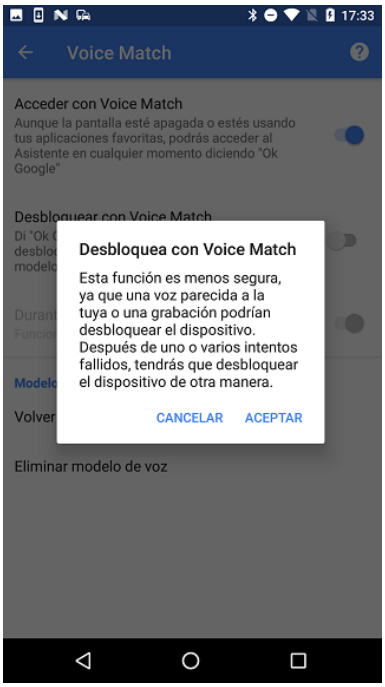
196. La funcionalidad "Ok Google" puede ser deshabilitada desde la app "Google", y en concreto, desde el botón de menú, a través de la opción "Ajustes - [Buscar] Voz":





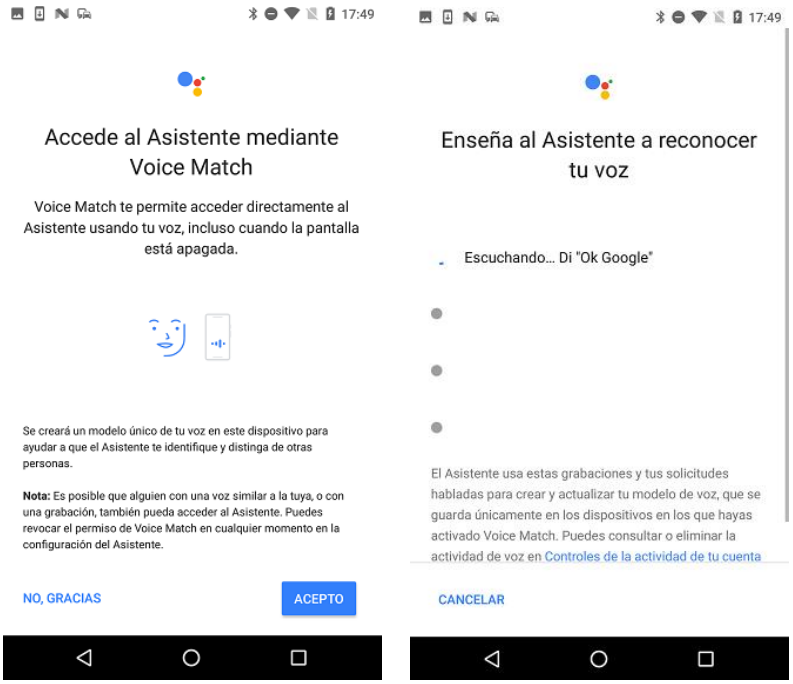
197. Si se activa el interruptor correspondiente a la función "Acceder con Voice Match" (que en otras versiones más antiguas de la app "Google" se mostraba como "Decir 'Ok Google' en cualquier momento"), al pronunciar "Ok Google" desde la app "Google" o desde cualquier pantalla de inicio, lanzará una búsqueda por voz.

198. La opción "Acceder con Voice Match" (denominada "Desbloquear con reconocimiento de voz" o "Desbloqueo por voz" en versiones menos recientes de la app "Google"), es la opción que corresponde a la función "Smart Lock - Desbloqueo por voz", la cual posibilita desbloquear el terminal al reconocer el patrón de voz del usuario al pronunciar "Ok Google" en la pantalla de bloqueo. El dispositivo informará de la repercusión que esta opción tiene desde el punto de vista de seguridad mediante el siguiente mensaje:



199. La opción "Durante la conducción": permite el envío de indicaciones de voz al dispositivo al hacer uso de Google Maps. Esta opción, habilitada por defecto, será deshabilitada si se activa la opción "Acceder con Voice Match", ya que se extiende su utilización a cualquier pantalla, incluida Google Maps.

200. La Sección "Modelo de voz de 'Ok Google'", que se habilitará al activar la opción "Acceder con Voice Match" permite registrar el modelo de voz del usuario. La opción permite volver a configurar o eliminar el modelo de voz existente (esta última opción deshabilita la opción "Acceder con Voice Match" y requiere que se vuelva a activar manualmente para poder usar de nuevo el modelo de voz). Si se selecciona la creación del modelo de voz, el dispositivo iniciará la grabación, siendo necesario decir en voz alta "OK Google" cuatro veces:



201. A la configuración de "Voice Match" se puede llegar también desde las opciones de Smart Lock: "Ajustes - [Personal] Seguridad - [Seguridad del dispositivo] Smart Lock - Voice Match".

202. Si se deshabilita la opción "Acceder con Voice Match", aún es posible hacer uso de esta funcionalidad de búsqueda mediante la voz pulsando manualmente el icono del micrófono para iniciar una búsqueda desde cualquiera de las pantallas de inicio.

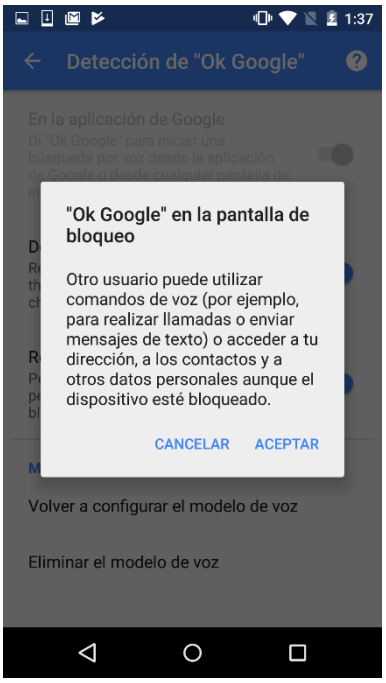
203. Por defecto, la app "Google" dispone del idioma "English (US)" preinstalado. Desde el botón de menú, y la opción "Ajustes" de la app "Google", es posible cambiar la configuración. Por ejemplo, la sección "Voz" permite seleccionar el idioma a emplear (opción "Idiomas"), mientras que la opción "Reconocimiento de voz sin conexión" permite administrar los idiomas descargados:

204. Desde la opción "Reconocimiento de voz sin conexión - Descargar idiomas" es posible configurar si se desea que se descarguen y actualicen los ficheros de reconocimiento de idiomas, a través de la pestaña "Actualizar". Por defecto, la opción seleccionada es "Actualizar idiomas solo a través de Wi-Fi", pudiéndose actualizar los idiomas en cualquier momento (a través de la conexión de datos móviles 2/3/4G), o bloquear la actualización automática por completo.

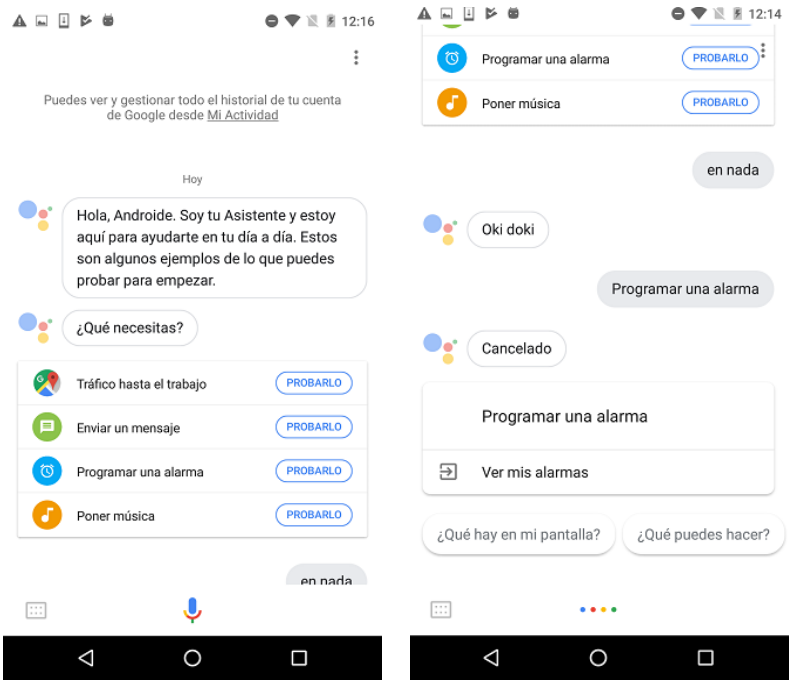
205. La opción "Salida de voz" permite configurar si se recibirá una respuesta audible para todas las búsquedas realizadas o sólo si el dispositivo está en modo manos libres.

206. La opción "Manos libres" permite determinar si se aceptarán conexiones con el dispositivo bloqueado, y proporciona un botón de activación "Auriculares Bluetooth" (habilitado por defecto). En versiones anteriores a la empleada para la elaboración de la presente guía, se disponía de la opción "Para auriculares con cable" (deshabilitado por defecto). Esta opción de auriculares con cable, de estar disponible, no debe marcarse, pues posibilitaría que alguien con acceso físico al dispositivo móvil pudiera utilizar comandos de voz con solo conectar unos auriculares. La opción de Bluetooth, al haber requerido un emparejamiento previo entre los dispositivos, proporciona algo más de seguridad, pero también se aconseja deshabilitarla ya que podrían presentarse escenarios de ataque desde una cierta distancia (sin acceso físico al dispositivo) mediante la suplantación de los dispositivos Bluetooth, de tipo manos libres, emparejados con el dispositivo móvil.

207. La opción "Ajustes de la app Google - Voz - Detección de 'Ok Google' - Resultados personalizados", existente en versiones más antiguas de la app "Google", y que permitía que otros usuarios (cuyo modelo de voz no está registrado) puedan realizar determinadas acciones mediante comandos de voz aun con el dispositivo bloqueado, no está disponible en versiones de la app "Google" más recientes, como la analizada en la presente guía. Su desaparición es ventajosa desde el punto de vista de seguridad, pues permitía acciones como las descritas en el mensaje informativo:



208. Una vez habilitado el servicio "Ok Google", se podrán realizar búsquedas por voz precedidas de la frase "Ok Google", que dará paso a la pantalla del asistente de Google y pondrá al dispositivo en modo de escucha y reconocimiento de voz, y presentará varias opciones a modo de ejemplo:



209. Desde el punto de vista de seguridad se recomienda no habilitar la funcionalidad de "Ok Google", salvo que se valoren los riesgos existentes frente a los beneficios obtenidos, sobre todo en caso de que un tercero no autorizado pueda grabar la voz del usuario, o imitarla, y disponer de acceso al dispositivo.

210. El uso de la funcionalidad "Voice Match" ("Ok Google") no requiere que la "Actividad de Voz y Audio" esté activa dentro de la sección "Controles de la actividad de tu cuenta" descritos en el apartado "6.2. Ajustes "Google"".

8.2.2. ¿QUÉ HAY EN MI PANTALLA?

211. Android 6.0 (Marshmallow) introdujo la funcionalidad "Now on Tap" o "Búsqueda directa", concebida como un asistente para proporcionar información contextualizada referente a los contenidos de la aplicación que esté ejecutando en primer plano cuando se invoca la ayuda de "Now on Tap".

212. Esta funcionalidad, que no está disponible como tal a fecha de elaboración de la presente guía[5], ha sido sustituida por "What is on my screen?" (¿Qué hay en mi pantalla?), aunque ésta última no ofrece todas las capacidades de su predecesora.

213. La funcionalidad "Now on Tap", también conocida como "Búsqueda directa" se concibió como un asistente para proporcionar información contextualizada referente a los contenidos de la aplicación que esté ejecutando en primer plano en un dispositivo móvil Android cuando se invoca la ayuda de "Now on Tap".

214. El propósito de esta funcionalidad era facilitar al usuario a través de una sola pulsación la búsqueda en Google sobre elementos que se referencian en las aplicaciones basándose en el contexto de la información concreta que se está mostrando. Así, por ejemplo, si se tiene abierta la aplicación "Google Maps", al invocar "Now on Tap" se lanzará una búsqueda sobre los puntos de interés que allí aparezcan. Si se está mencionando un personaje público en una ventana del navegador web, se mostrará una tarjeta con la información básica de dicha persona.

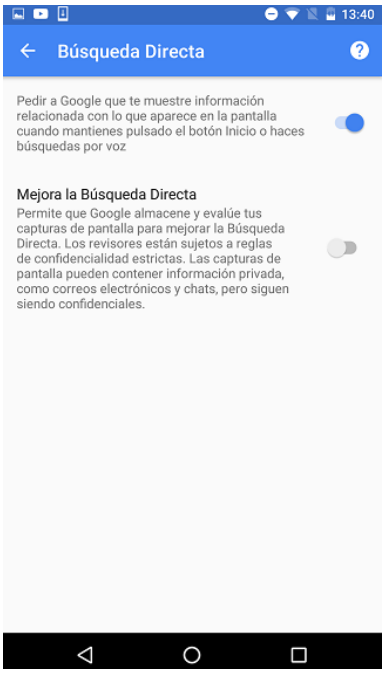
215. Con la versión inicial de Android 6.0, la función "Now on Tap" requería que el dispositivo móvil estuviese configurado con el idioma inglés para poder ser utilizada. Posteriormente, se incluyeron otros idiomas, entre ellos el español, como configuraciones válidas para acceder a esta funcionalidad.

216. "Now on Tap" está inhabilitado por defecto, y se requiere seguir una serie de pasos para poder utilizarla, los cuales se detallan a continuación. Se mantiene esta descripción en la presente guía, a pesar de no estar ya disponible, para cubrir las configuraciones de versiones de Android y de la app "Google" que aún la ofrezcan.

217. En primer lugar, ha de habilitarse el servicio "Mi Tablón", también conocido como *feed* o, en versiones anteriores, como "Google Now", siguiendo los pasos detallados en el apartado "8. Asistente de Google, Mi Tablón y Servicios de búsqueda de Google".

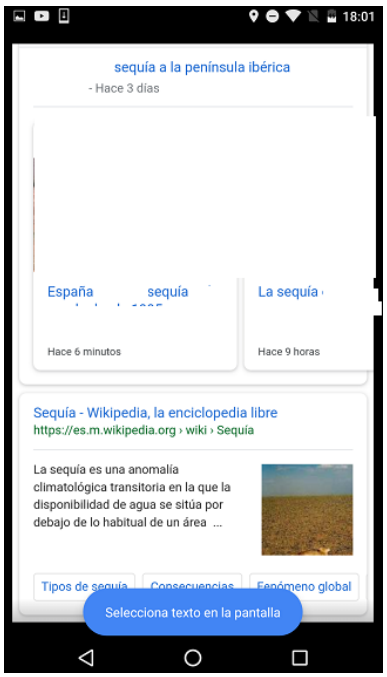
218. En segundo lugar, dentro de los ajustes de la app "Google", hay que entrar en el apartado "Búsqueda directa" y activar el botón que aparece en la parte superior de la siguiente imagen:

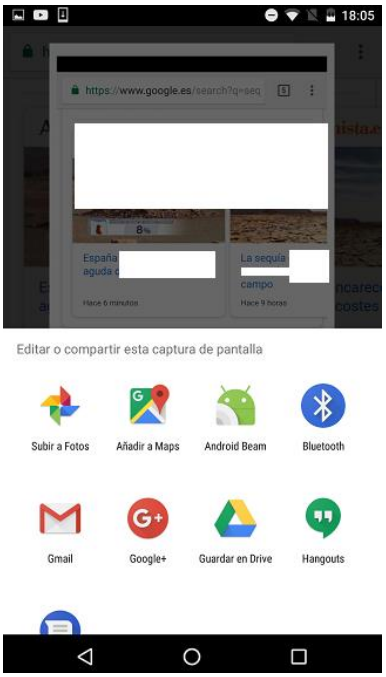
[5] https://support.google.com/websearch/forum/AAAAgtjJeM4xHc5zXjT08M?hl=es



219. A partir de ese momento, desde cualquier pantalla de la aplicación que esté en primer plano y pulsando prolongadamente el botón de inicio del dispositivo móvil, era posible buscar información contextualizada o lanzar acciones asociadas al tipo de búsqueda que se esté realizando, por ejemplo:

- Seleccionar texto para obtener detalles: tras pulsar el botón de inicio, aparecerá un menú en la parte inferior de la pantalla que ofrece la posibilidad de seleccionar texto (tocando sobre el icono de una mano con un dedo elevado y marcando el texto sobre el que se desea obtener más detalles).



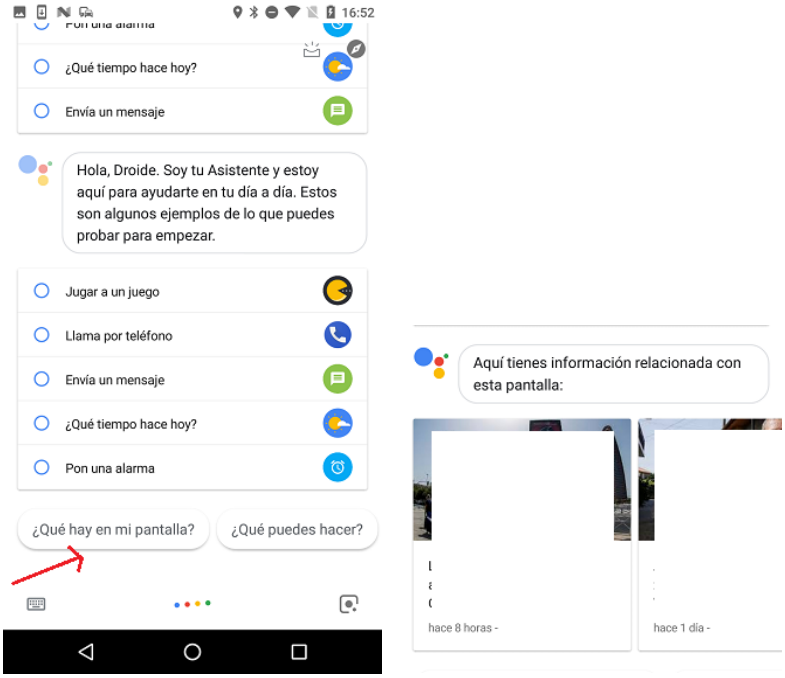


- Compartir la pantalla activa a través de otras aplicaciones (icono correspondiente a un grafo de tres puntos).
- Traducir: seleccionando el icono de tres puntos alineados en vertical (disponible solo para ciertos idiomas).

- Buscar por imagen: al pulsar prolongadamente sobre el botón de inicio cuando haya una imagen en pantalla, Google proporcionará información sobre dicha imagen.
- Buscar con la cámara: si, tras enfocar una imagen con la app "Cámara" se pulsa sobre el botón de inicio, Google proporcionará información sobre dicha imagen.

220. De nuevo, toda la actividad relativa a las búsquedas de "Now on Tap" se envía a los servidores de Google y se almacena en la cuenta del usuario, por lo que, desde el punto de vista de la privacidad, se desaconseja hacer uso de ella.

221. La funcionalidad "¿Qué hay en mi pantalla?" también se invoca mediante "Ok Google" o con una pulsación larga en el botón de inicio, pero no ofrece tantas opciones de búsqueda personalizada como "Now on Tap" [Ref.- 752].



9. RECOMENDACIONES GENERALES DE SEGURIDAD DE LA CUENTA DE GOOGLE

222. Dado que, como se documenta a lo largo de la presente guía, la cuenta de usuario de Google alberga multitud de datos e información personal del usuario, protegerla de accesos no autorizados es un elemento fundamental desde el punto de vista de seguridad, tanto del dispositivo móvil, como del propio usuario.

223. Por ello, el primer paso es elegir una contraseña de acceso robusta, diferente de cualquier otra contraseña empleada en otros servicios o aplicaciones y, preferiblemente, que sea suficientemente larga y (potencialmente) contenga múltiples caracteres dentro de los diferentes conjuntos de caracteres (letras minúsculas, mayúsculas, números y signos de puntuación). Como recomendación general, se debe dar prioridad al uso de una frase de paso (*passphrase*), de mayor longitud, frente a una contraseña de paso (*password*).

224. La configuración e información relativa a la seguridad de la cuenta de usuario de Google está disponible en la sección "Inicio de sesión y seguridad".

225. De forma general, se recomienda cambiar la contraseña asociada a la cuenta de usuario de Google con cierta periodicidad (según su robustez) a través del menú "Contraseña y método de inicio de sesión":

9.1. NOTIFICACIONES DE SEGURIDAD

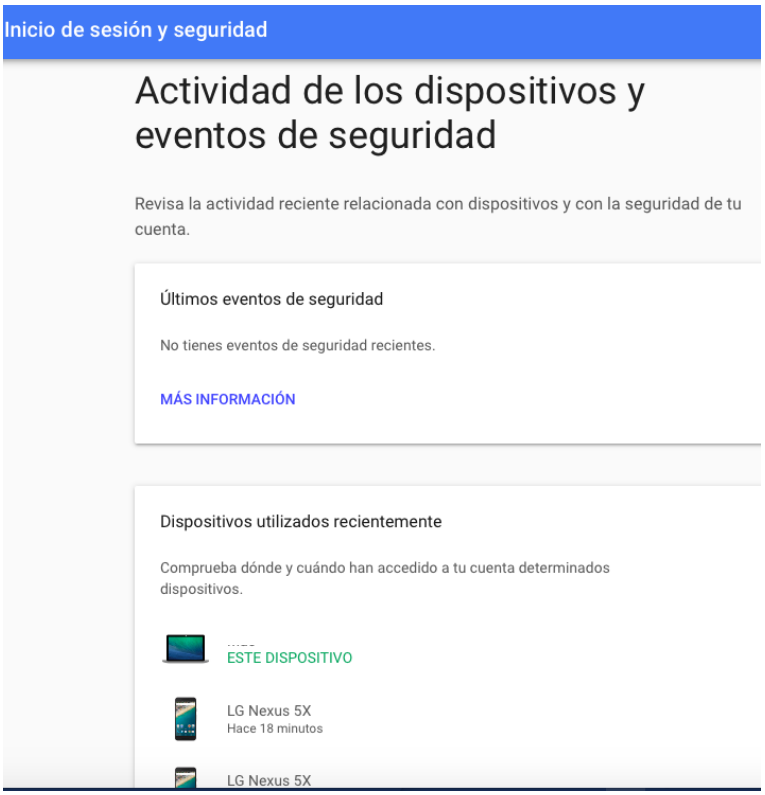
226. Google analiza la actividad relativa a una cuenta de usuario y envía notificaciones de seguridad cuando detecta un uso anormal.

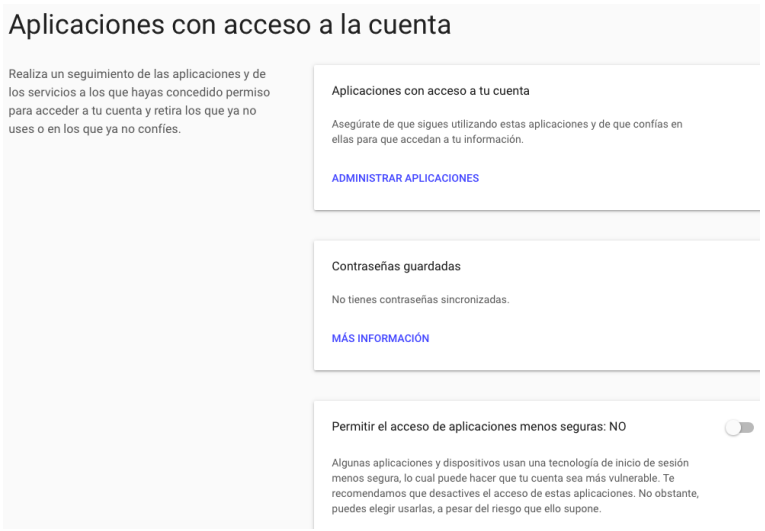
227. Estas notificaciones pueden ser de distinta naturaleza, pues dependen de la información que el propio usuario haya proporcionado en su cuenta. Por ejemplo, puede enviar un correo electrónico, un SMS o ambos con los detalles de la actividad sospechosa.

228. Entre estas notificaciones, se encuentra la relativa al acceso a la cuenta desde un dispositivo o aplicación que no se haya empleado previamente.

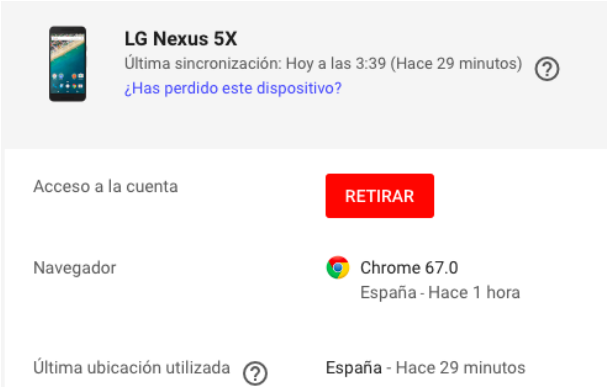
229. Se recomienda prestar especial atención a estas notificaciones y comprobar la información que proporcionan. Es importante, en primer lugar, verificar que la notificación se ha recibido directamente y de manera legítima de Google, y que no se trata de un ataque de phishing aprovechando este tipo de notificaciones.

230. Por ejemplo, en el caso de un aviso relativo al acceso desde un dispositivo nuevo, se puede recurrir al menú "Inicio de sesión y seguridad - Actividad de los dispositivos y eventos de seguridad":





231. En caso de detectarse cualquier tipo de acceso no realizado por el propio usuario, se deberá proceder al cambio inmediato de la contraseña de acceso como primera medida, y a retirar el acceso a la cuenta desde dicho dispositivo mediante el menú "Revisar los dispositivos - <seleccionar el dispositivo no reconocido> RETIRAR":



232. Se procederá de forma similar con las aplicaciones asociadas a una actividad no reconocida como propia por parte del usuario.

9.2. SERVICIO DE "ALERTA DE CONTRASEÑA" PARA CHROME

233. El servicio de "Alerta de contraseña" ("Password Alert") [Ref.- 274] es una extensión para el navegador web Chrome cuyo objeto es advertir al usuario sobre el uso de la contraseña de la cuenta de usuario de Google en sitios web no pertenecientes a Google, a fin de evitar ataques de *phishing.*

234. Para ello, cuando está activo, el servicio muestra una alerta si se introduce la contraseña de la cuenta de usuario de Google en cualquier página web diferente a la página web de autentificación de Google ("Google Sign in") disponible en "https://accounts.google.com".

235. Para habilitar el servicio, es preciso iniciar sesión en el navegador web Chrome con la cuenta de usuario de Google y descargar la extensión "Password Alert" de la tienda Chrome[6], siguiendo las instrucciones que aparecerán en pantalla.

236. El servicio "Alerta de contraseña" no almacena la contraseña de la cuenta de usuario de Google, sino un *thumbnail* (una versión reducida de un hash de la contraseña calculado con una semilla). Cuando el usuario accede a su cuenta de usuario de Google y proporciona su contraseña correcta, es decir Chrome accede de forma exitosa a la cuenta de usuario de Google, la extensión dispone de acceso temporal a la contraseña y calcula y guarda el *thumbnail* en el almacenamiento local de Chrome. Cada vez que el usuario se autentifica en cualquier otro sitio web, se calcula un nuevo *thumbnail* para la contraseña utilizada y se compara con el almacenado.

237. En entornos corporativos "G Suite", los administradores pueden hacer uso del servidor "Password Alert Server" para auditar los accesos de los usuarios mediante la contraseña de la cuenta de usuario de Google, enviar alertas por correo electrónico e incluso forzar a los usuarios a cambiar su contraseña si se detecta su uso en un sitio web que no sea de confianza.

238. Para obtener más información sobre el uso de este servicio en entornos corporativos, se recomienda consultar la referencia [Ref.- 34].

[6] https://chrome.google.com/webstore/detail/password-alert/noondiphcddnnabmjcihcjfbhfklnnep

9.3. NAVEGACIÓN PRIVADA

239. En términos generales, desde el punto de vista de seguridad se desaconseja el acceso a la cuenta de usuario de Google desde un dispositivo no propio.

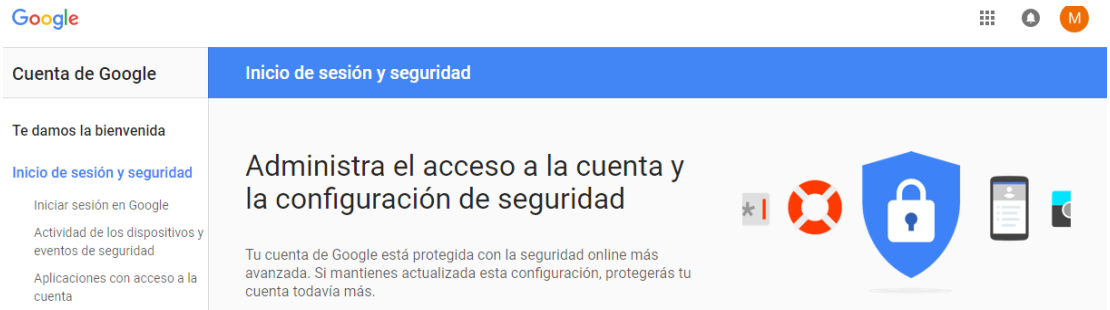
240. En caso de requerirse acceso web temporal a la cuenta de usuario de Google a través de un navegador web desde un dispositivo ajeno, se recomienda hacer uso de la denominada "Navegación privada" a través del modo "incógnito" de Chrome. Para ello:

- Desde el navegador Chrome, seleccionar la opción "Nueva ventana Incognito", que abrirá una nueva instancia de Chrome independiente de la que está en ejecución actualmente (en caso de existir alguna).
- Acceder al servicio de Google deseado e iniciar sesión con la cuenta de usuario.
- Una vez finalizado el acceso, acceder a la imagen asociada al perfil o la dirección de correo electrónico y seleccionar "Desconectar".
- Cerrar la ventana "incognito".

241. Cuando se usa un navegador web en modo incógnito (o privado) teóricamente no se almacena ningún tipo de actividad en el histórico, pero sí se aplicarán los controles de actividad de la cuenta que estén vigentes (ver apartado "6.2.1.2. Datos y personalización"), registrándose en la cuenta de usuario de Google los que se hayan definido.

9.4. INICIO DE SESIÓN Y SEGURIDAD

242. En el año 2017 Google añadió al interfaz de administración web de la cuenta de usuario de Google el apartado "Inicio de sesión y seguridad - Actividad de los dispositivos y eventos de seguridad", desde el que se pueden configurar todos los parámetros para proteger la cuenta de usuario de Google:



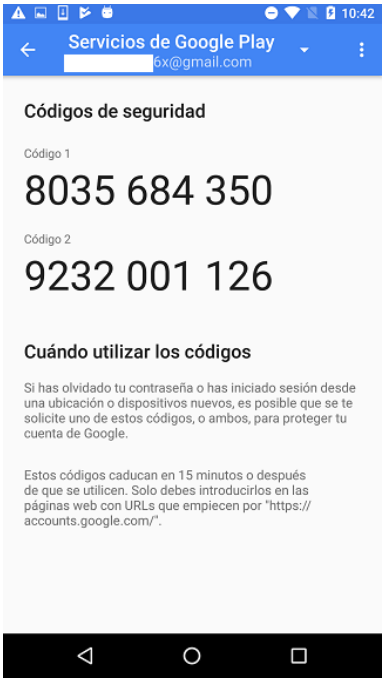
243. Además de la revisión de los últimos eventos de seguridad (descritos en el apartado "9.1. Notificaciones de seguridad", y que se recomienda consultar frecuentemente), este menú permite configurar los mecanismos de inicio de sesión en la cuenta de usuario de Google así como los dispositivos y las aplicaciones con acceso a la cuenta.

244. El equivalente en el interfaz de administración de Android es "Seguridad".

9.4.1. MECANISMOS PARA EL INICIO DE SESIÓN

245. Por defecto, el acceso a la cuenta de usuario de Google nada más crearse se lleva a cabo a través de un proceso de autenticación basado únicamente en usuario/contraseña (credenciales tradicionales).

246. El olvido de la contraseña, o la sospecha por parte de Google de que la misma puede estar siendo utilizada por un tercero no autorizado (por ejemplo, cuando se accede desde un dispositivo nuevo), puede llevar a que se solicite al usuario un código de verificación. Este código, denominado "de seguridad", se puede obtener a través de "Ajustes - [Personal] Google - [Cuenta de Google] - Cuenta de Google - [Seguridad] - Código de seguridad". Si el dispositivo móvil tiene configurado un método o código de acceso, se solicitará al usuario su introducción previa:



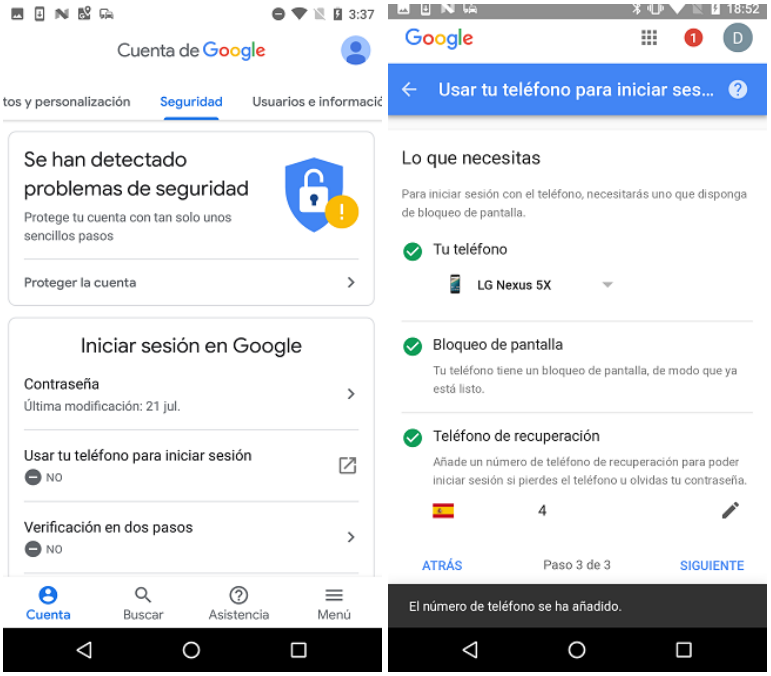
247. La pantalla mostrará dos códigos, que tienen 15 minutos de validez y varían con cada invocación de esta opción.

248. A fecha de elaboración de la presente guía, se ofrecen tres mecanismos para iniciar sesión en la cuenta del usuario de Google.

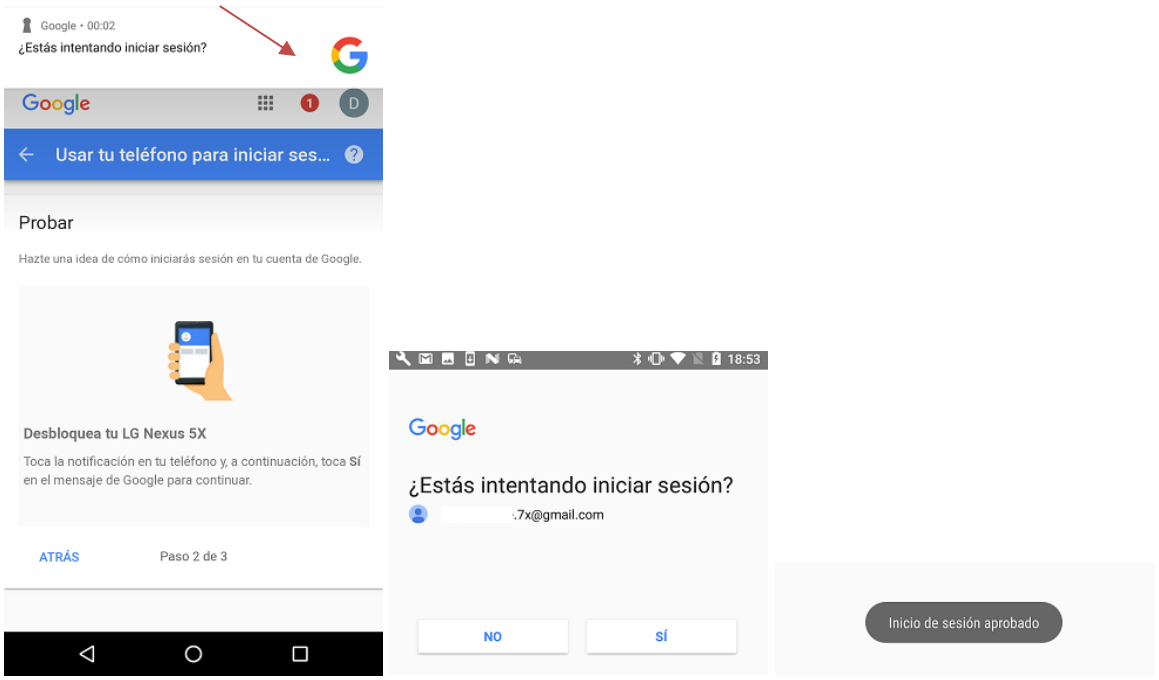
249. **Contraseña**: constituye el método de acceso tradicional y se puede consultar cuando se realizó la última modificación de la misma, así como cambiarla por otra diferente. Se recomienda actualizar la contraseña de la cuenta de usuario de Google periódicamente (según su robustez), especialmente si se utiliza para acceder a otros servicios.

250. **Usar tu teléfono para iniciar sesión**: para incrementar la protección de la cuenta de usuario, Google introdujo en el año 2016 la posibilidad de iniciar sesión en la cuenta de Google del usuario utilizando su dispositivo móvil, en lugar de la contraseña asociada a la cuenta de usuario. Esta opción permite para el acceso a la cuenta del usuario la confirmación de un mensaje que Google enviará al dispositivo móvil principal en el que está registrada dicha cuenta, a través de la conexión de datos, cuando se requiera autentificación en la cuenta. Por defecto, esta opción está desactivada.

251. Para su utilización se requiere que el bloqueo de pantalla esté activo, y que se haya vinculado un número de teléfono de recuperación a la cuenta de usuario de Google, como muestra la imagen inferior derecha:

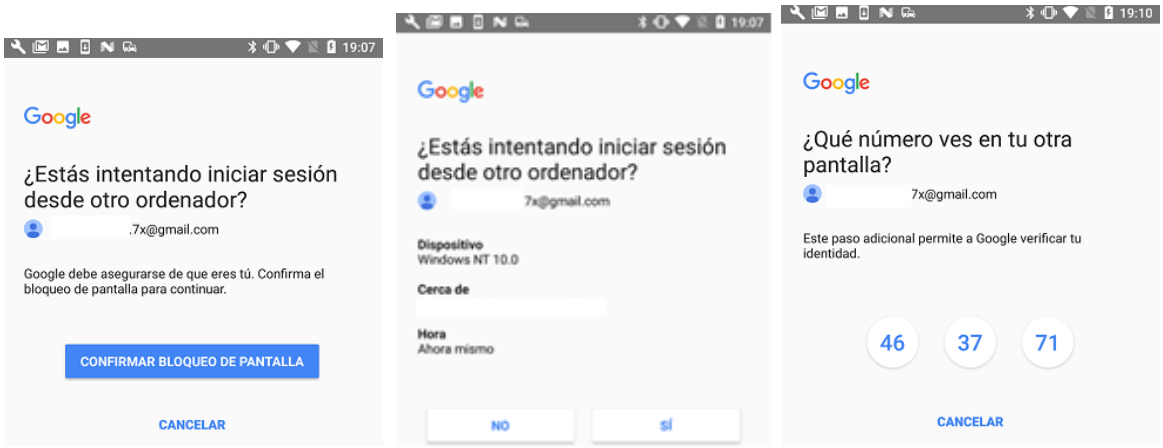


252. Al seleccionar esta opción, se mostrará la información sobre los requisitos asociados; pulsando en "Siguiente", se mostrará una notificación en el dispositivo móvil solicitando confirmación sobre el intento de inicio de sesión, que, al desplegarse, permite confirmar o denegar la operación. Si se pulsa en "Sí", aparecerá el mensaje (Toast) "Inicio de sesión aprobado" en la pantalla activa:

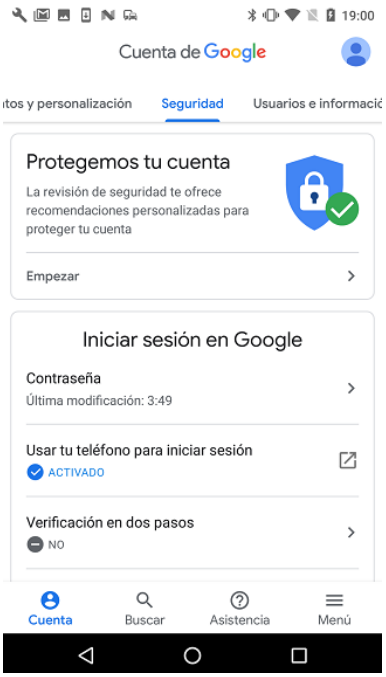


253. Un inconveniente que se ha observado (a fecha de elaboración del presente apartado) es que, a pesar de que se presenta una pantalla para introducir la contraseña de la cuenta de usuario de Google antes de proceder a la inclusión de este método de inicio de sesión, en realidad no es preciso escribirla.

254. Sin embargo, en la actualidad, una vez activo este tipo de acceso, si se intenta entrar en la cuenta desde otro equipo, se solicitará completar varios pasos en el dispositivo móvil: confirmar el bloqueo de pantalla (código de acceso) en el dispositivo móvil, confirmar el intento de inicio de sesión desde otro equipo, y elegir de entre tres valores numéricos el código que se está mostrando en el otro equipo. Estas comprobaciones adicionales no se proporcionaban anteriormente, y suponen una mejora en el mecanismo de protección de la cuenta.



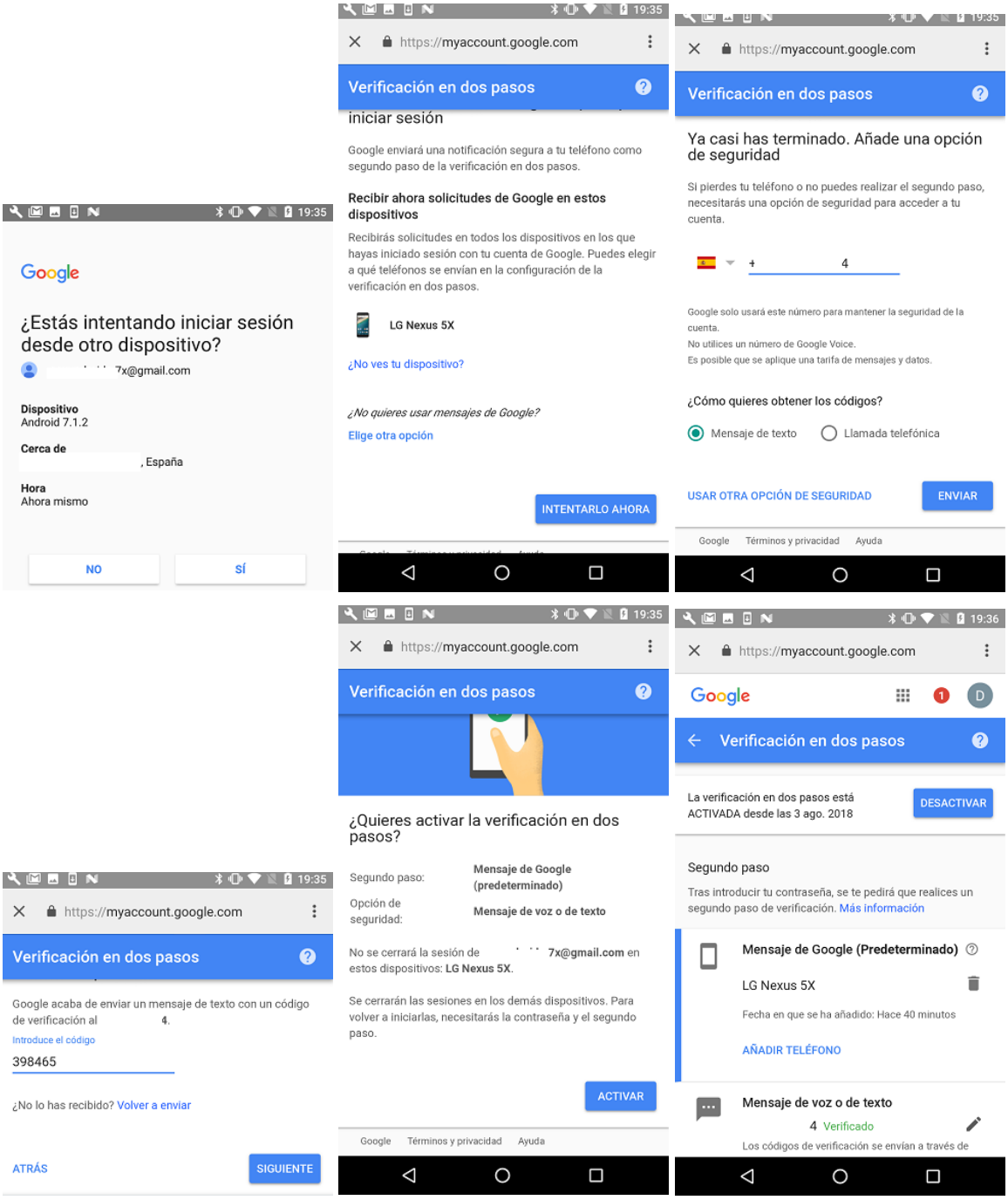
255. Una vez añadido el dispositivo móvil a la cuenta de usuario de Google para el inicio de sesión, la sección correspondiente del apartado "Seguridad" informará de ello mediante la sección "Usar tu teléfono para iniciar sesión":



256. **Verificación en dos pasos**: corresponde al uso de un segundo factor de autentificación [Ref.- 15] [Ref.- 20], y minimiza el riesgo que supone que la cuenta de Google del usuario pueda ser utilizada por un tercero.

257. Para poder hacer uso de este servicio, el dispositivo móvil que se vaya a configurar como el segundo factor tiene que estar registrado en la cuenta de Google del usuario, y, además, tener una versión actualizada de los servicios de Google Play (o *Google Play Services*, GPS).

258. Al iniciarse la configuración de este método se solicitará el código de acceso o desbloqueo definido en el dispositivo móvil (si está activo) y se mostrará una notificación solicitando confirmación sobre el intento de inicio de sesión. Una vez se muestre el mensaje de "Inicio de sesión aprobado", deberá introducirse un código (que se recibirá por SMS o a través de llamada telefónica):



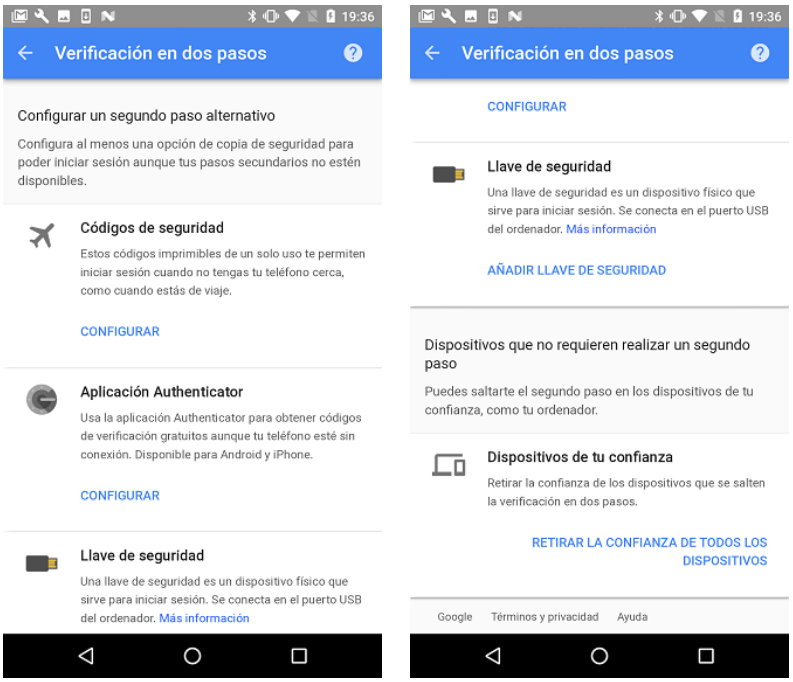
259. La verificación en dos pasos exigía en el pasado disponer de un código de acceso establecido (o método de bloqueo de pantalla) en el dispositivo móvil para poder llevar a cabo la configuración del segundo factor de autentificación; sin embargo, a fecha de elaboración de la presente guía, Google lo plantea como recomendación, pero es posible activar el mecanismo sin que exista un código de acceso definido en el dispositivo móvil.

260. Durante la activación de la verificación en dos pasos, si en algún momento futuro no se desea o se puede hacer uso de un SMS o una llamada de teléfono (por ejemplo, si

no se dispone de acceso al dispositivo móvil en el momento de utilización del servicio), se puede seleccionar "Usar otra opción de seguridad", que define como segundo factor una lista de diez códigos de verificación. El usuario podrá emplear estos códigos si en algún momento debe iniciar sesión en su cuenta de usuario de Google y no dispone de servicios de telefonía o incluso de acceso físico al dispositivo móvil:

261. Tras pulsar en "Siguiente", se solicitará la confirmación de activación del servicio.

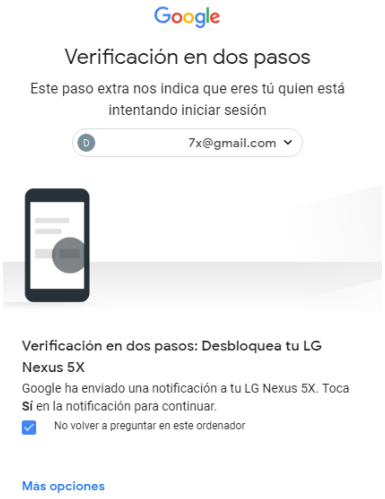
262. La verificación en dos pasos permite varios métodos alternativos:



- Códigos generados por la aplicación Google Authenticator (descrita en el apartado "12.1. Google Authenticator"), que permite generar los códigos de seguridad en el dispositivo móvil de manera *offline*, aunque no se disponga de conexión a Internet, en base a una semilla y a referencias de tiempo.
- El uso de una "llave de seguridad" compatible con el estándar abierto "FIDO Universal 2nd Factor (U2F)" [Ref.- 261]. La llave de seguridad es un pequeño dispositivo hardware que se puede conectar a un ordenador a través de USB o

al dispositivo móvil a través de Bluetooth Low Energy (BLE), en ambos casos se requiere disponer de una versión actualizada del navegador Chrome (al menos versión 38 o superior), y que almacena y/o genera los códigos de seguridad de manera segura, por lo que el usuario no se debe preocupar de introducirlos. Este mecanismo queda fuera del alcance de la presente guía.

263. A partir del momento en el que se ha completado el proceso de verificación en dos pasos, cada vez que se intente abrir sesión en la cuenta de usuario de Google en un dispositivo que no sea el propio móvil, se mostrará la siguiente pantalla:



264. Se aconseja desmarcar la opción "No volver a preguntar en este ordenador", que no aplicaría el segundo factor para solicitudes de conexión futuras procedentes de este mismo equipo.

265. Si los servidores de Google no pueden establecer comunicación con el dispositivo móvil en ese momento, intentarán completar la verificación utilizando el método de verificación alternativo previamente configurado.

266. Desde el punto de vista de seguridad, el introducir un segundo paso de verificación, o segundo factor de autentificación, para acceder a la cuenta de usuario de Google es altamente recomendable.

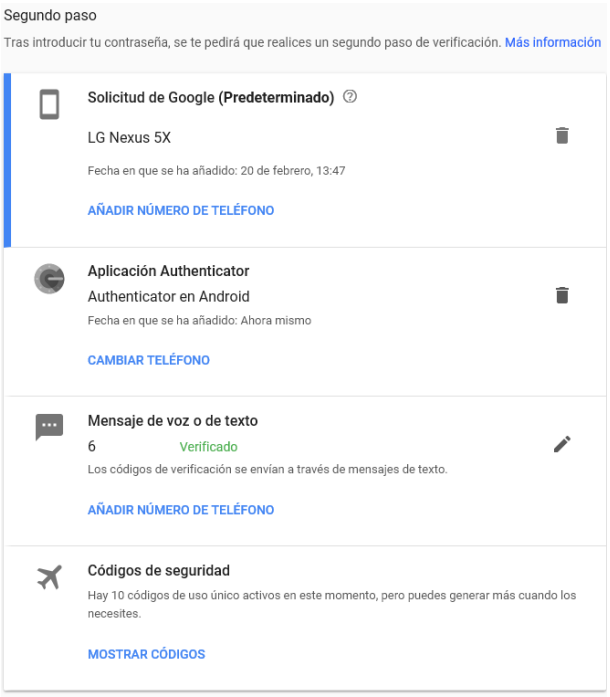
267. Sin embargo, al no requerirse por parte de Google que el dispositivo móvil tenga definido un código de acceso ni que la pantalla esté bloqueada cuando se envía la solicitud de verificación, se debe ser muy cuidadoso y asegurarse de que se dispone de un método de bloqueo en el dispositivo móvil, para minimizar el riesgo que supondría que el dispositivo móvil pudiera ser utilizado por un tercero sin autorización y hacer uso de las notificaciones empleando el dispositivo móvil como segundo factor de autentificación.

268. También se recomienda el uso de la app Google Authenticator, siempre teniendo definido un código de acceso en el dispositivo móvil en el que se vaya a emplear esta app, y que impida que un tercero no autorizado pueda utilizarla. Asimismo, se recomienda evitar que, en el momento de su utilización, un tercero disponga de acceso visual a la pantalla de la app que le permita ver los códigos generados por ésta.

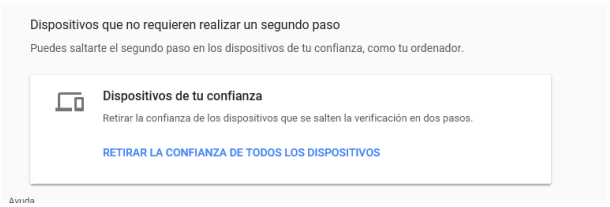
269. La alternativa más segura corresponde a las llaves de seguridad (previamente mencionadas) que, al tener asociada una clave privada criptográfica almacenada en

un dispositivo hardware específico de seguridad, con la que se cifran y/o generan los códigos de seguridad, y no requerir el envío de códigos que se puedan interceptar, protege potencialmente contra este tipo de ataques.

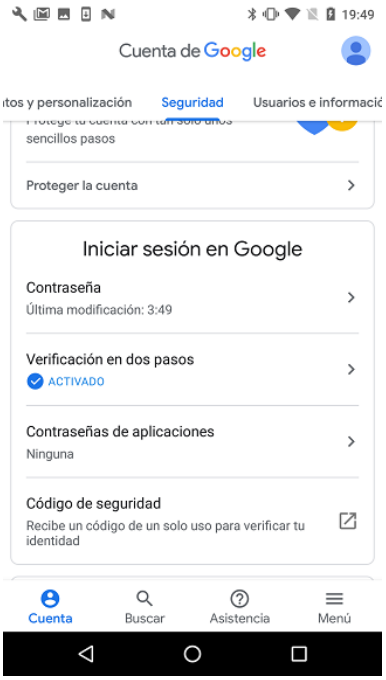
270. Cuando el método asociado a un segundo factor de autentificación está activo, el menú mostrará todas las opciones habilitadas:



271. El menú de "Verificación en dos pasos" también muestra la lista de dispositivos que el usuario ha designado como "Dispositivos de tu confianza", que son aquellos para los que el acceso a la cuenta de Google del usuario no requerirá la introducción del código asociado al segundo factor de autentificación:



272. Desde el punto de vista de seguridad, y aunque resulte menos cómodo tener que realizar dos pasos para completar el proceso de autentificación, se desaconseja disponer de servicios y cuentas de usuario en los que no se requiera el segundo factor, ante el riesgo que supondría que uno de ellos fuese utilizado por un tercero no autorizado.



10. SERVICIOS DE GOOGLE PLAY

273. En los últimos años Google ha adoptado un modelo de actualizaciones diferente y desconocido en muchas ocasiones, complementario y previo a las actualizaciones mensuales del nivel de parche de seguridad disponibles desde agosto de 2015, y de aplicación no sólo para los dispositivos móviles Nexus y/o Pixel, sino para un gran número de dispositivos Android.

274. A través de Google Play, y de sus servicios asociados, en concreto los Servicios de Google Play (GPS, *Google Play Services*), la plataforma móvil Android recibe numerosas actualizaciones que no sólo afectan a Google Play y al mercado de apps, sino también a otros componentes (o apps) críticas del sistema operativo y existentes por defecto [Ref.- 60].

275. Por tanto, el concepto de actualización en Android ha cambiado. Muchos componentes de la arquitectura de Android se han independizado del núcleo de la plataforma móvil, pudiendo ser actualizados independientemente y con mayor frecuencia. En lugar de tener que actualizar el sistema operativo a una nueva versión para poder disponer de funcionalidades o mecanismos de seguridad previamente ausentes, la actualización individual de la app Servicios de Google Play[7] [Ref.- 151] puede proporcionar nuevas actualizaciones para ciertos elementos de la plataforma móvil Android.

276. Otro ejemplo de esta independencia entre los componentes de la plataforma móvil y la versión concreta de Android es la propia aplicación "Google", que controla todos los ajustes relativos a los servicios de Google, incluyendo el asistente personal (Google Assistant) y los servicios conocidos como "*feed*".

277. Adicionalmente, es posible disponer de actualizaciones parciales para múltiples apps a través de la app de Google Play (denominada "Play Store"; el mercado oficial de apps de Android se llama actualmente Google Play, pero la app para acceder a éste

[7] https://play.google.com/store/apps/details?id=com.google.android.gms&hl=es

desde el dispositivo móvil sigue manteniendo el nombre antiguo del mercado oficial, "Play Store"), como por ejemplo, los teclados del sistema, el navegador web (Chrome), la app de correo electrónico (Gmail) y de mensajería (Hangouts) o la app de calendario pueden ser actualizadas independientemente como cualquier otra app de terceros.

278. La app asociada a Google Play se actualiza de forma automática sin intervención del usuario ni posibilidad sencilla de controlar o detener dichas actualizaciones.

279. La app de los ajustes de configuración (Google Settings o "Ajustes de Google"), que existía de forma independiente con la versión 6.0 de Android instalada por defecto, se integra como parte de la app de Google al actualizar dicha app a una versión reciente (lo cual también se lleva a cabo a través de la app "Play Store"). Además, buena parte de esos ajustes se puede controlar desde el menú general de Ajustes, y concretamente, desde el apartado "[Personal] Google".

280. Las actualizaciones parciales proporcionadas por los Servicios de Google Play son distribuidas incluso para dispositivos móviles que disponen de versiones antiguas de Android (desde Android 2.3, "Gingerbread") y para las que no se dispone de nuevas actualizaciones o versiones de sistema operativo.

281. Originalmente, las capacidades de *Google Play Services* versión 1.0, disponible desde septiembre de 2012, eran muy limitadas, añadiendo soporte para OAuth 2.0 y algunas APIs de Google+. A lo largo de los años, éstas se han extendido notablemente.

282. Una de las capacidades y/o ajustes de configuración existentes en Android que se actualizaban anteriormente vía Play Store pero que se eliminaron como componente autónomo del dispositivo son las asociadas al administrador de dispositivos de Android, responsable de la gestión remota del terminal (existente desde Android 2.2, e instalado por defecto desde Android 4.4). Este administrador ha pasado a integrarse como parte de los servicios asociados a la cuenta de Google del usuario y a independizarse del dispositivo físico o sistema operativo (ver apartado "10.4. Gestión remota de dispositivos Android por parte del usuario").

283. A través de Google Play se controlan asimismo las capacidades de escaneo o verificación de apps (ver apartado "10.2. Verificación de seguridad de las apps: Google Play Protect").

284. Una de las vulnerabilidades que fue resuelta a través de las capacidades de actualización de los Servicios de Google Play es la asociada (originalmente) a la versión 4.4.4 de Android, y específicamente a la vulnerabilidad de OpenSSL que permitía la realización de ataques MitM (Man-in-the-Middle), con CVE-2014-0224 y conocida como la vulnerabilidad de "inyección CCS (ChangeCipherSpec)" [Ref.- 139][Ref.- 140].

285. El proveedor de seguridad que proporciona las capacidades de comunicaciones de red seguras de Android fue actualizado con la versión 5.0 de los Servicios de Google Play (publicada en julio de 2014 [Ref.- 151]) para mitigar específicamente esta vulnerabilidad de "inyección CSS" [Ref.- 153].

286. Complementariamente, se recomienda que las apps hagan uso de los métodos y APIs asociados a los Servicios de Google Play, por un lado, para confirmar que se dispone de la última versión del proveedor de seguridad, y por otro, para asegurarse

de que ejecutan en un dispositivo móvil que hace uso de dicho proveedor de seguridad, que éste está actualizado, y que mitiga ataques basados en vulnerabilidades y *exploits* conocidos.

10.1. GOOGLE PLAY STORE

287. Google Play Store, o simplemente "Play Store" (anteriormente denominado Android Market), es la plataforma empleada por Google para la distribución y venta de apps y software para la plataforma Android, es decir, constituye el mercado oficial de aplicaciones móviles (apps) de Google.

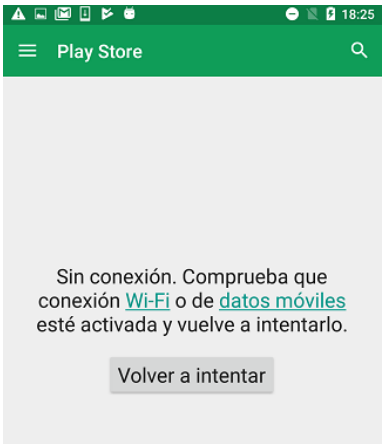
288. Para ello, Android incluye la app denominada "Play Store", disponible desde el *Launcher*, para el acceso a este servicio directamente desde el dispositivo móvil:

289. La versión de la app "Play Store" utilizada en la elaboración de la presente guía es la 11.0.50.

290. La primera vez que se utiliza la "Play Store", la app solicita al usuario disponer de una cuenta de usuario de Google (si no se ha configurado una todavía en el dispositivo móvil), y le permite darla de alta o crear una nueva (ver apartado "6. Cuenta de usuario de Google"), tras aceptar los términos y condiciones del servicio.

291. La conexión de autentificación empleando la cuenta de usuario de Google, y el acceso a Google Play, se realiza a través de HTTPS hacia los servidores "www.google.com", "android.clients.google.com", "*.googleusercontent.com", y hacia otros servicios complementarios de Google.

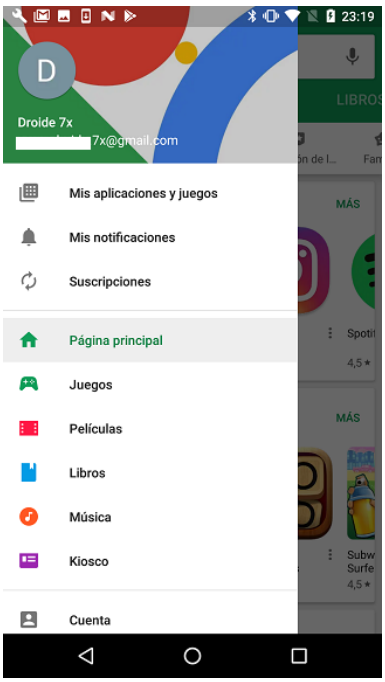
292. La app "Play Store" no puede ser ejecutada si no se dispone de conectividad de datos (autentificada y cifrada) hacia Google Play en Internet (Wi-Fi o 2/3/4G), mostrándose el siguiente mensaje: "*Comprueba tu conexión y vuelve a intentarlo. [Reintentar]*":



293. No obstante, es posible que este mensaje no se muestre si la app "Play Store" guardó en cache el resultado de su última invocación exitosa. En este caso, se verá una pantalla con los nombres de las apps pero sin los iconos.

294. Teóricamente, la integridad de las apps de Android se verifica a través de una firma digital asociada al fichero binario (.apk) descargado, pero una posible ausencia de cifrado en el tráfico empleado para descargar las apps (mediante HTTP), no así en el tráfico de acceso a Google Play que emplea HTTPS, abre potencialmente la puerta a la manipulación de este intercambio de datos, por ejemplo, mediante la sustitución de apps válidas firmadas digitalmente.

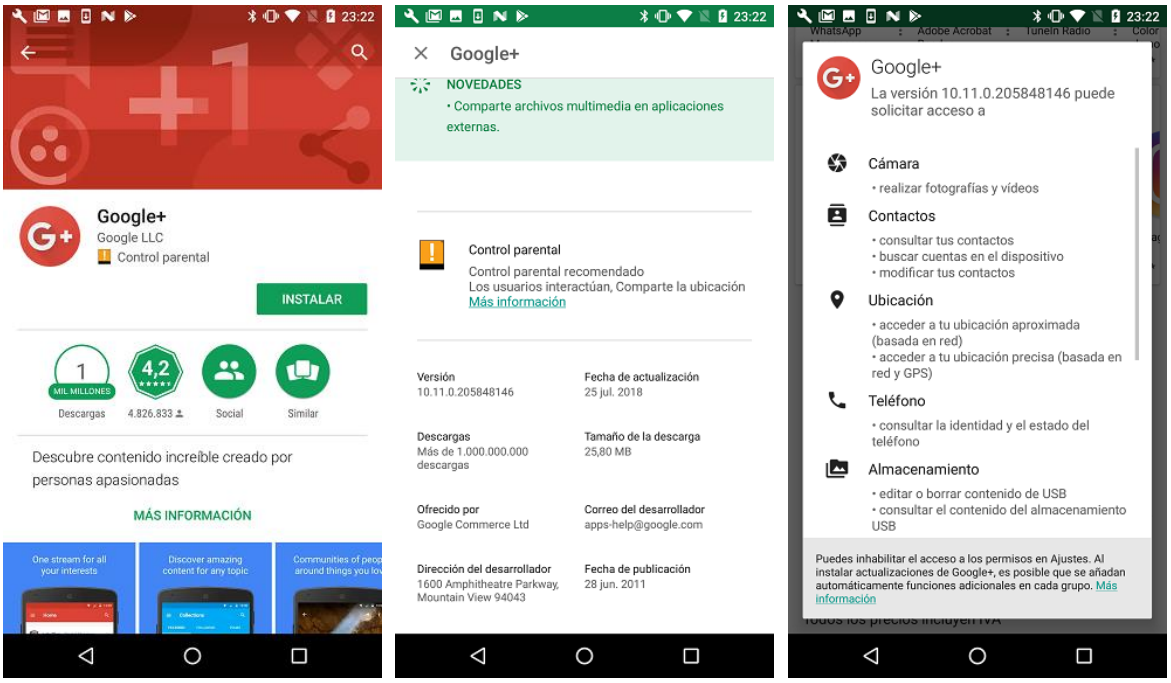
295. Se recomienda actualizar a la última versión de las apps ya instaladas en el dispositivo móvil, ya que éstas proporcionarán posibles soluciones frente a vulnerabilidades de seguridad públicamente conocidas.



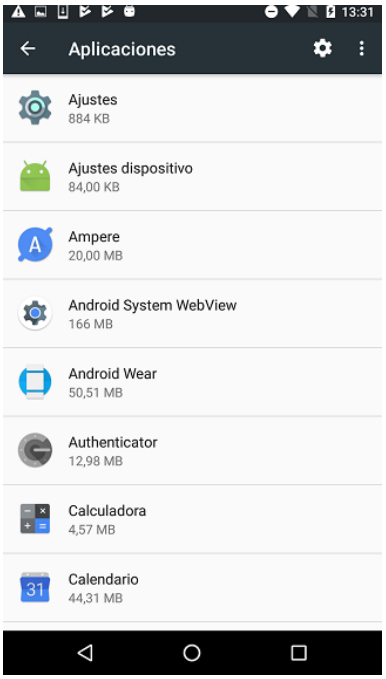
296. La lista de programas o apps instaladas desde Google Play es accesible desde la propia app "Play Store", mediante el icono del menú, "Mis aplicaciones y juegos" de Google Play, disponiéndose de tres pestañas para clasificar las apps: "Instaladas" (las instaladas en el dispositivo móvil), "Actualizaciones" (apps instaladas en el dispositivo móvil para las que existe alguna actualización) y "Colección" (apps instaladas en otro dispositivo, pero no en éste, con la cuenta de Google del usuario

y/o apps que estuvieron instaladas en el dispositivo móvil anteriormente pero que se eliminaron):

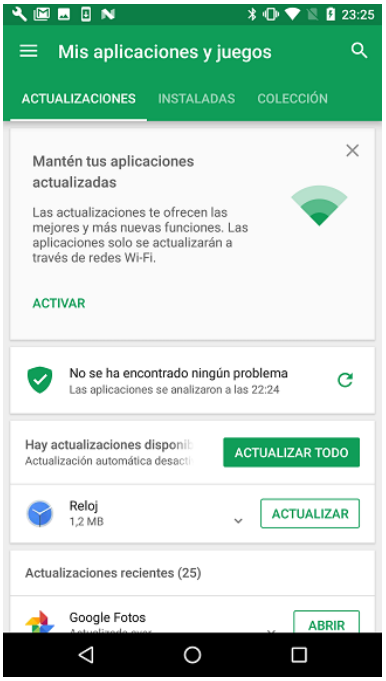
297. Desde la app "Play Store" es posible, una vez se ha seleccionado una app, ver todos sus detalles (al igual que desde la web de Google Play), como por ejemplo su descripción, las novedades, el número de descargas, las valoraciones y comentarios de otros usuarios (siendo posible emitir una valoración), las categorías o tipo de app, enlaces a apps similares, la clasificación de su contenido, la versión (o si existen múltiples versiones según el tipo de dispositivo móvil y la versión de Android) y fecha de la última actualización, el tamaño, la información de contacto del desarrollador, su política de privacidad, u obtener información sobre los permisos solicitados por la app, entre otros. Adicionalmente, es posible abrirla, actualizarla, e instalarla (si todavía no está disponible en el dispositivo móvil):



298. Adicionalmente, el listado de apps está disponible también desde el propio Android a través del menú "Ajustes [Dispositivo] - Aplicaciones".



299. Hasta Android 5.x, las aplicaciones se clasificaban en tres pestañas: "Descargadas", "En Ejecución", o "Todas", para clasificar las apps que han sido instaladas alguna vez en el dispositivo móvil, que están ejecutando actualmente, o todas las apps. Sin embargo, esta clasificación dejó de estar disponible en Android 6.x, pasando a listarse solo las instaladas y la información sobre las actualizaciones:



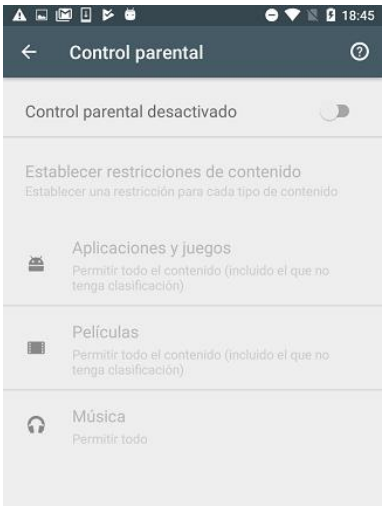
300. La pantalla de actualizaciones está disponible desde la propia app "Play Store", mediante el icono de menú, accediendo a la sección "Mis aplicaciones y juegos" y a la pestaña "Actualizaciones". En ella se mostrarán por un lado las actualizaciones pendientes (si las hay) y, debajo, las "Actualizaciones recientes".

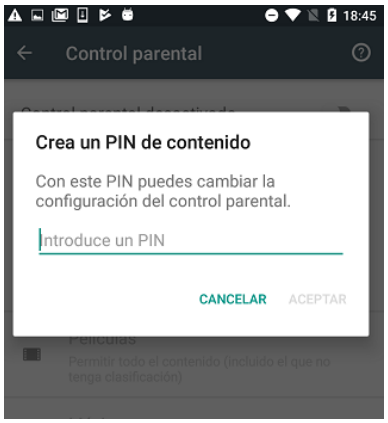
301. Desde esta pantalla el usuario puede actualizar manualmente cada una de las apps, o todas ellas simultáneamente (botón "Actualizar Todo").

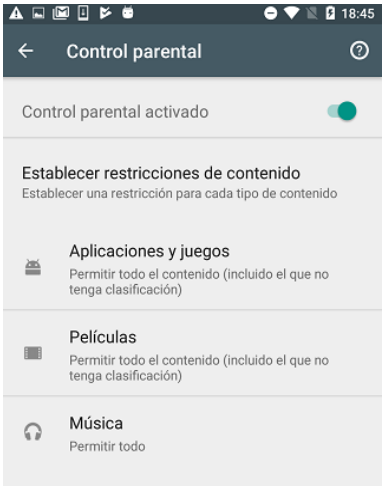
302. En la pestaña "Instaladas" de "Mis aplicaciones y juegos" se puede ver también qué aplicaciones tienen actualización disponible, que además tendrán a su derecha el botón "Actualizar".

303. Desde la misma se proporcionan detalles sobre las actualizaciones disponibles para las apps descargadas e instaladas en el dispositivo móvil, así como del resto de apps instaladas para las que no existe actualmente una actualización.

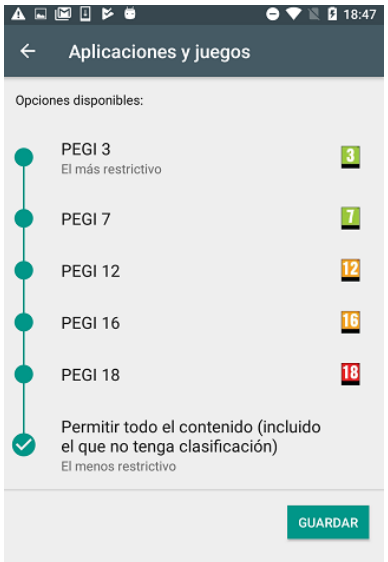
304. Adicionalmente, Android permite establecer restricciones de contenido desde la sección "Ajustes [Controles de Usuario] Control parental" de la app "Play Store", de forma que sólo se puedan instalar las aplicaciones que cumplan con el nivel de filtro establecido. El control parental requiere de la creación de un PIN para acceder a su configuración y así evitar cambios en los controles de usuario y filtros de contenido por parte de otros usuarios del dispositivo móvil (como por ejemplo menores de edad). Se recomienda que este PIN sea distinto del PIN de acceso al dispositivo si lo hubiere:





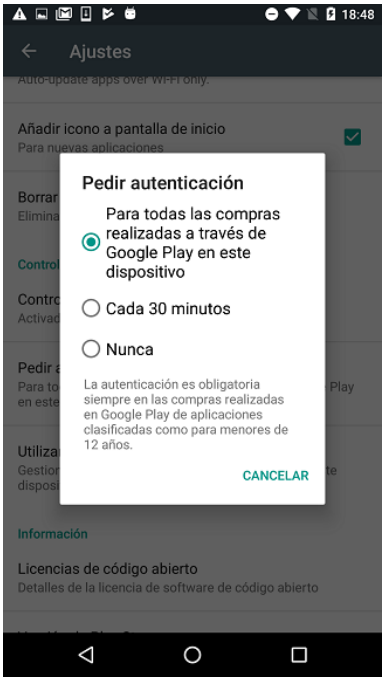


305. Las restricciones de contenido se pueden establecer según tres categorías: películas, música y aplicaciones y juegos. Por defecto, se encuentran activadas las opciones que no restringen contenido.



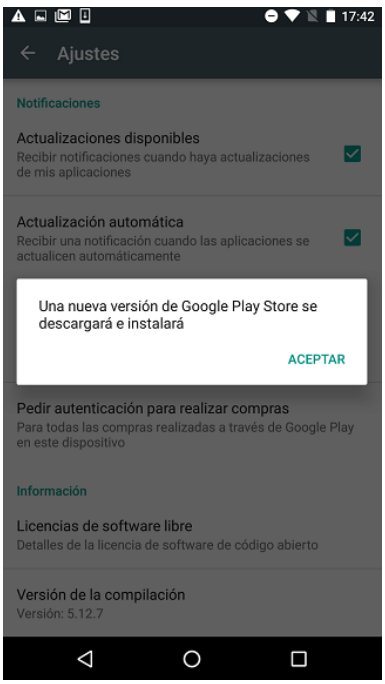
306. Todos los detalles sobre la clasificación y configuración del control parental se pueden consultar en [Ref.- 108].

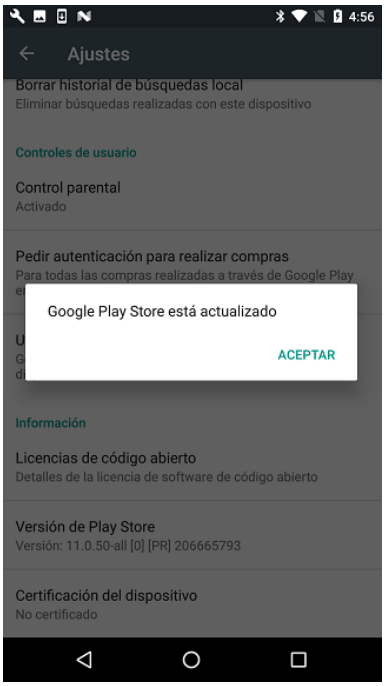
307. Asimismo, la opción "Pedir autenticación para realizar compras" (habilitada por defecto y opción recomendada desde el punto de vista de seguridad) permite establecer controles para que, a la hora de instalar una nueva app de pago desde Google Play, se solicite autorización al usuario, junto a sus credenciales:



308. Esta solicitud puede hacerse válida para los siguientes 30 minutos, con el objetivo de facilitar la realización de múltiples compras sin que sea necesario autentificarse para cada una de ellas, o nunca (opción desaconsejada).

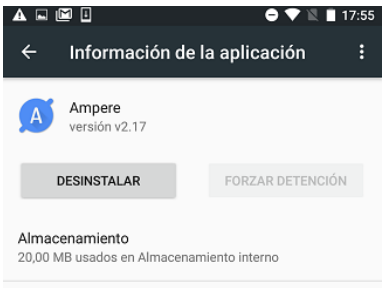
309. La app "Play Store" recibe actualizaciones silenciosas que se llevan a cabo automáticamente y sin aviso para el usuario. Se puede comprobar si hay alguna una actualización de la app "Play Store" disponible para el dispositivo entrando en los ajustes de la app "Play Store", "Ajustes - [Información] Versión de Play Store ". Al seleccionar ese campo, si hay actualizaciones disponibles, se mostrará un mensaje informativo "Una nueva versión de Google Play Store se descargará e instalará", pero ello no provoca que la descarga de la actualización se lleve a cabo inmediatamente. La única forma de forzar una actualización automática de la app "Play Store" (si se requiere una funcionalidad precisa no disponible en la versión actual) es llevar a cabo una actualización manual del fichero APK correspondiente a la app "Play Store" de un sitio web de confianza (no existe ningún sitio oficial desde el que se puedan descargar las versiones de la app "Play Store"). Cuando la versión está actualizada, se mostrará un mensaje informativo de ello.





310. La versión de la app "Play Store", al igual que de cualquier otra app instalada en Android, puede obtenerse tanto desde la propia app (menú "Ajustes [Información] - Versión de Play Store", como desde el menú "Ajustes [Dispositivo] - Aplicaciones", por ejemplo, desde la pestaña "Todas", seleccionando la app (en el ejemplo inferior, "Google Play Store") de la lista de todas las apps disponibles (por ejemplo, versión 11.0.50…).

311. La pantalla de información de una app permite tanto desinstalar la app (para aplicaciones de terceros), mediante el botón "Desinstalar", como desinstalar todas las actualizaciones disponibles (para aplicaciones nativas del sistema y disponibles por defecto en Android), mediante el botón "[…] Desinstalar actualizaciones". Las apps nativas no pueden ser desinstaladas completamente, sino que, al desinstalar actualizaciones, se devolverá la app a la versión que traía de fábrica.



312. Con el objetivo de disfrutar del mayor nivel de seguridad posible en el dispositivo móvil y de manera general, se recomienda disponer siempre de la última versión de todas las apps instaladas, independientemente del desarrollador. La última versión debería solucionar todas las vulnerabilidades de seguridad públicamente conocidas.

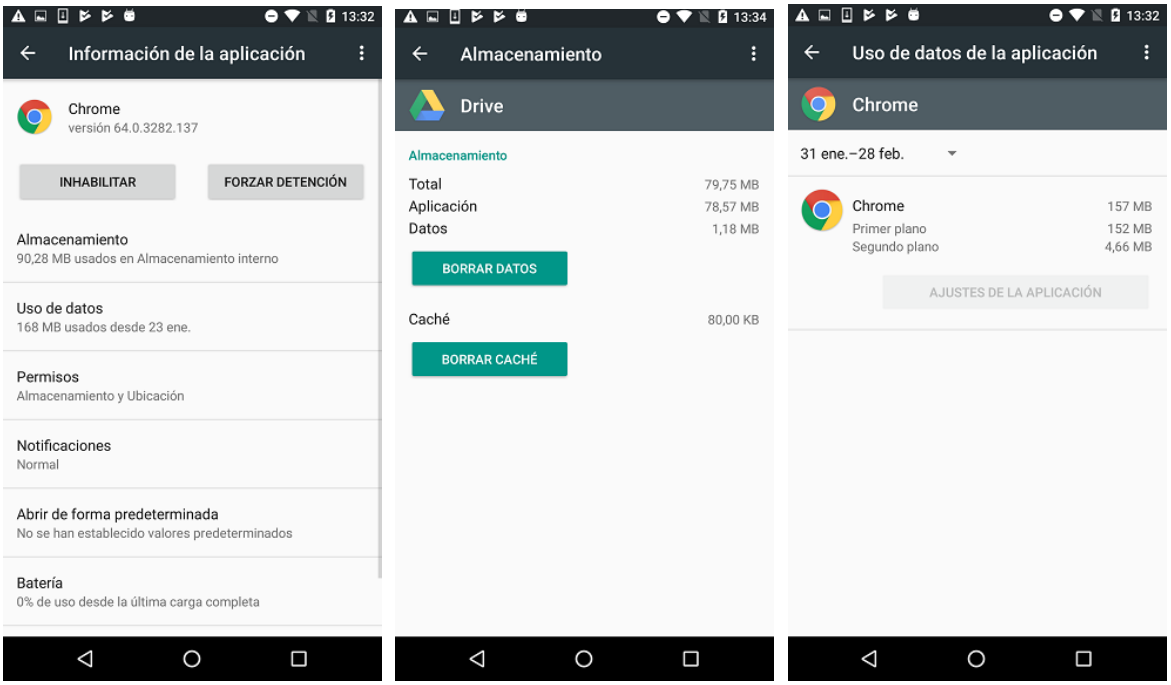
313. Las versiones recientes de la app "Play Store" incluyen un campo "Certificación del dispositivo" cuyo propósito es determinar si el dispositivo cumple los requisitos de compatibilidad de Android [Ref.- 272]. Las pruebas realizadas durante la elaboración de la presente guía ponen de manifiesto que un dispositivo móvil puede marcarse como "No certificado" si tiene desbloqueado el gestor de arranque (*bootloader*). A fecha de redacción de la presente guía, este estado no implica que no puedan

ejecutarse instalaciones o actualizaciones del sistema operativo o de apps desde Google Play, pese a que esta posibilidad se enumera entre las consecuencias posibles que pueden aplicar en el futuro a dispositivos móviles no certificados.

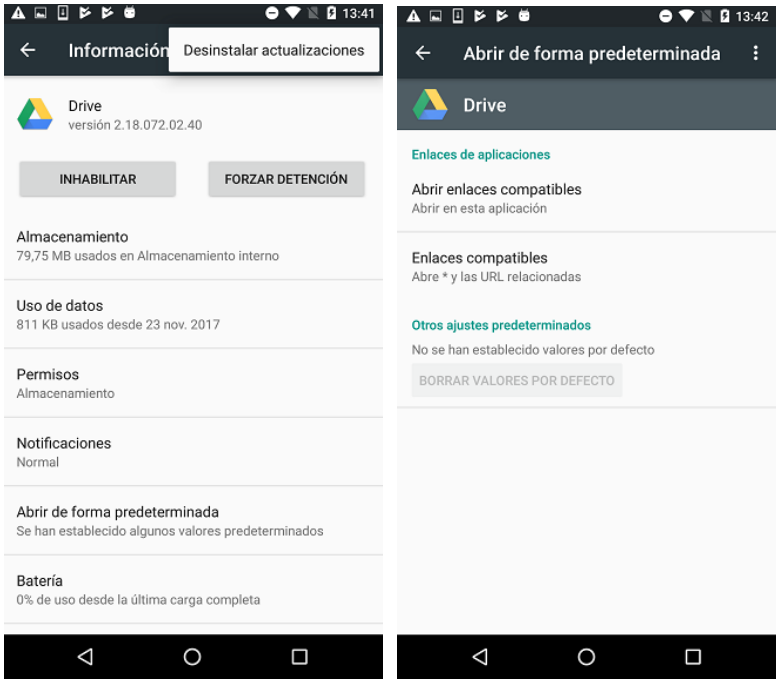
314. La información respecto a las actualizaciones de software y descargas disponibles para las apps de Android está disponible en Google Play y/o en la página web de su desarrollador.

315. La instalación de actualizaciones de software y apps en Android, si todas las apps se han obtenido a través de Google Play, tiene asociado un proceso homogéneo, facilitando el proceso de actualización para usuarios no experimentados y aumentando el nivel de seguridad de los dispositivos móviles, al agilizarse el proceso de sustitución de software vulnerable.

316. Desde el menú "Ajustes [Dispositivo] - Aplicaciones" es posible, una vez se ha seleccionado una app, acceder a sus detalles técnicos, como por ejemplo la versión, el tamaño que ocupa en el almacenamiento (total, y dividido por la app y por sus datos), el tamaño ocupado en caché, determinar si se mostrarán notificaciones generadas por la app, el uso de datos móviles en un período concreto, tanto en primer como en segundo plano, u obtener información sobre los permisos solicitados por la app, entre otros.



317. Mediante la selección de cualquier permiso es posible obtener una descripción general del mismo. Adicionalmente, es posible forzar la detención de la app si no responde, desinstalar actualizaciones (a través del menú "[…]" de la esquina superior derecha, lo cual permite la sustitución de la app por su versión de fábrica), inhabilitarla, borrar sus datos o su caché, y borrar los valores predeterminados, que indican para qué acciones se iniciará esta app:

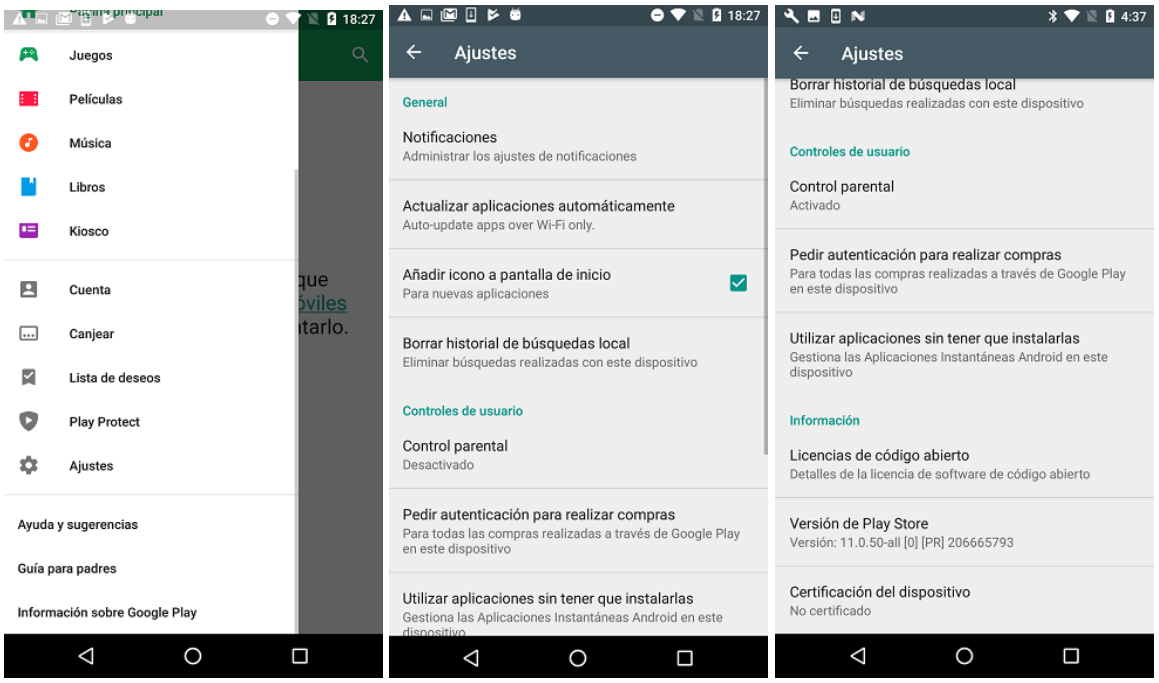


318. Debe tenerse en cuenta que la disponibilidad de una app en Google Play no asegura que la misma no sea maliciosa y pueda llevar a cabo acciones desde el dispositivo móvil en el que ha sido instalada que afecten a la seguridad y privacidad del usuario [Ref.- 400].

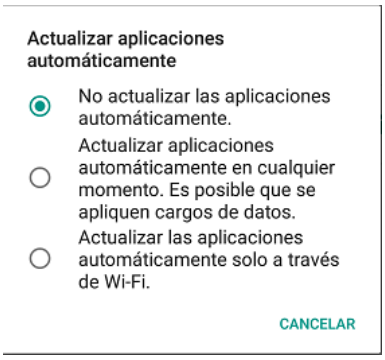
319. Se recomienda analizar en detalle el contenido y procedencia de una app de terceros antes de instalarla desde Google Play en el dispositivo móvil, por ejemplo, identificando a su desarrollador, el tiempo que lleva la app publicada en Google Play, su valoración y reputación por parte de otros usuarios, etc.

320. Una vez se ha configurado una cuenta de usuario de Google en el dispositivo móvil y ambos han sido vinculados (ver apartado "6. Cuenta de usuario de Google"), desde la sección de "Ajustes" de la aplicación web de Google Play ("https://play.google.com/store/account") también será posible gestionar las apps disponibles, como también lo será a través del "Administrador de dispositivos Android" (ver apartado "10.4. Gestión remota de dispositivos Android por parte del usuario"), el o los dispositivos móviles asociados a la cuenta del usuario.

321. Mediante el icono de menú formado por tres líneas horizontales es posible acceder a la sección de "Ajustes". En el apartado "General" es posible configurar como se desea que se produzca el proceso de actualización de las apps instaladas desde Google Play mediante la opción "Actualizar automáticamente". Se dispone de la opción de que no se actualicen las apps automáticamente, que se actualicen las apps automáticamente en cualquier momento, o sólo a través de redes Wi-Fi (opción por defecto):



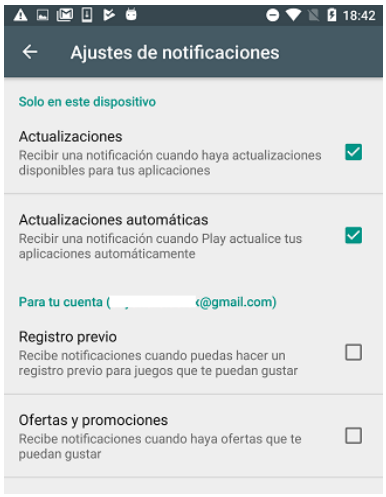
322. En caso de estar interesados en actualizar las apps tan pronto estén disponibles, tanto a través de redes Wi-Fi como de redes de datos móviles 2/3/4G, se recomienda activar la opción "Actualizar aplicaciones automáticamente en cualquier momento":



323. Por defecto, la barra de notificaciones de Android mostrará un aviso sobre la disponibilidad de actualizaciones para las apps, en caso de no haber seleccionado la opción de actualización automática, ya que en ese caso las actualizaciones podrían ser llevadas a cabo sin la intervención del usuario, en concreto, si éstas no solicitan nuevos (grupos de) permisos.

324. Mediante la selección de dicha notificación, el usuario puede identificar para qué apps se dispone de actualización y los detalles asociados.

325. La configuración de las notificaciones está disponible desde la app "Play Store", a través del icono de menú, de la sección de "Ajustes", y mediante la opción "Notificaciones". Las notificaciones se pueden configurar a nivel de dispositivo (para informar sobre las actualizaciones que se detecten o realicen sobre el terminal) y de cuenta de usuario de Google (para que, en base a las recomendaciones de Google resultantes del análisis que se hace del perfil de la cuenta de usuario, se envíen notificaciones sobre aplicaciones y promociones que puedan interesar al usuario). Estas últimas están desactivadas por defecto, y se recomienda mantenerlas así en aras de la privacidad.



326. En Android 7.x se utiliza "*certificate pinning*", a diferencia de lo que ocurría en Android 6.x. En este último, el acceso a Google Play (incluyendo el proceso de verificación de actualizaciones de las apps) se realizaba a través de una comunicación HTTPS cifrada, pero no se empleaban mecanismos de protección basados en certificate pinning, y, al igual que ocurría con otras aplicaciones de Google como Gmail, se aceptaba cualquier certificado digital de confianza que importado por el usuario al establecerse una conexión cifrada mediante TLS con los servidores de Google Play [Ref.- 80].

327. Este hecho permitía identificar fácilmente que la descarga de la actualización se realizaba desde el servidor "android.clients.google.com", mediante HTTPS. La respuesta redirige a la app "Play Store" hacia los servidores bajo el dominio "*.gvt1.com", también empleando HTTPS, para que ésta llevase a cabo una segunda petición solicitando el binario correspondiente a la app a actualizar.

328. El proceso de descarga e instalación de una nueva actualización en Android 6.x solicitaba el paquete o app a descargar y desvela numerosos detalles del dispositivo móvil y del software involucrado, como los números de versiones, identificadores, cookies, agente de usuario, incluso la cuenta de usuario de Google con la que se realizaba la petición:

```
Set-Cookie: PLAY_ACTIVE_ACCOUNT=ICrt_XL61NBE_S0rhk8RpG0j78e0XwQ23DlvB6kxiQ8=
<usuario>@gmail.com; Path=/; Secure
GET /play-apps-download-default/download/by-id/AF3DWBexsd0viV96e5U9-
SkM_V5zXTpNqxmJ1sSVllVjT4gYxn2GQhg_euHKyADbtejmDtpbuVsS4BSCkCIcQJ8G6QLXCrRnC
EjQchlu45EMGR2Eso66efY?cpn=1LAU9LZZZiqjfQq6&ctier=L&initcwndbps=7280&mm=31&m
n=sn-8vq54voxn25po-
h5q6&ms=au&mt=1520445713&mv=m&pl=24&expire=1520618655&ip=77.230.118.79&ipbit
s=0&sparams=expire,ipbits,ip,q:,initcwndbps,mm,mn,ms,mv,pl,ctier&signature=6
73EFC6625C2ECC91BEF6DED37A6E53FF4AEA15D.68C2FAE270BE0FD7D0ED455D1F25121DCA4C
D2BB&key=am3 HTTP/1.1
User-Agent: AndroidDownloadManager/6.0.1 (Linux; U; Android 6.0.1; Nexus 5X
Build/MTC20K)
Host: r2---sn-8vq54voxn25po-h5q6.gvt1.com
```

329. Además, durante el intercambio de las peticiones asociadas al proceso de actualización, también se desvelaba la versión de la app "Play Store" del dispositivo:

```
User-Agent: Android-Finsky/9.0.15-all%20%5B0%5D%20%5BPR%5D%20186388994
```

330. Desde Android 7.x, con la nueva característica conocida como "Network Security Configuration (NSC)", las apps de Android no confían en los certificados digitales importados por el usuario, no resultando tan sencillo analizar estas conexiones sin

modificar el fichero APK de la app objetivo (para más información, consultar el apartado "Certificate pinning y certificate blacklisting" de la "Guía CCN-STIC-453E - Seguridad de dispositivos móviles: Android 7.x" [Ref.- 407]).

10.1.1. ACTUALIZACIÓN AUTOMÁTICA DE APPS

331. Android proporciona capacidades para actualizar automáticamente las apps instaladas en el dispositivo móvil tan pronto se detecte que hay disponible una nueva versión de las mismas en Google Play.

332. Desde la app "Play Store", mediante el icono de menú es posible acceder a los "Ajustes" de Google Play. Desde la sección "General", es posible seleccionar la opción "Actualizar aplicaciones automáticamente".

333. Por defecto la funcionalidad de actualización automática de las apps en Google Play está habilitada sólo para llevarse a cabo mediante conexiones de datos a través de redes Wi-Fi. Adicionalmente, es posible definir si también es posible realizar las actualizaciones automáticas de las apps a través de la conexión de telefonía móvil (2/3/4G) del dispositivo móvil, ya que esta última puede tener costes asociados.

334. Finalmente, también es posible deshabilitar las actualizaciones automáticas de las apps por completo, siendo necesaria la intervención manual del usuario para completar la actualización de cualquier app. Se sugiere aplicar una configuración específica en base a las recomendaciones descritas posteriormente.

335. Para ello debe modificarse la opción "Actualizar las aplicaciones automáticamente solo a través de Wi-Fi" (opción habilitada por defecto) disponible en la app "Play Store", desde el icono de menú, accediendo a los "Ajustes" de Google Play y, en concreto, a la sección "General" (mostrada en las imágenes previas).

336. Aunque en versiones de Android anteriores a la 5 no existía la posibilidad de desactivar las actualizaciones automáticas para apps específicas (actualizaciones selectivas), desde Android 5 es posible seleccionar de manera individual qué aplicaciones se desea actualizar automáticamente [Ref.- 223]. Desde la app "Play Store", mediante el icono de menú es posible acceder a "Mis aplicaciones y juegos", seleccionar una app concreta de las ya instaladas, pinchar en los puntos representativos del icono de menú y habilitar o deshabilitar la opción "Actualizar autom.". El valor de esta opción por defecto es el que aplique de la política general de actualizaciones descrita previamente.

337. Si la funcionalidad de actualizaciones automáticas ha sido habilitada, las nuevas actualizaciones serán aplicadas sin la intervención del usuario si la actualización no modifica los permisos requeridos por la app o, más recientemente, incluso si la

actualización requiere disponer de nuevos permisos, pero estos están englobados en un grupo de permisos previamente aprobado por el usuario para dicha app.

338. Por tanto, pese a que para un usuario no avanzado sería recomendable dejar activadas las actualizaciones automáticas con el objetivo de disponer siempre de la última versión de cada app, que supuestamente solucionará las vulnerabilidades conocidas públicamente, debido al nuevo modelo de permisos simplificados de Android, es preferible llevar a cabo las actualizaciones de las apps manualmente.

339. Se recomienda por tanto no dejar habilitada la opción de actualizaciones automáticas, e independientemente del perfil del usuario del dispositivo móvil, forzar al usuario a revisar manualmente los nuevos permisos solicitados por cada una de las actualizaciones recibidas para todas y cada una de las diferentes apps instaladas en el terminal.

340. Especialmente, los usuarios avanzados deben estar interesados en no habilitar esta opción para poder revisar y analizar minuciosamente las actualizaciones disponibles, y sus "nuevos" permisos, antes de que éstas sean instaladas.

341. En caso de que los permisos de la app hayan cambiado con la actualización, el proceso de actualización manual mostrará los nuevos permisos requeridos por la nueva versión de la app que deberán ser aprobados por el usuario durante la instalación de la actualización de la app. Sin embargo, recientemente, si los nuevos permisos requeridos por la app están englobados en un grupo de permisos previamente aprobado por el usuario para dicha app, la actualización podrá ser instalada automáticamente sin la intervención del usuario.

10.1.2. INSTALACIÓN REMOTA DE APPS

342. En mayo de 2010 Google presentó la versión web de Google Play [Ref.- 4], que permite la consulta e instalación de apps en los dispositivos móviles Android desde otros ordenadores mediante un navegador web, en lugar de emplear la app de acceso al mercado oficial ("Play Store") desde los propios dispositivos móviles.

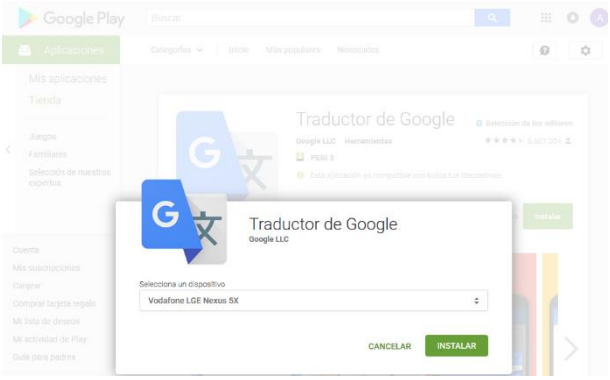
343. Una vez se adquiere una app a través de la versión web de Google Play desde el mercado oficial de apps, Google se encarga de instalarla en el dispositivo móvil a través de una conexión persistente disponible en los dispositivos móviles basados en Android a través de Internet (ver apartado "10.1.4. Conexión GTalkService").

344. La conexión permanente a través de Internet disponible entre los dispositivos móviles Android y Google se basa en el GTalkService [Ref.- 81]. Para la instalación remota de apps se emplea un mecanismo de envío de mensajes propio de Google y Android, y en concreto en este caso, el mensaje denominado INSTALL_ASSET [Ref.- 82].

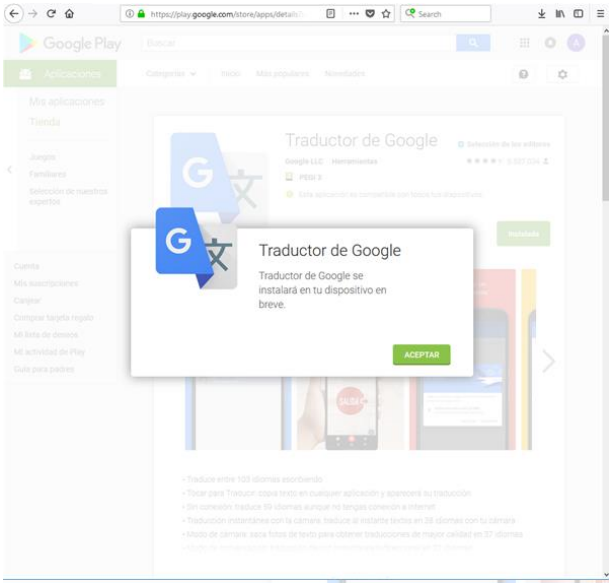
345. Antes de llevar a cabo la instalación de cualquier nueva app, se recomienda revisar y analizar exhaustivamente los permisos solicitados por la misma sobre el dispositivo móvil.

346. El acceso a Google Play se realiza mediante la cuenta de usuario de Google, por lo que el acceso no autorizado por parte de un atacante a dicha cuenta permitiría la instalación de apps en el dispositivo móvil asociado del usuario [Ref.- 8].

347. Tras seleccionar la app en la web de Google Play, el usuario puede seleccionar en cuál de los diferentes dispositivos móviles vinculados a la cuenta de usuario de Google se desea realizar su instalación:



348. Tras confirmar su instalación en el dispositivo móvil seleccionado, se obtiene la confirmación a través de la página web de Google Play, y en el dispositivo móvil el proceso de instalación se lleva a cabo automáticamente, conllevando únicamente un aviso en la barra de notificaciones del dispositivo (y la aparición del icono de la app en alguna de las pantallas de inicio y/o en el *Launcher*):



349. Es importante reseñar que, aunque la instalación no pueda llevarse a cabo en el preciso momento en que se solicita, tan pronto se pulse el botón "Aceptar" el interfaz de Google Play mostrará esa app como "Instalada". Esto ocurre incluso aunque en el momento de solicitarse la instalación el dispositivo móvil no tenga conexión a los servidores de Google. La petición queda encolada en la cuenta de Google del usuario y, tan pronto se restablezca la conexión con los servidores, se iniciará la descarga e instalación de la app.

350. En el pasado, la instalación remota de apps desde la web de Google Play de forma no autorizada podía suceder si un potencial atacante obtenía los identificadores de sesión empleados en el acceso web a Google Play del usuario [Ref.- 79]. Google resolvió el problema modificando la cookie "androidmarket" para que incluyese el flag *HttpOnly*, con lo cual el identificador de sesión solo es enviado por el navegador cuando hace una petición, por lo que no está disponible para ataques de XSS.

10.1.3. ELIMINACIÓN REMOTA DE APPS

351. Los dispositivos móviles basados en Android disponen también de capacidades por parte del vendedor, Google/Android, para eliminar apps de los mismos de forma remota.

352. Este mecanismo fue diseñado como medida de seguridad en situaciones de emergencia para poder proteger a los usuarios en caso de que se produzca una distribución masiva de apps dañinas o maliciosas concretas.

353. En junio de 2010 Google empleó estas capacidades por primera vez [Ref.- 5] [Ref.- 82] para eliminar una app creada como prueba de concepto que pretendía demostrar la facilidad para introducir apps maliciosas en los mercados de aplicaciones de varios fabricantes de dispositivos móviles, incluyendo Android Market (nombre empleado para Google Play en aquel momento).

354. Posteriormente, Google ha hecho uso de esta funcionalidad en (al menos) otra ocasión para eliminar otras apps maliciosas introducidas en Android Market. Por ejemplo, en marzo de 2011, se vieron afectadas unas 50 aplicaciones infectadas con malware bajo el nombre de DroidDream que fueron instaladas en más de 200.000 dispositivos móviles (cifras no oficiales). Estas apps hacían uso de vulnerabilidades conocidas en versiones de Android previas a la versión 2.2.2, y específicamente, técnicas empleadas habitualmente para conseguir acceso como root a dispositivos móviles Android (proceso conocido como *root*, *rooted* o *rooting* del dispositivo Android).

355. Esas capacidades permiten a Google no sólo eliminar las apps maliciosas de Google Play y suspender las cuentas de los desarrolladores sospechosos, sino también eliminar las apps de los dispositivos móviles de los usuarios donde han sido instaladas, notificando al usuario sobre las acciones realizadas. Tal y como se indica en [Ref.- 6], "*Nota: Si Google determina que la actualización de una aplicación permite solucionar una vulnerabilidad de seguridad crítica, es posible que actualicemos ciertas aplicaciones independientemente de la configuración de actualización establecida en la aplicación o en tu dispositivo. Para obtener más información, consulta las Condiciones de Servicio de Google Play.*"

356. La conexión persistente entre Google y los dispositivos móviles basados en Android también podría permitir la instalación remota de apps, y se emplea en la instalación de apps adquiridas desde el interfaz web de Google Play (detallada en el apartado previo).

10.1.4. CONEXIÓN GTALKSERVICE

357. La conexión GTalkService [Ref.- 81] [Ref.- 82], comunicación permanente a través de Internet disponible entre los dispositivos móviles Android y Google, emplea los protocolos TCP/SSL/XMPP para comunicarse periódicamente con los servidores de Google (mtalk.google.com) en el puerto TCP/5228 haciendo uso de las conexiones de datos del terminal, telefonía móvil (2/3/4G) o Wi-Fi.

358. El servicio GTalkService es empleado para el envío de mensajes desde Google a los dispositivos móviles Android, o para la instalación o eliminación remota de apps.

359. El protocolo empleado por GTalkService no hace uso de mecanismos adicionales de seguridad (por ejemplo, firmas criptográficas de los mensajes intercambiados) aparte del uso de HTTPS (SSL/TLS), por lo que un ataque sobre este protocolo permitiría potencialmente modificar el tráfico intercambiado y, por ejemplo, eliminar o instalar nuevas apps en el dispositivo móvil.

360. En Android 5.x y 6.x, el código USSD *#*#8255#*#* (o *#*#talk#*#*) del teclado del teléfono en Android, que ejecutaba el GTalk Service Monitor en Android 4.x y anteriores, deja de estar disponible, por lo que ya no es posible obtener todos los detalles de ejecución de GTalkService.

361. Por defecto, en Android 4.4.4, los detalles de este servicio estaban ocultos[8], y ni siquiera se pueden obtener los detalles de este servicio a través del botón de menú, y de la opción "Verbose logging". Para más información, consultar la versión para Android 4.x de la presente guía [Ref.- 402].

362. En versiones previas de Android, como 2.x, el *Gtalk Service Monitor* disponía de múltiples pantallas con información del servidor y puerto al que se encuentra conectado el dispositivo móvil, el identificador de usuario (Google JID) y de dispositivo móvil (Device ID), el intervalo de comprobación de la conexión (15 minutos), el estado de la conexión, un histórico de conexiones, o estadísticas de la transmisión de datos y las comunicaciones.

Nota: Los valores del "JID" (ejemplo, "usuario@gmail.com/android<CODIGO>", donde <CODIGO> es un string de 12 valores hexadecimales) y del "Device ID" (ejemplo, "android-<CODIGO>", dónde <CODIGO> es un string de 16 valores hexadecimales) no están relacionados con el valor del "ANDROID_ID".

10.2. VERIFICACIÓN DE SEGURIDAD DE LAS APPS: GOOGLE PLAY PROTECT

363. A lo largo del tiempo, Android ha incorporado diferentes mecanismos para analizar las aplicaciones publicadas por los desarrolladores a través del mercado oficial Google Play, llevando a cabo un proceso de escaneo o verificación de seguridad automático sobre dichas apps.

364. Para ello, hace uso de un sistema de análisis denominado Google Bouncer, cuyo principal propósito es identificar apps que contienen software malicioso (*malware*).

365. Google Bouncer [Ref.- 170] compara cada app con otras muestras de software malicioso conocidas, y también ejecuta las apps en un entorno virtual, simulando su ejecución en un dispositivo móvil Android, para analizar su comportamiento antes de proceder a su publicación oficial, e intentando identificar comportamientos maliciosos o anómalos normalmente asociados al *malware*.

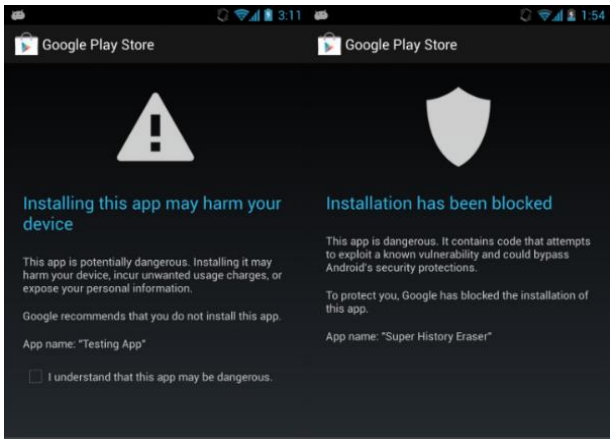
366. El sistema Google Bouncer analiza nuevas apps, apps existentes previamente en Google Play, reanaliza apps ya analizadas previamente una vez se incorporan nuevas capacidades al sistema, y también analiza cuentas de desarrolladores de Android (especialmente las de los nuevos desarrolladores, para evitar que agentes que distribuyen *malware* para Android lo hagan empleando la identidad de otros supuestos nuevos desarrolladores).

[8] A diferencia de como ocurría en versiones previas de Android, 2.x (ver la versión previa de la presente guía).

367. Por otro lado, desde la versión 4.2 de Android en el año 2012, Android dispuso de capacidades para el escaneo o verificación de seguridad de las apps durante el proceso de instalación, con el objetivo de identificar y detectar la existencia de software malicioso (*malware*) en las mismas, característica conocida (en inglés) como "Verify Apps" [Ref.- 171].

368. Inicialmente (desde Android 4.2), las capacidades de verificación de apps comparaban la app a instalar con una base de datos de apps existente en Google, con el objetivo de identificar si correspondía a un app ya conocida con comportamiento malicioso o dañino. El proceso de verificación envía a Google información sobre el nombre de la app, su tamaño, su *hash* SHA1, la versión y la URL asociada [Ref.- 174].

369. En caso de identificarse la app como dañina, en función del nivel de peligrosidad asociado a la app, Android podía recomendar al usuario que no instalase la app (en el caso de apps potencialmente dañinas), o incluso llegar a bloquearla (en el caso de apps confirmadas como dañinas), no siendo posible proceder con su instalación [Ref.- 171]. Las siguientes imágenes muestran un ejemplo de cómo se notificaba al usuario sobre la potencial peligrosidad de una app:



370. Esta verificación se lleva a cabo para las apps que son instaladas manualmente por el usuario, por ejemplo, desde una página web, un mercado de apps de Android no oficial, o a través de ADB (proceso conocido como *sideload*).

371. Para que sea posible instalar una app a través de un medio distinto a Google Play, es necesario habilitar previamente la instalación de apps de fuentes que no son de confianza, mediante la opción "Orígenes desconocidos" situada bajo "Ajustes - [Personal] Seguridad - [Administración del dispositivo]".

372. Este matiz es fundamental ya que, si la opción de "Orígenes desconocidos" no está activada, es aún posible instalar apps vía ADB (si se han permitido las opciones de desarrollo y la depuración vía USB) sin que se active la funcionalidad de verificación de apps.

373. Para las apps instaladas desde Google Play se confía fundamentalmente en la verificación realizada por el servicio Google Play Protect.

374. El framework "Verify Apps" se encargaba inicialmente de escanear las apps durante su instalación. A partir de 2014, se le añadió la capacidad de escanear (como servicio en segundo plano) las apps instaladas en el dispositivo móvil durante su ejecución, para identificar comportamientos inesperados que no fueron detectados durante la

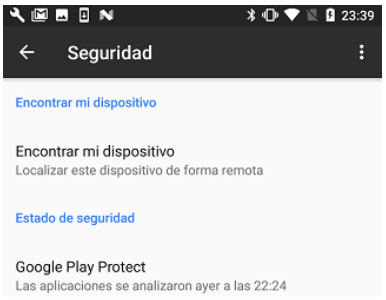
instalación [Ref.- 173] por si resultaban maliciosos. Así se extendió la funcionalidad a las apps que ya estaban instaladas en el dispositivo móvil.

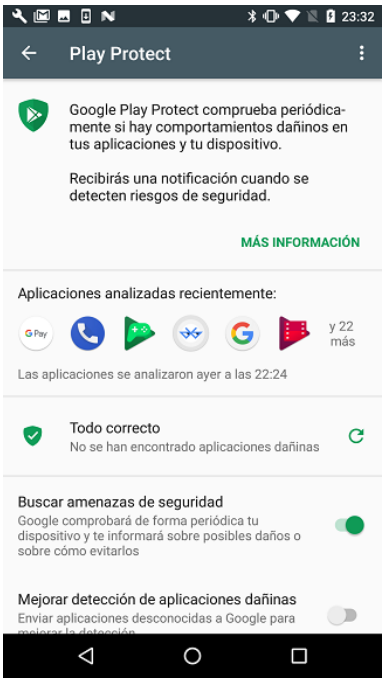
375. En el año 2015 la funcionalidad de "Verify Apps" fue extendida para poder eliminar apps que se registran como Administradores del Dispositivo, y para deshabilitar apps que han sido instaladas en la partición de sistema tras comprometer el modelo de seguridad de Android.

376. Asimismo, se añadieron mejoras en el interfaz gráfico de usuario para evitar la instalación de PHAs por descuido o desconocimiento por parte del usuario, y la posibilidad de que el usuario pueda remitir una app a Google desde el propio dispositivo móvil para su revisión.

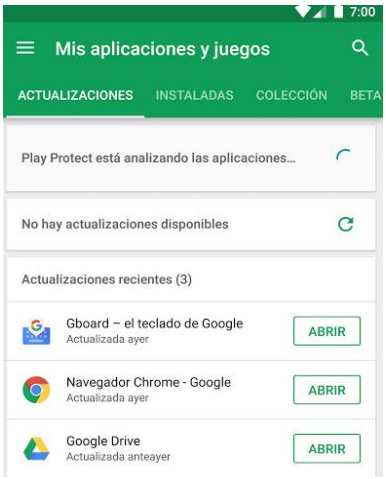
377. A partir de febrero de 2017, se añadió al interfaz gráfico de Android un menú que mostraba información sobre la funcionalidad "Verify Apps", al que se accedía desde "Ajustes - [Personal] Google - [Servicios] Seguridad - [Verificar aplicaciones] Verificar aplicaciones". En este menú se puede ver tanto el registro de las aplicaciones escaneadas como activar la opción "Buscar amenazas de seguridad en tu dispositivo".

378. En la conferencia Google I/O de julio de 2017, Google presentó el servicio "Google Play Protect", que integraba y extendía la funcionalidad "Verify Apps". Este servicio se empezó a distribuir como una actualización de los "Servicios de Google Play" a partir de su versión 11 y superiores, y, desde el punto de vista de configuración, se integra bajo "Ajustes - [Personal] Google - [Servicios] Seguridad - [Estado de seguridad] Google Play Protect", o, alternativamente, desde los ajustes de la app "Play Store": menú superior izquierdo (con tres líneas horizontales), "Play Protect":





379. El servicio Google Play Protect analiza automáticamente las apps del dispositivo cuando éste no está siendo utilizado y cuando está conectado a un cargador de corriente, a fin de afectar lo menos posible a su rendimiento. Desde la app "Play Store", y seleccionando el menú "Mis aplicaciones y juegos", es posible determinar cuándo se ha ejecutado el servicio Google Play Protect por última vez, así como lanzarlo en ese momento a través de la pulsación en la flecha circular situada a la derecha:

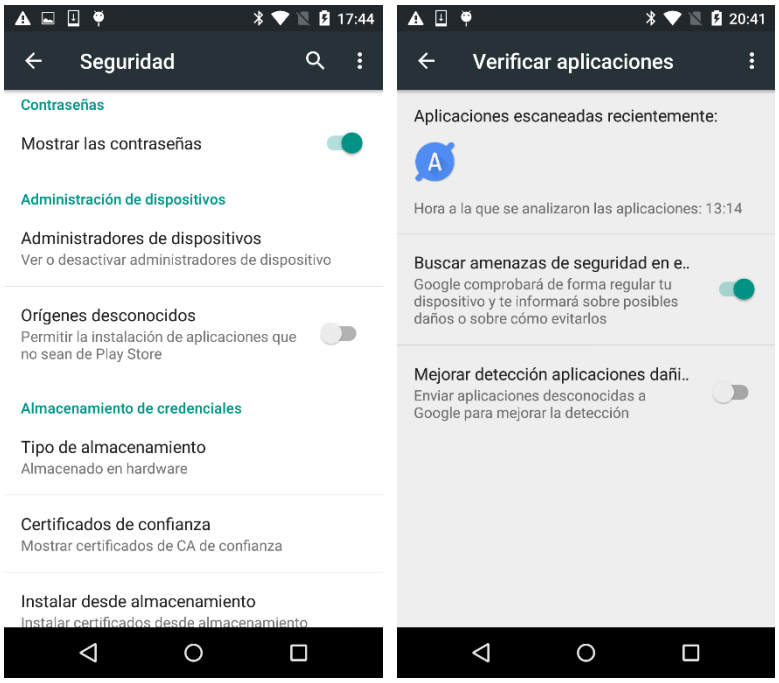


380. Como parte de la integración entre el servicio Google Play Protect y el mercado oficial de apps de Google, Google Play, mediante la app "Play Store", cuando se inicia la instalación de una app se mostrará el mensaje "Verificado por Play Protect" si la app ha sido ya analizada a través de dicho mecanismo:

381. Adicionalmente, en el menú "Play Protect", se añaden las opciones "Mejorar detección de aplicaciones dañinas", que enviará a Google información sobre las aplicaciones que se han instalado fuera de Google Play para que las analice en busca de malware, y "Buscar amenazas de seguridad", que es la opción para habilitar/deshabilitar el servicio "Play Protect".

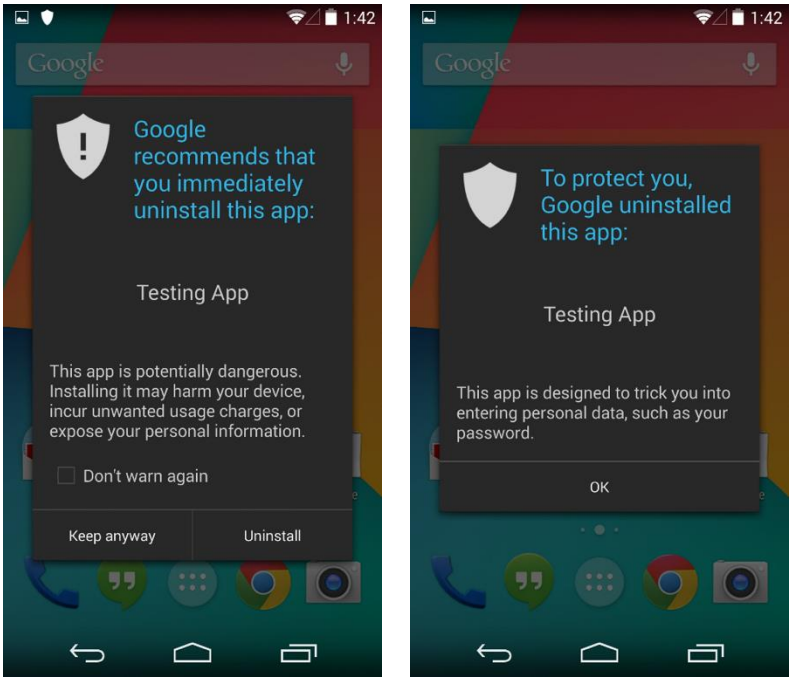
382. A pesar de que a fecha de elaboración de la presente guía existen estudios que no demuestran aún la efectividad de detección de este servicio, probablemente debido a su corta vida [Ref.- 272], se recomienda mantenerlo habilitado desde el punto de vista de seguridad.

383. La primera vez que se instala una app desde una fuente que no es de confianza, Android mostrará una pantalla solicitando al usuario la capacidad para enviar a Google, como parte de la funcionalidad "Verify Apps", información sobre el dispositivo móvil (como por ejemplo URLs asociadas a la app, el identificador del dispositivo móvil, la versión de Android, la dirección IP, cookies, etc.):



384. Adicionalmente, al activar la verificación de apps, Google recopilará información (supuestamente) anónima sobre las apps que son instaladas desde fuera de Google Play, con el objetivo de mejorar la detección de apps dañinas [Ref.- 174].

385. En caso de identificarse la app como dañina, Android puede recomendar al usuario que desinstale la app o incluso llegar a eliminar la app del dispositivo móvil[9]:



386. Las capacidades de verificación de apps se encuentran habilitadas por defecto en Android 6.x (no necesariamente en versiones previas de Android 4.2.x o superior).

387. En el caso de dispositivos móviles Android multi-usuario, únicamente el usuario propietario podrá activar o desactivar la verificación de apps.

[9] Imágenes: http://www.businessinsider.com/google-verify-apps-for-android-phones-2014-4

388. Desde el punto de vista de seguridad se recomienda dejar habilitada la opción de "Buscar amenazas de seguridad", para disponer de una verificación más regular y continua, y activar únicamente la opción "Mejorar detección de aplicaciones dañinas" si se desea colaborar con Google en el proceso de detección de *malware*.

389. Pese a que estas capacidades fueron introducidas en Android 4.2, actualmente están también disponibles para dispositivos móviles incluso basados en Android 2.3 (o superior) a través de la actualización de los servicios de Google Play. Por tanto, otros dispositivos móviles Android más antiguos, pueden disponer de estas capacidades de escaneo o verificación de apps, ya que las mismas fueron introducidas por Google en una de las actualizaciones del componente (y app) asociado a los servicios de Google Play[10] (sin ser necesario realizar una actualización de la versión del sistema operativo).

390. Debe tenerse en cuenta que tanto las capacidades introducidas por Google Bouncer [Ref.- 175], como las asociadas a "Verify Apps" [Ref.- 175] y a "Play Protect", añaden niveles de seguridad adicionales al ecosistema de Android, bajo el paradigma de seguridad en profundidad (es decir, añadir varios niveles o capas de protección), pero no proporcionan una protección completa (no son efectivas al 100%), pudiendo existir técnicas para evadir estos mecanismos de verificación de seguridad (tal como ya han demostrado en el pasado los estudios referenciados).

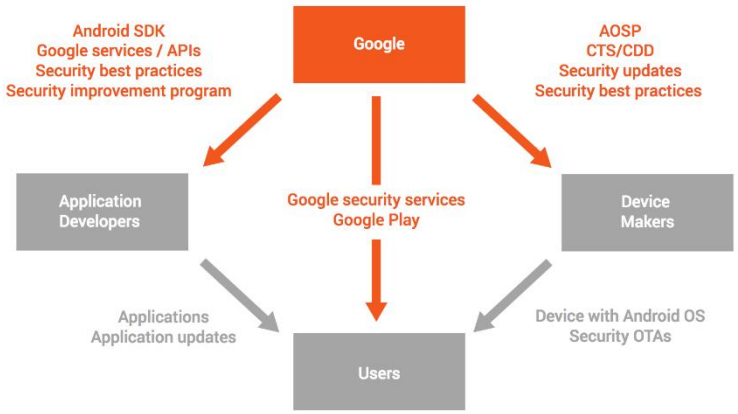
10.3. SAFETYNET

391. SafetyNet es una plataforma desarrollada por Google en 2013 para analizar la configuración de los dispositivos móviles Android, incluyendo un conjunto de servicios de seguridad, tanto en el propio dispositivo móvil como "en la nube", a través de Google Mobile Services (GMS)[11] y Google Play Services (GPS).

392. SafetyNet tiene implicaciones muy relevantes desde el punto de vista de seguridad y la integridad del dispositivo móvil, ya que es empleada por el equipo de seguridad de Android para monitorizar, junto a la funcionalidad de verificación de apps ("Verify Apps", ver apartado "10.2. Verificación de seguridad de las apps: Google Play Protect"), la existencia de ataques y código dañino o, como se han sido referenciados más recientemente, PHAs (*Potentially Harmful Applications*) [Ref.- 24], dentro del ecosistema de seguridad de Android.

[10] http://www.howtogeek.com/179638/not-getting-android-os-updates-heres-how-google-is-updating-your-device-anyway/

[11] https://www.android.com/gms/



393. Verify Apps se centra más en la detección y protección frente a PHAs (*Potential Harmful Application*), mientras que SafetyNet se centraba (al menos inicialmente) en ataques a través de la red, aunque las capacidades de ambos sistemas se han ido integrando y combinando a lo largo del tiempo.

394. Los dispositivos móviles Android pueden remitir a Google, a través de los servicios "en la nube" de SafetyNet, información de seguridad como eventos, logs, o información de configuración [Ref.- 24].

395. Desde 2013, Google comenzó a introducir mecanismos en el código de la plataforma Android y/o de las apps para detectar intentos de explotación de vulnerabilidades y generar eventos de log asociados, con el objetivo de poder identificar tendencias de ataque (así como estadísticas de amenazas según la localización geográfica) y evaluar la efectividad de los mecanismos de protección existentes. En 2015, se añadieron capacidades de detección para nuevas vulnerabilidades, como Stagefright.

396. En Android 4.2 se introdujeron capacidades de *certificate pinning* y de listas negras de certificados asociadas a la gestión de las autoridades certificadoras (CAs) en Android. Desde Android 4.4, Android genera un aviso al usuario indicando que se ha instalado localmente un certificado digital que podría permitir la intercepción del tráfico SSL/TLS. Desde octubre de 2014, SafetyNet hace uso de pruebas activas asociadas al tráfico de red para identificar escenarios en los que se haya podido manipular el almacén de CAs local.

397. Asimismo, SafetyNet ha sido empleada desde 2014 para identificar apps que intentan engañar al usuario a la hora de enviar mensajes SMS *premium* en campañas de fraude a través de SMS. La información obtenida es empleada para bloquear las apps dañinas a través de Verify Apps, o eliminarlas de Google Play.

398. En 2015 las capacidades de SafetyNet, y de envío de datos (supuestamente) anónimos a Google, se comenzaron a emplear para detectar PHAs y complementar la funcionalidad de Verify Apps, a través de un motor de correlación de anomalías (*Anomaly Correlation Engine*, ACE).

399. En 2015 también se ampliaron sus capacidades para realizar chequeos de integridad del dispositivo móvil (cuando éste está ocioso) a través de un servicio "en la nube" denominado *System Integrity Check* (SIC), pudiendo detectar modificaciones de la partición de sistema, como las realizadas por ROMS, versiones o *firmwares* de Android personalizados, por apps dañinas que realicen modificaciones del sistema y (potencialmente) detectar apps que podían permitir aplicar el proceso de *root* sobre

el dispositivo móvil. Este tipo de apps no están permitidas en Google Play por política de Google, y Verify Apps avisa al usuario cuando intenta instalar una app con estas capacidades, o (de nuevo) una app dañina que intenta explotar alguna vulnerabilidad de escalada de privilegios.

400. Asimismo, las capacidades de SafetyNet han sido ampliadas para detectar si el dispositivo móvil se encuentra *rooteado*. Gracias a la funcionalidad y capacidades de detección de SafetyNet, algunas apps como Android Pay no ejecutarán en dispositivos móviles *rooteados*.

401. Se introduce lo que se denomina "*SafetyNet attestation*" (testimonio de SafetyNet) como característica de los Google Play Services (GPS), que Google otorga a una aplicación (o a un dispositivo móvil) tras someterla a unos test de compatibilidad, o CTS (*Compatibility Test Suite*), antes de admitirla para su inclusión en los servicios de Google Play.

402. Además, el contexto de SafetyNet se extiende a que las aplicaciones no puedan ejecutar si un dispositivo se considera que este se encuentra en estado "*tampered*" (alterado), como en el caso de que haya sido *rooteado*, infectado con malware, monitorizado, etc.

403. Google emplea el término "CTS compatible" para los dispositivos que se consideran "no alterados", lo cual no significa que estén libres de vulnerabilidades o actualizados a las últimas versiones de las apps o de parches de seguridad del propio sistema operativo Android.

404. En este sentido, SafetyNet resulta útil para los desarrolladores y no tanto para el usuario final, pues asegura a los primeros que su aplicación solo ejecutará en dispositivos que se encuentren en el estado para el que la aplicación ha sido diseñada.

405. Para hacer uso de las capacidades de "SafetyNet Attestation" la aplicación debe invocar el método SafetyNetApi.attest() del SDK de Google Play Services incluyendo un timestamp, que se envía a los servidores de Google a través de GoogleApiClient [Ref.- 25].

406. Google responderá en formato "JSON Web Signature (JWS)" incluyendo el parámetro "*ctsProfileMatch*" con valor verdadero o falso.

407. La aplicación verificará este valor, con lo cual podrá determinar si el dispositivo es "CTS compatible" y, en consecuencia, permitir o denegar su ejecución en el dispositivo. Esta verificación se puede realizar también en el servidor designado por la aplicación, logrando así que se pueda impedir acceso a los servicios de una aplicación de forma centralizada, y no en la parte cliente, que podría ser fácil de manipular. Este es el caso de Android Pay.

408. El uso de estas características y capacidades de SafetyNet pueden consultarse en la página oficial de Google [Ref.- 99].

409. Con el objetivo de ocultar que se ha realizado el proceso de root en el dispositivo móvil Android, existen herramientas como Magisk [Ref.- 104] (u otras herramientas que ocultan la presencia del binario "su" y sus componentes), que modifican el comportamiento del sistema de cara a ocultarlo en SafetyNet, en un proceso constante de actualización de los mecanismos de detección por parte de Google

(dentro de SafetyNet) y de ocultación por parte de la comunidad (con nuevas herramientas).

410. Mediante apps como SafetyNet Helper Sample [Ref.- 12] y SafetyNet Playground [Ref.- 36] es posible consultar el estado del dispositivo móvil en SafetyNet y conocer los detalles de la evaluación actual según este servicio de Google.

411. Por otro lado, SafetyNet puede ser utilizada por parte de las apps (a través de una API vinculada a *Google Play Services*, GPS) para evaluar las capacidades, tanto hardware como software, de un dispositivo móvil y analizar la compatibilidad del mismo con la app (empleando perfiles de compatibilidad y en base a la CTS, *Compatibility Test Suite* [Ref.- 88]), intentando asegurar que la app funcionará correctamente en el dispositivo y mejorar la experiencia del usuario [Ref.- 91].

10.4. GESTIÓN REMOTA DE DISPOSITIVOS ANDROID POR PARTE DEL USUARIO

412. El soporte para aplicaciones empresariales fue introducido por Android 2.2 a través de la API "Android Device Administration" [Ref.- 269] [Ref.- 273]. Esta API proporcionaba capacidades de administración a nivel de sistema, como permitir establecer políticas de contraseñas, añadir capacidades de borrado remoto y servicios de gestión del dispositivo móvil y de sus aplicaciones.

413. Las políticas de administración de dispositivos pueden estar programadas dentro de una app de gestión o solicitarse dinámicamente desde un servidor corporativo. La app de gestión se puede instalar en el dispositivo móvil del usuario final a través de Google Play, de un mercado de apps conocido y de confianza (por ejemplo, privado a la organización), o a través de un servidor web.

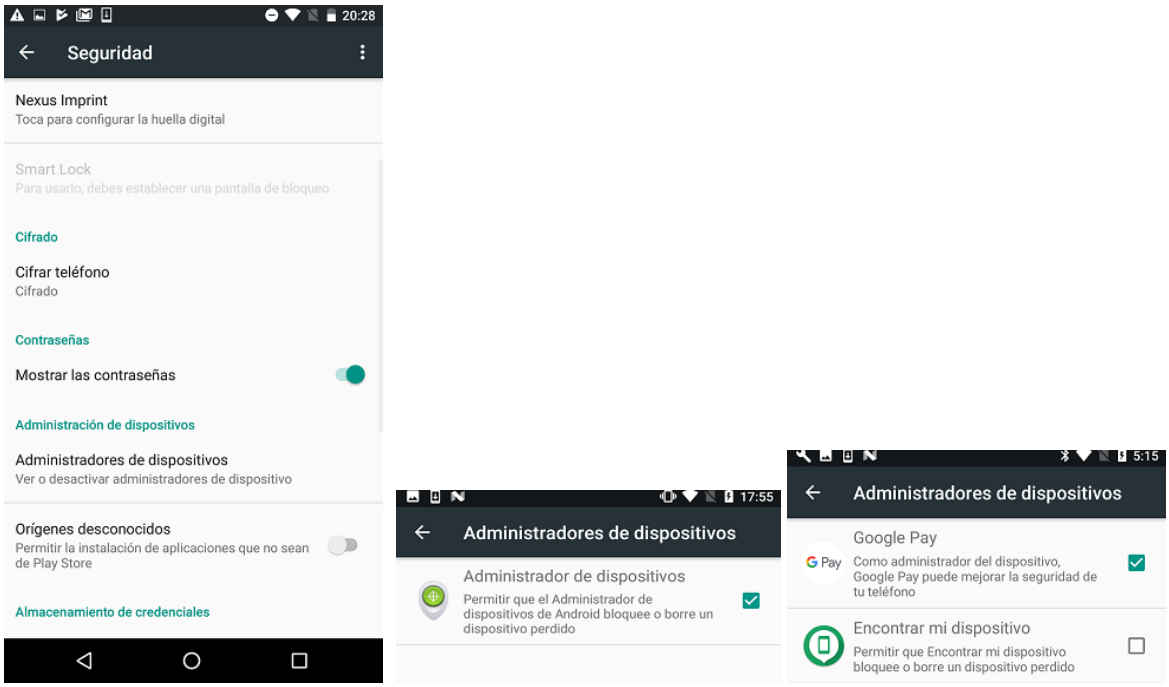
414. Cuando se instala la app de gestión, el sistema solicitará al usuario el permiso de "administrador de dispositivos". Si se le concede, la app impondrá sus políticas, y tendrá la capacidad de tomar las acciones definidas si éstas no se cumplen. Así, por ejemplo, si la app define una política de longitud mínima de contraseña y el usuario no la cumple, podría denegarle el acceso a un determinado servicio.

415. La administración de dispositivos móviles puede establecer políticas que actúen ante la instalación o borrado de determinadas apps, bien sea lanzando un mensaje de aviso o bloqueando por completo la acción.

416. La API de administración de dispositivos no permite cumplimientos parciales de las políticas, es decir, sólo aquellos dispositivos que cumplan todas las restricciones se considerarán aptos.

417. Si un dispositivo contiene varias apps con el permiso de administrador del dispositivo, se impondrá la que defina la política más restrictiva, ya que no existe ningún mecanismo para seleccionar una app de administración para diferentes escenarios.

418. Es posible consultar qué aplicaciones tienen el permiso de administración de dispositivos a través de "Ajustes [Personal] - Seguridad [Administración del dispositivo] - Administradores de dispositivos":



419. El permiso de administrador de dispositivos, al permitir la gestión remota del mismo, incluyendo su borrado, nunca debe ser concedido salvo en escenarios de plena confianza, ya que una app maliciosa podría solicitarlo y hacer uso de estas capacidades avanzadas.

420. En versiones anteriores de Android, el cliente o módulo de administración remota se denominaba "Administrador de dispositivos" (ver imagen superior central). Actualmente, este módulo app se denomina "Encontrar mi dispositivo".

421. El acceso a la gestión remota del dispositivo móvil por parte de los usuarios particulares, no asociados a un dominio de Google Apps o G Suite, se puede llevar a cabo a través del servicio de Google "Encontrar mi dispositivo", disponible en la URL "https://www.google.com/android/find", o desde la app "Encontrar mi dispositivo" (disponible en Google Play[12]) instalada y ejecutada desde otro terminal que tenga acceso a la misma cuenta de usuario de Google que la definida en el dispositivo móvil.

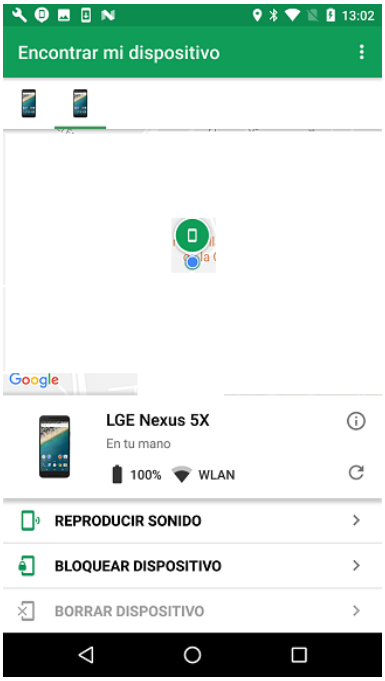
422. Este recurso y app han sustituido a los utilizados en versiones previas de Android, ambos denominados "*Android Device Manager*"[13].

423. El servicio "Encontrar mi dispositivo" (Find my device), cuyo cliente hasta Android 4.4 se ofrecía como una app disponible en Google Play (antiguamente denominado Play Store), pasó a formar parte del servicio "Google Play Protect" (ver apartado "10.2. Verificación de seguridad de las apps: Google Play Protect"), de modo que, desde Android 6.x en adelante, se ofrece como un componente con permisos de "administrador de dispositivos" [Ref.- 227], y, entre otras cosas, permite al usuario, tanto desde la web como desde otro terminal Android, encontrar el dispositivo móvil Android (*smartphones* o *tablets*).

[12] https://play.google.com/store/apps/details?id=com.google.android.apps.adm

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

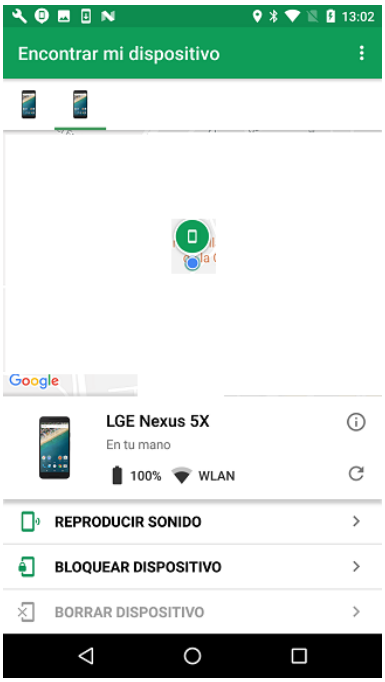
424. Es importante diferenciar entre el servicio "Encontrar mi dispositivo", y su cliente o módulo asociado presente por defecto en versiones actuales de Android (reflejado con el mismo nombre "Encontrar mi dispositivo" en la sección "Administradores de dispositivos"), y la app "Encontrar mi dispositivo", que se puede instalar desde la Play Store pero que no está instalada por defecto. El servicio interactúa con el cliente o módulo, que permite o deniega la gestión remota sobre el propio dispositivo móvil. La app actúa como interfaz gráfico, permitiendo el uso del servicio y de las capacidades de gestión remota sobre dispositivos externos que compartan con él la cuenta de usuario de Google.



425. La app "Encontrar mi dispositivo" disponible desde la Play Store, una vez instalada, aparece con el término "Buscar" en su icono asociado en el *Launcher*.

426. Es muy importante reseñar que, tanto la funcionalidad del portal de gestión remota como los mensajes que se muestran en respuesta a las diferentes acciones solicitadas a través de él, son dependientes de Google (y de sus servicios asociados) y pueden variar a lo largo del tiempo. Las opciones y mensajes descritos en la presente guía corresponden a los mostrados en julio de 2018.

427. La app "Encontrar mi dispositivo" también sigue estando disponible para Android 7.x, para el caso en que se desee localizar otro dispositivo desde el terminal móvil (ver la imagen inmediatamente anterior). Sus opciones son similares a las ofrecidas por el servicio de gestión remota "Encontrar mi dispositivo" (disponible en "https://www.google.com/android/find") de Google.

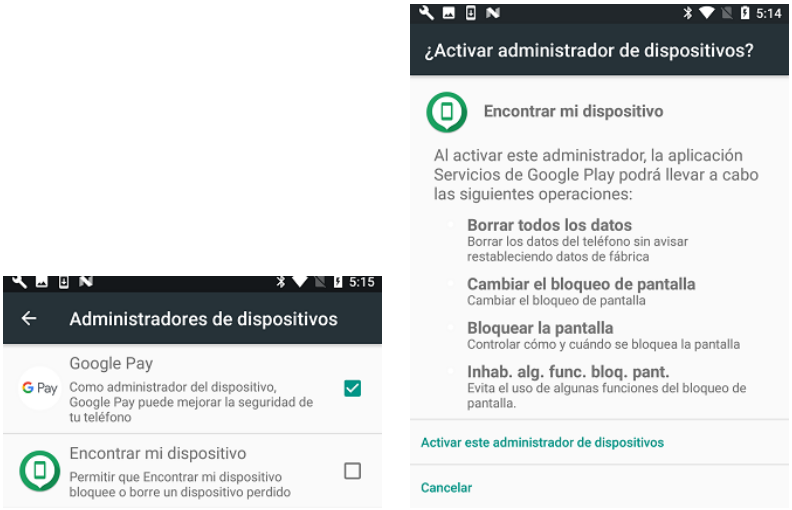


428. Los requisitos para hacer uso de la funcionalidad de gestión remota son [Ref.- 61]:

- Disponer de una conexión de datos: para poder hacer uso de las capacidades de gestión remota es necesario que el dispositivo móvil disponga de una conexión a una red Wi-Fi o de datos móviles (2/3/4G), a fin de poder comunicarse con los servidores de Google y responder a las acciones solicitadas por estos.
    - Si el dispositivo móvil no dispone de una conexión de datos, el administrador de dispositivos Android no podrá bloquear la pantalla, modificar el código de acceso (referido por Google como la contraseña de bloqueo de la pantalla), hacer sonar el dispositivo móvil, o borrar sus datos remotamente hasta que se establezca una conexión a través de una red Wi-Fi o de la red de datos móviles. Al seleccionar una acción en el administrador de dispositivos Android, ésta se llevará a cabo la próxima vez que el dispositivo móvil vuelva a estar conectado. Lógicamente, el administrador de dispositivos Android no funciona para dispositivos móviles que estén apagados o con en modo avión activado.
- Disponer del administrador de dispositivos Android activo: desde el menú "Ajustes - [Personal] Seguridad - [Administración del dispositivo] - Administradores de dispositivos - Encontrar mi dispositivo" es posible activar esta funcionalidad, y la pantalla de confirmación informará de las capacidades de gestión asociadas.

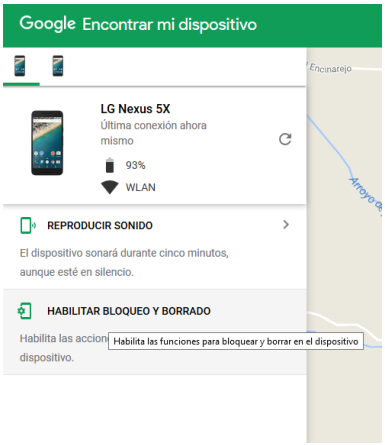
  Las capacidades de gestión remota que se obtienen al activar el administrador de dispositivos Android son: *bloquear la pantalla* (equivale a bloquear remotamente un dispositivo móvil perdido o robado), *cambiar el bloqueo de pantalla* (en caso de que no se hubiese configurado un código de acceso en el dispositivo móvil; desde el interfaz web de gestión remota se puede configurar uno; si ya hubiese uno vigente, la configuración de un nuevo código de acceso no modificará el código actual), *borrar todos los datos* (equivale a

una restauración a fábrica remota, o *remote wipe*) e *inhabilitar algunas funciones del bloqueo de pantalla*. Estas opciones se aceptan implícitamente al activar el administrador de dispositivos, no siendo posible activarlas/desactivarlas individualmente.



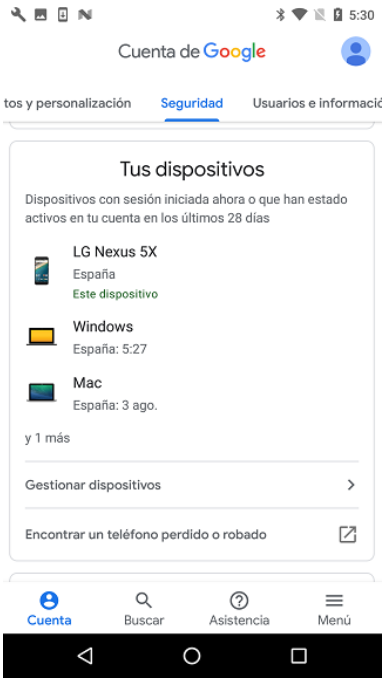
- Disponer de una sesión iniciada con la cuenta de Google del usuario desde el dispositivo móvil, disponible automáticamente en caso de haber sido configurada dicha cuenta.
- El dispositivo móvil debe estar visible en Google Play: el dispositivo se puede hacer visible desde la sección "Visibilidad" de Google Play ("https://play.google.com/settings"). Si un dispositivo móvil está oculto en Google Play, no aparecerá en la funcionalidad de "Encontrar mi dispositivo".
- Tener el servicio de ubicación (o localización) activo: desde la app "Ajustes de Google", mediante el menú "[Servicios] Ubicación", es posible habilitar la opción "Ubicación" (servicios de localización) mediante el botón "Sí".
    - Este acceso es equivalente al acceso estándar correspondiente a los servicios de localización, disponible desde "Ajustes - [Personal] Ubicación".

429. Sin embargo, aunque la opción "Ajustes [Servicios] - Seguridad - [Administrador de dispositivos] Administradores de dispositivos - Encontrar mi dispositivo" esté deshabilitada en el dispositivo móvil, el interfaz web de gestión remota https://www.google.com/android/find permite habilitar estas capacidades de forma remota.



430. Si se selecciona esta opción remotamente desde el interfaz web, se activará de nuevo el interruptor "Encontrar mi dispositivo" en el dispositivo móvil. En el interfaz web se mostrará el mensaje "*Las funciones para bloquear y borrar se han habilitado correctamente*". Es decir, estas capacidades son gestionadas remotamente desde el interfaz web y no desde el propio dispositivo móvil.

431. La información sobre los dispositivos asociados a una cuenta de usuario de Google está disponible en el menú "Seguridad - Tus dispositivos".



432. Si se desea acceder a las capacidades de gestión remota ante la pérdida o robo del dispositivo móvil, se dispone de tres opciones con funcionalidad similar, ambas descritas en detalle a continuación. Es importante tener en cuenta (especialmente para las dos primeras opciones) que los pasos descritos, así como su resultado, al depender de servicios en la nube de Google, pueden cambiar sin previo aviso, y sin que el usuario haya realizado ninguna actualización en su dispositivo móvil:

- Utilizar el recurso "Encontrar mi dispositivo" (opción 1), disponible en "https://www.google.com/android/find" (o "https://android.com/find/").
- Acceder a la cuenta de Google del usuario del dispositivo móvil desde "https://myaccount.google.com" y seleccionar la opción "Encontrar tu móvil" (opción 2), que mostrará la lista de dispositivos móviles que están (o han estado) vinculados a esa cuenta, pudiéndose seleccionar el dispositivo deseado.
- Ejecutar la app "Encontrar mi dispositivo" desde otro terminal en el que se haya dado de alta la cuenta de usuario de Google asociada al dispositivo móvil extraviado (los pasos son similares a los de la opción 1).

433. Si se hace uso del recurso "Encontrar mi dispositivo" (opción 1) [Ref.- 202] para acceder a las capacidades de gestión remota, tras introducir las credenciales de la cuenta de Google del usuario, se mostrarán las siguientes opciones:

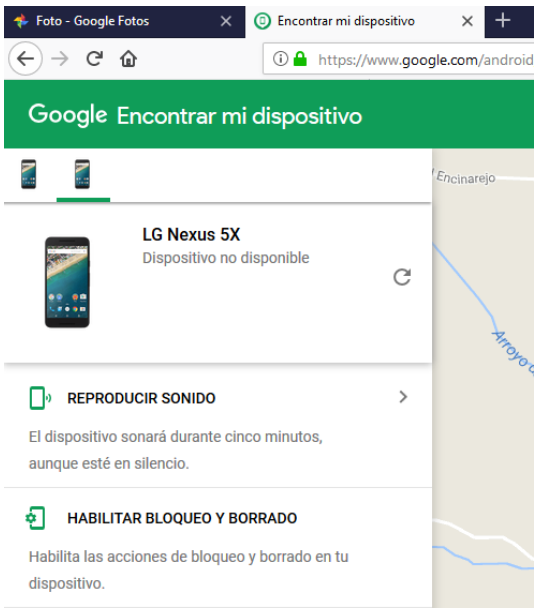
- Reproducir sonido: esta opción hace que el dispositivo móvil emita un sonido con el máximo volumen para poder localizar su ubicación, incluso si se

encontraba en silencio. El sonido se reproducirá durante 5 minutos o hasta que se interaccione físicamente con el dispositivo, a través de los botones físicos o de la pantalla.

- Habilitar bloqueo y borrado: para activar la funcionalidad del administrador de dispositivos "Encontrar mi dispositivo".

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

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

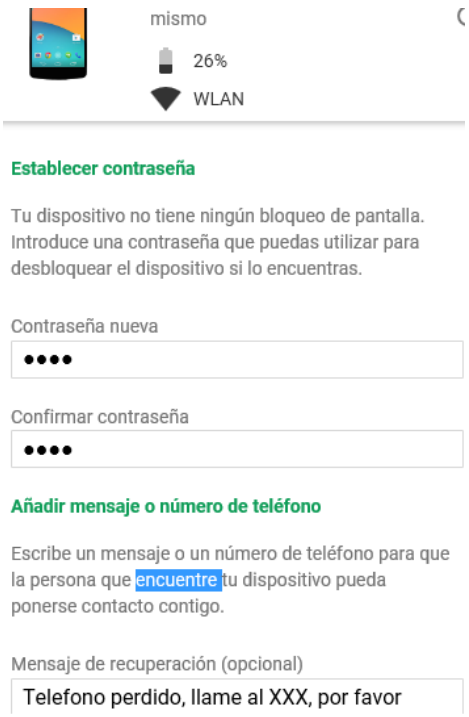


436. La opción "Bloquear" mostrará un menú que permite introducir un código de acceso (o contraseña) y proporcionar un mensaje que se mostrará en la pantalla de bloqueo del dispositivo móvil. La primera vez que se pulse esta opción, se muestra un mensaje indicando que el dispositivo no tiene ningún bloqueo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

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

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

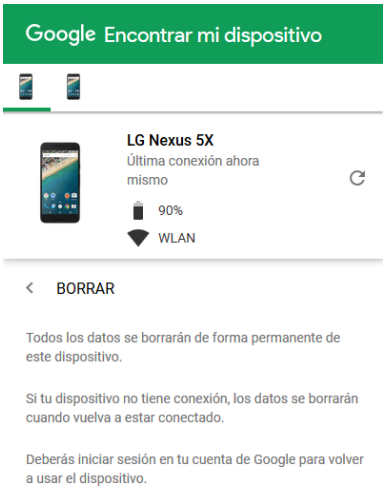
439. El interfaz web mostrará un mensaje que indicará si la operación tuvo éxito (se mostrará el mensaje "*Bloqueado*") o no; sin embargo, en el momento de elaboración de la presente guía, en múltiples ocasiones se ha recibido el mensaje "*No se ha podido bloquear el dispositivo*" aunque la operación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



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

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

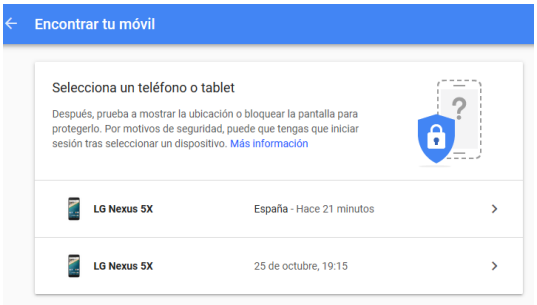
442. La opción "Borrar" eliminará todos los datos de usuario del dispositivo móvil y restaurará a fábrica el terminal, dejando la versión del sistema operativo Android disponible en el momento de llevar a cabo esta acción. El proceso de eliminación de los datos es equivalente a un *hard reset*, es decir, al restablecimiento del dispositivo móvil a la configuración de fábrica. Durante el proceso, por tanto, se eliminarán las apps instaladas, junto a todos los datos y configuraciones realizadas por el usuario.



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

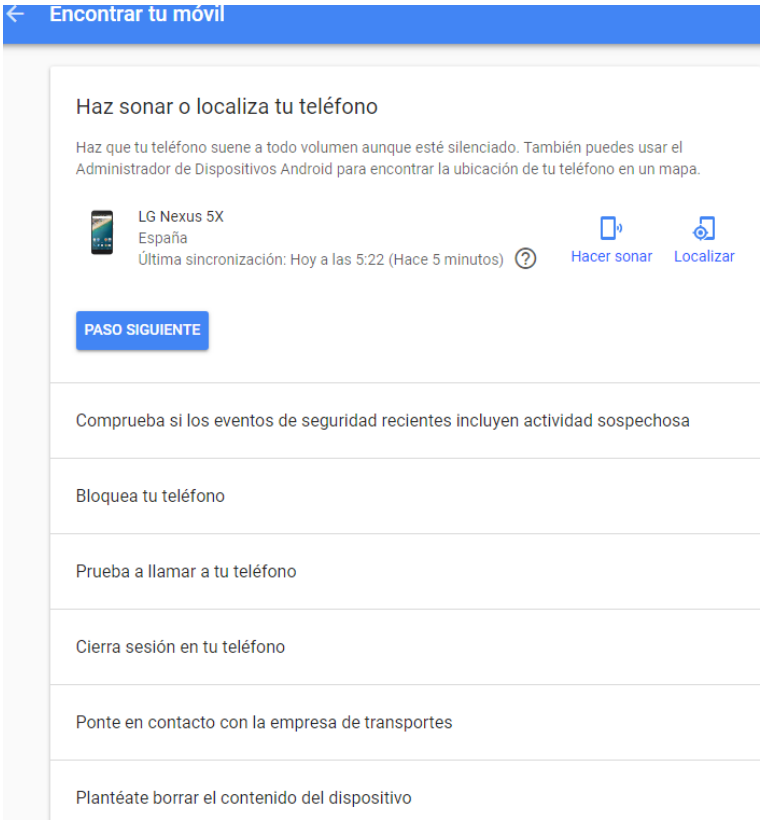
444. Es importante tener en cuenta que puede existir una demora entre que se ordena una determinada acción desde el interfaz web de gestión remota y su ejecución efectiva en el dispositivo móvil. Aunque normalmente se debería recibir un mensaje que confirme el éxito o fracaso de la operación, desafortunadamente se ha constatado que, en determinadas ocasiones, los mensajes de confirmación de la operación en la interfaz web de gestión remota no siempre son coherentes con la acción realizada, no se muestran o tienen un contenido erróneo. Sin embargo, la tasa de coherencia en Android 7.x es significativamente superior a la observada en Android 5.x.

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



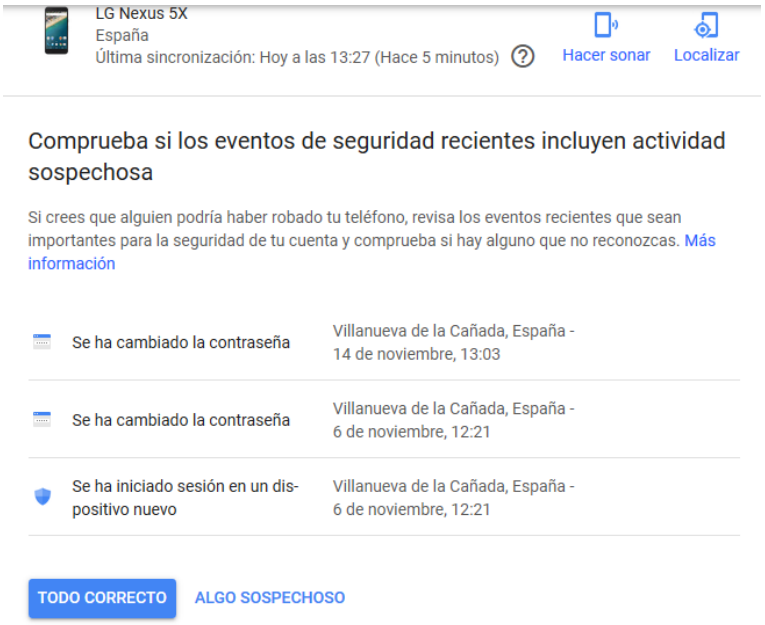
446. Se recomienda por defecto seguir las múltiples opciones disponibles en el orden en el que son presentadas, pues se parte de la premisa de que el dispositivo móvil podría estar aún próximo al usuario.

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

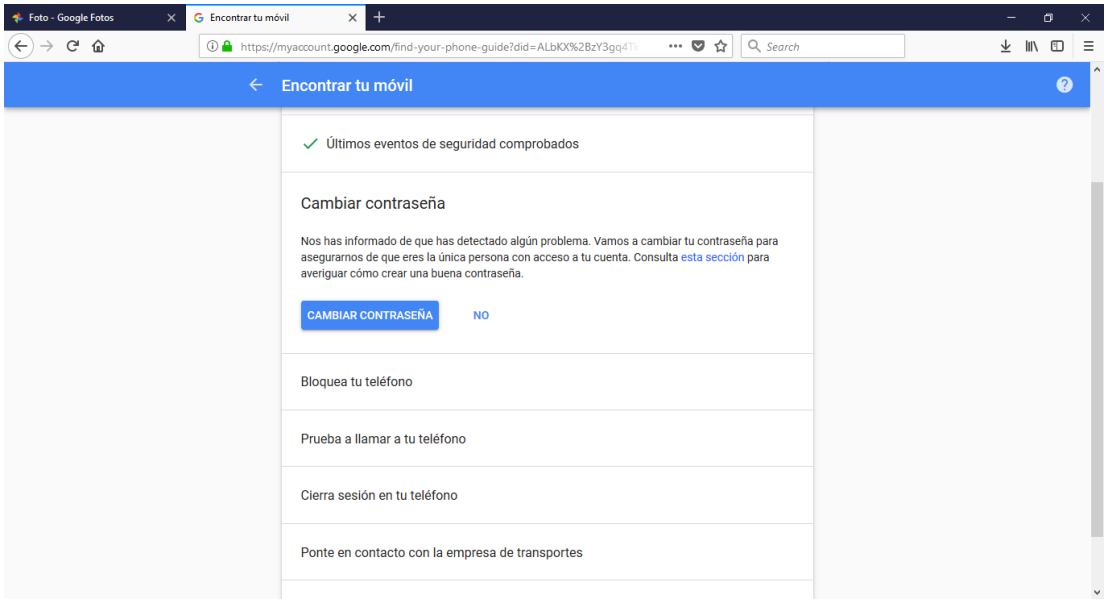


448. Si desde este interfaz web de gestión se selecciona la opción "Localizar", se abrirá el enlace "https://www.google.com/android/find" (equivalente al recurso "Encontrar mi dispositivo" correspondiente a la opción 1 descrita previamente).

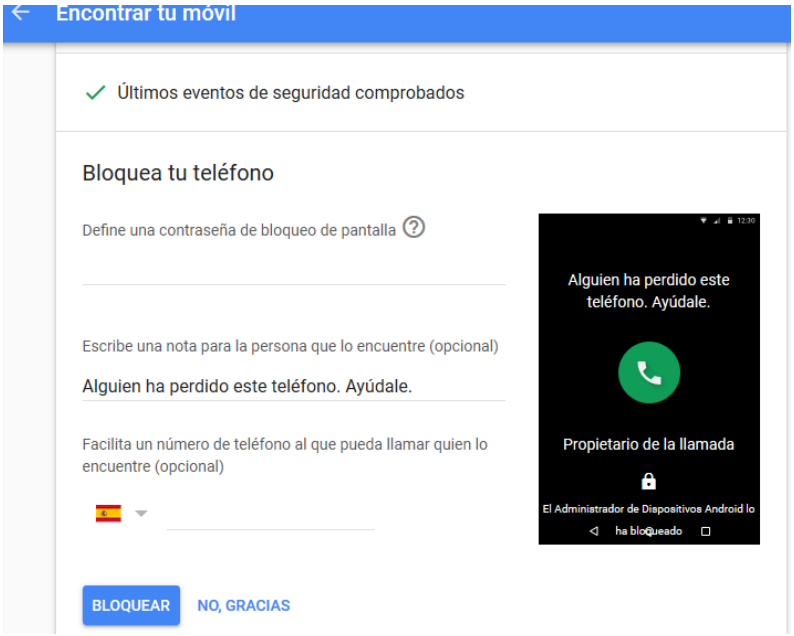
449. Si se selecciona la opción "Paso siguiente", se desplegará un menú que muestra los últimos eventos de seguridad registrados en la cuenta de Google del usuario, como por ejemplo un cambio de contraseña o un inicio de sesión en un nuevo dispositivo, desde el que no se había efectuado un inicio de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



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



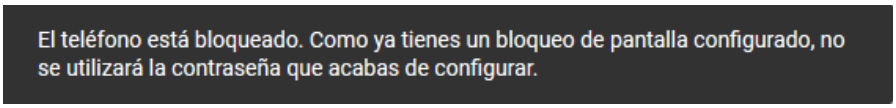
451. Si, por el contrario, no se identifica ninguna actividad extraña, se desplegará la opción "Bloquea tu teléfono" (equivalente a la opción "*Bloquea tu teléfono*" del listado de múltiples opciones disponibles), que permite bloquear remotamente el dispositivo móvil. Además, si el dispositivo móvil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



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

453. Una vez ejecutada la acción, si ésta ha tenido éxito, se recibe confirmación de la operación en el interfaz web de gestión remota. Si no ha sido posible contactar con el dispositivo móvil, se informa de que se ha enviado la solicitud mediante el mensaje "*Hemos enviado una solicitud de bloqueo a tu dispositivo correctamente*". Cuando el dispositivo móvil vuelva a disponer de conectividad de datos, recibirá la petición, y ejecutará la acción. Como se ha descrito previamente, esto implica que los servidores de Google encolan las peticiones destinadas al dispositivo, y las envían cuando detectan que el dispositivo móvil está de nuevo disponible. En ese momento se mostrará el mensaje de confirmación[14]:

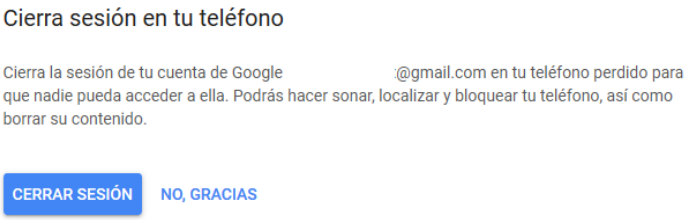
[14] Desafortunadamente, no se ha identificado la existencia de ningún registro (o *log*) que refleje las diferentes acciones llevadas a cabo mediante los mecanismos de gestión remota, junto a las confirmaciones del dispositivo móvil, incluyendo una referencia temporal.



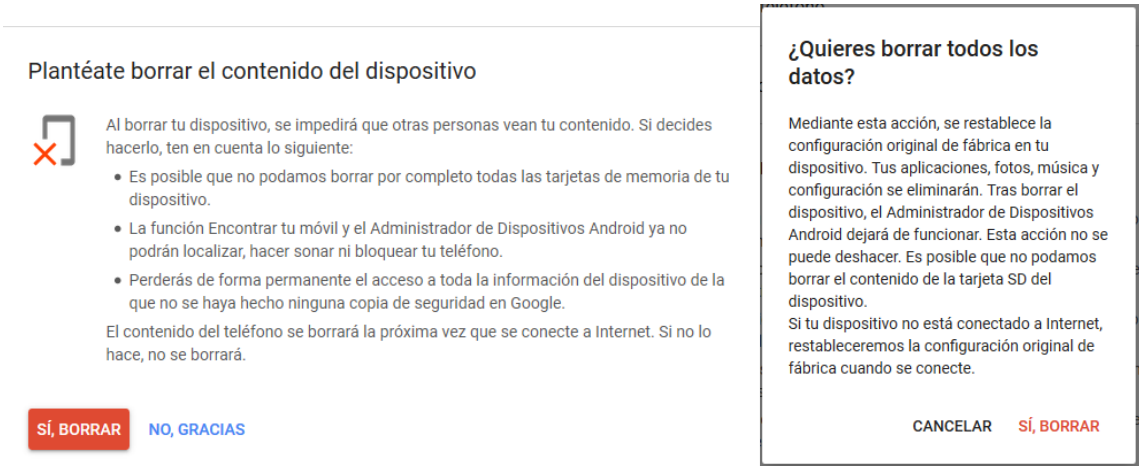
454. Como resultado, si la acción de bloqueo ha tenido éxito, el dispositivo móvil mostrará una nueva pantalla de desbloqueo, con el mensaje especificado previamente (cada vez que se apague la pantalla). En dicha pantalla se mostrará una nota que indica "Bloqueado por el `Encontrar mi dispositivo`".

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

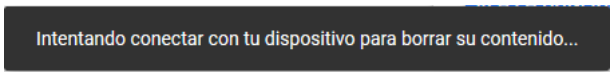
456. La opción "*Cierra sesión en tu teléfono*" provoca que se cierre la sesión asociada a la cuenta de Google del usuario en el dispositivo móvil. De ese modo se impedirá que, en caso de poderse desbloquear el dispositivo por parte de un tercero no autorizado, éste tenga acceso a los datos de la cuenta.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



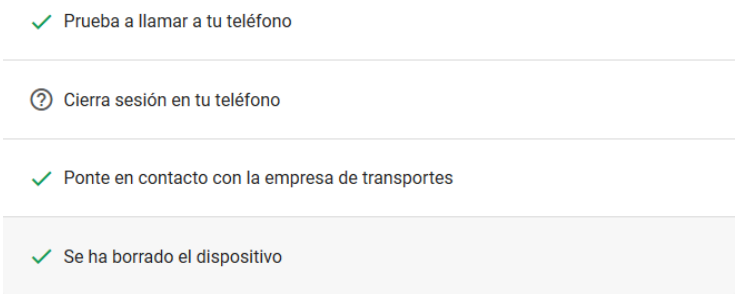
457. Por último, la funcionalidad "*Plantéate borrar el contenido del dispositivo*" ofrece al usuario la posibilidad de eliminar todos los datos del terminal remotamente desde el interfaz web de gestión. Una vez ejecutada la acción, mediante el botón "Sí, Borrar", si el dispositivo móvil disponía de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



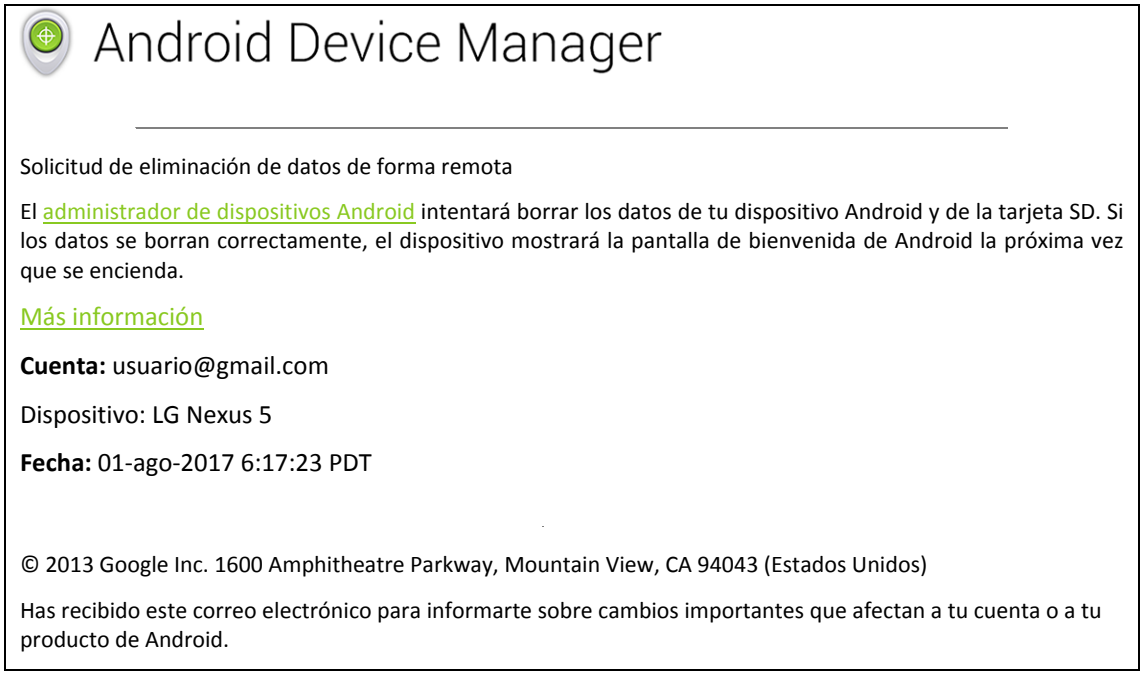
458. Tras confirmar la operación de borrado, se intentará contactar con el dispositivo:



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

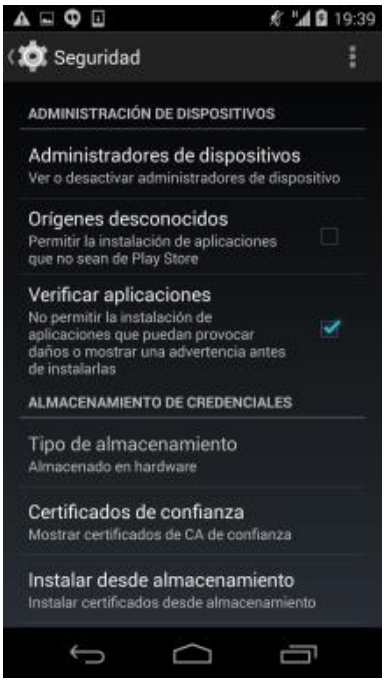


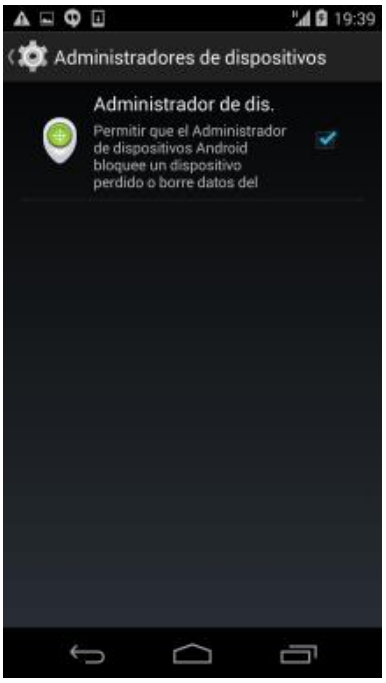
460. En el pasado, tras lanzarse la acción de borrado del dispositivo móvil, el administrador de dispositivos enviaba un mail a la cuenta de Google del usuario del dispositivo informando de que se la solicitud de borrado de datos había sido enviada y que el administrador de dispositivos Android intentaría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



461. Otros dispositivos móviles con versiones de Android más antiguas, anteriores a la versión Android 5.x, también pueden disponer del administrador de dispositivos Android (aunque pudiera no estar habilitado por defecto), ya que el mismo fue introducido por Google en una de las actualizaciones del componente (y app) asociado a los Servicios de Google Play[15] (sin ser necesario realizar una actualización de la versión del sistema operativo):

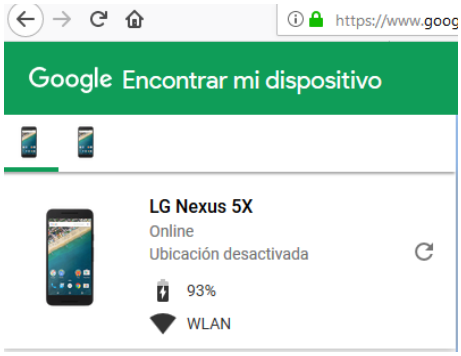
[15] http://www.howtogeek.com/179638/not-getting-android-os-updates-heres-how-google-is-updating-your-device-anyway/





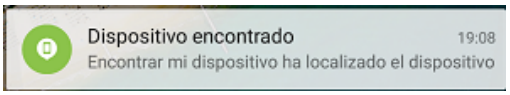
462. En el caso de dispositivos móviles con varios usuarios, únicamente el usuario administrador podrá habilitar o deshabilitar el administrador de dispositivos "Encontrar mi dispositivo".

463. Si el servicio de ubicación del dispositivo móvil estuviese desactivado en "Ajustes - [Personal] Ubicación", la opción "Localizar (este dispositivo de forma remota)" se mostraría inhabilitada y el interfaz web de gestión remota informaría de este hecho mediante el mensaje "Ubicación desactivada":



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

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



466. Recientemente, Google incorporó a su interfaz web de administración de la cuenta de usuario de Google (concretamente, en el apartado "Inicio de sesión y seguridad"), el apartado "Actividad de los dispositivos y eventos de seguridad", en el cual se pueden ver y gestionar eventos que, en caso de haberse extraviado el dispositivo móvil, permiten detectar si se está realizando algún acceso desde él en la cuenta de Google del usuario. Por su parte, el interfaz de administración de la cuenta de usuario de Google propio del dispositivo móvil también ofrece la sección "Seguridad - Protegemos tu cuenta", desde la que se puede consultar la denominada "revisión de seguridad".

10.5. DESBLOQUEO MEDIANTE SMART LOCK

467. Smart Lock de Google es una de las principales novedades introducidas en Android 5.x ("Lollipop"). Se trata de una funcionalidad que permite que el dispositivo móvil se mantenga desbloqueado en determinadas circunstancias (por ejemplo, si el dispositivo móvil está en una ubicación configurada por el usuario, o si está conectado a un dispositivo Bluetooth considerando de confianza), a pesar de que se cumplan otras condiciones de bloqueo, por ejemplo, por tiempo de inactividad. Además, Smart Lock permite también el desbloqueo "automático" del dispositivo móvil, omitiendo el resto de mecanismos de seguridad existentes, como el código de acceso, huella dactilar digital, etc., bajo ciertas circunstancias como, por ejemplo, si detecta la cara o la voz registradas por el usuario (en concreto, por el usuario considerado por Android el propietario del dispositivo, en dispositivos multi-usuario).

468. Toda la información asociada a este servicio se describe en la "Guía CCN-STIC-453E - Seguridad de dispositivos móviles: Android 7.x" [Ref.- 407], concretamente en el apartado "Desbloqueo mediante Smart Lock".

469. Desde el punto de vista de los servicios de Google, la funcionalidad de desbloqueo relevante es la denominada "sitios de confianza".

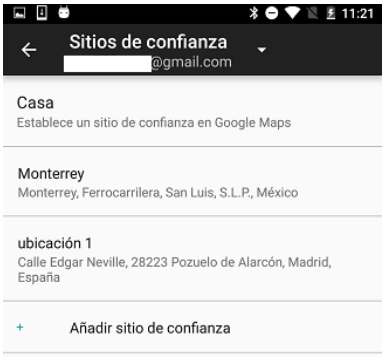
470. "Sitios de confianza": permite mantener el dispositivo móvil desbloqueado cuando el dispositivo detecta que se encuentra en una ubicación considerada de confianza, que ha debido ser previamente configurada, como por ejemplo, el domicilio o el lugar de trabajo del usuario. Este método está disponible únicamente para dispositivos móviles que cuentan con un módulo GPS integrado. Hay que reseñar que el dispositivo no se desbloqueará al entrar en el radio de cercanía del sitio de confianza, sino que únicamente se mantendrá desbloqueado si ya se encontraba en una ubicación de confianza, y permanece dentro de ésta.

471. Dado que el servicio de ubicación no es cien por cien preciso, la función sitios de confianza puede mantener el dispositivo desbloqueado en un radio de hasta 80 metros. Por esta razón, desde el punto de vista de seguridad, se desaconseja hacer uso de esta funcionalidad especialmente en lugares públicos, como el centro de trabajo, cafetería, restaurante, biblioteca, gimnasio, etc., pues el dispositivo móvil podría quedar accesible para un tercero no autorizado.

472. Otro aspecto importante a tener en cuenta desde el punto de vista de seguridad es que las señales de ubicación o localización se pueden copiar y/o manipular, por lo

que un hipotético atacante podría utilizar equipos especializados para desbloquear el dispositivo móvil en lugares que no son de confianza mediante la falsificación o suplantación de la señal GPS, como si realmente lo fueran.

473. Para configurar los sitios de confianza en Smart Lock, hay que acceder al menú Smart Lock, se solicitará el código de acceso al dispositivo, y la opción "Sitios de confianza - Añadir un sitio de confianza".



474. Para activar esta funcionalidad el dispositivo informa al usuario de que es requisito indispensable disponer de conexión a Internet, ya que, a la hora de añadir un sitio de confianza, se descargará la información de mapas para identificar el sitio a añadir.

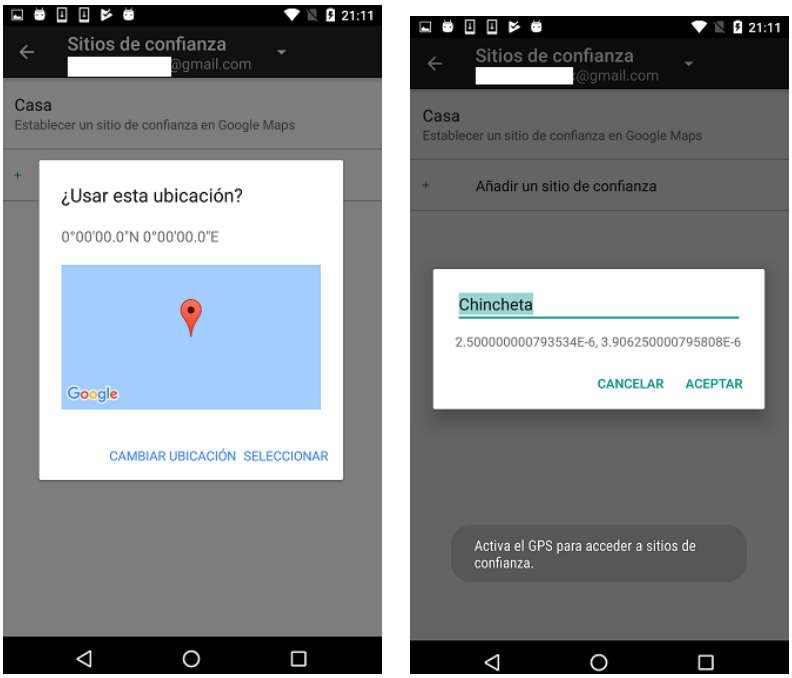
475. Si el servicio de ubicación no está activo, el dispositivo móvil también informa al usuario de que es necesario activarlo mediante un mensaje Toast: "Activa el GPS para acceder a sitios de confianza" para hacer uso de la funcionalidad de sitios de confianza. No obstante, no es necesario activarlo para registrar un nuevo sitio de confianza, por lo que se podría posponer su activación y activar los servicios de ubicación más adelante, a la hora de hacer uso de la funcionalidad de sitios de confianza.

476. Si el servicio de ubicación no está activo, el usuario puede buscar la dirección de interés desplazándose manualmente por el mapa mostrado, o introduciendo los detalles de la dirección en el campo de búsqueda de la parte superior.

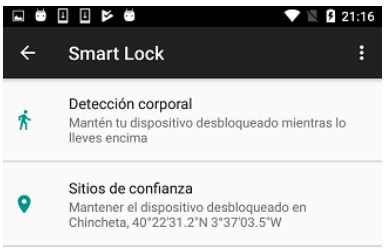
477. Tras disponer de los requisitos necesarios, aparece el menú "Elegir un sitio", que muestra un mapa de "Google Maps", con la ubicación actual si el servicio de ubicación está activo (y sobre el Ecuador si no lo está).

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

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



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



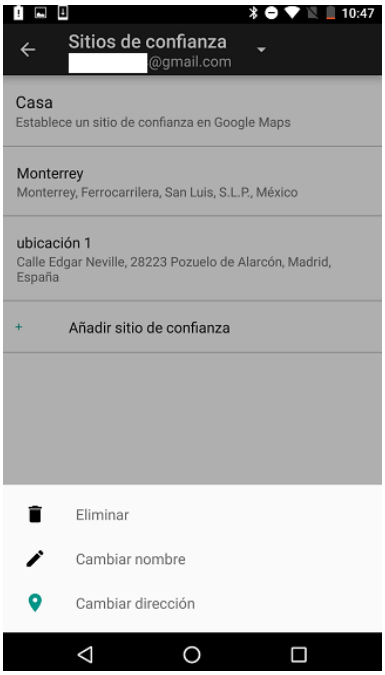
481. La configuración y detalles de los sitios de confianza se almacena en la cuenta de Google del usuario que esté realizando la configuración del sitio de confianza en Smart Lock, y que es mostrada en la parte superior de la pantalla de configuración de "Sitios de confianza".

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

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

484. Para eliminar un sitio de confianza, se ha de pulsar brevemente sobre el marcador del sitio que se muestra en el listado del menú "Smart Lock - Sitios de confianza".

Como resultado aparecerá un menú en la parte inferior de la pantalla con varias opciones, como cambiar el nombre, editar la dirección o eliminar el sitio.



10.6. DESBLOQUEO MEDIANTE LA CUENTA DE USUARIO DE GOOGLE

485. En versiones de Android 4.x y anteriores, existía la posibilidad de restablecer el código de acceso de un dispositivo móvil a través de la cuenta de usuario de Google o a través del administrador de dispositivos de Android (ver apartado 10.4. "Gestión remota de dispositivos Android por parte del usuario").

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

10.7. RESTAURACIÓN DEL CÓDIGO DE ACCESO

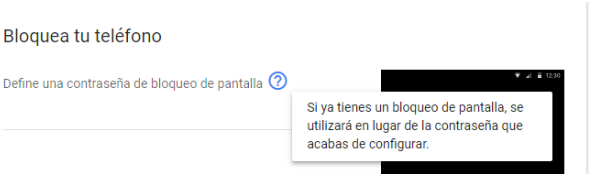
487. A través de las capacidades empresariales para la gestión de dispositivos móviles basados en Android proporcionadas por Google, y específicamente a través de la plataforma Google Apps (ver apartado 10.4. "Gestión remota de dispositivos Android por parte del usuario"), es posible llevar a cabo de forma remota la restauración (restablecimiento o reseteo) del código de acceso y desbloqueo del dispositivo móvil desde la versión 2.2 de Android, disponiendo de la app "Google Apps Device Policy"[16] instalada [Ref.- 13].

488. Esta funcionalidad sólo está disponible para los clientes de Google Apps en la categoría de Negocios (Business) que utilizan G Suite (ver apartado "Gestión empresarial de dispositivos móviles basados en Android" de la "Guía CCN-STIC-453E - Seguridad de dispositivos móviles: Android 7.x" [Ref.- 407]).

[16] https://play.google.com/store/apps/details?id=com.google.android.apps.enterprise.dmagent

489. El resto de usuarios que disponen de una cuenta de usuario de Google individual pueden hacer uso de la funcionalidad "Encontrar mi dispositivo" (ver apartado "10.4. Gestión remota de dispositivos Android por parte del usuario"), con funcionalidad similar pero que no dispone de las capacidades para restaurar el código de acceso del dispositivo móvil, sino únicamente de "Reproducir sonido" (si se piensa que el dispositivo está en una ubicación dónde la emisión de sonido pueda ayudar a localizarlo), "Habilitar bloqueo y borrado" (bloquea la pantalla y permite que se añada un mensaje personalizado) y "Borrar" (equivalente a realizar un reseteo remoto a fábrica) [Ref.- 61].

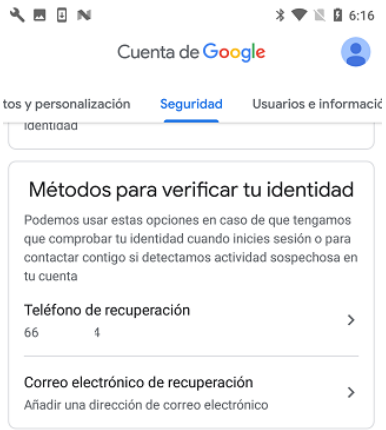
490. La funcionalidad "Encontrar tu móvil", aunque dispone de la opción "Bloquea tu teléfono", solo permite añadir un código de bloqueo si el dispositivo carecía de él. En caso contrario, no se modificará el vigente, tal como se indica en el mensaje correspondiente:



10.8. RECUPERACIÓN DE LA CONTRASEÑA DE GOOGLE

491. El olvido de la contraseña de usuario de Google puede suponer un inconveniente, tanto mayor cuantos más servicios de los asociados a ella se utilicen por parte del usuario.

492. Para poder restaurar la contraseña en ese caso, la sección "Seguridad" de la cuenta de usuario de Google ofrece el apartado "Métodos para verificar tu identidad", que, además de poder ser empleados por Google en caso de identificarse una actividad anómala, se pueden utilizar por el usuario para restablecer la contraseña.



493. Se recomienda configurar ambos métodos, tanto el teléfono de recuperación, como el correo electrónico de recuperación (que debe ser diferente al asociado a la propia cuenta de Google), a fin de poder restaurar el acceso a la cuenta a la mayor brevedad posible en caso de olvido de las credenciales.

10.9. MÚLTIPLES PERFILES DE USUARIO

494. Toda la información relativa a la gestión de perfiles de usuario en Android se puede consultar en el apartado "Múltiples perfiles de usuario" de la "Guía CCN-STIC-453E - Seguridad de dispositivos móviles: Android 7.x" [Ref.- 407].

495. En lo que respecta a la cuenta de usuario de Google, cada usuario diferente puede añadir su propia cuenta de Google al dispositivo móvil (bajo su perfil de usuario en Android), realizando las configuraciones que considere oportunas.

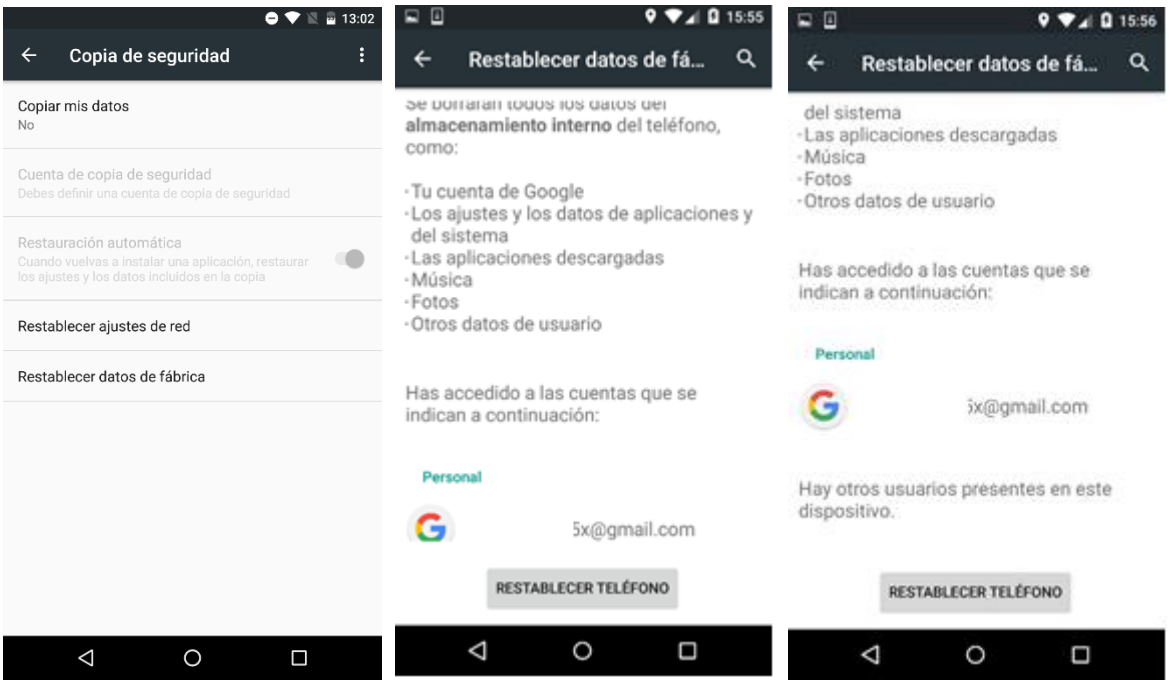
496. El uso de diferentes perfiles de usuario está desaconsejado desde el punto de vista de seguridad. En caso de ser preciso utilizar un dispositivo ajeno, se recomienda eliminar el perfil creado tan pronto finalice su uso, especialmente si se dio de alta la cuenta de usuario de Google en dicho perfil.

497. De cara al préstamo del dispositivo móvil de forma temporal a un tercero, se sugiere valorar la funcionalidad de "Fijar pantalla" (que permite acceso a una única app) frente a crear un perfil para él.

10.10. ELIMINACIÓN DE DATOS DEL DISPOSITIVO MÓVIL

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

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



500. El proceso de restablecimiento eliminará todos los datos del teléfono, incluyendo cuentas de Google, configuración y datos de apps y del sistema, así como apps de

terceros previamente descargadas e instaladas. No se eliminará el software del sistema operativo ni las actualizaciones de sistema ya aplicadas, es decir, el propio Android, ni los datos de las tarjetas de almacenamiento externas. También se eliminarán datos de otros usuarios si se han empleado las capacidades multi-usuario descritas en el apartado "10.9. Múltiples perfiles de usuario".

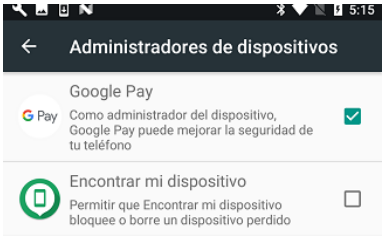
501. Para confirmar esta operación crítica es necesario introducir el código de acceso tras seleccionar el botón "Restablecer teléfono" de la pantalla que informa de que se borrarán todos los datos. Si existen otros usuarios en el dispositivo móvil, también se informará de este hecho por si se desea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

502. Estas capacidades de borrado de datos local también pueden ser activadas tras llevarse a cabo un número determinado de intentos de acceso incorrectos, pudiendo configurarse a través de las políticas de seguridad de los mecanismos de gestión empresarial de dispositivos móviles Android.

503. Las aplicaciones administradoras del dispositivo móvil pueden ser activadas o desactivadas en función de las necesidades del usuario. Antes de su ejecución, siempre verificarán si están activadas, y en caso de no estarlo, solicitarán al usuario su activación. Para verificar el estado de dichas aplicaciones, se puede acceder al menú "Ajustes - [Personal] Seguridad - [Administración del dispositivo] Administradores de dispositivos".

504. Además de mediante las capacidades de gestión empresarial de dispositivos móviles, el propietario de un dispositivo que lo haya asociado a su cuenta de usuario de Google puede efectuar labores de gestión remota (incluyendo el borrado de datos del dispositivo) siguiendo las indicaciones descritas en el apartado "10.4. Gestión remota de dispositivos Android por parte del usuario".

505. En Android 6.x, se incorporó "Android Pay" como un administrador de dispositivos. El objeto es permitir que los datos almacenados como medio de pago en Android Pay puedan ser borrados de forma remota en caso de pérdida o robo del dispositivo móvil, protegiendo así al usuario. En Android 7.x, "Android Pay" fue sustituido por "Google Pay", que también se incorpora como administrador de dispositivos:



11. LOCALIZACIÓN (O UBICACIÓN) GEOGRÁFICA

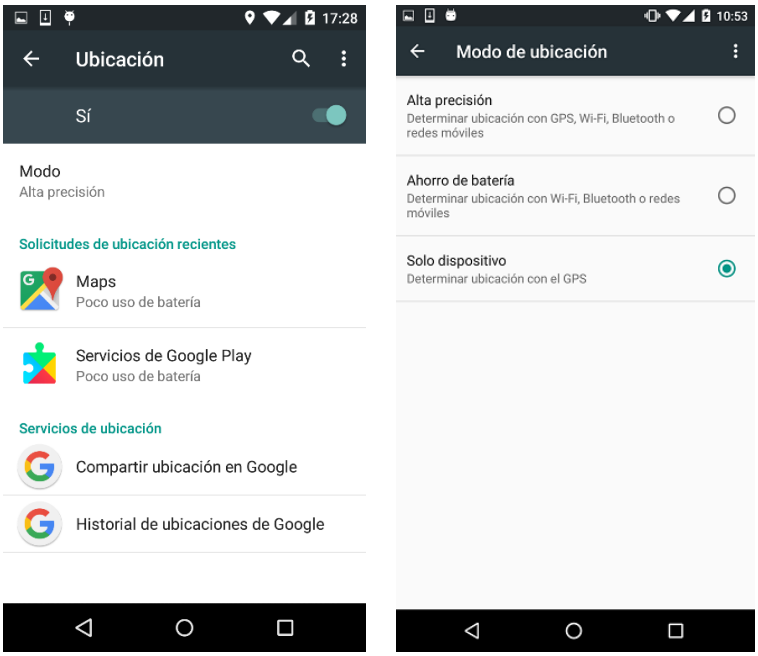
506. Las capacidades de localización (o ubicación) del dispositivo móvil a través del módulo de GPS, o de las redes de datos (telefonía móvil y Wi-Fi), pueden ser activadas y desactivadas por el usuario en función de su utilización.

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

508. En ese momento, y si el servicio de ubicación está activo, se mostrará un icono en la parte derecha de la barra de estado similar a una gota de agua invertida.

509. Si ninguna app hace uso del servicio de localización en ese instante, aunque la ubicación esté activa no se mostrará ningún indicador en la barra de estado. Ello dificulta que el usuario sea consciente de esa circunstancia.

510. Las capacidades de localización del dispositivo móvil se habilitan a través del interruptor "[SI | NO]" desde el menú "Ajustes [Personal] - Ubicación.



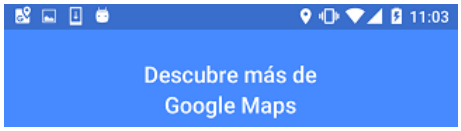
511. Desde Android 4.4 (KitKat) se proporciona un mayor control sobre los diferentes modos de localización (o ubicación) disponibles [Ref.- 149]: alta precisión, ahorro de batería o solo en dispositivo.

512. Las opciones disponibles para seleccionar el modo de localización son:

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

513. La nueva funcionalidad y API empleada por las apps para acceder a los servicios de localización, especialmente al usar el modo "Ahorro de batería", reduce drásticamente el consumo de batería. Previamente, cada app que necesitaba hacer uso de los servicios de localización despertaba al módulo GPS hardware y obtenía su información de ubicación propia individualmente.

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



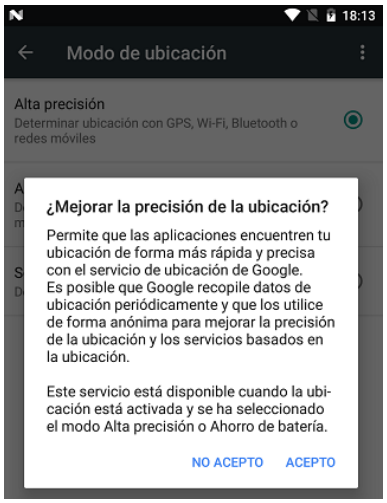
515. Todos estos modos están disponibles en los servicios de ubicación de Google, que extienden las capacidades del módulo GPS del dispositivo móvil con otras tecnologías.

516. La opción (o modo) habilitada por defecto dependerá de las opciones seleccionadas en la pantalla de "Ubicación y Google" durante el proceso inicial de instalación y configuración del dispositivo móvil (ver apartado "23. Apéndice A: Proceso de instalación y configuración inicial").

517. La activación del modo avión de Android deshabilitará los servicios de ubicación, no permitiendo ninguna transmisión inalámbrica ni con los satélites GPS, ni con las redes Wi-Fi o de telefonía móvil, ni con dispositivos Bluetooth.

518. Desde el punto de vista de seguridad, si se desea que no se genere ningún tráfico desde el dispositivo móvil hacia los servicios de Google, se recomienda seleccionar la opción o modo "Solo en dispositivo", pese a que tenga asociado un mayor consumo de batería y tarde más tiempo en localizar la ubicación del dispositivo inicialmente.

519. En el caso de habilitar las capacidades de localización a través de redes y conexiones inalámbricas (Wi-Fi, Bluetooth y telefonía móvil), mediante la selección de los modos "Alta precisión" o "Ahorro de batería", Android solicitará confirmación por parte del usuario para recopilar los datos de las señales inalámbricas recibidas y la ubicación del terminal de forma anónima:



Nota: Existen estudios pasados que reflejan que la información de localización intercambiada entre el dispositivo móvil Android y Google no es completamente anónima, ya que, aparte de incluir detalles de las señales de las redes inalámbricas recibidas y la ubicación del terminal, se incluye un identificador único del dispositivo móvil [Ref.- 83], lo cual puede afectar a la privacidad del usuario.

Adicionalmente, la información de las redes Wi-Fi recopilada por Google a través de los coches del programa StreetView y de los dispositivos móviles Android estuvo disponible

en el pasado para su consulta a través de la API de Google y de páginas web externas [Ref.- 84], siendo posible conocer la ubicación de una red Wi-Fi a nivel mundial en base a su dirección MAC o BSSID. El acceso a través de este servicio no está disponible actualmente de manera pública.

520. Es posible consultar las apps que han solicitado información sobre la ubicación del dispositivo móvil recientemente a través del menú "Ajustes [Personal] - Ubicación", y de la sección "Solicitudes de Ubicación Recientes".

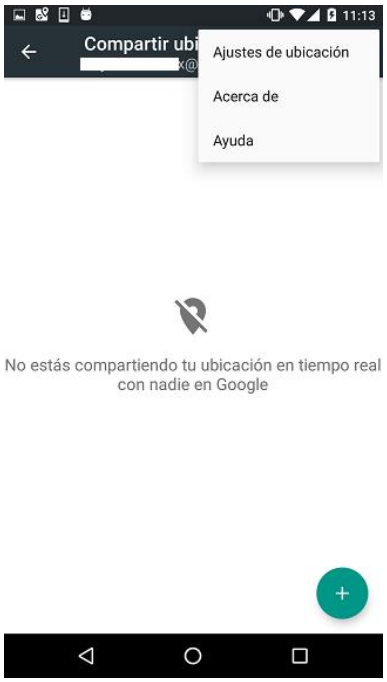
521. Mediante la selección de una app de la lista se accede a la información de la app (información también disponible desde el menú "Ajustes [Dispositivo] - Aplicaciones - Todas"), incluyendo su uso de batería, permisos, uso de almacenamiento, etc.

522. Adicionalmente, una vez se ha configurado una cuenta de usuario de Google en el dispositivo móvil, a través del menú "Ajustes [Personal] - Ubicación", y de la sección "Servicios de Ubicación", es posible seleccionar "Historial de ubicaciones de Google" y acceder a los ajustes de configuración para activar o desactivar los informes de ubicación y el historial de ubicaciones de la cuenta de usuario de Google (ver apartado "11.5. Historial de ubicaciones").

523. La opción "Ajustes - [Personal] Ubicación - [Servicios de Ubicación] Compartir ubicación en Google" permite ver con quién se está compartiendo la ubicación en un momento concreto.

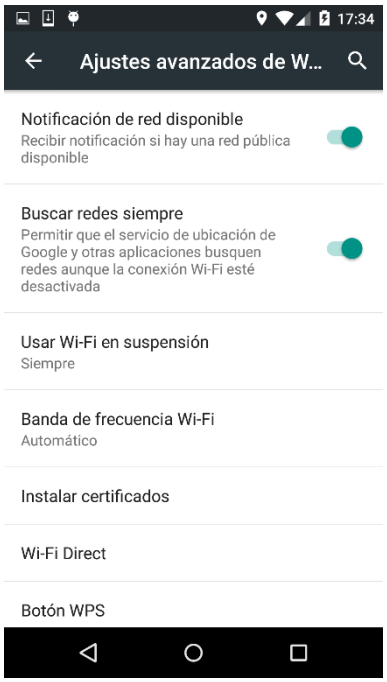
524. La opción de "Compartir ubicación" se habilita en el menú lateral de la aplicación "Google Maps". Esta opción requiere disponer de una conexión de datos.

525. Cuando se selecciona, aparecerá un menú que permite especificar el tiempo durante el cual se compartirá la ubicación, así como los contactos con los que se desea compartir (que deben poseer también una cuenta de usuario de Google). Es posible incluso crear un enlace que se puede enviar a través de aplicaciones de mensajería, Bluetooth, etc., de modo que los contactos elegidos o que reciban el enlace puedan realizar el seguimiento en tiempo real de la posición del dispositivo en un mapa. Por este motivo y debido a las implicaciones en la privacidad, una vez se comparte la ubicación con alguien, el usuario recibirá una notificación informándole de ello a modo de recordatorio. Para más detalles, consultar el apartado "12.2. Google Maps".

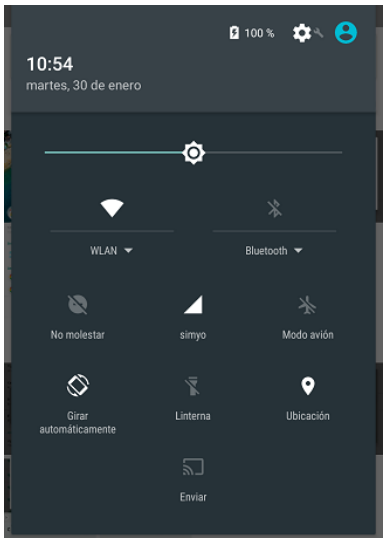


526. Adicionalmente, si se hace uso de alguno de los modos que emplean las redes Wi-Fi para obtener información sobre la ubicación del dispositivo móvil, es posible configurar si se permite el uso de las capacidades Wi-Fi del dispositivo móvil para estos servicios y, en concreto, para la búsqueda e identificación de redes Wi-Fi, aunque la conexión o el interfaz Wi-Fi esté desactivado.

527. Esta opción de configuración también está disponible en el proceso de instalación y configuración inicial del terminal, ver apartado "23. Apéndice A: Proceso de instalación y configuración inicial"), y se puede acceder a la misma posteriormente desde el menú "Ajustes - [Conexiones Inalámbricas y Redes] Wi-Fi - [...] - Ajustes avanzados - Buscar redes siempre":



528. Por último, la activación de los servicios de ubicación en el dispositivo móvil también está disponible a través de los ajustes rápidos, accesibles desde la barra superior de estado:



529. Para que el servicio "Encontrar mi dispositivo" (consultar apartado "8.1. Gestión remota de dispositivos Android por parte del usuario") esté operativo, es requisito indispensable que las capacidades de ubicación estén activas.

530. Se recomienda valorar el uso de las capacidades de localización del dispositivo móvil, buscando el equilibrio entre privacidad y funcionalidad. En caso de querer hacer uso de sus capacidades y evitar otras implicaciones de privacidad, se recomienda activar únicamente la localización mediante GPS, no haciendo uso de las capacidades de localización mediante redes Wi-Fi o redes de telefonía móvil.

531. En noviembre de 2017, la empresa Quartz publicó un informe en el que desvelaba que, desde el comienzo de dicho año, todos los dispositivos móviles Android recolectan información sobre la ubicación de las torres de telefonía móvil cercanas, y que envían esos datos a Google cuando se conectan a Internet, incluso aunque los servicios de ubicación hayan sido deshabilitados por el propietario del terminal. Google confirmó esta información alegando que los datos no se almacenaban, sino que se empleaban para mejorar el servicio de mensajes y notificaciones. En el momento de elaboración de la presente guía, no existe ninguna opción para deshabilitar este comportamiento en el dispositivo móvil, ni se incluye referencia alguna a esta práctica en la política de privacidad de Google [Ref.- 252].

11.1. SERVICIOS DE UBICACIÓN DE GOOGLE

532. Durante el proceso de configuración inicial del dispositivo móvil empleado para la elaboración de la presente guía, Android solicita al usuario si desea usar los servicios de ubicación de Google, incluso aunque se haya declinado la asociación del dispositivo a una cuenta de usuario de Google.

533. Las opciones disponibles "Usar el servicio de ubicación de Google" y "Ayudar a mejorar los servicios de ubicación" están habilitadas por defecto, por lo que se recomienda desactivarlas hasta determinar el uso que se desea hacer de ellas (ver apartado "23. Apéndice A: Proceso de instalación y configuración inicial").

534. Los servicios de ubicación o localización de Google (Google Location Services), permiten a las apps conocer la ubicación geográfica aproximada del dispositivo móvil, y por tanto del usuario, aun sin disponer de señal GPS, y hacer uso de esa información en los servicios de búsqueda (y otros servicios) de Google, o desde

cualquier app con los permisos adecuados, teóricamente de una forma más rápida y precisa.

535. La ubicación se obtiene a través de la información de localización disponible sobre torres (o redes) de telefonía móvil y redes Wi-Fi, y la señal recibida en cada momento por el dispositivo móvil para ambas tecnologías (telefonía móvil y Wi-Fi), en lugar de emplear información más precisa como la proporcionada por el dispositivo o módulo GPS.

536. Para hacer uso de la geolocalización en base a redes Wi-Fi, el dispositivo escaneará los puntos de acceso Wi-Fi que estén en su rango de alcance (independientemente de su nivel de seguridad) y, en base a las respuestas recibidas, y tras enviar los detalles a los servicios de Google, la respuesta obtenida por parte de estos le permitirá interpolar su ubicación aproximada.

537. El servicio de ubicación a través de Bluetooth se basa en el uso de las denominadas balizas Bluetooth LE y la tecnología conocida como beacons. Un beacon es un dispositivo inalámbrico que envía periódicamente un anuncio BLE (Bluetooth Low Energy) con su identificador, de forma que una app pueda extraer su ubicación a través de una base de datos con la posición de estas balizas. El dispositivo móvil recibe ese anuncio y la app (o el servicio de ubicación del sistema operativo) puede determinar así la ubicación aproximada.

538. Las dos principales (aunque no las únicas) tecnologías de beacons que existen actualmente en el mercado son iBeacon (de Apple) [Ref.- 254] y EddyStone (de Google) [Ref.- 255].

539. La utilización de los servicios de ubicación de Google puede conllevar por tanto el envío, supuestamente anónimo, a Google de los datos recopilados sobre las redes Wi-Fi, de telefonía móvil y de dispositivos Bluetooth basados en tecnologías basadas en beacons sobre la ubicación aproximada en la que se encuentra el dispositivo móvil, incluso aunque no se esté utilizando ninguna app.

540. El servicio Google Nearby (ver apartado "15.9. Google Nearby") también realiza acciones de localización, utilizando escaneos Wi-Fi, Bluetooth y BLE, incluso aunque ambos interfaces hayan sido deshabilitados a propósito por el usuario.

541. En resumen, estas peticiones de información hacia Google pueden desvelar información de las redes Wi-Fi, de telefonía móvil y de las balizas BLE existentes en el área de cobertura del dispositivo móvil, así como otros detalles relevantes del terminal, potencialmente a cualquiera que esté capturando el tráfico de datos generado desde el dispositivo móvil. Las respuestas de los servicios de ubicación de Google, en formato binario, contienen información de la ubicación estimada del dispositivo móvil.

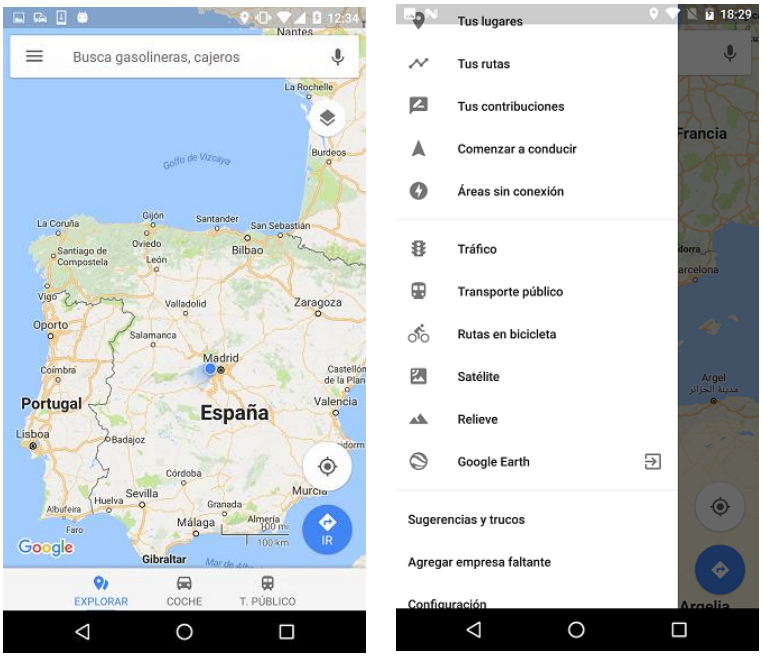
542. Se recomienda limitar el uso de estos servicios, especialmente a través de redes de datos inseguras, por parte de cualquier app como por ejemplo "Google Maps" (ver siguiente apartado), y específicamente su utilización cuando se emplea algo más que el módulo GPS, ya que los servicios de ubicación de Google a través de torres de telefonía móvil y redes Wi-Fi desvelan detalles privados del dispositivo móvil y de su ubicación.

11.2. GOOGLE MAPS

543. Los servicios de ubicación de Google son utilizados, entre otros, tanto por el propio sistema operativo Android como por las apps disponibles por defecto o proporcionadas por terceros, como por ejemplo la app "Maps" o "Google Maps" (https://maps.google.com) que, en el caso del dispositivo móvil empleado para la elaboración de la presente guía, está disponible como app por defecto a través de la app "Maps" (disponible desde el *Launcher*).

544. Tras aceptar los términos y condiciones del servicio (al ejecutar la app la primera vez), y en función de la configuración de los servicios de ubicación, la recopilación de información será activada y se permitirá su utilización por defecto por parte de las apps que hacen uso de los servicios de ubicación.

545. Desde Maps es posible hacer uso de la información de localización, en concreto, empleando el botón circular con una cruceta, que centrará el mapa en la localización actual del usuario (identificada por un indicador azul). Si el indicador de posición se muestra como un punto gris, significa que Maps no consigue detectar la ubicación actual y está mostrando la última ubicación que determinó anteriormente para el dispositivo móvil.



546. La versión de la aplicación Maps se puede consultar dentro del menú de la app, "Ajustes - Información, condiciones y privacidad".

547. Al hacer uso de apps que requieren conocer la ubicación del usuario, como Maps, y si han sido habilitadas, se emplearán las capacidades para localizar la ubicación del dispositivo móvil incluso cuando no se disponga de módulo GPS (o éste no esté activo o no haya cobertura de los satélites GPS), a través de A-GPS, que emplea la información de localización disponible a través de servicios de terceros (ver apartado "12.3. A-GPS"), y la funcionalidad extendida de los servicios de ubicación de Google descritos previamente, haciendo uso de la información de las redes Wi-Fi, las balizas BLE y las torres de telefonía móvil.

548. Los servicios de ubicación de Google integrados en Google Maps, así como los datos e información obtenida por la app (mapas, información extra, etc.), en el caso de la

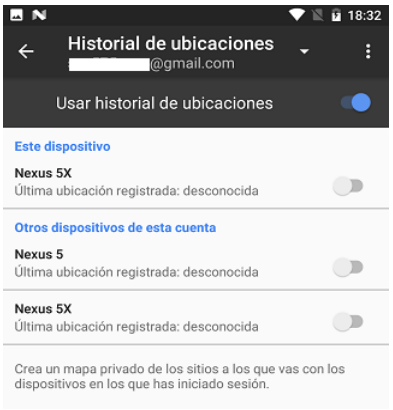
versión 9.82.2 de la app Maps (empleada en la elaboración de la presente guía) emplean únicamente conexiones mediante HTTPS (cifradas) desde el dispositivo móvil hacia múltiples servidores de Google. Versiones pasadas de los servicios de localización de Google enviaban tráfico no cifrado mediante HTTP.

549. Este cambio en el funcionamiento respecto al comportamiento de versiones previas de la app y versiones previas de Android evita que un potencial atacante acceda fácilmente al tráfico de red y pueda obtener detalles de la ubicación del usuario y de las redes inalámbricas (como por ejemplo el nombre de red, SSID, y su dirección MAC, BSSID) y de las torres de telefonía móvil (como por ejemplo el identificador de torre, y los códigos de área (LAC), operador de telefonía móvil (MNC) y país (MCC)) existentes en el área de cobertura del dispositivo móvil.

550. En versiones de Google Maps anteriores a 2017, se requería disponer de una conexión de datos (telefonía móvil o Wi-Fi) para funcionar y acceder a la información cartográfica de los mapas. Sin embargo, una de las capacidades que se añadieron a la aplicación Maps fue la de "zonas sin conexión", que posibilita la navegación aunque no haya conexión de datos activa si se ha descargado previamente el mapa correspondiente a esa zona. Todos los detalles sobre el uso y configuración de las zonas sin conexión pueden consultarse en [Ref.- 227].

551. A partir de la versión 9.12 de Google Maps para Android, se incorporó la opción de menú "Tu cronología" [Ref.- 228].

552. Para crear la cronología, además de la ubicación, el historial de ubicaciones debe estar activo en "Ajustes - [Personal] Ubicación - [Servicios de ubicación] Historial de ubicaciones de Google" (consultar apartado "11.5. Historial de ubicaciones"). Dado que esta opción se habilita para la cuenta de Google del usuario, el activarla implica que Google recordará la ubicación en todos los dispositivos en los que se inicie sesión con esa cuenta de usuario de Google. No obstante, se puede desactivar la opción correspondiente al dispositivo móvil si no se desea que los datos que se recopilen de él pasen a formar parte del historial de ubicaciones:

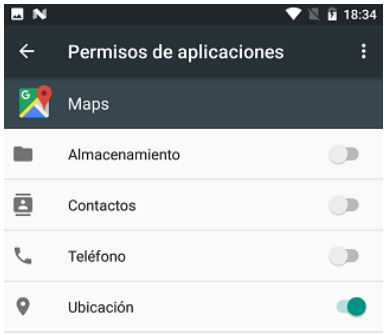


553. Se enviarán a Google datos de ubicación de los dispositivos que tengan activa la opción del historial de ubicaciones, aunque no se esté utilizando ningún producto de Google.

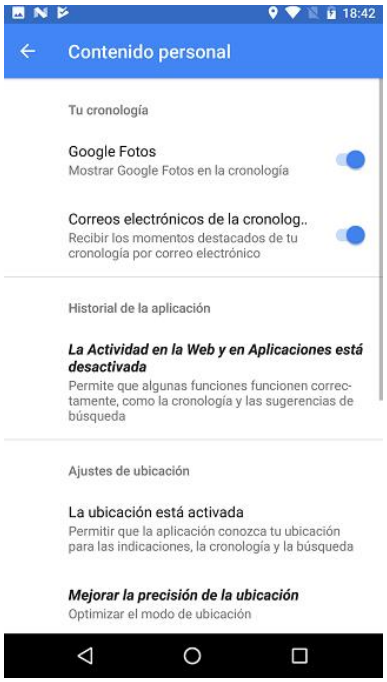
554. Si los servicios de ubicación están activos, el dispositivo móvil compartirá la ubicación con las aplicaciones que tengan permiso para ello.

555. Con el cambio en el modelo de permisos de Android, la aplicación Maps dejó de tener concedidos por defecto permisos muy sensibles, como "inhabilitar el bloqueo

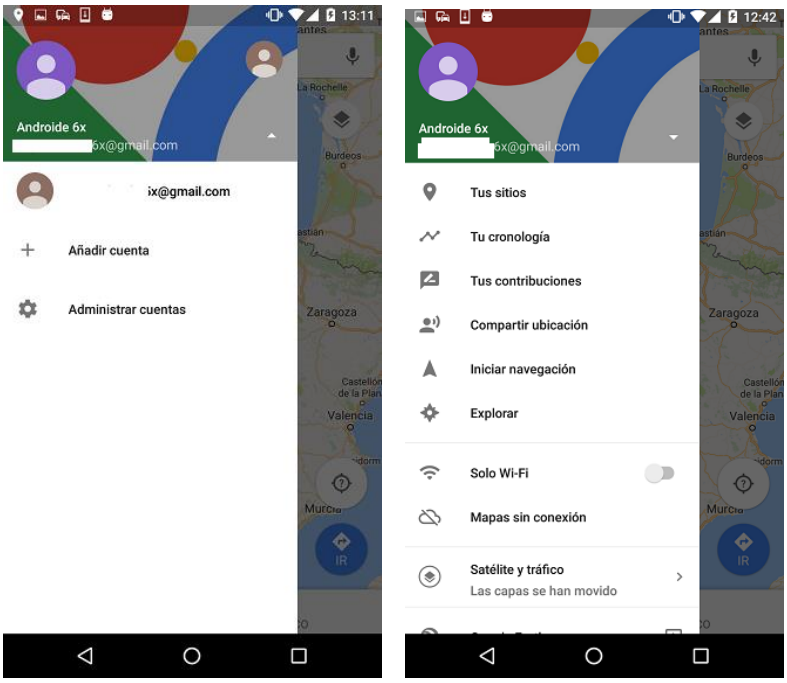
de pantalla", "añadir o eliminar cuentas", "editar o borrar el contenido de USB". Para verificar qué permisos tiene concedidos en un momento dado en el dispositivo móvil, se recurrirá a "Ajustes - [Dispositivo] Aplicaciones - Maps - Permisos". Para evitar potenciales vulnerabilidades de seguridad, se recomienda mantener la app actualizada y conceder únicamente el permiso de ubicación, que es el único que requiere para su correcto funcionamiento:



556. Hay que resaltar que estos permisos hacen referencia a permisos de sistema, no a las capacidades que tiene la aplicación Maps para interactuar con otros servicios de Google (como Google Fotos) y que afectan directamente a la privacidad del usuario. Por ejemplo, la opción "Correos electrónicos de la cronología" disponible en "Maps - Ajustes - Contenido personal", marcada por defecto, hará que Maps envíe periódicamente información al e-mail del usuario relacionada con los sitios visitados:



557. Si el dispositivo móvil tiene varias cuentas de usuario de Google dadas de alta, es posible seleccionar qué cuenta se utilizará para la actividad registrada por la app Maps. Para cambiar entre cuentas (o añadir una nueva), se deben abrir los ajustes de Maps y seleccionar la cuenta a emplear (en versiones anteriores de Google Maps, era preciso marcar la opción "Cerrar sesión en Google Maps" para poder acceder a la configuración de otra cuenta). Desde el menú desplegable de las cuentas dadas de alta en Maps es posible también añadir cuentas adicionales:



558. La cuenta de usuario que está siendo utilizada por la app Maps es la que se muestra en la parte superior del menú de "Ajustes de Maps", que figura tras el icono de un rostro.

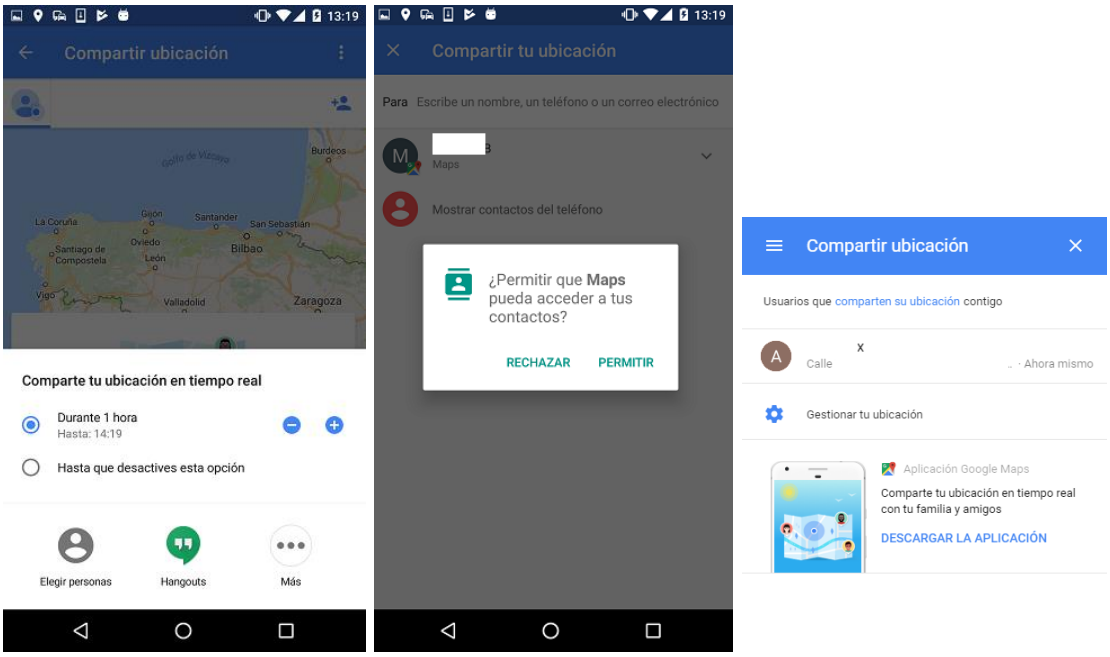
559. Dada la sensibilidad de los datos que pueden recopilarse mediante Google Maps, y para preservar la privacidad del usuario, se recomienda deshabilitar el historial de ubicaciones y eliminarlo si ha estado activo en algún momento. Para ello, se puede acceder al menú "Ajustes [Personal] - Ubicación [Servicios de ubicación] Historial de ubicaciones de Google" o emplear el menú "Ajustes de Maps - Ajustes de ubicación de Google".

560. Adicionalmente, si durante el uso de Maps se presenta el siguiente mensaje, se recomienda pulsar en "Omitir":

561. Una opción que se añadió a la app Maps en las versiones posteriores a marzo del 2017 fue la de "Compartir ubicación" [Ref.- 230], que permite que el usuario comparta su posición geográfica con los contactos de su elección.

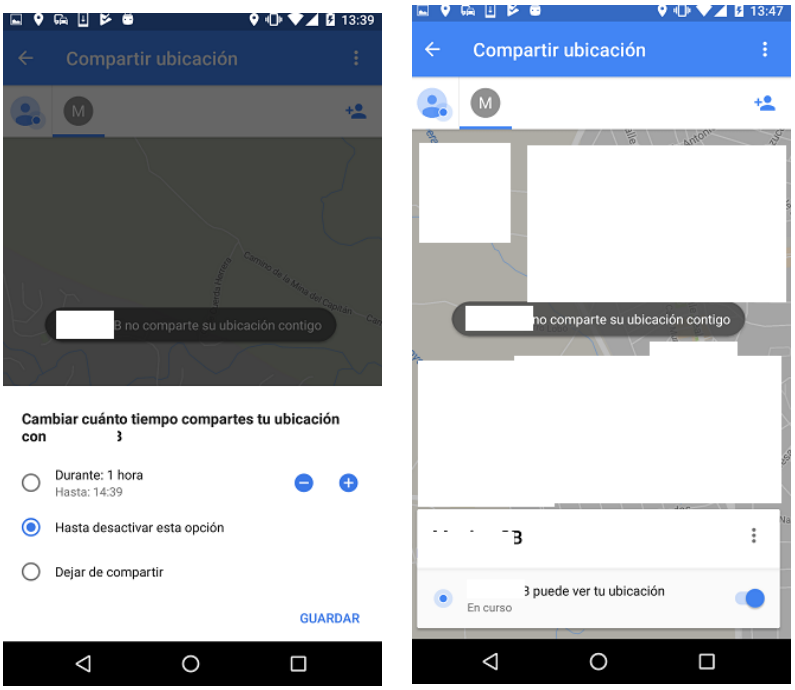
562. Dicha opción permite conceder permisos para ver la ubicación en tiempo real del dispositivo durante el tiempo especificado por el usuario. Esta opción se habilita a través del menú de la app Maps denominado "Compartir ubicación".

563. Durante el proceso de compartición de ubicación, Maps solicitará al usuario acceso a sus contactos en el teléfono. Es importante reseñar que, aunque este permiso no se conceda, y que, por tanto, los contactos no se puedan recopilar de los contactos del teléfono, Maps sí tendrá acceso a los contactos que el usuario haya añadido a su cuenta de usuario de Google. Por tanto, el denegar acceso a los contactos no implica que la app Maps pueda consultarlos a través de la cuenta de usuario de Google activa:

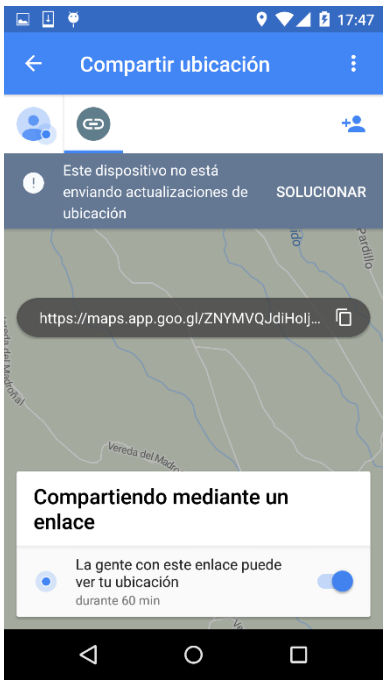


564. Si se desea compartir la ubicación con un contacto, éste ha de disponer de una cuenta de usuario de Google. En ese caso, el usuario con el que se ha compartido la ubicación recibirá un mensaje de correo en su cuenta de Gmail que le informa de que otra persona ha compartido su ubicación con él:

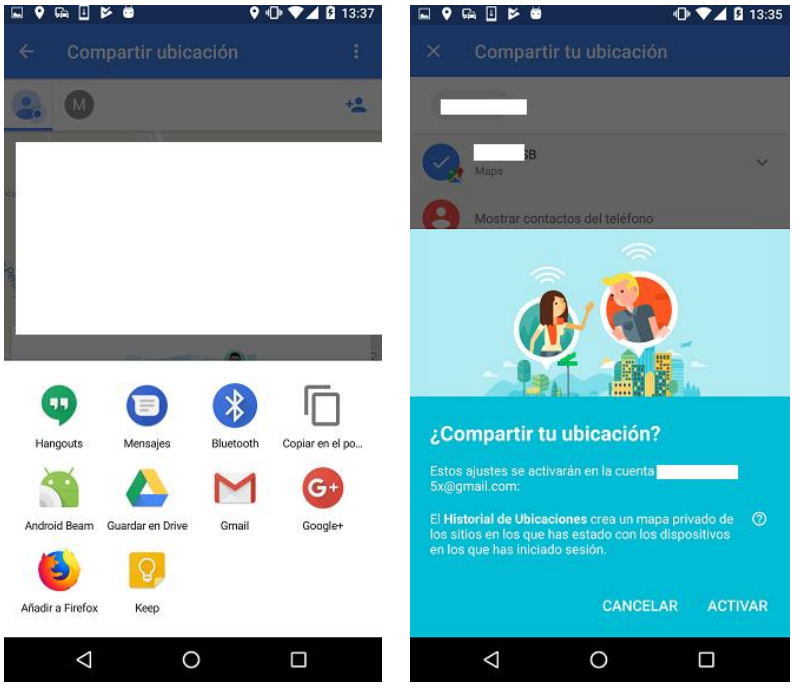
565. En versiones anteriores de Maps, la compartición de la ubicación con otros usuarios tenía una duración de 1 hora (por defecto) y de un máximo de 72 horas. En la versión empleada para la elaboración de la presente guía, no hay un máximo de tiempo definido, sino un interruptor que desactiva la compartición:



566. Si el contacto no dispone de una cuenta de usuario de Google o no se desea hacer uso de ella para acceder a la ubicación del dispositivo, se ha de crear un enlace mediante el menú de la app Maps, "Compartir ubicación - Más - Copiar en el portapapeles". Seguidamente, se puede compartir el enlace creado mediante la aplicación o servicio que se desee, y así se dará acceso a la ubicación durante un máximo de 1 hora.



567. Es posible también elegir una aplicación de mensajería instalada en el dispositivo móvil para compartir la ubicación seleccionando la misma a través del menú de la app Maps, "Compartir ubicación - Más - [seleccionar la aplicación de la lista mostrada]".



568. Para poder compartir la ubicación, es necesario habilitar el historial de ubicaciones, tal como se informa en el mensaje que aparece al intentar compartir la ubicación (ver imagen superior derecha).

569. Las opciones de uso de la opción "Compartir ubicación" están disponibles en la ayuda oficial de Google Maps en tiempo real [Ref.- 231].

570. Por cuestiones de privacidad, se recomienda no hacer uso de esta funcionalidad. En caso de requerirse por alguna circunstancia, se debe verificar que el canal de compartición es seguro y limitar el acceso en tiempo a la misma todo lo posible.

571. Por cuestiones de privacidad, no se recomienda en absoluto dar de alta la dirección de casa o del trabajo en el área de "Ajustes de Mapa - Ajustes - Editar casa o trabajo".

572. El resto de opciones de uso de la app Maps para navegación quedan fuera del alcance de la presente guía, pero se puede obtener información detallada al respecto en la "Ayuda de Google Maps" [Ref.- 229].

11.3. A-GPS

573. Assisted GPS (A-GPS o aGPS) es un sistema de ayuda para mejorar la obtención de información y la precisión de los datos de localización obtenidos mediante GPS, que permite disponer de una estimación de la ubicación del dispositivo móvil más rápidamente.

574. Especialmente A-GPS permite agilizar significativamente el tiempo necesario para ubicar inicialmente el dispositivo móvil, parámetro conocido como TTFF (Time-To-First-Fix).

575. El módulo A-GPS está (teóricamente) disponible en dispositivos móviles Android con GPS, especialmente cuando se hace uso del modo de alta precisión.

576. El sistema A-GPS es un sistema híbrido que se basa en obtener información de las torres de telefonía móvil detectadas desde la ubicación del dispositivo móvil (y que proporcionan información auxiliar o de asistencia sobre la ubicación), y

adicionalmente, hace uso de las conexiones de datos (habitualmente 2/3/4G, o Wi-Fi) del dispositivo móvil para obtener información actualizada de dónde se encuentran los diferentes satélites GPS en un momento temporal (información con datos de las órbitas y de sincronización - reloj - de los satélites, conocido también como almanaque).

577. Por tanto, la funcionalidad A-GPS también es visible a través del tráfico de datos del dispositivo móvil. Android 6.x, en diferentes momentos temporales como por ejemplo durante el proceso de arranque del dispositivo móvil, envía tráfico no cifrado hacia los servidores de gpsOneXTRA (ver apartado "12.4. gpsOneXTRA").

578. Debe tenerse en cuenta que, pese a que el uso del módulo GPS está siempre habilitado por defecto si los servicios de ubicación están activos, salvo que se haga uso del modo de ahorro de batería, hay escenarios en los que no es posible obtener señal de GPS (por ejemplo, en el interior de edificios), por lo que las apps como Maps harán uso automáticamente de las capacidades de ubicación sin hacer uso del módulo GPS si estas han sido habilitadas, por ejemplo, en el modo de alta precisión.

579. En resumen, se recomienda deshabilitar la funcionalidad A-GPS mediante la activación del modo "Solo en dispositivo" salvo que se quiera hacer uso explícito de estas capacidades, con el objetivo de evitar desvelar información de la ubicación del dispositivo móvil (por ejemplo, torres de telefonía móvil o redes Wi-Fi cercanas) a través del tráfico de datos cifrado destinado a los servidores de Google.

11.4. GPSONEXTRA

580. Con el objetivo de agilizar el proceso de localización, complementando las coordenadas obtenidas del módulo GPS y su precisión, los dispositivos móviles Android pueden disponer de la funcionalidad asociada a la asistencia mediante gpsOneXTRA (aplicación conocida como QuickGPS en otras plataformas móviles).

581. Hasta Android 5.x inclusive, esta funcionalidad se conectaba a un servidor web del dominio "gpsonextra.net" (xtra1, xtra2 o xtra3) para descargar la información semanal de la localización de los satélites GPS alrededor del planeta (o almanaque). Por defecto, la descarga automática de esta información está habilitada en Android. A partir de Android 6.x, la conexión se realiza con servidores web del dominio "izatcloud.net" (en el ejemplo utilizado para la presente guía, concretamente con el servidor "xtrapath1").

582. La descarga se lleva a cabo mediante los servidores de "izatcloud.net" mencionados previamente, descargándose el fichero "/xtra3grc.bin".

Nota: La configuración interna de Android tanto del servidor de tiempos NTP como de los servidores de gpsOneXTRA y A-GPS (ver apartado "11.3. A-GPS") está disponible en el fichero "/system/etc/gps.conf", aunque no se dispone de ningún ajuste de configuración a través del interfaz gráfico de usuario de Android para modificar estos parámetros. Ejemplo (parcial) del fichero "gps.conf":

```
XTRA_SERVER_1=http://xtrapath1.izatcloud.net/xtra3grc.bin
XTRA_SERVER_2=http://xtrapath2.izatcloud.net/xtra3grc.bin
XTRA_SERVER_3=http://xtrapath3.izatcloud.net/xtra3grc.bin
```

583. Las conexiones gpsOneXTRA ("xtrapathN.izatcloud.net", TCP/80), para incrementar la precisión de localización del GPS, se llevan a cabo (por ejemplo) cada vez que se enciende el dispositivo móvil y éste dispone de acceso a Internet.

584. A finales del año 2016 se identificó una vulnerabilidad de denegación de servicio que afectaba a los dispositivos móviles Android y que podía ser explotada mediante la manipulación de los ficheros de posicionamiento obtenidos mediante el servicio gpsOneXTRA [Ref.- 224].

11.5. HISTORIAL DE UBICACIONES

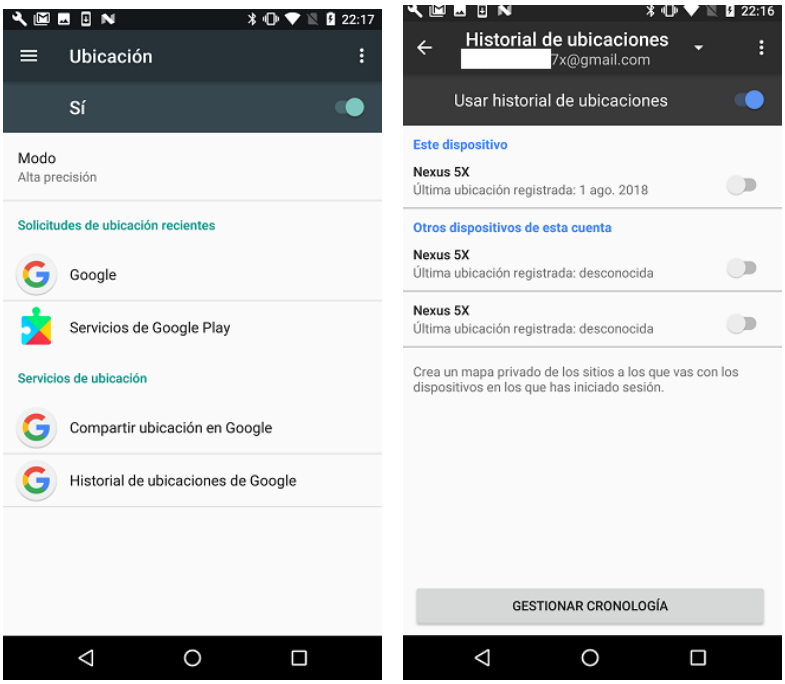
585. Los servicios de Google pueden hacer uso de los datos del historial de ubicaciones para, por ejemplo, mejorar los resultados de búsqueda de Google Maps (mediante la app Maps) en función de los sitios frecuentados habitualmente por el usuario [Ref.- 168].

586. El historial de ubicaciones almacena un registro histórico de la ubicación del usuario procedente de todos los dispositivos móviles en los que el usuario haya iniciado sesión con su cuenta de usuario de Google. Para que se envíe la información al historial, y se pueda almacenar, el dispositivo móvil debe tener habilitado el historial de ubicaciones.

587. El uso de la opción "historial de ubicaciones" permite a Google utilizar (y potencialmente almacenar) periódicamente los datos de ubicación más recientes del dispositivo móvil, así como la información sobre las actividades que conllevan movimiento (conducir, caminar, pasear en bicicleta, etc.) y asociarlos a la cuenta de usuario de Google, incluso aunque no se esté utilizando ningún producto o servicio de Google.

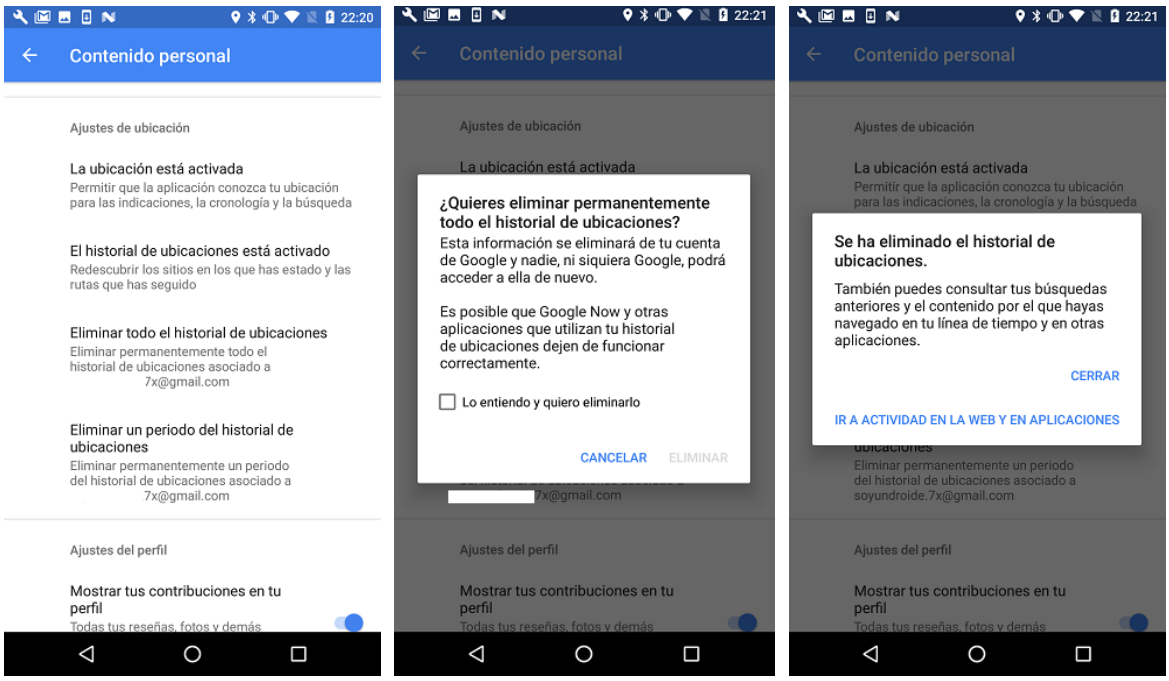
588. La frecuencia con la que los informes de ubicación actualizan los datos de ubicación no es fija y depende de diferentes factores, como la batería del dispositivo móvil, si el usuario se está desplazando, o la velocidad a la que se desplaza.

589. A través del menú "Ajustes [Personal] - Ubicación", y de la sección "Servicios de Ubicación", es posible seleccionar "Historial de ubicaciones de Google" y acceder a los ajustes de configuración para activar o desactivar el historial de ubicaciones de la cuenta de usuario de Google, tanto a nivel global como a nivel de dispositivo:

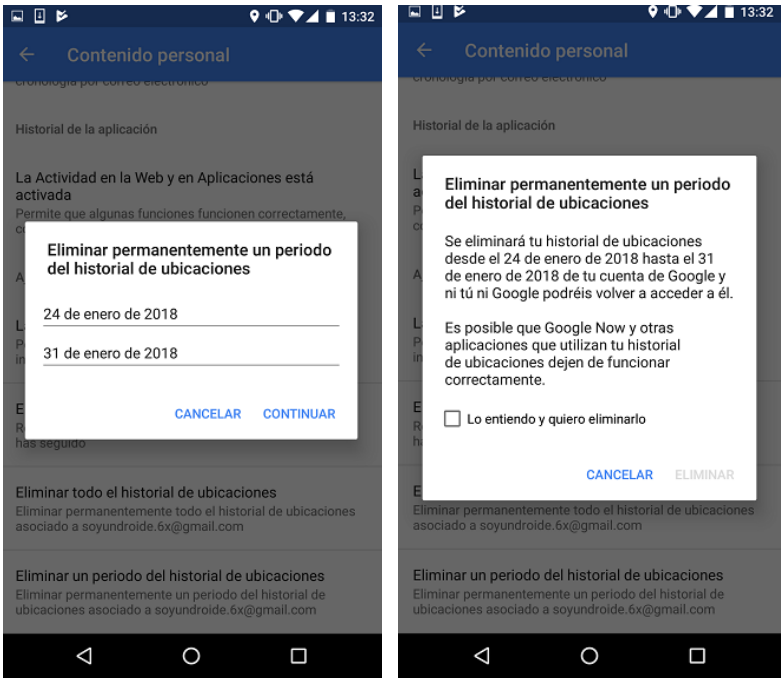


590. La configuración del historial de ubicaciones está disponible a través del menú mencionado previamente, pero, aunque se desactive a través de las opciones descritas, no se eliminarán los datos recopilados hasta ese momento.

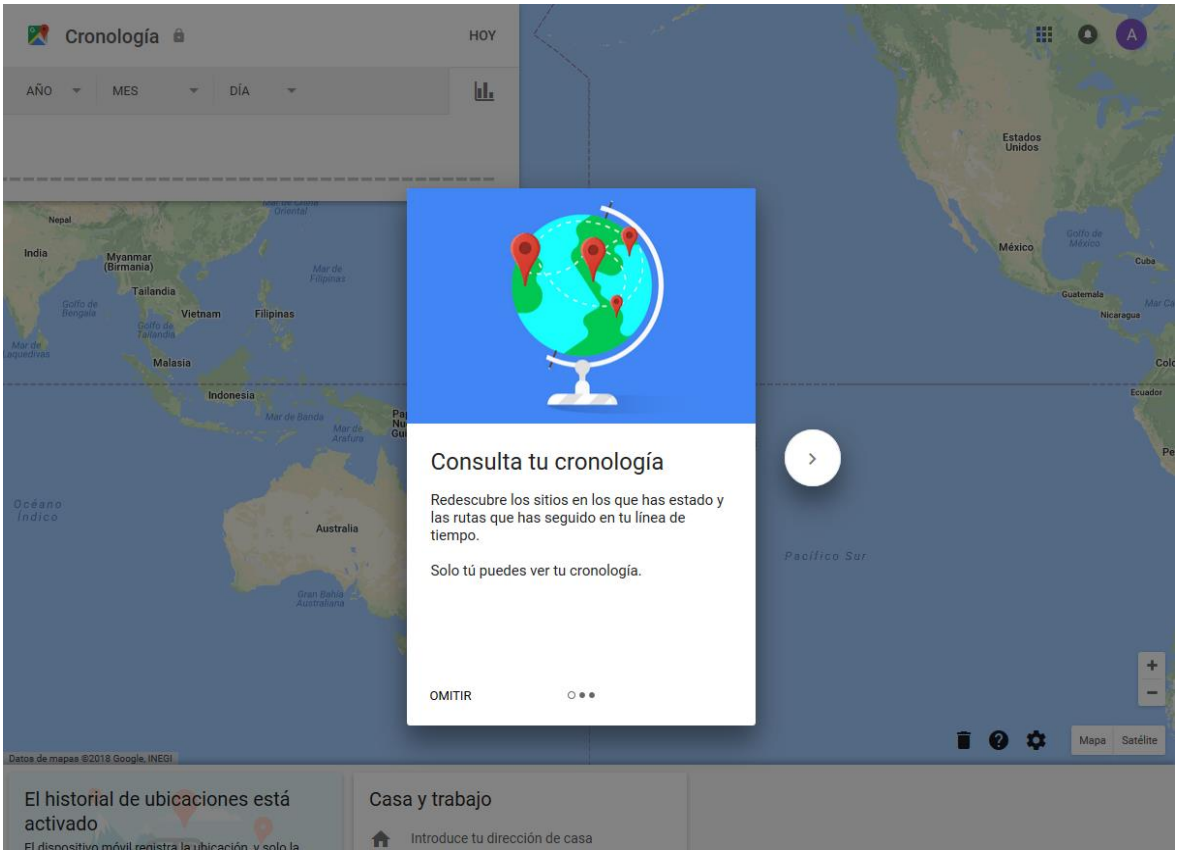
591. Si se desea eliminar el histórico, es necesario acceder a "Ajustes - [Personal] Ubicación - [Servicios de Ubicación] Historial de ubicaciones de Google - <…> Ver/Administrar", o, alternativamente, pulsar en el botón "Gestionar Cronología". Esto hará que se lance la app Maps (app empleada por defecto) en una ventana que muestra la ubicación actual y las demás ubicaciones registradas para el día actual; desde el menú "<…>" accesible desde la esquina superior derecha de la pantalla, se puede seleccionar "Ajustes - [Contenido personal] - Eliminar todo el historial de ubicaciones". Tras aceptar el mensaje de confirmación, se borrarán los datos de ubicaciones previamente almacenados por Google:



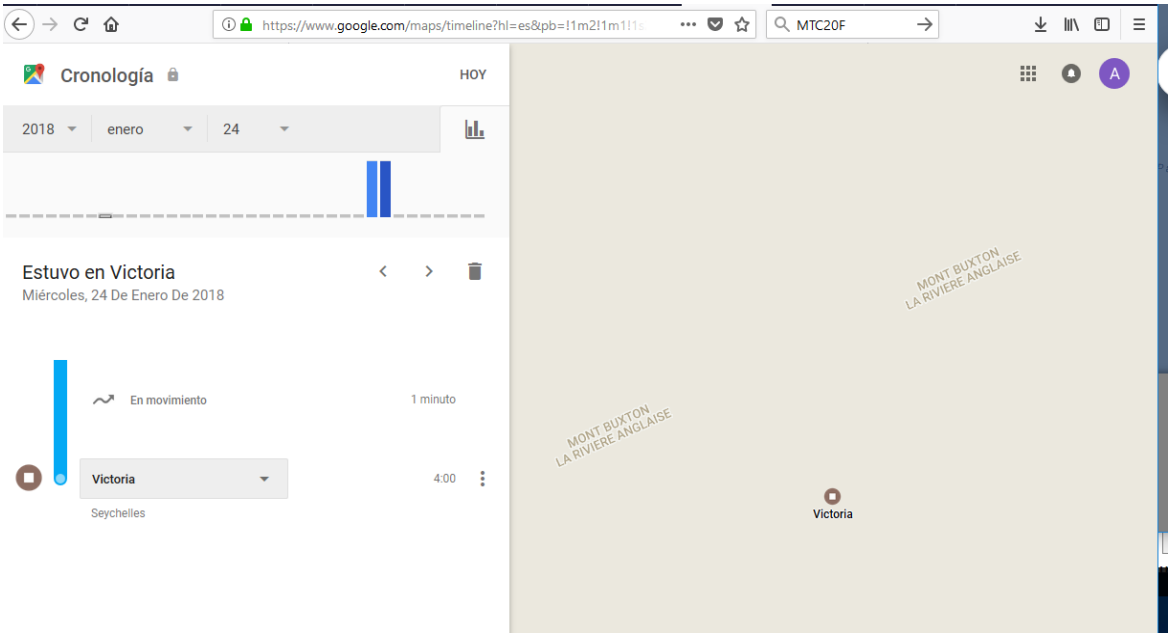
592. También es posible eliminar un periodo concreto del historial, seleccionando la fecha de inicio y de fin.



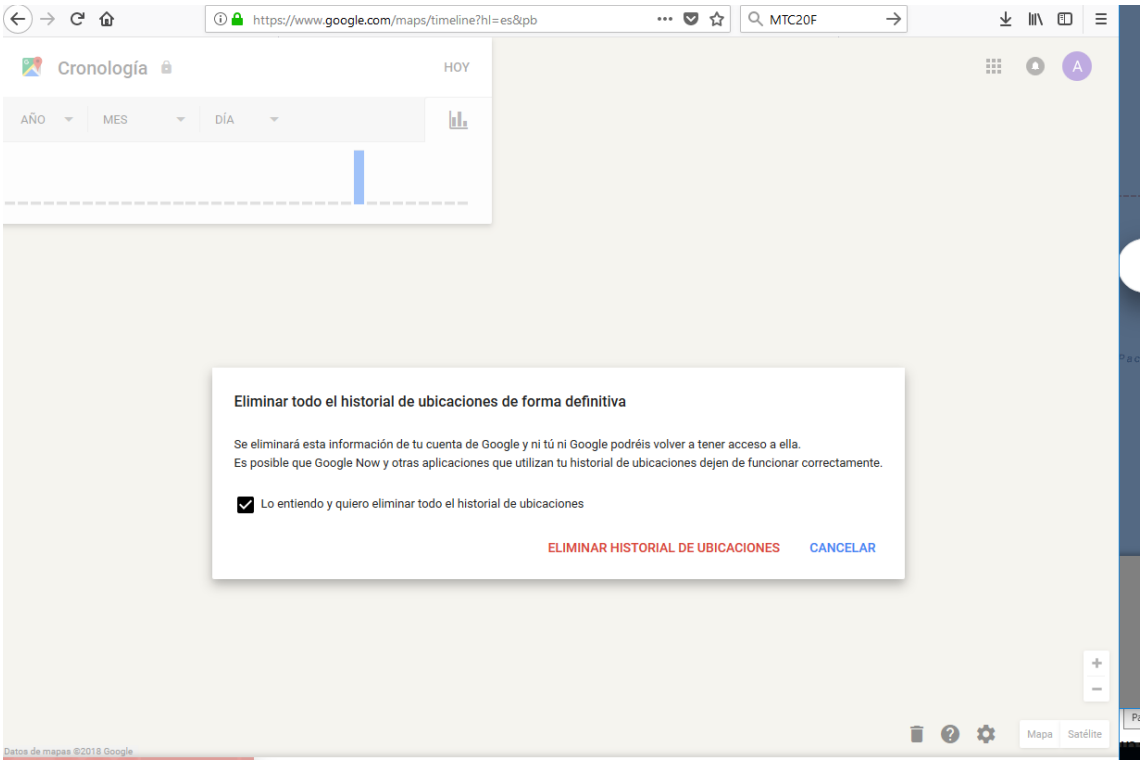
593. Finalmente, un usuario puede también acceder y administrar el historial de ubicaciones vinculado a su cuenta de usuario de Google a través de la siguiente URL: "https://maps.google.com/locationhistory/". Esta funcionalidad está asociada al "Historial de la cuenta", disponible desde la URL "https://myaccount.google.com/activitycontrols" (y que también permite el acceso al historial de actividad web y de aplicaciones).

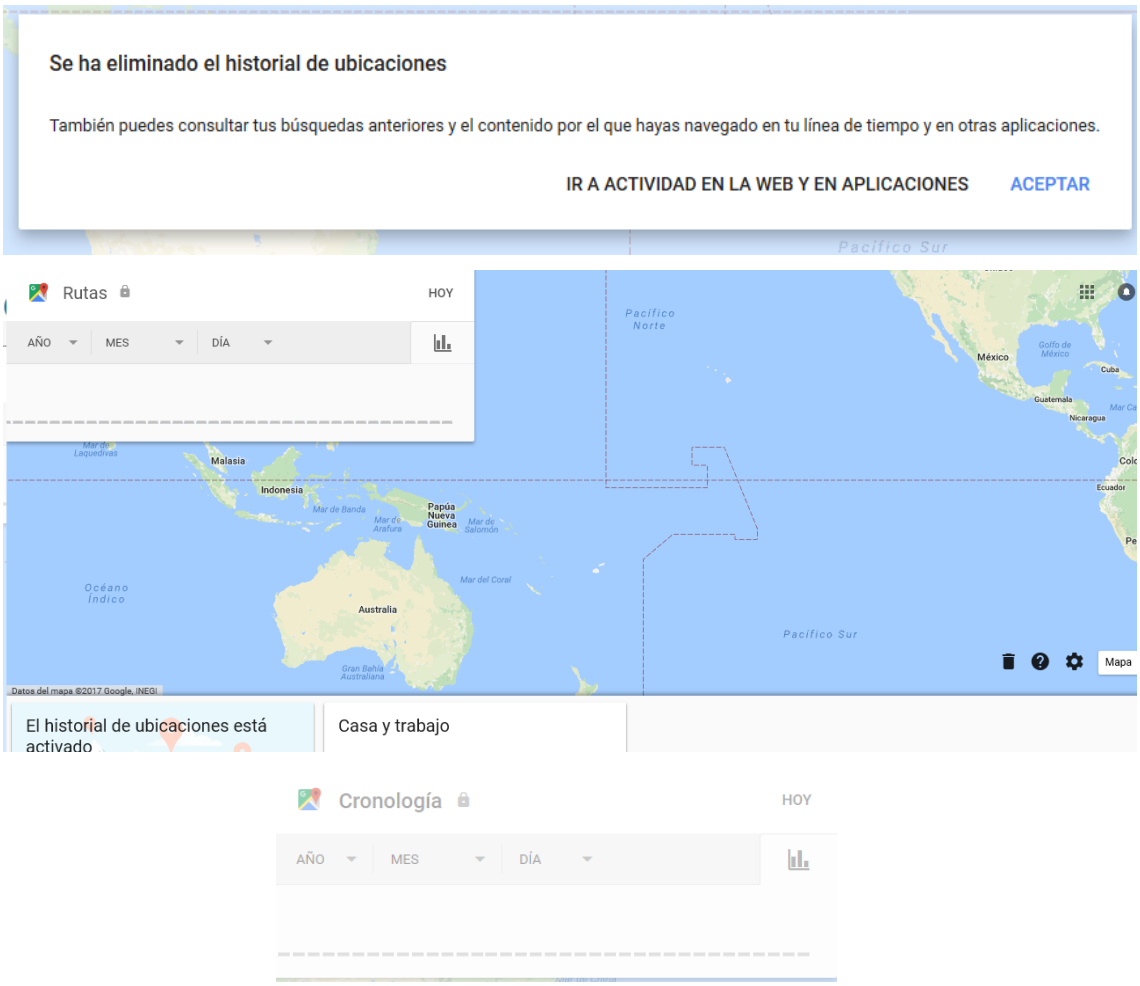


594. Desde la misma es posible obtener los detalles de las ubicaciones registradas para el usuario, incluso clasificadas por fechas y horas, y obtener información de distancias entre ubicaciones:



595. Desde las opciones situadas en el margen inferior derecho de la página web, es posible eliminar los registros del historial y pausar la recolección de datos. Cuando el historial ha sido eliminado, desde el dispositivo móvil o desde la página web, no se dispone de datos asociados a esta funcionalidad:





596. En resumen, desde el punto de vista de seguridad, y, especialmente, de la privacidad el usuario, no se recomienda hacer uso del historial de ubicaciones (es decir, permitir a Google que almacene un histórico de todos los datos de ubicación). Adicionalmente, se recomienda borrar el historial de ubicaciones actualmente existente en la cuenta de usuario de Google.

11.6. OTRAS APPS QUE HACEN USO DE LA LOCALIZACIÓN

597. A continuación, se muestran ejemplos de algunas apps existentes por defecto que hacen uso de los servicios de localización. Únicamente se recomienda verificar que las mismas hagan uso de tráfico cifrado mediante HTTPS, y si exponen o no los datos intercambiados entre ellas y los servidores remotos mediante tráfico no cifrado, normalmente empleando el protocolo HTTP. A modo de ejemplo, en algunos casos el valor del agente de usuario (o "User-Agent") desvelado por las apps proporciona numerosos detalles sobre la app y el dispositivo móvil asociado.

598. Queda fuera del alcance de la presente guía realizar un análisis detallado de seguridad de las diferentes apps que hacen uso de los servicios de localización de Google en Android, así como de la existencia de posibles vulnerabilidades en las mismas.

599. Se recomienda no hacer uso de apps o servicios que desvelan información detallada de la ubicación del usuario y del dispositivo móvil empleado, y que hacen uso de conexiones HTTP no cifradas, salvo que explícitamente se desee acceder a la información que éstos proporcionan.

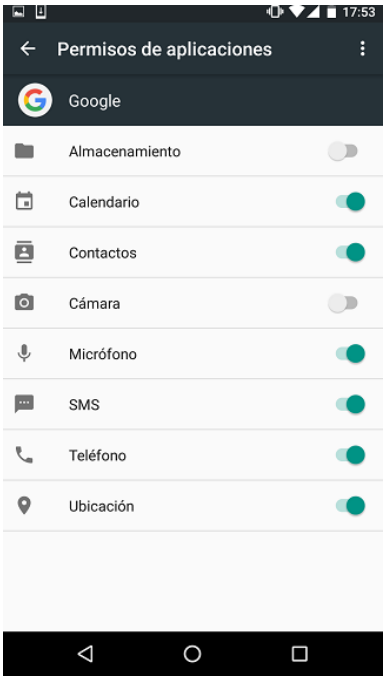
600. La mayoría de apps mencionadas requieren de una conexión de datos (telefonía móvil o Wi-Fi) para funcionar y acceder a la información necesaria para su funcionalidad.

11.7. BUSCADOR DE GOOGLE

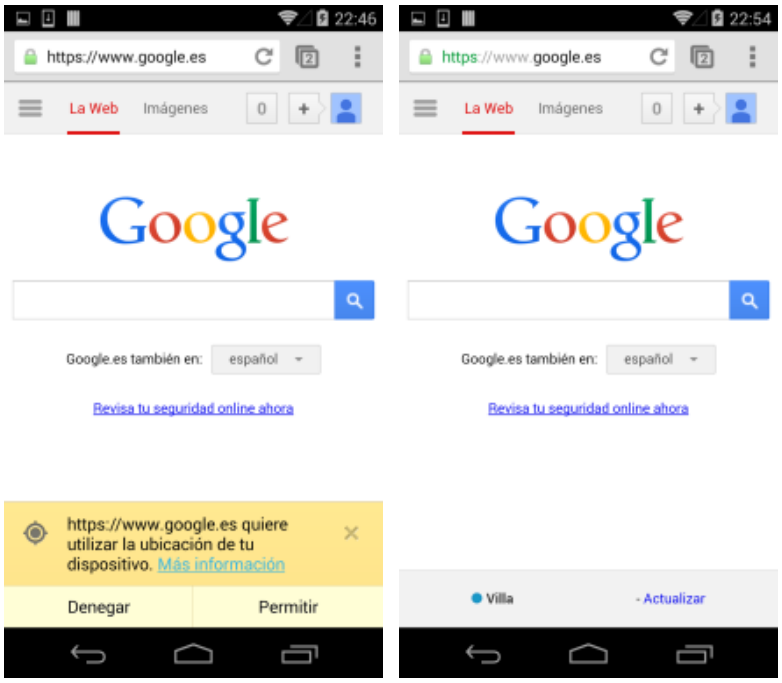
601. La app "Google", que proporciona acceso directo al buscador de Google y a otros servicios de la compañía, puede hacer uso también de los servicios de localización, integrándolos directamente en sus búsquedas y en las capacidades de notificaciones personalizadas asociadas a la actividad del usuario.

602. El buscador de Google está integrado en la pantalla de inicio aplicación "Google", y se accede a él pulsando en la barra de búsqueda situada bajo el banner "Google".

603. Android concede a la app "Google" durante su instalación multitud de permisos, entre los que se encuentra el de ubicación. Se recomienda deshabilitarlo salvo que se requiera por alguna causa:



604. En versiones anteriores de Android, el acceso al buscador de Google directamente desde el navegador web de Android (descrito posteriormente en el apartado "11.9. Navegador web"), solicitaba al usuario utilizar la ubicación del dispositivo móvil, pudiendo éste permitir o denegar dicho acceso (dicho comportamiento se ilustra en las imágenes siguientes). Sin embargo, desde Android 6.x y las versiones más recientes del navegador web y de la app "Google", el permiso de ubicación está concedido por defecto para ambas, por lo que ya no lo solicitan explícitamente al usuario.



605. Los permisos habilitados anteriormente para ciertos sitios web pueden ser modificados posteriormente.

11.8. REDES SOCIALES

606. La información de localización puede integrarse también con las apps de acceso a redes sociales, siendo posible la publicación de la ubicación del usuario a través, por ejemplo, de Twitter o Facebook.

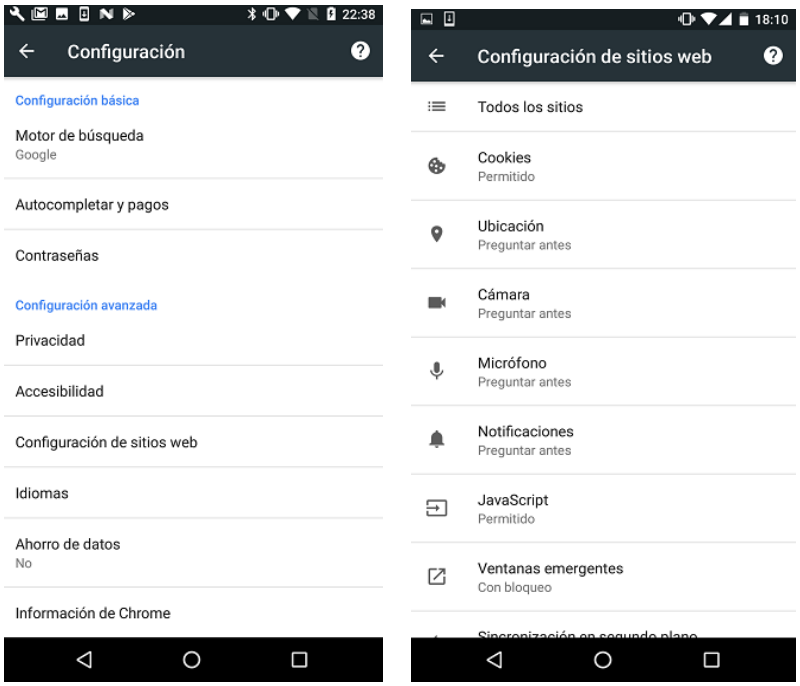
607. Debido a que las apps asociadas a estas redes sociales no están disponibles por defecto en Android 7.x (sí lo estaban en versiones previas de Android), no se profundizará en los detalles centrados en deshabilitar el uso de los servicios de localización desde las mismas.

608. En el caso de Android 7.x sólo se dispone de acceso a las apps para las redes sociales propias de Google, como por ejemplo YouTube, Hangouts y Google+.

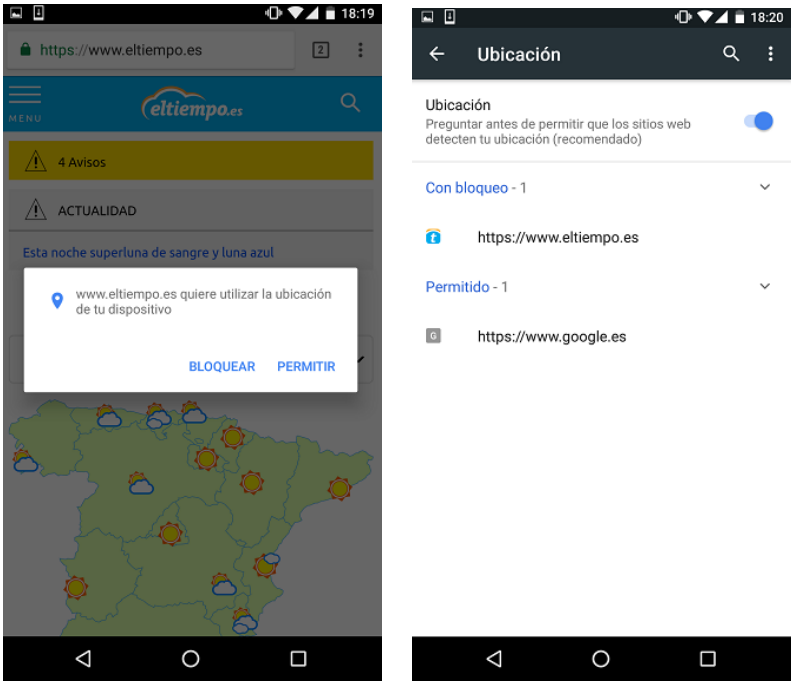
609. Desde el punto de vista de seguridad, se recomienda no hacer pública la ubicación en la que se encuentra el usuario en redes sociales o servicios avanzados similares con el objetivo de proteger su privacidad.

11.9. NAVEGADOR WEB

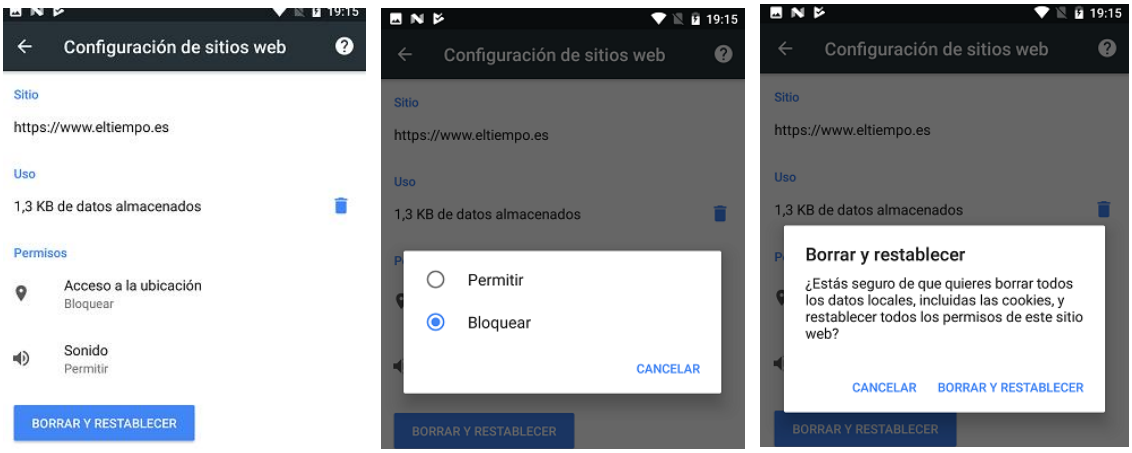
610. El navegador web existente por defecto en Android, Chrome, permite autorizar el acceso a la información de localización (o ubicación del dispositivo móvil) o bloquearlo de manera general. Para ello, se ha de acceder al menú de "Ajustes" de "Chrome", y en concreto a través de la opción "Ajustes - [Configuración] Configuración de sitios web - Ubicación". La opción asociada permite que se solicite al usuario autorización cuando una página web trate de detectar la ubicación del usuario o, si se desactiva, bloquear cualquier solicitud de ubicación por parte de cualquier página web. Esta opción sólo entrará en juego si Chrome tiene concedido el permiso de ubicación a nivel de aplicación en los ajustes de configuración de Android.



611. Si Chrome tiene permiso de ubicación y la opción "Ubicación - Preguntar antes" está activa, tan pronto se visite una página web que solicite acceso a la ubicación del usuario, se creará bajo el menú anterior la lista "Permitido" (si se concedió acceso) o la lista "Con bloqueo" (si se denegó el acceso).



612. Los permisos de acceso a la ubicación habilitados anteriormente para ciertos sitios web pueden ser modificados posteriormente desde el menú de "Ajustes" de "Chrome", y en concreto a través de la opción "Ajustes - [Opciones avanzadas] Configuración de sitios web - Ubicación". Android dispone de capacidades granulares para alterar el acceso a la información de localización para cada sitio web. Tras seleccionar un sitio web concreto, se puede cambiar su permiso "Acceso a la ubicación" seleccionando el nombre del sitio y eligiendo entre las opciones "Permitir" o "Bloquear":

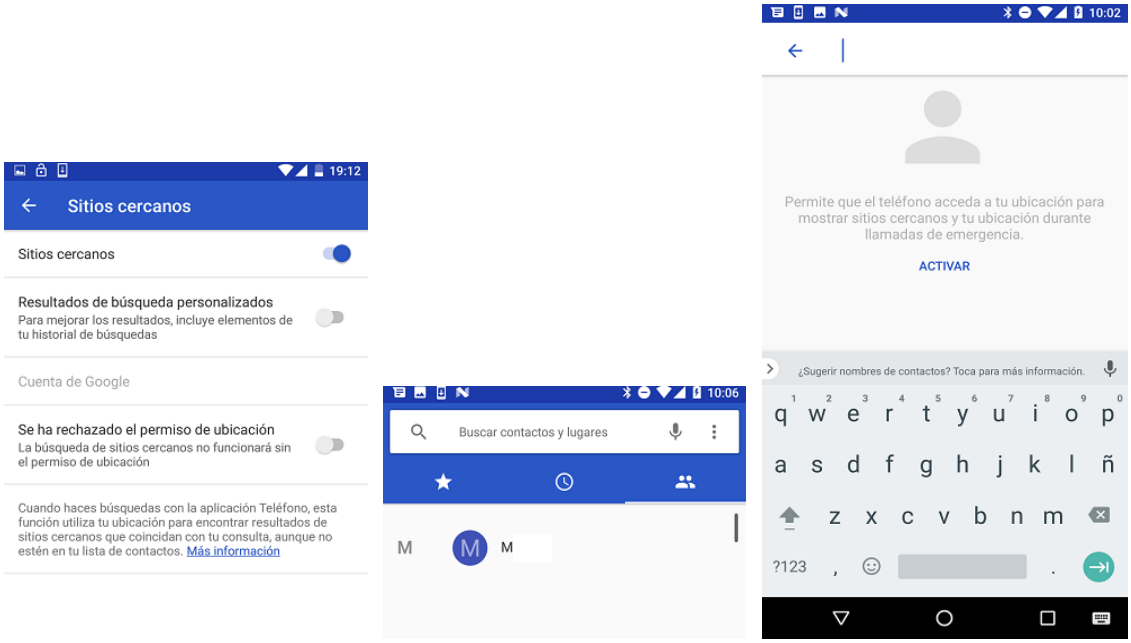


613. El botón "Borrar y restablecer" provocará que se elimine la configuración de permisos asociada al sitio web, además de borrar sus cookies.

614. Desde el punto de vista de seguridad se recomienda deshabilitar la opción "Ubicación" para todos los sitios web, con el objetivo de no permitir a ningún sitio web disponer de acceso a la información de localización, incluso aunque tuvieran este acceso previamente permitido de manera individual.

11.10. APLICACIÓN "TELÉFONO"

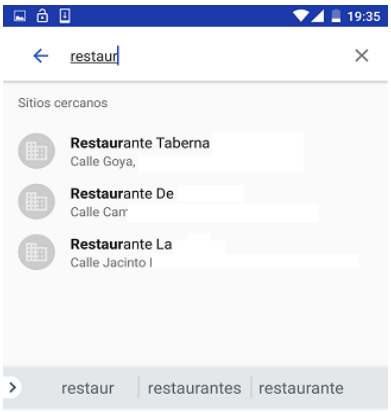
615. Android dispone de capacidades en el teléfono para utilizar la ubicación del dispositivo móvil con el fin de encontrar sitios cercanos que coincidan con las búsquedas realizadas en el dispositivo móvil, aunque la información proporcionada no esté disponible en la agenda o lista de contactos, actuando de guía telefónica, a través de la opción "Sitios cercanos".



616. La opción "Se ha rechazado el permiso de ubicación" aparecerá inactiva si se denegó el permiso de ubicación a la app "Teléfono". Si se activa este interruptor, se abrirá un menú que solicitará de nuevo al usuario el permiso de ubicación para dicha app.

617. Cuando se realiza una búsqueda en la agenda o lista de contactos desde la app "Teléfono", el teléfono buscará información relacionada de sitios cercanos y la

mostrará en la parte superior. Para ello es necesario que estén activos los servicios de localización en Android:



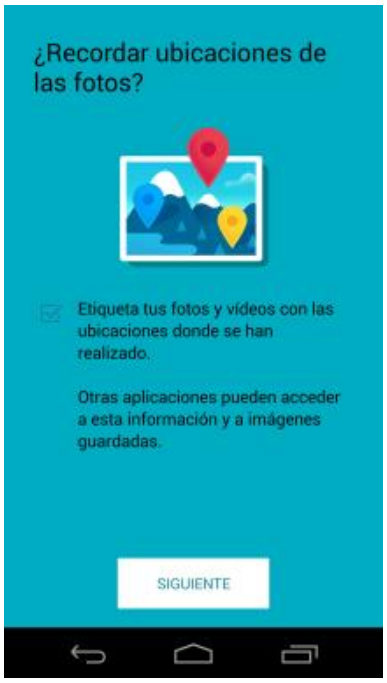
618. La configuración de esta funcionalidad está disponible desde la app del teléfono, mediante el menú de opciones avanzadas disponible en la parte superior derecha, a través del menú "Ajustes de la app Teléfono - Sitios cercanos" (por defecto la opción está habilitada).

619. Los teléfonos sugeridos para sitios cercanos no se añaden automáticamente a la lista de contactos, aunque sí se pueden guardar posteriormente de forma manual, mediante la opción "Añadir a contactos". De nuevo, desde el punto de vista de seguridad, si no se desea hacer uso de esta funcionalidad, se recomienda deshabilitarla.

11.11. INFORMACIÓN GEOGRÁFICA EN FOTOGRAFÍAS

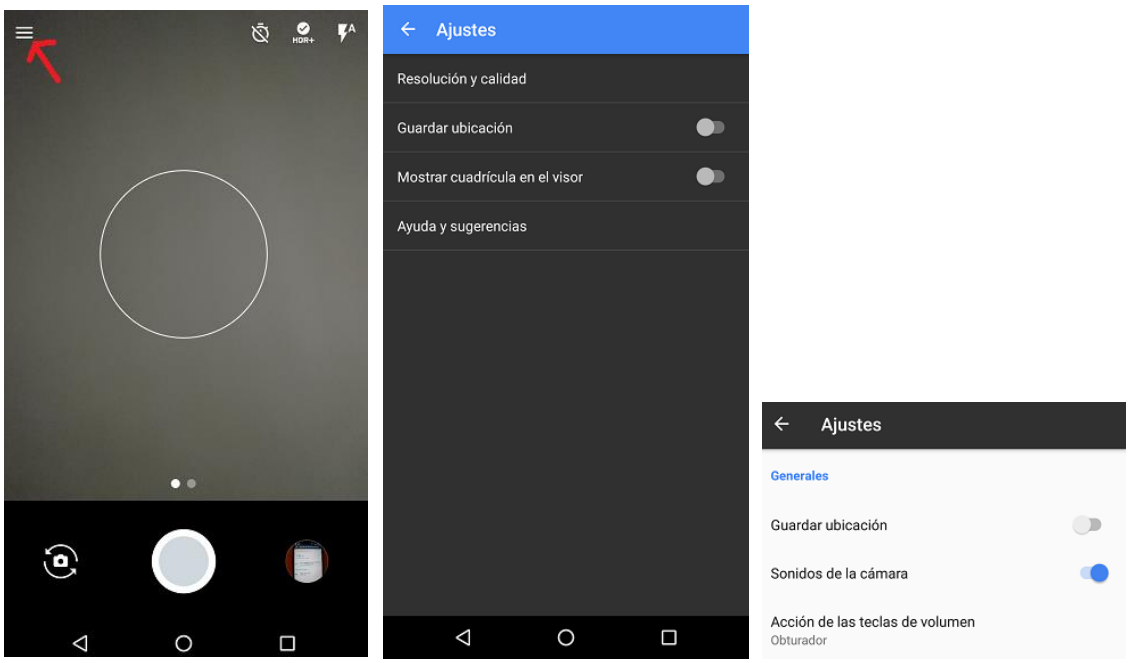
620. Android permite añadir información de la localización geográfica a las fotografías y vídeos realizados con la cámara del dispositivo móvil. Al realizar la fotografía (o vídeo) se añaden las coordenadas GPS en el momento de tomar la instantánea a la cabecera EXIF de la imagen.

621. En función de la versión de la app "Cámara", es posible se pregunte al usuario si desea etiquetar las fotografías y vídeos con la información de la ubicación dónde se han realizado (opción habilitada por defecto), información también accesible para otras apps:



622. Desde el punto de vista de seguridad se recomienda deshabilitar esta funcionalidad con el objetivo de no desvelar detalles de las ubicaciones del usuario.

623. Esta funcionalidad puede ser habilitada y deshabilitada en cualquier momento a través del menú de configuración de la cámara. Para ello es necesario abrir la cámara mediante la app "Cámara" desde el *Launcher*, pinchar en el menú de ajustes señalado con una flecha en la siguiente imagen y seleccionar "Ajustes":

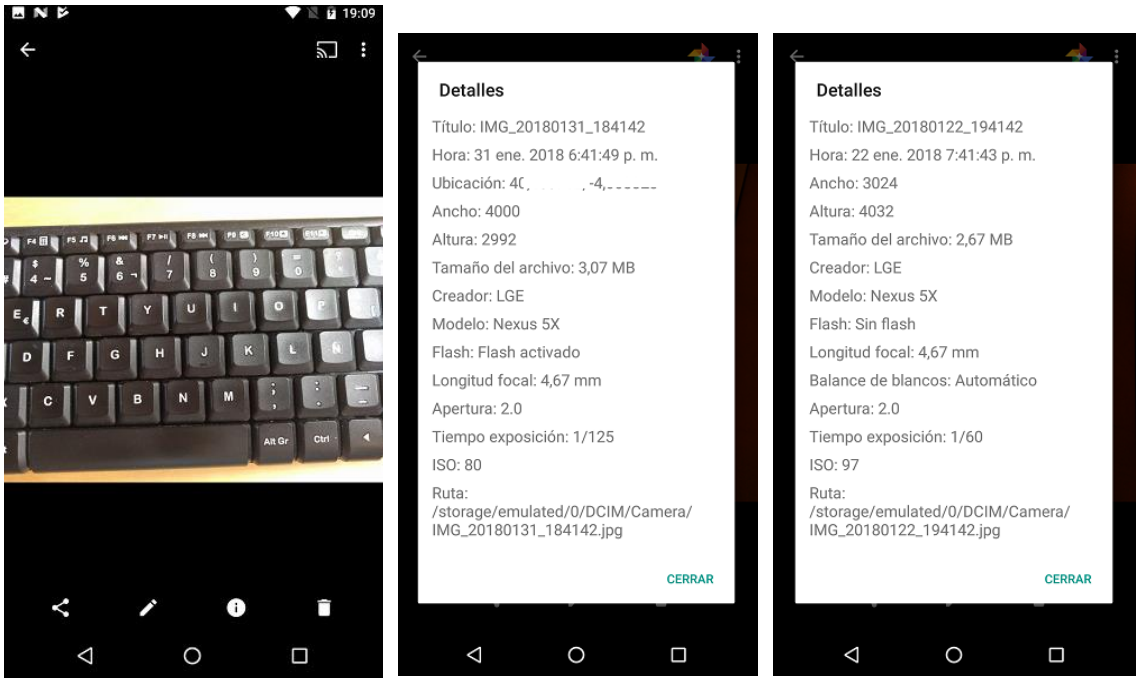


624. La opción "Guardar ubicación" permite habilitar o deshabilitar esta funcionalidad. En caso de elegir su almacenamiento, la app "Cámara" guarda las coordenadas GPS que tenía el dispositivo en el momento de tomarse la fotografía.

625. Los detalles de ubicación de las fotografías pueden ser visualizados desde el dispositivo móvil Android, y en concreto, desde la galería de imágenes de la cámara. La galería está disponible tanto desde la app "Cámara", desplazando desde la derecha hacia la izquierda la imagen de la cámara, o también desde la app "Fotos"

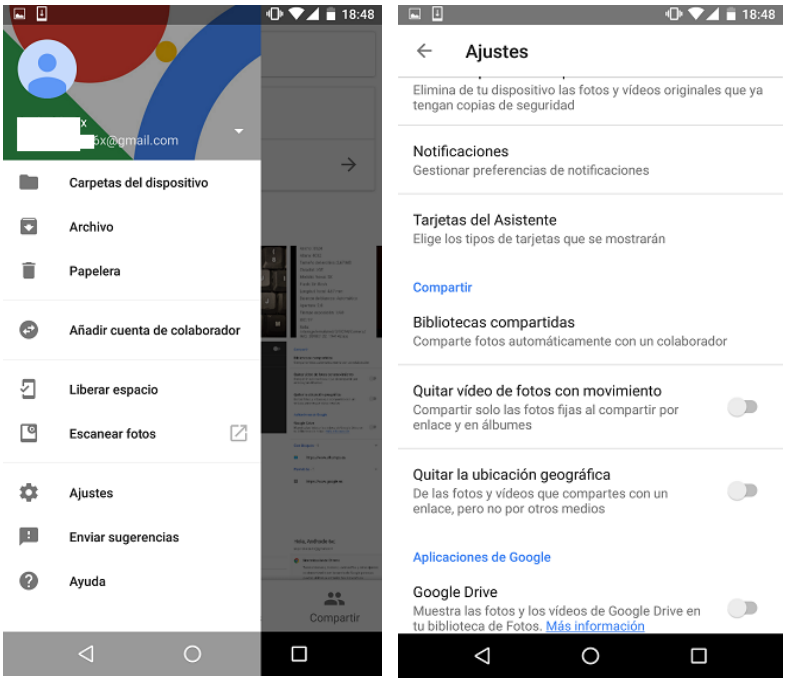
(en versiones anteriores de Android, existía también la app "Galería", pero desde Android 6.x ya no está disponible, y la funcionalidad que ésta tenía asociada se integra dentro de la app "Fotos").

626. Para ello es necesario emplear el botón de menú, y la opción "(i)" (ejemplo asociado a la app "Fotos"):



627. El campo "Ubicación" (al comienzo de la lista de atributos de la imagen) indicará la ubicación dónde fue tomada (latitud y longitud). En caso de no disponer de la información de ubicación de la imagen, este campo o atributo no será mostrado.

628. Respecto a la app "Fotos", dentro de sus ajustes incluye una opción ("Quitar la ubicación geográfica") que permite que, aunque una imagen o un vídeo hayan sido tomados con el permiso de ubicación activo para la cámara, al compartir dicho elemento a través de un enlace, se elimine la información de ubicación. Se recomienda activar dicha opción para evitar que la información de ubicación pueda compartirse inadvertidamente a través de otra app.



629. Aunque dentro de los ajustes de la app "Fotos" Google sugiere utilizar la ubicación para facilitar la organización y la búsqueda de imágenes, se recomienda no hacer uso de la funcionalidad que incluye la información del GPS en fotografías o vídeos, especialmente para su publicación o distribución en Internet, salvo que se quiera hacer uso explícito de estas capacidades. En caso contrario, las imágenes y vídeos revelarán los detalles exactos de donde han sido tomadas.

12. SINGLE SIGN-ON: AUTENTICACIÓN DE USUARIOS DE DISPOSITIVOS MÓVILES EN SERVICIOS Y APPS

630. Con la expansión de las plataformas móviles y la ampliación de los servicios que se hospedan y proporcionan desde la nube, la verificación de la identidad del usuario se desveló como un problema de seguridad relevante. Cada día surgen nuevas apps y servicios que requieren de un mecanismo de autenticación y protección de la identidad del usuario.

631. Este hecho lleva asociada otra problemática: la complejidad que supone para el usuario recordar y definir multitud de credenciales para los diferentes servicios, aplicaciones corporativas y otras apps a las que se accede desde el dispositivo móvil.

632. Para resolver ambas problemáticas, surgió el concepto de "Single Sign-On" (SSO) dentro del mundo Android, que pretende simplificar la situación descrita. Por un lado, SSO delega la gestión de identidad en un servicio de un tercero de confianza, el cual implementa los mecanismos de autenticación y protección de identidad de forma segura, tanto para el usuario como para el proveedor del servicio y, por otro, permite al usuario no tener que dar de alta y recordar nuevas credenciales por cada servicio al que accede.

633. Llevado al extremo, un ejemplo particular de SSO es el mecanismo de validación de credenciales a través de huella digital que soportan multitud de aplicaciones móviles de banca, delegando el proceso de autentificación parcialmente en un mecanismo propio del dispositivo móvil y su sistema operativo.

634. En el pasado (hasta abril de 2012), el protocolo de autentificación ClientLogin era empleado por las apps de Android que interactúan con los servicios y APIs de Google para obtener un *token* de autentificación ("authToken"), mediante el envío de las credenciales válidas (usuario y contraseña) de una cuenta de usuario de Google a través de HTTPS. El "authToken", denominado "auth", era intercambiado a través de la cabecera "Authorization: GoogleLogin auth=…" de HTTP.

635. El "authToken" era empleado para el acceso a las interfaces (o APIs) de los servicios de Google, de forma similar al uso de sesiones mediante cookies en aplicaciones web, y su valor era válido durante (como máximo) dos semanas (14 días) [Ref.- 114] [Ref.- 115].

636. Posteriormente, ClientLogin fue reemplazado por OAuth 2.0 [Ref.- 116] [Ref.- 260], mecanismo de autentificación y autorización que también permite a las apps de Android interactuar con los servicios web y APIs de Google (y de otros proveedores). Con el protocolo OAuth 2.0, el desarrollador de una app debe seguir los siguientes pasos:

- Obtener credenciales OAuth 2.0 de la "Google API console": un "client ID" y/o un "client secret" (éste último se requiere para un servidor web de aplicaciones) que sólo son conocidos para Google y para la app.
- Obtener un "Access token" del "Google Authorization Server": dicho token es necesario para obtener acceso a la API de Google; el token tendrá asociado un ámbito (scope) que determina el conjunto de recursos y operaciones a las que puede dar acceso (por ejemplo, un token emitido para la API de Google+ no permite acceder a la API de Contactos de Google). Los tokens tienen una validez limitada en el tiempo.
- Enviar el token de acceso a la API de Google a través de una cabecera de autorización HTTP, empleando HTTPS.

637. El mecanismo "Firebase Authentication" [Ref.- 259], desarrollado por Google, permite a una app conocer (y validar) la identidad del usuario a través de mecanismos como contraseñas, número de teléfono o proveedores de identidad federados (entre los que se encuentran Google, Facebook y Twitter). Con este mecanismo, la cuenta de usuario de Google se convierte en un medio para autentificar al usuario también en la app, lo que facilita a los desarrolladores la programación de su app, al no tener que preocuparse de la implementación de gestión de identidades.

638. El servicio "Google Sign-In" se basa en permitir al usuario la validación ante un servicio o una app a través de su cuenta de usuario de Google. Las apps que soportan "Google Sign-in" pueden acceder al perfil, email y OpenID del usuario. Un ejemplo típico de uso de este escenario son las apps que ejecutan en un *smartwatch* en modo *standalone*, es decir, sin la necesidad de una aplicación gemela (con funcionalidad específica) que ejecute en el dispositivo móvil asociado.

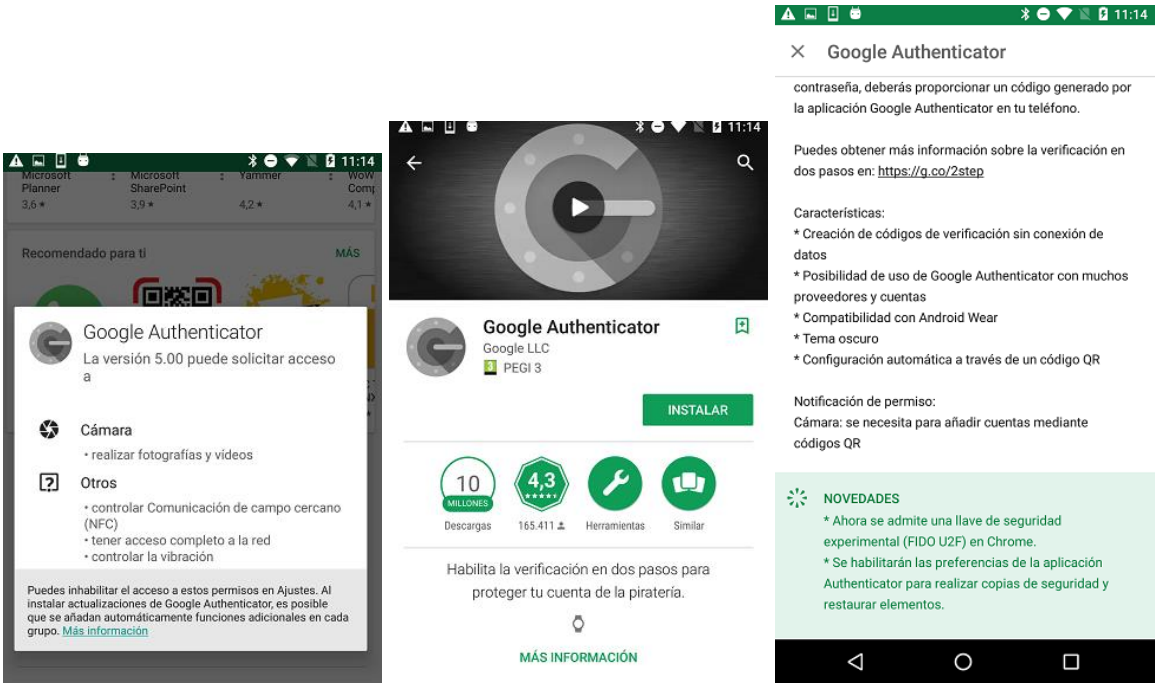
639. Con la aceptación de la cuenta de usuario de Google como medio (casi) universal de autentificación, no sólo para acceder a servicios "básicos" del dispositivo móvil, sino a otra multitud de servicios tanto de Google como de terceros o corporativos, la protección de la cuenta de usuario de Google se convierte irremediablemente en un elemento crítico.

12.1. GOOGLE AUTHENTICATOR

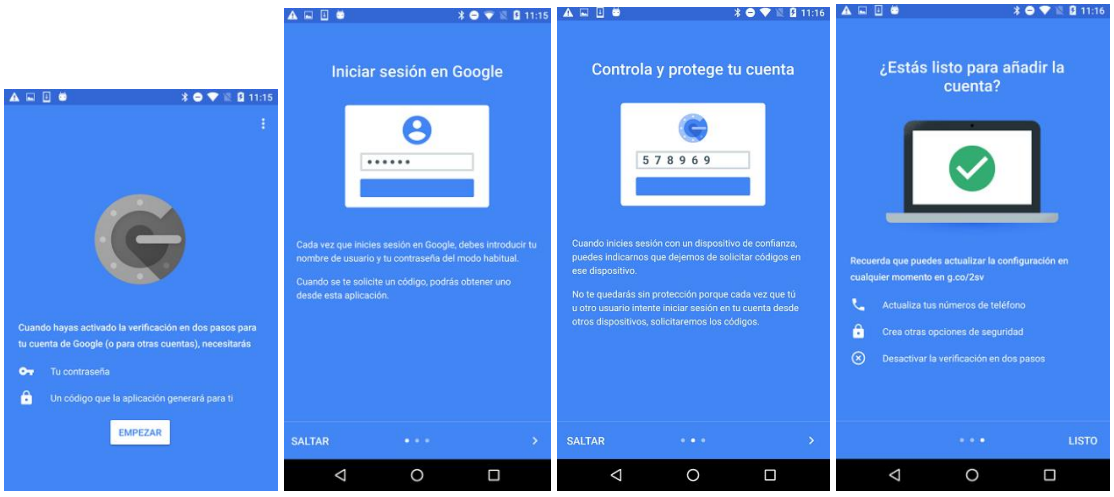
640. En el año 2014 Google publicó la primera versión de su app Google Authenticator [Ref.- 14] [Ref.- 261].

641. El objeto de la misma era complementar el uso de contraseñas personales con mecanismos de verificación de un solo uso (OTP, *One Time Password*), que eliminan el riesgo frente a los ataques de diccionario y/o fuerza bruta sobre la contraseña, y palían la amenaza asociada a que, frecuentemente, los usuarios reutilizan contraseñas, es decir, emplean las mismas (o muy parecidas) contraseñas para distintos servicios.

642. A fecha de elaboración de la presente guía, la versión de la app Google Authenticator disponible en Google Play es la 5.0:

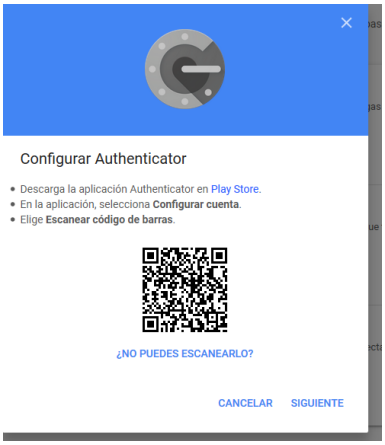


643. Una vez instalada la app y tras ejecutarse por primera vez, se mostrará la pantalla inferior izquierda. Tras pulsar en "Empezar", se lanzará un asistente que describe el propósito de la app:

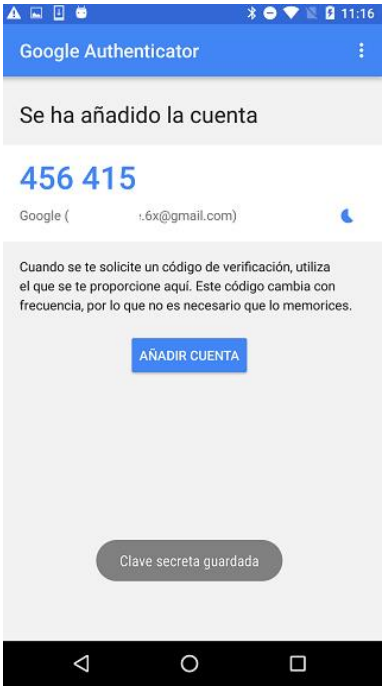


644. El usuario deberá simultáneamente entrar en el menú de verificación en dos pasos de su cuenta de usuario de Google (a través de la siguiente URL,

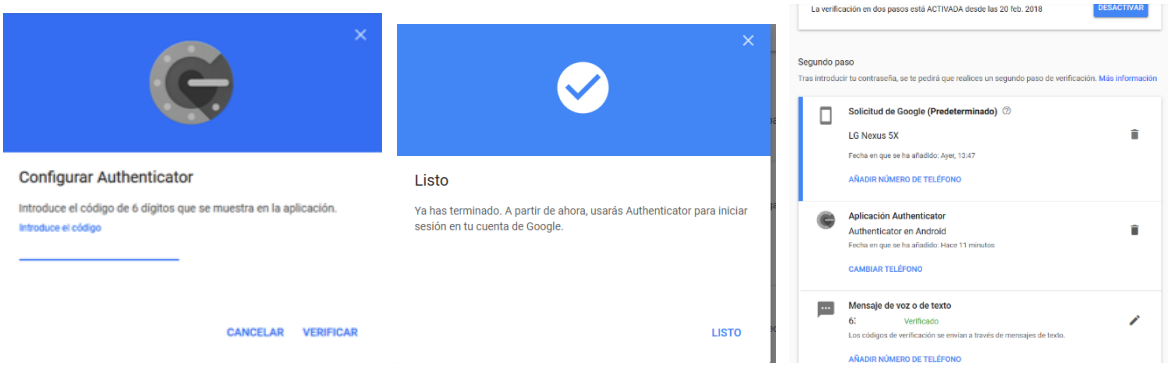
"https://myaccount.google.com/signinoptions/two-step-verification") y seleccionar la opción "[Configurar un segundo paso alternativo] - Aplicación Authenticator". Se mostrará la siguiente ventana que contendrá un código QR, el cual se deberá escanear desde la app Google Authenticator del dispositivo móvil:



645. Para escanear el código QR desde la app Google Authenticator en el dispositivo móvil, se solicitará el permiso "fotos y vídeo". Una vez concedido, se abrirá la app Cámara, desde la cual se encuadrará el código QR descrito anteriormente hasta que se muestre la siguiente ventana. En ella, se presentará un código de seis dígitos, el cual tendrá validez mientras se muestre en pantalla (el icono en forma de queso situado a la derecha representa la vida útil que le resta a dicho código):



646. En el dispositivo móvil o navegador web en el que se esté dando de alta el servicio de segundo factor de autentificación para la cuenta de usuario de Google mediante Google Authenticator, aparecerá la ventana que se ilustra a continuación, en la que se deberá introducir el código que muestra actualmente la app Google Authenticator. Tras pulsar "Verificar", se completará la configuración de Google Authenticator como mecanismo para el segundo factor de verificación:



647. En lo sucesivo, cuando se intente abrir sesión en la cuenta de Google del usuario, se deberá introducir el código mostrado por la app Google Authenticator como segundo factor de verificación.

648. Tal como se indicó anteriormente, se recomienda utilizar Google Authenticator para añadir una capa extra de seguridad a la cuenta de usuario de Google, que además no requiere disponer de acceso a Internet desde el dispositivo móvil.

12.2. SERVICIO DE CONTRASEÑAS DE GOOGLE SMART LOCK

649. Además del servicio Smart Lock para mantener dispositivos Android desbloqueados (ver apartado "10.5. Desbloqueo mediante Smart Lock"), Google incorporó con la actualización a la versión 7.5 de Google Play Services (GPS) un gestor de contraseñas referenciado como "Smart Lock para contraseñas", destinado a almacenar y sincronizar las contraseñas de sitios web accedidos con Chrome y otras aplicaciones desde los dispositivos móviles.

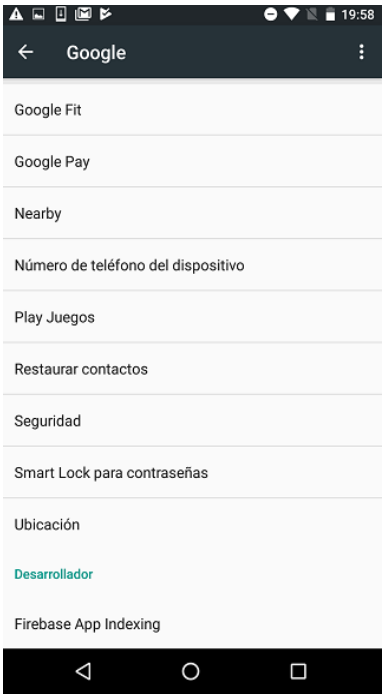
650. Smart Lock para contraseñas forma parte del ecosistema "Google Identity Platform" [Ref.- 245], cuyo objetivo es la gestión segura de la identidad de los usuarios.

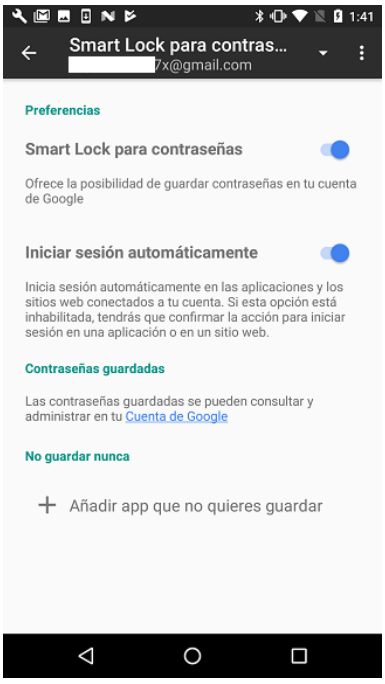
651. La sincronización de datos se realiza a través de la cuenta de Google del usuario, por lo que las contraseñas almacenadas a través del gestor Smart Lock estarán disponibles en todos los dispositivos en los que se haya iniciado sesión con dicha cuenta de usuario [Ref.- 244].

652. Cuando se visita por primera vez un sitio web o se utiliza una app que emplea esta funcionalidad y que requiere introducir credenciales, si Smart Lock para contraseñas está activo, se mostrará una ventana solicitando permiso para almacenar las credenciales. Si se acepta, la próxima vez que se visite el sitio web o se ejecute la app desde cualquier otro dispositivo que haya iniciado sesión en la cuenta de Google del usuario, no se solicitará identificación, sino que Smart Lock proporcionará automáticamente las credenciales para ingresar en dicha web o app.

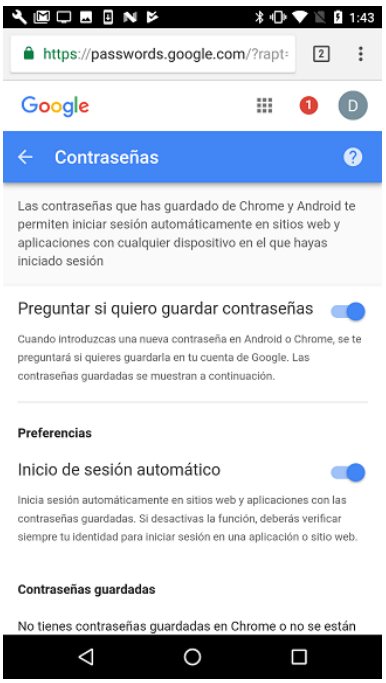
653. A nivel de app, los desarrolladores pueden integrar Smart Lock en su aplicación móvil utilizando la API "Credentials" [Ref.- 246].

654. La activación del servicio "Smart lock para contraseñas" se realiza a través de "Ajustes - [Personal] Google - [Servicios] Smart lock para contraseñas" [Ref.- 239]. Las opciones disponibles son las siguientes:





- [Preferencias] **Smart Lock para contraseñas**: esta opción habilita/deshabilita el servicio.
- [Preferencias] **Iniciar sesión automáticamente**: si se deshabilita, se solicitará al usuario confirmación para iniciar sesión; si se habilita, el inicio de sesión tendrá lugar sin intervención del usuario.
- [Contraseñas guardadas]: solicita al usuario la contraseña de la cuenta de usuario de Google en la que se almacenarán las contraseñas, y redirige a la página "https://passwords.google.com" para consultar la información de credenciales guardada.



- [No guardar nunca]: permite elegir qué apps de las instaladas por el usuario no podrán hacer uso del servicio y, por tanto, no verán sus credenciales almacenadas.

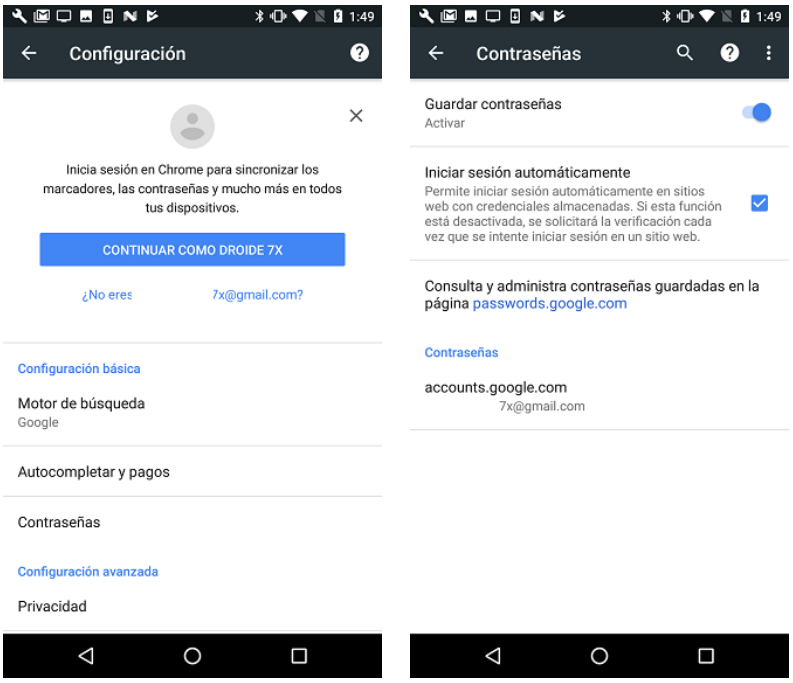
655. Si Smart Lock para contraseñas está activado (es el modo por defecto), Chrome hará uso de él para guardar las credenciales de los sitios web para los que el usuario acepte esta acción.

656. Si Smart Lock para contraseñas está desactivado, pero se ha iniciado sesión en la cuenta de Google del usuario, Chrome también almacenará las credenciales de los sitios web en "https://passwords.google.com".

657. Las contraseñas de páginas web y aplicaciones Android guardadas en este gestor, así como las opciones de configuración actual asociadas a él, se pueden consultar desde "https://passwords.google.com".

658. A través de este sitio web, se pueden eliminar entradas, pero también visualizar las contraseñas e identificadores de usuario de los sitios webs para los que se aceptó el almacenamiento:

659. La sección "Contraseñas guardadas" sólo contendrá información sobre las credenciales de sitios web si la configuración del navegador Chrome tiene habilitada la opción de "Guardar contraseñas" dentro de su configuración:



660. Desde el punto de vista de seguridad, se recomienda deshabilitar el uso de Smart Lock para contraseñas o, cuando menos, las opciones que implican llevar a cabo un inicio de sesión automático.

13. COPIAS DE SEGURIDAD

661. Además de la copia de seguridad del dispositivo móvil que se puede realizar a través del comando "*adb backup*" invocado desde un ordenador conectado al dispositivo móvil mediante un cable USB (consultar el apartado "Copias de seguridad" de la " Guía CCN-STIC-453E - Seguridad de dispositivos móviles: Android 7.x" [Ref.- 407] para más información), Google ofrece un servicio de copia de seguridad y restauración para los datos de los servicios y apps vinculados a un dispositivo con una cuenta de usuario de Google activa.

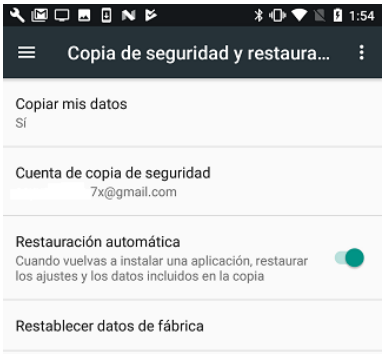
13.1. COPIA DE SEGURIDAD EN LOS SERVIDORES DE GOOGLE

662. El servicio de copia de seguridad de datos de Google (denominado *Android Backup Service*) permite almacenar información personal y datos del usuario en los servidores de Google, como los favoritos de navegación web, palabras añadidas al diccionario, una lista de las apps instaladas, parámetros de configuración y los datos utilizados por las apps de terceros, las contraseñas de las redes Wi-Fi, la mayoría de parámetros de configuración del dispositivo móvil y de los servicios de Google, etc., siendo posible restaurar los datos posteriormente si fuese necesario reemplazar el dispositivo móvil o reinstalar una app [Ref.- 105].

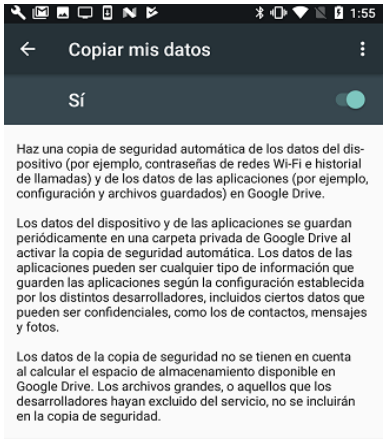
663. Durante el proceso de instalación y configuración inicial de Android y vinculación del dispositivo móvil (ver apartado "16. Proceso de instalación y configuración inicial") a una cuenta de usuario de Google (y/o de creación de la cuenta) se solicita confirmación por parte del usuario para activar el servicio de copia de seguridad de datos.

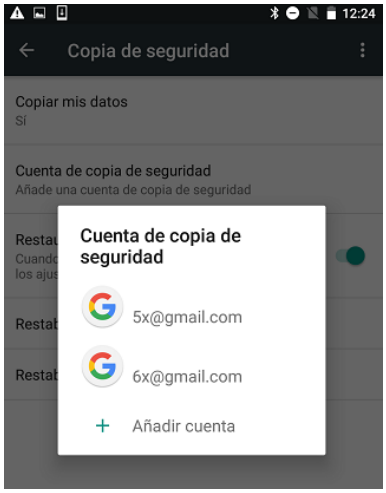
664. En el caso de dispositivos móviles Android multi-usuario, únicamente el usuario propietario (o usuario principal) puede gestionar las opciones de copia de seguridad y restauración.

665. El servicio de copia de seguridad de datos en los servidores de Google puede ser activado o desactivado posteriormente a través del menú "Ajustes [Personal] - Copia de seguridad y restauración", y en concreto, mediante la opción "Copiar mis datos" (siendo necesario disponer de una cuenta de usuario de Google vinculada al dispositivo móvil).

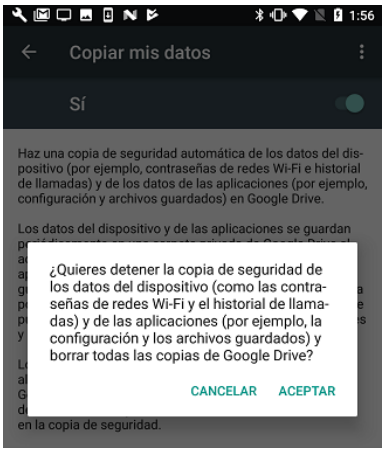


666. En el caso en que existan varias cuentas de usuario de Google en el dispositivo móvil, será necesario elegir la cuenta de la cual se realizará la copia de seguridad (no es posible realizarla de más de una cuenta). Para seleccionarla, se debe pulsar sobre "Cuenta de copia de seguridad":





667. Al desactivar la opción, no se llevarán a cabo más copias de seguridad de los datos en la cuenta de usuario de Google asociada, y las copias de seguridad existentes serán (supuestamente) eliminadas de los servidores de Google.



668. Si se reinstala una app de terceros (desde Google Play), el servicio puede almacenar y restaurar la configuración y los datos asociados a la app (algunas apps pueden no permitir la realización de copias de seguridad y la restauración de sus datos).

669. La opción "Restauración automática" permite restaurar la configuración y los datos asociados a una app al instalarla (o reinstalarla) en el dispositivo móvil desde la copia de seguridad disponible en los servidores de Google. Si la app fue instalada y usada en el mismo, o en otro dispositivo móvil, en el que se disponía del servicio de copia de seguridad de datos activo con la misma cuenta de usuario de Google, toda la información de la app será recuperada.

670. En caso de que el usuario reemplace, sustituya o renueve su dispositivo móvil, este servicio ofrece la posibilidad de restaurar los datos desde la copia de seguridad de Google en el nuevo dispositivo móvil la primera vez que se accede a Google con la cuenta de usuario asociada a este servicio.

671. Los datos que serán restaurados incluyen, entre otros, los ajustes de calendario y Gmail, los datos de redes Wi-Fi (incluyendo las credenciales y contraseñas de acceso), la configuración de la pantalla de inicio, los ajustes de idioma e introducción de texto, la lista de apps instaladas desde Google Play, junto a sus datos y ajustes de configuración, etc. [Ref.- 105].

672. El usuario u organización propietaria del dispositivo móvil Android debe evaluar en detalle el nivel de confianza depositado en Google para emplear este servicio y almacenar todos los datos personales y confidenciales de los usuarios en el mismo.

13.2. COPIA DE SEGURIDAD DE FOTOS Y VÍDEOS

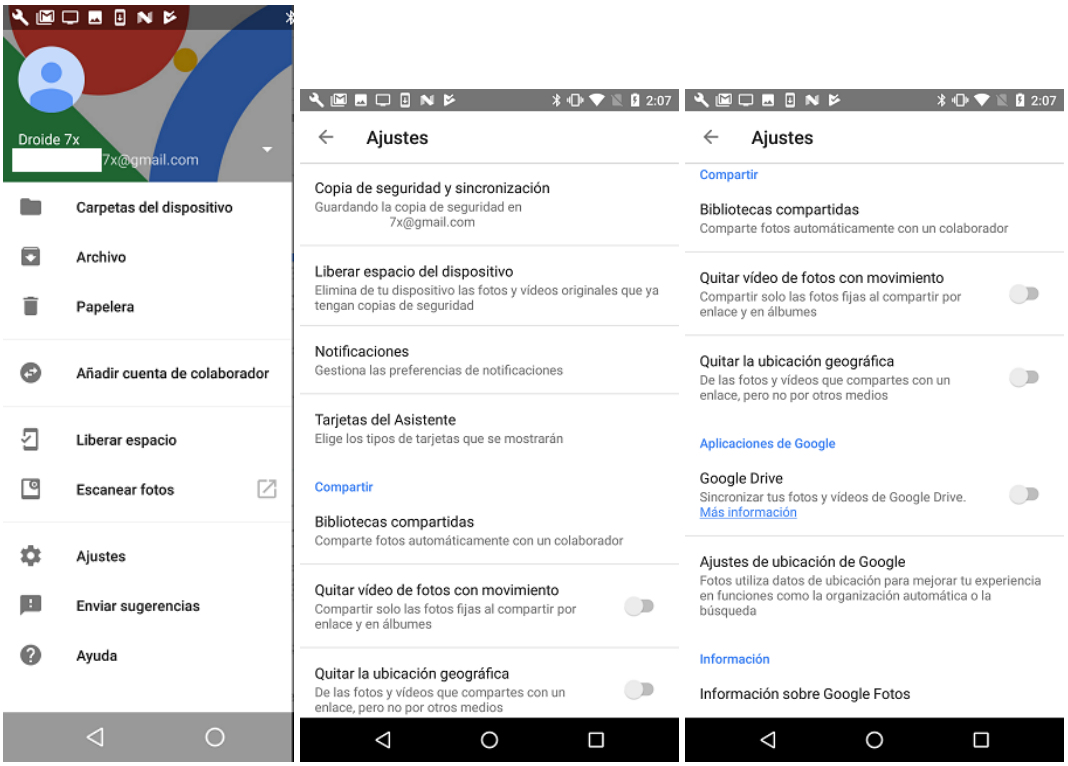
673. El servicio de copia de seguridad de datos de Google (descrito en el apartado previo) no incluye las fotos (o fotografías) y vídeos disponibles en el dispositivo móvil.

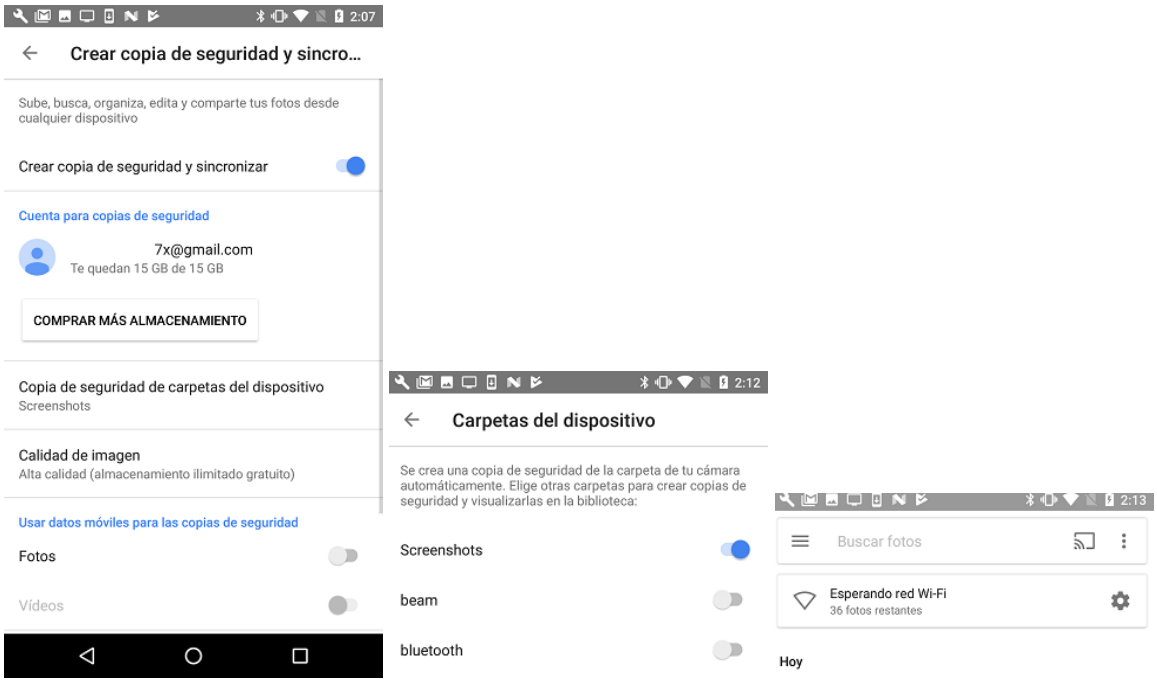
674. Para hacer una copia de seguridad de las fotos y vídeos automáticamente en la cuenta de usuario de Google es necesario configurar el servicio de copia de seguridad de fotos y vídeos de Google, disponible a través de la app "Fotos" [Ref.- 178]. Al activar este servicio, la copia de seguridad de las fotos y vídeos es (supuestamente) privada, salvo que el usuario decida compartirlas.

675. Las fotos (y vídeos) incluyen tanto las realizadas con la cámara del terminal, como las capturas de pantalla (*screenshots*), las descargadas desde Internet (*download*) y las que almacenan otras apps, como por ejemplo Hangouts.

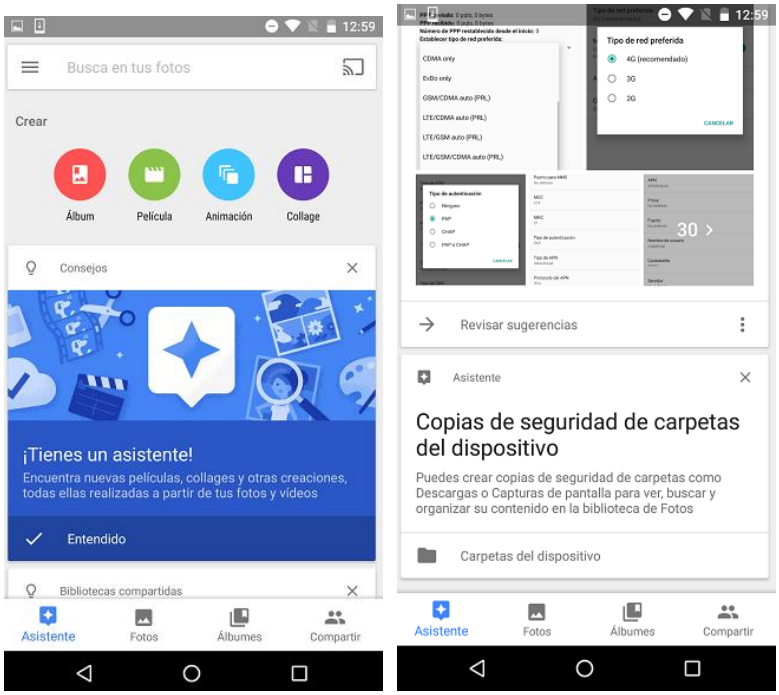
676. La primera vez que se ejecuta la app "Fotos" se consulta al usuario si quiere hacer copias de seguridad automáticamente de las fotos y vídeos, y si la transferencia de estos contenidos multimedia hacia la cuenta de usuario en Google se hará a través de redes Wi-Fi y redes de telefonía móvil (2/3/4G), con un posible gasto asociado, o sólo mediante redes Wi-Fi.

677. Es posible activar o desactivar las copias para carpetas concretas mediante la app "Fotos", desde el botón de menú superior izquierdo, y la opción "Ajustes - Copia de seguridad y sincronización - Crear copia de seguridad y sincroniz…". Por defecto, únicamente se realizará la copia de la carpeta asociada a la cámara del dispositivo móvil. Si se desea salvar el contenido de otras carpetas, se deberán activar los interruptores correspondientes a ellas (*Screenshots* para capturas de pantalla, *bluetooth* para las imágenes recibidas por Bluetooth, etc.):



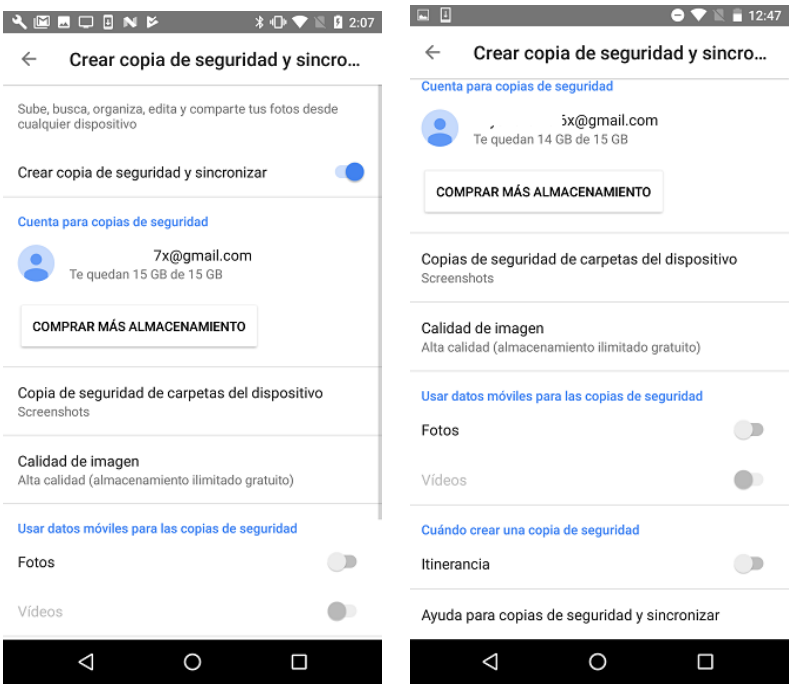


678. Además, el denominado "Asistente" (accesible desde el menú inferior de la app "Fotos") mostrará tarjetas informando sobre las distintas opciones de configuración: qué carpetas de las existentes en el dispositivo móvil se copiarán (además de las fotos y vídeos realizados con la cámara del dispositivo móvil, es posible incluir en la copia de seguridad las imágenes correspondientes a las capturas de pantalla, *screenshots*, las descargadas desde Internet o por Bluetooth, y las que almacenan otras apps), cuáles se desea archivar, crear álbumes, etc.:



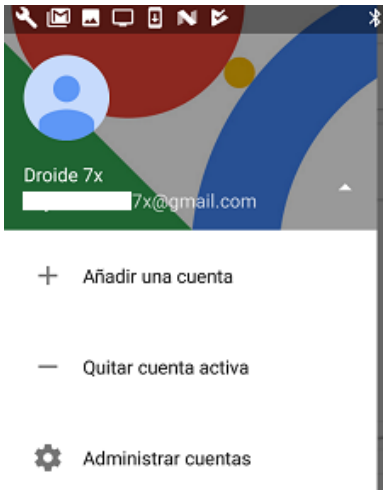
679. Desde el punto de vista de seguridad se recomienda tener un control estricto de la copia de fotos y vídeos entre los diferentes servicios de Google y no habilitar estas capacidades, salvo que se quiera hacer un uso explícito de las mismas. Se dispone de opciones de configuración (descritas a continuación) para controlar estas funcionalidades.

680. Al habilitar la funcionalidad " Crear copia de seguridad y sincronizar", será posible acceder a otros ajustes de configuración avanzados, disponiéndose de información de la cuenta de usuario de Google asociada, del espacio disponible (15 GB por defecto en el momento de elaboración de la presente guía), y detalles como la calidad de la imagen (alta u original), la posibilidad de "Comprar más almacenamiento" con un coste asociado y las carpetas sobre las que se realizará la copia.

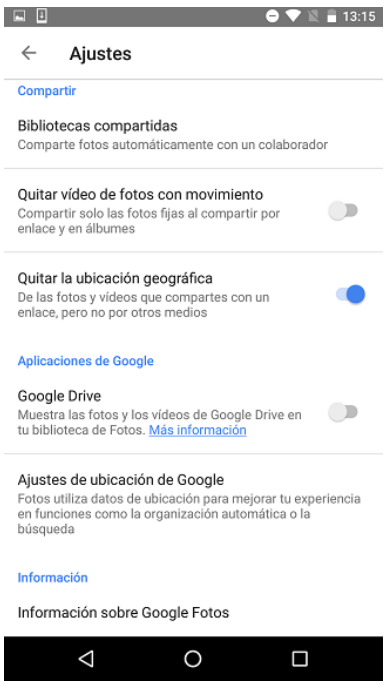


681. Las secciones "Usar datos móviles para las copias de seguridad" y "Cuándo crear una copia de seguridad" permiten respectivamente establecer los ajustes del tipo de redes a emplear para realizar las copias de fotos y vídeos por separado (mencionadas inicialmente) y si se desea hacer uso de la funcionalidad en itinerancia (redes móviles en el extranjero). Se recomienda deshabilitarlas (para evitar incurrir en gastos de telefonía móvil inesperados) y valorar si se desea hacer uso del servicio cuando llegue el momento.

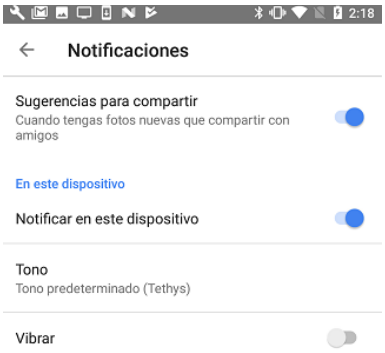
682. La cuenta de usuario de Google vinculada al dispositivo móvil y en la que se están almacenando las fotos y vídeos se muestra en la parte superior de los ajustes de la app "Fotos" y, pinchando sobre ella, es posible eliminarla o añadir más cuentas de usuario de Google adicionales.



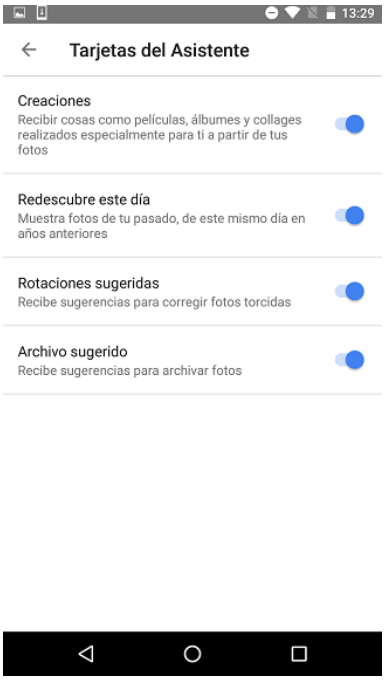
683. Dentro del menú de "Ajustes" de la app "Fotos" para la cuenta de usuario de Google, es posible configurar si estarán disponibles en Google Fotos las fotos y vídeos de Google Drive, y si se incluirá la ubicación geográfica de las fotos en los álbumes compartidos, pudiéndose cambiar esta configuración mediante la opción "Compartir - Quitar la ubicación geográfica":



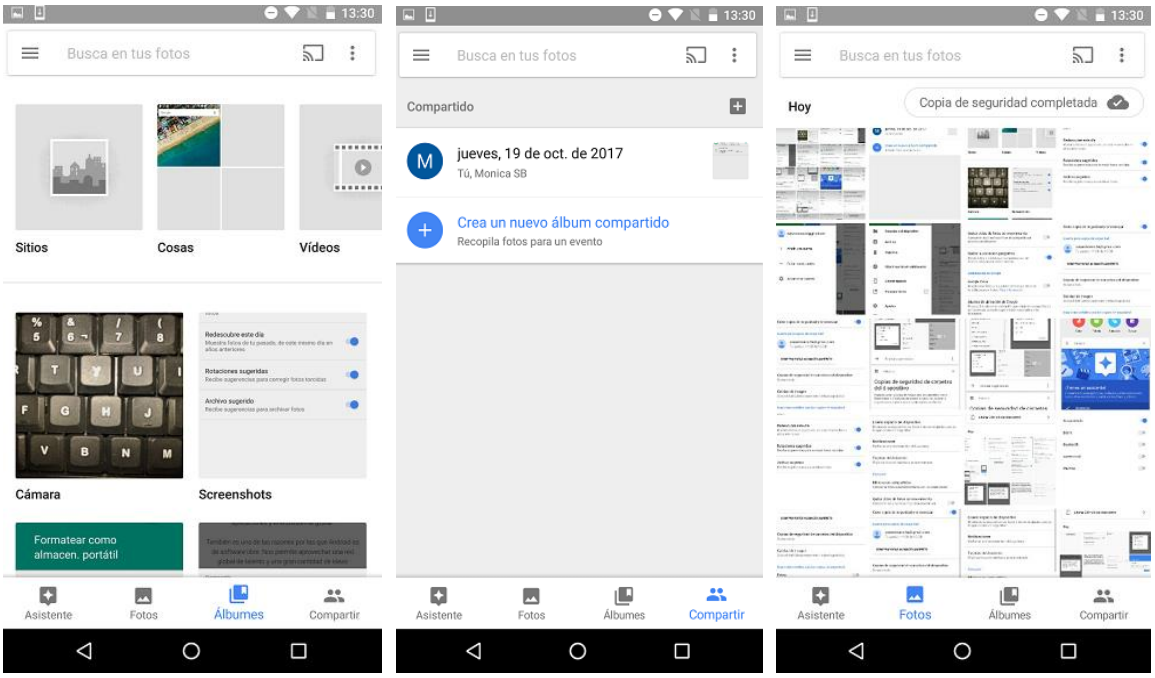
684. El apartado de "Notificaciones" permite habilitar/deshabilitar las notificaciones de la app "Fotos". Entre otras, se puede habilitar/deshabilitar la opción "Sugerencias para compartir", que se encarga de enviar notificaciones cuando se disponga de nuevas fotos para compartir.



685. El menú "Tarjetas del asistente" activará las tarjetas de Google Now correspondientes a la aplicación "Fotos" (ver apartado "8. Asistente de Google, Mi Tablón y Servicios de búsqueda de Google").

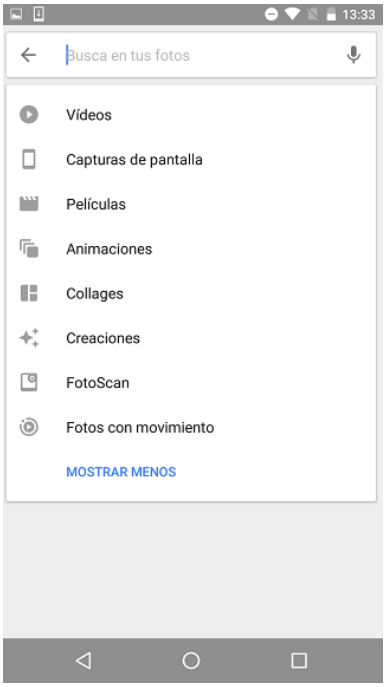


686. En el menú situado en el margen inferior, se pueden visualizar los "Álbumes" disponibles (algunos de los cuales son proporcionados por defecto según la propia clasificación de la app "Fotos"), "Compartir" un álbum y ver qué se ha compartido con otros usuarios o acceder a "Fotos" para verlas según la clasificación por fecha:



687. En el pasado, entre las etiquetas asociadas a las fotos (sitios, cosas, vídeos, etc.) existía la categoría "personas". Esta categoría no se muestra en la versión de la app "Fotos" empleada para la elaboración de la presente guía.

688. La barra de búsqueda, al ser seleccionada, permitirá realizar búsquedas por categoría:



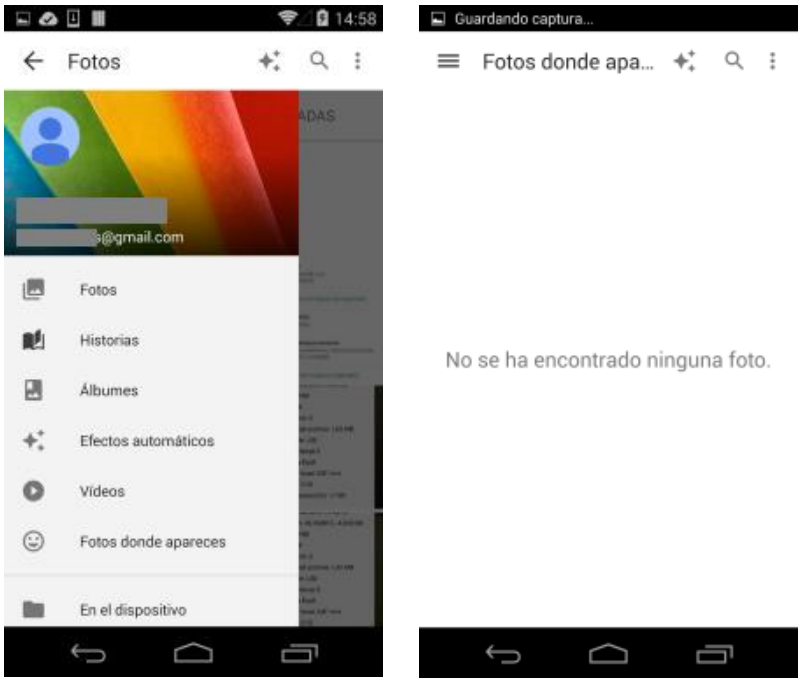
689. En versiones anteriores de la app Fotos, existía la opción "Reconóceme" [Ref.- 179], por medio de la cual se permitía a Google+ solicitar a otros usuarios que se etiquetasen entre ellos en fotos y vídeos, a fin de que fuese posible identificarlos con más facilidad (por cuestiones de seguridad y privacidad, no se recomienda habilitar la integración entre Google + y la app "Fotos").

690. Al activar esta funcionalidad, Google+ creaba un modelo de la cara del usuario en base a las fotos y vídeos en los que ya estaba etiquetado [Ref.- 180]. Este modelo se

actualizaba con las nuevas fotos y vídeos recibidos, y podía ser eliminado desactivando esta opción en cualquier momento.

691. En base a dicho modelo de cara, Google mostraba una sugerencia de etiqueta tanto al usuario como a sus conocidos cuando identificaba ese modelo o patrón de la cara del usuario en una nueva foto o vídeo. Si se desactivaba esta opción, los conocidos del usuario dejaban de recibir sugerencias para etiquetar al usuario en las fotos o vídeos, sin embargo, las etiquetas ya añadidas no se eliminaban.

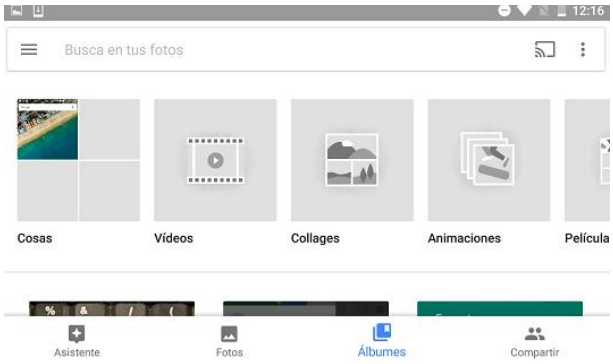
692. En versiones posteriores de la app "Fotos", existía una sección denominada "Fotos donde apareces", disponible desde el menú superior izquierdo, que permitía aprobar o rechazar etiquetas (respondiendo a la pregunta "¿Eres tú?"), así como revisar las fotos en las que el usuario había sido etiquetado [Ref.- 180]:



693. Si se rechazaba la etiqueta, ésta sería eliminada de la foto. Una vez se aprobaba una etiqueta, ésta se asociaba al perfil de Google+ del usuario, y la foto era incluida en la sección "Fotos donde apareces".

694. Para eliminar una etiqueta, desde esta misma sección, se requería seleccionar la foto etiquetada y, mediante el icono con una etiqueta en forma de cara de la parte inferior, emplear el icono de borrar (o papelera).

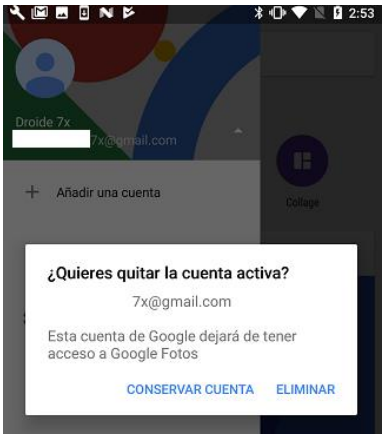
695. En las versiones más recientes de la app "Fotos", se dispone de una barra de búsqueda en la parte superior del menú en la que se muestran categorías para simplificar las búsquedas. Estas categorías son: sitios, cosas, vídeos, collages, animaciones y películas.



696. Adicionalmente, y en función del país que se haya configurado en el dispositivo móvil, pueden aparecer también "personas" y "mascotas", sobre los cuales también es posible aplicar etiquetas para agruparlos y clasificarlos. Tal y como se indica en la documentación oficial de Google para búsquedas en fotos [Ref.- 633], esta funcionalidad no está disponible en todos los países, y, concretamente, no lo está en España a fecha de elaboración de la presente guía.

697. Por el anterior motivo, y porque desde el punto de vista de seguridad y de la privacidad del usuario no se recomienda habilitar funcionalidades de reconocimiento del usuario a través de fotografías y vídeos, se desaconseja el hacer uso de las mismas, aunque se disponga de una configuración que sí lo permita.

698. Finalmente, la opción "Quitar cuenta activa" permite finalizar la sesión actual asociada a la cuenta de usuario de Google, incluida la vinculación entre éste y las fotos y vídeos del dispositivo móvil. Para poder hacer uso de la funcionalidad descrita es necesario volver a añadir una cuenta a través del botón de menú y la opción "Ajustes - Añadir cuenta":



13.3. COPIA DE SEGURIDAD AUTOMÁTICA DE LOS DATOS DE LAS APPS

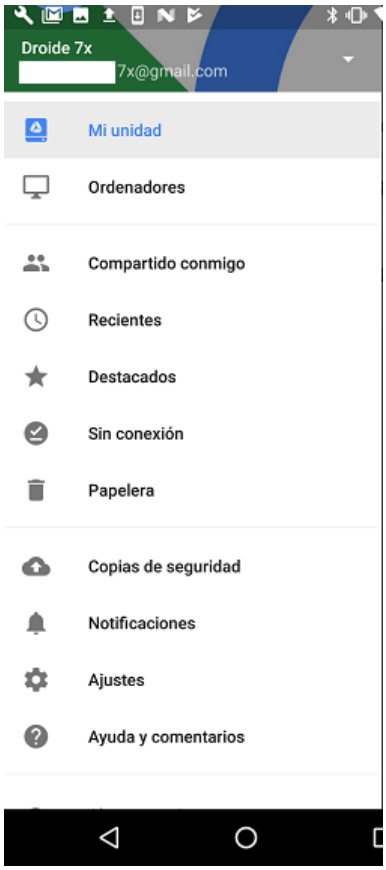
699. Con la introducción de Android 6.x y de la API de nivel 23, se añadió una característica denominada "Auto Backup for Apps" [Ref.- 635], consistente en permitir a las apps definir una política para decidir si hacen uso de las capacidades para salvaguardar los datos (del usuario) en la app en la cuenta de Google Drive asociada a la cuenta de Google del usuario configurada en el dispositivo móvil [Ref.- 634].

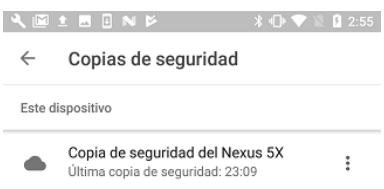
700. Entre los datos asociados a una app, se distinguen tres categorías:

- "Identity data" (datos de identidad): permiten simplificar el acceso a la app por parte del usuario cuando se instala la app en un nuevo dispositivo móvil, sin tener que introducir de nuevo las credenciales. Para que una app pueda ofrecer esta posibilidad, ha de adoptar el servicio "Google Sign-In" [Ref.- 264], por el cual la autentificación dentro de la app se llevará a cabo utilizando las credenciales de la cuenta de Google del usuario. Adicionalmente, la app dispondrá de acceso a la información que el usuario haya publicado en su perfil de la cuenta de usuario de Google.
- "App data" (datos de la aplicación): corresponden al contenido generado por el usuario durante su uso de la app como, por ejemplo, ficheros descargados, imágenes guardadas, etc.
- "Settings data" (ajustes de la aplicación): corresponden a los cambios realizados sobre la configuración por defecto de la app por parte del usuario, como el lenguaje, un tono de aviso, el bloqueo de una acción determinada, etc.

701. Las opciones de backup disponibles para las apps (siendo ambas excluyentes) son:

702. Auto Backup for Apps: los datos de la app se salvaguardan en la cuenta de usuario de Google Drive, con un límite de 25 MB por app (que no se descuentan del almacenamiento disponible para el usuario en Google Drive). Los detalles de los ficheros que se almacenan se describen en la documentación de Android para desarrolladores [Ref.- 265], y el usuario puede comprobar qué apps emplean este servicio a través del interfaz de los "Ajustes de Drive - Copias de seguridad".





703. Key/Value Backup (clave/valor): la app debe definir explícitamente qué contenido desea guardar empleando un formato clave/valor. Para ello, deberá implementar

dentro de su código un cliente de backup, el cual define qué datos se salvaguardarán y cómo se restaurarán cuando sea invocado por su gestor de backup durante los procesos de copia y restauración [Ref.- 266]. Este método se denominaba anteriormente "Android Backup Service", y está disponible desde Android 2.2 (API 8) y superiores.

704. El mecanismo de "Android Auto Backup" permite a las apps incluir y excluir ficheros de la copia de seguridad, y el proceso de backup se realiza de forma automática una vez al día, siempre que el dispositivo móvil tenga acceso a una red Wi-Fi (no puede llevarse a cabo a través de la conexión de datos de telefonía móvil).

705. Para poder salvar sus datos a través del mecanismo de "Android Auto Backup", la app será cerrada por el sistema.

706. El mecanismo de "Key/Value Backup" sí puede realizarse sobre una conexión de datos móviles, y es la app la que debe informar de cuándo tiene datos que desea salvar. El sistema no cerrará la app durante el proceso de backup.

707. El límite de datos que se pueden salvar a través del mecanismo "Key/Value Backup" es de 5MB por aplicación.

708. Dado que es la app y no el usuario quien declara el tipo de servicio de backup que se debe emplear, el único ajuste disponible para el usuario es el de decidir si desea hacer uso del servicio de backup en los servidores de Google a través de "Ajustes - [Personal] Copia de seguridad - Copiar mis datos", pero será la implementación de la app la que decida el mecanismo a emplear en caso de estar activo el servicio.

709. Debe tenerse en cuenta que, si el usuario deshabilita por completo el servicio de copias de seguridad en los servidores de Google, se deshabilitarán tanto las capacidades de copias automáticas de las apps, como las capacidades de backup asociadas al resto de ajustes de Google.

14. APLICACIONES MÓVILES (APPS) EN ANDROID

710. Los siguientes apartados proporcionan breves recomendaciones de seguridad asociadas a las aplicaciones más comunes y relevantes existentes por defecto en Android y asociadas a una cuenta de usuario de Google.

711. Queda fuera del ámbito de esta guía el análisis de seguridad exhaustivo del funcionamiento y de todas las opciones de configuración disponibles en cada app.

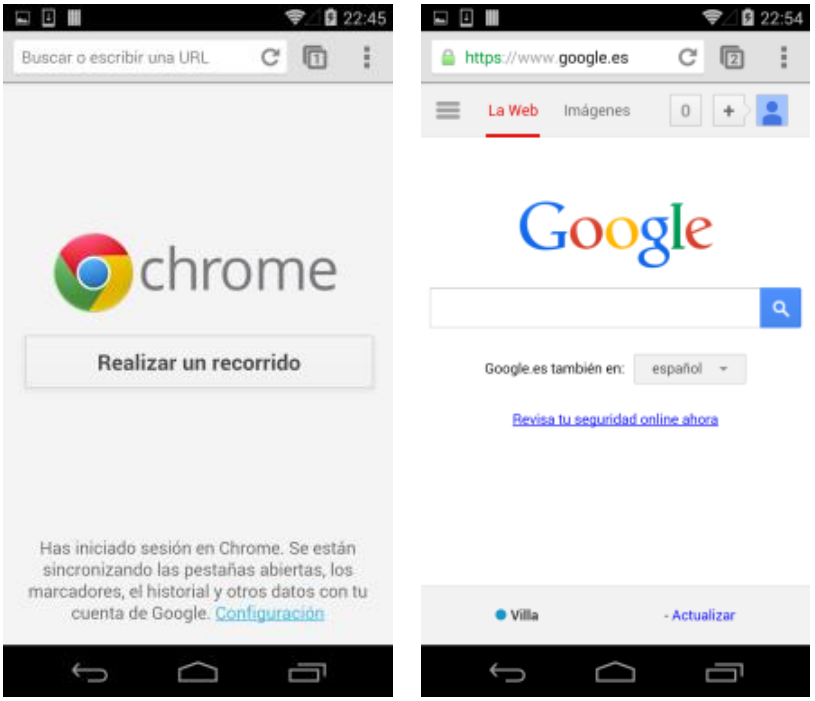
Nota: El número de aplicaciones móviles instaladas por defecto en Android por Google, el fabricante del dispositivo móvil o el operador de telefonía móvil, así como la variedad de apps de otras compañías que pueden ser instaladas posteriormente manualmente o desde Google Play, hace inviable su análisis de seguridad dentro del alcance de la presente guía.

Para todas las apps instaladas o a instalar en el dispositivo móvil, se recomienda realizar una análisis detallado, identificando la versión actualmente instalada, evaluando la gestión de credenciales de acceso (almacenamiento y utilización), así como los protocolos empleados durante el proceso de autentificación y durante el resto de la sesión, y las capacidades de cifrado, tanto para el envío y recepción de datos, como para el almacenamiento de los mismos localmente, junto a cualquier otra característica de

seguridad ofrecida por la app, especialmente los permisos que solicita de cara al dispositivo móvil y los que verdaderamente necesita para funcionar.

14.1. NAVEGACIÓN WEB: NAVEGADOR CHROME

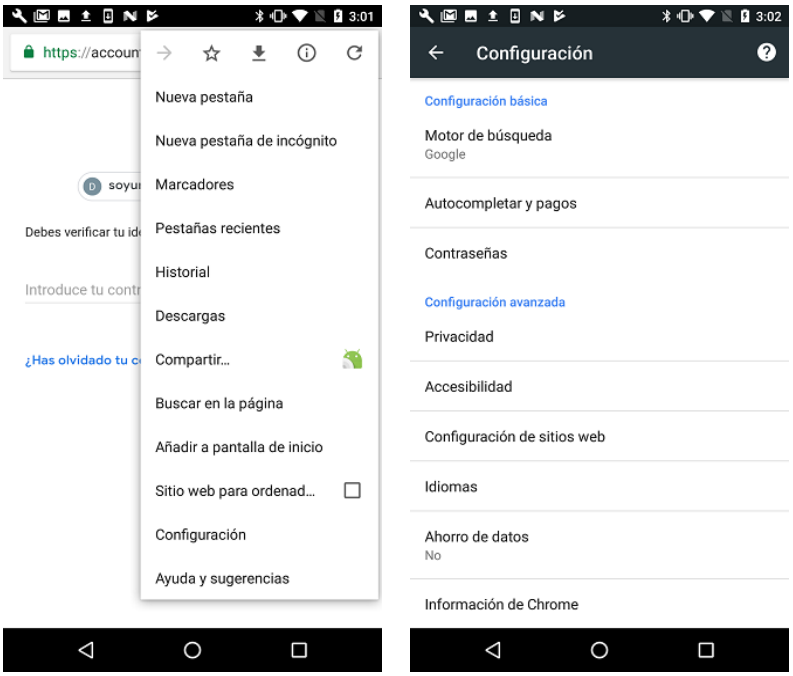
712. Una de las tareas más comunes realizadas desde los dispositivos móviles es la de navegación web por Internet. Android, a partir de la versión 4.3, incluye por defecto el navegador web Chrome, disponible desde el *Launcher*. Chrome está basado en el proyecto de código abierto Chromium [Ref.- 215].



713. Chrome sustituye al navegador web existente previamente por defecto en versiones anteriores de Android, que presentaba carencias de seguridad significativas, tal y como se describe en la versión previa de la guía para Android 2.x [Ref.- 401].

714. Cuando se accede a Chrome por primera vez (esto es válido para todos los usuarios que se den de alta en el dispositivo móvil), Chrome solicitará permiso para "Ayudar a mejorar Chrome enviando estadísticas de uso e informes sobre fallos". También solicitará (si no se ha aceptado previamente), permiso de ayuda a mejorar el teclado (que enviará a Google fragmentos tecleados en aplicaciones de Google). Se recomienda desmarcar estas opciones, por no disponer de control sobre la información que se enviará a Google.

715. A través del botón "Menú" (representado por tres puntos alineados verticalmente) cuando la app de Chrome está siendo ejecutada, es posible acceder mediante la opción "Ajustes" al menú de configuración de Chrome, desde donde se pueden (entre otros) gestionar múltiples ajustes, tanto "[Básicos]" como "[Avanzados]":



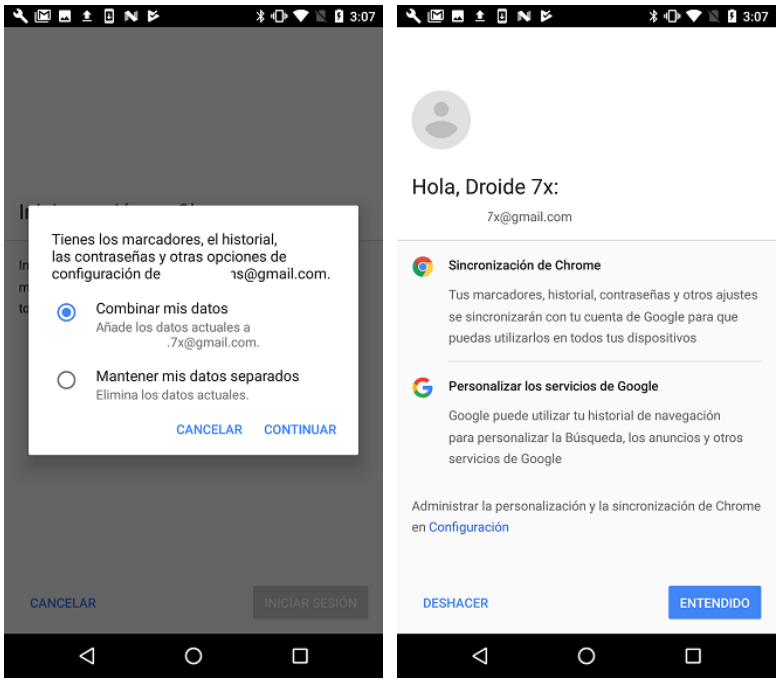
716. La versión de Chrome, que (se obtiene al seleccionar la opción "Información sobre Chrome" en su menú de "Configuración" utilizada en la elaboración de la presente guía) es la 67.0.3396.87.

717. Dado que cada actualización puede añadir, eliminar, renombrar y modificar opciones, puede que algunos de los puntos referenciados a continuación no se correspondan totalmente con los disponibles en otros dispositivos móviles que ejecuten Android 7.x.

718. Chrome soluciona algunas de las limitaciones de seguridad relevantes existentes en el navegador web de Android disponible por defecto en versiones previas del sistema operativo, como por ejemplo contar con soporte para cookies "HttpOnly", empleadas para proteger la sesión de un usuario frente a ataques de Cross-Site Scripting (XSS) [Ref.- 124].

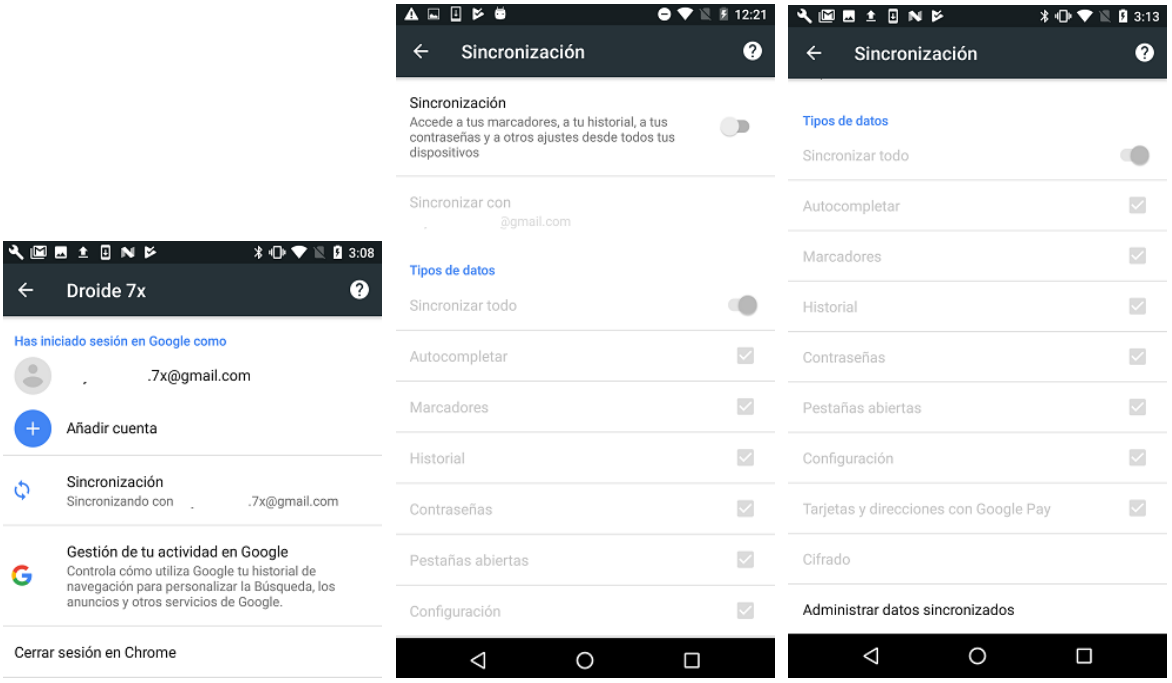
719. Mediante la selección de la cuenta de usuario de Google es posible definir si se hará uso del servicio de sincronización de datos de Chrome que permite sincronizar las pestañas abiertas en el navegador, los favoritos o marcadores, el historial de navegación, la información para autocompletar formularios, e incluso las contraseñas, entre el dispositivo móvil y un ordenador [Ref.- 64].

720. Si se añade una nueva cuenta de usuario de Google en Chrome, y en éste ya había otra configurada previamente, se preguntará si los datos de ambas se deben combinar o mantenerse independientes (lo cual eliminará del dispositivo móvil los datos asociados a la cuenta anterior):

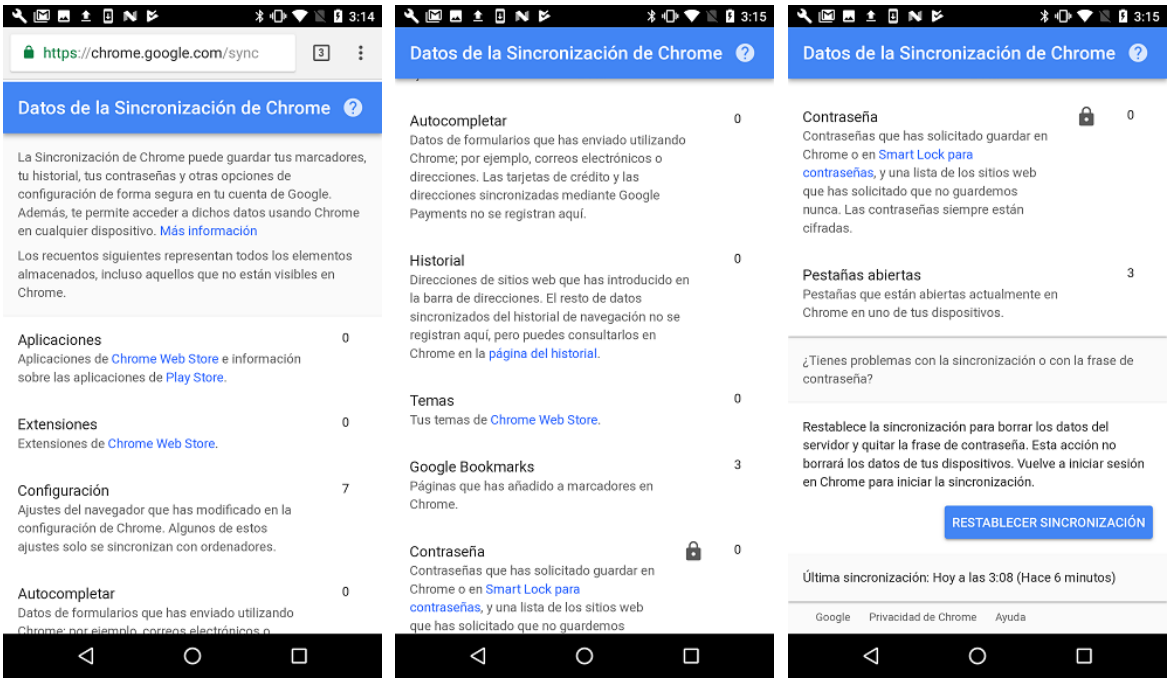


721. Para configurar las opciones de sincronización, dentro de los ajustes de Chrome se debe seleccionar la cuenta y "[Nombre asociado a la cuenta] - Sincronización". Se presentará entonces la pantalla con la opción para activar/desactivar toda la sincronización o marcar de forma selectiva qué se desea sincronizar:

- Sincronizar todo: si se desmarca, se activarán el resto de opciones de sincronización para seleccionarlas/deseleccionarlas individualmente. En caso de requerir hacer uso de esta funcionalidad, se recomienda restringir y minimizar el tipo de datos que serán sincronizados, especialmente, las contraseñas.

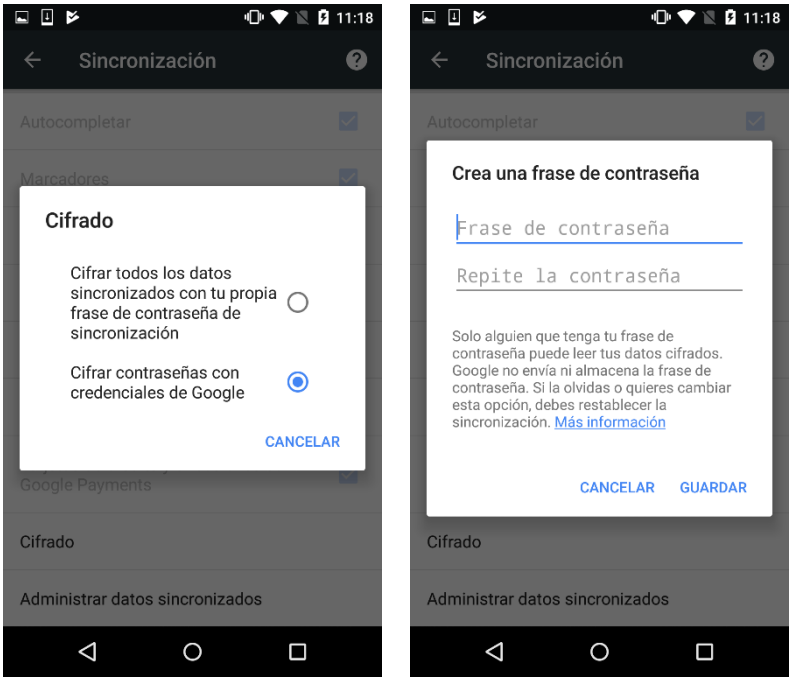


722. Mediante la opción "Administrar datos sincronizados" es posible conocer qué datos hay almacenados en la cuenta de Google del usuario asociados a la sincronización de Chrome:



723. Una opción crítica desde el punto de vista de seguridad y la sincronización de Chrome es la asociada a la opción "Cifrado". Ésta permite dos opciones:

- "Cifrar contraseñas con credenciales de Google" (habilitada por defecto), cifrándose las contraseñas con las credenciales de la cuenta de usuario de Google.
- "Cifrar todos los datos sincronizados con tu propia frase de contraseña de sincronización", opción que permite al usuario establecer una contraseña específica para acceder a los datos sincronizados:

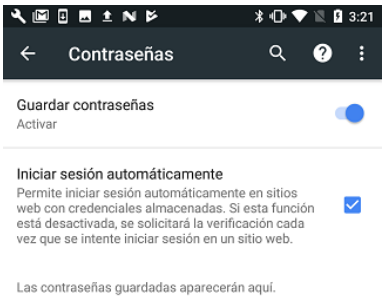


724. La opción recomendada desde el punto de vista de seguridad es no sincronizar las contraseñas mediante este servicio. En caso de hacerlo, se debe hacer uso de la opción de cifrado con la propia contraseña, empleando una contraseña independiente y diferente de la asociada a las credenciales de la cuenta de usuario

de Google, y, especialmente haciendo uso de una frase de paso o *passphrase*, es decir, una contraseña suficientemente larga y robusta [Ref.- 64].

725. Con anterioridad a marzo de 2016, existía un servicio "Chrome to Phone" (de Chrome al móvil", habilitado por defecto) que permitía enviar páginas web desde un ordenador que usara Chrome al dispositivo móvil. Chrome to Phone era un sistema formado por una app para Android y una extensión para el navegador Chrome de escritorio, pero Google dejó de ofrecerlo sin ofrecer ningún sustituto directo. Por tanto, la opción "De Chrome al móvil" que existía en versiones anteriores de Chrome deja de estar disponible.

726. La opción "[Configuración básica] Contraseñas" alberga dos opciones:



- Guardar contraseñas: la gestión de contraseñas se lleva a cabo mediante el servicio "Google Smart Lock" si este servicio está activo (ver apartado "12.2. Servicio de contraseñas de Google Smart Lock"), que almacena los campos en *passwords.google.com*. Salvo que se especifique lo contrario, no se almacenarán las contraseñas correspondientes a las cuentas de Google. Se recomienda deshabilitar esta opción y no recordar las contraseñas, debiendo eliminar las que están almacenadas actualmente. Para eliminar las contraseñas que se hayan almacenado, se ha de buscar la entrada en la lista "Contraseñas" y pulsar "Eliminar".
    - Si el servicio "Smart Lock para contraseñas" no está activo pero el usuario ha iniciado sesión en su cuenta de usuario de Google, Chrome solicitará confirmación para almacenar las credenciales la primera vez que se visite un sitio web que las requiera y también las almacenará en passwords.google.com.
    - Si no se ha iniciado sesión en la cuenta de usuario de Google y el servicio Smart Lock está deshabilitado, Chrome solicitará almacenamiento de credenciales y, en caso de recibir aprobación del usuario, las almacenará localmente en el perfil de Chrome del dispositivo.
- Iniciar sesión automáticamente: permite iniciar sesión automáticamente en los sitios web para los que estén disponibles las credenciales de acceso sin solicitar confirmación del usuario. Esta opción se desaconseja desde el punto de vista de seguridad.

727. En versiones anteriores de la app Chrome, se ofrecía como opción de configuración el "Inicio de sesión automático", que, de activarse, provocaba que se iniciase sesión con las credenciales de la cuenta Google del usuario en los sitios web de Google, de forma automática y sin que se solicitase la intervención del usuario [Ref.- 233]. Esta opción dejó de tener sentido en Android 6.x, ya que la sesión de la cuenta de usuario

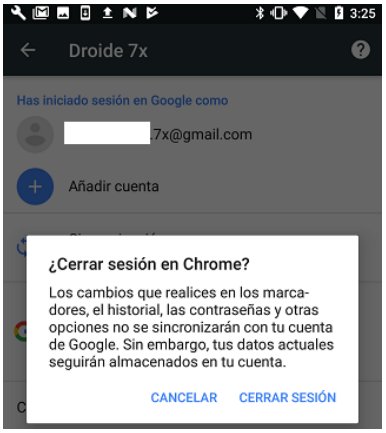
de Google no se cierra salvo que explícitamente se solicite esta acción a través de la opción "Cerrar sesión en Chrome".

728. El propósito de esta funcionalidad es que el usuario pueda sincronizar marcadores, historial de navegación, contraseñas, etc., cuando utilice el navegador web en dispositivos diferentes.

729. Desde el punto de vista de seguridad, se recomienda deshabilitar todas las opciones que implican un inicio de sesión automático, salvo que se requiera hacer un uso explícito de esta funcionalidad, y que se tenga plena consciencia de cuándo tiene lugar una autentificación tanto en los servicios de Google como en otros servicios.

730. Asimismo, se recomienda no almacenar contraseñas automáticamente en Chrome.

731. Para dejar de utilizar la cuenta de usuario de Google en Chrome, en versiones anteriores existía el botón "Desvincular cuenta de Google" (situado en la parte inferior), que permitía al usuario hacer uso de Chrome al margen de la cuenta de usuario de Google, es decir, de manera más anónima e independiente. Con las últimas versiones de Chrome, esta opción explícita desaparece y se incorpora en los ajustes de Chrome relativos a la cuenta y el botón "Cerrar sesión en Chrome". Los datos se dejarán de sincronizar, pero no se borrarán los ya existentes.

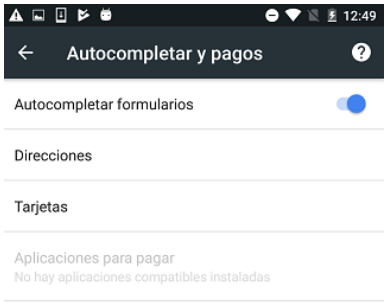


732. Al "Cerrar sesión en Chrome", los ajustes de Chrome pasarán a incorporar como primer campo "Iniciar sesión en Chrome", y, al acceder, se presentarán las cuentas de Google disponibles en el dispositivo móvil para que el usuario seleccione una de ellas. En caso de que exista más de una cuenta con datos ya almacenados por Chrome, se presentará la opción de combinar los datos de ambas cuentas o de mantenerlos separados. Si se opta por mantenerlos separados, los datos actuales se eliminarán ya que, en Android, sólo existe un perfil de Chrome para un usuario concreto (por ejemplo, no es posible tener un perfil de trabajo y otro personal, a diferencia de lo que ocurre en versiones de Chrome para ordenador).

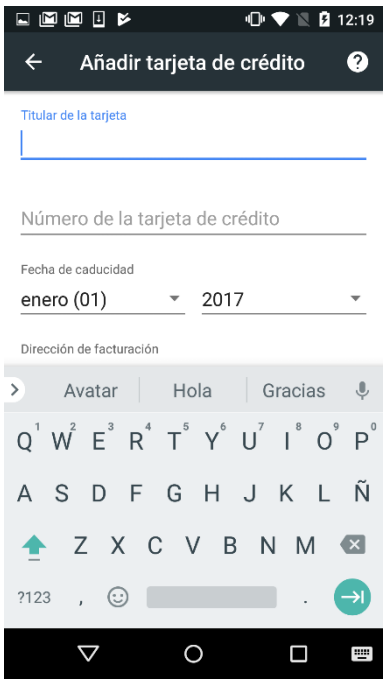
733. Si, aunque está desaconsejado, fuese preciso compartir el dispositivo móvil con otro usuario, se deberá crear un usuario independiente en el dispositivo, y que dicho usuario acceda con su cuenta de usuario de Google a Chrome. Para más información sobre cómo crear usuarios, consultar el apartado "10.9. Múltiples perfiles de usuario".

- Además, al iniciar sesión se activará el menú "Controles de la actividad de tu cuenta", que redirige a la opción "Actividad en la Web y en Aplicaciones" descrita en el apartado "6. Cuenta de usuario de Google".

734. La opción "[Configuración básica] Autocompletar y pagos" presenta 3 apartados:



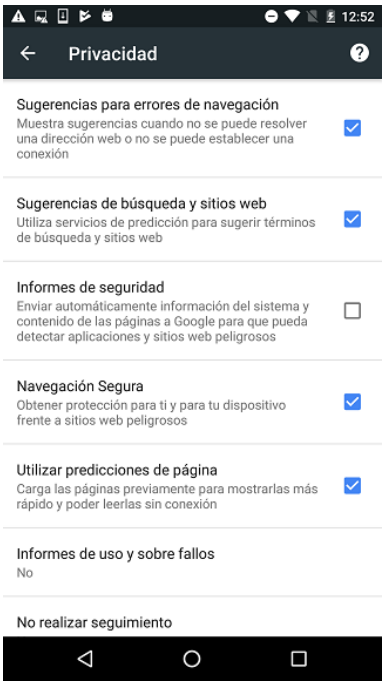
- Autocompletar formularios (habilitada por defecto): permite a Chrome autocompletar formularios con la información del perfil de usuario especificada (por defecto no se dispone de ningún perfil, y éste debe ser añadido con los datos de contacto del usuario).
- Direcciones: añade una dirección al perfil que se usará dentro de la función de autocompletar formularios.
- Tarjetas de crédito: contiene los campos necesarios para poder llevar a cabo la auto compleción de tarjetas de crédito en sitios web que soliciten pagos. Por defecto no se dispone de ninguna tarjeta de crédito, y ésta debe ser añadida manualmente:



735. Se recomienda deshabilitar la opción "Autocompletar formularios", y no recordar los datos introducidos en formularios. En caso de existir información sobre el perfil del usuario o tarjetas de crédito, se recomienda borrar los datos almacenados actualmente.

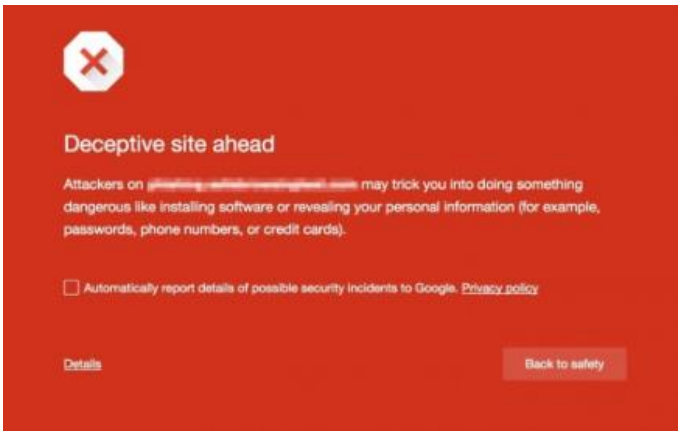
736. Desde la sección "[Configuración avanzada] Privacidad", se pueden obtener sugerencias al presentarse errores de navegación, sugerencias de URLs y búsquedas, y mejorar la carga de páginas web mediante las predicciones de acciones de red. Además, en versiones recientes se ha incorporado la opción "Navegación segura",

que se apoya en la tecnología "Navegación segura" (Google *Safe Browsing*) [Ref.- 235] [Ref.- 216].



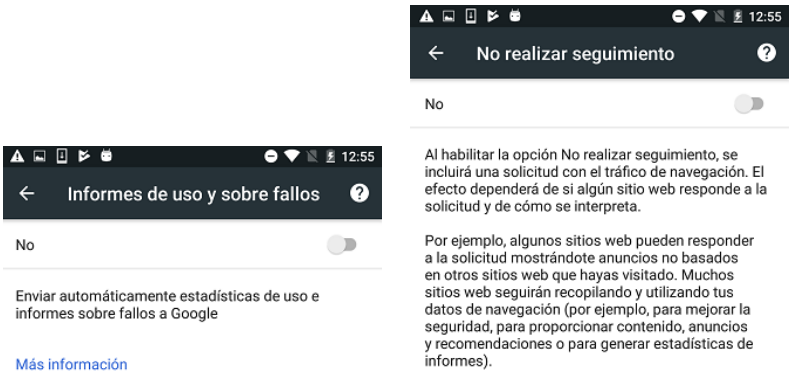
737. Entre otras funcionalidades, la *navegación segura*, la cual analiza millones de URL todos los días, realiza la búsqueda de sitios web no seguros para mostrar advertencias en la Búsqueda de Google y en los navegadores web. Todas estas opciones están habilitadas por defecto. Para deshabilitarlas, hay que desmarcar la opción "Ajustes de Chrome - [Opciones avanzadas] Privacidad - Navegación Segura" [Ref.- 217].

738. Además, la navegación segura pretende prevenir al usuario cuando una página web lanza una ventana en la que se insta a descargar o reproducir algún tipo de malware, o proporcionar información sensible. Chrome mostrará una ventana como la siguiente:



739. Existe también (desmarcada por defecto) la opción "Informes de seguridad", que envía a Google el contenido de las páginas web visitadas para que las incluya potencialmente en sus análisis de sitios no seguros.

740. Adicionalmente se dispone de opciones para el envío de informes de uso y fallos y de solicitudes de no seguimiento (deshabilitada por defecto):

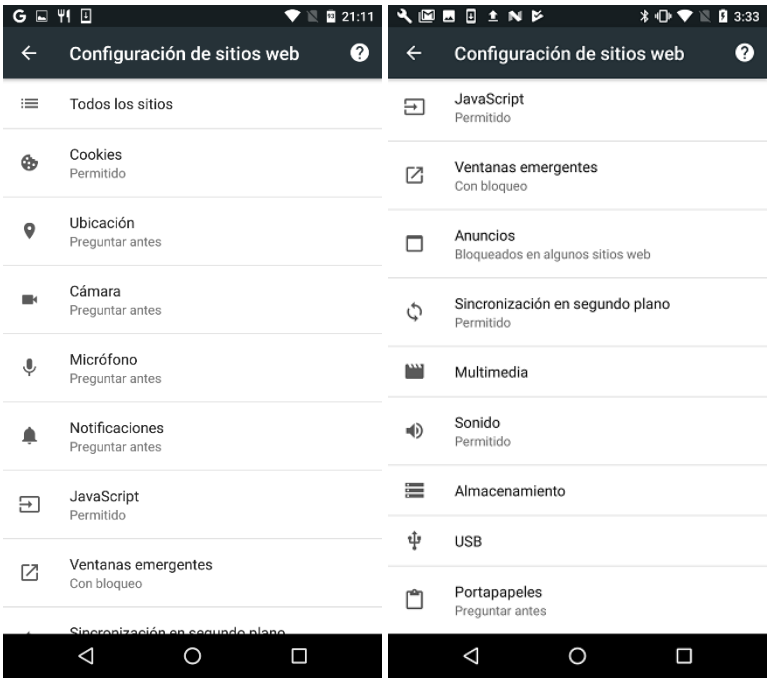


741. Desde el punto de vista de la privacidad del usuario, se recomienda deshabilitar todas las opciones de sugerencias y predicciones descritas.

742. Asimismo, se recomienda no enviar nunca informes de uso y errores, y habilitar las solicitudes de no seguimiento, para que el navegador web añada en sus peticiones la cabecera HTTP "DNT: 1" (Do Not Track, DNT) indicando a los sitios web visitados que no quiere ser monitorizado (el resultado de este ajuste de configuración depende únicamente del comportamiento de los sitios web visitados, que pueden tener en cuenta dicha cabecera, o hacer caso omiso de la misma).

743. La opción avanzada "Accesibilidad" no deberían tener un impacto directo en la seguridad del dispositivo móvil.

744. La opción avanzada "Configuración de sitios web" [Ref.- 218] permite realizar ajustes sobre el contenido de los sitios web visitados, como el uso de "*cookies*" (permitido por defecto), "*JavaScript*" (permitido por defecto), bloquear pop-ups o "*ventanas emergentes*" (bloqueadas por defecto), funcionalidad para la que los sitios web soliciten autorización para acceder al "*micrófono*" y la "*cámara*" del dispositivo móvil (configurados como "preguntar antes" por defecto), "*notificaciones*" (se solicitará autorización al usuario para que dé su aprobación a la petición de enviar notificaciones por parte de un sitio web), la opción "*sincronización en segundo plano*" (para retomar en segundo plano acciones que pueden haber quedado pendientes por haberse perdido la conexión a Internet temporalmente, como la descarga de un archivo), la opción "*multimedia*", que activa la protección de contenido necesaria para la reproducción de música y vídeos *premium* y/o protegidos por *copyright* (configurado como "preguntar antes" por defecto), el *traductor de Google* (configurado a "preguntar antes" por defecto) para que Chrome ofrezca la posibilidad de traducir páginas escritas en otros idiomas, acceso a los ajustes de "*ubicación*" (ver apartado "11. Localización (o ubicación) geográfica"), "*almacenamiento*" (muestra el almacenamiento local del dispositivo que ha utilizado un sitio web) y "*USB*" (permite a un sitio web controlar y registrar información en un dispositivo USB conectado al terminal) [Ref.- 219]:

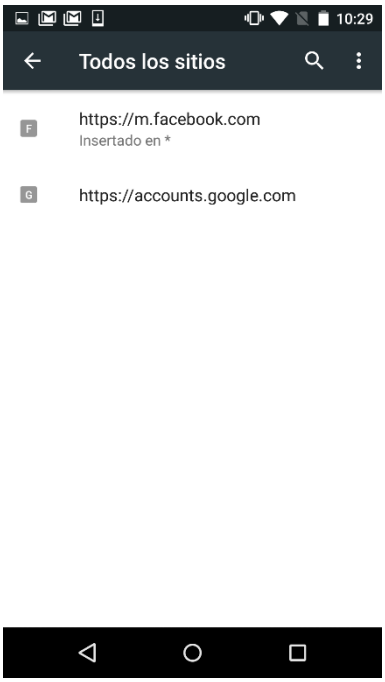


- Para una navegación web más segura, pero muy restringida desde el punto de vista de su funcionalidad, se recomienda deshabilitar la ejecución de scripts (JavaScript), poniendo a "off" el interruptor "Habilitar JavaScript", y el uso de cookies en el navegador web, mediante el interruptor "Aceptar cookies", con el objetivo de mitigar los ataques asociados a la ejecución de scripts maliciosos en el navegador web y a la privacidad del usuario a través de las cookies. Adicionalmente, el bloqueo de pop-ups es una opción que debe estar habilitada. Esta configuración podría dificultar la visualización de páginas web que utilizan scripts y cookies en sus contenidos web y para su funcionamiento (la mayoría de páginas web en Internet), por lo que puede ser necesario tener que dejar habilitadas ambas opciones.
- Se recomienda deshabilitar las opciones "micrófono" y "cámara" para evitar que sitios web puedan realizar llamadas de voz y vídeo no autorizadas o registrar imágenes y sonido sin permiso del usuario.
- La opción "Multimedia - Contenido protegido" permite a sitios web como Netflix o Google Play autentificar al dispositivo móvil para confirmar si dispone de permisos para acceder a contenidos protegidos por *copyright*. Salvo que se haga un uso explícito de este tipo de contenido, se recomienda deshabilitar esta opción.
- La opción "Multimedia - Reproducción automática" controla que se pueda reproducir un vídeo que forma parte de una página web. Se recomienda deshabilitar esta opción, especialmente cuando no se está conectado a una red Wi-Fi, pues la descarga de vídeos supone un importante consumo de datos móviles.

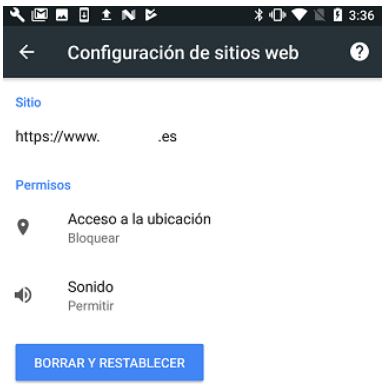
745. La opción avanzada "Ahorro de datos" hace que Chrome comprima las páginas antes de descargarlas. No se aplica a conexiones HTTPS o en el modo incógnito (que permite evitar que Chrome registre datos sobre la navegación) [Ref.- 220]. Se desaconseja habilitarla, pues implica que los datos de navegación serán enviados a los servidores de Google para que estos compriman los contenidos antes de

descargarlos. Es decir, Google podría disponer de todos los detalles sobre las páginas web visitadas por el usuario, excepto para las páginas web accedidas mediante HTTPS o desde una pestaña de incógnito. Aunque esta funcionalidad también ofrece otros mecanismos de protección, como por ejemplo la detección de páginas con contenido malicioso, o involucradas en esquemas de suplantación de identidad, se desaconseja su utilización ya que el impacto sobre la privacidad del usuario al habilitarla es muy elevado.

746. El menú de Chrome "Configuración - [Configuración avanzada] Configuración de sitios web - Todos los sitios" permite obtener una lista de sitios web visitados que han accedido al almacenamiento local y/o a la ubicación, y ver los permisos otorgados a cada uno de ellos individualmente. Cada uno de estos elementos puede ser gestionado de forma particular:

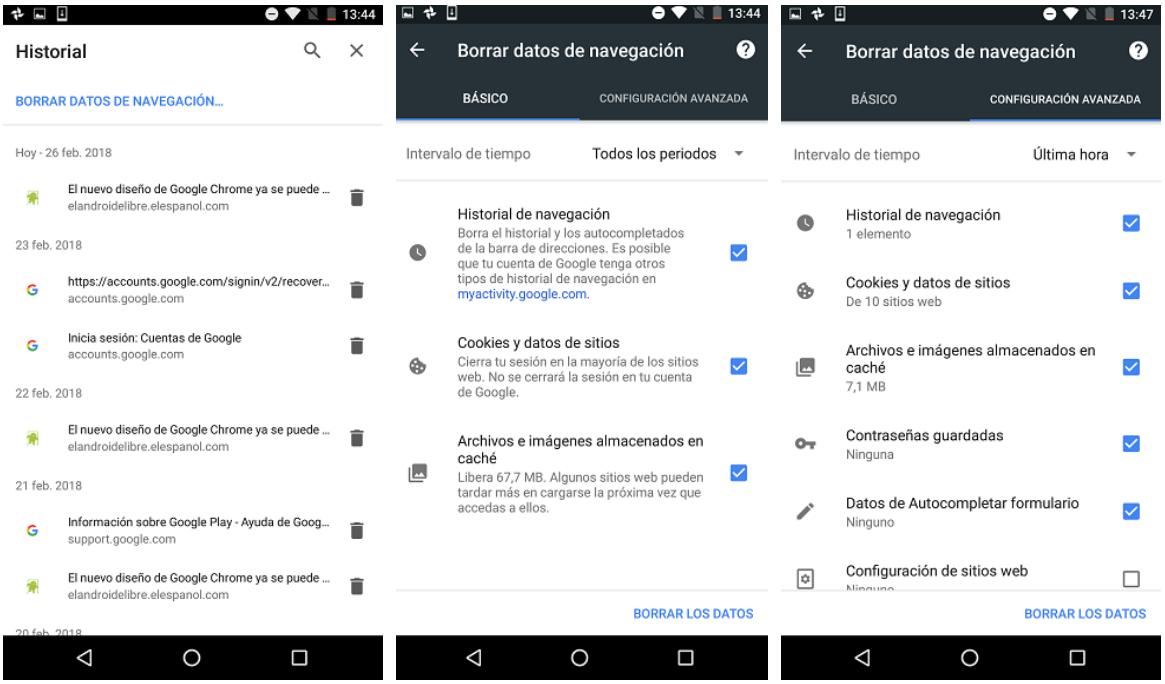


747. Accediendo a cada entrada específica de un sitio web, se puede consultar si se le han permitido notificaciones, pop-ups, si se ha aplicado algún ajuste de configuración por defecto (identificado con el carácter comodín "*"), o la posibilidad de borrar los datos almacenados en caché para un sitio web concreto, aparte de las capacidades de habilitar o deshabilitar el acceso a la ubicación:



748. Por otro lado, y en lugar de hacerlo de forma individual por cada sitio web, desde el menú "Historial" de Chrome (fuera del menú de "Configuración") es posible borrar

los datos de navegación de manera global, mediante la opción "Borrar datos de navegación" (que incluye un apartado de "Configuración avanzada"):



749. Estos datos incluyen el historial de navegación, la caché, las cookies y otros datos almacenados por los sitios web, las contraseñas y los datos para autocompletar formularios, almacenados actualmente.

750. Desde el punto de vista de seguridad y privacidad del usuario, se sugiere aplicar las recomendaciones descritas previamente para cada sección con el objetivo de limitar la exposición del dispositivo móvil durante las actividades de navegación web.

751. Se recomienda borrar de forma frecuente (tanto globalmente, como de forma individual para ciertos sitios web específicos, según las necesidades del usuario) tanto la caché como el historial de navegación web, así como el almacenamiento de cookies, y datos de formularios y contraseñas, con el objetivo de proteger la privacidad del usuario.

752. La versión de Chrome utilizada en la elaboración de la presente guía no permite el uso de perfiles compartidos en Chrome, lo cual resulta muy conveniente desde el punto de vista de la seguridad y la privacidad [Ref.- 234].

753. La opción "[Básica] Motor de búsqueda" determina qué motor se utilizará cuando se introduce un término en la barra de navegación del navegador que no corresponde con un servidor web (por ejemplo, una búsqueda por palabras). Por defecto, se realiza una búsqueda de dicho término a través del buscador de Google ("www.google.com")[17], pero es posible cambiarlo por Yahoo!, Ask, AOL o Bing.

754. Este comportamiento tiene implicaciones de seguridad relevantes al revelar (potencialmente) en Internet la información introducida en la barra de navegación, como por ejemplo el nombre de servidores internos de una organización.

[17] También puede emplearse la versión localizada del buscador de Google según el país. Ej. "www.google.es".

755. Adicionalmente, la información del dispositivo móvil se desvela en los parámetros de la URL de "www.google.com" empleada para las búsquedas, incluyendo referencias a Chrome para Android, es decir, del navegador web y del tipo de plataforma móvil:

```
GET /search?q=cni+ccn&oq=cni+ccn&aqs=chrome..69i57.4923j0j4&client=ms-
android-google&sourceid=chrome-mobile&ie=UTF-8 HTTP/1.1
Host: www.google.es
```

756. Cuando el navegador web accede a Internet, por ejemplo al buscador de Google, la cadena de caracteres que identifica al navegador web o agente de usuario (User-Agent) tiene el siguiente valor, revelando excesivos detalles sobre la versión del navegador web y la plataforma:

```
User-Agent: Mozilla/5.0 (Linux; Android 7.1.2; Nexus 5X Build/ N2G47O; wv)
AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/64.0.3282.137
Mobile Safari/537.36 MinuteMaid
```

757. Los detalles del dispositivo móvil incluyen la plataforma ("Android"), la versión de Android ("7.1.2"), el modelo de terminal ("Nexus 5X"), la versión de compilación de Android ("N2G47O"), o los detalles del navegador web (incluyendo su versión exacta y múltiples versiones de sus componentes: "64.0.3282.137 Mobile Safari/537.36 MinuteMaid").

758. Se recomienda modificar el valor del agente de usuario para que no desvele información adicional. Desde el botón de menú, es posible hacer uso de la opción "Sitio web para ordenad…" para forzar a Chrome a usar un agente de usuario distinto, similar al empleado por un ordenador. Este agente de usuario emula la utilización del navegador web Chrome sobre un ordenador Linux genérico, aunque incluye de nuevo los detalles del navegador web (como, por ejemplo, su versión exacta):

```
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/64.0.3282.137 Mobile Safari/537.36 MinuteMaid
```

759. Se recomienda evaluar si habitualmente se desea realizar la navegación web como un ordenador o equipo de sobremesa (opción recomendada desde el punto de vista de seguridad para no desvelar los detalles reales del dispositivo móvil), más expuesto a ataques genéricos sobre todas las versiones del navegador web pero que probablemente no tengan éxito en el dispositivo móvil, o como dispositivo móvil, más expuesto a ataques dirigidos a este tipo de terminales y con posibilidad mayor de éxito.

760. Debe tenerse en cuenta que la modificación del agente de usuario, y especialmente el valor de la plataforma (tradicional o móvil), podría afectar a la presentación de los contenidos web de ciertos servidores y aplicaciones web que personalizan las respuestas en función de si el cliente es un dispositivo móvil o un ordenador (de sobremesa o portátil).

Nota: La modificación o eliminación de información de las cabeceras HTTP puede afectar a la funcionalidad de servidores y aplicaciones web que hacen uso de dichos datos para procesar y mostrar contenidos web personalizados para el tipo de dispositivo cliente.

Estas implicaciones se han mencionado igualmente a lo largo de la presente sección al deshabilitar otras funcionalidades disponibles habitualmente en los navegadores web.

Las recomendaciones de seguridad descritas a lo largo de toda la sección pretenden incrementar el nivel de seguridad y privacidad del dispositivo móvil y de su usuario, pudiendo afectar por tanto a la funcionalidad, por lo que deben ser aplicadas únicamente si no es necesario hacer uso de la funcionalidad asociada.

761. En la versión de Chrome utilizada para la elaboración de la presente guía, las búsquedas en Google han introducido un nuevo procesamiento de las búsquedas que emplea el protocolo QUIC [Ref.- 221]. Cuando el navegador envía una búsqueda al motor de Google, como parte de la petición se devuelve que se puede utilizar QUIC en adelante, por lo que las siguientes peticiones de búsqueda se enviarán a través de este protocolo, que combina UDP, HTTP2 y TLS:

```
Alt-Svc: quic=":443"; ma=2592000; v="38,37,36,35"
```

762. Algunos módulos de navegación web de Android, como el asociado a la información del GPS y gpsOneXTRA (ver apartado "11.4. GpsOneXTRA"), añaden la siguiente cabecera WAP que permite identificar el tipo de terminal (fabricante y modelo):

```
x-wap-profile:
http://www.openmobilealliance.org/tech/profiles/UAPROF/ccppschema-20021212#
```

763. El UAProf (*User-Agent Profile*) es un documento XML que contiene información sobre las características y capacidades de un dispositivo móvil, estándar definido por OMA, Open Mobile Alliance. El documento está especificado en las cabecera HTTP "x-wap-profile" (o "Profile"), apuntando normalmente a una web del fabricante del terminal (repositorio de perfiles).

764. El perfil puede contener información muy detallada del dispositivo móvil, incluyendo los perfiles Bluetooth, los tipos y formatos de datos soportados, protocolos de seguridad y de transferencia de datos soportados, capacidades push, WAP, MMS y de *streaming*.

765. En el caso de Android, el perfil referenciado está asociado a una plantilla genérica para dispositivos móviles definida por la OMA, sin desvelar detalles particulares del terminal.

14.1.1. CONTENIDOS ADOBE FLASH

766. Adobe anunció en noviembre de 2011 que no soportaría Adobe Flash en dispositivos móviles [Ref.- 109], en favor de las tecnologías basadas en HTML 5.

767. Por este motivo, Adobe Flash no está soportado en el navegador web Chrome para Android [Ref.- 113] disponible por defecto en esta plataforma móvil.

768. Pese a que otros navegadores web para Android sí pueden disponer de soporte para Flash, como por ejemplo Firefox[18], Boat o Dolphin, desde el punto de vista de seguridad no se recomienda su instalación, ya que la misma se basa en la instalación de versiones antiguas del reproductor de Flash para dispositivos móviles (Adobe

[18] https://support.mozilla.org/es/kb/firefox-para-moviles-no-admite-flash

Flash Player), para el que con una muy alta probabilidad se conocerán vulnerabilidades existentes públicamente.

769. Debe tenerse en cuenta que las mejoras de seguridad incorporadas en las últimas versiones de Flash Player para los equipos de escritorio ya no están disponibles en Flash Player para Android.

14.1.2. CONTENIDOS ADOBE PDF

770. Hasta Android 4.4.4, se incluía por defecto una app para la lectura de ficheros PDF denominada Quickoffice, siendo también posible instalar el cliente oficial Adobe Reader desde Google Play. Con Android 5.x (Lollipop) se introdujo un *framework* denominado *PdfRenderer* que permite que la aplicación que lo invoque pueda abrir en su contexto ficheros PDF [Ref.- 222].

771. Se permite también al acceder a contenidos PDF desde el navegador web. Chrome descargará el fichero PDF automáticamente (a la carpeta general de "Descargas", o "Download", del almacenamiento interno del dispositivo móvil; ver imágenes siguientes) y el mismo podrá ser accedido también a través de la notificación del navegador web de que el fichero ha sido descargado:

772. Al seleccionar el fichero PDF, éste será abierto automáticamente mediante la actividad "PdfViewerActivity", según se puede ver a través de "*adb logcat*":

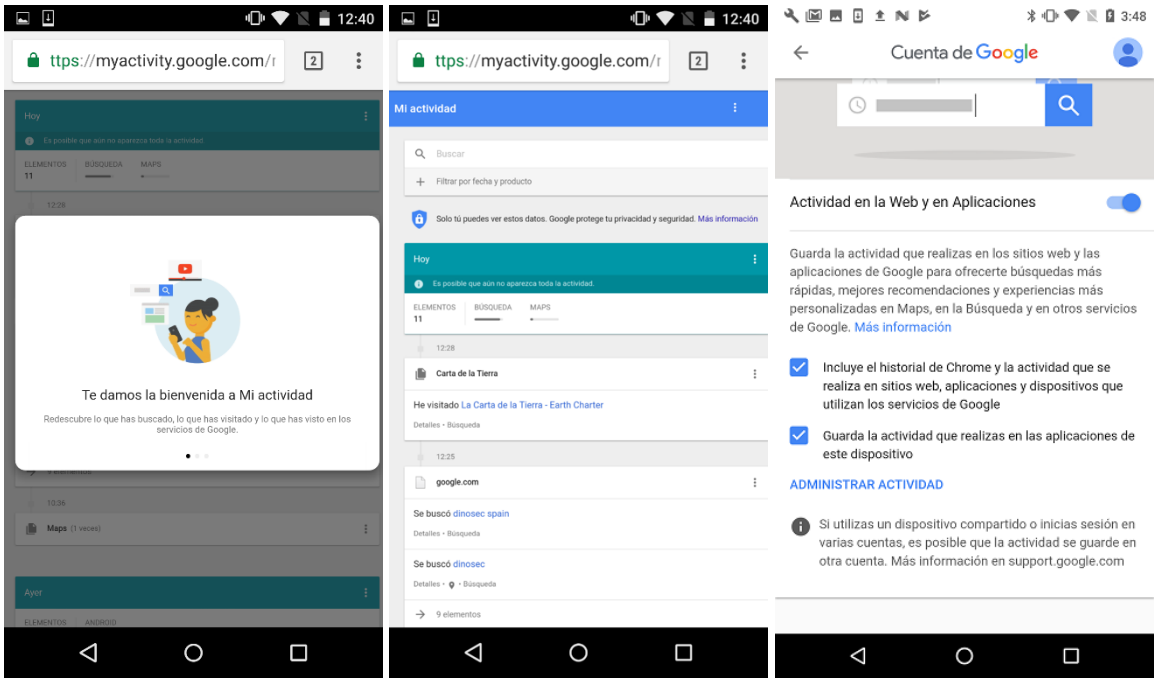
```
I ActivityManager: Displayed
com.google.android.apps.docs/com.google.android.apps.viewer.PdfViewerActivit
y: +322ms
```

773. En Android 7.x, el servicio de lectura de ficheros PDF se realiza a través de la app "Drive", la cual invoca internamente la actividad "PdfViewerActivity"). Adicionalmente, se puede instalar la app "Visor de PDF de Google" (o cualquier otro visor de un desarrollador de confianza, como Adobe Acrobat, Adobe Reader, Foxit, etc.) si no se desea que la visualización de PDFs se realice a través de "Drive".

774. Debido a las numerosas vulnerabilidades de seguridad en las aplicaciones cliente de visualización de ficheros PDF durante los últimos años, se recomienda siempre mantener actualizada la app de visualización de ficheros PDF a la última versión.

14.1.3. HISTORIAL DE ACTIVIDAD WEB Y DE APLICACIONES

775. La información correspondiente a las búsquedas realizadas por el usuario a través de Google, así como la actividad de navegación web y de otras apps, es almacenada en el portal "Mi actividad" de la cuenta de usuario de Google, disponible a través de la URL "https://myactivity.google.com/myactivity" y a través de la sección "Controles de la actividad de tu cuenta - Actividad en la Web y en Aplicaciones" de la sección "Datos y personalización" (imagen inferior derecha; ver apartado "6.2.1.2. Datos y personalización").

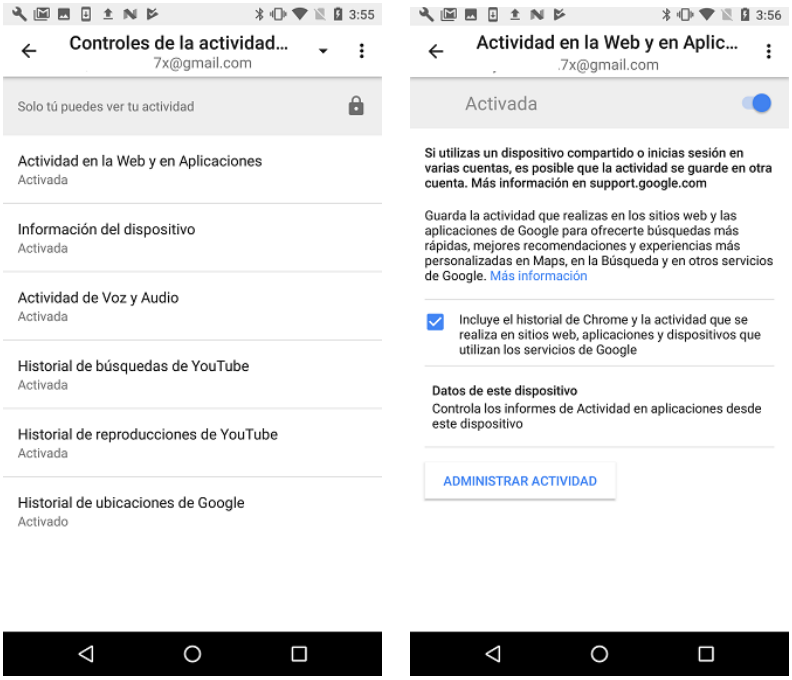


776. Supuestamente, esta información es utilizada para proporcionarle al usuario mejores resultados y recomendaciones (más relevantes) al usar los productos y servicios de Google, como por ejemplo los servicios de búsqueda web y de mapas (con predicciones de búsqueda más precisas), conocer los resultados de las búsquedas en los que el usuario pulsa, conocer los anuncios visualizados por el usuario, poder acceder rápidamente a páginas web que ya se han visitado (disponiendo del historial de búsquedas recientes realizadas en cualquier dispositivo móvil u ordenador con la misma cuenta de usuario), la dirección IP del usuario, el tipo de navegador web empleado y su idioma, etc. [Ref.- 177].

777. El historial de actividad web y de aplicaciones puede estar desactivado si la cuenta de usuario de Google no ha sido vinculada a ningún dispositivo móvil Android, pero en caso de haberse llevado a cabo esta vinculación, y dado que esta funcionalidad está habilitada por defecto, el servicio estará activo.

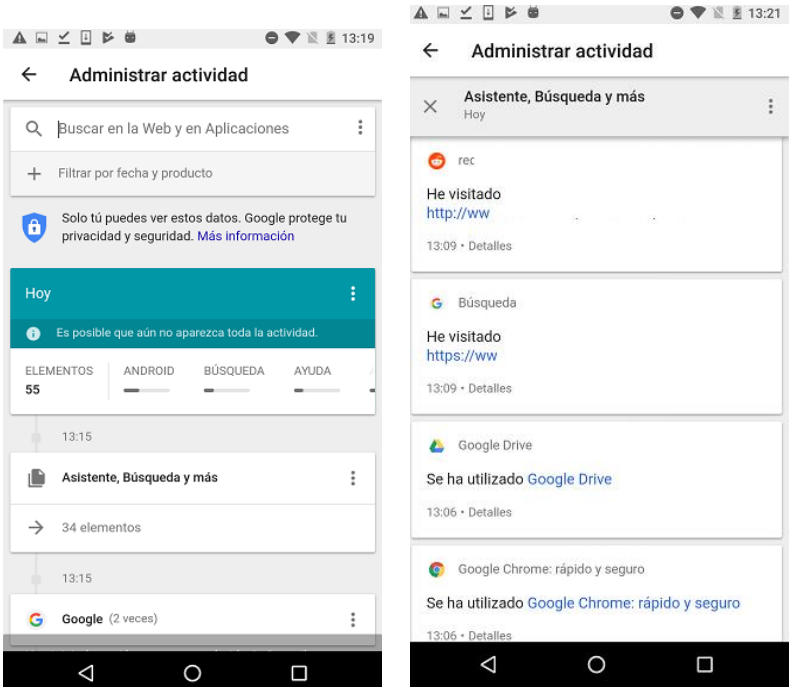
778. Si se activa desde la página web, es posible especificar si se desea incluir en el historial la actividad de Chrome "Controles de la actividad de tu cuenta". Asimismo, también es posible controlar los permisos y actividad de otras aplicaciones a través de la página "https://myaccount.google.com/permissions".

779. Para ello, también es posible utilizar los ajustes de la app "Google" bajo "[Buscar] Cuentas y privacidad - Controles de la actividad de tu cuenta de Google - Actividad en la Web y en Aplicaciones":

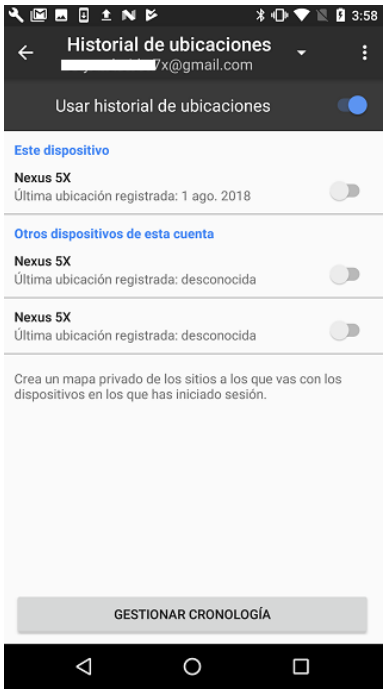


780. Se recomienda sopesar la activación de la funcionalidad de historial de actividad web y de aplicaciones, incluyendo estas capacidades adicionales que permiten incluir en el historial la actividad de Chrome y de otras aplicaciones, salvo que se desee hacer un uso explícito de las mismas.

781. La opción "Administrar mi Actividad" permite acceder y administrar el historial de actividad web y de aplicaciones, y dispone de detalles sobre las búsquedas y otras actividades clasificadas por servicios de Google e incluso clasificadas por fechas y horas, y obtener información detallada de todas las búsquedas realizadas:



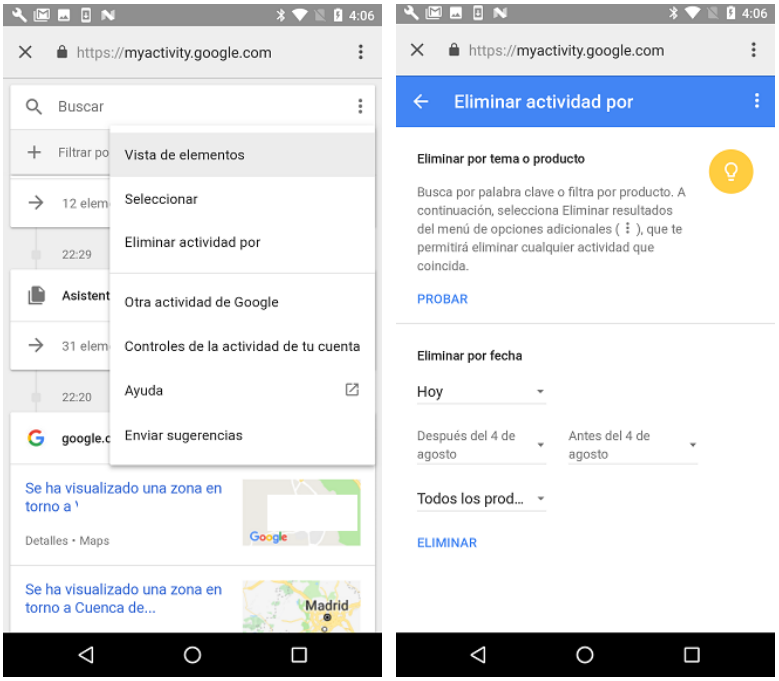
782. El menú "Controles de la actividad de tu cuenta" contiene también la opción "Historial de ubicaciones", que determina si se almacenará un mapa con las ubicaciones en las que algún dispositivo vinculado a la cuenta de usuario de Google ha sido localizado. Se recomienda mantenerlo sin activar por motivos de privacidad.



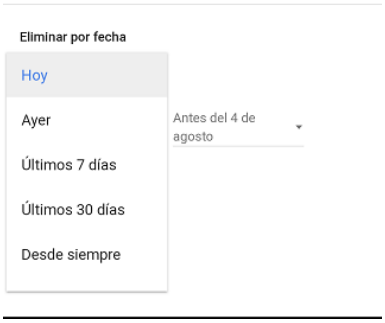
783. Mediante la opción "Gestionar cronología" es posible eliminar los registros del historial individualmente.

784. Para eliminar elementos en un rango temporal, se deben seguir las indicaciones expuestas en "Eliminar la actividad guardada en Mi Actividad" [Ref.- 177].

- Desde la app "Ajustes - [Personal] Google - Cuenta de Google - Datos y personalización - Actividad y cronología - Mi Actividad", seleccionando el icono de "..." del campo "Buscar" seguido de "Eliminar actividad por":

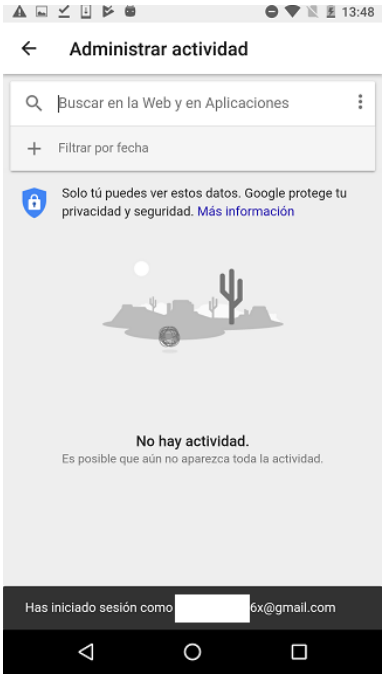


Para eliminar el historial completo, en lugar de existir un botón específico, se desplegará el menú de "Eliminar por fecha" y se deberá marcar "Desde siempre", seguido de "Eliminar". Se solicitará doble confirmación antes de proceder al borrado.



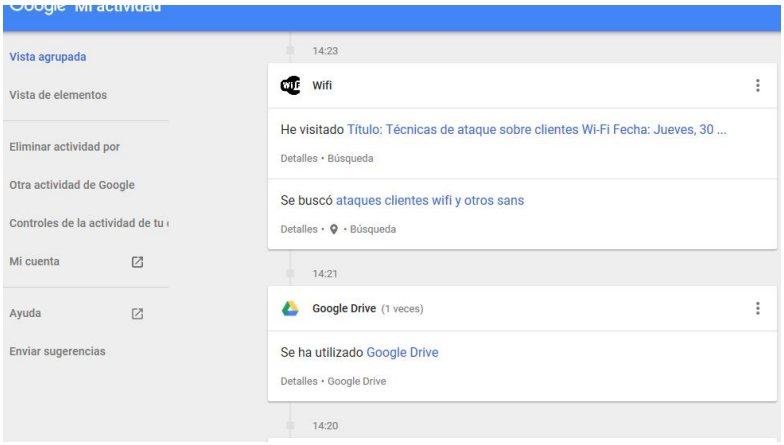
- El historial web puede ser desactivado en cualquier momento desde la página web y desde Android, y en concreto desde la app "Ajustes - [Personal] Google - Cuenta de Google - Datos y personalización - Controles de la actividad de tu cuenta - Actividad en la Web y en Aplicaciones", deshabilitando la opción "Activada" (para más información, consultar el apartado "6. Cuenta de usuario de Google").

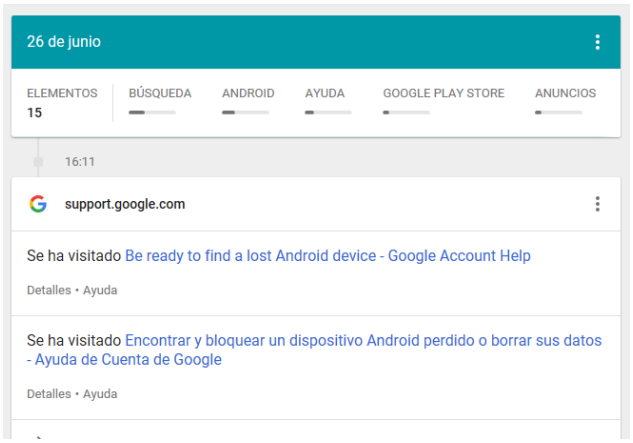
785. Cuando el historial ha sido eliminado, desde el dispositivo móvil o desde la página web, no se dispone de datos asociados a esta funcionalidad:



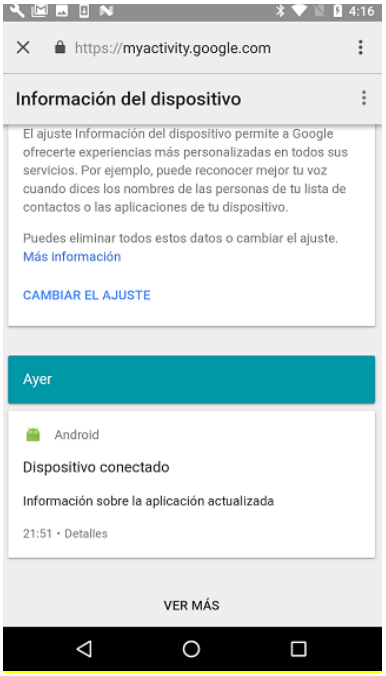
786. En el caso de haber incluido en el historial la actividad de Chrome y de otras aplicaciones, que estará disponible en la página "Mi actividad" (descrita previamente), mediante el botón "+ Filtrar por fecha y producto" también es posible eliminar elementos selectivamente en función del periodo temporal.

787. Los elementos del historial web incluyen términos de búsqueda, tanto en el buscador web general de Google como, por ejemplo, en las búsquedas por apps en Google Play, YouTube, etc., incluyendo el día y hora en que se utilizaron dichos términos, durante los últimos años:





788. Adicionalmente, es posible almacenar información sobre los dispositivos, que guardará datos sobre todos los dispositivos desde los que se haya iniciado sesión en la cuenta de usuario de Google. Esta opción se configura mediante "Controles de la actividad de tu cuenta - Información del dispositivo".



789. En caso de haberse activado esta opción y quererse eliminar, hay que acceder al menú " Controles de la actividad de tu cuenta - Información del dispositivos - Administrar actividad - […] Eliminar todo".

790. Cuando se detecta el acceso a la cuenta de Google de un usuario desde otro dispositivo diferente al que ya la tiene activa, el sistema Android mostrará una notificación indicando este hecho e invitando a revisar la configuración de la cuenta. Si se selecciona, se mostrará una ventana "Revisa el dispositivo" con información sobre el tipo de equipo, la versión de navegador, la ubicación y la hora del acceso. En ese punto, se puede confirmar o denegar que el acceso se llevó a cabo por parte del usuario.

14.2. CORREO ELECTRÓNICO (E-MAIL) Y GMAIL

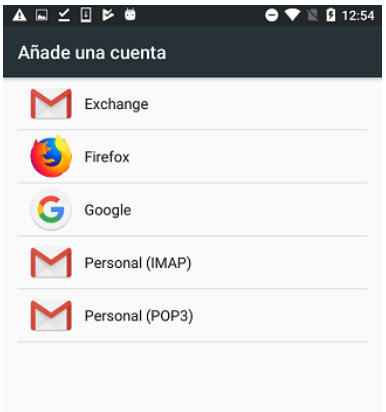
791. Android proporciona múltiples capacidades para la gestión de correos electrónicos (e-mails) desde el dispositivo móvil, disponibles a través del icono o app "Correo" (app genérica de correo) desde el *Launcher* (como por ejemplo cuentas de correo de Exchange, IMAP o POP3, cuyo análisis detallado queda fuera del alcance de la presente guía), o desde el icono o app de "Gmail" (app específica de acceso a Gmail), desde los cuales es posible configurar una o varias cuentas de correo electrónico.

792. Asimismo, existe una relación muy estrecha entre las cuentas de correo electrónico registradas, y las cuentas vinculadas al dispositivo móvil (ver apartado "6. Cuenta de usuario de Google").

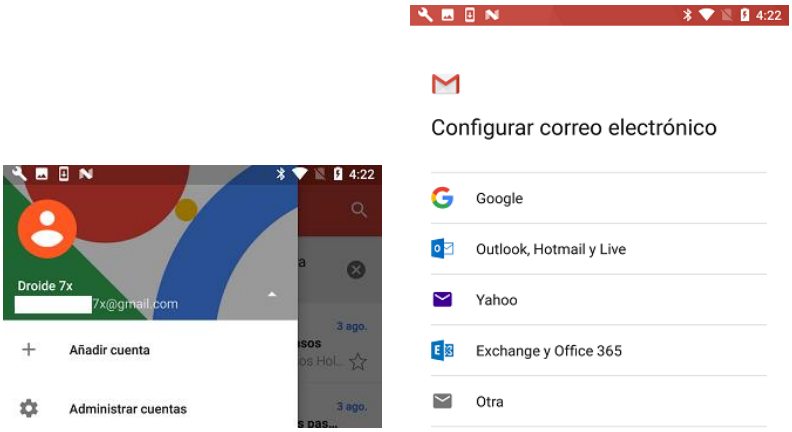
793. Si se lleva a cabo la configuración de cuentas de correo electrónico mediante Exchange, POP3, o IMAP, incluyendo el envío de e-mails mediante SMTP, se recomienda siempre habilitar la opción de seguridad para hacer uso de conexiones cifradas (TLS), y deshabilitar cualquier opción que permita aceptar todos los certificados TLS (como aquellos no válidos, que no son de confianza o que están autofirmados).

794. Para configurar una cuenta de correo en el dispositivo, las opciones son:

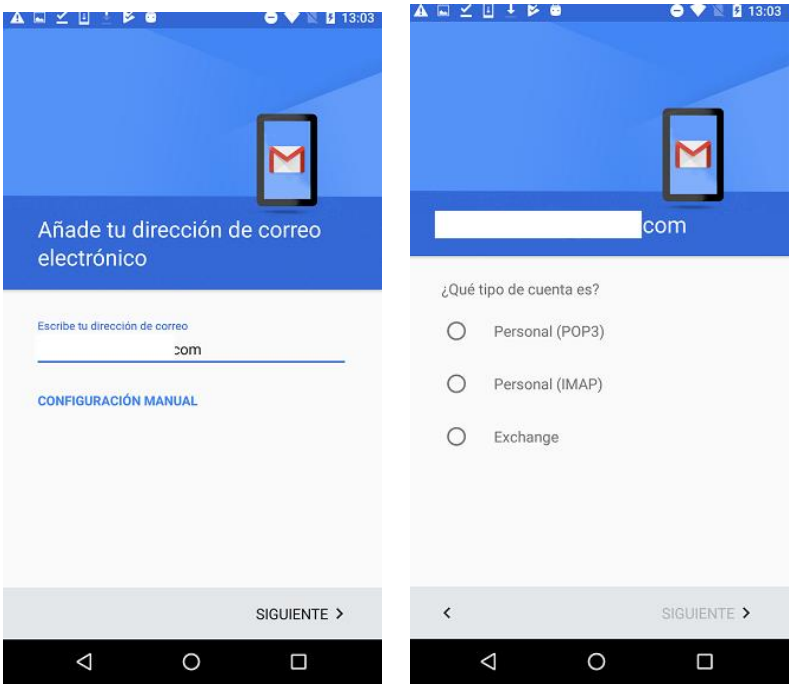
- "Ajustes - [Personal] Cuentas - + Añadir cuenta [Añade una cuenta]".

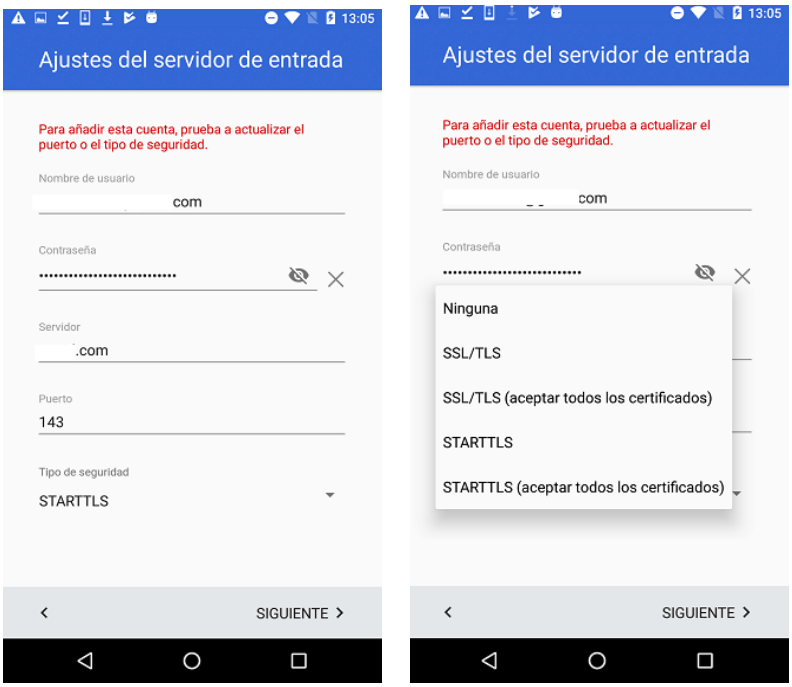


- Aplicación Gmail: "Ajustes - seleccionar a la derecha de una cuenta sobre el símbolo de desplegar - Añadir cuenta". Esta opción permite añadir los siguientes tipos de cuenta:



795. Desde Android 5.x, la opción de tipo de seguridad disponible por defecto para IMAP y POP3 al añadir una nueva cuenta de correo electrónico mediante configuración manual es "STARTTLS" (en Android 4.x y anteriores era "Ninguna"):





796. En el caso de Exchange, la opción por defecto es "SSL/TLS", disponiéndose adicionalmente de la posibilidad de seleccionar un certificado digital cliente de usuario para llevar a cabo la autentificación con el servidor de correo electrónico.

797. En cualquier caso, debe siempre seleccionarse "SSL/TLS" o "STARTTLS", haciendo énfasis en que en ningún caso debe seleccionarse ninguna de las opciones con el texto "(aceptar todos los certificados)".

798. Debido a que la vinculación del dispositivo móvil con una cuenta de usuario de Google es prácticamente obligatoria, y a la relación existente entre esta cuenta y el servicio de correo de Google, Gmail, esta funcionalidad estará habilitada normalmente.

799. Desde el punto de vista de seguridad, no se disponen de opciones avanzadas de configuración asociadas a Gmail desde el dispositivo móvil Android, ni siquiera a través del menú "Ajustes", haciendo por defecto uso de cifrado mediante TLS.

800. Aunque hasta la versión 4 de Android se podría utilizar las capacidades de *certificate pinning* (CP)[19], no aceptándose cualquier certificado digital como válido al establecerse una conexión cifrada mediante TLS con los servidores de Google [Ref.-80], los servicios de Google desde Android, por ejemplo Gmail, YouTube o Google Play (entre otros), no hacían uso de mecanismos de protección propios basados en *certificate pinning*, y aceptaban cualquier certificado digital de confianza que hubiera sido importado previamente por el usuario en Android. Esto permitía analizar las conexiones TLS con los servidores de Google y averiguar, por ejemplo, que el User-Agent de la app identifica a la propia app en la petición, así como el tipo de dispositivo móvil (bullhead) y el número de compilación.

```
User-Agent: Android-GmailProvider/60087425 (sw411dp; 420dpi) (bullhead MTC20K); gzip
```

801. Desde Android 7.x, con la nueva característica conocida como "Network Security Configuration (NSC)", las apps de Android no confían en los certificados digitales

[19] https://developer.android.com/training/articles/security-ssl.html

importados por el usuario, no resultando tan sencillo analizar estas conexiones sin modificar el fichero APK de la app.

802. Respecto a la gestión de las credenciales de acceso a Gmail, se recomienda seguir las recomendaciones descritas en el apartado "6. Cuenta de usuario de Google".

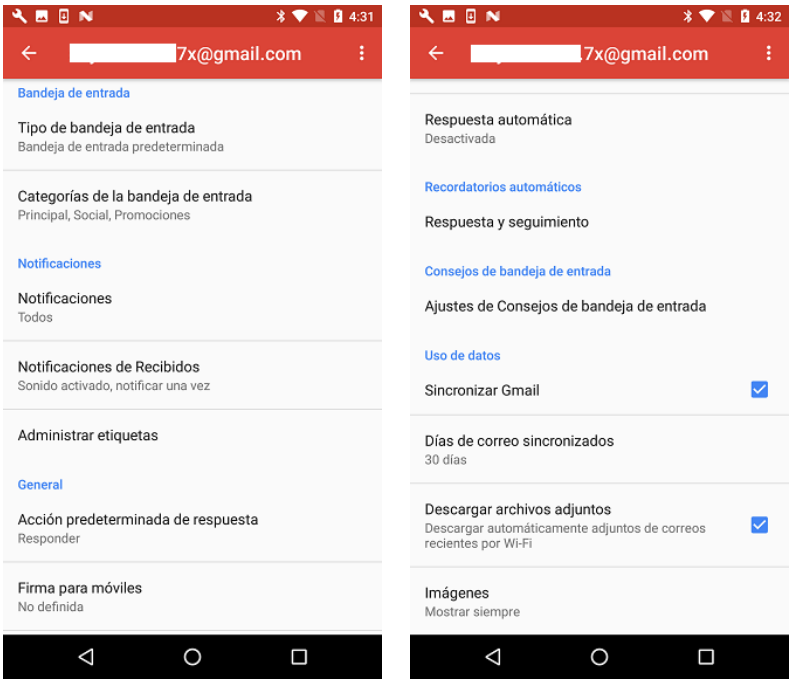
803. Los ajustes de la aplicación de correo son accesibles desde la propia aplicación, mediante el botón de menú y "Ajustes". Además de los "ajustes generales", comunes a todas las cuentas de correo gestionadas desde la aplicación Gmail, los ajustes específicos para la cuenta se acceden seleccionando la cuenta.

804. Los ajustes de la aplicación Gmail quedan fuera del alcance de la presente guía, por lo que, si se desea utilizar esta app, se recomienda al usuario revisarlos de forma detallada. Sin embargo, como carácter informativo, se expondrán algunos ajustes importantes desde el punto de vista de la seguridad y la privacidad.

805. Por defecto, al escribir un nuevo mensaje o e-mail desde la app de Gmail, el dispositivo móvil no añade ninguna firma, opción recomendada desde el punto de vista de seguridad para evitar indicar desde donde se realiza el envío, como por ejemplo "Enviado desde un dispositivo móvil".

806. Se recomienda mantener la configuración por defecto, con el valor de firma puesto a "No definida", para no revelar información del fabricante o tipo de dispositivo móvil. En caso de querer añadir una firma, en ningún caso debería incluir detalles del terminal.

807. La gestión de las firmas se puede realizar desde el botón de menú de la app de Gmail, mediante la opción "Ajustes - <cuenta de usuario de Google> - Firma para móviles" (por defecto "No definida"):



808. Por defecto, el ajuste "Descargar archivos adjuntos" está habilitado, de forma que los adjuntos a los correos se descargarán automáticamente si se detecta la utilización de una conexión Wi-Fi. Se recomienda deshabilitar esta opción y dejar que el usuario decida cuándo descargar y abrir un adjunto en función de la confianza que se tenga en el mismo.

14.3. INSTANT APPS

809. Las "Android Instant Apps" son aplicaciones nativas Android que se ejecutan de forma instantánea sin requerir instalación en el dispositivo móvil. En lugar de ello, el portal web que distribuye la app proporcionará una URL que, bajo demanda, cargará sólo la parte de una app necesaria para ejecutar una determinada acción.

810. Uno de los principales beneficios de las Instant Apps es no tener que instalar aplicaciones sólo para realizar una tarea específica desde una web (por ejemplo, realizar un pago, pedir un taxi, etc.), sino aprovechar una app propia disponible a través de un enlace web al portal que proporciona el servicio, desde el que se cargará la app requerida.

811. Al evitar la instalación y desinstalación de apps que sólo se requieren puntualmente, se ahorra espacio en el dispositivo móvil.

812. Las Instant Apps permiten a los desarrolladores segmentar su app en módulos que pueden ejecutarse independientemente dentro de un sandbox, de forma que sólo se descargará el código necesario para una determinada acción, con el consiguiente ahorro de RAM en el dispositivo móvil. Por ejemplo, un usuario está de viaje en el extranjero y necesita pedir comida rápida. En lugar de instalar la aplicación de una cadena de restauración, el portal web puede ofrecer un enlace que lance la funcionalidad de búsqueda de menú (en lugar de toda la app); además, se puede integrar con Android Pay para que el usuario pueda completar el pago sin requerir más acción por su parte.

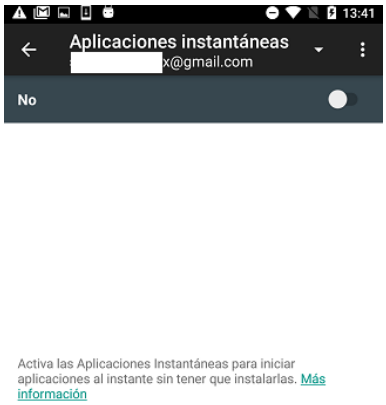
813. Según Google, el esfuerzo a nivel de desarrollo para transformar una app tradicional en una Instant App es mínimo, pues no requiere rediseñar la app.

814. Aunque las Instant Apps se presentaron en el Google I/O de 2016 [Ref.- 241], estas son compatibles con dispositivos desde Android 4.1 (nivel de API 16) y Google Play Services [Ref.- 240].

815. Son varios los propósitos de las Instant Apps: por un lado, pretenden mejorar la experiencia del usuario aprovechando su integración con las funciones de Google Play Services (como la ubicación, la identidad, los pagos, etc.); por otro, permitir a los desarrolladores de apps que las mismas sean usadas sin necesidad de instalarse físicamente en el dispositivo móvil.

816. Desde el punto de vista de seguridad, surgen varias cuestiones a tener en cuenta: cuál será la gestión de permisos de las Instant Apps (especialmente en dispositivos anteriores a Android 6.x), cómo saber si se puede confiar en una Instant App que se abre desde un determinado enlace web, cómo saber si una Instant App cumple con políticas de seguridad corporativas, qué potenciales riesgos introduce la propia traducción de un enlace web a código ejecutable… [Ref.- 242] [Ref.- 243]. Por el momento, Google no ha elaborado ningún documento técnico abordando estas cuestiones, por lo que se recomienda tener prudencia a la hora de hacer uso de esta funcionalidad.

817. Si no se desea hacer uso de este tipo de aplicaciones, se puede deshabilitar su uso a través de "Ajustes - [Personal] Google - [Servicios] Aplicaciones instantáneas" y mover el interruptor a la posición "No".



15. GOOGLE NEARBY

818. 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.

819. En sus orígenes, se fundamentaba en las denominadas "Nearby Notifications", soportadas desde Android 4.4 (KitKat), mediante la generación de notificaciones dependientes de la ubicación en apps y sitios webs. Por ejemplo, estas permiten mostrar mensajes sobre productos en promoción dentro de un supermercado, guiar al usuario dentro de un museo, o iniciar conversaciones entre apps de mensajería.

820. Para ello, la app o sitio web que desea hacer uso de estas notificaciones, debe asociarse con un dispositivo BLE (Bluetooth LE o Smart) o un beacon EddyStone o iBeacon [Ref.- 255]. Cuando un dispositivo móvil Android con capacidad Nearby se aproxima a un dispositivo de ese tipo, la pizarra de ajustes "Nearby Quick Settings" parpadeará y 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.

821. La funcionalidad de notificaciones Nearby está implementada internamente en los servicios de Google Play.

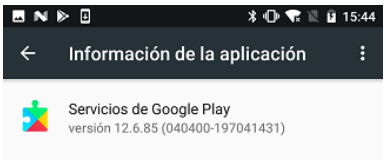
822. Las denominadas "Nearby Connections" son una API de comunicaciones extremo a extremo destinada al descubrimiento, conexión e intercambio de datos entre dispositivos en tiempo real, aunque no estén conectados a través de una red con una infraestructura [Ref.- 751].

823. Para ello, 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.

824. En el Google I/O de septiembre de 2017, Google comunicó las novedades relativas a la API de conexiones Nearby, que proporcionan mayor ancho de banda, menor latencia y transferencias de datos cifradas entre dispositivos con capacidades Nearby,

y basadas en comunicaciones P2P offline[20]. Estas novedades están disponibles desde la versión 11.0 de los servicios de Google Play.

825. La versión de los servicios de Google Play es la 12.6.85 a fecha de elaboración de la presente guía.



826. Su configuración detallada se realiza a través del menú "Ajustes - [Personal] Google - Nearby", y requiere activar tanto Bluetooth como el servicio de ubicación [Ref.- 751].

827. No obstante, debido al uso que hace de las comunicaciones Bluetooth y Wi-Fi, la recomendación desde el punto de vista de seguridad sería poder deshabilitar el servicio Nearby.

Importante: No se conoce ningún ajuste en Android 7.x que permita deshabilitar el uso de Nearby en los dispositivos Nexus o Pixel. Ni tan siquiera mantener deshabilitados los interfaces Bluetooth o Wi-Fi impedirá que se realicen escaneos Bluetooth y/o Wi-Fi si en el sistema existen aplicaciones con capacidades Nearby, tal como se constata en la siguiente imagen, procedente de la ayuda de Google para Nearby [Ref.- 751].

Sí se tiene constancia de que otros fabricantes ofrecen ajustes para deshabilitar estos escaneos.

828. En general, desde el punto de vista de seguridad, se recomienda prescindir de las aplicaciones que hagan uso de ese servicio.

[20] https://youtu.be/1a0wII96cpE?t=23m2s

16. PROCESO DE INSTALACIÓN Y CONFIGURACIÓN INICIAL VINCULADO CON UNA CUENTA DE USUARIO DE GOOGLE

829. El presente apartado ilustra el proceso de instalación de Android 7.1.2 vinculando el dispositivo móvil a una cuenta de usuario de Google, que puede ser nueva o existente.

16.1. CREACIÓN DE UNA CUENTA DE USUARIO DE GOOGLE NUEVA

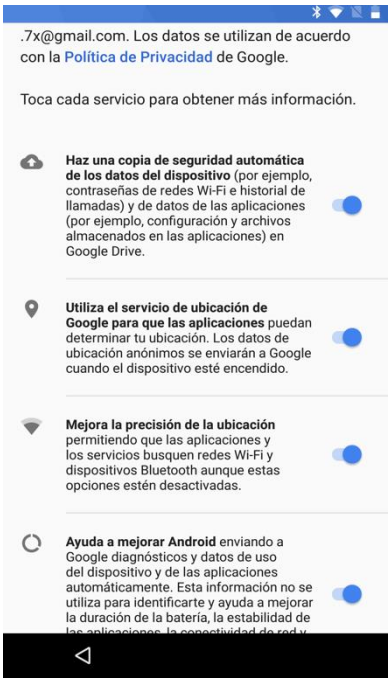
830. Si no se dispone de una cuenta de usuario de Google y se desea que el dispositivo móvil se vincule a una, se procederá a su creación.

831. Para crear una nueva cuenta de usuario de Google, se solicita el nombre y apellidos del usuario, seguido de lo que se denomina "Información Básica" y que consta de la fecha de nacimiento y el sexo del usuario (pudiéndose omitir éste). Estos campos deben rellenarse antes de proceder, si bien se permite la opción "Prefiero no decirlo" para el campo "sexo".

832. Tras introducir la información anterior, se debe de elegir el nombre de la cuenta de usuario de Google, asociado a la cuenta de Gmail (nombredeusuario@gmail.com). Hay ciertos nombres de usuarios no permitidos, por ejemplo, los que contengan la palabra "android". Una vez se elige un nombre de usuario válido (que no incumpla ningún criterio no permitido, ni se encuentre ya en uso), se podrá seleccionar la contraseña asociada, y se presentará la pantalla de aceptación de las condiciones de servicio.

833. El siguiente paso propone establecer el bloqueo asociado al dispositivo mediante huella dactilar. Este proceso es similar al descrito en el apartado anterior, por lo que no se repetirá:

834. Tras definir el método de acceso, se iniciará sesión con la nueva cuenta de usuario de Google, empleando una conexión cifrada mediante HTTPS, y se presentan al usuario los distintos servicios de Google disponibles (todos ellos marcados por defecto):

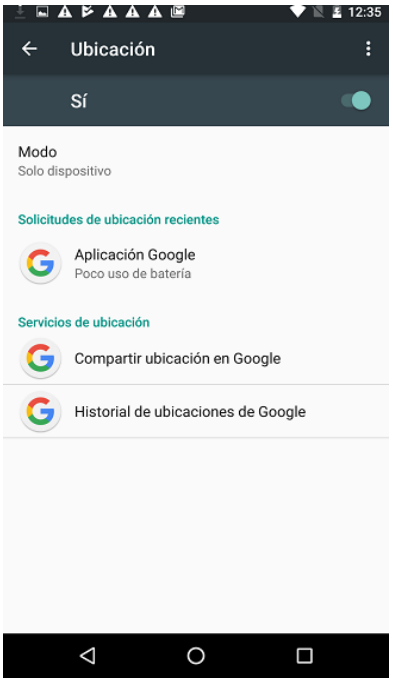


835. Entre los servicios de Google disponibles para seleccionar, se incluye el servicio de ubicación, la ayuda para mejorar los servicios de ubicación (descritos posteriormente) y la ayuda para mejorar la experiencia del usuario con Android.

836. Respecto a los servicios de ubicación (o localización), se dispone de dos opciones:

- Usar el servicio de ubicación de Google: es necesario para que las aplicaciones puedan determinar la ubicación del dispositivo móvil, pudiendo éstas remitir datos de ubicación anónimos a Google, aunque no estén siendo utilizadas (teóricamente del módulo GPS, de redes Wi-Fi y de las torres de telefonía móvil).
- Ayudar a mejorar los servicios de ubicación: las apps y servicios pueden identificar las redes Wi-Fi próximas (aunque el interfaz Wi-Fi del dispositivo móvil esté deshabilitado) y proporcionar dicha información a Google para mejorar la precisión de los servicios de ubicación.

837. Se ha constatado que, aunque se hayan desmarcado todas las opciones correspondientes a los servicios de ubicación descritas previamente, el botón de activación del menú "Ajustes - [Personal] Ubicación" se quedará activo en modo "Solo dispositivo", comprobándose que los informes de ubicación de Google acceden a los servicios de ubicación (aunque en los pasos correspondientes del proceso de instalación se hubieran desmarcado las opciones de ubicación). Por tanto, se recomienda revisar de nuevo minuciosamente los ajustes de ubicación tras completar el proceso de instalación. La siguiente pantalla atestigua esta situación nada más finalizar el proceso de instalación:

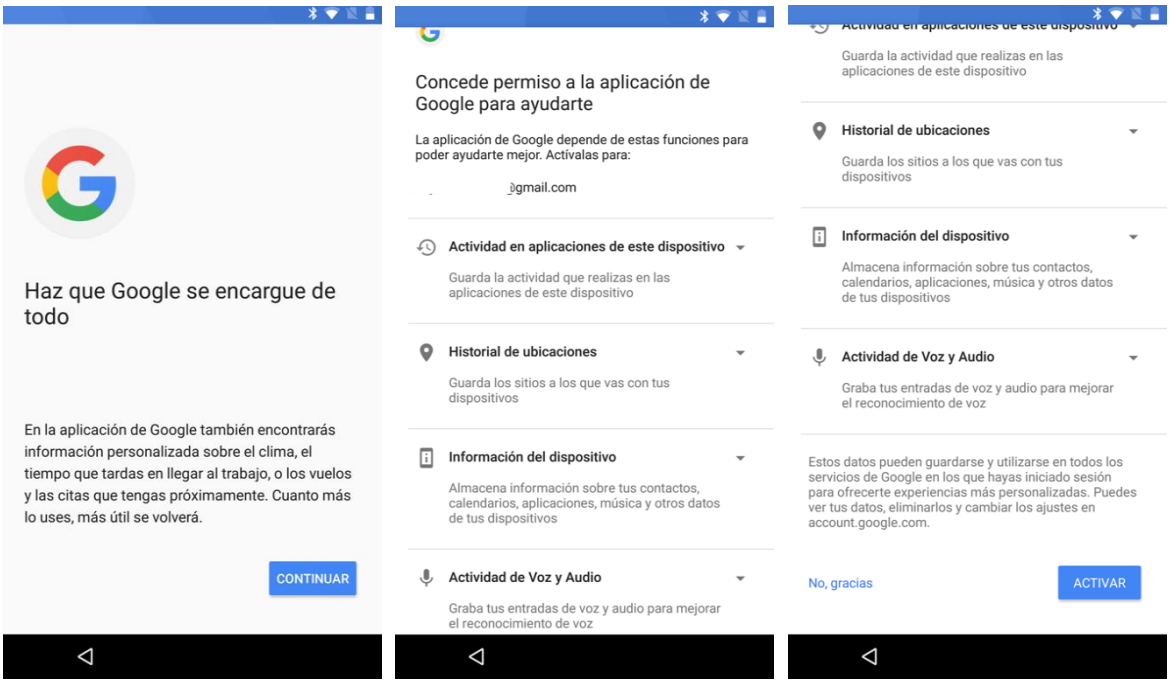


838. También aparece marcada por defecto la opción "Ayuda a mejorar Android", que será empleada para enviar datos de uso y diagnósticos a Google.

839. Desde el punto de vista de seguridad y privacidad, se recomienda desactivar todas las opciones, salvo que se disponga de plena confianza en el tratamiento que Google hará de estos datos del usuario.

840. La opción relativa a la copia de seguridad no aparecía en versiones anteriores de Android, y también se aconseja deshabilitarla hasta evaluar la conveniencia de este sistema de backup en la nube.

841. En versiones anteriores de Android, el proceso de instalación ofrecía activar el servicio "Google Now" (actualmente denominado "Mi Tablón", también referenciado como "*feed*"), que proporciona información en tiempo real al usuario. En la versión 7.1.2, empleada en la elaboración del presente apartado, no se referencia directamente ni al concepto de "Google Now" ni a "Mi Tablón", aunque la funcionalidad que se ofrece en esta pantalla es la correspondiente a esos servicios:



842. Se recomienda no activar ninguna de estas funciones y proseguir mediante el botón "No, gracias".

843. En caso de haberse activado dichas opciones, se iniciarán los servicios de ubicación, el envío de estadísticas a Google y el historial de ubicaciones de Google (ver apartado "11.5. Historial de ubicaciones"), y se accederá a los datos del calendario del usuario, sus búsquedas web, incluyendo el historial web y otros datos del usuario disponibles en los productos y servicios de Google (y/o de terceros):

16.2. UTILIZACIÓN DE UNA CUENTA DE USUARIO DE GOOGLE EXISTENTE

844. Si ya se dispone de cuenta de usuario de Google, las credenciales asociadas se pueden introducir en la pantalla de instalación, y aceptar las condiciones de servicio:

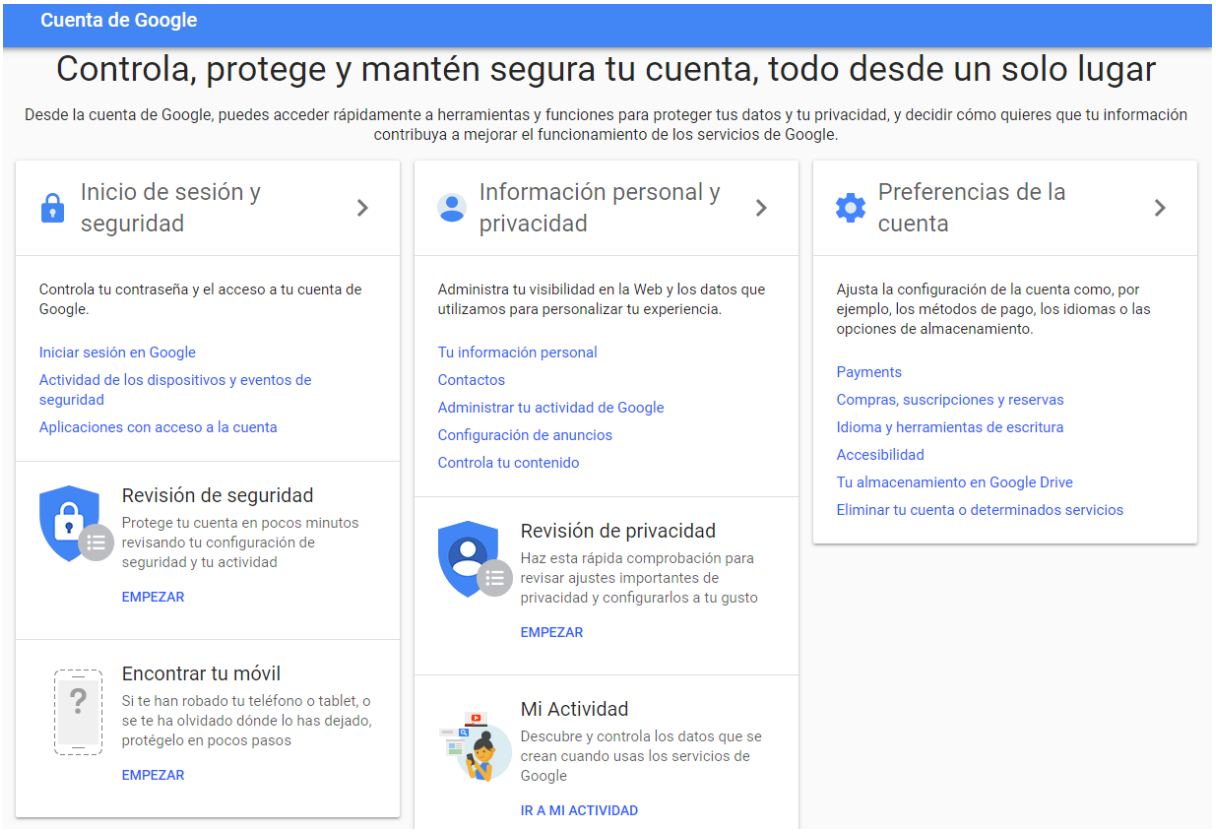
845. Tras pulsar en "Acepto", los pasos de instalación son idénticos a los del apartado anterior, "16.1. Creación de una cuenta de usuario de Google nueva".

846. Tras finalizar el proceso de instalación con una cuenta de usuario de Google ya existente, el dispositivo recibirá de los servidores de Google las apps que estuviesen vinculadas a la cuenta como "instaladas".

17. APÉNDICE A: INTERFAZ WEB DE GESTIÓN DE LA CUENTA DE GOOGLE

847. Además del interfaz propio de la plataforma móvil para la administración de la cuenta de usuario de Google, se dispone de un interfaz web accesible desde cualquier equipo conectado a Internet.

848. En el momento de elaboración de la presente guía, el interfaz web "https://myaccount.google.com", accedido desde un ordenador personal con Windows 10, está estructurado según ilustra la siguiente imagen:

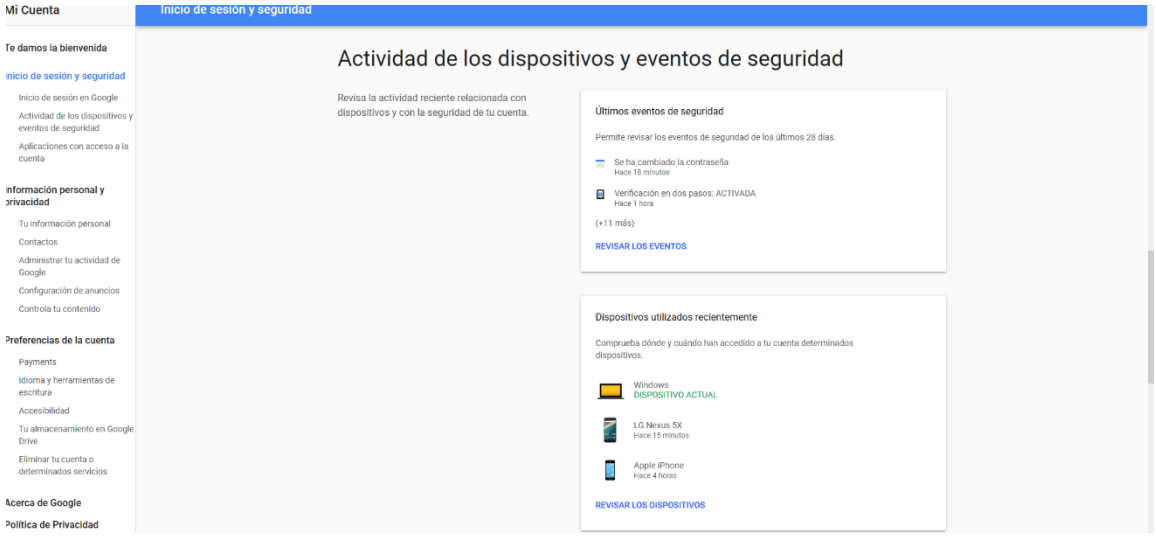


849. Dado que tanto las opciones disponibles, como la apariencia del interfaz web, dependen de múltiples factores, se han de tomar como orientativas las explicaciones relativas a los mismos que se detallan en la presente guía, debiendo consultar la última documentación disponible en la web de Google para realizar la configuración necesaria en el futuro.

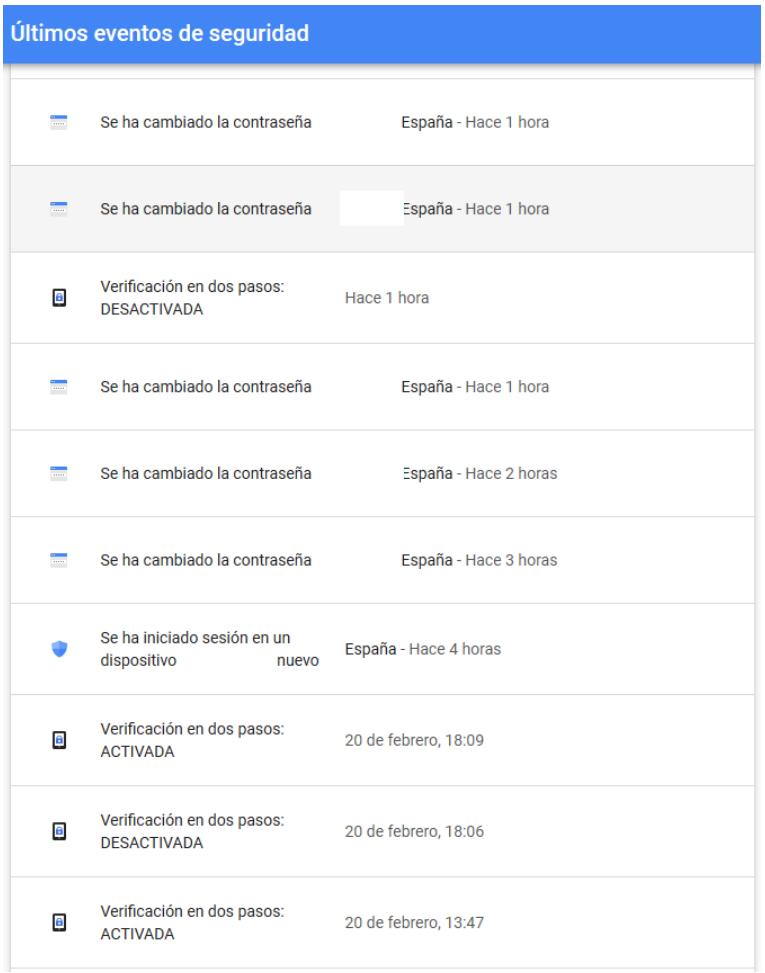
850. La organización de las opciones no es totalmente equivalente con la del interfaz de la plataforma móvil, pero la correspondencia es sencilla de interpretar, por lo que no se repetirán los elementos. Por ejemplo, la sección "Inicio de sesión y seguridad" del interfaz web se corresponde con la sección "Seguridad" de la plataforma móvil.

17.1. INICIO DE SESIÓN Y SEGURIDAD

851. En el 2017 Google añadió al interfaz de administración de la cuenta de usuario de Google el apartado “Inicio de sesión y seguridad - Actividad de los dispositivos y eventos de seguridad”:

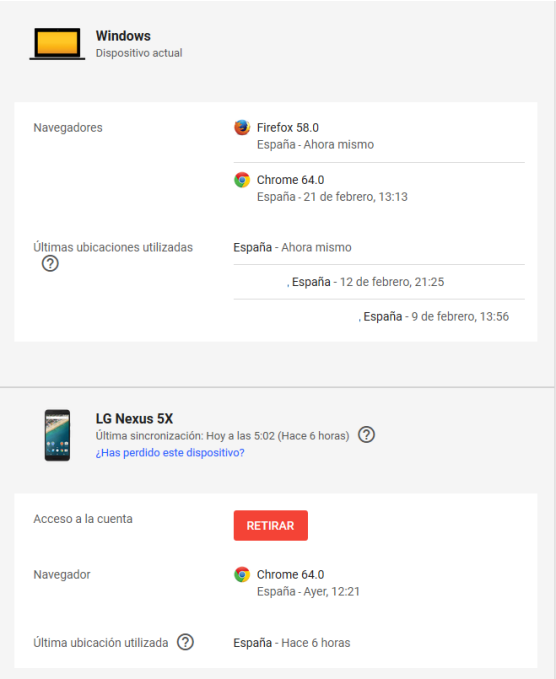


852. Este apartado permite consultar los eventos de seguridad de los últimos 28 días que Google genera relacionados con la cuenta del usuario, como los cambios de contraseña, la activación/desactivación del mecanismo de verificación en dos pasos, el inicio de sesión en un dispositivo móvil nuevo, y otros eventos:

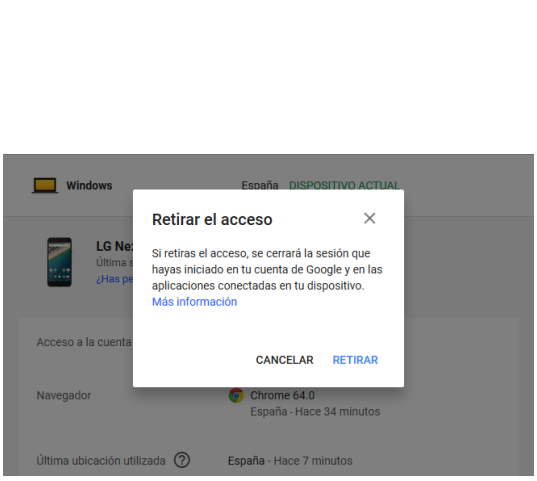


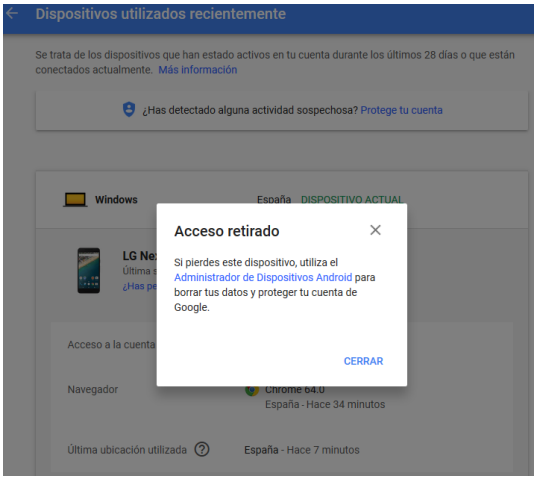
853. Adicionalmente, permite determinar desde qué dispositivos se ha abierto sesión en la cuenta de Google del usuario. La opción “Revisar los dispositivos” muestra la lista de dispositivos (tanto móviles como tradicionales) que han accedido a la cuenta y la fecha del último acceso. Si se selecciona la entrada de cualquiera de ellos, se indicará el mecanismo empleado para el acceso (por ejemplo, el tipo y versión del navegador

web si se accedió mediante éste), y permite retirar el acceso a la cuenta de aquellos dispositivos que hayan iniciado sesión en la cuenta de Google del usuario:



854. Si se sospecha sobre el origen de alguna actividad en un dispositivo concreto, se puede "Retirar" el acceso a la cuenta desde el mismo mediante el botón correspondiente.



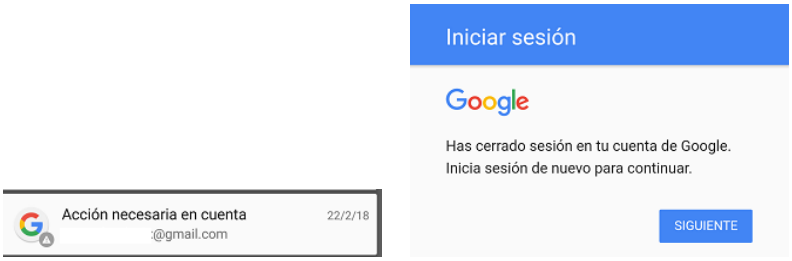


855. En el dispositivo móvil se perderá el acceso a la cuenta de usuario de Google y ninguna aplicación se sincronizará con su servicio asociado.

856. Una vez se haya retirado el acceso a la cuenta de usuario de Google para el dispositivo móvil sospechoso, y que potencialmente está utilizándola de manera no autorizada, se evaluarán las acciones correspondientes a llevar a cabo (por ejemplo, si se el dispositivo móvil se ha extraviado, consultar las recomendaciones indicadas en el apartado "10.4. Gestión remota de dispositivos Android por parte del usuario").

857. Además de a través del interfaz web "Inicio de sesión y seguridad", Google envía a la cuenta de correo de Gmail del usuario mensajes relativos a los eventos de seguridad relevantes. En dichos mensajes, se proporcionan enlaces al interfaz web de gestión de la cuenta (concretamente, al apartado relacionado con el tipo de evento particular).

858. También se pueden recibir notificaciones como la que se muestra a continuación, que informan de que hay alguna incidencia con la cuenta de usuario de Google y, que, al abrirlas, redirigirán a la acción que se considera necesaria por parte de Google:



859. Dada la extrema importancia que tiene la cuenta de usuario de Google, no sólo por lo sensible de la información relativa al usuario que alberga, sino por las acciones que desde ella se pueden realizar, se recomienda encarecidamente prestar atención a los mensajes relativos a eventos de seguridad, y consultar asiduamente el capítulo "Actividad de los dispositivos y eventos de seguridad" para identificar cualquier actividad no reconocida como propia sobre la cuenta de usuario de Google y los dispositivos asociados de un modo u otro a estas actividades sospechosas.

860. Ante cualquier mínima sospecha, se deberán evaluar las acciones pertinentes, empezando por cambiar la contraseña actual de la cuenta de usuario de Google.

17.2. INFORMACIÓN PERSONAL Y PRIVACIDAD

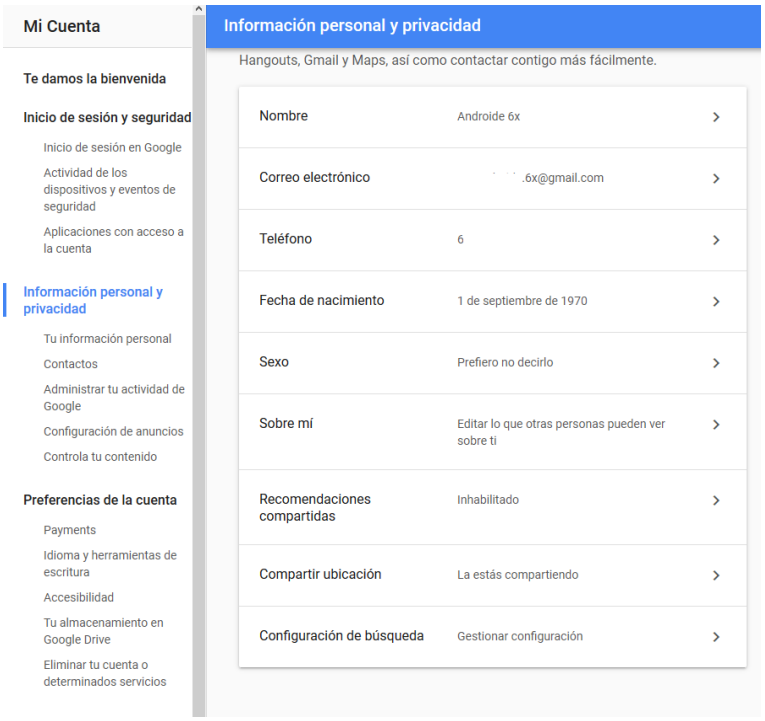
861. Bajo esta sección de configuración se pueden consultar y modificar elementos como los datos personales (el nombre, correo electrónico y número de teléfono) que se utilizan por los productos y servicios de Google, como Hangouts, Gmail y Maps para que otros usuarios puedan consultarlos, así como administrar la actividad de la cuenta de usuario de Google y controlar su contenido.

862. Desde el dispositivo móvil, el acceso a esta configuración está en "Ajustes - [Personal] Google - Información personal y privacidad", que lanza el correspondiente menú del interfaz "Mi cuenta".

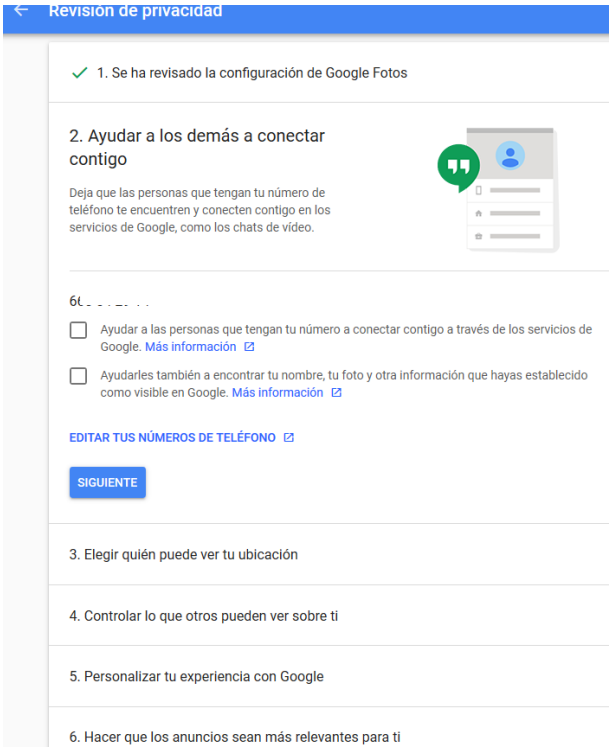
863. Debido a la extrema sensibilidad de estos datos, se recomienda minimizar en lo posible la información personal a la que dan acceso.

17.2.1. TU INFORMACIÓN PERSONAL

864. Los parámetros definidos para la cuenta de usuario se pueden modificar seleccionándolos y a través del icono del lápiz de la página web que se abrirá. A fecha de elaboración de la presente guía, éstas son las opciones que se muestran, tanto desde el interfaz web como desde la pantalla de Android (dado que este servicio se modifica frecuentemente por parte de Google, algunas de las opciones pueden no corresponderse con las aquí descritas):



865. La opción "Sobre mí" proporciona acceso al portal "https://aboutme.google.com", desde el que se gestiona la información propia visible para otros usuarios de productos de Google. Concretamente, la opción "Ir a la revisión de privacidad" despliega un menú con múltiples detalles personales, todos ellos editables:



- La opción "Elegir quién puede ver tu ubicación" muestra si se está compartiendo actualmente la ubicación con otros usuarios (ver apartado "11. Localización (o ubicación) geográfica").
- La opción "Controlar lo que otros pueden ver sobre ti" permite editar los datos personales que serán accesibles por otros usuarios de servicios de Google y que, potencialmente, se pueden emplear en el contexto de

recomendaciones compartidas (es decir, lo que se publica cuando se emite un voto desde una aplicación de Google, incluyendo las que se publican como parte de los anuncios).

- La opción "Controles de la actividad de tu cuenta" se describe en el apartado "6.2.1.2. Datos y personalización".
- La opción "Hacer que los anuncios sean más relevantes para ti" se describe en el apartado "17.2.3. Anuncios".

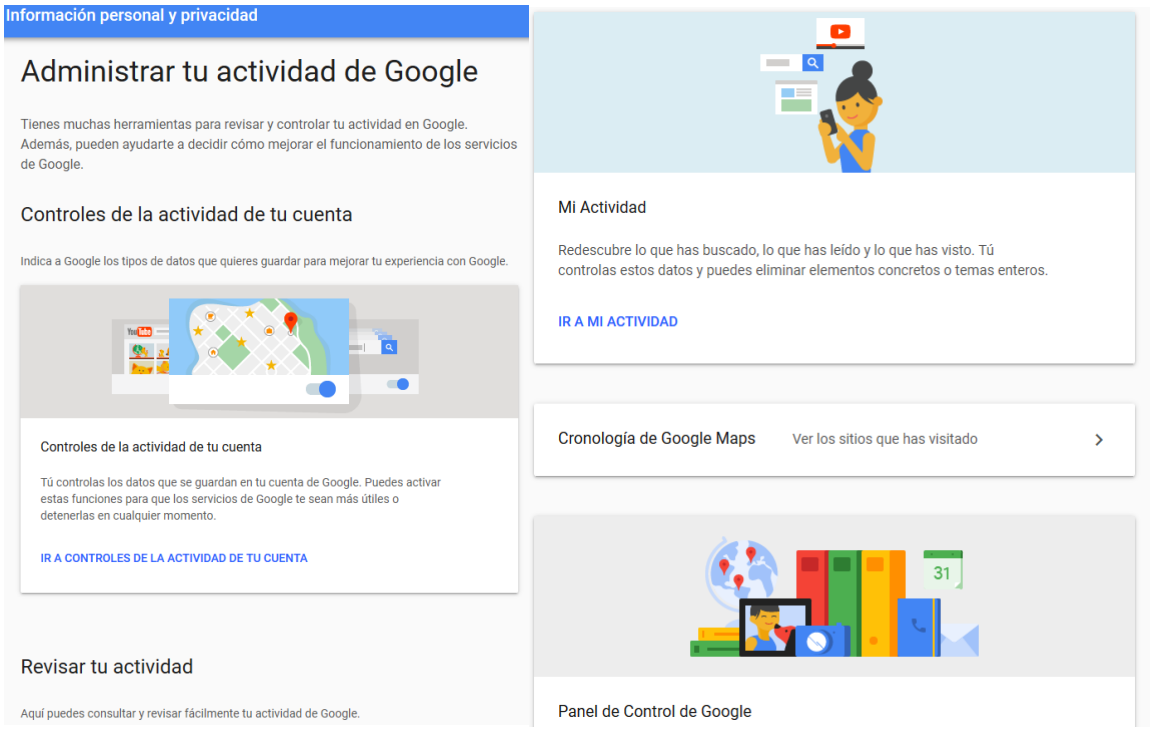
866. Además, el interfaz "Información personal y privacidad" incluye el apartado "Contactos", en el que se dispone de la opción "Usuarios bloqueados": este apartado permite consultar si actualmente hay algún usuario cuya cuenta se desea bloquear para que no pueda interaccionar con la cuenta propia utilizando los productos de Google, concretamente Google+, Hangouts, Fotos, YouTube y Maps [Ref.- 181]. El bloqueo de un usuario en uno de estos productos implica que su cuenta será bloqueada en todos ellos.

867. No se incluyen en la lista anterior los usuarios que se han bloqueado a nivel de su cuenta de usuario de Google. Por ejemplo, es posible bloquear una dirección de correo en Gmail y un número de teléfono en el dispositivo móvil, pero estas acciones de bloqueo no se muestran en el apartado "Usuarios bloqueados". Para más información sobre cómo bloquear números de teléfono, consultar el apartado "6.2.1.4. Usuarios e información compartida".

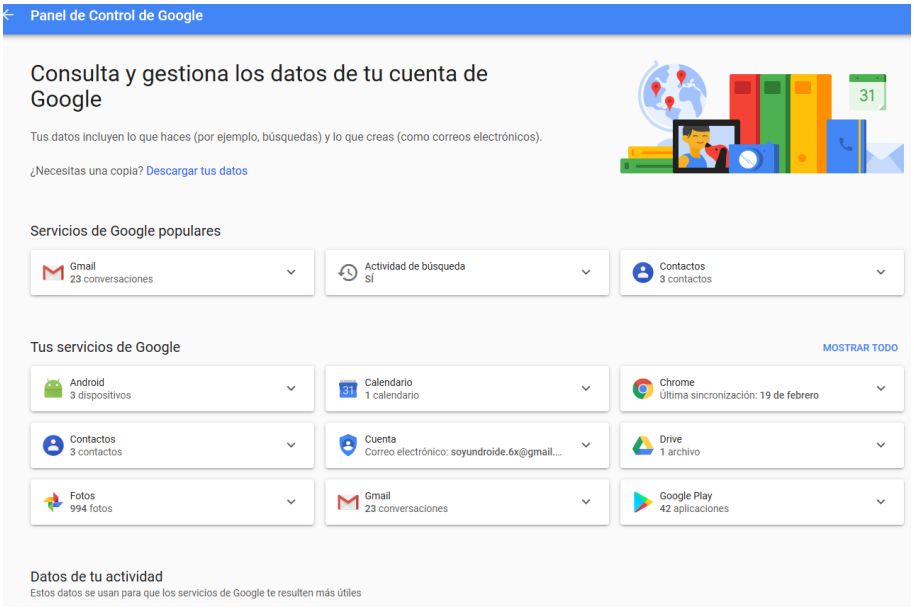
868. La opción "Administrar tu actividad de Google" se detalla en el apartado "17.2.2. Administrar tu actividad de Google".

17.2.2. ADMINISTRAR TU ACTIVIDAD DE GOOGLE

869. En esta sección se ofrecen las opciones relativas a cómo se almacena la actividad de la cuenta de Google del usuario:



- La opción "Controles de la actividad de tu cuenta" coincide con la descrita en el apartado"6.2.3. Cuentas y privacidad".
- La opción "Revisar tu actividad" engloba las opciones "Mi actividad" (corresponde a la descrita en el apartado "14.1.3. Historial de actividad web y de aplicaciones") y "Cronología de Google Maps" (descrita en el apartado "11.5. Historial de ubicaciones").
- La opción "Panel de control de Google" ofrece a los usuarios individuales no asociados a un dominio de Google G-Suite (ver apartado "17.2.2. Administrar tu actividad de Google") acceder a la administración de servicios de la cuenta de usuario, como el tipo de acceso, a través del Panel de Control de Google (o *dashboard*), disponible en "https://myaccount.google.com/dashboard".

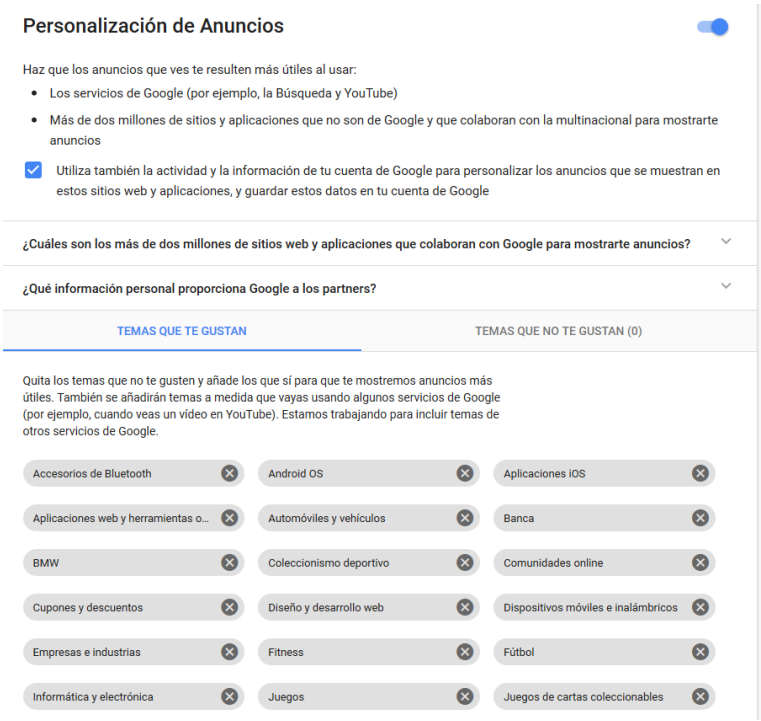


870. Dentro de las opciones disponibles en el *dashboard* o panel de control de Google, se encuentra la gestión de la cuenta de usuario de Google, de los dispositivos móviles vinculados, de todos los servicios de Google (Audio, Calendario, sincronización de Chrome, Cloud Print, Contactos, Gmail, Google Fotos, Google+, histórico de ubicaciones, Play Store o Google Play, perfil, histórico de búsquedas, Talk, y YouTube), siendo posible acceder a todos los detalles de cada servicio, como por ejemplo, gestionar las apps instaladas desde Google Play (a través de un enlace directo a la cuenta de usuario de Google en Google Play: "https://play.google.com/store/account?hl=es/"), así como verificar los datos almacenados por Google para los dispositivos móviles vinculados a la cuenta. Estos datos incluyen, entre otros, para cada dispositivo móvil: el modelo, fabricante, operador de telefonía, fecha de registro, fecha de la última actividad, etc., así como una lista de las apps que almacenan una copia de seguridad de sus datos en los servidores de Google:

17.2.3. ANUNCIOS

871. La configuración de anuncios en Android 6.x no se puede gestionar desde el propio dispositivo móvil (al contrario de lo que sucedía en Android 5.x con la app "Ajustes de Google - [Servicios] Anuncios").

872. La única alternativa para gestionar, según las posibilidades que se ofrecen, los anuncios es recurrir a la interfaz web que es accesible desde el siguiente enlace, "https://myaccount.google.com/privacy?hl=es#ads", "Administrar la configuración de anuncios", que redirige a "https://adssettings.google.com/authenticated".



873. Hay que recalcar que no es posible inhabilitar la presentación de anuncios, tal y como refleja la política de Google[21], y que todos los parámetros que se definan afectarán únicamente al tipo de anuncio que se recibirá.

874. En el caso de la configuración de anuncios, el usuario puede filtrar por temas, utilizar la actividad y la información de la cuenta de usuario de Google para personalizar los anuncios que se muestran en estos sitios web y aplicaciones, y guardar estos datos en la cuenta de usuario de Google. Esta opción (habilitada por defecto) no está recomendada desde el punto de vista de la privacidad, pues, aunque deshabilitarla

[21] https://support.google.com/ads/answer/2662922?hl=es

hará que los anuncios mostrados sean más genéricos, y muy probablemente no del interés del usuario, evita que se haga un seguimiento del usuario en este tipo de servicios.

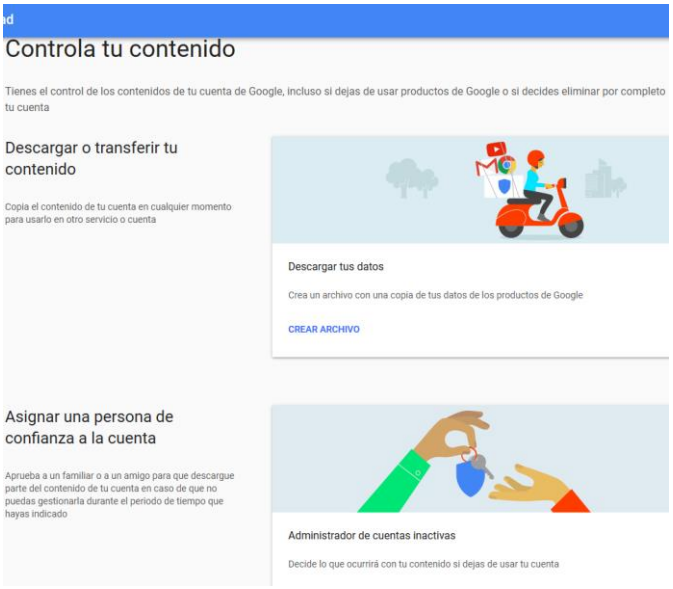
875. La versión 4.x de los servicios de Google Play introdujo lo que se denomina "ID de publicidad", un número aleatorio y único (supuestamente anónimo) que se generaba en el momento de la instalación inicial del dispositivo móvil, o cada vez que éste es restablecido a fábrica, y que se emplea por los servicios de anuncios, asociados a Google Play y a las apps de terceros, para hacer un seguimiento del usuario [Ref.-187].

876. La configuración del identificador (o ID) de publicidad se encuentra en "Ajustes - [Personal] Google - [Servicios] Anuncios".

877. Por último, la opción "Anuncios Google" redirige al usuario a la página web de Google que informa de los servicios de anuncios y publicidad.

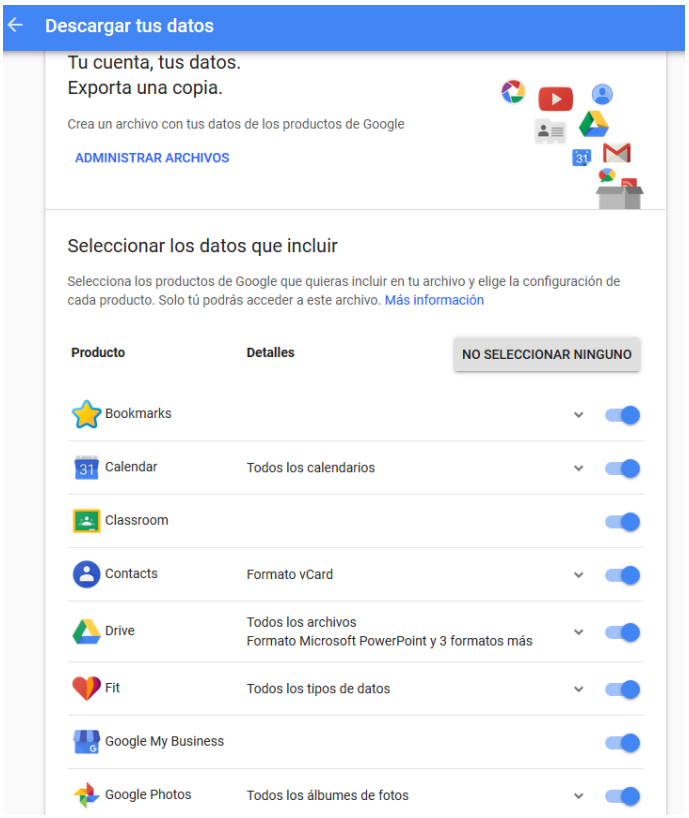
17.2.4. CONTROLA TU CONTENIDO

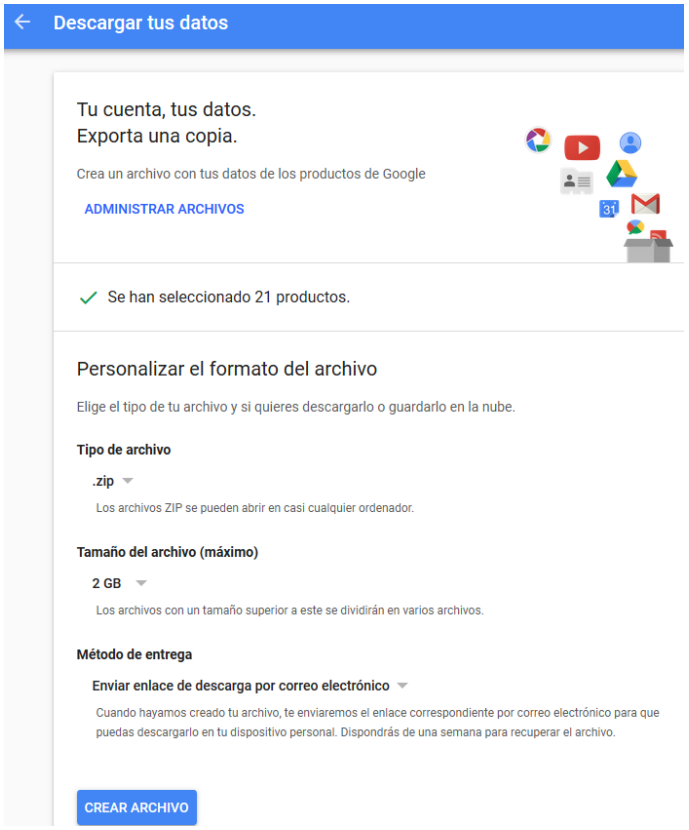
878. El interfaz "Controla tu contenido" alberga dos opciones a fecha de elaboración de la presente guía:



879. Descargar o transferir tu contenido: Esta opción permite crear y descargar un archivo con los datos y la configuración de los servicios y aplicaciones de Google que el usuario seleccione.

- Al seleccionar "Crear archivo", se ofrece un menú que permite elegir qué datos se salvarán y transmitirán al archivo de copia.

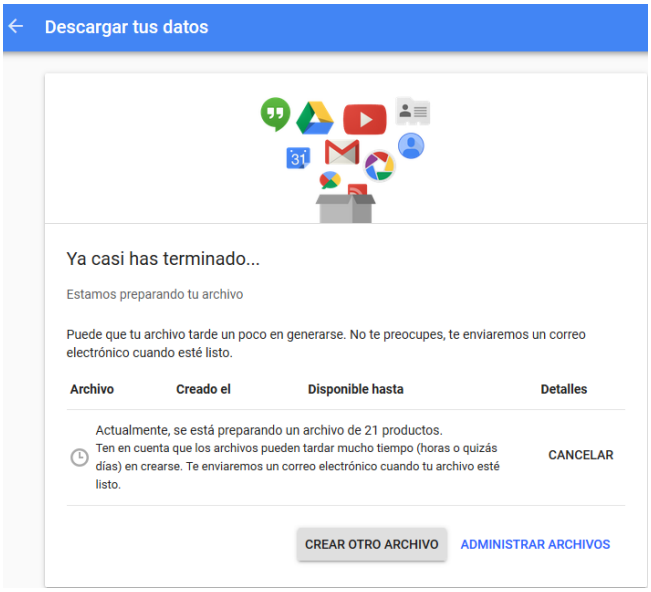




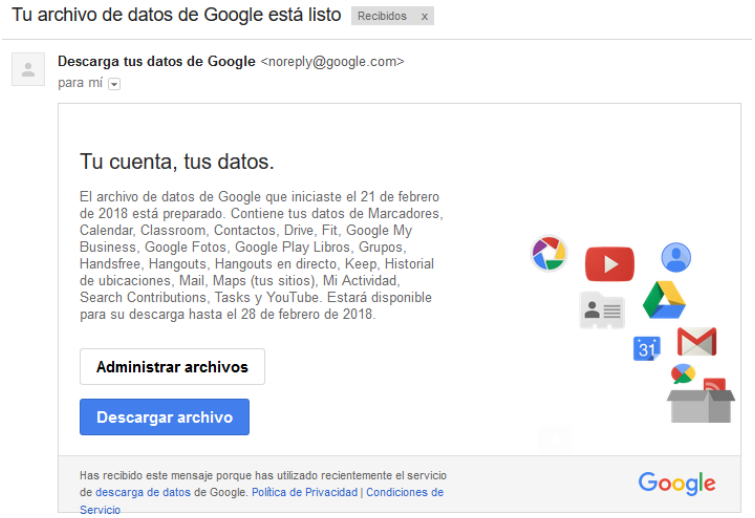
- El formato del archivo puede ser .zip, .tgz o .tbz, y el tamaño máximo de 50 GB.
- Como métodos para obtener el archivo, se puede seleccionar el correo electrónico, Google Drive, Dropbox o Microsoft OneDrive (en cuyo caso el archivo se guardará en el servicio de la nube especificado y el enlace a su

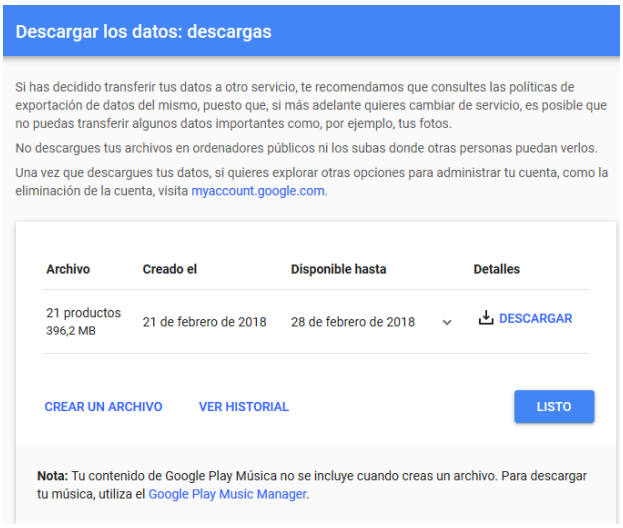
ubicación se enviará por correo electrónico a la cuenta de usuario de Google). El detalle de estos servicios queda fuera del alcance de la presente guía.

- Cuando se selecciona "Crear archivo", se mostrará un mensaje de confirmación:

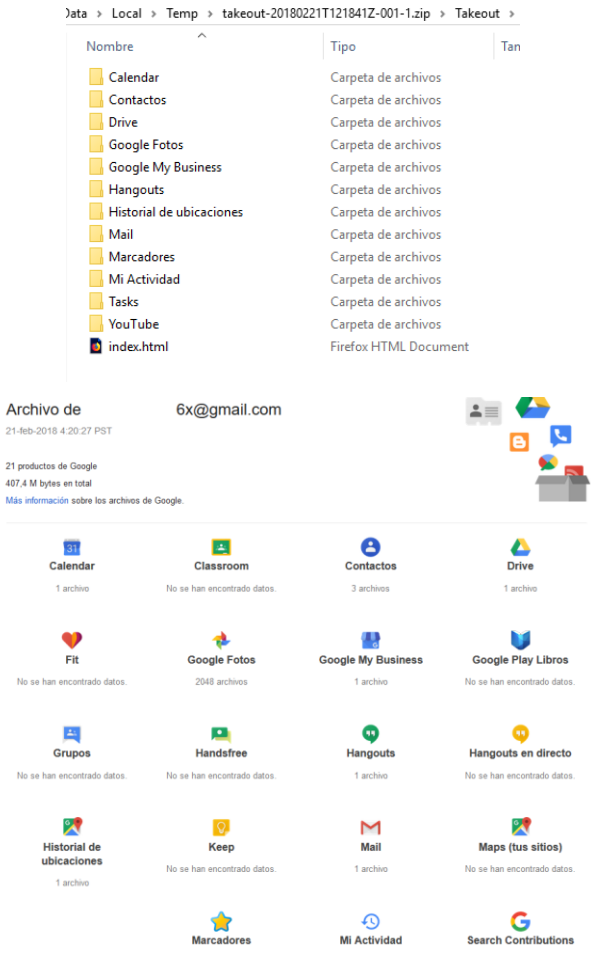


- Cuando el archivo se encuentre disponible, se recibirá un e-mail en la cuenta de usuario y se podrá descargar el archivo:





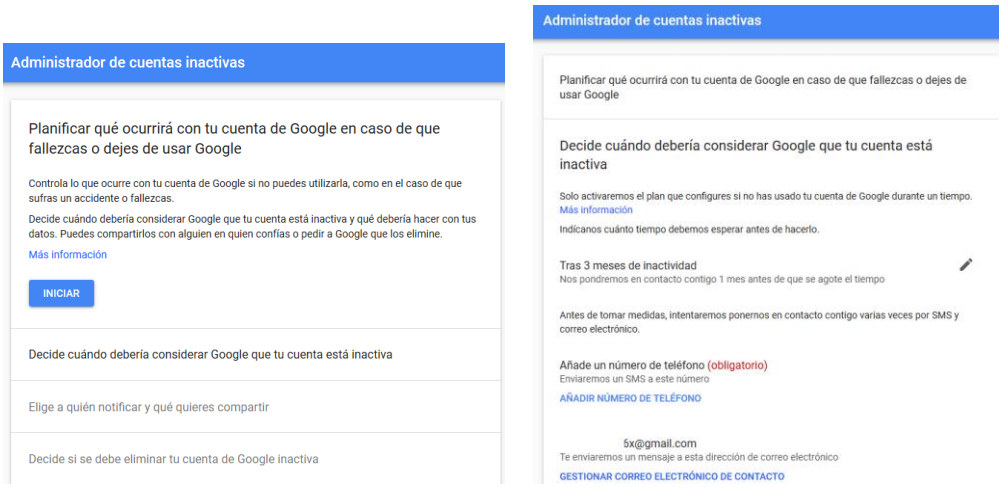
- El archivo tiene la nomenclatura "takeout-fecha-ID.extensión_designada". Por ejemplo, "takeout-20180221T115317Z-001.zip. El contenido del archivo sigue una estructura de subdirectorios, uno por cada aplicación seleccionada, y un fichero index que muestra lo que se ha salvado y, al seleccionar el icono de cada aplicación, el formato empleado (MBOX para el mail, JSON para las búsquedas y Hangouts, ICS para el calendario, HTML para los marcadores, etc.):



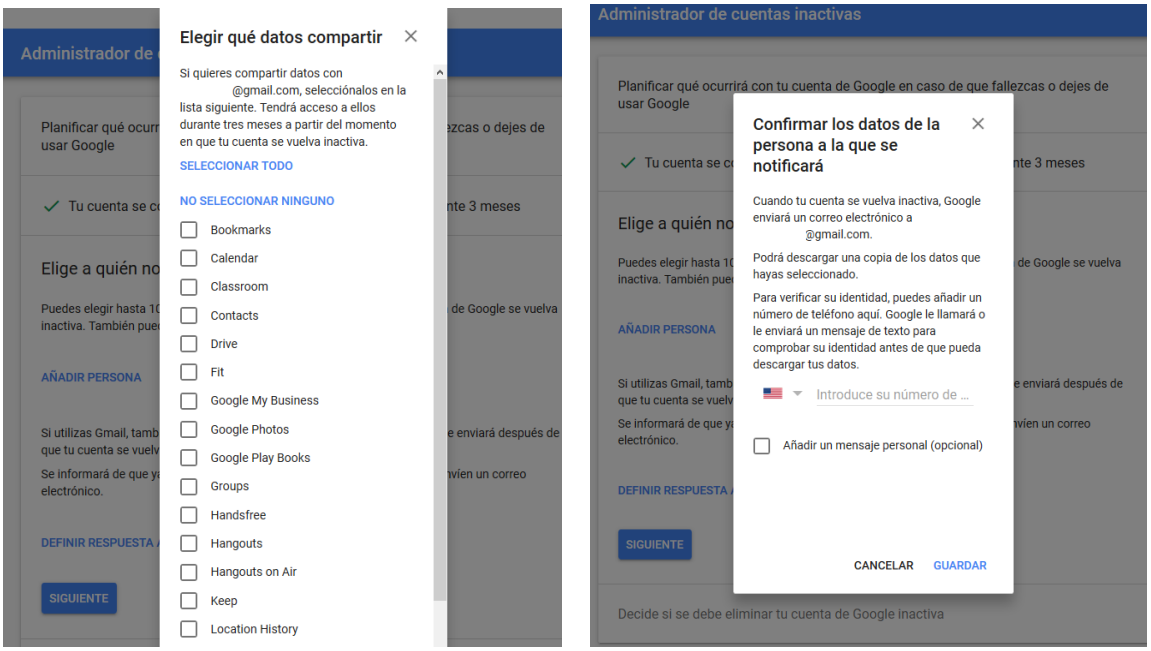
- La creación de un archivo de descarga no elimina ninguna parte de la información almacenada en la cuenta de Google del usuario.

- Este método se puede utilizar si se desea exportar los datos a otro tipo de servicios, y también como una alternativa para realizar una copia de seguridad de los datos.

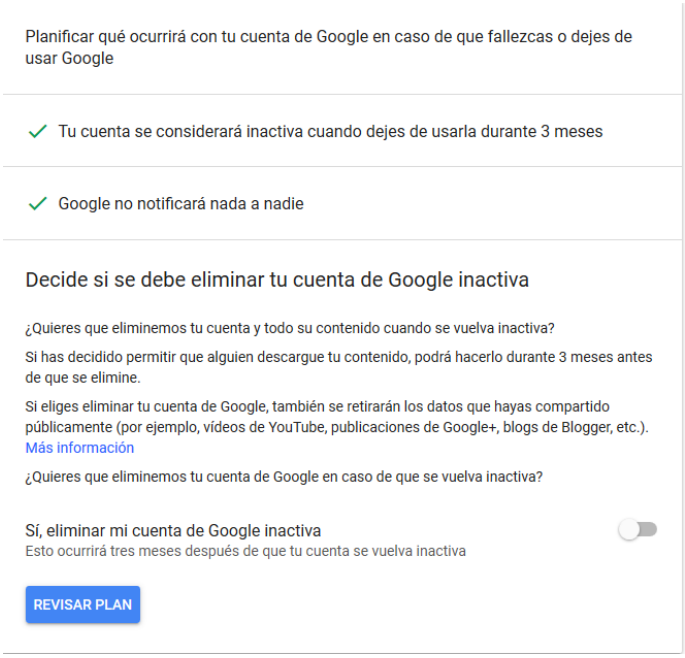
880. Administrador de cuentas inactivas: permite configurar diversas opciones de actuación sobre cuentas de usuario que permanecen inactivas, independientemente del motivo. Al acceder a la opción "Administrador de cuentas inactivas - Cambiar esta configuración", se abre un interfaz que permite definir un plan para el supuesto en que se deje de utilizar la cuenta de Google del usuario:



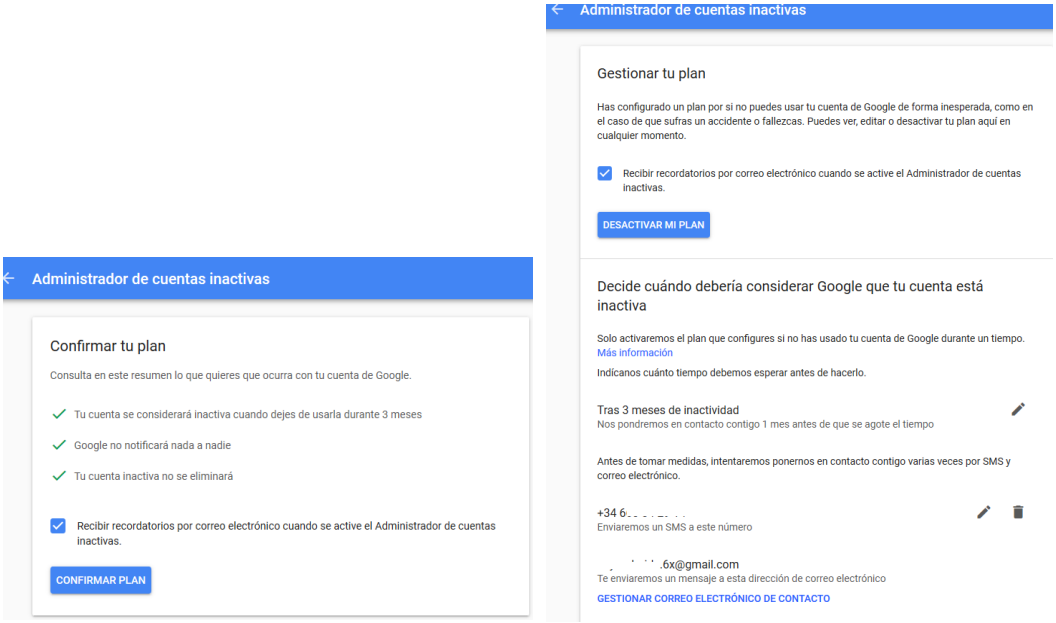
- Por defecto, se establece un periodo mínimo de espera de tres meses tras el cual la cuenta se considerará inactiva (el máximo configurable es 18 meses) y a quién se enviarán las alertas antes de que se cumpla el tiempo para que la cuenta se marque como inactiva; además, se puede configurar un máximo de 10 personas a quienes se notificará sobre la designación de la cuenta como inactiva, e incluso darles acceso a los datos que el propietario de la cuenta considere oportunos.



- Además, se puede configurar la opción de eliminar por completo la cuenta en caso de que se declare inactiva según los parámetros definidos anteriormente:



- Una vez finalizada la configuración, se ofrece revisar el plan y, en caso de ser adecuado, confirmarlo:



- Si se añade un contacto de confianza, se ofrecerá la posibilidad de marcar qué datos pueden ser accedidos por dicho contacto. Además de su dirección de correo electrónico, se puede proporcionar un número de teléfono del contacto para comprobar su identidad e impedir accesos no autorizados a los datos. Los contactos de confianza recibirán dicho código de verificación después de que la cuenta se marque como inactiva.

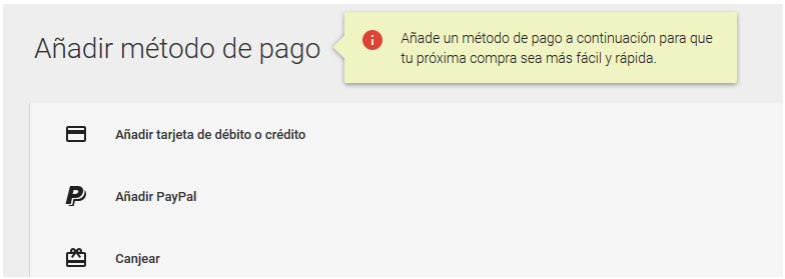
881. Desde el punto de vista de seguridad y privacidad, no se recomienda hacer uso de la funcionalidad "Administrador de cuentas inactivas", pues pueden ser múltiples las circunstancias que provoquen que una cuenta deje de ser utilizada y no en todas ellas el propietario podrá revocar una autorización de acceso a sus datos habilitada previamente.

17.3. PREFERENCIAS DE LA CUENTA

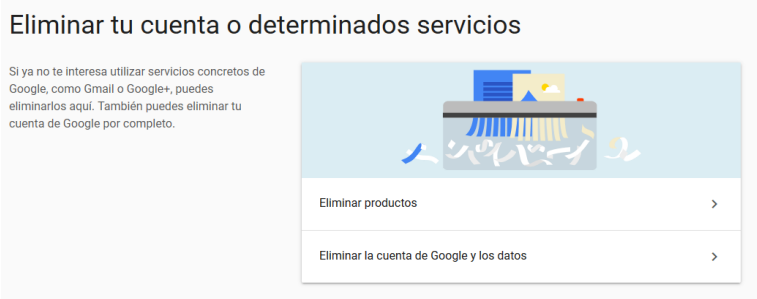
882. A fecha de elaboración de la presente guía, el acceso a esta configuración desde el dispositivo móvil se encuentra en "Ajustes - [Personal] Google - Preferencias de la cuenta", que lanza el correspondiente menú del interfaz "Mi cuenta".

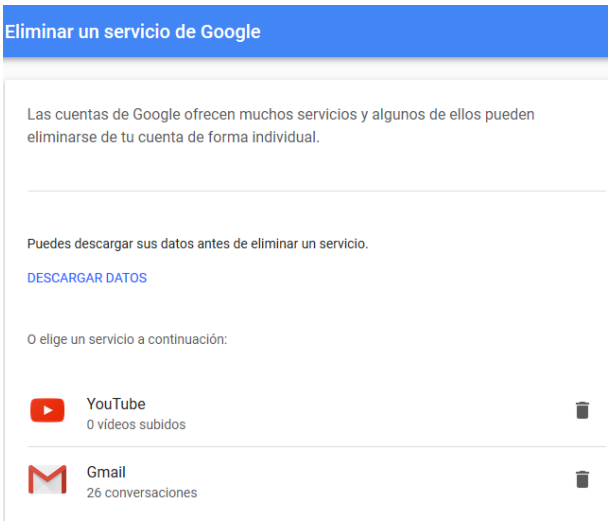
883. Bajo esta sección se encuentran las siguientes opciones:

- Payments: el denominado "Centro de pagos de Google" [Ref.- 263] es un servicio que pretende albergar perfiles de pago del usuario para utilizarlos en las compras de productos y servicios de Google (como la Google Play). La configuración detallada de este servicio queda fuera del ámbito de la presente guía.

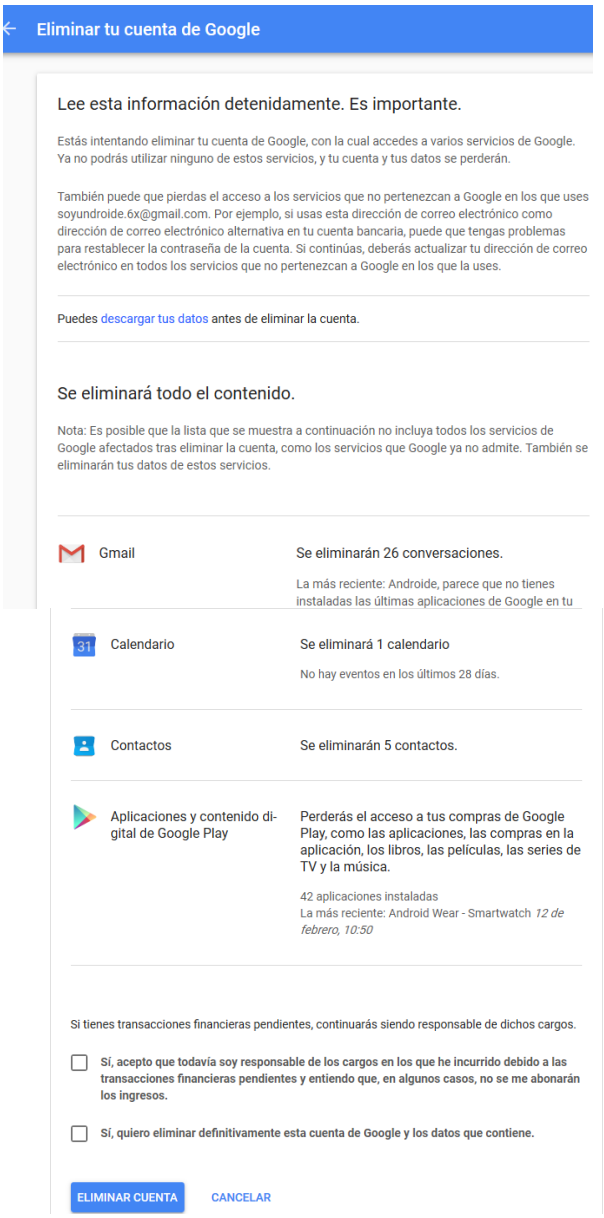


- Idioma y herramientas de escritura: permite definir el idioma predeterminado en el que se mostrará el contenido de la web y añadir otros idiomas, así como seleccionar las herramientas de introducción de texto, como el formato del teclado.
- Accesibilidad: en caso de que sea necesario configurar algún elemento relacionado con este aspecto.
- Tu almacenamiento en Google Drive: proporciona la información sobre el espacio ocupado en Google Drive en el momento actual, por aplicaciones, así como contratar espacio adicional.
- Eliminar tu cuenta o determinados servicios: permite eliminar servicios que ya no se desea utilizar como parte de la cuenta de usuario, pudiéndose descargar previamente los datos asociados a ellos, e incluso la cuenta de usuario de Google en su totalidad.





- Por último, la opción "Eliminar la cuenta y los datos de Google" permite eliminar por completo la cuenta, no sólo del dispositivo actual, sino la totalidad de la cuenta. Dado el impacto de esta acción, se solicitará introducir las credenciales del usuario de nuevo, así como confirmación y aceptación de las condiciones del servicio. Además, se instará al usuario a descargar los datos antes de proceder a la eliminación de la cuenta.


Eliminar tu cuenta de Google
Lee esta información detenidamente. Es importante.
Estás intentando eliminar tu cuenta de Google, con la cual accedes a varios servicios de Google. Ya no podrás utilizar ninguno de estos servicios, y tu cuenta y tus datos se perderán.
También puede que pierdas el acceso a los servicios que no pertenezcan a Google en los que uses soyundroide.6x@gmail.com. Por ejemplo, si usas esta dirección de correo electrónico como dirección de correo electrónico alternativa en tu cuenta bancaria, puede que tengas problemas para restablecer la contraseña de la cuenta. Si continúas, deberás actualizar tu dirección de correo electrónico en todos los servicios que no pertenezcan a Google en los que la uses.
Puedes descargar tus datos antes de eliminar la cuenta.
Se eliminará todo el contenido.
Nota: Es posible que la lista que se muestra a continuación no incluya todos los servicios de Google afectados tras eliminar la cuenta, como los servicios que Google ya no admite. También se eliminarán tus datos de estos servicios.
Gmail
Se eliminarán 26 conversaciones.
La más reciente: Androide, parece que no tienes instaladas las últimas aplicaciones de Google en tu
Calendario
Se eliminará 1 calendario
No hay eventos en los últimos 28 días.
Contactos
Se eliminarán 5 contactos.
Aplicaciones y contenido digital de Google Play
Perderás el acceso a tus compras de Google Play, como las aplicaciones, las compras en la aplicación, los libros, las películas, las series de TV y la música.
42 aplicaciones instaladas
La más reciente: Android Wear - Smartwatch 12 de febrero, 10:50
Si tienes transacciones financieras pendientes, continuarás siendo responsable de dichos cargos.
Sí, acepto que todavía soy responsable de los cargos en los que he incurrido debido a las transacciones financieras pendientes y entiendo que, en algunos casos, no se me abonarán los ingresos.
Sí, quiero eliminar definitivamente esta cuenta de Google y los datos que contiene.
ELIMINAR CUENTA
CANCELAR

18. REFERENCIAS

La siguiente tabla muestra las fuentes de información a las que se hace referencia a lo largo de la presente guía[22]:

Nota: Por completitud se ha empleado la siguiente tabla de referencias completa de la guía "CCN-STIC-453D - Seguridad de dispositivos móviles: Android 6.x" [Ref.- 406], aunque muchas de las referencias no son utilizadas a lo largo de la presente guía (marcadas en color gris). La tabla de referencias, a su vez, ha sido ampliada con referencias específicas para la presente guía.

Referencia	Título, autor y ubicación
[Ref.- 1]	Android. Google. URL: http://www.android.com
[Ref.- 2]	Google Nexus 5. Google. URL: http://www.google.com/nexus/5/
[Ref.- 3]	Google Nexus 5X. Google. URL: https://www.google.com/nexus/5x/
[Ref.- 4]	Google Play. URL: https://play.google.com
[Ref.- 5]	"Exercising Our Remote Application Removal Feature". Rich Cannings. Android. June 2010. URL: http://android-developers.blogspot.com/2010/06/exercising-our-remote-application.html
[Ref.- 6]	"Actualizar las aplicaciones Android". Google. URL: https://support.google.com/googleplay/answer/113412?hl=es
[Ref.- 7]	Android Developers. Google. URL: http://developer.android.com
[Ref.- 8]	"The dark side of the new Google Play". Denis. Kaspersky Lab Expert. February 2011. URL:http://www.securelist.com/en/blog/11153/The_dark_side_of_the_new_Android_Play
[Ref.- 9]	"Android 2.3 Platform and Updated SDK Tools". December 2010. Google. URL: http://android-developers.blogspot.com/2010/12/android-23-platform-and-updated-sdk.html
[Ref.- 10]	"Android 2.3.3 Platform, New NFC Capabilities". February 2011. Google. URL: http://android-developers.blogspot.com/2011/02/android-233-platform-new-nfc.html
[Ref.- 11]	"Android Architecture Components". Google. URL: https://developer.android.com/develop/index.html
[Ref.- 12]	"SafetyNet Helper Sample". Google Play. URL: https://play.google.com/store/apps/details?id=com.scottyab.safetynet.sample
[Ref.- 13]	"Google Apps Device Policy". Google. URL: https://play.google.com/store/apps/details?id=com.google.android.apps.enterprise.dmagent URL: https://www.google.com/support/mobile/bin/answer.py?hl=en&answer=190930
[Ref.- 14]	"Google Authenticator". Google. Google Play. URL: https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2 URL: https://www.google.com/support/accounts/bin/answer.py?answer=1066447
[Ref.- 15]	"About 2-step verification". Google. URL: https://support.google.com/accounts/answer/180744
[Ref.- 16]	"Application Fundamentals". Android Developers. Google. URL: http://developer.android.com/guide/components/fundamentals.html
[Ref.- 17]	Android Developers - Direct Share. Google. URL: https://developer.android.com/samples/DirectShare/index.html
[Ref.- 18]	"Mobile Application Security". Himanshu Dwivedi, Chris Clark, David Thiel. McGraw-Hill. ISBN: 0071633561. 2010. URL: http://www.mhprofessional.com/product.php?isbn=0071633561

[22] El texto "[old]" indica que se tiene constancia de que el enlace pudiera no estar operativo, o estar desactualizado, en la actualidad, pero se mantiene debido a su relevancia y por motivos históricos. En algunos casos se acompaña de una referencia actualizada, indicada por el texto "[actualizada]".

Referencia	Título, autor y ubicación
[Ref.- 19]	"API Levels". Android Developers. Google. URL: http://developer.android.com/guide/appendix/api-levels.html
[Ref.- 20]	"Verificación en dos pasos (two-step verification)". Google. URL: https://www.google.com/landing/2step/ URL: https://www.google.com/landing/2step/features.html
[Ref.- 21]	"Android VPN Connectivity". pfSense. URL: https://doc.pfsense.org/index.php/Android_VPN_Connectivity
[Ref.- 22]	Android Studio & SDK (Software Development Kit). Google. URL: http://developer.android.com/sdk/index.html
[Ref.- 23]	Manifest Permission (Since API Level 1). Google. URL: http://developer.android.com/reference/android/Manifest.permission.html
[Ref.- 24]	"Android Security Reports". Google Report. Android security Center. URL: https://source.android.com/security/overview/reports
[Ref.- 25]	"SafetyNet: Google's tamper detection for Android". John Kozyrakis. URL: https://koz.io/inside-safetynet/
[Ref.- 26]	"Code signing in Android's security model". Nikolay Elenkov. May 2013. URL: http://nelenkov.blogspot.com.es/2013/05/code-signing-in-androids-security-model.html
[Ref.- 27]	"BouncyCastle Key Store (BKS) library". The Legion of the Bouncy Castle. URL: http://bouncycastle.org/download/bcprov-jdk16-141.jar
[Ref.- 28]	"Signing Your Applications". Android Developers. URL: http://developer.android.com/guide/publishing/app-signing.html
[Ref.- 29]	RedPhone. Open WhisperSystems. 2015. URL: https://whispersystems.org URL: https://play.google.com/store/apps/details?id=org.thoughtcrime.redphone
[Ref.- 30]	"Getting Your SMS Apps Ready for KitKat". Android Developers Blog. October 2013. URL: http://android-developers.blogspot.com.es/2013/10/getting-your-sms-apps-ready-for-kitkat.html
[Ref.- 31]	"Android 3.0 Platform Highlights". Google. 2011. URL: http://developer.android.com/sdk/android-3.0-highlights.html#enterprise
[Ref.- 32]	Signal (Private Messenger). Open Whisper Systems. URL: https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms URL: https://github.com/WhisperSystems/Signal-Android
[Ref.- 33]	TextSecure. Open Whisper Systems. 2015. URL: https://whispersystems.org URL: https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms
[Ref.- 34]	"Prevent phishing attacks on your users". G Suite Administrator Help. Google. URL: https://support.google.com/a/answer/6197480
[Ref.- 35]	"Using KitKat verified boot". Nikolai Elenkov. May 2014. URL: https://nelenkov.blogspot.com/2014/05/using-kitkat-verified-boot.html
[Ref.- 36]	"SafetyNet Playground". Google Play. URL: https://play.google.com/store/apps/details?id=com.cigital.safetynetplayground
[Ref.- 37]	"Understanding Exchange ActiveSync Mailbox Policies·. MS Exchange 2010 SP2 & SP3. Microsoft Technet. 2014. URL: https://technet.microsoft.com/en-us/library/bb123484.aspx
[Ref.- 38]	"View or Configure Exchange ActiveSync Mailbox Policy Properties" (Microsoft Exchange 2010). Microsoft Technet. 2010. URL: http://technet.microsoft.com/en-us/library/bb123994.aspx
[Ref.- 39]	"Android support for Microsoft Exchange in pure Google devices". Google. 2013. URL: http://static.googleusercontent.com/media/www.google.com/es//help/hc/images/android/MicrosoftExchangePoliciesinAndroid.pdf
[Ref.- 40]	"Issue 82: wifi - support ad hoc networking". Android Google Code. 2008. URL: https://code.google.com/p/android/issues/detail?id=82
[Ref.- 41]	"Ad-Hoc (IBSS) mode support for Android 4.2.2 / 4.3 / 4.4". Thinktube. March 2014. URL: http://www.thinktube.com/tech-en/android/wifi-ibss
[Ref.- 42]	"Why Wi-Fi Direct cannot replace Ad-hoc mode". szym. Thinktube. 2014. URL: http://www.thinktube.com/tech-en/android/wifi-direct
[Ref.- 43]	"Issue 1041: Hidden SSID Fails to Connect". Android Google Code. 2008. URL: https://code.google.com/p/android/issues/detail?id=1041

Referencia	Título, autor y ubicación
[Ref.- 44]	"How can I trust CAcert's root certificate?". CAcert Wiki. URL: http://wiki.cacert.org/ImportRootCert#Android_Phones
[Ref.- 45]	"Android code signing". Nikolay Elenkov. April 2013. URL: http://nelenkov.blogspot.com.es/2013/04/android-code-signing.html
[Ref.- 46]	"RealmB's Android Certificate Installer". RealmB. URL: http://www.realmb.com/droidCert/
[Ref.- 47]	"Settings-Secure". Android Developers. URL: http://developer.android.com/reference/android/provider/Settings.Secure.html
[Ref.- 48]	dhcpcd. Roy Marples. URL: https://roy.marples.name/projects/dhcpcd
[Ref.- 49]	"Guía CCN-STIC-406: Seguridad en redes inalámbricas". CCN-CERT. URL: https://www.ccn-cert.cni.es (Guías)
[Ref.- 50]	"Description of the Wireless Client Update for Windows XP with Service Pack 2". Microsoft. 2010. URL: http://support.microsoft.com/kb/917021
[Ref.- 51]	"Guía CCN-STIC-418: Seguridad en Bluetooth". CCN-CERT. URL: https://www.ccn-cert.cni.es (Guías)
[Ref.- 52]	"ConnectivityManager". Android Developers. URL: https://developer.android.com/reference/android/net/ConnectivityManager.html
[Ref.- 53]	"Wi-Fi Direct ("P2P")". Wi-Fi Alliance. 2013. URL: http://www.wi-fi.org/discover-and-learn/wi-fi-direct
[Ref.- 54]	"Issue 3389: Full IPv6 Android support". Android Google Code. 2009. URL: https://code.google.com/p/android/issues/detail?id=3389 URL: https://code.google.com/p/android/issues/detail?id=3389#c107
[Ref.- 55]	"Issue 14013: Enable IPv6 Privacy Extensions". Android Google Code. 2011. URL: https://code.google.com/p/android/issues/detail?id=14013 URL: http://www.h-online.com/security/news/item/IPv6-Smartphones-compromise-users-privacy-1169708.html
[Ref.- 56]	"These aren't the permissions you're looking for". A. Lineberry, D. Richardson, T. Wyatt". Defcon 18. 2010. URL: https://media.defcon.org/DEF%20CON%2018/DEF%20CON%2018%20slides/DEF%20CON%2018%20Hacking%20Conference%20Presentation%20By%20-%20Lineberry%20Richardson%20and%20Wyatt%20-%20These%20Aren%27t%20the%20Permissions%20-%20Slides.m4v
[Ref.- 57]	"Support connecting to IPv6-only wireless networks". Android Google Code. June 2012. URL: https://code.google.com/p/android/issues/detail?id=32630
[Ref.- 58]	"Best Practices for Security & Privacy". Android Developers. URL: https://developer.android.com/training/best-security.html
[Ref.- 59]	"Use of IPv6 privacy extensions should be configurable ". Android Google Code. May 2012. URL: https://code.google.com/p/android/issues/detail?id=31102
[Ref.- 60]	"2 big points critics always miss about Android upgrades". Computer World. June 2015. URL: http://www.computerworld.com/article/2476391/android/2-big-points-critics-always-miss-about-android-upgrades.html
[Ref.- 61]	"Encontrar un dispositivo Android que has perdido". Google. URL: https://support.google.com/accounts/answer/3265955?hl=es
[Ref.- 62]	"12 Days of HaXmas: A year of Metasploit Android exploits". Rapid 7. January 2015. URL: https://community.rapid7.com/community/metasploit/blog/2015/01/02/2014-a-year-of-android-exploits-in-metasploit
[Ref.- 63]	"WebView addJavascriptInterface Remote Code Execution". MRW Labs. September 2013. URL: https://labs.mwrinfosecurity.com/blog/2013/09/24/webview-addjavascriptinterface-remote-code-execution/ URL: https://labs.mwrinfosecurity.com/blog/2012/04/23/adventures-with-android-webviews/
[Ref.- 64]	"Por qué se debe iniciar sesión en Chrome". Google. URL: https://support.google.com/chrome/answer/165139?hl=es URL: https://support.google.com/chrome/answer/1181035 URL: https://support.google.com/chrome/answer/2591582?hl=es
[Ref.- 65]	Android Vulnerabilities. 2015. URL: http://androidvulnerabilities.org

Referencia	Título, autor y ubicación
[Ref.- 66]	"No puedes desbloquear el dispositivo Android". Google. URL: https://support.google.com/nexus/answer/3388218?hl=es
[Ref.- 67]	"Android Security Announcements". Google Groups. 2008. URL: https://groups.google.com/group/android-security-announce
[Ref.- 68]	"Android Security Discussions". Google Groups. 2008. URL: http://groups.google.com/group/android-security-discuss
[Ref.- 69]	[old] "Android Security FAQ". Android Developers. URL: http://developer.android.com/resources/faq/security.html URL [actualizada]: https://developer.android.com/training/best-security.html
[Ref.- 70]	"Android Security Bulletines (or Updates)". Google. August 2015. URL: https://source.android.com/security/bulletin/ URL: https://groups.google.com/forum/#!forum/android-security-updates
[Ref.- 71]	"LG Security Bulletins". LG. URL: https://lgsecurity.lge.com/security_updates.html
[Ref.- 72]	"Google Play Devices". Google. URL: https://play.google.com/store/devices
[Ref.- 73]	"Google Experience Devices". DanKor. 2012. URL: http://about.me/googleexperiencedevice URL: http://googleexperiencedevice.blogspot.com
[Ref.- 74]	"Factory Images for Nexus and Pixel Devices". Google. URL: https://developers.google.com/android/images
[Ref.- 75]	"Nexus help. Check & update your Android version". Google. URL: https://support.google.com/nexus/answer/4457705
[Ref.- 76]	"History of the Nexus family". Android Authority. URL: http://www.androidauthority.com/history-nexus-smartphone-line-536352/
[Ref.- 77]	"Android WiFi-Direct Denial of Service". Core Security. January 2015. URL: http://www.coresecurity.com/advisories/android-wifi-direct-denial-service
[Ref.- 78]	"Android Screen Lock Bypass". Thomas Cannon. 2011. URL: http://thomascannon.net/blog/2011/02/android-lock-screen-bypass/
[Ref.- 79]	"Android Market Security". Thomas Cannon. 2011. URL: http://thomascannon.net/blog/2011/02/android-market-security/
[Ref.- 80]	"Certificate pinning in Android 4.2". Nikolay Elenkov. December 2012. URL: http://nelenkov.blogspot.com/2012/12/certificate-pinning-in-android-42.html
[Ref.- 81]	"A Peek Inside the GTalkService Connection". Jon Oberheide. 2010. URL: http://jon.oberheide.org/blog/2010/06/28/a-peek-inside-the-gtalkservice-connection/
[Ref.- 82]	"Remote Kill and Install on Google Android". Jon Oberheide. 2010. URL: http://jon.oberheide.org/blog/2010/06/25/remote-kill-and-install-on-google-android/
[Ref.- 83]	"Apple. Google Collect User Data". Wall Street Journal. 2011. URL: http://on.wsj.com/gDfmEV
[Ref.- 84]	"Android Map". Samy Kamkar. 2011. URL: http://samy.pl/androidmap/
[Ref.- 85]	Android Open Source Project (AOSP). URL: http://source.android.com
[Ref.- 86]	"Android Encryption". Android. URL: https://source.android.com/security/encryption/
[Ref.- 87]	"Android X.Y Platform Highlights" & "Welcome to Android 4.x" & "Android <version>". Android Developers. URL (2.2): http://developer.android.com/about/versions/android-2.2-highlights.html URL (2.3): http://developer.android.com/about/versions/android-2.3-highlights.html URL (3.0): http://developer.android.com/about/versions/android-3.0-highlights.html URL (4.0): http://developer.android.com/about/versions/android-4.0-highlights.html URL (4.1): http://developer.android.com/about/versions/jelly-bean.html#android-41 URL (4.2): http://developer.android.com/about/versions/jelly-bean.html#android-42 URL (4.3): http://developer.android.com/about/versions/jelly-bean.html#android-43 URL (4.4): https://developer.android.com/about/versions/kitkat.html URL (5.0): https://developer.android.com/about/versions/lollipop.html URL (6.0): https://developer.android.com/about/versions/marshmallow/index.html

Referencia	Título, autor y ubicación
[Ref.- 88]	"Compatibility Test Suite (CTS)". Google. URL: http://source.android.com/compatibility/cts/index.html
[Ref.- 89]	"Malware-Infected Apps Yanked From Android Market". Thread post. URL: https://threatpost.com/malware-infected-apps-yanked-android-market-030211/74985/
[Ref.- 90]	CTS (Compatibility Test Suite). AOSP. URL: http://source.android.com/compatibility/cts-intro.html
[Ref.- 91]	"Checking Device Compatibility with SafetyNet". Android Developers. URL: https://developer.android.com/training/safetynet/index.html
[Ref.- 92]	"Device Policy for Android" & "Device Policy Administration for Android" & "Google Apps Mobile Management: Overview". Google Mobile. URL: https://support.google.com/mobile/bin/answer.py?hl=en&answer=190930 URL: http://support.google.com/a/bin/answer.py?hl=en&answer=1056433 URL: https://support.google.com/a/bin/answer.py?hl=en&answer=1734200
[Ref.- 93]	"Issue 6111: Allow a hostname to be specified". Android Google Code. January 2010. URL: https://code.google.com/p/android/issues/detail?id=6111
[Ref.- 94]	"Unpacking Android backups". Nikolay Elenkov. June 2012. URL: http://nelenkov.blogspot.com.es/2012/06/unpacking-android-backups.html URL: https://github.com/nelenkov/android-backup-extractor
[Ref.- 95]	"Establecer conexión mediante zona Wi-Fi, Bluetooth o USB". Google Mobile. URL: https://support.google.com/nexus/answer/2812516?hl=es
[Ref.- 96]	"[TAD-2011-003] Vulnerability in Android: To add, or not to add (a Wi-Fi network), that is the question". Raúl Siles. Taddong. Mayo 2010. URL: http://blog.taddong.com/2011/05/vulnerability-in-android-to-add-or-not.html
[Ref.- 97]	"Issue 1215: IP settings for WiFi networks". Android Android Google Code. November 2008. URL: https://code.google.com/p/android/issues/detail?id=1215
[Ref.- 98]	"Putting Android to work for your business". Official Google Enterprise Blog. April 2011. URL: http://googleenterprise.blogspot.com/2011/04/putting-android-to-work-for-your.html
[Ref.- 99]	"SafetyNet". Google. URL: https://developer.android.com/training/safetynet/index.html
[Ref.- 100]	"Issue 11855: Support settings change in Android WIFI/USB Tether". Android Google Code. October 2010. URL: https://code.google.com/p/android/issues/detail?id=11855
[Ref.- 101]	"A Tale Of Another SOP Bypass In Android Browser < 4.4". Rafay Baloch . October 2014. URL: http://www.rafayhackingarticles.net/2014/10/a-tale-of-another-sop-bypass-in-android.html URL: https://community.rapid7.com/community/metasploit/blog/2014/11/06/metasploit-weekly-wrapup
[Ref.- 102]	"Android Fake ID bug exposes smartphones and tablets". BBC. URL: http://www.bbc.com/news/technology-28544443
[Ref.- 103]	"Package javax.net.ssl". Android Developers. URL: http://developer.android.com/reference/javax/net/ssl/package-summary.html
[Ref.- 104]	"Magisk (Manager)". XDA Developers. URL: http://forum.xda-developers.com/apps/magisk/official-magisk-v7-universal-systemless-t3473445
[Ref.- 105]	"Copia de seguridad y restauración de datos del dispositivo". Google. URL: https://support.google.com/nexus/answer/2819582?hl=es
[Ref.- 106]	"The AndroidManifest.xml File: <permission>". Android Developers. URL: http://developer.android.com/guide/topics/manifest/permission-element.html#plevel
[Ref.- 107]	"SE Android". SE Linux Project. 2012. URL: https://seandroid.bitbucket.io/ URL: http://selinuxproject.org/~jmorris/lss2011_slides/caseforseandroid.pdf
[Ref.- 108]	"Configurar el control parental". Google Play. URL: https://support.google.com/googleplay/answer/1075738?hl=es
[Ref.- 109]	"Flash to Focus on PC Browsing and Mobile Apps; Adobe to More Aggressively Contribute to HTML5". Adobe. Noviembre 2011. URL: http://blogs.adobe.com/conversations/2011/11/flash-focus.html
[Ref.- 110]	"Issue 10809: Password is stored on disk in plain text". Android Google Code. August 2010. URL: https://code.google.com/p/android/issues/detail?id=10809

Referencia	Título, autor y ubicación
[Ref.- 111]	"Android Debug Bridge (ADB)". Android Developers. URL: http://developer.android.com/guide/developing/tools/adb.html
[Ref.- 112]	"Catching AuthTokens in the Wild - The Insecurity of Google's ClientLogin Protocol". Bastian Könings, Jens Nickels, and Florian Schaub. Mayo 2011. URL: http://www.uni-ulm.de/en/in/mi/staff/koenings/catching-authtokens.html URL: https://freedom-to-tinker.com/blog/dwallach/things-overheard-wifi-my-android-smartphone URL: http://android.stackexchange.com/questions/3129/what-android-syncd-data-is-encrypted
[Ref.- 113]	"Chrome for Android". Google. URL: https://developer.chrome.com/multidevice/faq
[Ref.- 114]	"Google Data Protocol - FAQ". Google Code. URL: https://code.google.com/apis/gdata/faq.html#clientlogin_expire
[Ref.- 115]	"Authentication and Authorization for Google APIs - ClientLogin for Installed Applications". Google Code. URL: https://code.google.com/apis/accounts/docs/AuthForInstalledApps.html
[Ref.- 116]	"Using OAuth 2.0 to Access Google APIs". Google. URL: https://developers.google.com/accounts/docs/OAuth2
[Ref.- 117]	"LOOK-10-007 - TapJacking". Lookout. December 2010. URL: http://blog.mylookout.com/look-10-007-tapjacking/ URL: http://blog.mylookout.com/blog/2010/12/09/android-touch-event-hijacking/
[Ref.- 118]	[old] "Android Master Key Exploit - Uncovering Android Master Key That Makes 99% of Devices Vulnerable". BlueBox. July 2013. URL: https://bluebox.com/technical/uncovering-android-master-key-that-makes-99-of-devices-vulnerable/
[Ref.- 119]	"Android Browser Same Origin Policy Bypass < 4.4 - CVE-2014-6041". Rafay Baloch . September 2014. URL: http://www.rafayhackingarticles.net/2014/08/android-browser-same-origin-policy.html URL: https://community.rapid7.com/community/metasploit/blog/2014/09/15/major-android-bug-is-a-privacy-disaster-cve-2014-6041
[Ref.- 120]	"Android WebView fixes". Adrian Ludwig. January 2015. URL: https://plus.google.com/+AdrianLudwig/posts/1md7ruEwBLF URL: https://community.rapid7.com/community/metasploit/blog/2015/01/11/google-no-longer-provides-patches-for-webview-jelly-bean-and-prior URL: https://community.rapid7.com/community/metasploit/blog/2015/01/16/weekly-metasploit-wrapup
[Ref.- 121]	"Issue 8196: Enhancement: Client Certificate Authentication in Browser". Android Google Code. May 2010. URL: https://code.google.com/p/android/issues/detail?id=8196
[Ref.- 122]	"Issue 11231: Provide support for managing CA and client certificates". Android Google Code. September 2010. URL: https://code.google.com/p/android/issues/detail?id=11231
[Ref.- 123]	"KeyChain". Android Developers. URL: http://developer.android.com/reference/android/security/KeyChain.html
[Ref.- 124]	"Browser Security Handbook, part 2". Michal Zalewski. Marzo 2011 (actualizado). URL: https://code.google.com/p/browsersec/wiki/Part2#Same-origin_policy_for_cookies
[Ref.- 125]	"Uso del ID de publicidad de Android": Google Play. URL: https://play.google.com/intl/es/about/monetization-ads/ads/ad-id/
[Ref.- 126]	"Issue 6348: Bluetooth should have the option to be constantly discoverable and not just have a set time limit". Android Google Code. January 2010. URL: https://code.google.com/p/android/issues/detail?id=6348
[Ref.- 127]	"Malicious Android Applications: Risks and Exploitation". Joany Boutet. SANS Reading Room. Marzo 2010. URL: https://www.sans.org/reading_room/whitepapers/malicious/malicious-android-applications-risks-exploitation_33578

Referencia	Título, autor y ubicación
[Ref.- 128]	"App Ops Brings Granular Permissions Control to Android 4.3". Will Verduzco. Julio 2013. URL: http://www.xda-developers.com/app-ops-brings-granular-permissions-control-to-android-4-3/ URL: http://www.androidpolice.com/2013/07/25/app-ops-android-4-3s-hidden-app-permission-manager-control-permissions-for-individual-apps/
[Ref.- 129]	"App Ops Lives On In Android 4.4, Can Now Deny Even More Permissions". Android Police. November 2013. URL: http://www.androidpolice.com/2013/11/25/new-app-app-ops-lives-on-in-android-4-4-can-be-unleashed-with-app-ops-from-color-tiger-and-enhanced-with-root/
[Ref.- 130]	"Using WebView - Security Tips". Google. 2015. URL: http://developer.android.com/training/articles/security-tips.html#WebView
[Ref.- 131]	"Android Version History". Wikipedia. URL: https://en.wikipedia.org/wiki/Android_version_history
[Ref.- 132]	"AppOps". Sylvain Galand. URL: https://play.google.com/store/apps/details?id=fr.slvn.appops&hl=en URL: https://github.com/slvn/android-appops-launcher
[Ref.- 133]	"Security". Android. URL: https://www.android.com/security-center/
[Ref.- 134]	"Security". Android Open Source. URL: https://source.android.com/security/index.html
[Ref.- 135]	"Revisiting Android disk encryption". Nikolay Elenkov. Octubre 2014. URL: http://nelenkov.blogspot.com.es/2014/10/revisiting-android-disk-encryption.html
[Ref.- 136]	"DevBytes: Android L Developer Preview". Google Developers. Julio 2014. URL: https://www.youtube.com/watch?v=s7JLYYkJuNs#t=90
[Ref.- 137]	"Sharing what's up our sleeve: Android coming to wearables". Official Android Blog. Julio 2014. URL: https://android.googleblog.com/2014/03/sharing-whats-up-our-sleeve-android.html
[Ref.- 138]	"DevBytes: Restricted Profiles in Android 4.3". Google Developers. Julio 2014. URL: https://www.youtube.com/watch?v=pdUcANNm72o
[Ref.- 139]	"CCS Injection Vulnerability". Lepidum. June 2014. URL: http://ccsinjection.lepidum.co.jp URL: http://ccsinjection.lepidum.co.jp/blog/2014-06-05/CCS-Injection-en/index.html
[Ref.- 140]	"Early ChangeCipherSpec Attack". Imperial Violet - Adam Langley. Junio 2014. URL: https://www.imperialviolet.org/2014/06/05/earlyccs.html
[Ref.- 141]	"Security Enhancements in Android x.y". Android Source. URL: https://source.android.com/security/enhancements/index.html URL: https://source.android.com/security/enhancements/enhancements41.html URL: https://source.android.com/security/enhancements/enhancements42.html URL: https://source.android.com/security/enhancements/enhancements43.html URL: https://source.android.com/security/enhancements/enhancements44.html URL: https://source.android.com/security/enhancements/enhancements50.html URL: https://source.android.com/security/enhancements/enhancements60.html
[Ref.- 142]	"Android Hacker's Handbook". Wiley. 2014.
[Ref.- 143]	"Security-Enhanced Linux in Android". Android Source. URL: http://source.android.com/devices/tech/security/se-linux.html
[Ref.- 144]	Google Cloud Messaging (GCM) for Android. Google. URL: http://developer.android.com/google/gcm/index.html
[Ref.- 145]	"Credential storage enhancements in Android 4.3". Nikolay Elenkov. August 2013. URL: http://nelenkov.blogspot.com.es/2013/08/credential-storage-enhancements-android-43.html
[Ref.- 146]	"Android's 5.x Lock Screen may be bypassed by attackers". Martin Brinkmann. Ghacks.net URL: https://www.ghacks.net/2015/09/16/androids-5-x-lock-screen-may-be-bypassed-by-attackers/
[Ref.- 147]	"Secure USB debugging in Android 4.2.2". Nikolay Elenkov. Febrero 2013. URL: http://nelenkov.blogspot.com.es/2013/02/secure-usb-debugging-in-android-422.html URL: http://android-developers.blogspot.jp/2013/02/security-enhancements-in-jelly-bean.html
[Ref.- 148]	"Utilizar el identificador de llamada de Google". Google. 2014. URL: https://support.google.com/nexus/answer/3459196?hl=es

Referencia	Título, autor y ubicación
[Ref.- 149]	"Android 4.4 - KitKat". Google. URL: http://www.android.com/versions/kit-kat-4-4/ URL: https://www.youtube.com/watch?v=sONcojECWXs
[Ref.- 150]	"Administrar la ubicación de tu dispositivo". Google. URL: https://support.google.com/nexus/answer/3467281?hl=es
[Ref.- 151]	Google Play Services. Google. URL: https://developer.android.com/google/play-services/index.html
[Ref.- 152]	"On the WebView addJavascriptInterface Saga". DroidSec. February 2014. URL: http://www.droidsec.org/news/2014/02/26/on-the-webview-addjsif-saga.html
[Ref.- 153]	"Updating Your Security Provider to Protect Against SSL Exploits". Android. URL: http://developer.android.com/training/articles/security-gms-provider.html
[Ref.- 154]	"Issue 52314: unlock password is limited to 16 characters". Android Google Code. February 2013. URL: https://code.google.com/p/android/issues/detail?id=52314
[Ref.- 155]	"Issue 29468: Different passwords for encryption and screen lock". Android Google Code. April 2012. URL: https://code.google.com/p/android/issues/detail?id=29468
[Ref.- 156]	"EncPassChanger". Kibab. December 2012. URL: https://github.com/kibab/encpasschanger URL: https://play.google.com/store/apps/details?id=com.kibab.android.EncPassChanger
[Ref.- 157]	"Cryptfs Password". Nikolay Elenkov. August 2013. URL: https://play.google.com/store/apps/details?id=org.nick.cryptfs.passwdmanager URL: https://github.com/nelenkov/cryptfs-password-manager
[Ref.- 158]	"Changing Android's disk encryption password". Nikolay Elenkov. August 2012. URL: http://nelenkov.blogspot.com/2012/08/changing-androids-disk-encryption.html
[Ref.- 159]	"Android encryption switched to scrypt in 4.4.2". AOSP. URL: https://android.googlesource.com/platform/system/vold/+/android-4.4_r1/cryptfs.c URL: https://android.googlesource.com/platform/system/vold/+log/android-4.4_r1/cryptfs.c (commit c4c70f1) URL: https://android.googlesource.com/platform/system/vold/+/c4c70f15bb8845b02f9ec1d624794757badd6933
[Ref.- 160]	"Android Security Internals". Nikolay Elenkov. No Starch Press. October 2014. URL: http://www.nostarch.com/androidsecurity
[Ref.- 161]	"Android's Permissions System Is Broken and Google Just Made It Worse". Chris Hoffman. December 2013. URL: http://www.howtogeek.com/177904/androids-permissions-system-is-broken-and-google-just-made-it-worse/
[Ref.- 162]	"Android's App Permissions Were Just Simplified - Now They're Much Less Secure". Chris Hoffman. June 2014. URL: http://www.howtogeek.com/190863/androids-app-permissions-were-just-simplified-now-theyre-much-less-secure/
[Ref.- 163]	"Revisar los permisos de aplicaciones en Android 5.1.1 o anteriores ". Google. 2015. URL: https://support.google.com/googleplay/answer/6014972?hl=es
[Ref.- 164]	"Android 5.x Lockscreen Bypass (CVE-2015-3860)". Austin University of Texas. http://sites.utexas.edu/iso/2015/09/15/android-5-lockscreen-bypass/
[Ref.- 165]	"Añadir aplicaciones, accesos directos y widgets a las pantallas de inicio ". Google. URL: https://support.google.com/nexus/answer/2781850?hl=es
[Ref.- 166]	"Storage Access Framework". Google. URL: https://developer.android.com/guide/topics/providers/document-provider.html URL: https://www.youtube.com/watch?v=zxHVeXbK1P4 URL: https://www.youtube.com/watch?v=UFj9AEz0DHQ
[Ref.- 167]	"Activar o desactivar SafeSearch". Google. URL: https://support.google.com/websearch/answer/510?hl=es
[Ref.- 168]	"Ubicación en Ajustes de Google". Google. URL: https://support.google.com/accounts/answer/3118687?hl=es
[Ref.- 169]	"ART (Android RunTime)". Google. URL: http://source.android.com/devices/tech/dalvik/
[Ref.- 170]	"Android and Security" (Google Bouncer). Google Mobile Blog. February 2012. URL: http://googlemobile.blogspot.com/2012/02/android-and-security.html

Referencia	Título, autor y ubicación
[Ref.- 171]	"Android 4.2 'Verify apps' security feature explained by Google". Android Authority. November 2012. URL: http://www.androidauthority.com/android-4-2-verify-apps-security-feature-explained-by-google-131514/
[Ref.- 172]	"Expanding Google's security services for Android". Android Official Blog. April 2014. URL: http://officialandroid.blogspot.com.es/2014/04/expanding-googles-security-services-for.html
[Ref.- 173]	"Protegerse frente a aplicaciones dañinas". Google. URL: https://support.google.com/accounts/answer/2812853?hl=es URL: https://plus.google.com/+MichaelMorrissey/posts/dutcnbu72pv
[Ref.- 174]	"An Evaluation of the Application ("App") Verification Service in Android 4.2". Xuxian Jiang. December 2012. URL: http://www.cs.ncsu.edu/faculty/jiang/appverify/
[Ref.- 175]	"Dissecting the Android Bouncer". Jon Oberheide. 2012. URL: https://jon.oberheide.org/files/summercon12-bouncer.pdf
[Ref.- 176]	"Actividad web y de aplicaciones". Google. URL: https://support.google.com/accounts/answer/54068?hl=es
[Ref.- 177]	"Eliminar búsquedas y actividad de navegación". Google. URL: https://support.google.com/accounts/answer/465?hl=es
[Ref.- 178]	"Crear una copia de seguridad de tus fotos y vídeos automáticamente". Google. URL: https://support.google.com/plus/answer/1647509
[Ref.- 179]	"Función Reconóceme en fotos y vídeos". Google. URL: https://support.google.com/plus/answer/2370300?hl=es
[Ref.- 180]	"Ver fotos en las que te hayan etiquetado". Google. URL: https://support.google.com/plus/answer/1254833?hl=es
[Ref.- 181]	"Bloquear o desbloquear cuentas de otras personas". Google. URL: https://support.google.com/accounts/answer/6388749?visit_id=1-636343239744150110-383769448&p=block_list&hl=es&rd=1
[Ref.- 182]	"New NFC capabilities through Host Card Emulation". Google. URL: http://developer.android.com/about/versions/kitkat.html#44-hce
[Ref.- 183]	"Cómo compartir contenido con Android Beam". Google. URL: https://support.google.com/nexus/answer/2781895?hl=es
[Ref.- 184]	"Utilizar la función Tocar y pagar con tu dispositivo". Google. URL: https://support.google.com/nexus/answer/3470787?hl=es
[Ref.- 185]	"Security Tips". Google. 2015. URL: http://developer.android.com/training/articles/security-tips.html
[Ref.- 186]	"Utilizar certificados". Google. URL: https://support.google.com/nexus/answer/2844832?hl=es
[Ref.- 187]	"ID de publicidad". Google. URL: https://support.google.com/googleplay/android-developer/answer/6048248?hl=es
[Ref.- 188]	"Nexus 5 Stock OTA URLs". XDA Developers. URL: http://forum.xda-developers.com/google-nexus-5/general/ref-nexus-5-stock-ota-urls-t2475327
[Ref.- 189]	"Using the ICS KeyChain API" (4.0, ICS). Nikolay Elenkov. November 2011. URL: http://nelenkov.blogspot.com.es/2011/11/using-ics-keychain-api.html "ICS Credential Storage Implementation". Part 1 & 2. November/December 2011. URL: http://nelenkov.blogspot.com.es/2011/11/ics-credential-storage-implementation.html URL: http://nelenkov.blogspot.com.es/2011/12/ics-credential-storage-implementation.html
[Ref.- 190]	"ICS Trust Store Implementation" (4.0, ICS). Nikolay Elenkov. December 2011. URL: http://nelenkov.blogspot.com.es/2011/12/ics-trust-store-implementation.html
[Ref.- 191]	"Certificate blacklisting in Jelly Bean" (4.1, JB). Nikolay Elenkov. July 2012. URL: http://nelenkov.blogspot.com.es/2012/07/certificate-blacklisting-in-jelly-bean.html
[Ref.- 192]	"Jelly Bean hardware-backed credential storage" (4.1, JB). Nikolay Elenkov. July 2012. URL: http://nelenkov.blogspot.jp/2012/07/jelly-bean-hardware-backed-credential.html
[Ref.- 193]	"Questioning the chain of trust: investigations into the root certificates on mobile devices". Andrew Blaich. Bluebox. October 2014. URL: https://bluebox.com/blog/technical/questioning-the-chain-of-trust-investigations-into-the-root-certificates-on-mobile-devices/

Referencia	Título, autor y ubicación
[Ref.- 194]	"Iniciar sesión con tu teléfono en lugar de usar una contraseña". Google. URL: https://support.google.com/accounts/answer/6361026?hl=es
[Ref.- 195]	"Why Do Wi-Fi Clients Disclose their PNL for Free Still Today?". Raúl Siles. DinoSec. February 2015. URL: http://blog.dinosec.com/2015/02/why-do-wi-fi-clients-disclose-their-pnl.html
[Ref.- 196]	"A Systematic Security Evaluation of Android's Multi-User Framework". 2014. URL: http://www.cis.syr.edu/~wedu/Research/paper/multi_user_most2014.pdf
[Ref.- 197]	"Android Internals: A Confectioner's Cookbook". Jonathan Levin. 2015. URL: http://newandroidbook.com URL: http://newandroidbook.com/files/Andevcon-ART.pdf ("ART (& OAT) Internals")
[Ref.- 198]	"Android for Work". Android. URL: https://www.android.com/work/ URL: https://enterprise.google.com/android
[Ref.- 199]	"Samsung Android Security Updates". Samsung. October 2015. URL: http://security.samsungmobile.com/smrupdate.html
[Ref.- 200]	"Full OTA Images for Nexus and Pixel Devices". Google. URL: https://developers.google.com/android/ota
[Ref.- 201]	"Application Signing". Android Source. URL: https://source.android.com/security/apksigning/
[Ref.- 202]	"Encontrar un dispositivo Android que has perdido". Google. https://support.google.com/accounts/answer/3265955?hl=es
[Ref.- 203]	"Android History". Android. URL: https://www.android.com/history/
[Ref.- 204]	"Android Security Center". Android. URL: https://www.android.com/intl/es_es/security-center/monthly-security-updates/
[Ref.- 205]	"Security Updates and Resources". Android. URL: https://source.android.com/security/overview/updates-resources
[Ref.- 206]	"All together now. Introducing G Suite.". Google Cloud Official blog. September 2016. URL: https://cloud.googleblog.com/2016/09/all-together-now-introducing-G-Suite.html
[Ref.- 207]	"Dissecting Lollipop's Smart Lock". Nelenkov. December 2014. URL: https://nelenkov.blogspot.com.es/2014/12/dissecting-lollipops-smart-lock.html
[Ref.- 208]	Android Security Bulletin. Google. URL: https://source.android.com/security/bulletin/2016-12-01
[Ref.- 209]	"How many combinations does Android 9 point unlock have?". Quora. February 2011. URL: https://www.quora.com/Android-operating-system-How-many-combinations-does-Android-9-point-unlock-have/answer/Yoyo-Zhou URL: http://beust.com/weblog2/archives/000497.html
[Ref.- 210]	"Password storage in Android M". Nikolay Elenkov. June 2015. URL: https://nelenkov.blogspot.com.es/2015/06/password-storage-in-android-m.html
[Ref.- 211]	"Añadir aplicaciones, accesos directos y widgets a las pantallas de inicio". Google. URL: https://support.google.com/nexus/answer/2781850?hl=es
[Ref.- 212]	"Administrar invitados y usuarios". Google. URL: https://support.google.com/nexus/answer/2865944?hl=es
[Ref.- 213]	"Utilizar perfiles restringidos en tablets". Ayuda de Nexus. URL: https://support.google.com/nexus/answer/3175031
[Ref.- 214]	"Configurar la gestión de dispositivos móviles". Ayuda de G-Suite. Google. URL: https://support.google.com/a/answer/6328699?hl=es
[Ref.- 215]	"The Chromium Projects". URL: https://www.chromium.org/
[Ref.- 216]	"Informe de transparencia". Google. URL: https://www.google.com/transparencyreport/safebrowsing/?hl=es-419
[Ref.- 217]	"Administrar advertencias sobre sitios web no seguros". Google. URL: https://support.google.com/chrome/answer/99020?co=GENIE.Platform%3DAndroid
[Ref.- 218]	"Modificar la configuración de contenido de los sitios web". Google. URL: https://support.google.com/chrome/answer/114662?co=GENIE.Platform%3DAndroid&hl=es
[Ref.- 219]	"Conectar un sitio web a un dispositivo Bluetooth o USB". Google. URL: https://support.google.com/chrome/answer/6362090

Referencia	Título, autor y ubicación
[Ref.- 220]	"Navegar en privado con el modo incógnito". Google. URL: https://support.google.com/chrome/answer/95464?co=GENIE.Platform%3DAndroid&hl=es
[Ref.- 221]	"QUIC, a multiplexed stream transport over UDP". "The Chromium project". URL: https://www.chromium.org/quic
[Ref.- 222]	"PdfRenderer". Android Developers. URL: https://developer.android.com/reference/android/graphics/pdf/PdfRenderer.html
[Ref.- 223]	"Actualizar las aplicaciones Android". Ayuda de Google Play. URL: https://support.google.com/googleplay/answer/113412?hl=es
[Ref.- 224]	"Advisory: Crashing Android devices with large Assisted-GPS Data Files [CVE-2016-5348]". Nightwatch Cybersecurity. October 2016. URL: https://wwws.nightwatchcybersecurity.com/2016/10/04/advisory-cve-2016-5348-2/
[Ref.- 225]	"USB Host and Accessory". Android developers. URL: https://developer.android.com/guide/topics/connectivity/usb/index.html
[Ref.- 226]	"Android HAX". Jon Oberheide. URL: https://jon.oberheide.org/files/summercon10-androidhax-jonoberheide.pdf
[Ref.- 227]	"Android Device Manager has a new name: Find My Device". Engadget. URL: https://www.engadget.com/2017/05/18/google-lost-android-find-my-device/
[Ref.- 228]	"Descargar zonas y navegar sin conexión". Google. URL: https://support.google.com/maps/answer/6291838?co=GENIE.Platform%3DAndroid&hl=es
[Ref.- 229]	"Ver o editar tu cronología". Google. URL: https://support.google.com/maps/answer/6258979?hl=es&ref_topic=3092425&co=GENIE.Platform%3DAndroid&oco=1
[Ref.- 230]	"Ayuda de Google Maps". Google. URL: https://support.google.com/maps#topic=3092425
[Ref.- 231]	"Share your trips and real-time location from Google Maps". Google blog. URL: https://www.blog.google/products/maps/share-your-trips-and-real-time-location-google-maps/
[Ref.- 232]	"Compartir tu ubicación en tiempo real con otros usuarios". Ayuda de Google Maps. URL: https://support.google.com/maps/answer/7326816?hl=es&ref_topic=3092425&co=GENIE.Platform%3DAndroid&oco=1
[Ref.- 233]	"Iniciar sesión en Chrome". Google. URL: https://support.google.com/chrome/answer/185277?co=GENIE.Platform%3DDesktop&hl=es
[Ref.- 234]	"Compartir Chrome con otros usuarios o añadir un perfil". Google. URL: https://support.google.com/chrome/answer/2364824?co=GENIE.Platform%3DAndroid&oco=1
[Ref.- 235]	"Protecting hundreds of millions more mobile users". Google Security Blog. URL: https://security.googleblog.com/2015/12/protecting-hundreds-of-millions-more.html
[Ref.- 236]	"Gestionar la opción Información de los dispositivos". Google. URL: https://support.google.com/accounts/answer/6135999?p=account_device_info&hl=es&authuser=0&visit_id=1-636342504159902489-3147238312&rd=1
[Ref.- 237]	"Cómo fijar y dejar de fijar pantallas". Google. URL: https://support.google.com/nexus/answer/6118421?hl=es-419
[Ref.- 238]	"Hardware-accelerated disk encryption in Android 5.1". Nikolay Elenkov. May 2015. URL: https://nelenkov.blogspot.com.es/2015/05/hardware-accelerated-disk-encryption-in.html
[Ref.- 239]	"Sincronizar contraseñas en tus dispositivos". Google. URL: https://support.google.com/accounts/answer/6197437?co=GENIE.Platform%3DAndroid
[Ref.- 240]	"Android Instant Apps". Google Developer. URL: https://developer.android.com/topic/instant-apps/index.html
[Ref.- 241]	"Presentación de las Instant Apps en Google I/O 2016". Google. URL: https://youtu.be/cosqlfqrpFA
[Ref.- 242]	"Android Instant Apps: The security jury is out". NowSecure. URL: https://www.nowsecure.com/blog/2016/05/19/android-instant-apps-the-security-jury-is-out/
[Ref.- 243]	"Will Google's Instant Apps Undermine Enterprise Security?". Appthority. URL: https://www.appthority.com/mobile-threat-center/blog/will-googles-instant-apps-undermine-enterprise-security/
[Ref.- 244]	"Sincronizar contraseñas en tus dispositivos". Google. URL: https://support.google.com/accounts/answer/6197437?co=GENIE.Platform%3DAndroid&oco=1

Referencia	Título, autor y ubicación
[Ref.- 245]	"Introducing the Google Identity Platform". Google developers blog. URL: https://developers.googleblog.com/2015/05/introducing-google-identity-platform.html
[Ref.- 246]	"Smart Lock for Passwords on Android". Google developers. URL: https://developers.google.com/identity/smartlock-passwords/android/
[Ref.- 247]	"Android One". Google. URL: https://www.android.com/one/
[Ref.- 248]	"Taking the next step with Android One". Google. URL: https://www.blog.google/products/android/taking-next-step-android-one/
[Ref.- 249]	"Cómo administrar tus claves de firma de apps". Google. URL: https://support.google.com/googleplay/android-developer/answer/7384423?hl=es-419
[Ref.- 250]	"Security-Enhanced Linux in Android". Google. URL: https://source.android.com/security/selinux/
[Ref.- 251]	"KeyChain". Android Developers. URL: https://developer.android.com/reference/android/security/KeyChain.html
[Ref.- 252]	"Google collects Android users' locations even when location services are disabled". Quartz. URL: https://qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled/
[Ref.- 253]	"Google Privacy Policy". Google. URL: https://www.google.com/policies/privacy/
[Ref.- 254]	"iBeacon". Apple. URL: https://developer.apple.com/ibeacon/
[Ref.- 255]	"Platform Overview". Google Beacon Platform. URL: https://developers.google.com/beacons/
[Ref.- 256]	"G Pay". Google. URL: https://www.blog.google/topics/shopping-payments/announcing-google-pay/?
[Ref.- 257]	"Legacy Core Specifications". Bluetooth SIG. URL: https://www.bluetooth.com/specifications/bluetooth-core-specification/legacy-specifications
[Ref.- 258]	"Wireshark". Wireshark.org. URL: https://www.wireshark.org
[Ref.- 259]	"Firebase". Google. URL: https://firebase.google.com/docs
[Ref.- 260]	"OAuth 2.0". OAuth.net. URL: http://oauth.net/2/
[Ref.- 261]	"Instalar Google Authenticator". Google. URL: https://support.google.com/accounts/answer/1066447
[Ref.- 262]	"Utilizar la llave de seguridad para la verificación en dos pasos". Google. URL: https://support.google.com/accounts/answer/6103523?hl=es
[Ref.- 263]	¿Qué es el centro de pagos de Google?. Google. URL: https://support.google.com/payments/answer/7500996
[Ref.- 264]	"Add Google Sign-In to Your Android App". Google. URL: https://developers.google.com/identity/sign-in/android/
[Ref.- 265]	"Files that are backed up". Google. URL: https://developer.android.com/guide/topics/data/autobackup.html#Files
[Ref.- 266]	"Back Up Key-Value Pairs with Android Backup Service". Google. URL: https://developer.android.com/guide/topics/data/keyvaluebackup.html
[Ref.- 267]	"Inhabilitar el inicio de sesión automático". Google. URL: https://support.google.com/accounts/answer/39273?hl=es
[Ref.- 268]	"DigiNotar Certificate Authority Breach Crashes e-Government in the Netherlands". IEEE Spectrum. URL: https://spectrum.ieee.org/riskfactor/telecom/security/diginotar-certificate-authority-breach-crashes-egovernment-in-the-netherlands
[Ref.- 269]	"Device Administration". Android Developers. URL: https://developer.android.com/guide/topics/admin/device-admin.html
[Ref.- 270]	"Google Digital Asset Links". Google Developers. URL: https://developers.google.com/digital-asset-links/v1/getting-started

Referencia	Título, autor y ubicación
[Ref.- 271]	"The Android Trojan Svpeng now capable of Mobile Phising". SecureList. URL: https://securelist.com/the-android-trojan-svpeng-now-capable-of-mobile-phishing/57301/ "The evolution of Acecard". SecureList. URL: https://securelist.com/the-evolution-of-acecard/73777/
[Ref.- 272]	"The best antivirus software for Android". The Independent IT-Security Institute. URL: https://www.av-test.org/en/antivirus/mobile-devices/android/september-2017/?_ga=2.224379036.604887240.1508931778-1860796072.1508931778
[Ref.- 273]	"android.app.admin overview". Android developers. URL: https://developer.android.com/reference/android/app/admin/package-summary.html
[Ref.- 274]	"Phishing prevention with Password Alert FAQ". G Suite Administrator Help. Google. URL: https://support.google.com/a/answer/6197508?hl=en URL: https://support.google.com/accounts/answer/6206323?hl=en

Nota: Por completitud se han empleado las siguientes tablas de referencias completas de la guía "CCN-STIC-453E - Seguridad de dispositivos móviles: Android 7.x" [Ref.- 407], aunque muchas de las referencias no son utilizadas a lo largo de la presente guía. Las tablas de referencias, a su vez, han sido ampliadas con referencias específicas para la presente guía.

La siguiente tabla muestra las fuentes de información a las que se hace referencia a lo largo de la presente guía, en concreto las referencias asociadas directamente al CCN-CERT:

Referencia	Título, autor y ubicación
[Ref.- 400]	"Guía CCN-STIC-450: Seguridad de dispositivos móviles". CCN-CERT. Marzo 2013. URL: 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]	"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. Enero 2018. URL: <*enlace correspondiente a la versión previa de la presente guía*>
[Ref.- 406]	"Guía CCN-STIC-453D - Seguridad de dispositivos móviles: Android 6.x". CCN-CERT. Marzo 2018. URL: https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2901-ccn-stic-453d-seguridad-de-dispositivos-moviles-android-6-x.html
[Ref.- 407]	"Guía CCN-STIC-453E - Seguridad de dispositivos móviles: Android 7.x". CCN-CERT. SEP 2018:

La siguiente tabla muestra las fuentes de información a las que se hace referencia a lo largo de la presente guía relacionadas específicamente con la versión 5.x (Lollipop) de Android:

Referencia	Título, autor y ubicación
[Ref.- 500]	"Android 5.0 Lollipop". Android. URL: https://www.android.com/versions/lollipop-5-0/
[Ref.- 501]	"Android Lollipop". Android Developers. URL: https://developer.android.com/about/versions/lollipop.html
[Ref.- 502]	"Android 5.0 APIs". Android Developers. URL: https://developer.android.com/about/versions/android-5.0.html
[Ref.- 503]	"Android 5.0 Behavior Changes". Android Developers. URL: https://developer.android.com/about/versions/android-5.0-changes.html
[Ref.- 504]	"Android 5.1 APIs". Android Developers. URL: https://developer.android.com/about/versions/android-5.1.html
[Ref.- 505]	"Android in the Workplace and in Education". Android 5.0 Developers. URL: https://developer.android.com/about/versions/android-5.0.html#Enterprise
[Ref.- 506]	"Android Platform Tools r20". URL: http://dl-ssl.google.com/android/repository/platform-tools_r20-macosx.zip URL: http://dl-ssl.google.com/android/repository/platform-tools_r20-windows.zip URL: http://dl-ssl.google.com/android/repository/platform-tools_r20-linux.zip
[Ref.- 507]	"Notifications". Android Developers - Google. URL: https://developer.android.com/guide/topics/ui/notifiers/notifications.html

Referencia	Título, autor y ubicación
[Ref.- 508]	"Android developers". Google. URL: https://developer.android.com/about/versions/android-5.0-changes.html#BehaviorNotifications
[Ref.- 509]	"Android Official Blog". Google. URL: https://android.googleblog.com/2015/03/android-51-unwrapping-new-lollipop.html
[Ref.- 510]	"Memory Leak on Lollipop crashing Apps" - Google issue tracker. https://issuetracker.google.com/issues/37010796
[Ref.- 511]	"UICC Carrier Privileges". Android Source. URL: https://source.android.com/devices/tech/config/uicc
[Ref.- 512]	"Verified Boot". Android. URL: https://source.android.com/security/verifiedboot/ URL: https://source.android.com/security/verifiedboot/verified-boot.html
[Ref.- 513]	"Reiniciar en modo seguro para detectar aplicaciones con problemas". Soporte de Google. URL: https://support.google.com/nexus/answer/2852139?hl=es
[Ref.- 514]	"Cambio de nombre de Android for Work a Android y de Google Play for Work a Google Play". Google. URL: https://support.google.com/work/android/answer/7218437 URL: https://blog.google/topics/connected-workspaces/update-android-and-google-plays-progress-enterprise/
[Ref.- 515]	"Screen Pinning (Fijación de pantalla)". Android Developers. URL: https://developer.android.com/about/versions/android-5.0.html#ScreenPinning
[Ref.- 516]	"¿Qué es un perfil de trabajo?". Google. URL: https://support.google.com/work/android/answer/6191949
[Ref.- 517]	"Tricking Android Smart Lock with Bluetooth". Martin Herfurt. May 2015. URL: https://mherfurt.wordpress.com/2015/05/08/tricking-android-smart-lock-with-bluetooth/ URL: https://youtu.be/Xb0YG6EpY48
[Ref.- 518]	"Set up your device for automatic unlock". Google. Nexus Help. URL: https://support.google.com/nexus/answer/6093922?hl=en
[Ref.- 519]	"Consultar el estado de certificación del dispositivo". Ayuda de Google Play. URL: https://support.google.com/googleplay/answer/7165974?hl=es
[Ref.- 520]	"Device Policy Manager - Password quality". Android Developers. URL: https://developer.android.com/reference/android/app/admin/DevicePolicyManager.html#setPasswordQuality(android.content.ComponentName,%20int)
[Ref.- 521]	"Evitar que otros usuarios utilicen tu dispositivo sin permiso". Google. URL: https://support.google.com/nexus/answer/6172890?hl=es

La siguiente tabla muestra las fuentes de información a las que se hace referencia a lo largo de la presente guía relacionadas específicamente con la versión 6.x (Marshmallow) de Android:

Referencia	Título, autor y ubicación
[Ref.- 600]	"Android 6.0 Marsmallow". Android. URL: https://www.android.com/versions/marshmallow-6-0/
[Ref.- 601]	"Android 6.0 Marshmallow". Android Developers. URL: https://developer.android.com/about/versions/marshmallow/index.html
[Ref.- 602]	"Android 6.0 Changes". Android Developers. URL: https://developer.android.com/about/versions/marshmallow/android-6.0-changes.html
[Ref.- 603]	"Android 6.0 APIs". Android Developers. URL: https://developer.android.com/about/versions/marshmallow/android-6.0.html
[Ref.- 604]	"Handling App Links". Android Developers. URL: https://developer.android.com/training/app-links/index.html
[Ref.- 605]	"BoringSSL". Google. URL: https://boringssl.googlesource.com/boringssl/
[Ref.- 606]	"Android (Marshmallow) Compatibility Definition Document (CDD)" (7.3.10. Fingerprint Sensor). Google. URL: https://source.android.com/compatibility/6.0/android-6.0-cdd

Referencia	Título, autor y ubicación
[Ref.- 607]	"Fingerprint and payments APIs (100 Days of Google Dev)". Google Developers. May 2015. URL: https://www.youtube.com/watch?v=VOn7VrTRlA4
[Ref.- 608]	"Fingerprint security on Nexus devices". Google Support. URL: https://support.google.com/nexus/answer/6300638
[Ref.- 609]	"Desbloque mediante huella dactilar digital". Google Support. URL: https://support.google.com/nexus/answer/6285273
[Ref.- 610]	"Fingerprint Unlock Security: iOS vs. Google Android (Part I & II)". Elcomsoft. June 2016. URL: http://blog.elcomsoft.com/2016/06/ios-fingerprint-unlock-security/ URL: http://blog.elcomsoft.com/2016/06/fingerprint-unlock-security-ios-vs-google-android-part-ii/
[Ref.- 611]	"Fingerprints On Mobile Devices: Abusing and Leaking". FireEye Labs. BH USA 2015. URL: https://www.blackhat.com/docs/us-15/materials/us-15-Zhang-Fingerprints-On-Mobile-Devices-Abusing-And-Leaking-wp.pdf
[Ref.- 612]	"App Install Location". Android Developers. URL: https://developer.android.com/guide/topics/data/install-location.html
[Ref.- 613]	"Apps on SD Card: The Details". Android Developers Blog. July 2010. URL: http://android-developers.blogspot.com/2010/07/apps-on-sd-card-details.html
[Ref.- 614]	"Decrypting Android M adopted storage". Nikolay Elenkov. Android Explorations. June 2015. URL: https://nelenkov.blogspot.com.es/2015/06/decrypting-android-m-adopted-storage.html
[Ref.- 615]	"Fingerprint HAL". Android Source. URL: https://source.android.com/security/authentication/fingerprint-hal.html
[Ref.- 616]	"Optimizing for Doze and App Standby". Android Developers. URL: https://developer.android.com/training/monitoring-device-state/doze-standby.html
[Ref.- 617]	"Requesting Permissions at Run Time". Android Developers. URL: https://developer.android.com/training/permissions/requesting.html
[Ref.- 618]	"Cómo trabajar con permisos del sistema". Android Developers. URL: https://developer.android.com/training/permissions/index.html URL: https://developer.android.com/training/permissions/best-practices.html#testing
[Ref.- 619]	"Warning about operating system safety". Nexus. URL: http://g.co/ABH URL: https://support.google.com/nexus/answer/6185381?p=verified_boot
[Ref.- 620]	"Password storage in Android M". Nikolay Elenkov. Android Explorations. June 2015. URL: https://nelenkov.blogspot.com.es/2015/06/password-storage-in-android-m.html
[Ref.- 621]	"Hardware-backed Keystore". Google. URL: https://source.android.com/security/keystore/
[Ref.- 622]	"BoringSSL". Google. URL: https://boringssl.googlesource.com/boringssl/ & https://github.com/google/boringssl URL: https://www.imperialviolet.org/2015/10/17/boringssl.html URL: https://developer.android.com/about/versions/marshmallow/android-6.0-changes.html?#boringSSL
[Ref.- 623]	"Controlar los permisos de una aplicación en Android 6.0 y versiones superiores". Ayuda de Google Play. URL: https://support.google.com/googleplay/answer/6270602
[Ref.- 624]	"Cómo activar o desactivar tu feed". Google. URL: https://support.google.com/websearch/answer/2824784?hl=es-419&co=GENIE.Platform=Android
[Ref.- 625]	"Usar Mi tablón en la aplicación de Google". Google. URL: https://support.google.com/websearch/answer/2819496?hl=es
[Ref.- 626]	"Personalizar el Tablón de la aplicación de Google". Google. URL: https://support.google.com/websearch/answer/6237870?&co=GENIE.Platform%3DAndroid
[Ref.- 627]	"Requesting Permissions". Google developers. URL: https://developer.android.com/guide/topics/permissions/requesting.html#normal-dangerous
[Ref.- 628]	"Lock screen notifications". Android developers. URL: https://developer.android.com/guide/topics/ui/notifiers/notifications.html#lockscreenNotification

Referencia	Título, autor y ubicación
[Ref.- 629]	"Keystore redesign in Android M". Nelenkov. June 2015. URL: https://nelenkov.blogspot.com.es/2015/06/keystore-redesign-in-android-m.html
[Ref.- 630]	"Android Keystore System". Android developers. URL: https://developer.android.com/training/articles/keystore.html
[Ref.- 631]	GateKeeper. "Android Source". URL: https://source.android.com/security/authentication/gatekeeper
[Ref.- 632]	"Bluetooth Services". Android Source. URL: https://source.android.com/devices/bluetooth/services
[Ref.- 633]	"Find people, things, & places in your photos". Google. URL: https://support.google.com/photos/answer/6128838
[Ref.- 634]	"Back Up User Data with Auto Backup". Android Developers. URL: https://developer.android.com/guide/topics/data/autobackup.html
[Ref.- 635]	"Auto Backup for Apps made simple". Android developers blog. URL: https://android-developers.googleblog.com/2015/07/auto-backup-for-apps-made-simple.html

La siguiente tabla muestra las fuentes de información a las que se hace referencia a lo largo de la presente guía relacionadas específicamente con la versión 7.x (Nougat) de Android:

Referencia	Título, autor y ubicación
[Ref.- 700]	"Android 7.0 Nougat". Android. URL: https://www.android.com/versions/nougat-7-0/
[Ref.- 701]	"Android 7.0 Nougat". Android Developers. URL: https://developer.android.com/about/versions/nougat/index.html
[Ref.- 702]	"Android 7.0 for Developers". Android Developers. URL: https://developer.android.com/about/versions/nougat/android-7.0.html
[Ref.- 703]	"Android 7.0 Behavior Changes". Android Developers. URL: https://developer.android.com/about/versions/nougat/android-7.0-changes.html
[Ref.- 704]	"Pixel y Pixel XL". Made by Google. October 2016. URL: https://madeby.google.com/phone/
[Ref.- 705]	"Six years of Nexus: A Google Phone History". Android Police. September 2016. URL: https://www.youtube.com/watch?v=7_tAJIjm6xA
[Ref.- 706]	"Keeping Android safe: Security enhancements in Nougat". Android Developers Blog. Sep 2016. URL: http://android-developers.blogspot.com.es/2016/09/security-enhancements-in-nougat.html
[Ref.- 707]	"Hardening the media stack". Android Developers Blog. May 2016. URL: http://android-developers.blogspot.com/2016/05/hardening-media-stack.html
[Ref.- 708]	Seccomp. WikiPedia. URL: https://en.wikipedia.org/wiki/Seccomp
[Ref.- 709]	"Security "Crypto" provider deprecated in Android N". Android Developers Blog. June 2016. URL: https://android-developers.blogspot.com.es/2016/06/security-crypto-provider-deprecated-in.html
[Ref.- 710]	"Improving Stability with Private C/C++ Symbol Restrictions in Android N". Android Developers Blog. June 2016. URL: https://android-developers.blogspot.com.es/2016/06/improving-stability-with-private-cc.html
[Ref.- 711]	"Changes to Trusted Certificate Authorities in Android Nougat". Android Developers Blog. July 2016. URL: https://android-developers.blogspot.com.es/2016/07/changes-to-trusted-certificate.html
[Ref.- 712]	"APK Signature Scheme v2". Android. URL: https://source.android.com/security/apksigning/v2.html
[Ref.- 713]	Android Security Center. Google. November 2016. URL: https://www.android.com/security-center/

Referencia	Título, autor y ubicación
[Ref.- 714]	"The Google Android Security Team's Classications for Potentially Harmful Applications". Android security Center. April 2016. URL: https://static.googleusercontent.com/media/source.android.com/en//security/reports/Google_Android_Security_PHA_classifications.pdf
[Ref.- 715]	"File System/Autoupdate". The Chromium projects. URL: https://www.chromium.org/chromium-os/chromiumos-design-docs/filesystem-autoupdate
[Ref.- 716]	"Stagefright (bug)". Wikipedia. URL: https://en.wikipedia.org/wiki/Stagefright_(bug)
[Ref.- 717]	"How we keep harmful apps out of Google Play and keep your Android device safe". Android security Center. February 2016. URL: https://static.googleusercontent.com/media/source.android.com/en//security/reports/Android_WhitePaper_Final_02092016.pdf
[Ref.- 718]	"Android 7.1, (N) Compatibility Definition Document - 7.3.10. Fingerprint Sensor". Google. https://source.android.com/compatibility/7.1/android-7.1-cdd
[Ref.- 719]	"Bloquear o desbloquear un número de teléfono". Google. URL: https://support.google.com/nexus/answer/6325463
[Ref.- 720]	"Utilizar el ID de llamada y la protección contra spam". Google. URL: https://support.google.com/nexus/answer/3459196?hl=es
[Ref.- 721]	"Factory Images and Full OTA Images for Android 7.0". XDA Developers. https://www.xda-developers.com/factory-images-and-full-ota-images-for-android-7-0-nougat-for-nexus-going-live-updated-with-nexus-6p-links/ "7.1.2 OTA and device Images now available". XDA Developers. https://forum.xda-developers.com/pixel-xl/help/7-1-2-ota-device-images-available-t3583895
[Ref.- 722]	"Protecting Android with more Linux kernel defenses". Android Developers Blog. July 2016. URL: http://android-developers.blogspot.com/2016/07/protecting-android-with-more-linux.html
[Ref.- 723]	"Strictly Enforced Verified Boot with Error Correction". Android Developers Blog. July 2016. URL: http://android-developers.blogspot.com/2016/07/strictly-enforced-verified-boot-with.html
[Ref.- 724]	"Strict Mode". Android Developers. URL: https://developer.android.com/reference/android/os/StrictMode.html
[Ref.- 725]	"Partition selection (slots)". Android Source. URL: https://source.android.com/devices/tech/ota/ab/#slots
[Ref.- 726]	"A/B (Seamless) System Updates". Android Source. URL: https://source.android.com/devices/tech/ota/ab/
[Ref.- 727]	"Implementing dm-verity". Android Source. URL: https://source.android.com/security/verifiedboot/dm-verity
[Ref.- 728]	"Verified Boot". The Chromium projects. URL: http://www.chromium.org/chromium-os/chromiumos-design-docs/verified-boot
[Ref.- 729]	"Build a device policy controller". Android developers. URL: https://developer.android.com/work/dpc/build-dpc.html
[Ref.- 730]	"Android 7.0 Behavior Changes - Android for work". Android developers. URL: https://developer.android.com/about/versions/nougat/android-7.0-changes.html#afw
[Ref.- 731]	"Work profile". Android EMM Developers. URL: https://developers.google.com/android/work/requirements/work-profile
[Ref.- 732]	"Work profile security challenge". Android developers. URL: https://developer.android.com/work/dpc/security.html#work_profile_security_challenge
[Ref.- 733]	"Here's a list of Android devices that support Seamless Updates". XDA-Developers. URL: https://www.xda-developers.com/list-android-devices-seamless-updates/
[Ref.- 734]	"File-Based Encryption". Android Source. URL: https://source.android.com/security/encryption/file-based
[Ref.- 735]	"Supporting Direct Boot". Android developers. https://developer.android.com/training/articles/direct-boot.html
[Ref.- 736]	"Security-Enhanced Linux in Android". Android Source. URL: https://source.android.com/security/selinux/device-policy

Referencia	Título, autor y ubicación
[Ref.- 737]	"SELinux concepts". Android Source. URL: https://source.android.com/security/selinux/concepts
[Ref.- 738]	"Nexus Security Bulletin - March 2016". Android Security. URL: https://source.android.com/security/bulletin/2016-03-01#elevation_of_privilege_vulnerability_in_mediatek_wi-fi_kernel_driver
[Ref.- 739]	"ioctl command whitelisting in SELinux". Jeff Vander Stoep. URL: http://kernsec.org/files/lss2015/vanderstoep.pdf
[Ref.- 740]	"Protecting Android with more Linux kernel defenses". Android Developers Blog. URL: https://android-developers.googleblog.com/2016/07/protecting-android-with-more-linux.html
[Ref.- 741]	"Protecting Android with more Linux kernel defenses". Android Developers Blog. URL: https://android-developers.googleblog.com/2016/07/protecting-android-with-more-linux.html
[Ref.- 742]	"How does Android save your fingerprints?". Android Central. URL: https://www.androidcentral.com/how-does-android-save-your-fingerprints
[Ref.- 743]	"Trusty API Reference". Android Source. URL: https://source.android.com/security/trusty/trusty-ref
[Ref.- 744]	"[PSA - Update] Google breaks their silence and gives an Official reason for the Removal of NFC Smart Unlock on Android". Reddit. URL: https://www.reddit.com/r/Android/comments/73ejrk/psa_update_google_breaks_their_silence_and_gives/
[Ref.- 745]	"Key Generator". Android developers. URL: https://developer.android.com/training/articles/keystore?hl=es-419#SupportedKeyGenerators
[Ref.- 746]	"Add protection against LE scanning abuse". Android Open Source Project. May 2016. URL: https://android-review.googlesource.com/c/platform/packages/apps/Bluetooth/+/215844
[Ref.- 747]	"Network security configuration". Android Developers. URL: https://developer.android.com/training/articles/security-config
[Ref.- 748]	"Secure boot and image authentication in mobile tech". Qualcomm. January 2017. URL: https://www.qualcomm.com/news/onq/2017/01/17/secure-boot-and-image-authentication-mobile-tech
[Ref.- 749]	"Conectarse automáticamente a redes Wi‑Fi abiertas". Ayuda de Nexus. Google. URL: https://support.google.com/nexus/answer/6327199?hl=es
[Ref.- 750]	"Project Fi". Google. URL: https://fi.google.com/about/
[Ref.- 751]	"Utilizar Nearby para interactuar con lo que te rodea". Ayuda de cuenta de Google. URL: https://support.google.com/accounts/answer/6260286?hl=es
[Ref.- 752]	"Obtener información sobre lo que aparece en la pantalla". Ayuda de Google. URL: https://support.google.com/assistant/answer/7393909
[Ref.- 753]	"Gestionar la actividad de voz y audio de Google". Ayuda de Búsqueda de Google. URL: https://support.google.com/websearch/answer/6030020
[Ref.- 754]	"Configurar Voice Match en Google Home". Ayuda de Google Home. URL: https://support.google.com/googlehome/answer/7323910?hl=es
[Ref.- 755]	"Bloquear resultados con contenido explícito en Google mediante Búsqueda Segura ". Ayuda de Google. URL: https://support.google.com/websearch/answer/510?hl=es