Informe de Amenazas CCN-CERT IA-28/15

Medidas de Seguridad en Telefonía Móvil

Octubre de 2015

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

ÍNDICE

1. SOBRE CCN-CERT

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad.

De acuerdo a todas ellas, el CCN-CERT tiene responsabilidad en ciberataques sobre **sistemas clasificados** y sobre sistemas de las **Administraciones Públicas** y de **empresas y organizaciones de interés estratégico** para el país. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

2. INTRODUCCIÓN

Este documento recoge un compendio de las medidas de seguridad más relevantes incluidas en las siguientes guías CCN-STIC:

- CCN-STIC 450 Seguridad en dispositivos móviles
- CCN-STIC 453A Seguridad en Android 2.x
- CCN-STIC 453B Seguridad en Android 4.x
- CCN-STIC 454 Seguridad en iPad
- CCN-STIC 455 Seguridad en iPhone

Atendiendo a varios criterios:

- Seguridad en la pantalla de bloqueo
- Seguridad en las comunicaciones
- Seguridad en el software
- Seguridad en el mantenimiento

3. IOS

Los siguientes apartados recogen las medidas de seguridad más relevantes para dispositivos móviles con sistema operativo iOS.

3.1 PANTALLA DE DESBLOQUEO

Es necesario restringir al máximo las acciones que se puedan realizar con acceso físico al teléfono, de modo que únicamente el dueño del mismo sea capaz de usarlo.

3.1.1 ESTABLECER PIN PARA TARJETA SIM

Establecer un PIN en la tarjeta SIM nos ayudará a restringir el acceso a las capacidades telefónicas del dispositivo (llamadas, mensajería SMS y MMS, y uso de datos a través de la red móvil).

Los dispositivos móviles iOS permiten forzar la utilización de un PIN para la tarjeta SIM, así como fijar o modificar el PIN asociado a la tarjeta SIM (opción "**Cambiar PIN**"), a través del menú "**Ajustes – Teléfono – PIN de la SIM**":

Ilustración 1. Cambio de PIN en iOS

Ilustración 2. Cambio de PIN en iOS

Se recomienda, por tanto, modificar el valor por defecto del PIN empleando un valor o secuencia de números que no sea fácilmente adivinable, es decir, excluyendo valores típicos como 0000, 1111, 1234 ó la fecha de cumpleaños del dueño del dispositivo, y empleando 8 dígitos:

Ilustración 3. Cambio de PIN en iOS

Ilustración 4. Cambio de PIN en iOS

3.1.2 ESTABLECER CÓDIGO DE ACCESO AL DISPOSITIVO

Se recomienda que el usuario configure un código de bloqueo para acceder al dispositivo, así se evitará el acceso físico por parte de terceros al contenido del terminal (aplicaciones, imágenes, contactos, etc.).

Para establecer el código de acceso al dispositivo móvil hay que acceder a través del menú "**Ajustes – Código**":

Ilustración 5. Bloqueo con código en iOS

iOS permite establecer dos tipos de contraseña de acceso: un código simple o PIN numérico tradicional (opción "**Código simple**"), compuesto por cuatro dígitos (0-9), o una contraseña alfanumérica:

Ilustración 6. Introducir código de bloqueo en iOS

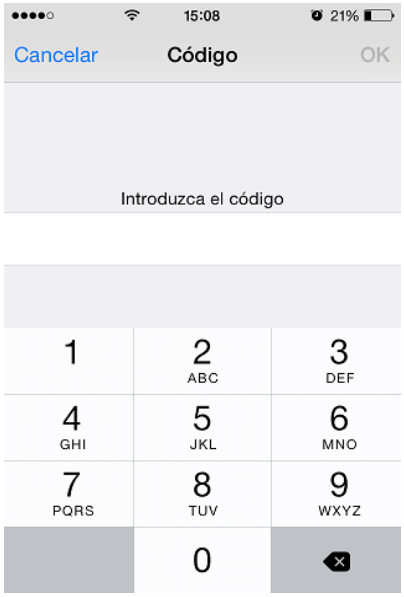

Ilustración 7. Introducir código de bloqueo en iOS

La opción de contraseña es la más segura y recomendada, debe ser configurada adecuadamente para ser realmente más segura y contener, al menos, ocho caracteres alfanuméricos (de 8 a 50 dígitos o caracteres).

3.1.3 ESTABLECER BLOQUEO AUTOMÁTICO DEL DISPOSITIVO

Establecer el bloqueo automático del terminal permitirá que tras un tiempo concreto de inactividad el dispositivo se bloquee y pida inmediatamente el código de acceso.

iOS dispone de dos ajustes para determinar cuándo es necesario introducir de nuevo el código de acceso al utilizar el dispositivo móvil. El primer ajuste determina cuándo se bloqueará (o suspenderá) la pantalla del dispositivo móvil tras un tiempo de inactividad. El segundo determina cuándo se solicitará el código de acceso una vez el dispositivo móvil ha sido bloqueado (o suspendido) por inactividad, en base al primer ajuste, o intencionadamente y de forma manual por el usuario.

Se recomienda por tanto establecer el bloqueo del dispositivo móvil tras un tiempo de inactividad (primer ajuste), en un rango entre 1 y 2 minutos.

El tiempo de bloqueo de la pantalla por inactividad se establece a través del menú "**Ajustes – General – Bloqueo automático**", siendo el periodo máximo de 5 minutos:

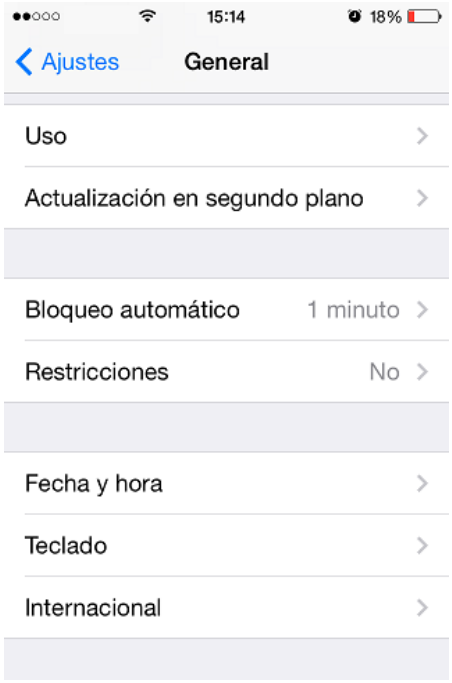

Ilustración 8. Bloqueo automático en iOS

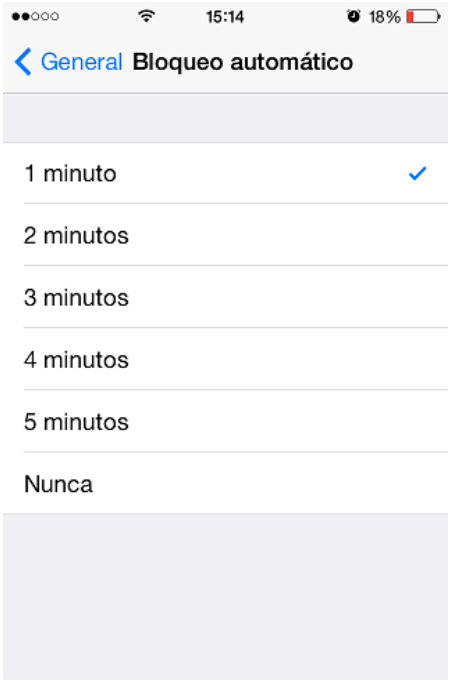

Ilustración 9. Bloqueo automático en iOS

Por otro lado, el menú "**Ajustes - Código**" dispone de la opción "**Solicitar**", que permite definir cuánto tiempo esperará el iPhone después de bloquearse para solicitar de nuevo el código de acceso que le permita volver a desbloquearse (segundo ajuste).

iOS permite elegir entre 1 minuto, 5, 15, 1 hora y 4 horas. La opción recomendada desde el punto de vista de seguridad es "**De inmediato**", de forma que tan pronto se bloquee el dispositivo móvil por falta de actividad, o por haber sido apagada su pantalla por parte del usuario manualmente, sea necesario introducir el código de acceso para volver a desbloquearlo:

Ilustración 10. Solicitud de código de bloqueo

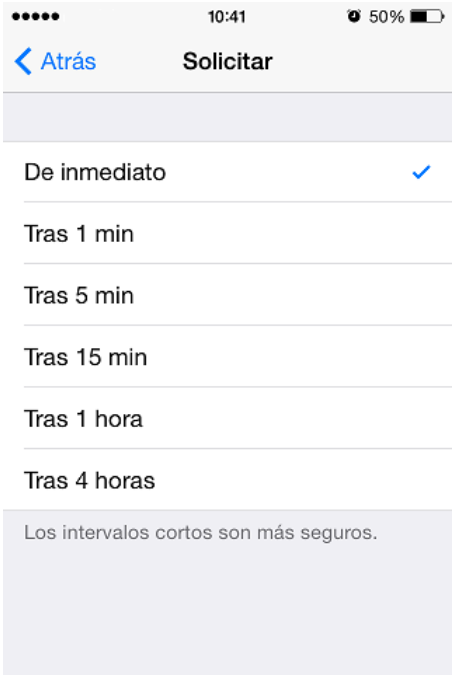

Ilustración 11. Solicitud de código de bloqueo

3.1.4 DESACTIVAR SIRI DESDE LA PANTALLA DE BLOQUEO

Siri es el sistema de reconocimiento de voz y lenguaje natural introducido por Apple que permite al usuario realizar multitud de tareas mediante comandos de voz, como por ejemplo enviar mensajes SMS, realizar llamadas de voz, crear citas en el calendario, añadir recordatorios, etc., convirtiéndose en un asistente personal electrónico.

Sin embargo, por defecto es posible usar Siri sin necesidad de desbloquear el dispositivo desde la pantalla de desbloqueo. Esto supone una grave amenaza para la privacidad. Se recomienda por tanto bloquear el uso de Siri hasta que el dispositivo haya sido desbloqueado.

Una vez que Siri ha sido habilitado, desde el menú "Ajustes - Código", bajo la sección "Permitir acceso mientras está bloqueado", es posible desactivar Siri a través de su botón de activación asociado:

Ilustración 12. Desactivar Siri

Ilustración 13. Desactivar Siri

3.1.5 DESACTIVAR EL CENTRO DE CONTROL DESDE LA PANTALLA DE BLOQUEO

El Centro de Control está accesible al desplazar hacia arriba la parte inferior de la pantalla de iOS, por defecto tanto en la pantalla de bloqueo como una vez el dispositivo móvil ha sido desbloqueado.

Desde el punto de vista de seguridad es crítico desactivar el Centro de Control si la pantalla está bloqueada, ya que en caso contrario un potencial atacante con acceso físico al dispositivo móvil podría fácilmente, por ejemplo, activar el modo avión (o activar o desactivar cualquiera de los otros interfaces de comunicaciones: Wi-Fi, Bluetooth, etc.).

Ilustración 14. Desactivar centro de control desde la pantalla de bloqueo

Para desactivar la posibilidad de acceder al Centro de Control desde la pantalla de desbloqueo del dispositivo móvil accederemos al menú "**Ajustes - Centro de control**". La pantalla asociada pertenece al Centro de Control de iOS y permite configurar tanto el acceso a éste desde la pantalla de bloqueo como desde las aplicaciones:

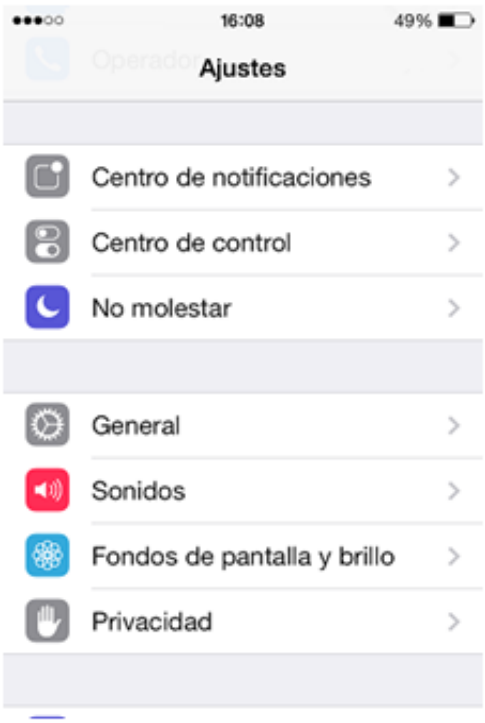

Ilustración 15. Desactivar centro de control

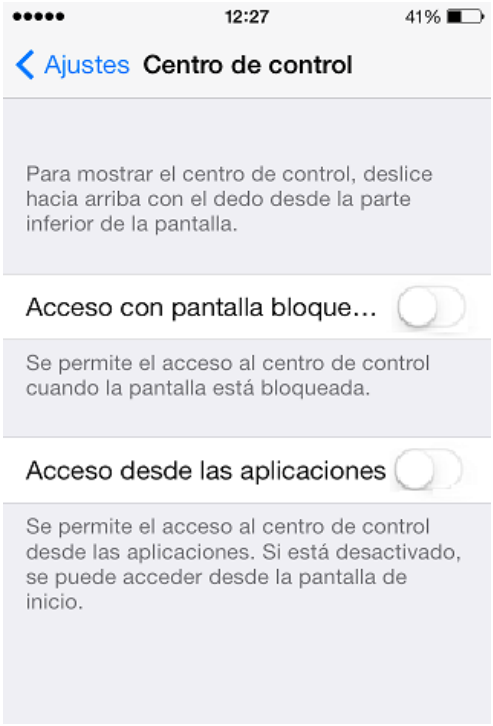

Ilustración 16. Desactivar centro de control

3.1.6 DESACTIVAR CENTRO DE NOTIFICACIONES EN LA PANTALLA DE BLOQUEO

El Centro de Notificaciones está accesible al desplazar hacia abajo la parte superior de la pantalla de iOS, por defecto tanto en la pantalla de bloqueo como una vez el dispositivo móvil ha sido desbloqueado.

Desde el punto de vista de seguridad, en el caso de gestionar información sensible, se recomienda desactivar la previsualización de notificaciones mediante el menú "**Ajustes - Centro de notificaciones**". La pantalla asociada pertenece al Centro de Notificaciones de iOS y permite la gestión centralizada de mensajes así como establecer qué aplicaciones pueden generar qué tipo de notificaciones:

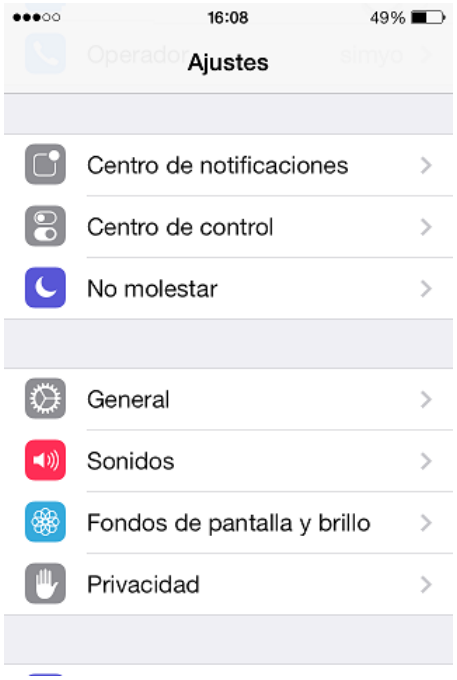

Ilustración 17. Desactivar notificaciones desde la pantalla de bloqueo en iOS

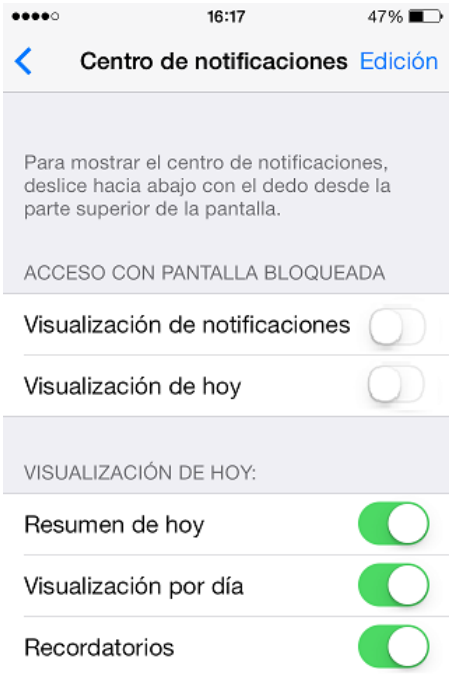

Ilustración 18. Desactivar notificaciones desde la pantalla de bloqueo en iOS

Aunque esta configuración afecta a la funcionalidad del dispositivo móvil, evita que un tercero no autorizado pueda acceder a todos los detalles de las notificaciones existentes con sólo disponer de acceso temporal al dispositivo móvil, incluso por un breve espacio de tiempo.

3.2 COMUNICACIONES

El dispositivo móvil dispone de diferentes interfaces de comunicación, tanto físicas (a través de la conexión por cable a un ordenador) como por radiofrecuencia (Wifi, 2G/3G/4G, Bluetooth, GPS). Es necesario configurar de manera segura cada una de estas conexiones para que la exposición de nuestra privacidad sea la menor posible.

3.2.1 DESACTIVAR LOCALIZACIÓN

Los servicios de localización de iOS permiten conocer la ubicación geográfica aproximada del dispositivo móvil, y por tanto del usuario, sin disponer de señal GPS, y hacer uso de esa información en distintas aplicaciones y servicios web.

Desde el menú "**Ajustes - Privacidad - Localización**", y en concreto a través del botón "**Localización**", es posible habilitar los servicios de localización del dispositivo móvil, tanto mediante el módulo GPS (en caso de disponer de uno), como mediante redes Wi-Fi y torres de telefonía móvil, no disponiéndose de opciones directas para habilitar o desactivar las diferentes fuentes de información de localización de forma independiente:

Ilustración 19. Desactivar localización en iOS

Se recomienda desactivar la localización del dispositivo.

3.2.2 DESACTIVAR LOCALIZACIÓN EN SERVICIOS DEL SISTEMA

Desde el menú "**Ajustes - Privacidad - Localización**", y en concreto a través de la opción "**Servicios del sistema**", es posible configurar qué servicios de iOS (Búsqueda de red móvil, Calibración de la brújula, Zona horaria, etc.) dispondrán de acceso a los servicios de localización. Por defecto, todos los servicios del sistema disponen de estos permisos:

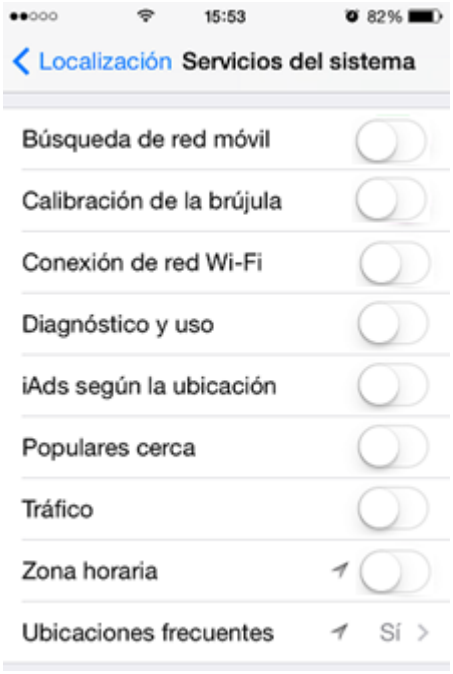

Ilustración 20. Desactivar localización en servicios del sistema

De manera general se recomienda desactivar el acceso a los servicios de localización por parte de los servicios de sistema salvo que sea necesario hacer uso de alguno de ellos específicamente y de manera puntual como parte de la funcionalidad asociada al uso del dispositivo móvil.

3.2.3 DESACTIVAR UBICACIONES FRECUENTES

Bajo la sección "Ubicaciones frecuentes" del menú "Ajustes - Privacidad - Localización - Servicios del sistema" se dispone de información de los lugares que son visitados frecuentemente por el dispositivo. Esta información es almacenada en el dispositivo móvil, y se emplea para proporcionar información útil en base a la ubicación, y es transmitida a Apple de manera anónima para la mejora de la aplicación de Mapas:

Ilustración 21. Desactivar ubicaciones frecuentes en iOS

Esta funcionalidad puede ser habilitada o desactivada a través de la opción "**Ubicaciones frecuentes**" disponible desde el menú "**Ajustes - Privacidad - Localización - Servicios del sistema - Ubicaciones frecuentes**" (situada en la parte inferior) y el historial puede ser eliminado mediante la opción "**Borrar historial**":

Ilustración 22. Desactivar ubicaciones frecuentes en iOS

Se recomienda desactivar esta funcionalidad desde el punto de vista de la privacidad para evitar que Apple obtenga información sobre las ubicaciones frecuentes, y realice la correlación de éstas con la dirección postal asociada al Apple ID del usuario para la mejora de los Mapas.

3.2.4 DESACTIVAR INTERFAZ BLUETOOTH

La principal recomendación de seguridad asociada a las comunicaciones Bluetooth en dispositivos móviles es no activar el interfaz inalámbrico Bluetooth salvo en el caso en el que se esté haciendo uso del mismo, evitando así la posibilidad de ataques sobre el hardware del interfaz, el driver o la pila de comunicaciones Bluetooth, incluyendo los perfiles Bluetooth disponibles.

El interfaz inalámbrico Bluetooth puede ser desactivado en iOS, situación por defecto, a través del menú "**Ajustes - Bluetooth**", mediante el botón "**Bluetooth**":

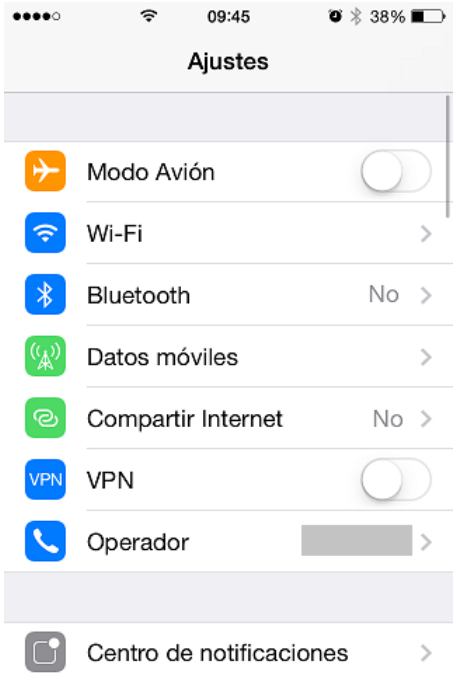

Ilustración 23. Desactivar bluetooth en iOS

Ilustración 24. Desactivar bluetooth en iOS

3.2.5 DESACTIVAR INTERFAZ WI-FI

De igual modo que con el interfaz Bluetooth, la principal recomendación de seguridad asociada a las comunicaciones Wi-Fi en dispositivos móviles es no activar el interfaz inalámbrico Wi-Fi salvo en el caso en el que se esté haciendo uso del mismo, evitando así la posibilidad de ataques sobre el hardware del interfaz, el driver o la pila de comunicaciones Wi-Fi.

El interfaz inalámbrico Wi-Fi puede ser desactivado en iOS a través del menú "Ajustes – Wi-Fi", mediante el botón "Wi-Fi":

Ilustración 25. Desactivar wifi en iOS

3.2.6 CONEXIÓN MEDIANTE USB

Hasta la versión 7 de iOS existía la posibilidad de instalar aplicaciones dañinas sin la intervención del usuario, y extraer información del dispositivo móvil, a través de la utilización de un cargador de electricidad dañino o de la conexión por USB a un equipo.

Apple solucionó el problema en iOS 7 notificando al usuario de la existencia de una conexión de datos al conectar su dispositivo a un periférico externo:

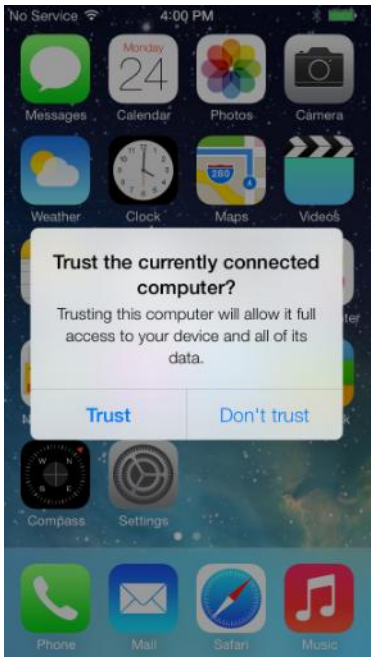

Ilustración 26. Conexión USB en iOS

En todo caso se recomienda conectar por USB nuestro dispositivo iOS a aquellos periféricos que sean de confianza, como el PC doméstico, y nunca hacerlo con equipos de la calle o públicos por el riesgo que podría conllevar.

3.3 SOFTWARE Y APLICACIONES

El potencial de un dispositivo móvil está directamente relacionado con la cantidad y calidad del software que sea posible instalar en el mismo. En este sentido iOS posee un *market* muy grande de aplicaciones, la AppStore, desde la que será posible descargar e instalar un sinfín de programas, que pueden suponer una amenaza contra nuestra privacidad y seguridad.

Es importante destacar que la AppStore no ofrece ninguna garantía de que la aplicación descargada no suponga un riesgo de seguridad para nuestro dispositivo. La recomendación general cuando se instala una aplicación es restringir los permisos de la misma al máximo.

3.3.1 JAILBREAK

El proceso de jailbreak permite al usuario disponer de control completo sobre el dispositivo móvil y acceder al mismo como "root", o usuario privilegiado, eliminando así los controles y/o restricciones establecidos por la plataforma iOS. Jailbreak otorga la posibilidad de instalar aplicaciones, modificaciones y componentes del sistema no proporcionados a través de la tienda oficial AppStore.

Los dispositivos móviles iOS jailbroken ignoran el modelo de seguridad impuesto por Apple, ya que todas las aplicaciones que sean instaladas dispondrán de los máximos privilegios en el dispositivo ("root"), exponiendo a los usuarios a código dañino que podría tomar control completo del terminal.

Se recomienda no realizar el proceso de jailbreak sobre el dispositivo.

Ilustración 27. Jailbreak

3.3.2 RESTRICCIÓN DE PERMISOS EN APLICACIONES

Desde el punto de vista de la seguridad es importante prestar atención a los permisos requeridos por cada aplicación, ya que, por ejemplo, aquellas que dispongan de acceso al micrófono podrán escuchar todo el sonido y audio existente alrededor del dispositivo móvil, grabarlo y/o enviarlo a través de Internet.

El panel de control de privacidad permite restringir el acceso de las aplicaciones instaladas a los servicios de localización, bluetooth, agenda de contactos, calendarios, recordatorios, fotos, micrófono y cámara, entre otros.

El panel de control de la privacidad está disponible a través de "Ajustes - Privacidad":

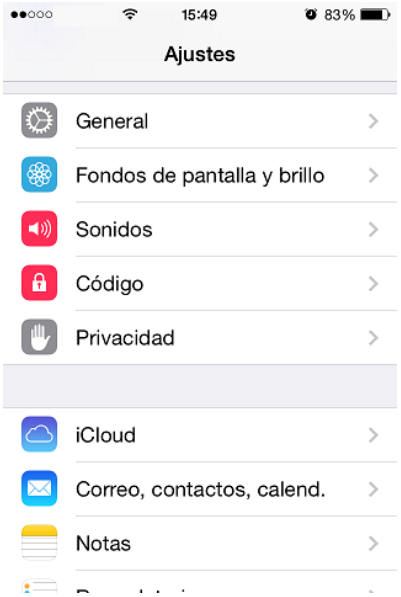

Ilustración 28. Permisos de aplicaciones en iOS

Ilustración 29. Permisos de aplicaciones en iOS

3.3.3 LIMITAR SEGUIMIENTO DE PUBLICIDAD

Desde la versión 7 de iOS se permite limitar el seguimiento del usuario por parte de anunciantes y agencias de publicidad en base a un identificador temporal. Si la opción "Ajustes - Privacidad - Publicidad - Limitar seguimiento" está activa (opción recomendada desde el punto de vista de la privacidad), se evita recibir anuncios de iAd:

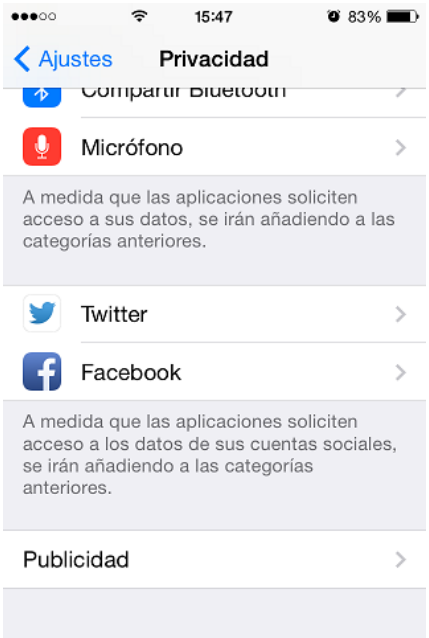

Ilustración 30. Seguimiento de publicidad

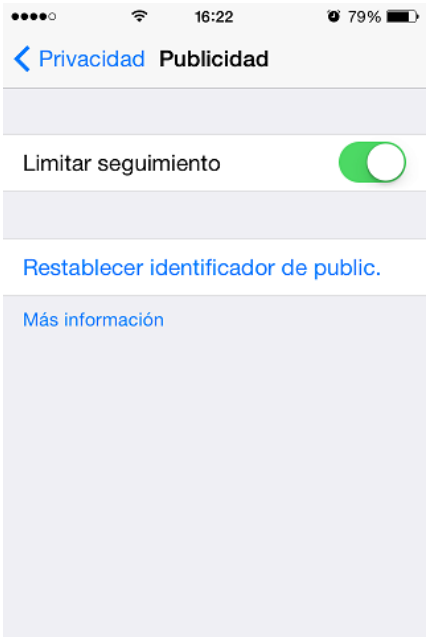

Ilustración 31. Seguimiento de publicidad

Adicionalmente, desde la sección de publicidad restablecer el identificador de publicidad empleado para ofrecer anuncios personalizados según las preferencias o intereses del usuario, generando un nuevo valor aleatorio y temporal, no asociado al dispositivo móvil, al usuario, o al valor existente previamente:

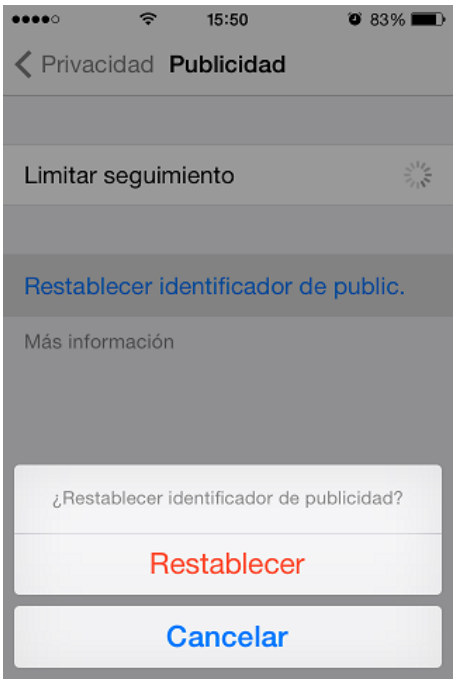

Ilustración 32. Limitar seguimiento de publicidad

Desde el punto de vista de la privacidad, se recomienda restablecer periódicamente este identificador para que terceros no puedan realizar un seguimiento detallado del usuario a través de las redes de anuncios y publicidad (iAd).

3.3.4 ACTUALIZACIÓN DE APLICACIONES

Una vez que el dispositivo móvil establece conexión con la AppStore, iOS comprueba automáticamente la última versión disponible de las aplicaciones instaladas en el dispositivo móvil. El menú "AppStore - Actualizaciones" permite disponer de acceso a las nuevas versiones de las aplicaciones que ya están instaladas en el dispositivo móvil:

Ilustración 33. Actualización de aplicaciones

Se recomienda mantener las aplicaciones instaladas en el dispositivo actualizadas a la última versión disponible, ya que éstas pueden corregir posibles fallos de seguridad.

Además iOS permite al usuario configurar el dispositivo para que lleve a cabo actualizaciones automáticamente cuando se identifique que existe una nueva versión de una aplicación, sin que el usuario tenga que intervenir en el proceso de actualización. Para ello desde el menú "**Ajustes - iTunes Store y AppStore**" accediendo a "**Descargas automáticas - Actualizaciones**" habilitaremos la descarga automática de actualizaciones:

Ilustración 34. Actualizaciones automáticas

3.4 MANTENIMIENTO

Además de todas las medidas de seguridad descritas anteriormente, es importante realizar un correcto mantenimiento del dispositivo. A continuación se describen algunas recomendaciones complementarias para nuestro dispositivo iOS.

3.4.1 REALIZAR COPIAS DE SEGURIDAD PERIÓDICAS

Para prevenir cualquier tipo de pérdida de información en nuestro dispositivo Apple proporciona dos alternativas para realizar una copia de seguridad: iTunes e iCloud.

iTunes puede llevar a cabo una copia de seguridad del dispositivo móvil durante el proceso de sincronización de datos. Adicionalmente, el usuario puede forzar la realización de una copia de seguridad tras conectar el dispositivo a iTunes seleccionando el dispositivo móvil de la lista de dispositivos de iTunes, mediante la opción "**Copia**" ("**Back Up**"; disponible a través del botón derecho del ratón):

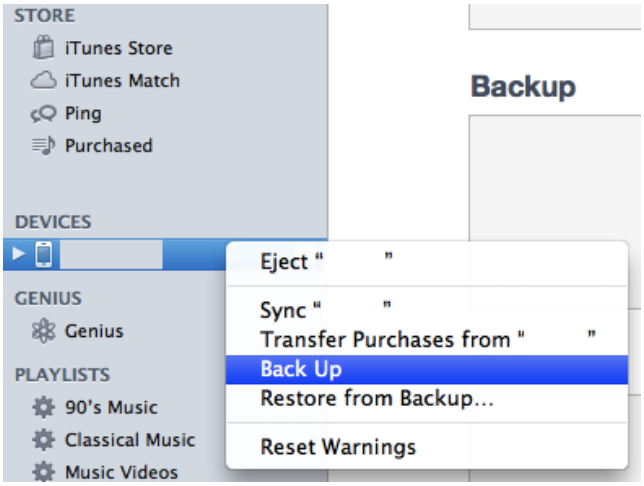

Ilustración 35. Backups en iOS

El cifrado de las copias de seguridad puede ser habilitado desde la pantalla de resumen del dispositivo móvil en iTunes, mediante la opción "**Cifrar copia de seguridad local**" (desactivada por defecto; en inglés en la imagen inferior "**Encrypt local backup**"):

Ilustración 36. Cifrado de backup

Ilustración 37. Cifrado de backup

Adicionalmente es posible realizar copias de seguridad a través del servicio iCloud, que permite realizar copias de seguridad de los datos "en la nube". Por cuestiones de privacidad se recomienda no utilizar iCloud, en su lugar se realizarán copias de seguridad locales desde iTunes con la opción de "Cifrar copia de seguridad local" activada y utilizando una contraseña robusta.

Para desactivar la realización automática de copias de seguridad desde iCloud accederemos a "Ajustes - iCloud - Almacenamiento y copia", desactivando la opción "Copia en iCloud":

Ilustración 38. Desactivar iCloud

Ilustración 39. Desactivar iCloud

3.4.2 ACTUALIZAR FIRMWARE

Una de las medidas de seguridad fundamentales, sino la más importante, es tener actualizado el dispositivo iOS a la última versión disponible. Apple lanza periódicamente estas actualizaciones del software del dispositivo con el fin de introducir nuevas características y parchear los fallos de seguridad que hayan sido identificados hasta esa fecha.

Cuando se disponga de una actualización, el dispositivo móvil mostrará en el icono de Ajustes un mensaje indicando que hay una actualización disponible, al igual que en la sección "Ajustes – General":

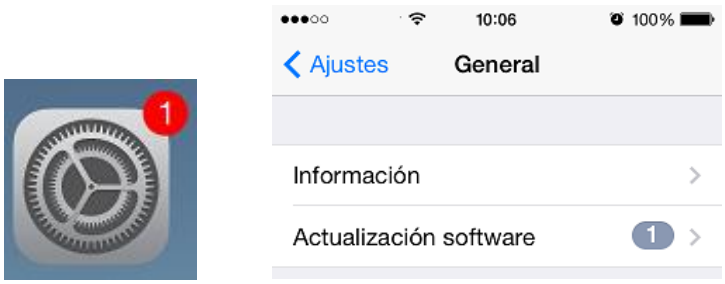

Ilustración 40. Actualizar firmware iOS

Mediante el botón "Descargar e instalar" es posible llevar a cabo la actualización de la versión de iOS en el dispositivo móvil, tras aceptar los términos y condiciones asociados:

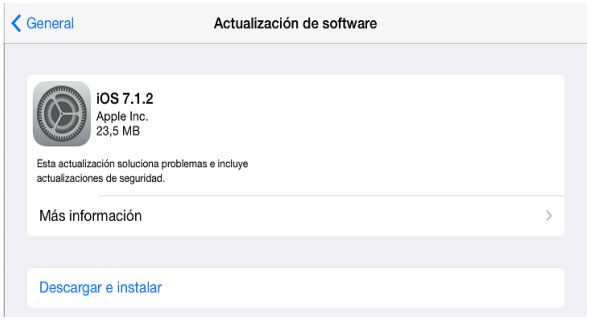

Ilustración 41. Instalar firmware iOS

Ilustración 42. Firmware de iOS actualizado

3.4.3 MANTENER ACTUALIZADO ITUNES

iTunes es el software de ordenador utilizado para comunicar el terminal iOS con el PC doméstico. Desde él se pueden realizar tanto copias de seguridad como actualizaciones de firmware, entre otras cosas. Es clave mantener este programa actualizado a su última versión, ya que vulnerabilidades en el mismo podrían ser utilizadas por un atacante para tomar el control de nuestro dispositivo iOS o robar información (imágenes, contactos, etc.).

4. ANDROID

Los siguientes apartados recogen las medidas de seguridad más relevantes para dispositivos móviles con sistema operativo Android.

4.1 PANTALLA DE DESBLOQUEO

Es necesario restringir al máximo las acciones que se puedan realizar con acceso físico al teléfono, de modo que únicamente el legítimo dueño sea capaz de usar el dispositivo.

4.1.1 ESTABLECER PIN PARA TARJETA SIM

Establecer un PIN en la tarjeta SIM nos ayudará a restringir el acceso a las capacidades telefónicas del dispositivo (llamadas, mensajería SMS y MMS, y uso de datos a través de la red móvil).

Los dispositivos móviles Android permiten forzar la utilización de un PIN para la tarjeta SIM (opción "**Bloquear tarjeta SIM**"), así como fijar o modificar el PIN asociado a la tarjeta SIM (opción "**Cambiar PIN de tarjeta SIM**"), a través del menú "**Ajustes - Seguridad [Bloqueo de tarjeta SIM] - Bloqueo de tarjeta SIM**":

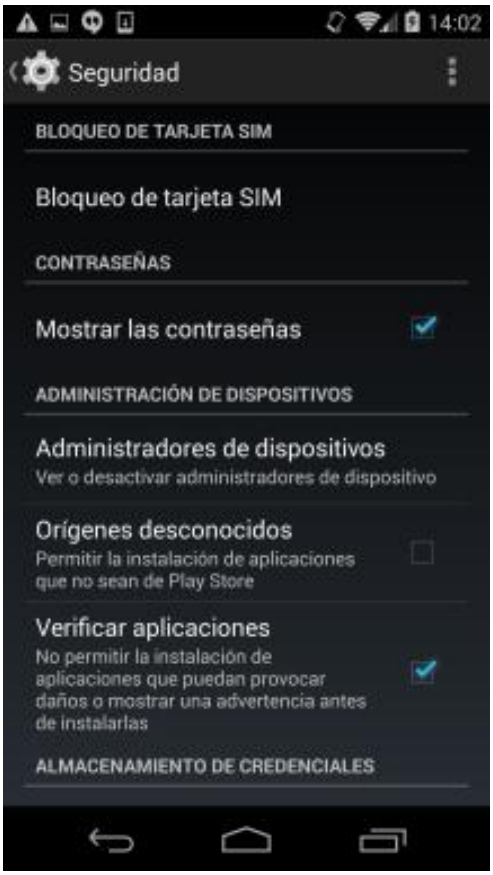

Ilustración 43. Cambiar PIN de SIM en Android

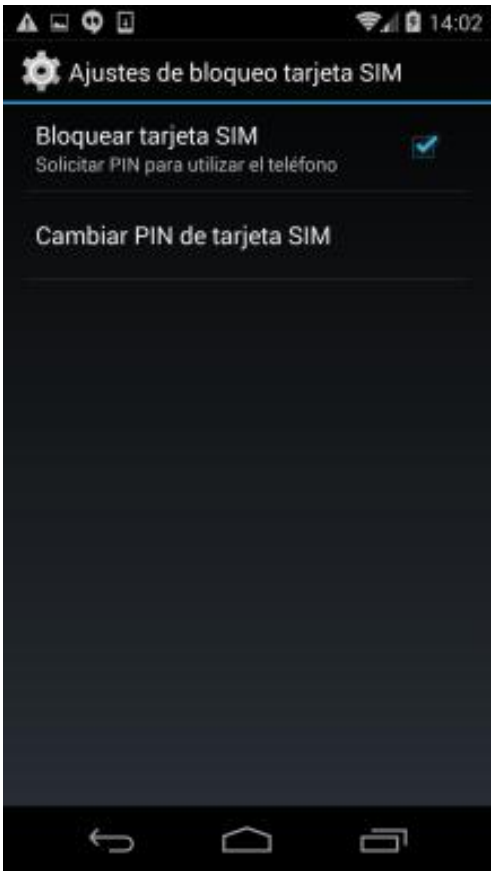

Ilustración 44. Cambiar PIN de SIM en Android

Se recomienda, por tanto, modificar el valor por defecto del PIN empleando un valor o secuencia de números que no sea fácilmente adivinable, es decir, excluyendo valores típicos como 0000, 1111, 1234 ó la fecha de cumpleaños del dueño del dispositivo, y empleando 8 dígitos:

Ilustración 45. Cambiar PIN de SIM en Android

Ilustración 46. Cambiar PIN de SIM en Android

4.1.2 ESTABLECER CÓDIGO DE ACCESO AL DISPOSITIVO

Se recomienda que el usuario configure un código de bloqueo para acceder al dispositivo, así se evitará el acceso físico por parte de terceros al contenido del terminal (aplicaciones, imágenes, contactos, etc.).

Para establecer un código de acceso al dispositivo móvil accederemos a través del menú "Ajustes [Personal] - Seguridad - Bloqueo de pantalla".

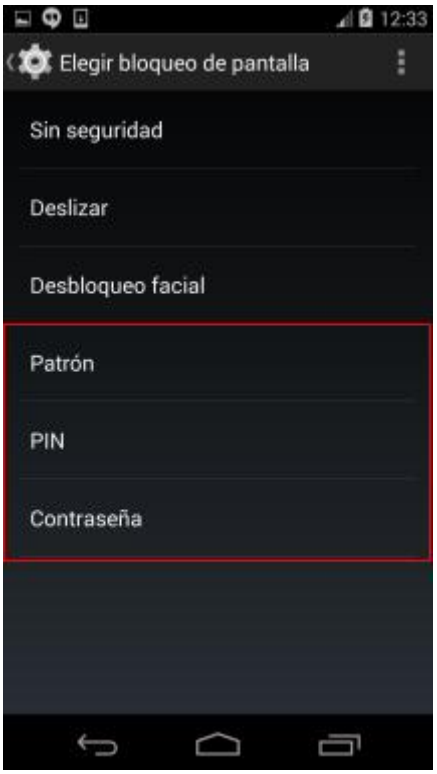

Ilustración 47. Bloqueo de pantalla en Android

A continuación se listan las opciones de bloqueo recomendadas que permite configurar Android para bloquear el acceso al dispositivo:

- **Patrón**: el número máximo de puntos posibles en el patrón de desbloqueo es de nueve, ya que no es posible repetir la selección de un mismo punto. Por tanto, se recomienda emplear patrones de desbloqueo complejos, que hagan uso de un mayor número de puntos, como por ejemplo, de 6 a 9 (y en ningún caso del número mínimo de tan sólo 4 puntos).

  Se recomienda desactivar la visibilidad del patrón durante el proceso de desbloqueo, para ello desmarcaremos la opción "**Mostrar el patrón dibujado**" (habilitada por defecto).

Ilustración 48. Desactivar dibujo de patrón

Ilustración 49. Desactivar dibujo de patrón

- **PIN**: permite establecer un PIN o código numérico tradicional, compuesto por al menos ocho dígitos (0-9) hasta 16, no desvelándose en la pantalla de desbloqueo la longitud del mismo.

Ilustración 50. Bloqueo con PIN en Android

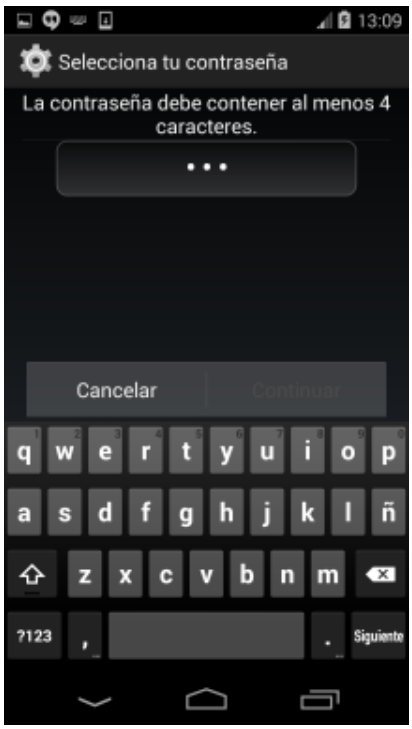

Ilustración 51. Bloqueo con PIN en Android

Android no realiza ninguna verificación de seguridad sobre el valor del PIN, permitiendo el uso de secuencias simples de dígitos, como por ejemplo 1111, 1234, la fecha de cumpleaños del dueño, etc. Por lo tanto, en caso de escoger protección de desbloqueo por PIN se recomienda utilizar uno complejo y de al menos, 8 caracteres.

- **Contraseña**: permite establecer una contraseña alfanumérica, compuesta por al menos cuatro caracteres alfanuméricos (incluyendo letras minúsculas, mayúsculas, dígitos y símbolos de puntuación). Es la opción más segura y recomendada, siempre que nuestra contraseña sea de al menos, 8 caracteres.

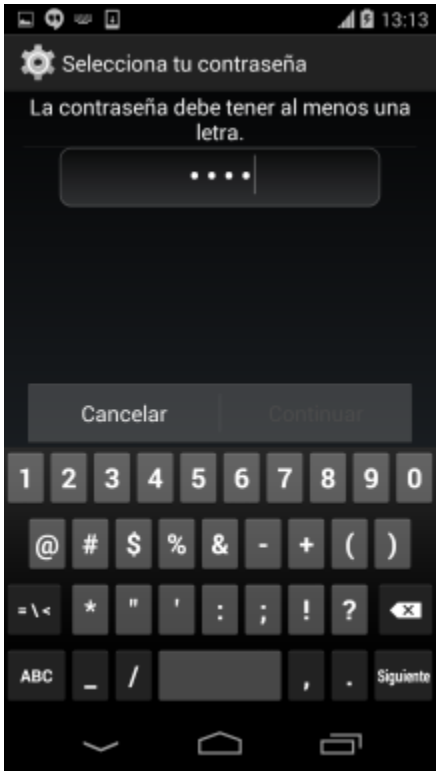

Ilustración 52. Bloqueo con contraseña en Android

Al emplear una contraseña de acceso, Android por defecto muestra los valores de los caracteres introducidos (únicamente el último dígito o carácter pulsado) mientras se escribe. Desde el punto de vista de seguridad se recomienda no habilitar el uso de contraseñas visibles, para evitar que alguien con acceso visual a la pantalla del dispositivo móvil durante el proceso de desbloqueo pueda obtener la contraseña empleada.

Para desactivar la visualización de contraseñas accederemos a la opción "**[Contraseñas] Mostrar las contraseñas**" (habilitada por defecto) y disponible desde el menú "**Ajustes [Personal] - Seguridad [Seguridad de la Pantalla]**".

Ilustración 53. Visualización de contraseñas

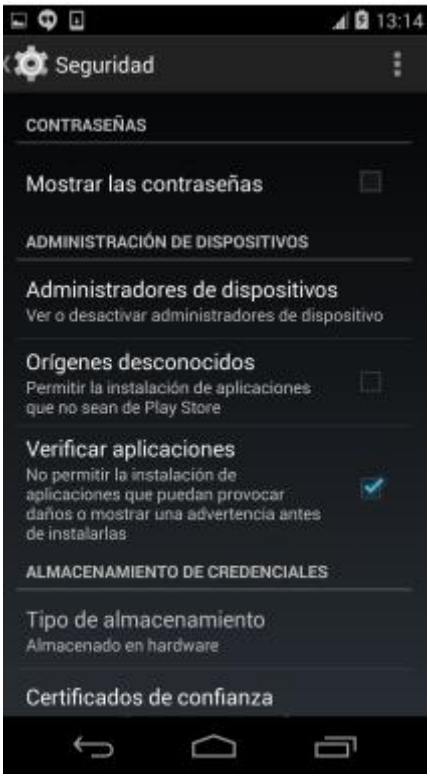

Ilustración 54. Visualización de contraseñas

4.1.3 ESTABLECER BLOQUEO AUTOMÁTICO DEL DISPOSITIVO

Establecer el bloqueo automático del terminal es fundamental, de modo que tras un tiempo concreto de inactividad el dispositivo se bloquee y pida inmediatamente el código de acceso.

Se recomienda establecer el bloqueo del dispositivo móvil tras un tiempo de inactividad, por ejemplo a 1 minuto. Por un lado, el tiempo de bloqueo de la pantalla por inactividad se establece a través del menú "Ajustes [Dispositivo] - Pantalla - Suspender después de":

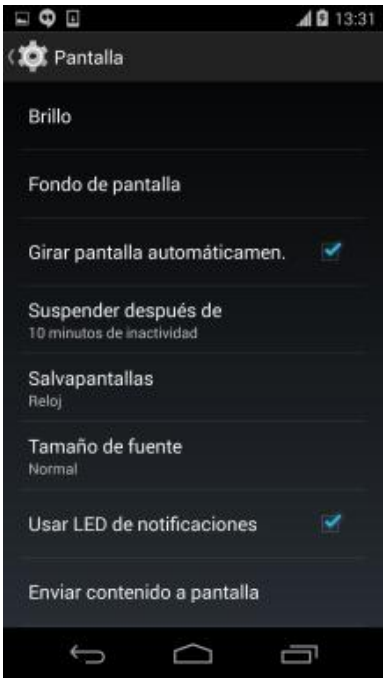

Ilustración 55. Suspender pantalla

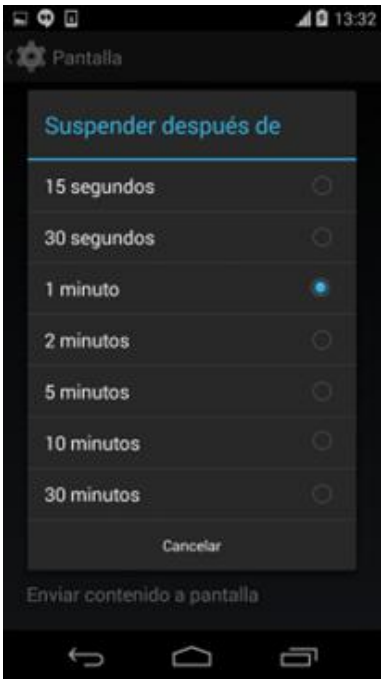

Ilustración 56. Suspender pantalla

Por otro lado, el tiempo de bloqueo de la pantalla una vez suspendida por inactividad se establece a través del menú "**Ajustes [Personal] - Seguridad [Seguridad de la Pantalla] - Bloquear automáticamente**". Se recomienda establecer "**Inmediatamente**":

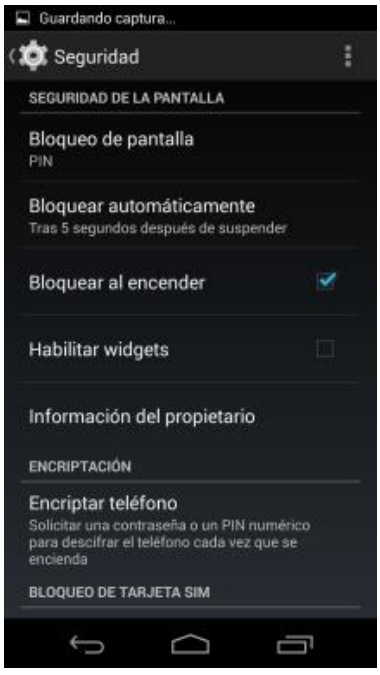

Ilustración 57. Bloqueo de pantalla en Android

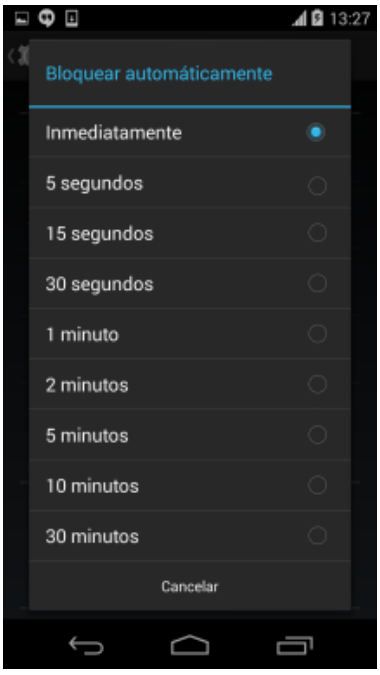

Ilustración 58. Bloqueo de pantalla en Android

4.2 COMUNICACIONES

El dispositivo móvil dispone de diferentes interfaces de comunicación, tanto físicas (a través de la conexión por cable a un ordenador) como por radiofrecuencia (Wifi, 2G/3G/4G, Bluetooth, GPS). Es necesario configurar de manera segura cada una de estas conexiones para que la exposición de nuestra privacidad sea la menor posible.

4.2.1 DESACTIVAR LOCALIZACIÓN

Los servicios de localización de Android permiten conocer la ubicación geográfica aproximada del dispositivo móvil, y por tanto del usuario, a través del módulo de GPS, o de las redes de datos (telefonía móvil y Wi-Fi).

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

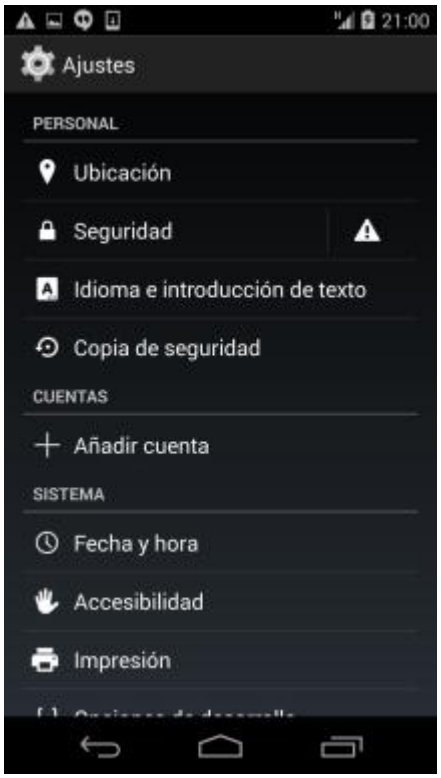

Ilustración 59. Desactivar localización Android

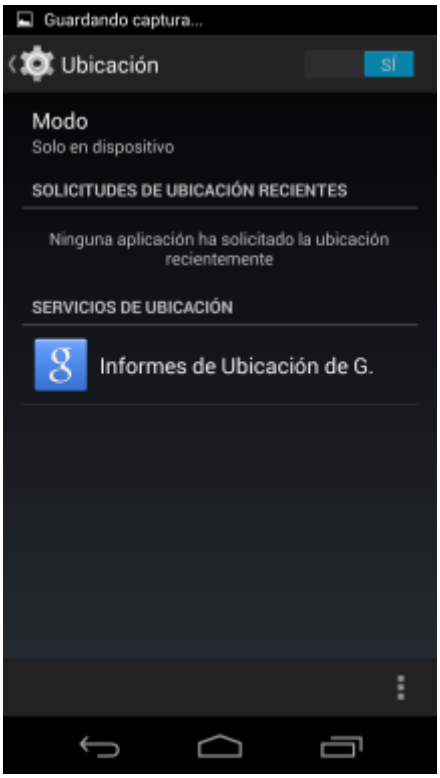

Ilustración 60. Desactivar localización Android

Android 4.4 (KitKat) proporciona un mayor control sobre los diferentes modos de localización disponibles: alta precisión, ahorro de batería o solo en dispositivo.

Ilustración 61. Determinar ubicación con GPS

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.

Para restringir el empleo de redes Wi-Fi para obtener información sobre la ubicación del dispositivo móvil hay que acceder a desde el menú "Ajustes [Conexiones Inalámbricas y Redes] - Wi-Fi - [...] - Ajustes avanzados - Buscar redes siempre" y desactivar la opción:

Ilustración 62. Desactivar búsqueda de redes

Se recomienda desactivar las capacidades de localización del dispositivo móvil salvo que se esté haciendo uso explícito de esta funcionalidad. En caso de habilitar dichas capacidades, 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.

4.2.2 DESACTIVAR SERVICIOS DE UBICACIÓN DE GOOGLE

Durante el proceso de configuración inicial del móvil, Android solicita al usuario si desea usar los servicios de ubicación de Google. Las dos opciones disponibles ("Permitir que el servicio de ubicación de Google recopile datos de ubicación anónimos…" y "Utilizar Mi ubicación para los resultados de búsqueda de Google y otros servicios…") están habilitadas por defecto.

Se recomienda desactivar ambas opciones durante el proceso inicial de instalación y configuración del dispositivo móvil.

Ilustración 63. Desactivar servicios de Google

4.2.3 HISTORIAL DE UBICACIONES E INFORMES DE UBICACIÓN

El historial de ubicaciones y los informes de ubicación permiten a Google almacenar un registro histórico de la ubicación del usuario. También permiten el envío de información de uso y diagnóstico a Google sobre el funcionamiento de los informes de ubicación, incluyendo información detallada sobre las diferentes actividades del terminal y del usuario. Desde el punto de vista de la privacidad es necesario desactivar ambas opciones.

A través del menú "Ajustes [Personal] - Ubicación", y de la sección "Servicios de Ubicación", es posible seleccionar "Informes de Ubicación de G." (Google) y acceder a los ajustes de configuración para desactivar los informes de ubicación y el historial de ubicaciones de la cuenta de usuario de Google:

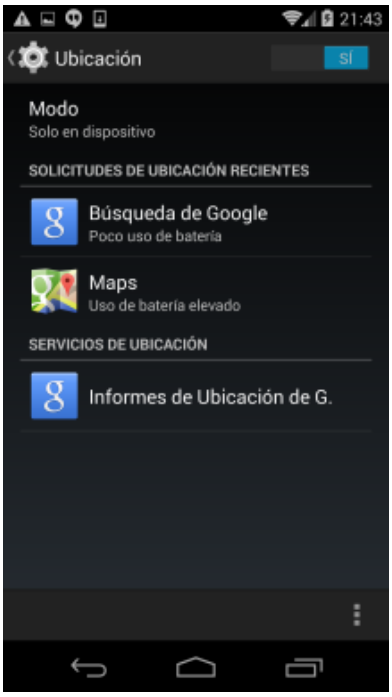

Ilustración 64. Desactivar informes de ubicación

La configuración de los informes de ubicación está disponible a través del menú mencionado previamente, la opción "**Informes de ubicación**" puede desactivarse mediante el botón "[SI | **NO**]":

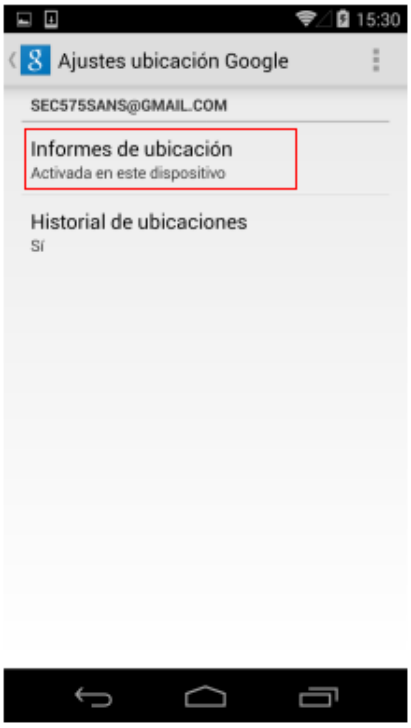

Ilustración 65. Desactivar informes de ubicación

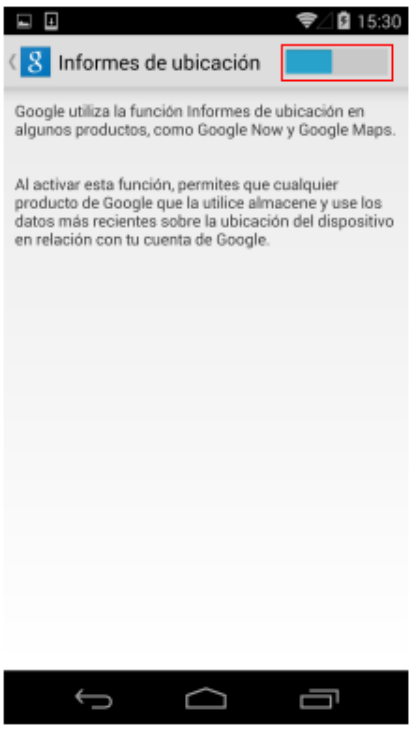

Ilustración 66. Desactivar informes de ubicación

Por otro lado, la configuración del historial de ubicaciones está disponible a través del menú mencionado previamente, la opción "Historial de ubicaciones" puede desactivarse mediante el botón "[SI | **NO**]". La pantalla asociada dispone del botón "**Eliminar Historial de Ubicaciones**" en su parte inferior para borrar los datos de ubicaciones previamente almacenados por Google:

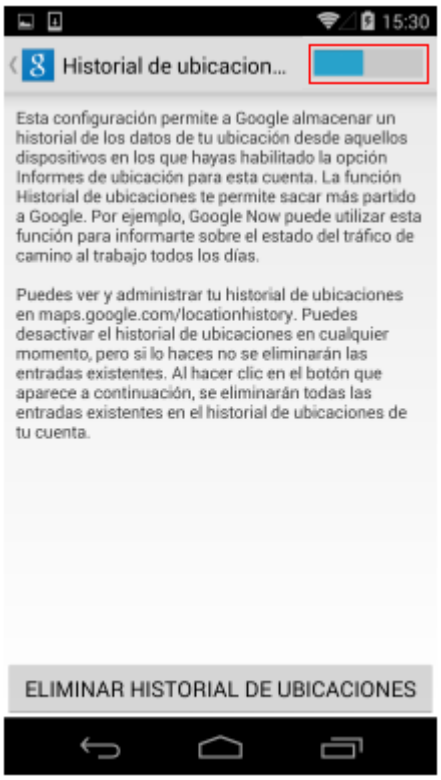

Ilustración 67. Desactivar historial de ubicación

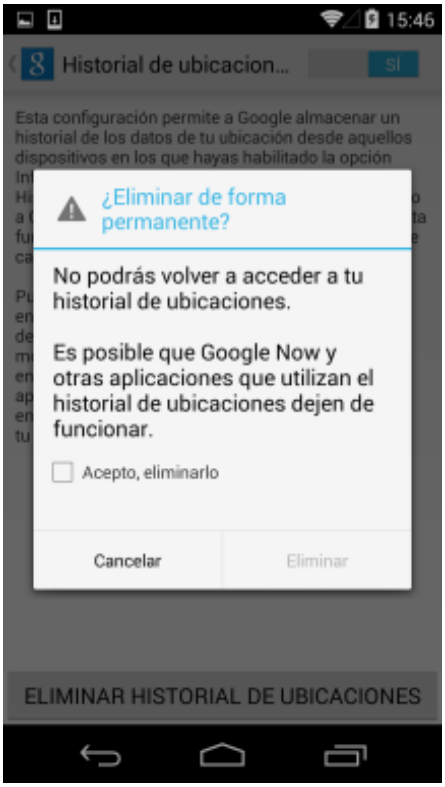

Ilustración 68. Desactivar historial de ubicación

Desde el punto de vista de seguridad, y de la privacidad el usuario, no se recomienda hacer uso de los informes de ubicación, ni del historial de ubicaciones. Adicionalmente, se recomienda borrar el historial de ubicaciones actualmente existente en la cuenta de usuario de Google.

4.2.4 DESACTIVAR INTERFAZ BLUETOOTH

La principal recomendación de seguridad asociada a las comunicaciones Bluetooth en dispositivos móviles es no activar el interfaz inalámbrico Bluetooth salvo en el caso en el que se esté haciendo uso del mismo, evitando así la posibilidad de ataques sobre el hardware del interfaz, el driver o la pila de comunicaciones Bluetooth, incluyendo los perfiles Bluetooth disponibles.

El interfaz inalámbrico Bluetooth puede ser desactivado en Android a través del menú "Ajustes [Conexiones Inalámbricas y Redes] - Bluetooth", mediante el botón "SÍ|NO" de la opción "Bluetooth".

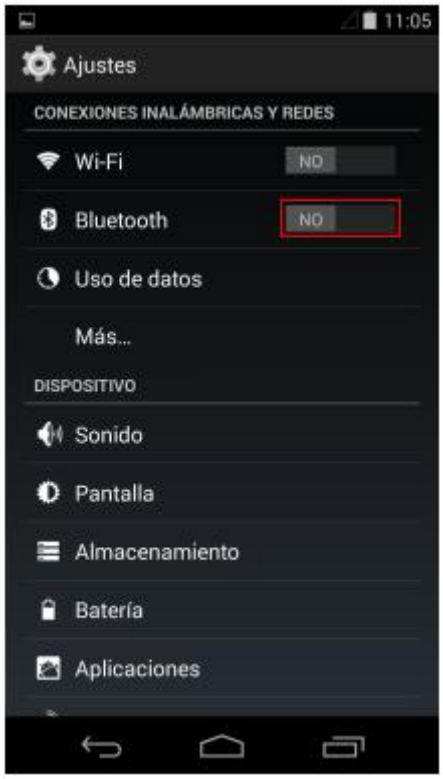

Ilustración 69. Desactivar Bluetooth en Android

4.2.5 DESACTIVAR INTERFAZ WI-FI

La principal recomendación de seguridad asociada a las comunicaciones Wi-Fi en dispositivos móviles es no activar el interfaz inalámbrico Wi-Fi salvo en el caso en el que se esté haciendo uso del mismo, evitando así la posibilidad de ataques sobre el hardware del interfaz, el driver o la pila de comunicaciones Wi-Fi.

El interfaz inalámbrico Wi-Fi puede ser desactivado en Android a través del menú "Ajustes [Conexiones Inalámbricas y Redes] - Wi-Fi", mediante el botón "SÍ|NO" de la opción "Wi-Fi":

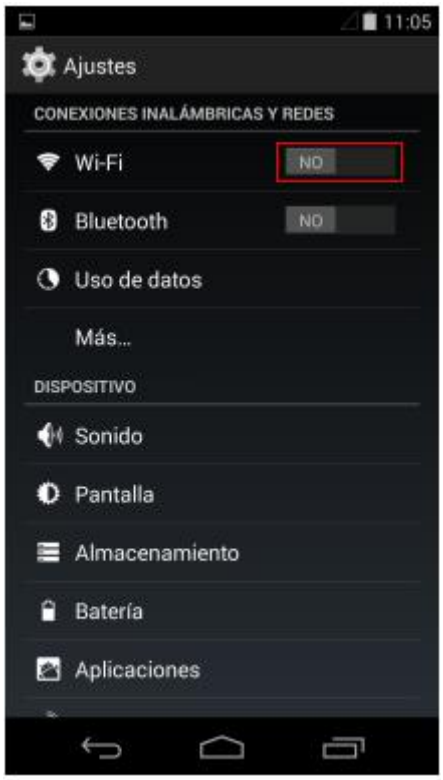

Ilustración 70. Desactivar Wi-Fi en Android

4.2.6 SELECCIÓN DE LA RED DE DATOS

Con el objetivo de mitigar las vulnerabilidades existentes actualmente en las redes de telefonía móvil 2G (o GSM), se recomienda forzar al dispositivo móvil a conectarse únicamente, tanto para comunicaciones de voz como de datos, a las redes de telefonía 3G (UMTS) o 4G (LTE).

A través del menú "Ajustes [Conexiones Inalámbricas y Redes] - Más... - Redes móviles", y en concreto de la opción "Tipo de red preferido", es posible indicar que sólo se haga uso de redes 4G:

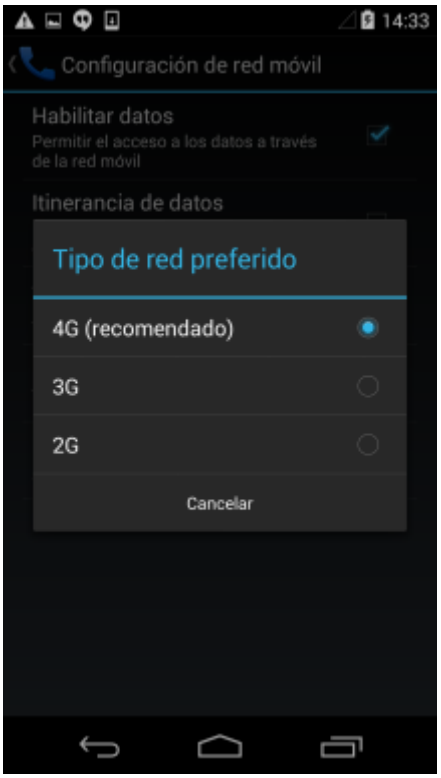

Ilustración 71. Selección del tipo de red

Desde el punto de vista de seguridad podría considerarse más seguro cursar todo el tráfico de datos a través de las redes de telefonía móvil en lugar de a través de redes Wi-Fi (especialmente con redes Wi-Fi públicas) siempre que se fuerce a que la conexión de datos de telefonía móvil empleé tecnologías 3/4G frente a 2G. Para ello sería necesario desactivar el interfaz Wi-Fi y habilitar las comunicaciones móviles de datos.

4.2.7 CONEXIÓN MEDIANTE USB

Android requiere por defecto desbloquear el teléfono para poder acceder por USB a los ficheros del dispositivo. A pesar de ello, se recomienda conectar por USB nuestro dispositivo Android a aquellos periféricos que sean de confianza, como el PC doméstico, y nunca hacerlo con equipos de la calle o públicos por el riesgo que podría entrañar.

4.3 SOFTWARE Y APLICACIONES

El potencial de un dispositivo móvil está directamente relacionado con la cantidad y calidad del software que sea posible instalar en el mismo. En este sentido Android posee un market muy grande de aplicaciones, la Play Store, desde la que será posible descargar e instalar un sinfín de programas, que pueden suponer una amenaza contra nuestra privacidad.

Es importante destacar que la Play Store no ofrece ninguna garantía de que la aplicación descargada no suponga un riesgo de seguridad para nuestro dispositivo. La recomendación general cuando se instala una aplicación es desconfiar de aplicaciones que piden demasiados permisos o permisos sospechosos.

4.3.1 DESACTIVAR GOOGLE NOW

Google Now está siempre funcionando en segundo plano y haciendo uso de los servicios de ubicación, 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.

Desde el punto de vista de seguridad y privacidad, salvo que se deseé hacer uso de la funcionalidad ofrecida por Google Now, se recomienda no activar esta funcionalidad.

Google Now puede ser desactivado en cualquier momento desde la app "Ajustes de Google" y el menú "Búsqueda y Google Now" y el botón "[SI | NO]" de Google Now.

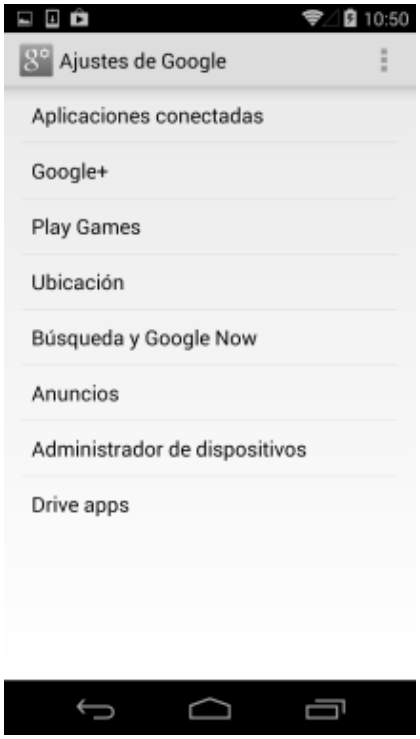

Ilustración 72. Desactivar Google Now

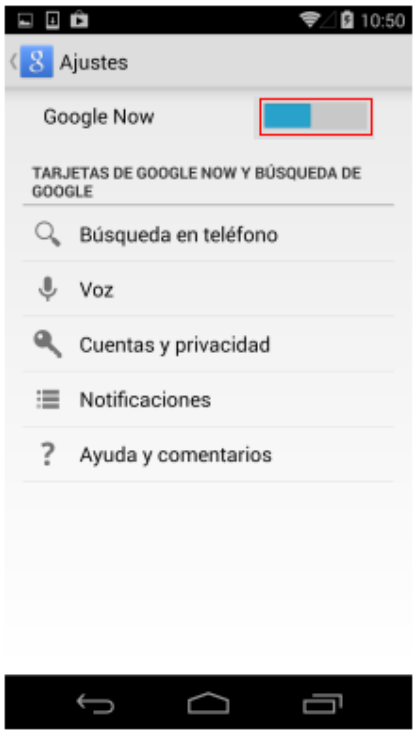

Ilustración 73. Desactivar Google Now

4.3.2 ROOTEO DEL DISPOSITIVO

El proceso de *rooteo* permite al usuario disponer de control completo sobre el dispositivo móvil y acceder al mismo como "root", o usuario privilegiado, eliminando así

los controles y/o restricciones establecidos por la plataforma Android. El *rooteo* otorga la posibilidad de instalar aplicaciones, modificaciones y componentes del sistema no proporcionados a través de la tienda oficial Play Store.

Los dispositivos móviles Android *rooteados* ignoran el modelo de seguridad impuesto por Google, ya que todas las aplicaciones que sean instaladas dispondrán de los máximos privilegios en el dispositivo ("root"), exponiendo a los usuarios a código dañino que podría tomar control completo del terminal.

Se recomienda encarecidamente **no realizar el proceso de root sobre el dispositivo**.

4.3.3 PERMISOS EN APLICACIONES

Desde el punto de vista de la seguridad es importante prestar atención a los permisos requeridos por cada aplicación, ya que, por ejemplo, aquellas que dispongan de acceso al micrófono podrán escuchar todo el sonido y audio existente alrededor del dispositivo móvil, grabarlo y/o enviarlo a través de Internet.

El sistema notifica al usuario estos permisos en el momento de la instalación de la aplicación. Una vez el usuario autoriza a una aplicación a disponer de dichos permisos, ésta será instalada y podrá hacer uso de los mismos en cualquier momento durante su ejecución. En ningún caso se solicitará autorización al usuario durante la ejecución de la aplicación, sino únicamente en el momento de su instalación.

Android no proporciona granularidad suficiente para seleccionar únicamente un subconjunto de todos los permisos solicitados por una aplicación y restringir así su funcionalidad. Si el usuario no está interesado en proporcionar ciertos permisos a una aplicación, la única opción disponible es no instalarla.

Para comprobar qué permisos utiliza una aplicación hay que prestar atención a la notificación que presenta Play Store en pantalla tras solicitar la instalación de la misma:

Ilustración 74. Permisos en aplicaciones Android

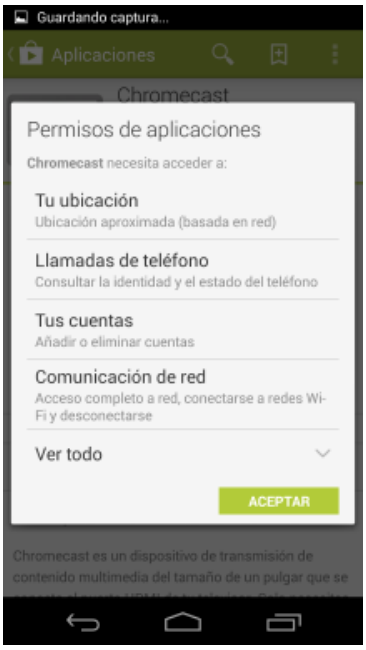

Ilustración 75. Permisos en aplicaciones Android

A través del botón "Ver todo" se puede obtener la lista completa de permisos solicitados por la aplicación, incluyendo los permisos considerados menos relevantes por Google:

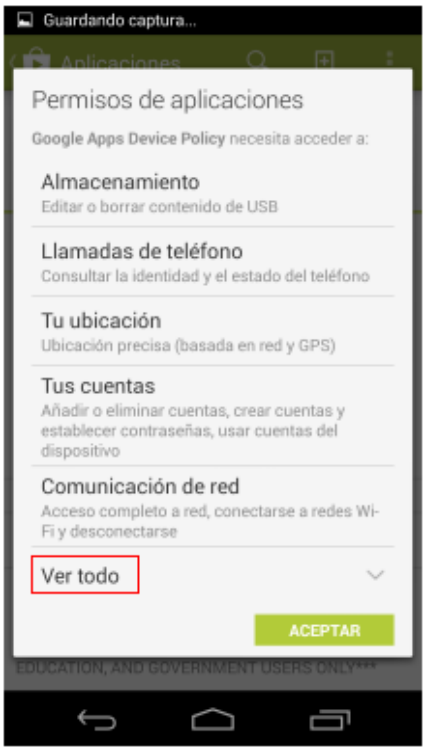

Ilustración 76. Permisos en aplicaciones Android

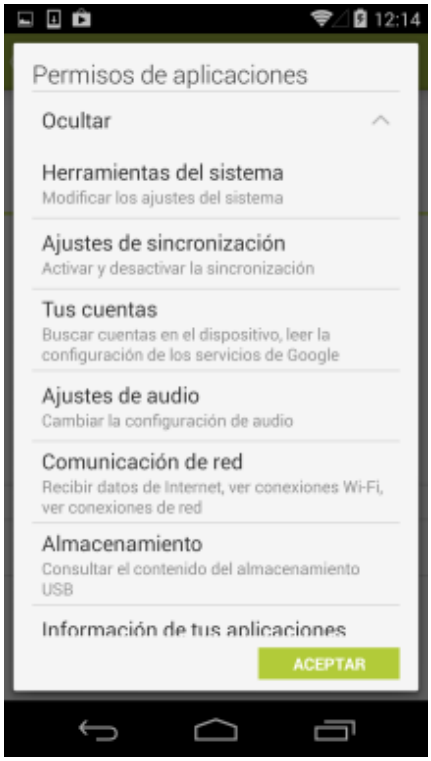

Ilustración 77. Permisos en aplicaciones Android

Una vez la aplicación ha sido instalada, es posible ver los permisos de los que hace uso desde el menú "**Ajustes [Dispositivo] - Aplicaciones**", seleccionando la aplicación correspondiente, por ejemplo:

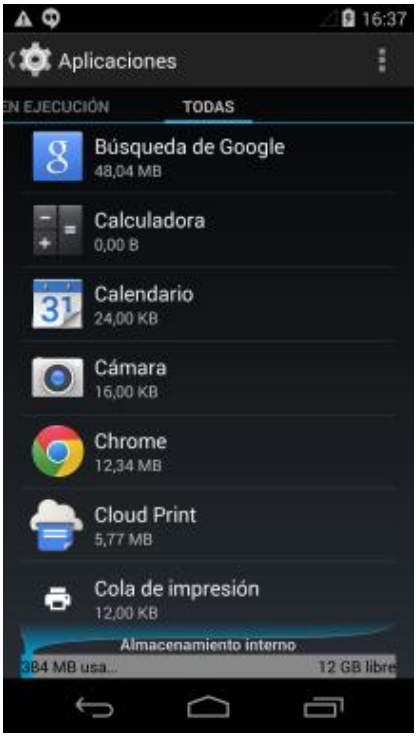

Ilustración 78. Permisos en aplicaciones Android

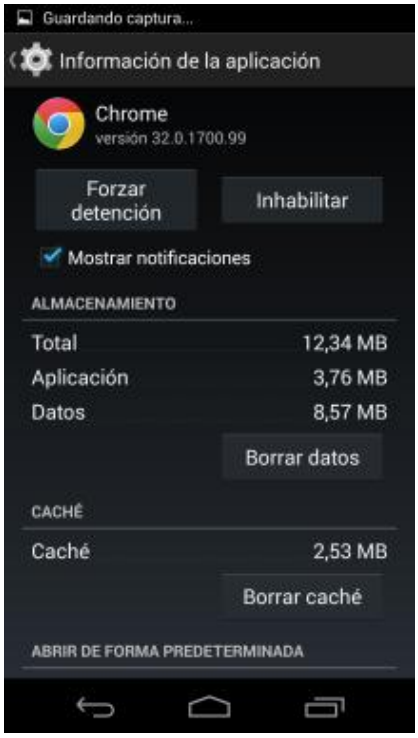

Ilustración 79. Permisos en aplicaciones Android

Ilustración 80. Permisos en aplicaciones Android

Se recomienda por tanto ser precavido y evaluar la reputación y los permisos requeridos por el software antes de proceder a instalar cualquier aplicación en el dispositivo móvil.

4.3.4 ACTUALIZACIÓN DE APLICACIONES

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

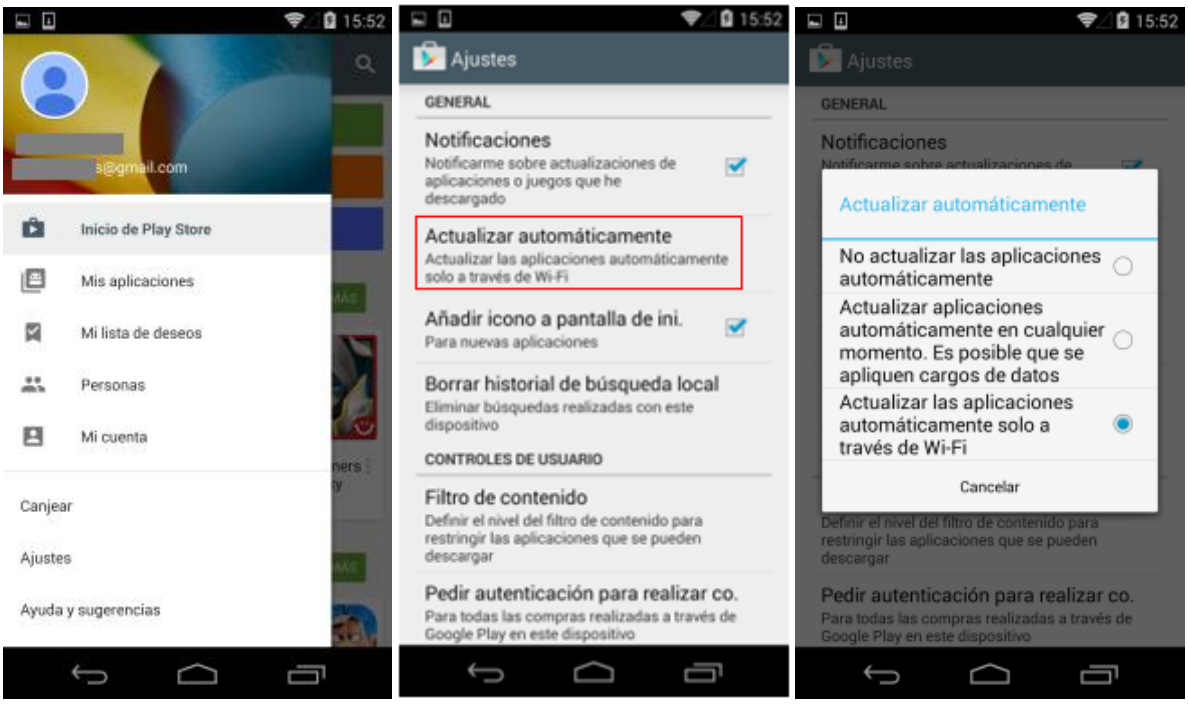

Ilustración 81. Actualización de aplicaciones en Android

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 aplicación 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 aplicación.

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 aplicación, 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 aplicaciones manualmente:

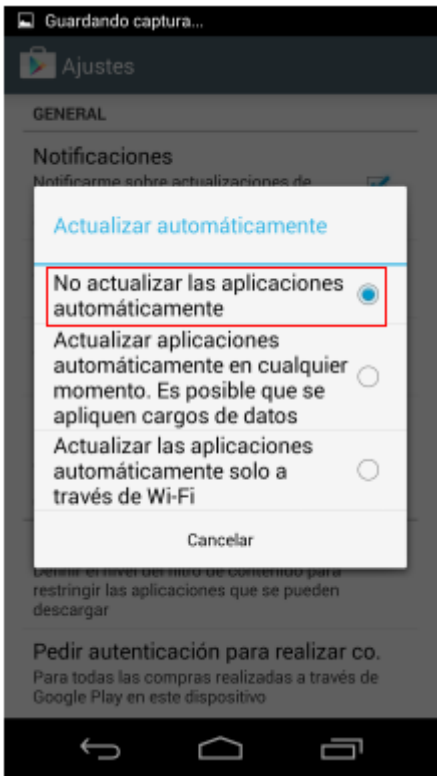

Ilustración 82. Desactivar actualizaciones automáticas

Se recomienda por tanto no dejar habilitada la opción de actualizaciones automáticas y forzar al usuario a revisar manualmente los nuevos permisos solicitados por cada una de las actualizaciones recibidas cada una de las diferentes aplicaciones instaladas en el terminal.

4.4 MANTENIMIENTO

Además de todas las medidas de seguridad descritas anteriormente, es importante realizar un correcto mantenimiento del dispositivo. A continuación se describen algunas recomendaciones complementarias para nuestro dispositivo Android.

4.4.1 REALIZAR COPIAS DE SEGURIDAD PERIÓDICAS

Las copias de seguridad en local se llevan a cabo a través de ADB, por lo que es necesario disponer de las capacidades de desarrollo y depuración a través de USB habilitadas.

Nota: para habilitar dicha opción es necesario acceder al menú "**Ajustes [Sistema] - Información del teléfono**", y pulsar en siete ocasiones sobre la opción "**Número de compilación**", disponible en la parte inferior:

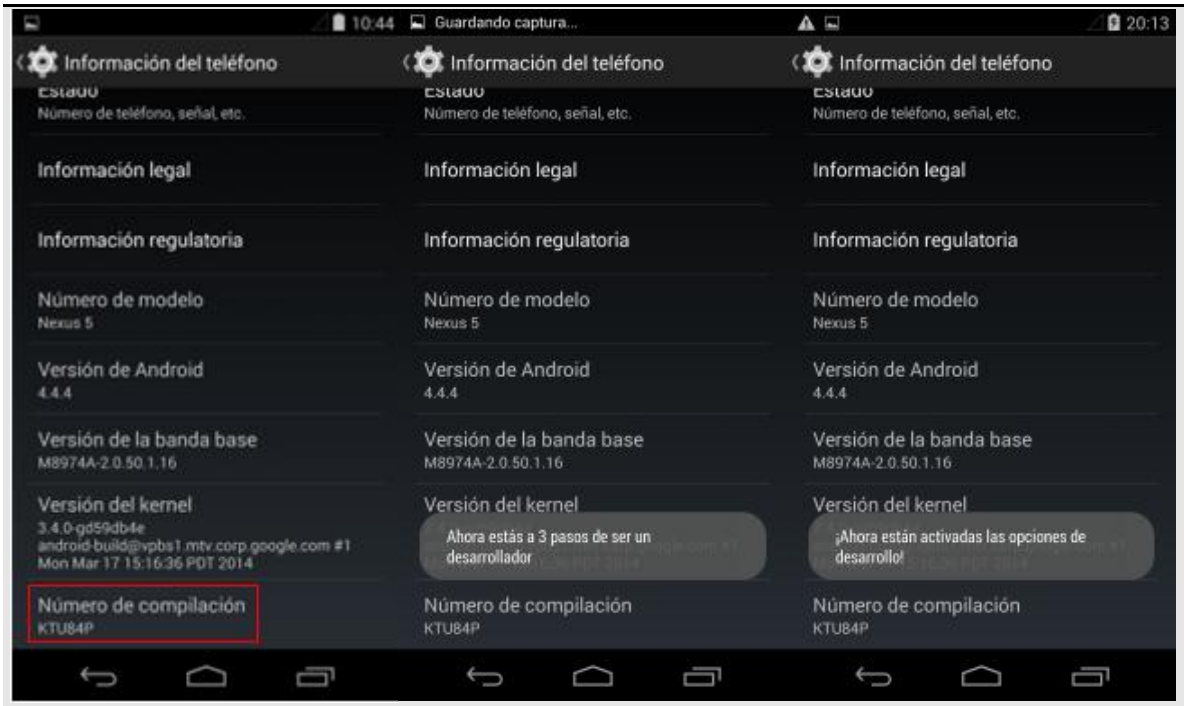

Ilustración 83. Activar opciones de desarrollador

Al completar las pulsaciones, aparecerá un nuevo menú, "**Opciones de desarrollo**", en la sección de "**Ajustes [Sistema]**", antes de la opción "**Información del teléfono**":

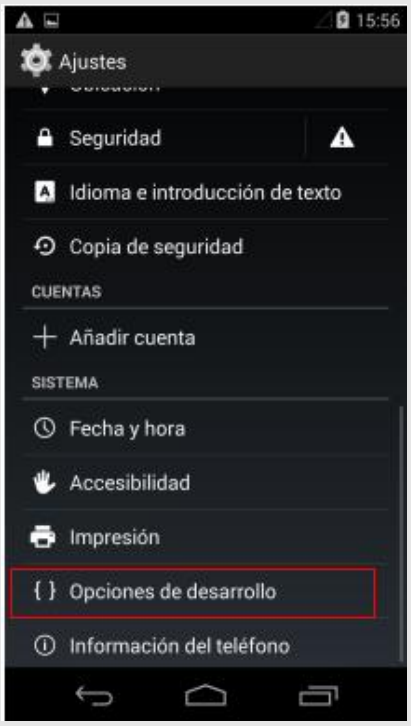

Ilustración 84. Acceder a opciones de desarrollo

A través de este nuevo menú es posible disponer de acceso a múltiples opciones para el desarrollo y depuración de apps en Android, incluyendo la opción "**Depuración USB**", que permite el acceso a través de USB a las opciones avanzadas de depuración del dispositivo móvil:

Ilustración 85.Activar depuración USB

Desde el punto de vista de seguridad se recomienda habilitar estas capacidades únicamente en el momento de llevar a cabo la copia de seguridad, y volverlas a desactivar inmediatamente después.

En concreto, el comando "**adb backup**" permite realizar la copia de seguridad, pudiéndose especificar el fichero dónde se almacenará la misma (mediante la opción "**-f**", y por defecto en "**backup.ab**").

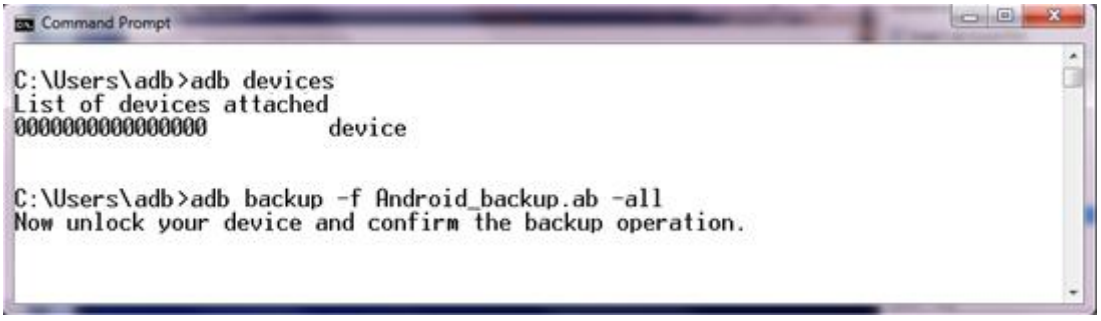

Ilustración 86. Backup desde ADB

Tras ejecutar el comando "adb backup", el dispositivo móvil mostrará una pantalla de confirmación para autorizar la realización de la copia de seguridad:

Ilustración 87. Backup en Android

Ilustración 88. Backup en Android

Se recomienda siempre hacer uso de una contraseña para cifrar los contenidos de la copia de seguridad.

4.4.2 ACTUALIZAR FIRMWARE

Una de las medidas de seguridad fundamentales, sino la más importante, es tener actualizado el dispositivo Android a la última versión disponible. Google lanza periódicamente estas actualizaciones del software del dispositivo con el fin de introducir nuevas características y parchear los fallos de seguridad que hayan sido identificados hasta esa fecha.

Si hay disponible una actualización, el dispositivo móvil mostrará en la barra superior de estado un mensaje notificando su disponibilidad, "Actualización del sistema disponible - Toca para descargar" o "Descargar":

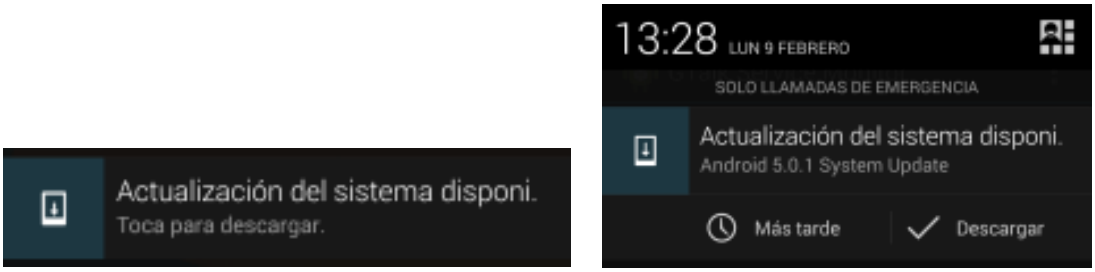

Ilustración 89. Actualizar firmware en Android

Adicionalmente es posible llevar a cabo esta operación de verificación de disponibilidad de actualizaciones en cualquier momento a través del menú "Ajustes - Información del teléfono - Actualizaciones del sistema":

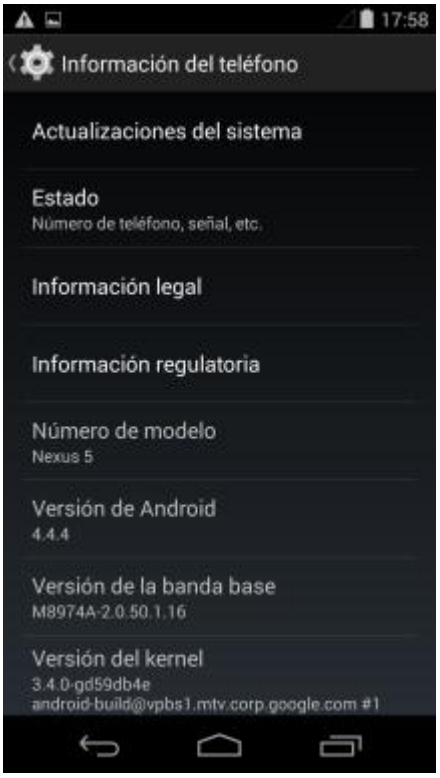

Ilustración 90. Actualizar firmware en Android

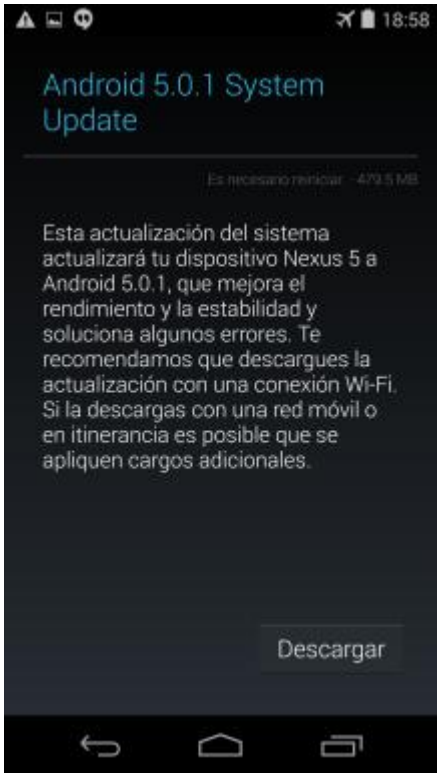

Ilustración 91. Actualizar firmware en Android

5. REFERENCIAS

- CCN-STIC 450 Seguridad en dispositivos móviles
- CCN-STIC 453A Seguridad en Android 2.x
- CCN-STIC 453B Seguridad en Android 4.x
- CCN-STIC 454 Seguridad en iPad
- CCN-STIC 455 Seguridad en iPhone
- CCN-STIC 457 Herramientas de gestión de dispositivos móviles: MDM

ANEXO I – MITIGACIÓN DE VULNERABILIDAD STAGEFRIGHT

StageFright ha sido calificada como la vulnerabilidad más crítica en la historia de Android. Ésta afecta a las versiones de Android comprendidas entre la 2.2 y la 5.1.1, esto representaba el 95% de los dispositivos Android en septiembre de 2015.

Para explotar la vulnerabilidad basta con que un atacante envíe un MMS dañino al número de teléfono de la víctima, de este modo podría tomar instantáneamente el control remoto del sistema. Esto sucede ya que Android, por defecto, descarga automáticamente los ficheros multimedia adjuntos a un mensaje.

Para evitar que el dispositivo Android sea explotado a través de esta vulnerabilidad existen dos opciones:

1. Actualizar el sistema operativo a una versión superior a la 5.1.1, así quedará parcheado el fallo de seguridad.
2. En caso de que el modelo concreto del dispositivo Android en cuestión no disponga de una actualización superior a la versión 5.1.1, será necesario deshabilitar manualmente la descarga automática de contenidos multimedia desde las aplicaciones:
    a. Hangouts
    b. Mensajería

Deshabilitar descarga multimedia desde Hangouts

A continuación se detallan los pasos que hay que seguir:

1. Abrir la aplicación Hangouts, en el caso de que estuviera instalada, y presionar el botón ubicado en la esquina superior izquierda de la pantalla:

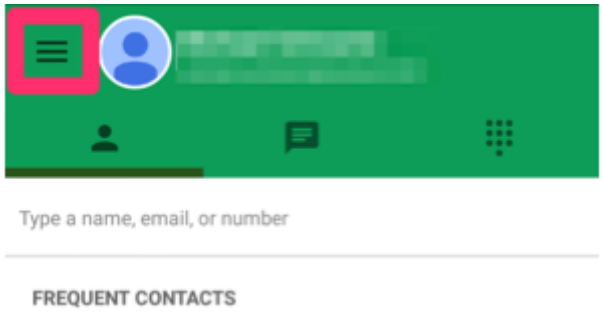

Ilustración 92. Acceso a MMS desde Hangouts

2. A continuación presionaremos la pestaña “Preferencias” (*Settings*):

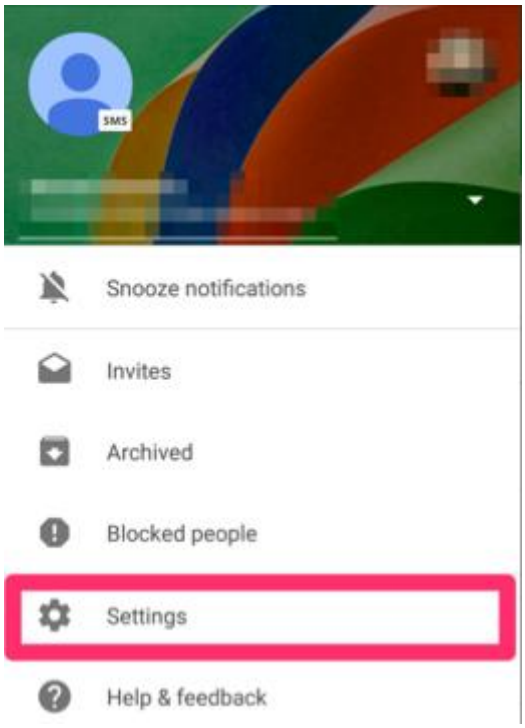

Ilustración 93. Acceso a ajustes de SMS

3. Presionaremos sobre la opción SMS (en caso de no figurar dicha opción en el menú, el dispositivo no está utilizando Hangouts para recibir los mensajes MMS):

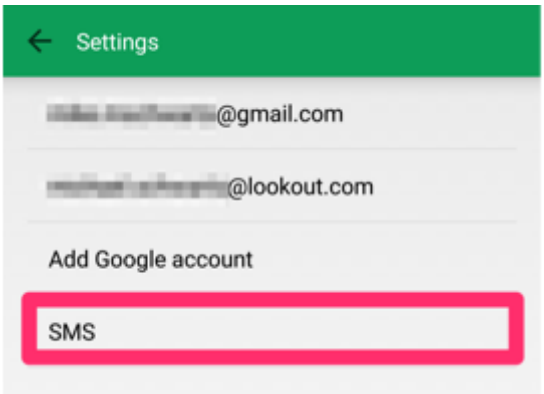

Ilustración 94. Acceso a ajustes de SMS II

4. Se desactivará la opción de "descargar automáticamente MMS" (*Auto Retrieve MMS*):

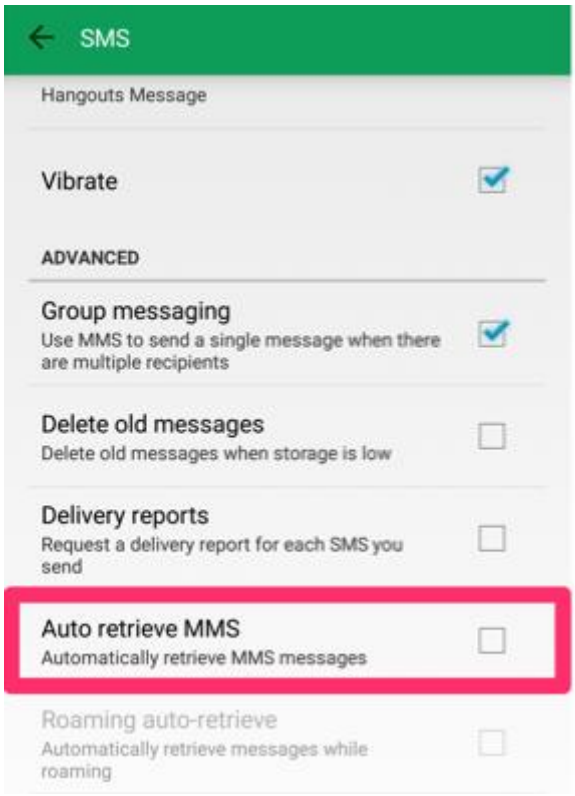

Ilustración 95. Deshabilitar la descarga automática de MMS

Deshabilitar descarga multimedia desde Mensajes

A continuación se detallan los pasos que hay que seguir:

1. Abrir la aplicación Mensajes y presionar en el botón ubicado en la parte superior derecha de la pantalla:

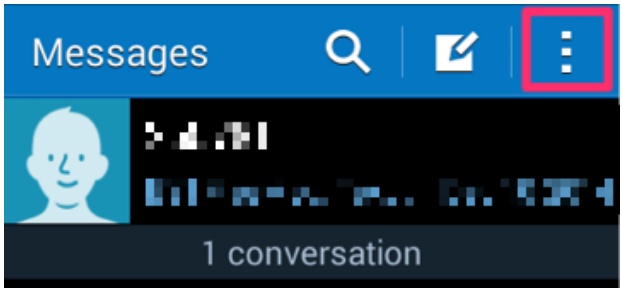

Ilustración 96. Acceder a la aplicación Mensajes

2. Se presionará la opción de Ajustes (Settings):

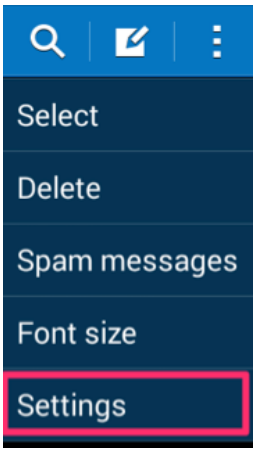

Ilustración 97. Acceder a los ajustes de la mensajería

3. Accederemos al menú de ajustes de "Mensajes Multimedia" (Multimedia messages):

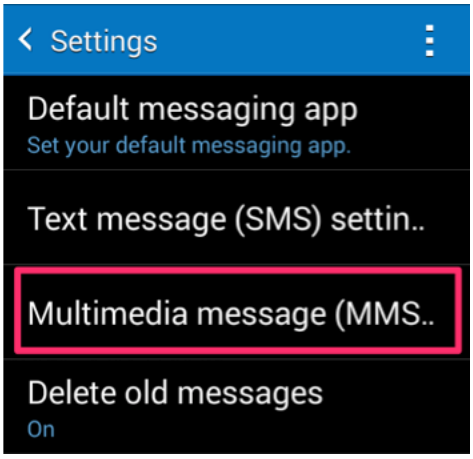

Ilustración 98. Ajustes de mensajes multimedia

4. Deshabilitaremos la opción de "descargar automáticamente" (Auto retrieve):

Ilustración 99. Deshabilitar la opción de descarga