GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-453)

SEGURIDAD DE DISPOSITIVOS MÓVILES: ANDROID

MAYO 2013

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE LA PRESIDENCIA

NIPO 002-13-027-1

Fecha de Edición: mayo de 2013
Raúl Siles ha participado en la elaboración y modificación del presente documento y sus anexos.

PRÓLOGO

Entre los elementos más característicos del actual escenario nacional e internacional figura el desarrollo alcanzado por las Tecnologías de la Información y las Comunicaciones (TIC), así como los riesgos emergentes asociados a su utilización. La Administración no es ajena a este escenario, y el desarrollo, adquisición, conservación y utilización segura de las TIC por parte de la Administración es necesario para garantizar su funcionamiento eficaz al servicio del ciudadano y de los intereses nacionales.

Partiendo del conocimiento y la experiencia del Centro sobre amenazas y vulnerabilidades en materia de riesgos emergentes, la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, 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 en su artículo 9.2.f).

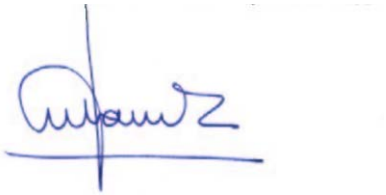
Una de las funciones más destacables que, asigna al mismo, el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración.

La ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 crea del Esquema Nacional de Seguridad (ENS), que establece las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos.

El Real Decreto 3/2010 de 8 de Enero desarrolla el Esquema Nacional de Seguridad y fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración. En su artículo 29 se autoriza que a través de la series CCN-STIC el CCN desarrolle lo establecido en el mismo.

La serie de documentos CCN-STIC se ha elaborado para dar cumplimiento a esta función y a lo reflejado en el ENS, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Mayo 2013



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, así como de los mecanismos de protección de la información que gestionan, dentro de los entornos de Tecnologías de la Información y las Comunicaciones (TIC).
3. Se considera dispositivo móvil aquél dispositivo de uso personal o profesional de reducido tamaño que permite la gestión de información y el acceso a redes de comunicaciones y servicios, 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), tabletas (o tablets) y agendas electrónicas (PDA), independientemente de sí disponen de teclado o pantalla táctil.
4. Pese a que los dispositivos móviles se utilizan para comunicaciones personales y profesionales, privadas y relevantes, y para el almacenamiento de información sensible, el nivel de percepción de la amenaza de seguridad real existente no ha tenido trascendencia en los usuarios finales y las organizaciones.
5. El presente documento realiza un análisis detallado de los mecanismos y la configuración de seguridad recomendados para uno de los principales sistemas operativos de dispositivos móviles utilizados en la actualidad, Android, con el objetivo de reducir su superficie de exposición frente a ataques de seguridad.

2. OBJETO

6. El propósito del presente documento es proporcionar una lista de recomendaciones de seguridad para la configuración de dispositivos móviles basados en el sistema operativo Android versión 2.2 (en adelante Android) [Ref.- 2], cuyo objetivo es proteger el propio dispositivo móvil, sus comunicaciones y la información y datos que gestiona y almacena.
7. La presente guía proporciona los detalles específicos de aplicación e implementación de las recomendaciones de seguridad generales descritas en la guía principal de esta misma serie, 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.
8. La serie CCN-STIC-450, “Seguridad de dispositivos móviles”, se ha estructurado en dos niveles: una guía genérica centrada en al análisis de seguridad de dispositivos móviles (CCN-STIC-450), complementada por guías específicas para los principales sistemas operativos empleados por los dispositivos móviles hoy en día. Por este motivo, antes de la lectura y aplicación de la presente guía, asociada a un sistema operativo (y versión concreta del mismo), se recomienda la lectura de la guía general de seguridad:

    - CCN-STIC-450 - Seguridad de dispositivos móviles

9. Adicionalmente, se recomienda la lectura de las guías de esta misma serie asociadas a otros sistemas operativos y versiones en caso de ser necesaria su aplicación en otros terminales:

    - 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 - Seguridad de dispositivos móviles: Android 2.x
    - CCN-STIC-455 - Seguridad de dispositivos móviles: iPhone

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

3. ALCANCE

10. 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. ENTORNO DE APLICACIÓN DE ESTA GUÍA

11. Android es un entorno software de código abierto (open-source) basado en Linux (kernel 2.6) y diseñado para dispositivos móviles que incluye el sistema operativo, el middleware (o módulo de comunicaciones interno) y un conjunto reducido de aplicaciones [Ref.- 11]. Inicialmente desarrollado por Android Inc., fue adquirido por Google en el año 2005, colaborando en su desarrollo la Open Handset Alliance, y encargándose de su mantenimiento el Android Open Source Project (AOSP) [Ref.- 81].

12. Android versión 2.2 (con nombre en clave “Froyo”) es la versión por defecto incluida en numerosos dispositivos móviles disponibles en el mercado durante los años 2010 y 2011, complementando versiones previas, como la versión 2.0/2.1 de Android (“Eclair”), 1.6 (“Donut”) y 1.5 (“Cupcake”) [Ref.- 128].

13. La versión 2.2 añade, entre otras, mejoras de rendimiento, la versión V8 del motor de JavaScript Chrome, la posibilidad de actuar como hotspot Wi-Fi para compartir la conexión de datos de telefonía móvil con otros dispositivos, y soporte para Adobe Flash en el navegador web.

14. Android dispone de una actualización anunciada en diciembre de 2010 y asociada a la versión 2.3 (“Gingerbread”) [Ref.- 9], que añade mejoras en el interfaz de usuario, el teclado táctil y las capacidades de copiar y pegar datos, así como soporte para SIP (voz sobre IP, VoIP) y NFC (Near Field Communication – con capacidades añadidas en la versión 2.3.3 [Ref.- 10]).

15. La versión 3.0 de Android (“Honeycomb”) ha sido diseñada para dispositivos tablet, con pantalla de mayor tamaño y mayor capacidad de procesamiento (tanto procesador principal como gráfico). Esta versión añade la posibilidad de aplicar un cifrado completo a los datos almacenados en el dispositivo móvil [Ref.- 82]. El primer dispositivo móvil basado en Android 3.0, el tablet Motorola Xoom, se empezó a comercializar en el mercado en febrero de 2011.

16. Adicionalmente se publicaron las versiones 3.1 y 3.2 en mayo y julio de 2011 respectivamente. La versión 3.1 añade soporte para más dispositivos de entrada y conexión

USB para la transferencia de ficheros, mientras que la versión 3.2 añade soporte para tarjetas de memoria SD y mejoras en la gestión de la pantalla y de distintas resoluciones.

17. La versión 4.0 de Android ("Ice Cream Sandwich") fue anunciada en octubre de 2011 y proporciona la funcionalidad de "Honeycomb" a los smartphones (no únicamente a tablets), añade control de acceso mediante reconocimiento facial, control y monitorización del tráfico de red y la posibilidad de compartir información mediante NFC, entre otros. El primer dispositivo móvil basado en Android 4.0, el smartphone Galaxy Nexus (Samsung & Google), se empezó a comercializar en el mercado en diciembre de 2011.
18. Las principales diferencias y novedades de cada una de las versiones de la plataforma Android están disponibles en la página web para usuarios y desarrolladores: 2.2, 3.0 y 4.0 [Ref.- 83].
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 – Idioma y teclado – Seleccionar idioma".
20. La guía ha sido probada y verificada con la versión 2.2 del sistema operativo Android.

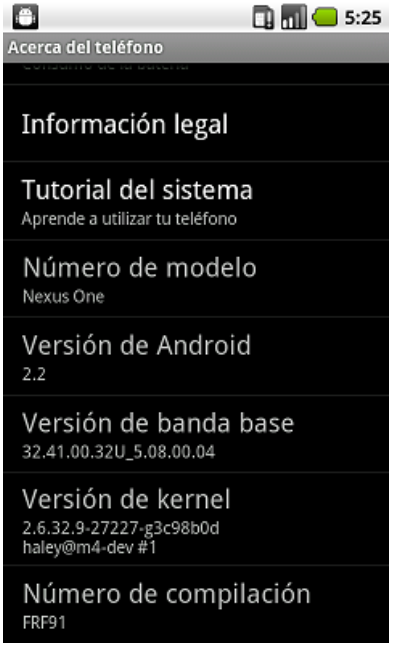
Nota: la información general del dispositivo móvil está disponible bajo la opción "Ajustes – Acerca del teléfono", y en concreto, la información de la versión del sistema operativo se encuentra bajo la categoría "Versión de Android".

21. Las particularidades de seguridad asociadas a Android 2.3, respecto a la versión 2.2, se analizan en el apartado "6. Apéndice A: Guía de seguridad de Android 2.3" y a través de anotaciones y puntualizaciones a lo largo de la presente guía.
22. Las operaciones que requieren del uso de un ordenador han sido llevadas a cabo mediante Windows 7 Home Premium 64-bits (Service Pack 1) en inglés.

Nota: para la elaboración de la guía se ha empleado la versión de Windows 7 en inglés en el ordenador utilizado para la sincronización con el dispositivo móvil, con el objetivo de ejemplificar la compatibilidad de idiomas entre el terminal y el ordenador. La simplicidad de las funciones realizadas a través del ordenador, pese a utilizarse otro idioma, no debería dificultar la comprensión de la presente guía.

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

23. El hardware sobre el que se ha verificado la presente guía tiene las siguientes características:
    - Dispositivo móvil Google Nexus One (fabricado por HTC) [Ref.- 3]:
        - Versión de Android (disponible por defecto): 2.2
        - Versión de banda base: (ver imagen inferior): 32.41.00.32U_5.08.00.04
        - Versión de kernel: (ver imagen inferior): 2.6.32.9.27227-g3c98b0d…
        - Número de compilación: FRF91



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*. Este proceso permite al usuario disponer de control completo del dispositivo móvil y acceder al mismo como "root", 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 los operadores de telefonía móvil asociados al dispositivo móvil.

Las aplicaciones de usuario 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 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 *rooted* ignoran el modelo de seguridad descrito a lo largo de la presente guía, 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. Android no requiere llevar a cabo el proceso de *rooting* para permitir la instalación de aplicaciones de terceros no oficiales, es decir, no distribuidas a través de Google Play, tal como sucede en otras plataformas de dispositivos móviles, como el iPhone, donde es necesario realizar el proceso de "jailbreak" (equivalente a *rooting*) para poder instalar ese tipo de aplicaciones no oficiales.

Las particularidades del proceso de actualizaciones en Android (ver apartado "5.1. Actualización del sistema operativo: Android"), con largos periodos de tiempo hasta que una nueva actualización está disponible para algunos usuarios finales, es uno de los motivos que

incentiva a muchos usuarios a realizar el proceso de *rooting* para así poder instalar la última versión de Android en su dispositivo móvil.

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 Android, debido al modelo, fabricante o versión 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.

24. La versión 2.2 de Android para el dispositivo móvil Nexus One estuvo disponible desde el 28 de junio de 2010 [Ref.- 58].
25. 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 de seguridad.
26. Debe prestarse atención al contrato de telefonía, y en concreto de datos, asociado a la tarjeta SIM (Subscriber Identity Module) empleada en el dispositivo móvil Android. La ausencia de capacidades de comunicación de datos es notificada al usuario en función de las aplicaciones que requieren disponer de la misma.
27. Igualmente, debe prestarse especial atención al tipo de dispositivo móvil (marca y modelo) donde se desea aplicar la guía ya que la relación de los elementos descritos o referenciados en la presente guía (interfaz de usuario, capacidades hardware, aplicaciones, etc.) puede diferir ligeramente en función de la personalización del sistema operativo realizada por el fabricante del terminal.
28. 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 se ajusten a los criterios 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 entre los dispositivos móviles Android y los diferentes servicios de Google.

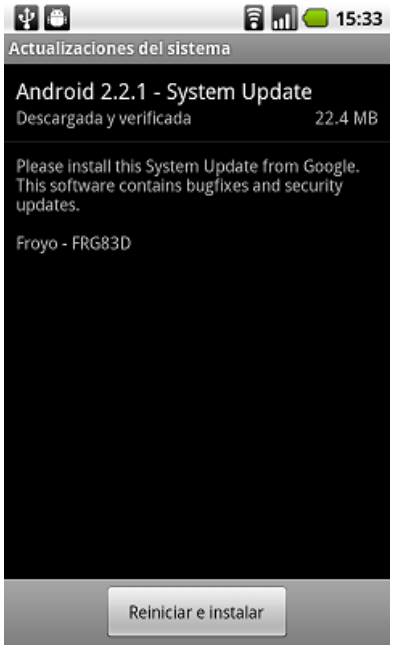
5. CONFIGURACIÓN DE SEGURIDAD DE ANDROID

5.1 ACTUALIZACIÓN DEL SISTEMA OPERATIVO: ANDROID

29. Los dispositivos móviles Android, una vez disponen de conectividad de datos hacia Internet a través de las redes de telefonía móvil (2G/3G) o de redes Wi-Fi, verifican automáticamente si existe una nueva versión o actualización del sistema operativo.

30. Para ello, se establece una conexión cifrada con el servidor "android.clients.google.com", mediante HTTPS (TCP/443). Otra opción empleada frecuentemente para la distribución de actualizaciones de Android es la basada en mensajes OTA (Over-The-Air), que complementa la opción manual por parte del usuario de descargar el fichero correspondiente a la actualización directamente de los servidores oficiales de Google (analizada en detalle posteriormente).

31. Es posible llevar a cabo esta operación de verificación de disponibilidad de actualizaciones en cualquier momento a través del menú "Ajustes – Acerca del teléfono – Actualizaciones del sistema":



32. Mediante el código *#*#checkin#*#* (o *#*#2432546#*#*) de llamada del teléfono en Android es posible forzar una búsqueda inmediata de actualizaciones y parches.

33. El dispositivo móvil establecerá una conexión cifrada mediante HTTPS con el servidor "android.clients.google.com" para verificar si hay una actualización disponible, y mostrará en la barra de estado un mensaje con el resultado de la operación (en inglés):

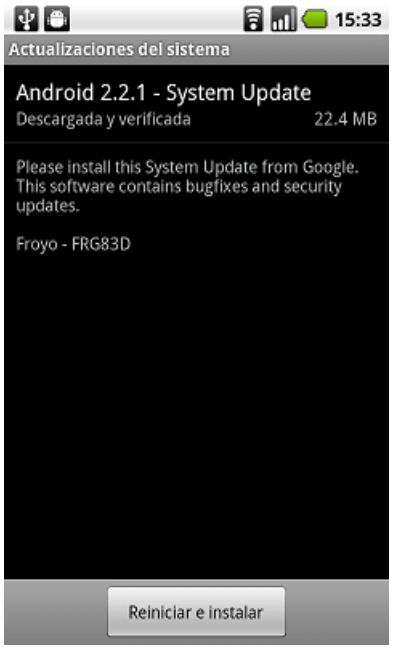
34. Tras realizar la verificación, si existe una actualización disponible, Android establecerá una conexión no cifrada HTTP con el servidor "android.clients.google.com" para descargar la misma, empleando el agente de usuario "AndroidDownloadManager" (en el ejemplo inferior desde Android 2.3.3 GRI40 a Android 2.3.4 GRJ22). Como respuesta se recibe una redirección (HTTP 302) a uno de los servidores de caché de Google para obtener la nueva actualización:

```
GET         /packages/ota/passion/71d2f9ecd610.signed-passion-GRJ22-from-
    GRI40.71d2f9ec.zip HTTP/1.1
Host: android.clients.google.com
User-Agent: AndroidDownloadManager

HTTP/1.1 302 Found
Location:http://v23.lscache6.c.android.clients.google.com/packages/data/o
    ta/passion/71d2f9ecd610.signed-passion-GRJ22-from-GRI40.71d2f9ec.zip
...
```

35. Teóricamente, la integridad de las actualizaciones de las nuevas versiones de Android se verifica a través de una firma digital asociada al fichero de actualización (.zip) descargado, pero la ausencia de cifrado abre la puerta a la manipulación de este intercambio de datos, por ejemplo, mediante la sustitución de la versión entre actualizaciones válidas firmadas digitalmente.
36. Por otro lado, la utilización de un canal no cifrado HTTP permite a un atacante conocer la versión y compilación actual (y potencialmente futura) del dispositivo móvil víctima, pudiendo explotar vulnerabilidades conocidas sobre dichas versiones.
37. El dispositivo móvil mostrará en la barra de estado un mensaje indicando que hay una actualización disponible (ejemplo de mensaje en Android 2.3.x):

38. Si existe una versión disponible, como por ejemplo la actualización a Android 2.2.1 desde la versión empleada como referencia en la presente guía, Android 2.2, el dispositivo móvil mostrará una notificación sobre su disponibilidad, siendo posible obtener los detalles de la actualización a través del botón “Más información…”:



Nota: en el momento de finalización de la elaboración de la presente guía, febrero de 2012, Google no proporciona la actualización automática para el terminal Google Nexus One desde

Android 2.2 (Froyo) a 2.2.1, y la actualización manual [Ref.- 125] tampoco está disponible (los detalles para actualizar a la versión 2.3.x desde la versión 2.2 de Android están disponibles en el apartado "5.1.2. Actualización manual de Android").

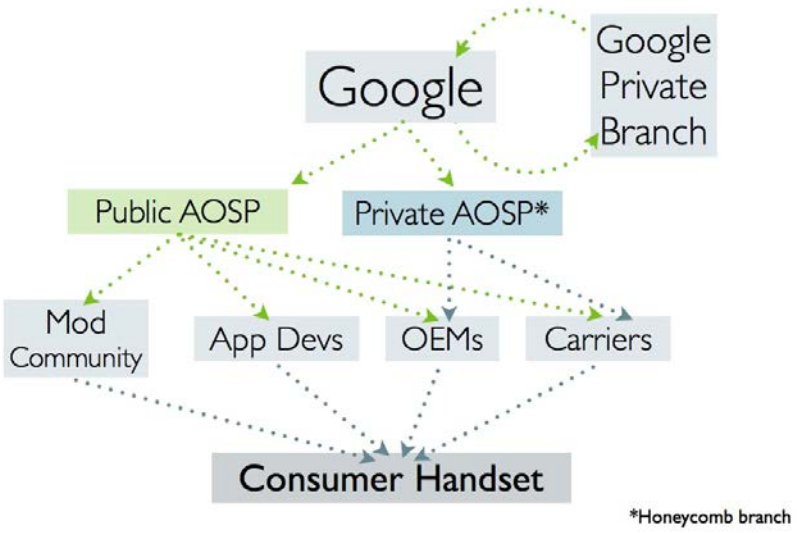
39. Android 2.2.1 (liberada en mayo de 2010, compilación FRG83 o FRG83D) [Ref.- 125] incorpora pequeñas diferencias y mejoras con respecto a versiones anteriores de este sistema operativo [Ref.- 59], como por ejemplo una nueva aplicación de GMail, mejoras para Microsoft Exchange ActiveSync, una actualización del widget de información meteorológica y de la aplicación Twitter, así como corrección de errores y bugs. Las mejoras en la aplicación de GMail incluyen soporte para Priority Inbox, posibilidad de modificar la dirección origen (From:), y mejoras a la hora de responder mensajes de correo electrónico [Ref.- 66].
40. Android 2.2.2 (liberada en julio de 2010, compilación FRG83G [Ref.- 60]) se publicó con el propósito de solucionar, entre otros, el bug de la aplicación de mensajería (SMS) que reenviaba un mensaje aleatorio de los disponibles en el buzón de entrada a recipientes de la lista de contactos a los que no iba dirigido el mensaje original [Ref.- 61].
41. Android 2.2.3 fue liberada en julio de 2011, compilación FRK76 [Ref.- 84], con notables mejoras en el entorno de aplicaciones para los desarrolladores y resolvía vulnerabilidades en libpng y en la gestión de certificados digitales (ej. DigiNotar), entre otras. La revisión 1 de la versión 2.2.3 corresponde a la compilación FRK76, disponible por ejemplo para el Motorola Droid, y la revisión 2, "android-2.2.3_r2", a la compilación FRK76C.
42. Supuestamente, y en base a la documentación y referencias oficiales [Ref.- 69] (incluido el propio mensaje de anuncio), las notificaciones y actualizaciones de seguridad de Android deberían estar disponibles en el grupo o lista de distribución "Android Security Announcements", sin embargo, esta lista únicamente contiene una entrada sobre el anuncio inicial del equipo de seguridad de Android de agosto de 2008 [Ref.- 67].
43. Desafortunadamente no se dispone de un repositorio oficial de notificaciones con el listado de vulnerabilidades que han afectado a Android, y en consecuencia, no existe un listado de actualizaciones disponibles para resolver esas vulnerabilidades.
44. Existe otro grupo o lista de distribución para la discusión de temas relacionados con seguridad en Android, denominado "Android Security Discussions" [Ref.- 68]. La problemática actual respecto al modelo de actualizaciones de seguridad de Android (reflejado posteriormente) ha sido analizada y discutida en numerosas ocasiones en dicho grupo.
45. Oficialmente, las actualizaciones de Android, al tratarse de un sistema operativo de código abierto basado en Linux y con modificaciones particulares según los modelos de terminal, deben ser proporcionadas por los diferentes fabricantes de los dispositivos móviles [Ref.- 69] u operadores de telefonía móvil, en base a las modificaciones y ajustes realizados sobre las actualizaciones proporcionadas por el proyecto Android. Google, como líder del proyecto Android, no proporciona directamente actualizaciones para los dispositivos móviles Android (salvo para sus propios modelos: Google Nexus).

Nota: debido a que el dispositivo móvil Android empleado para la elaboración de la presente guía es distribuido por Google (actuando como fabricante), los procesos de actualización descritos en este documento afectan únicamente a Google.

46. No existe ningún estándar ni modelo definido para la distribución de las actualizaciones de seguridad de Android, ni ninguna periodicidad definida para su publicación, por lo que Google y otros fabricantes (miembros o no de la Open Handset Alliance) pueden seguir procedimientos de actualización diferentes.

47. El fabricante del dispositivo móvil o el operador de telefonía es el que publicará actualizaciones para el terminal. Como norma general, y salvo que exista un motivo que desaconseje su instalación, se recomienda aplicar sobre el dispositivo móvil todas las actualizaciones facilitadas por el fabricante, ya que pese a que las mismas no reflejen explícitamente que se trata de actualizaciones de seguridad, pueden solucionar vulnerabilidades de seguridad públicamente conocidas.

48. Google ha desarrollado un modelo para la resolución de problemas de seguridad y la distribución de actualizaciones en Android a través de CTS (Compatibility Test Suite) [Ref.- 86], actividad integrada en el Android Open Source Project (AOSP), encargada de asegurar la compatibilidad entre dispositivos Android [Ref.- 85]:



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

50. La siguiente imagen refleja las vulnerabilidades más significativas en Android durante los últimos años, algunas de las cuales han sido aprovechadas por código dañino públicamente distribuido, como DroidKungFu y DroidDream [Ref.- 85]:

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

51. Mediante la realización de una búsqueda por el término “Android” en la US CERT NVD (National Vulnerability Database: http://web.nvd.nist.gov/view/vuln/search-results?query=android&search_type=all&cves=on) es posible obtener un listado de las vulnerabilidades de seguridad conocidas públicamente que han afectado a diferentes versiones del sistema operativo Android en los últimos años, así como a aplicaciones de terceros desarrolladas para Android. Por ejemplo, entre las vulnerabilidades críticas más recientes de finales de 2011 de Android, destacan:

    - CVE-2011-4276: “The Bluetooth service in Android 2.3 before 2.3.6 allows remote attackers within Bluetooth range to obtain contact data via an AT phonebook transfer”
    - CVE-2011-3874: “Stack-based buffer overflow in libsysutils in Android 2.2.x through 2.2.2 and 2.3.x through 2.3.6.”
    - CVE-2011-2357: “Cross-application scripting vulnerability in the Browser URL loading functionality in Android 2.3.4 and 3.1 allows local applications to bypass the sandbox and execute arbitrary JavaScript”
    - CVE-2011-1823: “The vold volume manager daemon on Android 3.0 and 2.x before 2.3.4 trusts messages that are received from a PF_NETLINK socket, which allows local users to execute arbitrary code and gain root privileges”
    - Múltiples vulnerabilidades en Adobe Flash Player: CVE-2011-2444 y 2445 (2), CVE-2011-2450 al 2460 (11), CVE-2011-2424 al 2430 (7), etc.

52. Adicionalmente, las soluciones publicadas para corregir vulnerabilidades de seguridad conocidas suelen estar disponibles únicamente para las últimas versiones de Android, no existiendo un mecanismo establecido para proporcionar dichas soluciones para versiones previas de Android, también vulnerables.

53. Por otro lado, numerosos fabricantes y operadores de telefonía móvil no proporcionan actualizaciones para modelos de dispositivos móviles previos, por ejemplo, basados en la versión 1.x de Android, por lo que estos serán siempre vulnerables.

54. Este hecho se ve agravado por la velocidad de consumo de las nuevas tecnologías, que afecta a cuando los dispositivos móviles son considerados obsoletos, dónde en la actualidad, un dispositivo con dos o más años difícilmente estará soportado e incluido en el ciclo de actualizaciones de software.

55. Por ejemplo, en octubre de 2011 Google confirmó que el dispositivo móvil empleado para la elaboración de la presente guía, Google (HTC) Nexus One (lanzado al mercado por

Google en enero de 2010), no dispondrá de una actualización oficial a Android 4.0 (“Ice Cream Sandwich”) [Ref.- 100]. Ésta versión de Android sí está disponible para otros modelos, como el Nexus S y el Galaxy Nexus.

56. La importancia, por un lado, de actualizar la versión de Android en el dispositivo móvil a la última versión disponible, y por otro, de verificar si la actualización corrige vulnerabilidades previas públicamente conocidas, se refleja en vulnerabilidades como la de TapJacking [Ref.- 113].

57. La vulnerabilidad de TapJacking, similar a clickjacking en aplicaciones web, permite a una aplicación maliciosa engañar al usuario para que a través de la pulsación (tap) en diferentes diálogos (menús y opciones) de la pantalla de Android, lleve a cabo acciones de las que el usuario no es consciente, como modificar la configuración de seguridad del terminal o instalar otras aplicaciones maliciosas.

58. La vulnerabilidad de TapJacking fue solucionada supuestamente en la versión 2.3 de Android, sin embargo, posteriores estudios confirman su presencia, por ejemplo, en Android 2.3.4 [Ref.- 114].

59. En el caso de disponer de un dispositivo móvil Android para el que se sí dispone de una actualización a una versión superior de Android, por ejemplo 2.3 para un terminal basado en Android 2.2, se recomienda aplicar la actualización sobre el dispositivo con el objetivo de instalar la última versión disponible y protegerlo de vulnerabilidades conocidas.

60. Las diferentes versiones del sistema operativo Android son proporcionadas como una imagen parcial (se dispone de varios ejemplos en [Ref.- 125] [Ref.- 60] [Ref.- 62] [Ref.- 98] [Ref.- 127]) que contiene las actualizaciones para el firmware actual del dispositivo móvil, y que debe ser cargada en el terminal actualizando la versión existente previamente, o como una imagen completa de la plataforma (por ejemplo, para Android 2.3.3 [Ref.- 126]), que instala una nueva versión en el terminal.

61. Si la imagen es parcial, todos los datos y configuración del usuario son conservados, mientras que si la imagen es completa, se eliminarán todos los datos y configuración del usuario, fijando los valores de configuración de fábrica durante el proceso.

62. Debe tenerse en cuenta que antes de realizar una actualización del sistema operativo del dispositivo móvil se recomienda realizar una copia de seguridad de los datos del usuario.

63. Pese a que existen foros en Internet dónde se distribuyen imágenes de ROM para múltiples sistemas operativos y fabricantes de terminales (como XDA Developers - http://forum.xda-developers.com), desde el punto de vista empresarial, en ningún caso se recomienda la instalación del sistema operativo desde una fuente no oficial.

64. En el mundo Android, las actualizaciones individuales adicionales a las actualizaciones de la versión completa del sistema operativo son muy limitadas, en contraposición a las actualizaciones para otros sistemas operativos de sobremesa cliente o servidor. Esta situación afecta tanto a las actualizaciones generales sobre los distintos componentes del sistema operativo, como a las actualizaciones específicas de seguridad.

65. Con el objetivo de mantener el dispositivo móvil actualizado, se recomienda comprobar periódicamente desde el propio dispositivo la disponibilidad de actualizaciones desde el menú “Ajustes – Acerca del teléfono – Actualizaciones del sistema”.

66. Desde el punto de vista de seguridad es necesario actualizar igualmente todas las aplicaciones (cliente) instaladas sobre el sistema operativo (ver apartado “5.26. Actualización de aplicaciones (cliente) en Android”).

5.1.1 VULNERABILIDAD DE ACCESO A FICHEROS Y ROBO DE INFORMACIÓN EN ANDROID

67. El siguiente ejemplo asociado a una vulnerabilidad concreta de Android refleja la situación real actual del modelo de notificación y eliminación de vulnerabilidades de seguridad en esta plataforma móvil.

68. A final de noviembre de 2010 se descubrió una vulnerabilidad en la versión 2.2 de Android que permitía a cualquier sitio web acceder a ficheros locales del usuario en el dispositivo móvil Android mediante el navegador web y JavaScript [Ref.- 70].

69. Simplemente si el usuario navega a una página web preparada previamente, ésta podría robar datos del usuario almacenados en su dispositivo móvil, como por ejemplo fotografías ("/sdcard/DCIM/100ANDRO/IMG0001.jpg"), vídeos, descargas de Internet ("/sdcard/download/"), es decir, cualquier fichero de la tarjeta de almacenamiento externa y otros ficheros asociados a aplicaciones cliente instaladas en Android.

70. La vulnerabilidad permite acceder a todos los ficheros de la tarjeta de almacenamiento externa y a un número reducido de ubicaciones en las que el usuario tiene acceso (ficheros con lectura para todo el mundo, desde el sandbox de Android, ya que la vulnerabilidad no permite disponer de privilegios de sistema en Android). Como requisito, el atacante debe conocer (o adivinar) el nombre del fichero.

71. El comportamiento vulnerable fue solucionado parcialmente en el repositorio de código del sistema operativo del proyecto Android (GIT) el mismo mes, pero no se aplicó (por motivos de tiempo, y pese a la información de diferentes fuentes) en la versión 2.3 de Android.

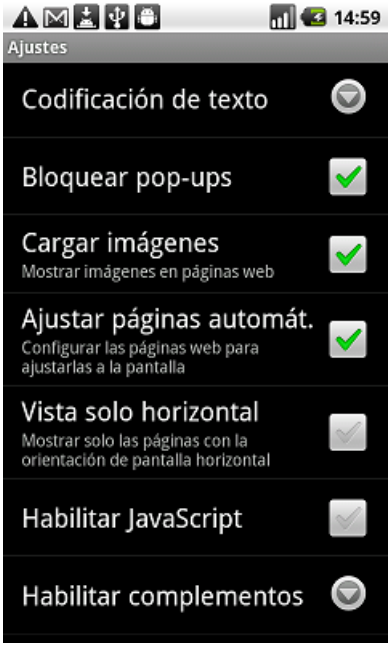
72. En enero de 2011 se liberó un módulo de Metasploit que permitía explotar esta vulnerabilidad [Ref.- 71]. Posteriormente, a final de enero de 2011, se descubrió la posibilidad de explotar la misma vulnerabilidad en Android de forma ligeramente distinta, afectando a la versión 2.3.2 de Android en un dispositivo móvil Nexus S [Ref.- 72], pese a que la vulnerabilidad se suponía solucionada en alguna versión de Android asociada a la rama 2.3.x. Por tanto, aún es posible emplear la vulnerabilidad para el robo de información en Android 2.3.2.

73. Google ha indicado que está trabajando en una solución más amplia para esta vulnerabilidad que evite el problema en todos los componentes del sistema y que será supuestamente incluida en la siguiente versión principal de Android.

74. La vulnerabilidad puede ser explotada no sólo para obtener copia de algunos ficheros del dispositivo móvil, sino también para conocer la lista de aplicaciones instaladas en el mismo u obtener copia de las aplicaciones (ubicadas en "/system" y "/sdcard").

75. La protección actual frente a esta vulnerabilidad pasa por deshabilitar JavaScript en el navegador web por defecto de Android, utilizar otro navegador web, como Opera Mini o Firefox para Android, que no son vulnerables o solicitan confirmación por parte del usuario antes de realizar transferencias de ficheros, o no hacer uso de la tarjeta de almacenamiento externa (lo que impone limitaciones en el uso del dispositivo móvil).

76. JavaScript puede ser deshabilitado en el navegador web por defecto de Android desde el botón "Menú" disponible una vez se ejecuta el navegador web, empleando la opción "Más – Ajustes". En la página de ajustes de configuración existe una opción denominada "Habilitar JavaScript", habilitada por defecto, y que debería ser desactivada para evitar la vulnerabilidad descrita (ver apartado "5.22. Navegación web: Navegador"):



77. La disponibilidad de actualizaciones para aplicaciones cliente de terceros (ver apartado "5.26. Actualización de aplicaciones (cliente) en Android"), en lugar de componentes integrados en el sistema operativo de Android como el navegador web vulnerable existente por defecto en Android 2.2 y 2.3, puede ser más flexible y ágil a la hora de solucionar problemas de seguridad similares al descrito.

5.1.2 ACTUALIZACIÓN MANUAL DE ANDROID

78. Alternativamente a la actualización automática realizada por Android (o cuando ésta no está disponible para ciertos fabricantes u operadores de telefonía móvil), es posible realizar la actualización del sistema operativo de Android de forma manual mediante la descarga de los ficheros de actualización oficiales desde la web de Google.

79. Estos ficheros no son publicados oficialmente, aunque su ubicación está disponible desde numerosas fuentes en Internet. Existe una lista no oficial (incompleta) con los ficheros de actualización proporcionados por Google y los diferentes fabricantes de dispositivos móviles basados en Android [Ref.- 65].

80. Por motivos de seguridad, las descargas siempre deben realizarse desde enlaces que referencien a la web oficial de Google, y es recomendable actualizar siempre hasta la última versión, como por ejemplo la asociada a Android 2.3.6 (GRK39F) [Ref.- 98].

81. El proceso de actualización requiere renombrar el fichero de actualización oficial descargado desde Google por "update.zip", y copiarlo en el directorio raíz de una tarjeta de almacenamiento externa (ej. tarjeta SD).

82. Una vez se ha introducido la tarjeta de almacenamiento externa en el dispositivo móvil, y estando éste apagado, debe encenderse el terminal manteniendo pulsada la tecla de bajar el volumen y pulsando la tecla de encendido simultáneamente.

83. Se mostrará una pantalla de arranque del sistema de color blanco (en la que aparecen tres androides patinando en la parte inferior), dónde el dispositivo móvil muestra que está buscando diferentes ficheros. Bajando a través de las diferentes opciones utilizando las teclas de volumen, debe seleccionarse la opción "Recovery", y pulsar el botón de encendido para seleccionarla.

Nota: en función de la versión de HBOOT, disponible en la parte superior de la pantalla de arranque del sistema de color blanco, puede ser necesario seleccionar el menú “Bootloader” antes de disponer de acceso al menú “Recovery”. La versión de HBOOT empleada por el dispositivo móvil utilizado para la elaboración de la presente guía es la 0.35.0017.

84. El dispositivo móvil rearrancará y mostrará una pantalla de recuperación que muestra un androide y un icono de peligro, con una admiración dentro de un triángulo (/!\). A continuación deben pulsarse los botones de encendido y de subir el volumen simultáneamente.
85. Una vez aparece el siguiente menú en color azul, debe seleccionarse la opción "apply sdcard:update.zip" mediante el botón de trackball. Cuando aparezca el mensaje de que se ha completado la instalación, "Install from sdcard complete", se debe seleccionar la opción "reboot system now" para reiniciar el dispositivo móvil con la nueva actualización aplicada, proceso que puede llevar algún tiempo.
86. Por ejemplo, en el dispositivo móvil empleado para la elaboración de la presente guía es posible aplicar este proceso de actualización manual para actualizar la versión de Android, por ejemplo, desde la versión 2.2.1 hasta la versión 2.2.2 [Ref.- 60], desde la 2.2.2 a la 2.3.3 [Ref.- 62], desde la 2.3.3 a la 2.3.4 [Ref.- 127], o desde la 2.3.4 a la versión 2.3.6 [Ref.- 98].

Nota: para aplicar la actualización a Android 2.3.x en el terminal empleado para la elaboración de la presente guía, Google Nexus One, es necesario en primer lugar realizar una restauración de la versión Android 2.2 compilación FRG33 (“PASSIMG.zip”), previa a la compilación FRF91 disponible de fábrica en el momento de su adquisición [Ref.- 129].

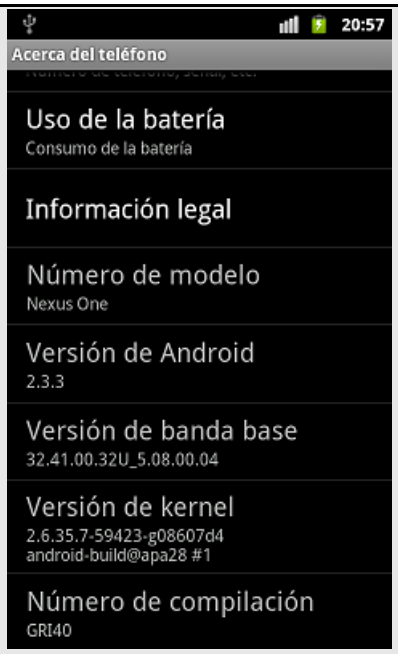
Los hashes de la versión Android 2.2 FRG33 son:

```
MD5: d90635c2d269c6a26f77ae1a681e5424
SHA-1: 228ec6b1caef92b6f3f3ecd17b71932c45c94b99
```

En caso contrario, al realizar la actualización manual a la versión 2.3.3 [Ref.- 126] directamente, el proceso de verificación de la actualización desde la tarjeta de almacenamiento externo generará errores de la firma (*signature*) del fichero “udpate.zip”:

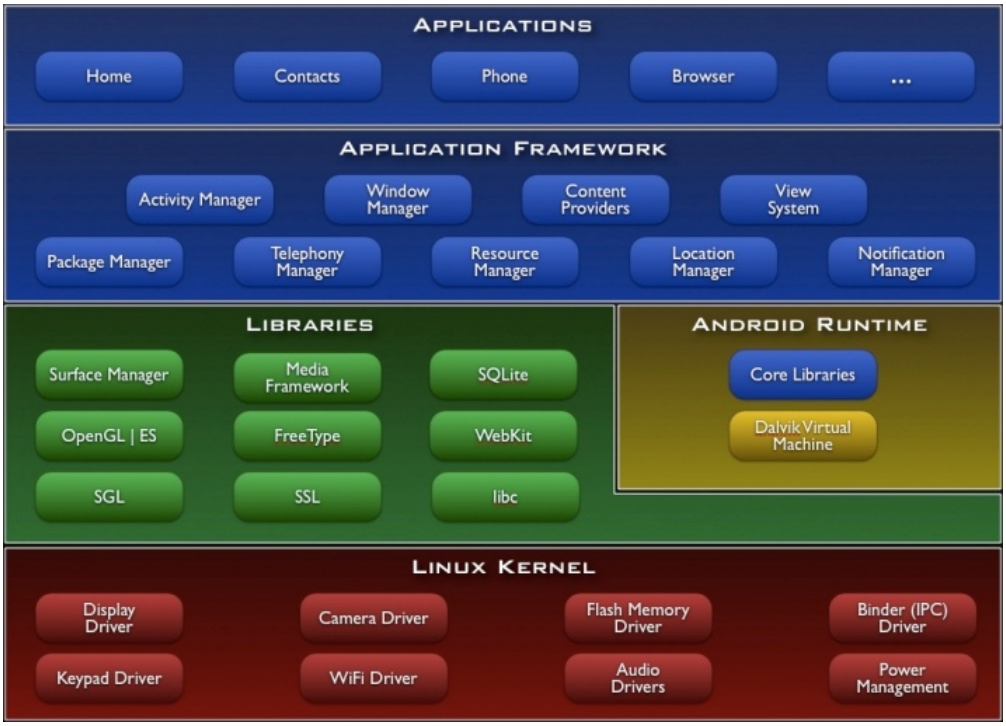
```
E: failed to verify whole-file signature
E: signature verification failed
Installation aborted.
```

Tras aplicar la actualización a Android 2.3.3, compilación GRI40 [Ref.- 126], las versiones, disponibles desde el menú “Ajustes – Acerca del teléfono”, son:
- Versión de Android: 2.3.3
- Versión de banda base: (ver imagen inferior): 32.41.00.32U_5.08.00.04
- Versión de kernel: (ver imagen inferior): 2.6.35.7-59423-g08607d4…
- Número de compilación: GRI40



5.2 MODELO Y ARQUITECTURA DE SEGURIDAD DE ANDROID

87. El modelo o arquitectura de seguridad de Android está basado en el sistema operativo Linux [Ref.- 17] y proporciona adicionalmente numerosas librerías y entornos de ejecución para las aplicaciones [Ref.- 11]:



88. Android aplica el principio de mínimo privilegio por defecto, donde cada aplicación únicamente dispone de acceso a sus propios componentes, incrementando así la seguridad general de la plataforma, y limitando las acciones que una aplicación puede realizar sobre otras aplicaciones, en el sistema o en su interacción con el usuario.

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

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

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

92. Adicionalmente, para ciertos permisos, como el de acceso a Internet, sería deseable disponer de suficiente granularidad en Android para poder autorizar a una aplicación a conectarse a Internet sólo a ciertos sitios web, y no a cualquier destino.

93. El siguiente ejemplo muestra los diferentes permisos solicitados por una aplicación Android concreta durante el proceso de instalación. En la aplicación de descarga de aplicaciones de Android, “Google Play”, tras pulsar el botón de instalación en la página de descripción de la aplicación, se solicita la aceptación por parte del usuario de los permisos demandados por la aplicación (por ejemplo, en “Play” versión “3.7.13”):

94. A través del botón “Ver todo” se puede obtener la lista completa de permisos solicitados por la aplicación; en este ejemplo incluyen, entre otros, acceso a los contactos, capacidades de telefonía (SMS y llamadas), controles de hardware, Ubicación, etc.:

95. Una vez la aplicación ha sido instalada, es posible ver los permisos de los que hace uso desde el menú “Ajustes – Aplicaciones – Administrar aplicaciones”, seleccionando la aplicación de la lista. En la parte inferior de la pantalla de información de la aplicación se encuentra la lista de permisos empleados (por ejemplo, de la aplicación “Play” versión 3.7.13):

96. Por defecto, las aplicaciones no disponen de ningún permiso. Si durante la instalación una aplicación no solicita ningún permiso no quiere decir que (debido a vulnerabilidades en Android) no pueda llevar a cabo acciones que afecten la privacidad del usuario [Ref.- 56], por lo que el usuario debe evaluar minuciosamente la instalación de nuevas aplicaciones incluso cuando éstas parecen no requerir ningún permiso.

97. Los permisos requeridos por una aplicación también están disponibles a través de su página web de descripción en el Google Play antes de su instalación, y en concreto, desde la pestaña “Permisos”:

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

99. En otros casos, la aplicación fraudulenta no incorpora ningún código dañino durante la instalación, y éste es añadido al dispositivo móvil posteriormente, en uno de los habituales procesos de actualización de las aplicaciones. Este proceso en Android no requiere de aprobación por parte del usuario de los permisos requeridos por la funcionalidad del nuevo código descargado, tal como demostró Jon Oberheide con "RootStrap" en el 2010 [Ref.- 87], ejecutando código nativo ARM fuera de la máquina virtual Dalvik (descrita posteriormente).

100. Mediante técnicas de ingeniería social es también posible instar al usuario a realizar la actualización de una aplicación maliciosa [Ref.- 124].

101. 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.

102. Por ejemplo, durante el 2011 se identificaron aplicaciones dañinas para Android qué, una vez autorizados los permisos que solicitaban, espiaban al usuario mediante la grabación de las conversaciones telefónicas en formato "amr" en la tarjeta SD [Ref.- 116], para ser posteriormente enviadas al atacante.

Nota: Los usuarios de dispositivos móviles Android de HTC deben prestar especial atención a una vulnerabilidad (CVE-2011-3975) que permite a todas las aplicaciones con el permiso de acceso a Internet (android.permission.INTERNET), muy habitual, poder acceder a la información de cuentas del usuario, última red conocida, localización del GPS, números de teléfono, datos de mensajes SMS, logs del sistema, etc. [Ref.- 115].

HTC ha incorporado a sus terminales Android un conjunto de herramientas de logging para recabar información, a través del paquete HTCLoggers.apk. Estas herramientas recopilan numerosa información sobre el uso del dispositivo móvil y el usuario, y facilitan la misma a cualquiera que la solicite a través de una conexión TCP/IP local (permiso de Internet).

103. Las aplicaciones en Android ejecutan de forma independiente en su propio entorno de ejecución o sandbox [Ref.- 16]. Cada aplicación está asociada a un usuario de sistema operativo diferente.

104. En el momento de su instalación, Android asigna a cada aplicación un identificador de usuario único (user ID y group ID, ID en adelante) a nivel de sistema operativo, y asocia todos los ficheros de la aplicación a dicho ID. De esta forma, sólo la aplicación tendrá acceso a sus ficheros asociados.

105. El ID es asignado y gestionado por Android y las aplicaciones no tienen conocimiento del mismo.

106. Excepcionalmente una aplicación puede crear datos y asignarles permisos de lectura y/o escritura globales, de forma que cualquier otra aplicación pueda acceder a ellos.

107. Cada aplicación ejecutada es un proceso (Linux) independiente a nivel de sistema operativo. El proceso es iniciado cuando cualquiera de los componentes de la aplicación

necesita ejecutarse, y es finalizado al no utilizarse más la aplicación o durante las tareas específicas de gestión (y liberación) de memoria del sistema operativo.

108. Cada proceso tiene asignada su propia máquina virtual (Virtual Machine o VM), por lo que el código de cada aplicación ejecuta de manera aislada al resto de aplicaciones.

109. Las aplicaciones pueden compartir datos con otras aplicaciones a través de la compartición del un mismo ID, y acceder a servicios del sistema operativo mediante la solicitud de permisos para interactuar con componentes y datos del sistema, como la lista de contactos del usuario, los mensajes SMS, la tarjeta de memoria externa, la cámara, el interfaz Bluetooth, disponer de acceso a Internet, el interfaz Wi-Fi, poder realizar llamadas de voz, etc.

110. La lista de permisos disponibles en Android está disponible en la definición del manifest (descrito posteriormente) donde se especifican todos los permisos requeridos [Ref.- 23].

111. Las aplicaciones que comparten un mismo ID tienen acceso a los mismos ficheros, pueden ejecutar en el mismo proceso y compartir la misma máquina virtual. Para ello deben haber sido firmadas con el mismo certificado digital, y desde el punto de vista de seguridad, podrían considerarse la misma aplicación.

112. Las aplicaciones de Android pueden estar constituidas por diferentes componentes, que permiten la interacción de la aplicación con el sistema y con el usuario, existiendo cuatro tipos de componentes: actividades, servicios, proveedores de contenidos y receptores de anuncios o eventos (broadcast) [Ref.- 16].

113. Los mensajes asíncronos de notificación o solicitud de petición entre componentes (de la misma o de distintas aplicaciones) para que se lleve a cabo una acción se denominan intents.

114. Cada aplicación Android dispone de un fichero de definición, o manifest (“AndroidManifest.xml”) [Ref.- 18], que contiene información sobre los diferentes componentes que constituyen la aplicación. Adicionalmente, el manifest incluye los permisos que requiere la aplicación (por ejemplo, acceso a Internet, lectura de la lista de contactos, etc.), las librerías (o APIs, Application Programming Interface) empleadas por la aplicación, tanto de sistema como externas (ej., librería de Google Maps), o los elementos o capacidades hardware y software empleados por la aplicación (ej. cámara, interfaz Bluetooth, pantalla táctil, etc.).

115. Estos requisitos hardware y software pueden ser empleados para decidir en qué dispositivos móviles puede instalarse y ejecutar una aplicación en función de sus necesidades, principalmente desde Google Play. Los requisitos pueden ser definidos como necesarios o requeridos, u opcionales, en cuyo caso la aplicación podrá ser instalada pero no hará uso de la funcionalidad asociada al requisito no disponible, como por ejemplo, la cámara.

116. Adicionalmente a los permisos estándar [Ref.- 23], existen una serie de permisos que requieren disponer de un nivel de protección elevado (protectionLevel) y que están disponibles únicamente para las aplicaciones existentes en la imagen de sistema de Android o que han sido firmadas con los mismos certificados que éstas [Ref.- 102].

117. Las librerías de sistema, denominadas API Level [Ref.- 19], e identificadas por su número o versión, están asociadas a la versión de Android. Por ejemplo, la API Level 8 corresponde a la versión 2.2 de Android.

118. Adicionalmente al código, las aplicaciones disponen de recursos (definidos mediante ficheros XML) asociados principalmente a la parte visual o interfaz gráfico de la aplicación, es decir, imágenes, ficheros de audio, contenidos en diferentes idiomas, etc.

119. Con el objetivo de incrementar el modelo y los mecanismos de seguridad disponibles en Android por defecto, la NSA publicó en enero de 2012 una versión de Android restringida, denominada SE Android, y equivalente en filosofía y funcionalidad a SE Linux para las plataformas Linux estándar [Ref.- 103].

120. Security Enhanced (SE) Android, SE Android, mejora la seguridad de Android limitando el daño que puede infringir un código dañino que afecte al dispositivo móvil, así como añadiendo capacidades para aislar las aplicaciones y ficheros entre sí.

5.3 GESTIÓN EMPRESARIAL DE DISPOSITIVOS BASADOS EN ANDROID

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

122. Google proporciona capacidades empresariales para la gestión de dispositivos móviles basados en Android a través de la plataforma Google Apps [Ref.- 12], accesibles desde un navegador web y que no requiere el despliegue de servidores dedicados para este propósito, al emplearse los servicios de Google “en la nube”.

123. Desde la versión 2.2 de Android los administradores de un dominio Google Apps (ediciones Premier o Business, Government o Education) disponen de capacidades para gestionar políticas de seguridad sobre los dispositivos móviles, incluyendo [Ref.- 88]:

- Borrado remoto de los datos del dispositivo móvil (*wipe*), en caso de haber sido perdido o robado (ver apartado “5.8. Eliminación de datos del dispositivo móvil”).

  Nota: Este proceso es equivalente a la opción “Restablecer datos de fábrica” disponible desde el menú “Ajustes – Privacidad”.

- Forzar la solicitud de un PIN o contraseña de acceso al dispositivo móvil.
- Definir la longitud mínima de los PINs o contraseñas de acceso.
- Forzar la utilización de letras y números en las contraseñas de acceso.
- Bloqueo del dispositivo móvil tras un periodo de inactividad, cuya duración puede ser también definida en la política de seguridad.

124. Adicionalmente, los usuarios de los terminales pueden de forma remota restaurar (o resetear) el PIN (ver apartado “5.4.4. Restauración de la contraseña de acceso”), hacer que suene el dispositivo móvil, bloquear el mismo, y localizar su ubicación.

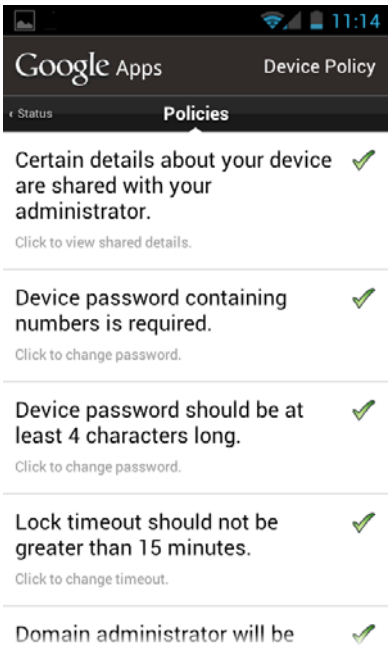
125. Para poder implantar estas políticas de seguridad es necesario que el dispositivo móvil disponga de la aplicación “Google Apps Device Policy”, disponible de forma gratuita en el Google Play (antes Android Market [Ref.- 13]).

126. La versión 2.0 (o superior) de la aplicación “Google Apps Device Policy” permite adicionalmente a los administradores definidos en Google Apps incluir como requisito de la política de seguridad el cifrado de los datos de los tablets basados en Android 3.0 o

smartphones de la versión 4.0 (ver apartado “5.6.1. Cifrado del dispositivo móvil”), opción disponible desde el panel de control asociado en Google Apps [Ref.- 94].

127. El acceso a la gestión de políticas para los usuarios empresariales de Google Apps está disponible desde el panel de control de Google Apps, y en concreto desde la pestaña “Service Settings” y la opción “Mobile”.

128. Las políticas también están disponibles desde el propio dispositivo móvil empleando el menú “Device Policy” de la aplicación “Google Apps Device Policy” [Ref.- 95]:

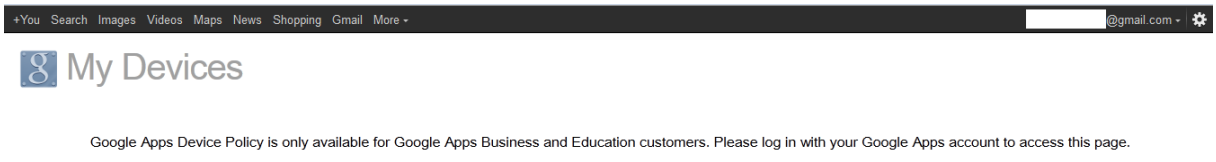


129. La capacidad de borrado remoto de datos sólo afecta al almacenamiento local del dispositivo móvil, no siendo posible actualmente eliminar también los datos de la tarjeta de almacenamiento externa conectada al dispositivo móvil.

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

131. El acceso a la gestión empresarial del dispositivo por parte de los usuarios finales, y no de los administradores del dominio asociado en Google Apps, puede realizarse mediante la sección “Mis dispositivos” (o “My devices”), disponible en la URL “http://www.google.com/apps/mydevices”, de la página web de Google Apps.

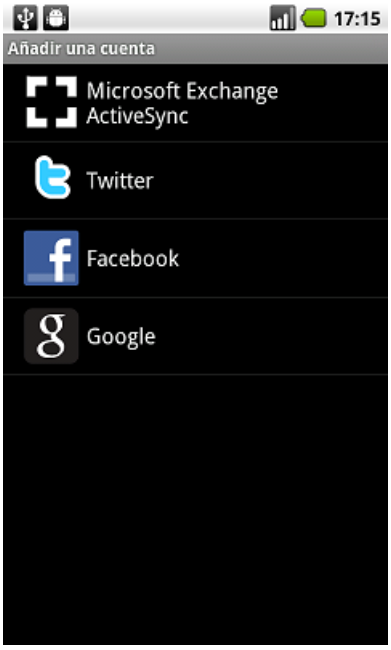
132. Sin embargo, el acceso a “My Devices” por parte de un usuario no asociado a un dominio de Google Apps no está permitido, obteniéndose el siguiente mensaje informativo:

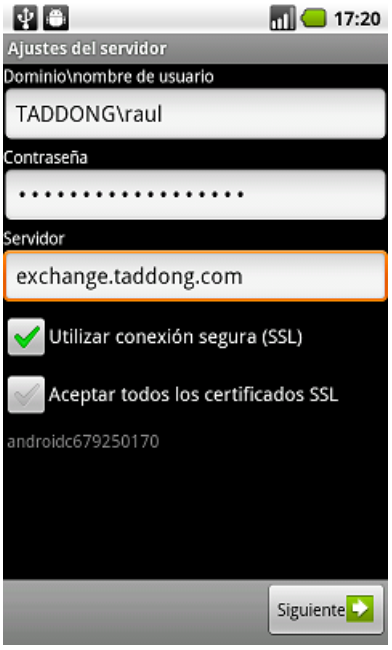


133. Microsoft, a través de Microsoft Exchange ActiveSync, también proporciona capacidades de gestión empresarial de dispositivos móviles Android [Ref.- 38], siendo posible la aplicación de políticas de seguridad [Ref.- 36] [Ref.- 39], incluyendo:

- Borrado remoto de los datos del dispositivo móvil (*wipe*), en caso de haber sido perdido o robado.
- Borrado local de los datos del dispositivo móvil (*wipe*), en caso de realizar un número determinado de intentos de acceso incorrectos.
- Forzar la solicitud de un PIN o contraseña de acceso al dispositivo móvil.
- Definir la longitud mínima de los PINs o contraseñas de acceso.
- Forzar la utilización de letras y números en las contraseñas de acceso.
- Bloqueo del dispositivo móvil tras un periodo de inactividad, cuya duración puede ser también definida en la política de seguridad.
- Gestión y permisos de dispositivos móviles que no soportan todas las políticas de seguridad de Exchange.

134. El dispositivo móvil Android puede ser configurado mediante la creación de una cuenta de Microsoft Exchange ActiveSync desde el menú “Ajustes – Cuentas y sincronización – Añadir cuenta – Microsoft Exchange ActiveSync”, siendo necesario proporcionar la dirección de correo electrónico del usuario, la contraseña, el dominio (ej. “DOMINIO\usuario”) y el servidor Exchange:





135. Para proteger las comunicaciones extremo a extremo entre el dispositivo móvil y el servidor Exchange es necesario habilitar la opción “Utilizar conexión segura (SSL)” (habilitada por defecto) y no habilitar la opción “Aceptar todos los certificados SSL” (deshabilitada por defecto).

Nota: La opción “Aceptar todos los certificados SSL” implica que Android aceptaría cualquier certificado digital recibido por parte del servidor Exchange (certificados autofirmados, expirados, o no válidos), permitiendo la realización de ataques *Man-in-the-Middle* (MitM) por parte de un atacante para interceptar y manipular el tráfico intercambiado.

136. Android versión 2.2 permite añadir múltiples cuentas de Microsoft Exchange.

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

5.4 ACCESO FÍSICO AL DISPOSITIVO MÓVIL

137. La posibilidad de disponer de acceso físico al dispositivo móvil permitiría a un potencial atacante acceder a los contenidos del mismo o hacer uso de los servicios de telefonía móvil disponibles.

138. Para evitar ambos tipos de acceso es posible fijar un PIN (Personal Identification Number) o clave de acceso tanto en la tarjeta SIM como en el propio dispositivo móvil.

5.4.1 PIN DE LA TARJETA SIM

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

140. Sin embargo, si sólo se establece el PIN en la tarjeta SIM y no en el dispositivo móvil (ver apartado “5.4.2. PIN, contraseña o patrón de acceso al dispositivo móvil”), aún es posible para un potencial atacante acceder al terminal directamente, incluyendo sus datos y aplicaciones, tras extraer el SIM del dispositivo móvil.

141. No es posible acceder al dispositivo móvil simplemente mediante el botón “Cancelar”, ya que Android continua solicitando el PIN de la tarjeta SIM para permitir el acceso al terminal si se ha fijado la restricción de usar PIN en la tarjeta SIM, siendo necesario extraer la tarjeta SIM previamente para disponer de acceso sin introducir el PIN:

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

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

144. Android permite emplear un PIN de la tarjeta SIM con un valor de 4 a 8 dígitos:

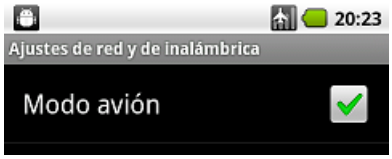
145. Pese a la debilidad de un PIN de 4 dígitos frente a ataques de adivinación o fuerza bruta, los operadores de telefonía móvil y fabricantes de dispositivos móviles implementan otros mecanismos para evitar este tipo de ataques, como el bloqueo de la tarjeta SIM tras tres intentos de acceso fallidos. En ese caso, para poder desbloquear la tarjeta SIM es necesario emplear una segunda clave de acceso denominada PUK (PIN Unlock Key).

146. Los dispositivos móviles Android 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 de la tarjeta SIM”), a través del menú “Ajustes – Ubicación y seguridad – Bloqueo de tarjeta SIM”:

Nota: El menú "Ajustes" empleado y referenciado en numerosas tareas de configuración del dispositivo Android está disponible desde el botón "Menú" (Menú) del dispositivo móvil, o desde el icono del Launcher (Launcher).

147. Se recomienda por tanto modificar el valor por defecto del PIN y fijar el PIN de la tarjeta SIM empleando un valor o secuencia de números que no sea fácilmente adivinable, es decir, excluyendo valores típicos como 0000, 1111 ó 1234.

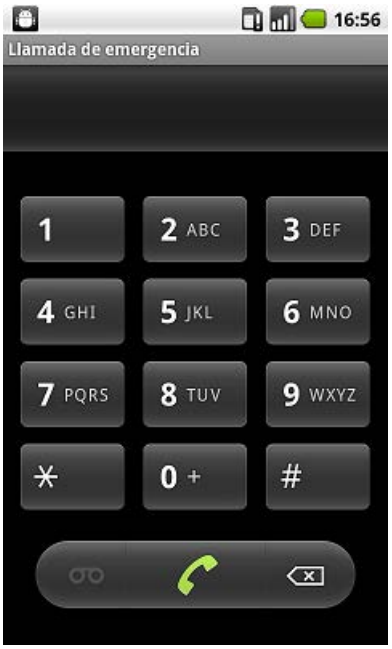
148. Debe tenerse en cuenta que cada vez que el dispositivo móvil sale del "Modo avión" (cuando este modo es desactivado; menú "Ajustes – Conexiones inalámbricas (y redes) – Modo avión"), solicitará el PIN de la tarjeta SIM al usuario desde la pantalla de bloqueo inicial, al activarse de nuevo los servicios de telefonía móvil:



5.4.2 PIN, CONTRASEÑA O PATRÓN DE ACCESO AL DISPOSITIVO MÓVIL

149. El PIN del dispositivo móvil bloquea el acceso no autorizado al terminal, incluyendo sus datos, capacidades de comunicación y aplicaciones.

150. Una vez el dispositivo móvil está bloqueado, únicamente se permite la realización de llamadas de emergencia (112) sin el código PIN o contraseña del terminal. Para ello es necesario marcar el número de teléfono de emergencias tras pulsar el botón "+ Llamada de emergencia":



151. Sin embargo, si únicamente se establece el PIN en el dispositivo móvil y no en la tarjeta SIM (ver apartado "5.4.1. PIN de la tarjeta SIM"), aún es posible para un potencial atacante acceder físicamente al terminal, extraer la tarjeta SIM y hacer uso de la misma en otro terminal, incluidos sus servicios y capacidades de telefonía móvil asociados.

152. Por defecto, los dispositivos móviles basados en Android no disponen de un PIN o contraseña de acceso para bloquear accesos no autorizados al terminal.

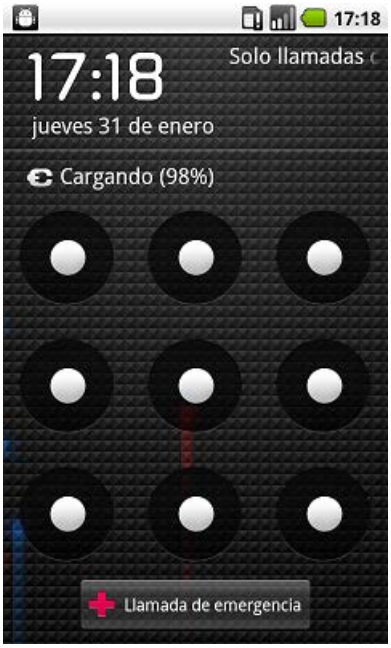
153. Se recomienda por tanto establecer el PIN o contraseña de acceso al dispositivo móvil a través del menú "Ajustes – Ubicación y seguridad – Bloqueo pantalla" (denominado "Cambio bloqueo pantalla" una vez se dispone de un mecanismo de bloqueo establecido).

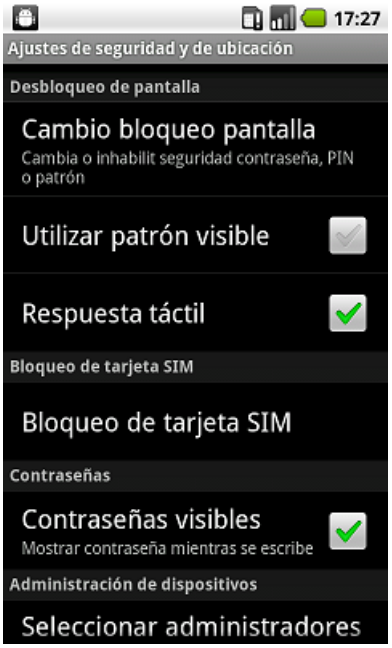
154. Android permite establecer tres tipos de contraseña de acceso (ver imagen inferior izquierda): un PIN numérico tradicional (opción "PIN"), compuesto por al menos cuatro dígitos (0-9), una contraseña (opción "Contraseña"), compuesta por al menos cuatro caracteres alfanuméricos (incluyendo símbolos de puntuación), y por tanto, opción más segura y recomendada, o un patrón de desbloqueo de pantalla, a través del cual es posible definir un patrón de movimiento (en una matriz ubicada en la pantalla del dispositivo móvil) para proceder a desbloquearlo.

155. Android proporciona la ayuda necesaria para que el usuario aprenda a crear un patrón de desbloqueo, siendo necesario que el patrón incluya al menos cuatro puntos de los nueve (matriz de 3 x 3) en los que se divide la pantalla del dispositivo móvil (ver imagen inferior derecha). Se recomienda emplear patrones de desbloqueo más complejos que hagan uso de un mayor número de puntos, como por ejemplo, de 6 a 9.

156. En caso de seleccionar un patrón de desbloqueo, es posible definir si el patrón es o no visible durante el proceso de desbloqueo del dispositivo móvil mediante la opción “Utilizar patrón visible” (habilitada por defecto), y si Android proporcionará una respuesta táctil durante la introducción del patrón mediante la opción “Respuesta táctil” (deshabilitada por defecto).

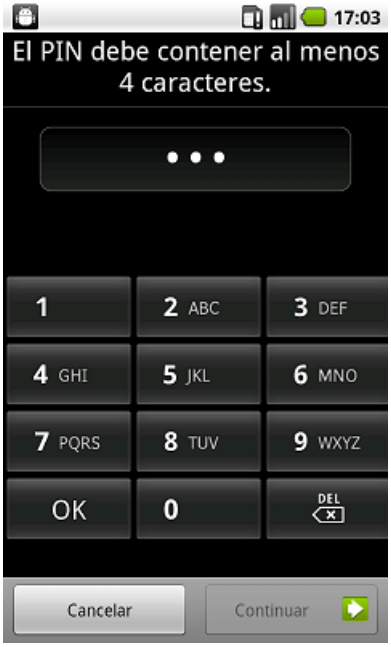
157. Desde el punto de vista de seguridad se recomienda no habilitar el uso de un patrón visible (que dibujaría las líneas de unión de los puntos que conforman el patrón), para evitar que alguien con acceso visual al dispositivo móvil durante el proceso de desbloqueo pueda obtener el patrón empleado. El uso de una respuesta táctil no tiene implicaciones desde el punto de vista de seguridad.

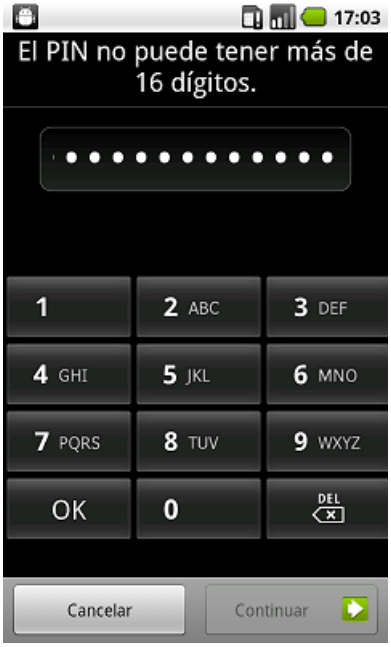


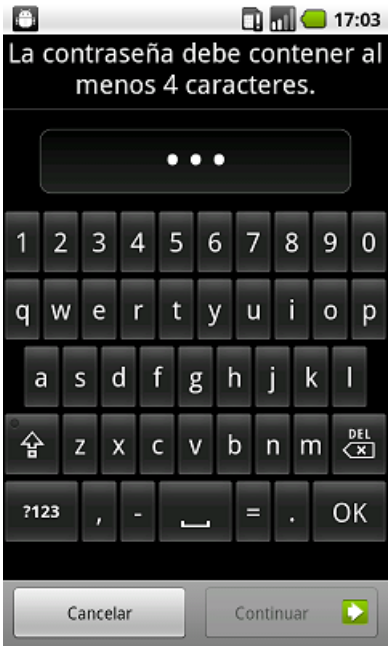


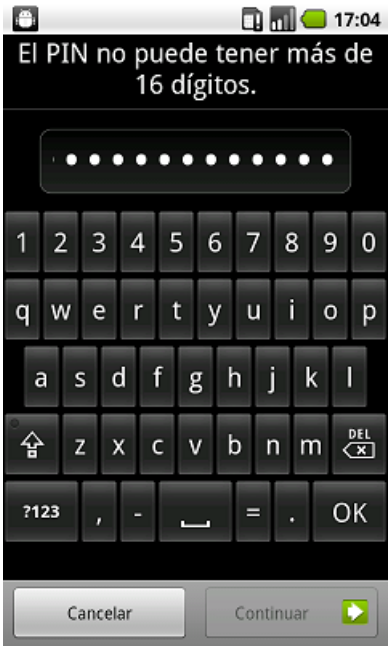
158. El tamaño mínimo tanto del PIN como de la contraseña alfanumérica en Android es de 4 dígitos o caracteres. El tamaño máximo de ambos es de 16 dígitos o caracteres

respectivamente. Por error el interfaz de Android hace referencia a la contraseña con el término PIN al alcanzar el tamaño máximo en la versión 2.2 (FRF91):









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

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

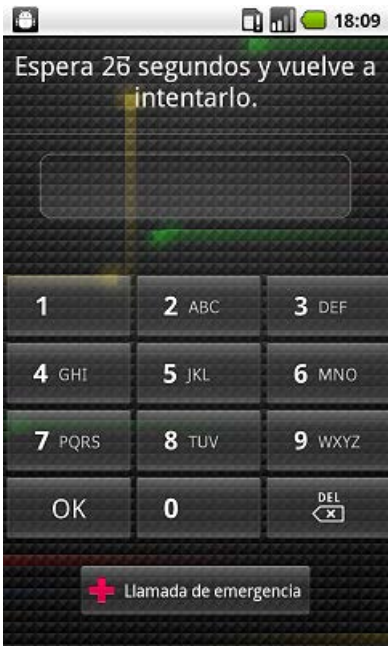
161. La única restricción de las contraseñas es que contengan al menos una letra, para diferenciarlas de los PINs, basados únicamente en dígitos.

162. Al emplear un PIN o contraseña de acceso, Android permite definir si se muestran o no los valores introducidos (únicamente el último dígito o carácter pulsado) mientras se escribe, a través de la opción “Contraseñas visibles” (habilitada por defecto).

163. Desde el punto de vista de seguridad se recomienda no habilitar el uso de contraseñas visibles, para evitar que alguien con acceso visual al dispositivo móvil durante el proceso de desbloqueo pueda obtener el PIN o contraseña empleada.

164. Pese a la debilidad de un PIN de 4 dígitos frente a ataques de adivinación o fuerza bruta, Android implementa un mecanismo que hace que sólo sea posible introducir cinco PINs, contraseñas o patrones incorrectos cada periodo de (al menos) 30 segundos.

165. Tras introducir cinco veces un PIN, contraseña o patrón incorrectos el dispositivo bloquea la posibilidad de acceso durante 30 segundos, notificando al usuario este hecho y mostrando un contador de cuenta atrás que indica los segundos pendientes hasta poder volver a intentar acceder al dispositivo (26 segundos en el ejemplo de la imagen inferior):



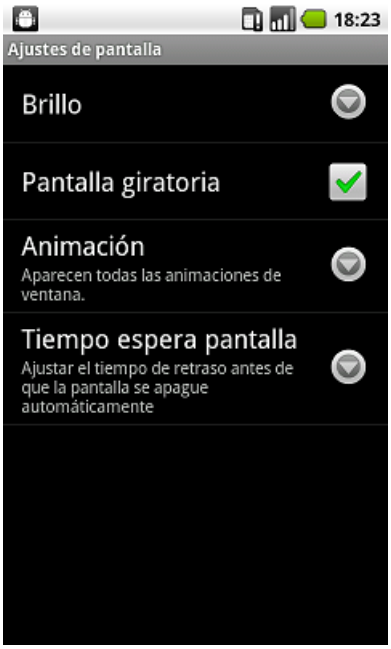
166. Este mecanismo permite la realización de ataques de adivinación o fuerza bruta del PIN, contraseña o patrón de acceso con un máximo de 600 intentos por hora. Este cálculo considera el caso ideal para el atacante, con un máximo de cinco intentos cada 30 segundos, despreciando el tiempo empleado para realizar los propios intentos de acceso.

167. Para proceder a modificar el PIN, contraseña o patrón de acceso al dispositivo móvil, en caso de disponer de un valor ya fijado, es necesario introducir el PIN, contraseña o patrón actual.

168. Una vez ha sido establecido el PIN, contraseña o patrón, el dispositivo móvil solicitará al usuario el PIN, contraseña o patrón para desbloquear el acceso al terminal cada vez que esté bloqueado, como por ejemplo al encender el terminal o tras un tiempo de inactividad.

169. Se recomienda por tanto establecer el bloqueo del dispositivo móvil tras un tiempo de inactividad, como por ejemplo 1 minuto (valor por defecto). El rango razonable debería estar entre 1 y 2 minutos, pero debe ser definido por la política de seguridad de la organización propietaria del terminal.

170. El tiempo de bloqueo de la pantalla por inactividad se establece a través del menú “Ajustes – Pantalla – Tiempo espera pantalla”:



171. Android no dispone de una opción que permita que la pantalla no se bloquee tras un periodo de inactividad (opción desaconsejada desde el punto de vista de seguridad en el caso de existir), siendo el periodo máximo de 30 minutos.

172. Como se puede apreciar en las siguientes dos imágenes, la pantalla de desbloqueo de Android permite diferenciar visualmente entre las tres configuraciones de desbloqueo del terminal (PIN, contraseña o patrón), lo que puede facilitar a un potencial atacante una primera aproximación al nivel de seguridad existente en el dispositivo móvil:

173. Adicionalmente, es posible establecer éstos y otros parámetros de configuración asociados al proceso de desbloqueo del dispositivo móvil a través de las políticas de seguridad de Google Apps (ver apartado “5.3. Gestión empresarial de dispositivos basados en Android”).

174. Cuando se establece un PIN, contraseña o patrón de acceso al dispositivo móvil, si el modo de depuración está habilitado (ver apéndice "Apéndice B: Captura de la pantalla en Android") es posible acceder al terminal mediante el interfaz USB, por ejemplo para capturar su pantalla, intercambiar datos, gestionar sus ficheros, instalar aplicaciones y leer datos del registro de actividades, sin necesidad de desbloquear el dispositivo móvil. Un atacante, mediante acceso físico al terminal, podría realizar múltiples tareas de administración del dispositivo móvil sin conocer la contraseña de acceso.

175. Se recomienda por tanto desde el punto de vista de seguridad deshabilitar el modo de depuración mediante el menú "Ajustes – Aplicaciones – Desarrollo", deshabilitando la opción "Depuración USB".

176. Una vez fijados tanto el PIN en la tarjeta SIM como en el dispositivo móvil, al encender el terminal, el dispositivo móvil solicitará el PIN de la tarjeta SIM y después el del terminal, en este orden:

177. Pese a que la obligatoriedad de introducir dos PINs (o contraseñas) diferentes puede suponer una molestia para el usuario, cuyos valores desde el punto de vista de seguridad se recomienda sean distintos, es necesario establecer ambos niveles de seguridad para que, tanto la tarjeta SIM y sus servicios asociados, como el dispositivo móvil y sus datos asociados, estén protegidos.

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

179. Adicionalmente a los métodos de acceso analizados y con el objetivo de introducir las nuevas capacidades disponibles en las últimas versiones de Android, cabe reseñar que la versión 4.0 de Android ("Ice Cream Sandwich") añade control de acceso mediante reconocimiento facial [Ref.- 83], denominado "Face Unlock". Este sistema es inseguro ya que es posible desbloquear el dispositivo móvil utilizando una imagen o foto del usuario:

5.4.3 DESBLOQUEO DE ANDROID MEDIANTE SCREEN LOCK BYPASS

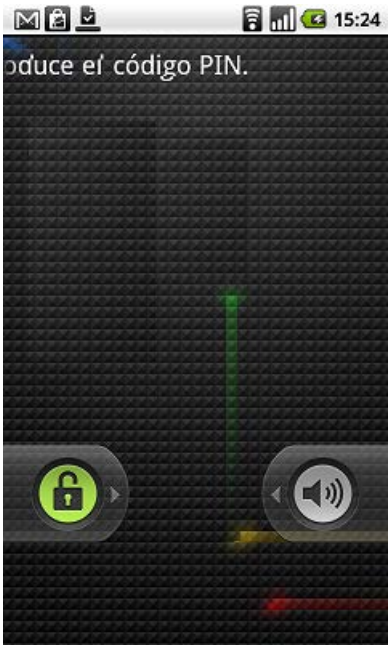
180. Mediante la instalación remota de una aplicación desde la web de Google Play (ver apartado “5.19.1. Instalación remota de aplicaciones”) es posible desbloquear un dispositivo móvil Android que se encuentre bloqueado y para el que no se conoce el PIN, contraseña o patrón de acceso.

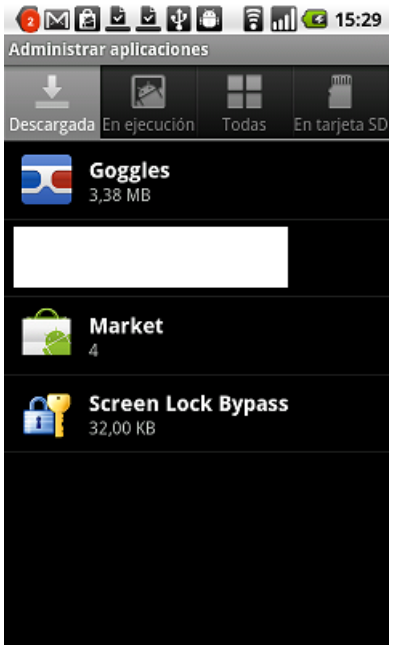
181. La aplicación que permite este tipo de acción se denomina “Screen Lock Bypass” [Ref.-74] y está disponible públicamente en Google Play.

182. Se han identificado escenarios en los que si el terminal está bloqueado y no se dispone del código de acceso no es posible resetear el dispositivo móvil. Un usuario legítimo podría utilizar esta aplicación para desbloquear su propio dispositivo móvil si ha olvidado el PIN, contraseña o patrón de acceso, y desea hacer copia de seguridad de los datos contenidos en el terminal.

183. Este desbloqueo remoto puede llevarse a cabo por parte de un atacante simplemente si consigue las credenciales de acceso a la cuenta principal de Google del usuario que está configurada en el dispositivo móvil Android, ya que es el único elemento necesario para instalar la aplicación de forma remota desde la web de Google Play.

184. Una vez “Screen Lock Bypass” ha sido instalada, el evento de instalación de cualquier otra aplicación (como la aplicación “Goggles” en el ejemplo inferior) permitirá su ejecución, y llevará a cabo el desbloqueo de la pantalla del dispositivo móvil previamente bloqueado (ver imagen inferior izquierda) sin conocer el PIN, contraseña o patrón de desbloqueo. El dispositivo móvil mostrará la pantalla en la que se encontraba antes del bloqueo (ver imagen inferior derecha):





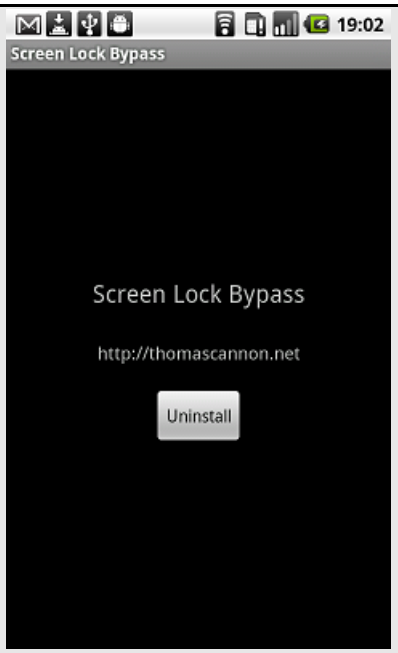
185. La instalación de las aplicaciones desde la web de Google Play se lleva a cabo de forma automática en el dispositivo móvil Android y sin ninguna intervención por parte del usuario, únicamente dejando constancia en la barra de notificaciones del dispositivo móvil:

Nota: Una vez la aplicación "Screen Lock Bypass" ha sido instalada y se ha empleado para desbloquear el dispositivo móvil, éste no volverá a bloquearse, incluso aunque se apague la pantalla o el terminal sea apagado completamente. La aplicación emplea el método "disableKeyguard()" del "KeyguardManager", pero deja la protección deshabilitada a propósito.

El procedimiento para deshabilitar el bloqueo de la pantalla también influye sobre el botón para acceder directamente a la pantalla principal, y sobre la posibilidad de introducir el PIN de desbloqueo de la tarjeta SIM, no siendo posible tras reiniciar el dispositivo.

Sin embargo, el mecanismo de bloqueo de pantalla sigue habilitado en los ajustes y para cambiar su configuración es necesario introducir el PIN, contraseña o patrón de desbloqueo (supuestamente desconocido). Por tanto, el bloqueo de pantalla del dispositivo queda en un estado inconsistente, dónde no es posible configurarlo, pero la protección no es efectiva.

Es posible desinstalar la aplicación desde el "Launcher", a través de su icono asociado (ver imagen inferior izquierda), o desde el menú "Ajustes – Aplicaciones – Administrar aplicaciones", seleccionando la aplicación de la lista (ver imagen inferior derecha):



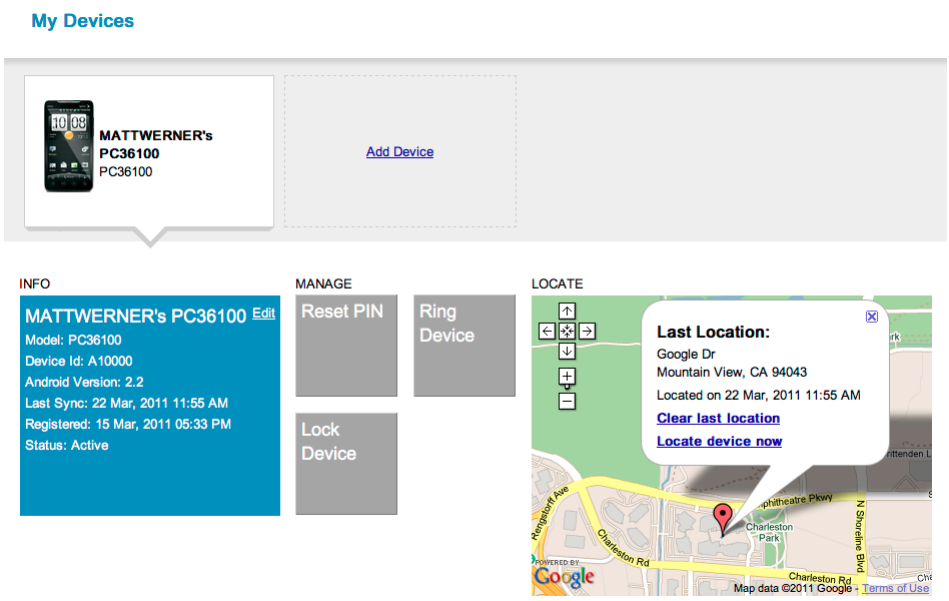
Tras desinstalar la aplicación "Screen Lock Bypass", pese a que se genere un mensaje que indica que la desinstalación no se ha realizado con éxito, la protección del bloqueo de la pantalla vuelve a ser habilitada automáticamente.

El proceso de desinstalación de una aplicación en Android no genera ningún tráfico hacia Google sobre dicha operación, por lo que la aplicación desinstalada seguirá apareciendo en la pestaña de "Pedidos" de la cuenta del usuario en la web de Google Play, reflejándose que fue instalada en alguna ocasión.

5.4.4 RESTAURACIÓN DE LA CONTRASEÑA DE ACCESO

186. A través de las capacidades empresariales para la gestión de dispositivos móviles basados en Android proporcionadas por Google a través de la plataforma Google Apps (ver apartado "5.3. Gestión empresarial de dispositivos basados en Android"), es posible llevar a cabo de forma remota la restauración (o reset) del PIN o contraseña de acceso y desbloqueo del dispositivo móvil desde la versión 2.2 de Android [Ref.- 94].

187. La sección "Mis dispositivos" (o "My devices"), disponible en la URL "http://www.google.com/apps/mydevices", de la página web de Google Apps dispone de una opción para llevar a cabo la restauración del PIN ("Reset PIN") [Ref.- 95]:



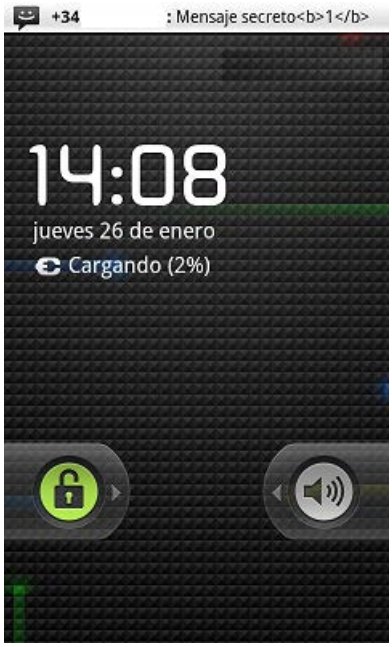
188. Esta funcionalidad permite a los usuarios de Google Apps la generación de un nuevo PIN o contraseña para disponer de acceso al dispositivo móvil, por ejemplo, cuando el acceso al dispositivo móvil está protegido por PIN (o contraseña) y el usuario olvida dicho PIN (o contraseña).

189. El proceso se basa en la generación y utilización de un nuevo PIN que permita al usuario desbloquear el dispositivo móvil y establecer una nueva clave de acceso (PIN o contraseña) sin tener que eliminar los datos del dispositivo móvil (wipe).

5.5 PANTALLA DE DESBLOQUEO: PREVISUALIZACIÓN DE DATOS

190. La pantalla de desbloqueo del terminal (lock screen) en Android permite, sin necesidad de introducir el PIN o contraseña de acceso y, por tanto, sin necesidad de desbloquear el teléfono, junto a la hora y la fecha, la previsualización del nombre del operador de telecomunicaciones y de la barra de estado, que incluye los iconos de conectividad y de notificaciones.

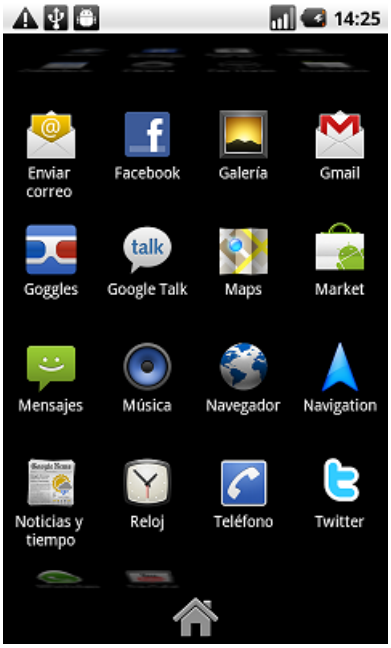
191. La pantalla de bloqueo puede desvelar por tanto información potencialmente confidencial a un potencial atacante, pero sólo temporalmente. Por ejemplo, en el caso de recibirse un mensaje SMS, el comienzo del mismo es mostrado durante un segundo en la barra de estado. La información del SMS mostrada incluye el número de teléfono del remitente y los primeros caracteres del mensaje en la parte superior de la pantalla de desbloqueo:

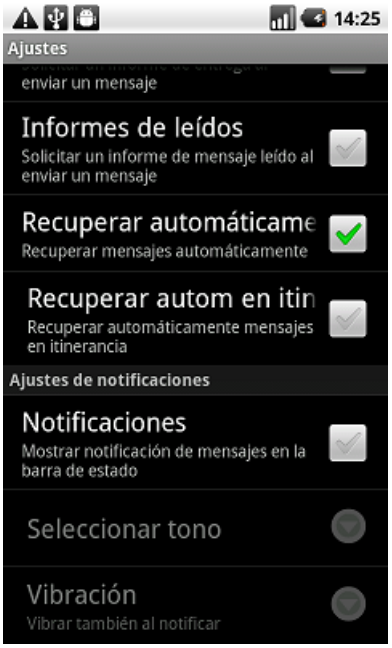


192. Desde el punto de vista de seguridad, esta funcionalidad de previsualización podría permitir a un potencial atacante la lectura de información de mensajes SMS simplemente con poder tener acceso visual a la pantalla del dispositivo móvil en el momento en que son recibidos.

193. Debido a las limitaciones de tiempo asociadas al proceso encargado de mostrar los mensajes SMS, el riesgo es reducido.

194. Desde el punto de vista de seguridad, en el caso de gestionar información sensible y confidencial, se recomienda deshabilitar esta previsualización mediante el menú de "Ajustes" de la aplicación de "Mensajes" (accesible desde el "Launcher"), disponible a través del botón "Menú" una vez la aplicación se encuentra en ejecución:





195. La opción "Notificaciones" debe ser deshabilitada para que al recibirse un mensaje SMS éste no sea previsualizado en la pantalla de desbloqueo del terminal. Como resultado, no se

notifica de ninguna forma (ni mediante un aviso acústico) al usuario acerca de la recepción del mensaje, lo que implica limitaciones en la funcionalidad SMS del terminal.

5.6 CIFRADO DE DATOS EN ANDROID

5.6.1 CIFRADO DEL DISPOSITIVO MÓVIL

196. Android, versiones 2.x, no dispone de capacidades para el cifrado de los datos almacenados en la memoria interna o el sistema de ficheros completo del dispositivo móvil de forma nativa.

197. Existen numerosas aplicaciones de cifrado en Google Play (ej. OpenPGP para Android, AGP) que permiten el cifrado de sus propios datos, como por ejemplo notas, información confidencial o contraseñas, pero no de la totalidad del dispositivo móvil.

198. La versión 3.0 de Android ("Honeycomb") [Ref.- 31], orientada a dispositivos móviles de tipo tablet, añade capacidades de cifrado nativas a los dispositivos móviles basados en Android, junto a otras mejoras en las políticas de cifrado y de contraseñas (complejidad, expiración e histórico). Esta opción está también disponible en versiones posteriores, como Android 4.x para teléfonos móviles o smartphones.

199. La opción "Encrypt tablet" está disponible desde el menú "Ajustes – Ubicación y seguridad", disponible por ejemplo en el modelo Motorola Xoom (tablet).

200. La opción de cifrado también está disponible en versiones posteriores como Android 4.0 para teléfonos móviles o smartphones, tanto del teléfono como de la tarjeta de almacenamiento externa de forma separada, permitiendo excluir del proceso de cifrado los archivos multimedia. Para poder ejecutar dicho cifrado, el sistema exige la definición de una contraseña de desbloqueo de al menos 6 caracteres, conteniendo al menos un número.

Nota: Algunos fabricantes de dispositivos móviles, como Motorola, han anunciado la disponibilidad de soluciones propietarias para el cifrado transparente tanto de la memoria interna del terminal como de las tarjetas de almacenamiento externas, empleando AES-128 y siendo necesario disponer de una contraseña de acceso al dispositivo móvil. Estas soluciones solo aplican a modelos concretos de Android [Ref.- 29] de este fabricante.

Otras soluciones propietarias, como WhisperCore, proporcionadas por terceras compañías de forma gratuita para uso personal, habilitan la posibilidad de cifrar tanto el dispositivo móvil Android (la partición de datos del dispositivo) como, opcionalmente, las tarjetas externas [Ref.- 32] mediante AES-256 y una contraseña de cifrado. Inicialmente la solución sólo está disponible para el modelo de terminal Nexus S.

Adicionalmente, existen soluciones de código abierto, en fase de pruebas, como Guardian Project, la versión para Android de LUKS (Linux Unified Key Setup) en Linux [Ref.- 30].

201. Se recomienda por tanto, en el caso de disponer de las capacidades necesarias, habilitar el cifrado del dispositivo móvil con el objetivo de evitar ataques de acceso a los datos en caso en el que un potencial atacante disponga de acceso físico al dispositivo móvil y desconozca el PIN o contraseña de acceso.

5.6.2 CIFRADO DE LAS TARJETAS DE ALMACENAMIENTO EXTERNAS

202. Android, versiones 2.x, no dispone de capacidades para el cifrado de los datos que vayan a ser guardados en tarjetas de almacenamiento externas de forma nativa.

203. La mayoría de las soluciones de cifrado existentes (ver apartado "5.6.1. Cifrado del dispositivo móvil") contemplan tanto la protección o cifrado de la memoria interna del dispositivo móvil como de las tarjetas de almacenamiento externas.

204. Con el objetivo de evitar el acceso a los datos almacenados en tarjetas externas por parte de un potencial atacante, se recomienda, en el caso de disponer de las capacidades necesarias, habilitar esta opción de cifrado.

205. Adicionalmente debe tenerse en cuenta que el sistema de ficheros (FAT o FAT32) empleado por defecto en la tarjeta de almacenamiento externa no establece permisos e impone restricciones, por lo que cualquier aplicación con permisos sobre la tarjeta dispondrá de acceso a todos los datos almacenados en ella.

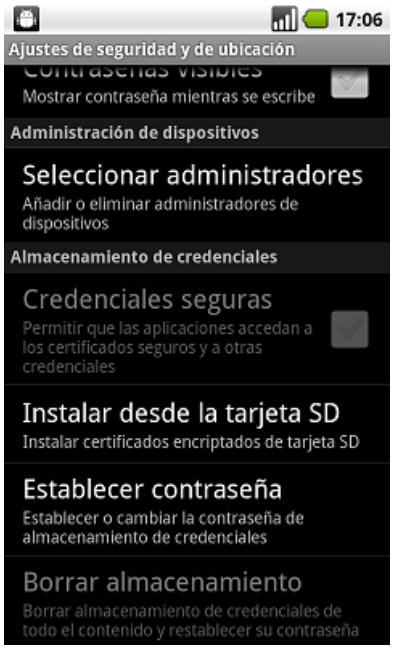
206. La disponibilidad de una tarjeta de almacenamiento externa en el dispositivo móvil (así como la memoria total y disponible en la misma) puede ser confirmada a través del menú "Ajustes –Almacenamiento", y concretamente bajo la sección "Tarjeta SD":

5.7 GESTIÓN DE CERTIFICADOS DIGITALES Y CREDENCIALES EN ANDROID

5.7.1 CERTIFICADOS DIGITALES Y CREDENCIALES DEL USUARIO

207. Android dispone de un repositorio (o almacén) de credenciales, también denominado "almacenamiento de credenciales", protegido por mecanismos de cifrado, dónde se almacenan los certificados digitales, contraseñas y otras credenciales, como por ejemplo las asociadas a redes VPN y redes Wi-Fi.

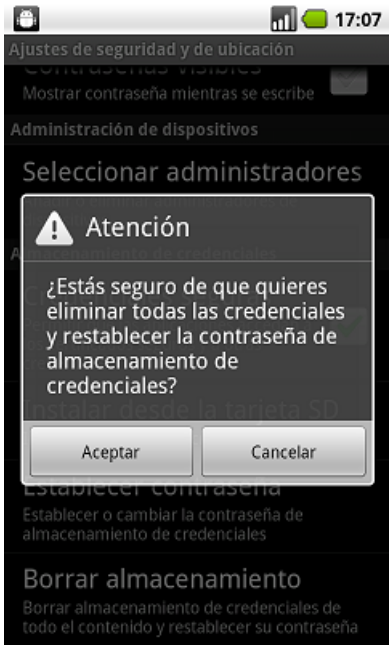
208. La contraseña de acceso al repositorio de credenciales se establece a través del menú "Ajustes – Ubicación y seguridad" mediante la opción "Establecer contraseña":



209. La contraseña del repositorio de credenciales debe tener una longitud mínima de 8 caracteres y su longitud máxima puede ser de (al menos) 50 caracteres. Android no impone ninguna restricción respecto a su contenido (números, letras mayúsculas y minúsculas, símbolos, etc.).

210. Se recomienda establecer una contraseña suficientemente larga y compleja (ej. frase de paso o passphrase) para proteger el repositorio de credenciales.

211. Es posible restablecer la contraseña del repositorio de credenciales, acción que conlleva el borrado de todas las credenciales existentes, mediante el menú “Ajustes – Ubicación y seguridad” y la opción “Borrar almacenamiento”:



212. La opción “Credenciales seguras” (del mismo menú) permite habilitar o deshabilitar el repositorio de credenciales, es decir, que las aplicaciones puedan acceder al repositorio cifrado del dispositivo móvil (habilitada por defecto una vez se establece la contraseña del repositorio). Si no se ha establecido una contraseña para el acceso al repositorio de

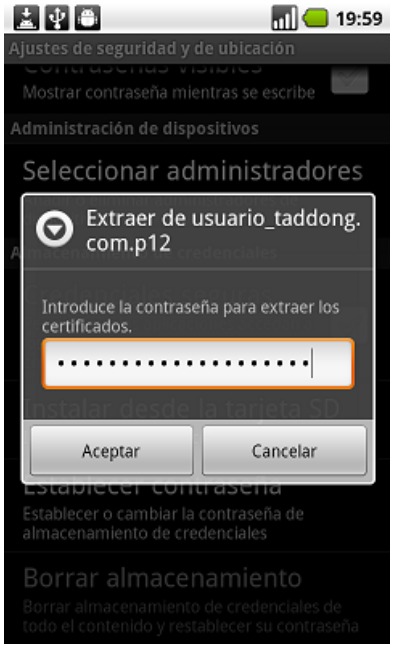
credenciales, esta opción no está disponible (aparece en color gris). Si se ha deshabilitado temporalmente el repositorio de credenciales, al habilitarlo de nuevo, Android solicitará la contraseña asociada.

213. Los contenidos del repositorio de credenciales pueden ser visualizados únicamente desde las aplicaciones que hacen uso de él, como por ejemplo, la configuración de redes Wi-Fi basadas en 802.1x EAP (TLS) a la hora de seleccionar el certificado de usuario a utilizar (ver apartado "5.13.3. Recomendaciones de seguridad para la conexión a redes Wi-Fi").

214. Los certificados digitales cliente asociados a redes VPN o redes Wi-Fi pueden ser obtenidos (e importados) desde un sitio web o desde la tarjeta de almacenamiento externa (en concreto, desde el directorio raíz de la misma) en formato PKCS#12 (extensión .p12).

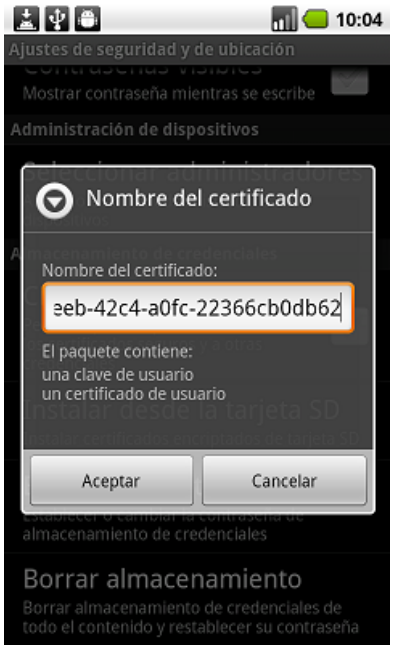
215. Si el certificado digital es obtenido desde la web, Android solicitará al usuario una contraseña para el repositorio de credenciales si aún no se ha establecido una.

216. Si el certificado digital es obtenido desde la tarjeta de almacenamiento externa (fichero con extensión .p12), es necesario emplear la opción "Instalar desde la tarjeta SD" disponible en el menú "Ajustes – Ubicación y seguridad", tal como se detalla en el proceso de importación de certificados digitales de la guía de usuario [Ref.- 24]. Android solicitará al usuario la contraseña que fue empleada para proteger el fichero .p12 que contiene el certificado digital y la clave privada (ver imagen inferior izquierda):



217. De nuevo, Android solicitará al usuario una contraseña para el repositorio de credenciales si aún no se dispone de una (ver imagen superior derecha), o solicitará la contraseña existente para acceder al repositorio de credenciales. Esta contraseña será necesaria siempre que se realicen operaciones con el repositorio de credenciales.

218. Durante el proceso de importación es posible modificar el nombre asignado por defecto al certificado digital por uno que permita al usuario identificarlo fácilmente:



219. El certificado digital importado será eliminado automáticamente de la tarjeta de almacenamiento externa una vez se ha completado la operación de importación.

220. El repositorio de credenciales es también empleado para almacenar contraseñas de redes Wi-Fi o VPN, solicitándose la contraseña asociada antes de almacenar la nueva configuración (ver apartados “5.13.3. Recomendaciones de seguridad para la conexión a redes Wi-Fi” y “5.16.6. VPN”).

221. El proceso de solicitud de contraseña tiene definido un máximo de 5 intentos antes de eliminarse por completo el contenido del repositorio de credenciales. Si se realizan dos intentos fallidos de acceso al proporcionar la contraseña, Android generará un mensaje de error indicando que sólo quedan 3 intentos antes de que se borre el repositorio:

222. Desde el punto de vista de las aplicaciones, Android proporciona dos métodos para la gestión de credenciales: Authenticator Manager (gestor de autentificación) y Shared Preferences (preferencias compartidas) [Ref.- 124].

223. El gestor de autentificación permite que las aplicaciones que disponen del permiso USE_CREDENTIALS puedan acceder al repositorio de credenciales y obtener un token de autentificación haciendo uso de las credenciales que fueron introducidas previamente por el usuario.

224. El método de preferencias compartidas permite a las aplicaciones almacenar y acceder a las credenciales del usuario, pero sin embargo esta información se almacena sin cifrar en un fichero XML bajo el directorio "shared_prefs" (opción desaconsejada desde el punto de vista de seguridad).

5.7.2 CERTIFICADOS DIGITALES RAÍZ DE ANDROID

225. En la versión 2 de Android, por defecto, no es posible acceder al listado de autoridades certificadoras reconocidas por el dispositivo móvil desde el interfaz gráfico de usuario. En la versión 4.0 si es posible acceder al repositorio de credenciales de confianza tanto de usuario como de sistema (en "Ajustes", "Seguridad", "Credenciales de confianza") pudiendo desactivar de forma independiente cada uno de los certificados de CA contenidos en el repositorio.

226. Mediante el SDK (Software Development Kit) de Android es posible extraer desde un ordenador, a través del puerto USB, el conjunto de certificados raíz asociado a las autoridades certificadoras (CAs) existente por defecto en el dispositivo móvil, usando los siguientes comandos que hacen uso, entre otros, del Android Debug Bridge (adb):

Nota: El apéndice "Apéndice B: Captura de la pantalla en Android" incluye los detalles y requisitos necesarios para la instalación y configuración del entorno de desarrollo de Android y Java para la realización de tareas más específicas, como las reflejadas en el presente apartado mediante "adb".

```
C:\> adb pull /system/etc/security/cacerts.bks cacerts.bks
844 KB/s (61391 bytes in 0.071s)

C:\> dir
 ...
   01/01/2011  18:30            61.391 cacerts.bks
```

227. Para poder inspeccionar el contenido del fichero "cacerts.bks" es necesario emplear la herramienta "keytool", disponible en el JRE (o JDK) estándar de Java [Ref.- 26]:

```
C:\>   keytool   -keystore   cacerts.bks   -storetype   BKS   -provider
   org.bouncycastle.jce.provider.BouncyCastleProvider          -storepass
   changeit -v -list > android_2.2_root_cas.txt
```

228. Previamente, para que "keytool" pueda gestionar ficheros BKS (BouncyCastle Key Store) es necesario copiar la librería "bcprov-jdk16-141.jar" [Ref.- 27] a la carpeta de librerías externas del JRE (o JDK) de Java, es decir, "$JAVA_HOME/lib/ext".

229. Como resultado se obtendrá un fichero de texto con todos los certificados digitales raíz con las autoridades certificadoras disponibles por defecto en Android, "android_2.2_root_cas.txt", que contiene 56 entradas en la versión 2.2 (FRF91).

230. Cada uno de los certificados raíz existentes en el almacén de autoridades certificadoras raíz puede ser extraído individualmente mediante el nombre del alias (o identificador numérico) de cada certificado, disponibles en el listado obtenido previamente:

```
C:\> keytool –exportcert –alias 1 -keystore cacerts.bks -storetype BKS -
    storepass                changeit                -provider
    org.bouncycastle.jce.provider.BouncyCastleProvider  –printcert  –file
    1.der
C:\> keytool –printcert –file 1.der
```

231. El ejemplo superior extrae el certificado digital asociado a la primera autoridad certificadora (ej. alias "1") del almacén de Android en formato binario DER, "1.der". Los datos del certificado pueden ser obtenidos mediante la opción "-printcert" de "keytool".

Nota: Es posible también añadir nuevos certificados digitales (ej. fichero.crt) al almacén de autoridades certificadoras de Android mediante la opción "-importcert" (y "-trustcacerts") de "keytool", para importar un certificado en el fichero "cacerts.bks", y mediante la opción "push" de "adb", para transferir el fichero "cacerts.bks" del ordenador al dispositivo móvil [Ref.- 44].

232. Android no dispone de ninguna opción en el interfaz de usuario que permita modificar la lista de autoridades certificadoras raíz, ni añadir nuevos certificados digitales a dicha lista (salvo a través del interfaz de depuración o de mensajes OTA, Over-the-Air), aunque podría existir la posibilidad de disponer de esta funcionalidad en futuras versiones [Ref.- 45].

233. El proceso para añadir certificados digitales raíz específicos para su utilización en conexiones Wi-Fi o VPN se detalla en el apartado "5.13.3. Recomendaciones de seguridad para la conexión a redes Wi-Fi".

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

5.7.3 FIRMA DIGITAL DE APLICACIONES EN ANDROID

235. Para que una aplicación sea considerada válida y pueda ser distribuida oficialmente a través del Google Play debe haber sido firmada digitalmente por el desarrollador [Ref.- 28].

236. Sin embargo, Android no realiza ninguna verificación adicional sobre la seguridad de la aplicación o la firma digital, salvo comprobar la fecha de expiración del certificado asociado a la firma en el momento de la instalación de la aplicación, permitiéndose certificados auto-firmados y no generados o validados por ninguna autoridad certificadora.

237. Por tanto, la firma digital de las aplicaciones Android no evita que las mismas contengan vulnerabilidades de seguridad o código malicioso. La firma únicamente permite vincular la aplicación a su desarrollador, asegura su integridad frente a modificaciones, y en algunos

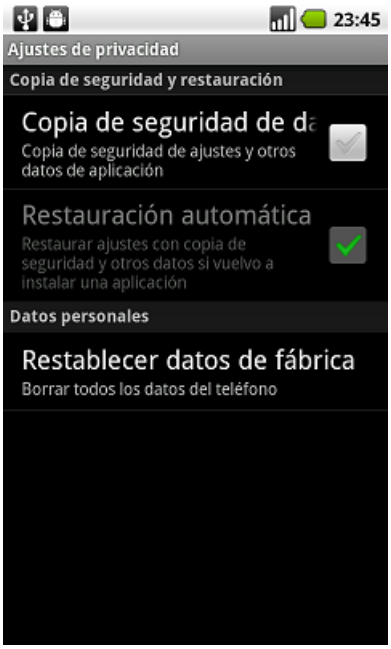
escenarios como la compartición del ID entre aplicaciones, define el nivel de privilegios de ejecución de la aplicación con respecto a otras aplicaciones.

238. La vinculación entre la aplicación y el desarrollador no ofrece fiabilidad desde el punto de vista de seguridad, ya que al permitirse emplear certificados auto-firmados, los mismos pueden contener información que no está asociada al desarrollador real de la aplicación.

5.8 ELIMINACIÓN DE DATOS DEL DISPOSITIVO MÓVIL

239. Android proporciona capacidades locales para la eliminación de todos los datos almacenados en el dispositivo móvil a través del menú "Ajustes – Privacidad", bajo la sección "Datos personales" y la opción "Restablecer datos de fábrica".

240. El proceso de restablecimiento eliminará todos los datos del teléfono, incluyendo cuentas de Google, configuración y datos de aplicaciones y del sistema, y aplicaciones previamente descargadas. 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:



241. 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 empresariales de dispositivos móviles Android (ver apartado "5.3. Gestión empresarial de dispositivos basados en Android"). El número máximo de intentos fallidos de acceso en Android 2.2 es de 31 [Ref.- 38].

242. Inicialmente Android no proporcionaba capacidades remotas para la eliminación de todos los datos almacenados en el dispositivo móvil en caso de que el mismo se encuentre en manos de un potencial atacante, proceso conocido como wipe (limpieza de datos). Sin embargo, desde la versión 2.2 de Android [Ref.- 34], estas capacidades están disponibles mediante las distintas soluciones de gestión empresarial de dispositivos móviles basados en Android.

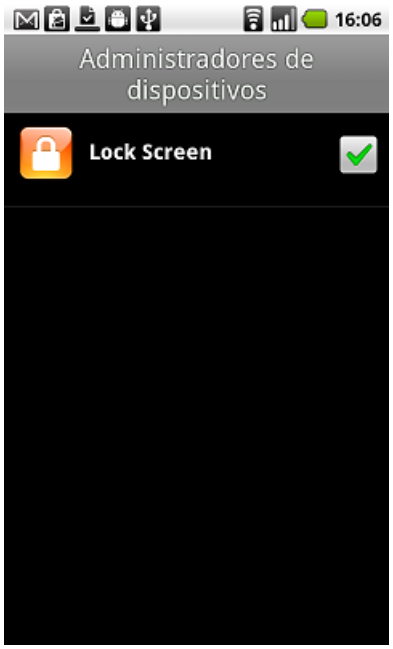
243. Tal y como se mencionaba en el apartado "5.3. Gestión empresarial de dispositivos basados en Android", desde la versión 2.2 de Android, los administradores de un dominio

Google Apps (ediciones Premier o Business, Government o Education) disponen de capacidades para borrar de forma remota los datos del dispositivo móvil (wipe), en caso de haber sido perdido o robado [Ref.- 88].

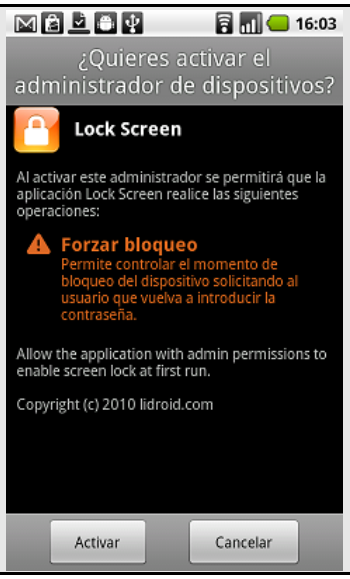
244. Igualmente ese apartado describe la gestión de dispositivos móviles Android a través de Microsoft Exchange y como ésta proporciona capacidades de borrado de datos remoto (wipe) similares [Ref.- 35].

245. Para que estas capacidades estén disponibles es necesario definir a la aplicación de gestión asociada como aplicación administradora del dispositivo móvil, y que así pueda hacer uso del interfaz "Device Administrator API" y controlar ciertos elementos de seguridad del terminal, como por ejemplo la longitud de la contraseña o el borrado remoto de datos [Ref.- 34].

246. Las aplicaciones (o cuentas) habilitadas como administradoras del dispositivo móvil están disponibles desde el menú "Ajustes – Ubicación y seguridad" bajo la sección "Administración de dispositivos" y la opción "Seleccionar administradores":



Nota: La imagen superior derecha muestra a modo de ejemplo la aplicación "Lock Screen", que requiere disponer de permisos como administradora del dispositivo móvil. La primera vez que es ejecutada solicita permisos para ser activada como tal, ya que la operación de bloqueo de la pantalla y solicitud de la contraseña o PIN requiere disponer de permisos de administrador:



247. 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.

248. 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 además se eliminarán los programas instalados, los datos y las configuraciones realizadas por el usuario.

Nota: Algunos fabricantes de dispositivos móviles basados en Android, como HTC, ofrecen servicios para algunos modelos de terminal, como el HTC Sense (www.htcsense.com), que permite la realización de copias de seguridad y la eliminación de los datos del dispositivo móvil de forma remota. Adicionalmente, otras soluciones comerciales (ver apartado "5.25. Aplicaciones de terceros: ") incluyen estas capacidades.

Dada la naturaleza de código abierto de Android, estas capacidades de borrado de datos remotos están también disponibles a través de aplicaciones gratuitas no oficiales, como "Autowipe Free" (http://forum.xda-developers.com/showthread.php?t=717469), y pueden ser activadas tras un número de intentos de acceso fallidos definido por el usuario, tras la recepción de un mensaje SMS con una contraseña, o tras el cambio de la tarjeta SIM.

5.9 CONFIGURACIÓN POR DEFECTO DEL DISPOSITIVO MÓVIL

249. El dispositivo móvil está configurado por defecto con valores fijados por el fabricante del sistema operativo, el fabricante del hardware o el operador de telefonía móvil, que pueden desvelar detalles del terminal o de su propietario.

250. Para evitar la revelación de información sensible, se recomienda modificar esos valores existentes por defecto por valores elegidos por su propietario.

251. El nombre del dispositivo móvil Android, o hostname al tratarse de un dispositivo Linux, no puede ser fijado a través de los menús de configuración. Su valor por defecto es "android_CÓDIGO", dónde "CÓDIGO" es un valor de 16 caracteres hexadecimales (ver análisis de la propiedad "net.hostname" posteriormente; ejemplo "android_2c9e795a34a0bc17").

252. El código corresponde al identificador de Android (ANDROID_ID), un valor de 64 bits (16 caracteres hexadecimales) generado aleatoriamente en el primer arranque del dispositivo móvil y que permanece constante durante toda la vida del dispositivo [Ref.- 47].

253. Únicamente los dispositivos móviles Android dónde se ha realizado el proceso de rooting permiten la modificación del nombre del dispositivo móvil (por ejemplo, mediante el comando "hostname" de Linux y la modificación de scripts de arranque) [Ref.- 89], pese a tratarse de una característica solicitada hace más de tres años (enero de 2009).

254. Para ello es necesario, como "root" (su), ejecutar los siguientes comandos en un terminal para obtener y fijar el nombre del dispositivo móvil Android, aunque el cambio no persistirá tras reiniciar el dispositivo:

```
$ getprop net.hostname
$ su
# setprop net.hostname NUEVO-NOMBRE
```

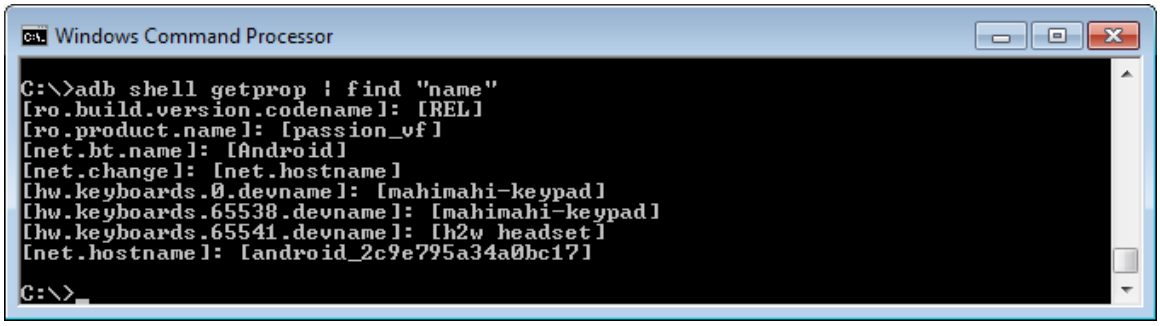
255. Las acciones de consulta también pueden ser llevadas a cabo a través del modo de depuración de Android y el comando "adb" (ver apéndice "Apéndice B: Captura de la pantalla en Android") mediante la ejecución del siguiente comando desde Windows:

```
C:\> adb.exe shell getprop net.hostname
android_2c9e795a34a0bc17
C:\> adb.exe root
adbd cannot run as root in production builds
```

256. La operación de modificación del nombre no se puede llevar a cabo con "adb" al ser necesario disponer de permisos de administración como el usuario "root". "adb" no puede ejecutar como "root" en versiones del sistema operativo Android de producción, es decir, en dispositivos móviles y no emuladores, salvo en dispositivos Android rooted.

257. En algunas versiones no oficiales de Android, como la versión rooted CyanogenMod 7 (CM7), es posible modificar de forma permanente el nombre del dispositivo a través del menú "Ajustes – Aplicaciones – Desarrollo – Nombre del dispositivo".

258. Las referencias internas a nombres empleadas por el dispositivo móvil Android por defecto pueden ser obtenidas a través del comando "adb" y sus capacidades de depuración de las propiedades del dispositivo móvil ("adb shell getprop"; ver apéndice "Apéndice B: Captura de la pantalla en Android"):



259. En caso de desvelarse el nombre del dispositivo en sus comunicaciones, como por ejemplo en el tráfico DHCP (donde se desvela el valor de la propiedad "net.hostname"; ver apartado "5.16.2. Seguridad en TCP/IP"), éste podría revelar detalles tanto del fabricante del dispositivo móvil, como por ejemplo el modelo del terminal, como del propietario. Estos datos serían muy útiles para un potencial atacante interesado en explotar vulnerabilidades en ese tipo concreto de dispositivo móvil o interesado en realizar ataques dirigidos hacia una persona concreta.

260. Adicionalmente, Android puede emplear otros nombres para el dispositivo móvil al hacer uso de diferentes servicios y tecnologías, como por ejemplo Bluetooth (ver apartado "5.12. Comunicaciones Bluetooth"), por lo que la configuración de ajustes de Bluetooth permite modificar su valor.

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

261. De ser posible en versiones futuras de Android, se recomienda modificar el nombre del dispositivo móvil por uno que no revele detalles ni del dispositivo móvil (fabricante o modelo) ni del propietario (evitando tanto referencias al nombre de la persona como de la organización asociadas al mismo), como por ejemplo "dm0001" (dispositivo móvil 0001).

5.10 LOCALIZACIÓN GEOGRÁFICA

262. Las capacidades de localización del dispositivo móvil a través 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.

263. El uso del GPS en el dispositivo móvil Android viene reflejado por los siguientes iconos:

	GPS is on
	Receiving location data from GPS

Nota: El dispositivo GPS en Android está activo únicamente cuando se está haciendo uso de una aplicación con capacidades de localización, es decir, que hace uso del GPS.

264. Desde el menú "Ajustes – Ubicación y seguridad", y en concreto desde la sección "Mi ubicación", es posible habilitar las capacidades de localización del dispositivo móvil, tanto mediante el módulo de GPS, opción "Utilizar satélites GPS" (habilitada por defecto), como mediante redes Wi-Fi y torres de telefonía móvil, opción "Usar redes inalámbricas" (deshabilitada por defecto):

265. En el caso de habilitar las capacidades de localización a través de redes inalámbricas (ver apartado "5.10.1. Servicio de localización de Google" y "5.10.2. A-GPS"), Android solicita confirmación por parte del usuario para recopilar los datos de las señales inalámbricas recibidas y la ubicación del terminal de forma anónima (ver imagen superior derecha).

Nota: Existen estudios 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 inalámbricas recibidas y la ubicación del terminal, se incluye un identificador único del dispositivo móvil [Ref.- 79], afectando 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 está disponible para su consulta a través de la API de Google y de páginas web externas [Ref.- 80], siendo posible conocer la ubicación de una red Wi-Fi a nivel mundial en base a su dirección MAC o BSSID.

266. Se recomienda deshabilitar 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.

5.10.1 SERVICIO DE LOCALIZACIÓN DE GOOGLE Y GOOGLE MAPS

267. Durante el proceso de configuración inicial asociado al dispositivo móvil empleado para la elaboración de la presente guía, incluso aunque se omita la asociación del dispositivo a una cuenta de Google, Android solicita al usuario si desea usar el servicio 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.

268. Se recomienda deshabilitarlas antes de completar el proceso inicial de configuración.

269. El servicio de ubicación o localización de Google, denominado Google Location, permite 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 los servicios de búsqueda (y otros) de Google.

270. La ubicación se obtiene a través de la información de localización disponible sobre torres 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 GPS.

271. Este servicio de ubicación con o sin GPS (mencionado en el apartado "5.10. Localización geográfica") es utilizado, entre otros, por la aplicación "Google Maps for Mobile" (GMM, http://m.google.com/maps), que en el caso del dispositivo móvil empleado para la elaboración de la presente guía, está disponible como aplicación por defecto a través del menú "Launcher – Maps".

Nota: La aplicación Google Maps requiere de una conexión de datos (telefonía móvil o Wi-Fi) para funcionar y acceder a la información cartográfica de los mapas.

272. Desde "Google Maps" es posible hacer uso de la información de localización, en concreto, desde el botón "Menú" y la opción "Mi ubicación", que centrará el mapa en la localización actual del usuario (identificada por una flecha azul).

273. Si se acepta el uso del servicio, la recopilación de información será activada y se permitirá su utilización por defecto por parte de las aplicaciones que hacen uso de los servicios de ubicación.

274. Es posible deshabilitar el servicio de ubicación de Google en cualquier momento desde el menú "Ajustes – Ubicación y seguridad", y en concreto mediante la opción "Usar redes inalámbricas".

275. Al hacer uso de aplicaciones que requieren conocer la ubicación del usuario, como "Google Maps", si han sido habilitadas se emplearán las capacidades para localizar la ubicación del dispositivo móvil incluso cuando no se dispone de GPS (o éste no está activo), a través de A-GPS, que emplea la información de localización disponible sobre torres de telefonía móvil (ver apartado "5.10.2. A-GPS"), y la funcionalidad extendida de Google mediante redes Wi-Fi.

276. El servicio de ubicación de Google integrado en Google Maps emplea conexiones HTTP (no cifradas) desde el dispositivo móvil hacia "mobilemaps.clients.google.com" ("/glm/mmap") y envía a Google información de las redes inalámbricas (incluyendo el nombre de red, SSID, y su dirección MAC, BSSID) y de las torres de telefonía (incluyendo el identificador de torre, y los códigos de área (LAC), operador de telefonía móvil (MNC) y país (MCC)) [Ref.- 57] existentes en el área de cobertura del dispositivo móvil.

277. En función de la versión de Android disponible, también se han identificado conexiones HTTP no cifradas hacia "www.google.com" y el recurso "/loc/m/api" para este servicio. Mediante peticiones POST HTTP el dispositivo móvil envía a Google numerosos detalles de la ubicación actual del usuario, incluyendo la dirección MAC (BSSID) y el nombre de todas las redes Wi-Fi visibles actualmente, junto al operador de telefonía empleado:

```
POST /loc/m/api HTTP/1.1
...
Content-Type: application/binary
Host: www.google.com
User-Agent: GMM/3.0 (passion FRF91); gzip
```

```
...."location,1.0,android,android,en_US.........g...4.......g:loc/ul....
    ."q.1.0.Mandroid/google/passion_vf/passion/mahimahi:2.2/FRF91/209740:
    user/release-keys*.es_ES2.....<OPERADOR TELEFONIA> .(.."..\
...
.00:01:02:03:04:05..WLAN ..........*
.00:01:02:03:04:06..Wireless ..........'
.00:01:02:03:04:07..WIFI ..........%
...
```

278. Este tipo de peticiones HTTP (a ambos recursos) también desvelan numerosos detalles del dispositivo móvil en sus cabeceras, como la plataforma (“android”), la versión de Android (“2.2”), el modelo de terminal (“HTC-passion-Nexus One”), idioma empleado (“es_ES”), o los detalles del navegador web (ver “User-Agent”), así como la aplicación empleada (Google Maps for mobile de Android, “gmm-android-vf-es”) y su versión (“4.3.0.07”), aparte de los detalles de la ubicación del usuario. Ver apartado “4. Entorno de aplicación de esta guía” para contrastar la información del dispositivo móvil empleado para la elaboración de la presente guía:

```
POST /glm/mmap HTTP/1.1
...
Host: mobilemaps.clients.google.com
User-Agent: Mozilla/5.0 (Linux; U; Android 2.2; es-es; Nexus One
Build/FRF91) AppleWebKit/533.1 (KHTML, like Gecko) Version/4.0 Mobile
Safari/533.1 (passion FRF91); gzip

.......F|]..es_ES..android:HTC-passion-Nexus One..4.3.0.07..gmm-android-
vf-es>..."
.426... .*.GMM...SYSTEM.........8K....
```

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

280. Se recomienda limitar el uso del servicio “Google Maps”, y específicamente su utilización sin emplear el GPS, ya que el servicio de ubicación a través de torres de telefonía y redes Wi-Fi desvela detalles privados del dispositivo móvil y su ubicación.

5.10.2 A-GPS

281. Assisted GPS (A-GPS) es un sistema de ayuda para mejorar la obtención de información de localización mediante GPS, y utiliza las torres de telefonía móvil para disponer de una estimación de la ubicación del dispositivo móvil más rápidamente.

282. El módulo A-GPS está disponible en dispositivos móviles Android con GPS, pero está deshabilitado por defecto. Como se describía en el apartado “5.10. Localización geográfica“, A-GPS puede ser habilitado mediante la opción “Usar redes inalámbricas” del menú “Ajustes – Ubicación y seguridad”.

283. La funcionalidad A-GPS envía tráfico hacia los servidores y puerto definidos en el fichero “gps.conf” (ver apartado “5.10.3. gpsOneXTRA”), por defecto TCP/7276 del servidor de Google “supl.google.com”.

284. Los servidores A-GPS pueden ser proporcionados por los operadores de telefonía móvil ("agps.operador.es" o "supl.operador.es"), qué normalmente sólo ofrecen su servicio A-GPS a través de la red de datos de telefonía móvil, para limitar su uso a sus clientes, y no permitir el acceso por parte de cualquiera desde Internet. Adicionalmente, algunos fabricantes de terminales proporcionan servidores A-GPS usando el estándar SUPL, arquitectura "Secure User Plane Location".

Nota: Pese a que el dispositivo móvil Android lleva a cabo la resolución de nombres (DNS) del servidor "supl.google.com", asociada a "mobile-agps.l.google.com", posteriormente emplea el servicio de ubicación de Google integrado en Google Maps, en lugar de la funcionalidad nativa de A-GPS.

285. Debe tenerse en cuenta que pese a que el uso del GPS esté seleccionado (opción "Utilizar satélites GPS"), hay escenarios en los que no es posible obtener señal de GPS (por ejemplo, en el interior de edificios), por lo que "Google Maps" hará uso de las capacidades de ubicación sin GPS si estás han sido habilitadas.

286. En resumen, se recomienda deshabilitar la funcionalidad A-GPS mediante la desactivación de la opción "Usar redes inalámbricas" 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, torre de telefonía a la que está asociado o redes Wi-Fi cercanas) a través del tráfico de datos destinado a los servidores A-GPS.

5.10.3 GPSONEXTRA

287. Con el objetivo de agilizar el proceso de localización de coordenadas del GPS y su precisión, el dispositivo móvil dispone de la funcionalidad asociada a la asistencia mediante gpsOneXTRA (aplicación conocida como QuickGPS en otras plataformas móviles).

288. Esta funcionalidad se conecta a un servidor web de "gpsonextra.net" (xtra1, xtra2 ó xtra3) para descargar la información semanal de la localización de los satélites GPS alrededor del planeta. Por defecto, la descarga automática de esta información está habilitada.

289. La descarga se lleva a cabo mediante HTTP (TCP/80) hacia los servidores mencionados previamente, descargándose el fichero "/xtra.bin". Para ello, Android emplea el siguiente agente de usuario que permite identificarle: "User-Agent: Android".

Nota: La configuración interna de Android tanto del servidor de tiempos NTP (ver apartado "5.16.2. Seguridad en TCP/IP"), como de los servidores de gpsOneXTRA y A-GPS (ver apartado "5.10.2. A-GPS") está disponible en el fichero "/system/etc/gps.conf" aunque no se dispone de posibilidad de configuración a través del interfaz gráfico de usuario. Ejemplo:

```
NTP_SERVER=europe.pool.ntp.org
XTRA_SERVER_1=http://xtra1.gpsonextra.net/xtra.bin
XTRA_SERVER_2=http://xtra2.gpsonextra.net/xtra.bin
XTRA_SERVER_3=http://xtra3.gpsonextra.net/xtra.bin
SUPL_HOST=supl.google.com
SUPL_PORT=7276
```

290. Las conexiones NTP ("europe.pool.ntp.org", udp/123), para la sincronización horaria, y gpsOneXTRA ("xtraN.gpsonextra.net", tcp/80), para incrementar la precisión de localización del GPS, se llevan a cabo cada vez que se enciende el dispositivo móvil y éste dispone de acceso a Internet.

291. Si no se desea que el dispositivo móvil realice las conexiones NTP, gpsOneXTRA y A-GPS indicadas, por motivos de seguridad y para limitar las conexiones de datos y la posible información revelada, será necesario modificar el fichero "gps.conf" a través del interfaz de depuración de Android desde un ordenador vía USB, empleando la utilidad "adb" (ver apéndice "Apéndice B: Captura de la pantalla en Android"). Este fichero de configuración sólo puede ser modificado en dispositivos móviles Android rooted, ya que el sistema de ficheros "/system" está montado como sólo lectura:

```
C:\> adb shell
$ cd /system/etc
cd /system/etc
$ mv gps.conf gps.conf.bak
mv gps.conf gps.conf.bak
failed on 'gps.conf' - Read-only file system
$ mount
...
/dev/block/mtdblock3 /system yaffs2 ro,relatime 0 0
```

292. La funcionalidad de dichos protocolos se verá afectada al ser deshabilitados.

5.10.4 OTRAS APLICACIONES QUE HACEN USO DE LA LOCALIZACIÓN

5.10.4.1 GOOGLE MAPS NAVIGATION

Las capacidades de localización también pueden ser empleadas por otras aplicaciones como Google Maps Navigation (http://www.google.com/mobile/navigation/), que en el caso del dispositivo móvil empleado para la elaboración de la presente guía, está disponible como aplicación por defecto a través del menú "Launcher – Navigation".

Nota: La aplicación Google Maps Navigation requiere de una conexión de datos (telefonía móvil o Wi-Fi) para funcionar y acceder a la información de los mapas y navegación.

293. El agente de usuario de Google Maps Navigation es "User-Agent: GoogleMobile/1.0 (passion FRF91); gzip".

5.10.4.2 GOGGLES

294. Las capacidades de localización también pueden ser empleadas por otras aplicaciones como Goggles (http://www.google.com/mobile/goggles/), que en el caso del dispositivo móvil empleado para la elaboración de la presente guía, está disponible como aplicación de Google Play (pese a estar referenciada como aplicación por defecto en la guía de usuario de Android [Ref.- 24]).

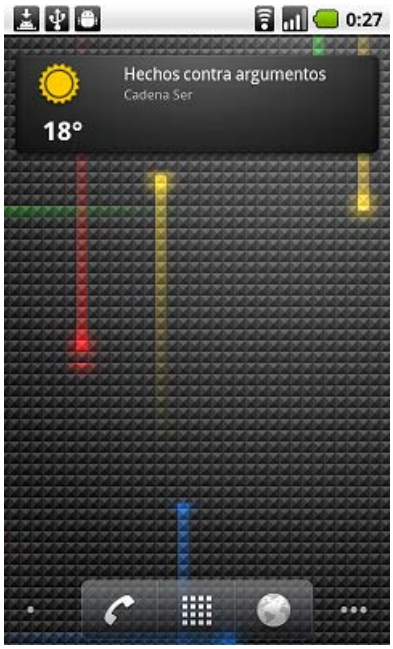
295. Goggles es una aplicación de realidad aumentada que permite realizar búsquedas en Google mediante fotografías en lugar de emplear términos de búsqueda. Para ello el usuario únicamente debe tomar una fotografía de algo que esté viendo o en lo que esté interesado, y emplear dicha fotografía para encontrar más información sobre su contenido (como por ejemplo cosas, lugares o negocios) a través de Google.

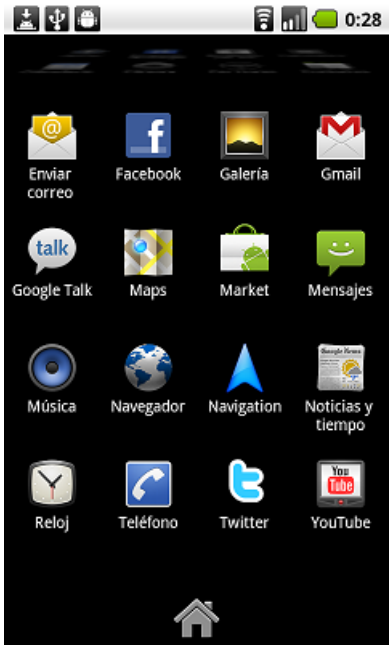
Nota: La aplicación Goggles requiere de una conexión de datos (telefonía móvil o Wi-Fi) para funcionar y acceder a la información de búsqueda en Google.

296. Googles puede ser empleada para obtener información de lugares y negocios cercanos al que nos encontramos en un momento determinado. Para ello hace uso de la información de localización del GPS del dispositivo móvil.

5.10.4.3 NOTICIAS Y TIEMPO

297. El widget disponible por defecto sobre noticias e información meteorológica (tiempo) está asociado a la aplicación "Noticias y tiempo" disponible bajo el mismo nombre desde el "Launcher":



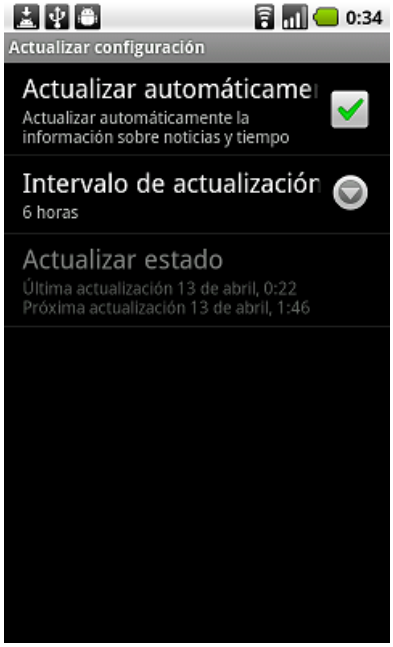


Nota: La aplicación "Noticias y tiempo" requiere de una conexión de datos (telefonía móvil o Wi-Fi) para funcionar y acceder a la información meteorológica y de noticias recientes.

298. El componente de la aplicación encargado de la información meteorológica (tiempo) puede hacer uso del servicio de ubicación. La configuración por defecto de tiempo utiliza la ubicación automáticamente, y puede ser modificada desde el botón "Menú" y la opción "Ajustes" de la aplicación "Noticias y tiempo" (donde adicionalmente se muestra la versión de la aplicación; ver imagen inferior izquierda):

299. El componente de información meteorológica puede tanto hacer uso de la ubicación actual del dispositivo móvil (opción "Utilizar Mi ubicación", habilitada por defecto), como de una ubicación prefijada por el usuario (opción "Establecer ubicación") mediante un nombre de ciudad o código postal (ver imagen superior derecha).

300. Adicionalmente, la configuración permite definir si la información de ambos componentes (noticias y tiempo) se actualizará automáticamente (opción habilitada por defecto), y con qué periodicidad (por defecto, 6 horas). Se recomienda evaluar las capacidades de actualización automáticas con el objetivo de limitar los detalles enviados de forma periódica sobre el dispositivo móvil Android, especialmente si no se hace uso de este servicio:



301. Android establece conexiones con Google (www.google.com) mediante el widget de noticias y tiempo, y en concreto al recurso "/m/appreq", empleando el agente de usuario

"GMM/3.0 (passion FRF91); gzip", que identifica el hardware del terminal y el número de compilación de Android, junto a la versión 3.0 de Google Maps for Mobile (GMM):

```
POST /m/appreq HTTP/1.1
Content-Type: application/binary
Content-Length: 99
Host: www.google.com
Connection: Keep-Alive
User-Agent: GMM/3.0 (passion FRF91); gzip

...."newswidget,0.0.0,android,web,en_US6....+Tu..g...*.......g:gne/r.....
.2.x.......ES...es-ES.....
```

Nota: La denominación "passion" en el agente de usuario permite identificar el tipo de dispositivo móvil, en este caso Google Nexus One, también conocido como HTC Passion.

302. Los intercambios entre la aplicación y el servicio de Google mediante HTTP se realizan en formato binario.

303. Adicionalmente, este tipo de peticiones HTTP (TCP/80) están acompañadas de peticiones HTTP POST similares solicitando noticias concretas, como por ejemplo http://nt2.ggpht.com/news/tbn/ipbQSkNUXDsJ (GET), dónde el servidor empleado cambia (nt0, nt1, nt2, nt3, etc.), al igual que el identificador de noticia o imagen al final de la URL.

304. Los diferentes temas asociados a las noticias (internacional, economía, deportes, etc.) son obtenidos desde otro recurso web de www.google.com ("/m/gne/newsTopics?hl=es_ES") empleando un agente de usuario diferente que también revela detalles del dispositivo móvil: "User-Agent: Dalvik/1.2.0 (Linux; U; Android 2.2; Nexus One Build/FRF91)", que emplea el nombre de la máquina virtual Java de Android ("Dalvik").

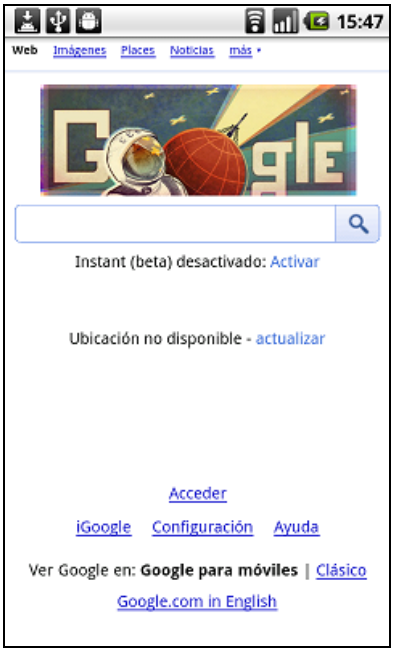
305. Se recomienda no hacer uso de este tipo de servicios que desvelan información detallada de la ubicación del usuario y del dispositivo móvil empleado, y que hacen uso de conexiones HTTP no cifradas, salvo que explícitamente se deseé acceder a la información que éstos proporcionan.

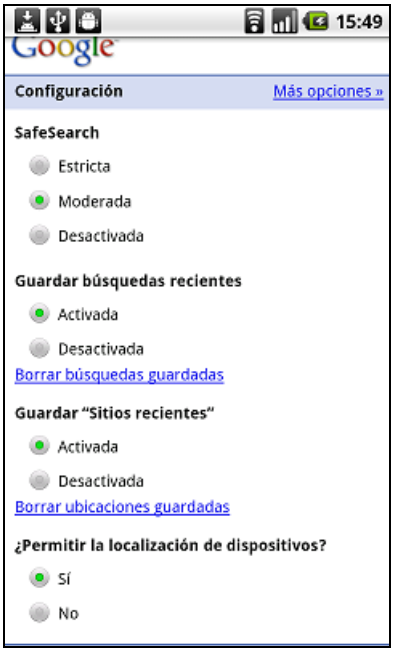
5.10.4.4 BUSCADOR DE GOOGLE

306. La información de localización de GPS puede ser empleada por otros servicios de Google, como por ejemplo el buscador web.

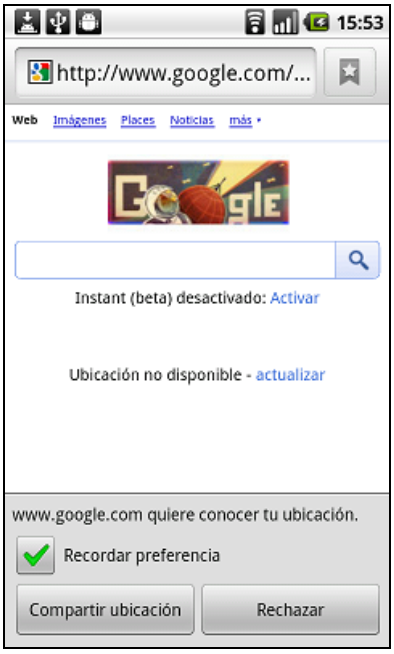
307. Debe recordarse que desde el menú "Ajustes – Ubicación y seguridad", y en concreto desde la sección "Mi ubicación", es posible habilitar las capacidades de localización del dispositivo móvil, tanto a través de GPS como de redes Wi-Fi.

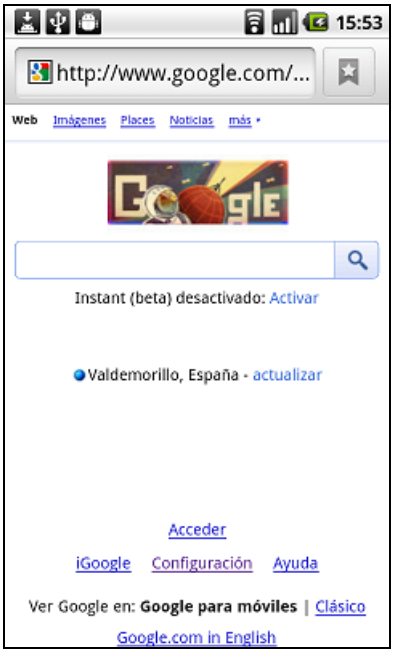
308. Adicionalmente es posible habilitar esta funcionalidad directamente desde Google empleando el navegador web desde el dispositivo móvil Android ("Launcher – Navegador"). A través de la opción "Configuración" disponible en la parte inferior de la página web principal de "www.google.com" se puede habilitar el parámetro "¿Permitir la localización de dispositivos?" (desactivada por defecto: "Ubicación no disponible"), para lo que es necesario guardar la nueva configuración (mediante el botón "Guardar" de la página web):





309. El acceso a la página web principal del buscador de Google solicitará autorización al usuario para compartir su ubicación, y reflejará si se está haciendo uso de la ubicación del dispositivo móvil o no, y cuál es la ubicación actual empleada:





310. Si se va a hacer uso de la funcionalidad de búsqueda considerando la ubicación de manera puntual, se recomienda desactivar la opción de "Recordar preferencia", activa por defecto. Se recomienda hacer un uso limitado de esta funcionalidad con el objetivo de proteger la privacidad del usuario, en base a los detalles técnicos que se exponen a continuación.

311. El agente de usuario empleado por el navegador web de Android desvela los detalles de la plataforma, versión y modelo de dispositivo móvil (ver apartado "5.22. Navegación web: Navegador").

312. Adicionalmente, las peticiones y redirecciones HTTP de acceso a Google reflejan el uso de Android: "http://www.google.com/m?client=ms-android-vf-es&source=android-home".

313. Todos los accesos web al buscador de Google, tanto de preferencias (“/m/preferences?”), como de intercambio de información de la ubicación (ver abajo, “/m/gn/rgc”), como de búsqueda (“/m/search?”), se realizan sin cifrar mediante HTTP (TCP/80).

314. Las peticiones de intercambio de información de ubicación, que se llevan a cabo una vez el usuario autoriza al dispositivo a compartir su ubicación, emplean el siguiente tipo de solicitudes HTTP (POST), proporcionando los valores de latitud y longitud correspondientes a la ubicación actual del dispositivo móvil en el parámetro “sll”:

```
POST /m/gn/rgc HTTP/1.1
Host: www.google.com
...
Content-Type: application/x-www-form-urlencoded
Content-Length: 23

sll=40.488147,-4.026275
```

315. Como respuesta web a dicha petición se obtiene una línea de información con la ubicación actual, como “Valdemorillo, España” en el ejemplo empleado previamente.

316. Cualquier búsqueda posterior (“/m/search?”) incorporará un parámetro GET denominado “ltoken” (ej. “ltoken=112f1c9c”) que permite afinar y vincular la búsqueda a la ubicación del dispositivo móvil.

5.10.4.5 REDES SOCIALES

317. La información de localización puede integrarse también con las aplicaciones de acceso a redes sociales y Web 2.0, siendo posible la publicación de la ubicación del usuario a través por ejemplo de Twitter.

318. No se ha identificado ninguna opción de configuración asociada en la versión 3.0.1 de “Twitter para Android” para habilitar o deshabilitar la gestión de la ubicación del usuario. Esta funcionalidad estará disponible en la aplicación de la red social si el servicio de ubicación está habilitado en el dispositivo móvil de manera general:

319. Para que la ubicación del usuario sea compartida a través de Twitter, el usuario debe activar esta funcionalidad explícitamente a través del botón destinado a tal efecto (abajo a la derecha) a la hora de escribir un nuevo “Tweet” o mensaje (opción desaconsejada desde el punto de vista de seguridad):

320. Servicios como Google Latitude (http://www.google.com/mobile/latitude/) también ofrecen este tipo de funcionalidad para compartir la ubicación física entre usuarios. En el caso de Android, este servicio está integrado con “Google Maps for mobile” a través del botón “Menú” y la opción “Unirme a Latitude”.

321. Servicios más avanzados, como Google Location History, disponible desde la versión 5.3 de Google Maps en Android (e integrado con Google Latitude), permiten disponer de un histórico completo de la ubicación del usuario, incluso con análisis y porcentajes de dónde ha estado el usuario (casa, trabajo, viajando, etc.) [Ref.- 64]:

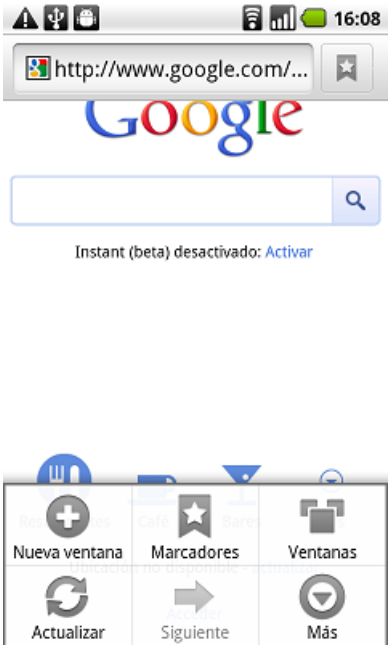
322. Pese a que se supone que este tipo de servicios avanzados son privados para el usuario, los mismos permiten disponer de un nivel demasiado detallado de información sobre la ubicación del usuario a lo largo del tiempo, y constituyen un riesgo relevante para la privacidad del mismo. En caso de haber habilitado este servicio es posible eliminar el histórico de ubicaciones previamente almacenado en Google.

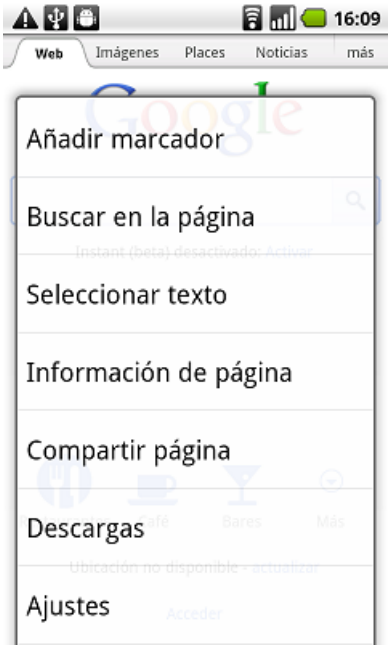
323. Se recomienda no hacer pública la ubicación en la que se encuentra el usuario en redes sociales o servicios avanzados similares con el objetivo de proteger su privacidad.

5.10.4.6 NAVEGADOR WEB

324. El navegador web existente por defecto en Android permite autorizar el acceso a la información de localización (o ubicación del dispositivo móvil) a todas las páginas web, de forma general, o a páginas web individuales.

325. Para ello es necesario ejecutar la aplicación del navegador web, “Navegador”, y a través del botón de “Menú”, y la opción “Más”, acceder a la sección “Ajustes”:



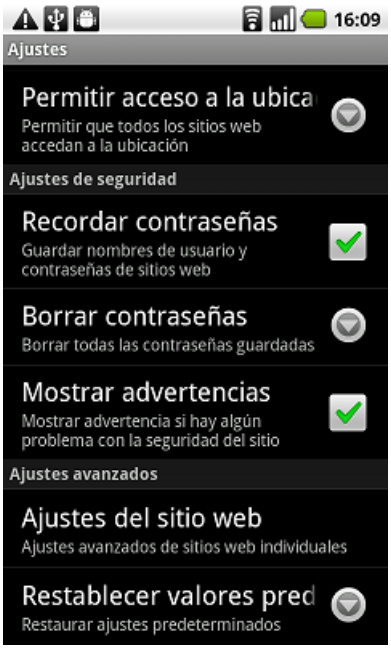


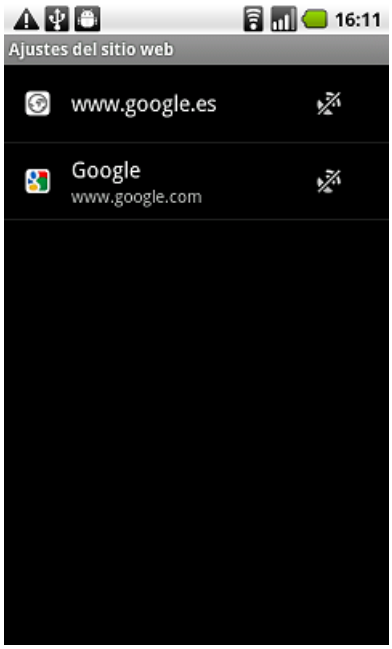
326. Desde la pantalla de “Ajustes”, la opción “Permitir acceso a la ubicación” permite a todos los sitios web acceder a la ubicación actual del dispositivo móvil, opción desaconsejada desde el punto de vista de seguridad:

Nota: El comportamiento de "Navegador" versión 2.2 respecto a la ubicación del usuario no es consistente, existiendo escenarios en los que no es posible deshabilitar ciertas opciones de configuración, apareciendo como no disponibles (en color gris) en la pantalla de ajustes (por ejemplo, ver imagen superior derecha), pese a no permitirse el acceso a la ubicación, ni ser solicitada por el sitio web. La única alternativa identificada para restaurar este permiso requiere emplear la opción de "Restablecer valores predeterminados" (disponible al final de la pantalla de "Ajustes").

327. Desde el punto de vista de seguridad se recomienda deshabilitar la opción "Habilitar ubicación", también disponible en la pantalla de "Ajustes", con el objetivo de no permitir a los sitios web disponer de acceso a la información de localización, incluso aunque lo tuvieran previamente permitido de forma individual (como se describe posteriormente) o general.

328. Android dispone de capacidades más granulares para definir qué sitios web disponen de acceso a la información de localización. Desde la pantalla de "Ajustes", en la parte inferior, debe accederse a la sección "Ajustes del sitio web". Esta sección contiene un listado de sitios web con ajustes avanzados de configuración para sitios web específicos:





329. Los sitios web aparecerán en esta lista cuando han solicitado acceso a la ubicación y este acceso ha sido rechazado por el usuario, o cuando ha sido permitido por el usuario, quedando reflejado en esta misma lista.

330. Uno de los permisos disponibles para sitios web que lo soliciten es el disponer de acceso a la ubicación actual del dispositivo móvil, siendo posible para el usuario permitir o denegar dicho acceso:

331. Una vez el acceso ha sido permitido desde la propia lista, el sitio web individual desaparecerá de la lista. La única alternativa identificada para deshabilitar este permiso requiere emplear la opción de “Restablecer valores predeterminados” (disponible al final de la pantalla de “Ajustes”) o borrar los datos y la caché del “Navegador” desde el administrador de aplicaciones.

332. La gestión del navegador web de Android a los datos de ubicación es confusa e inconsistente, ya que no permite al usuario analizar en cada momento qué sitios web sí

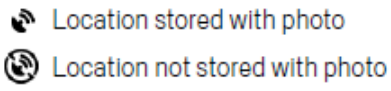
tienen permitido, o denegado, el acceso a esta información, y depende de si el permiso se llevó a cabo desde el propio navegador web al ser solicitado, o desde la lista disponible en los ajustes de configuración.

5.10.5 INFORMACIÓN GEOGRÁFICA EN FOTOGRAFÍAS

333. Android permite añadir información de la localización geográfica a las fotografías realizadas con la cámara del dispositivo móvil. Al realizar la fotografía se añaden las coordenadas GPS en el momento de tomar la instantánea a la cabecera EXIF de la imagen.

334. Esta funcionalidad puede ser utilizada a través del menú de configuración de la cámara. Para ello es necesario abrir la cámara mediante la aplicación "Cámara" desde el "Launcher", y seleccionar el segundo botón de configuración:

335. La opción "Almacenar ubicación" permite habilitar o deshabilitar esta funcionalidad, indicándose la configuración actual mediante los iconos siguientes:



336. Por defecto, las fotografías tomadas con el dispositivo móvil no incluyen la información del GPS. Es necesario habilitar la opción para almacenar esta información.

337. 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 (disponible desde la aplicación "Cámara" o desde la aplicación "Galería"; desde el "Launcher"), empleando la opción "Menú – Más – Detalles" (situada abajo a la derecha).

338. El campo "Ubicación" (al final de la lista de atributos de la imagen) indicará la ubicación dónde fue tomada (calle, número y población) o "Ubicación desconocida" en caso de no disponer de la información.

339. Se recomienda no hacer uso de la funcionalidad que incluye la información del GPS en fotografías, especialmente para su publicación o distribución en Internet, salvo que se quiera hacer uso explícito de estas capacidades. En caso contrario, las imágenes revelarán los detalles exactos de dónde han sido tomadas.

5.11 COMUNICACIONES USB

340. La conexión USB del dispositivo móvil a un ordenador proporciona dos funcionalidades o tipos de conexiones diferentes: [Ref.- 91]

- Unidad de disco, para compartir la tarjeta de almacenamiento externo del dispositivo móvil con el ordenador.
- Conexión de telefonía móvil de datos, o *tethering*, para compartir la conexión de datos 2G/3G o Wi-Fi del dispositivo móvil con el ordenador.

341. Ambas funcionalidades USB no pueden ser utilizadas simultáneamente. En caso de estar usando las capacidades de tethering, éstas deben ser deshabilitadas para tener acceso al almacenamiento vía USB, y viceversa.

5.11.1 ALMACENAMIENTO USB

Nota: El acceso al dispositivo móvil como unidad de almacenamiento USB puede estar disponible incluso con el modo de depuración habilitado en Android. En caso de conflictos y estar habilitado, basta con deshabilitar este modo (opción recomendada desde el punto de vista de seguridad), para disponer de las capacidades de almacenamiento USB únicamente. El modo de depuración se puede deshabilitar mediante el menú "Ajustes – Aplicaciones – Desarrollo", desactivando la opción "Depuración USB".

342. Para acceder a las capacidades de almacenamiento USB basta con seleccionar la notificación correspondiente en la barra de estado, "Conectado por USB", y seleccionar el botón "Activar almacenamiento USB" en la pantalla de "Almacenamiento USB masivo" (con el androide en color verde):

343. Una vez se ha activado el almacenamiento USB, el androide aparece en color naranja. Antes de desactivar el almacenamiento USB mediante el botón disponible a tal efecto, y accesible también desde el panel de notificaciones, se recomienda desmontar la unidad de almacenamiento en el ordenador.

344. La unidad de almacenamiento compartida con el ordenador corresponde únicamente a la tarjeta de almacenamiento externo (tarjeta SD) disponible en el propio dispositivo móvil.

345. Mientras la tarjeta de almacenamiento externo está siendo compartida con el ordenador, no puede ser usada desde el dispositivo móvil, por lo que las aplicaciones que hacen uso de ella no deben ser ejecutadas (Android deshabilita su funcionalidad automáticamente).

346. Debe prestarse especial atención a la configuración de seguridad del ordenador, y en concreto a los mecanismos de auto-ejecución de Windows (autorun y autoplay), para evitar la propagación de software malicioso (como por ejemplo el troyano Ambler u otros códigos dañinos, como en el caso de Vodafone y Android en 2010 [Ref.- 1]) desde la tarjeta de almacenamiento externa del dispositivo móvil al ordenador.

347. Android proporciona la posibilidad de desmontar la unidad de almacenamiento externo antes de ser extraída del dispositivo móvil, a través del menú "Ajustes – Almacenamiento – Desactivar tarjeta SD", opción recomendada para evitar corrupción de datos antes de extraer la tarjeta SD mientras el terminal se encuentra encendido.

5.11.2 CONEXIÓNDE RED USB (*TETHERING*)

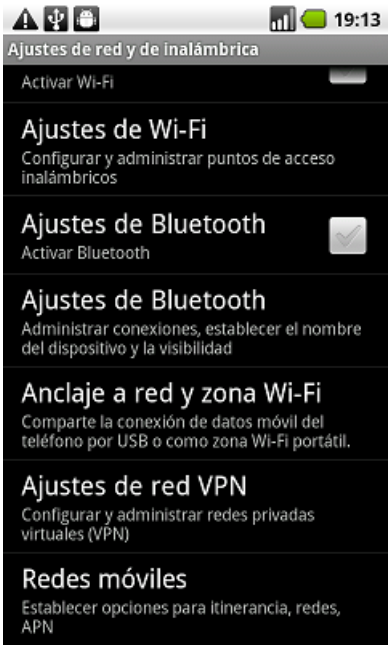
348. La opción de conexión compartida, o tethering, permite compartir la conexión de datos de telefonía móvil (2G/3G) o Wi-Fi del terminal con el ordenador. Desde el punto de vista de seguridad se recomienda hacer uso de tethering mediante cable USB, en lugar de mediante Bluetooth [Ref.- 91].

349. Los iconos de notificación empleados por Android para este tipo de conexiones, junto a la de punto de acceso Wi-Fi (ver apartado "5.13.5. Punto de acceso Wi-Fi") son:

	USB tethering is active
	Portable Wi-Fi hotspot is active
	Both USB tethering and portable hotspot are active

350. Las capacidades de tethering y de punto de acceso Wi-Fi (ver apartado "5.13.5. Punto de acceso Wi-Fi") pueden ser utilizadas simultáneamente en Android, proporcionando conexión de red a otros dispositivos u ordenadores simultáneamente tanto por USB como por Wi-Fi.

351. Android proporciona capacidades nativas de tethering para Windows Vista/7 y Linux (siendo necesaria una configuración adicional en Windows XP [Ref.- 90]). Para hacer uso de estas capacidades es necesario conectar el dispositivo móvil al ordenador mediante USB y acceder al menú "Ajustes – Conexiones inalámbricas (y redes) – Anclaje a red y zona Wi-Fi" (en las versión 2.3 "Ajustes – Conexiones inalámbricas– Modem USB y Mi zona Wi-Fi – Modem USB" y en versión 4.0 "Ajustes – Conexiones inalámbricas–Zona Wi-Fi y Modem USB – Modem USB"):



352. A través de la opción “Anclaje de USB” (ver imagen superior derecha) es posible habilitar el servicio de tethering, de forma que el ordenador utilice el dispositivo móvil como su conexión de red.

Nota: Al habilitar la conexión de red por USB o *tethering*, el modo de depuración, de estar previamente habilitado en Android, será deshabilitado automáticamente.

353. Tras establecerse la conexión de red, y tomando Windows 7 como sistema operativo del ordenador de referencia, se crea automáticamente un interfaz de red de tipo “Remote NDIS based Internet Sharing Service” configurado con una dirección IP dinámica (DHCP) por defecto de clase C (/24), como por ejemplo 192.168.42.123.

354. Este interfaz de red NDIS del ordenador tiene asociada una dirección MAC con el OUI “3a:8c:30”, qué no está asignado a ningún vendedor públicamente en el momento de elaboración de la presente guía.

355. La configuración de este interfaz de red toma todos los valores por defecto existentes en el sistema operativo del ordenador. Así por ejemplo en Windows 7 la pila de comunicaciones de TCP/IP versión 6 está activa, al igual que NetBIOS sobre TCP/IP, soportado por el servidor DHCP de Android.

356. Se recomienda modificar y restringir la configuración de este interfaz de red para habilitar únicamente los protocolos y servicios que se consideren necesarios en el ordenador.

357. El dispositivo móvil (por ejemplo, con dirección IP 192.168.42.129) actúa de gateway, router o pasarela por defecto, de servidor DHCP, y de servidor DNS, y es alcanzable mediante ping (ICMP).

Nota: El direccionamiento IP empleado por Android para la conexión de red compartida a través de USB (192.168.42.x) no puede ser modificado salvo en dispositivos móviles *rooted* [Ref.- 96].

358. La dirección MAC asociada al interfaz de red empleado para proporcionar la conexión de red compartida a través de USB por el dispositivo móvil tiene asociado un OUI con valor

"fe:2b:99", qué no está asignado a ningún vendedor públicamente en el momento de elaboración de la presente guía.

359. Un análisis de los puertos TCP/IP y servicios disponibles en el interfaz de red del dispositivo móvil empleado para proporcionar la conexión de red compartida a través de USB permite obtener las siguientes conclusiones:

- El único puerto TCP abierto es el correspondiente al servidor DNS (53/tcp). El servidor DNS es identificado por Nmap como "dnsmasq 2.51".
- Los únicos puertos UDP abiertos son los correspondientes al servidor DNS (53/udp) y al servidor DHCP (67/udp).

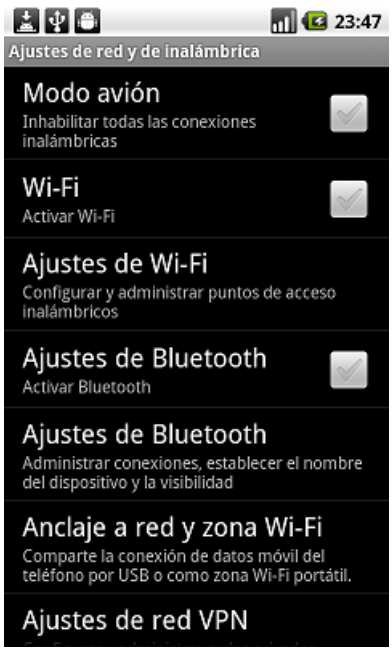
360. Es posible finalizar la compartición de la conexión de datos deshabilitando la opción "Anclaje de USB" habilitada previamente, opción recomendada desde el punto de vista de seguridad una vez no se desea disponer de la conexión de red compartida.

5.12 COMUNICACIONES BLUETOOTH

5.12.1 DESACTIVACIÓN DE LAS COMUNICACIONES BLUETOOTH

361. La principal recomendación de seguridad asociada a las comunicaciones Bluetooth (802.15) en dispositivos móviles es no activar el interfaz inalámbrico Bluetooth salvo en el caso en el que se esté haciendo uso del mismo, evitando así la posibilidad de ataques sobre el hardware del interfaz, el driver o la pila de comunicaciones Bluetooth, incluyendo los perfiles Bluetooth disponibles [Ref.- 51].

362. El interfaz inalámbrico Bluetooth puede ser desactivado en Android, situación por defecto, a través del menú "Ajustes – Conexiones inalámbricas (y redes)", mediante el botón de la opción "Ajustes de Bluetooth (Activar Bluetooth)":



363. El estado del interfaz Bluetooth puede ser verificado de forma rápida y sencilla por el usuario del dispositivo móvil a través de la barra superior de estado.

364. Android proporciona información en la barra superior de estado sobre el estado del interfaz Bluetooth, y si existe una conexión establecida actualmente, a través del siguiente conjunto de iconos:

	Bluetooth is on
	Connected to a Bluetooth device

365. Android mantiene el estado del interfaz Bluetooth tras reiniciar el dispositivo móvil, es decir, si el interfaz Bluetooth estaba activo al apagar el terminal, al encender el dispositivo móvil seguirá activo.

366. La activación inicial del interfaz Bluetooth se llevará a cabo tan pronto el dispositivo móvil se haya reiniciado, incluso aunque aún no haya sido desbloqueado por primera vez tras encenderlo (igual que el interfaz Wi-Fi; ver apartado “5.13. Comunicaciones Wi-Fi”).

367. Igualmente, al salir del modo avión (o modo de vuelo) el estado del interfaz Bluetooth será restaurado, activándose en el caso de haber estado activo previamente (antes de activar el modo avión).

368. El interfaz Bluetooth también permanece activo cuando el dispositivo móvil está en espera o stand-by, es decir, encendido pero con la pantalla apagada y bloqueado.

Nota: Tras un restablecimiento de fábrica, o *hard-reset*, el dispositivo móvil empleado para la elaboración de la presente guía responde a peticiones Bluetooth tan pronto el interfaz es habilitado (en modo oculto o no visible por defecto).

369. La dirección del interfaz Bluetooth, BD_ADDR (Bluetooth Device Address) está disponible a través del menú “Ajustes – Acerca del teléfono – Estado”, y en concreto, en el campo “Dirección de Bluetooth”. La dirección no es visible, se muestra el mensaje “No disponible” en su lugar, si el interfaz Bluetooth no se encuentra en el estado activo:

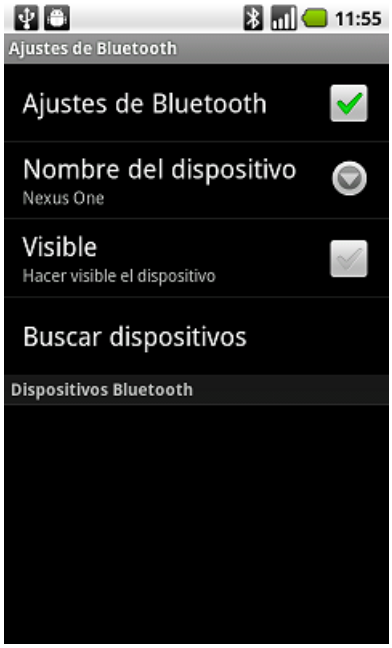
Nota: La parte de la dirección Bluetooth (BD_ADDR) asociada al fabricante, NAP+UAP (primeros tres *bytes* de la dirección) puede permitir identificar el tipo de dispositivo móvil. En

el ejemplo analizado, el valor "90:21:55" está asignado por el IEEE (http://standards.ieee.org/regauth/oui/index.shtml) a "HTC":

```
90-21-55    (hex)        HTC Corporation
902155      (base 16)    HTC Corporation
                         No.23 Xinghua Road
                         Taoyuan City
                         Taoyuan County  330
                         TAIWAN, REPUBLIC OF CHINA
```

5.12.2 CONFIGURACIÓN GENERAL DE BLUETOOTH

370. Debe tenerse en cuenta que, al igual que para el interfaz Wi-Fi, para poder llevar a cabo la configuración de la pila de comunicaciones Bluetooth a través del interfaz de usuario del dispositivo móvil es obligatorio activar el interfaz (como se muestra en las dos siguientes imágenes) por lo que se recomienda activar el interfaz y realizar las modificaciones de la configuración en un entorno seguro, para evitar potenciales ataques cuando los mecanismos de seguridad no han sido aún aplicados:



371. La pantalla de configuración (imagen superior derecha) permite llevar a cabo múltiples acciones, como habilitar y deshabilitar el interfaz Bluetooth, configurar el nombre del dispositivo móvil empleado para las conexiones Bluetooth, configurar el estado del interfaz Bluetooth (oculto o visible), o buscar otros dispositivos Bluetooth con los que conectarse.

372. En caso de no especificar ningún nombre para Bluetooth, el valor por defecto empleado como nombre de dispositivo móvil para las conexiones Bluetooth por Android es "Nexus One", tal como se indica en el menú correspondiente al "Nombre del dispositivo" de los ajustes de Bluetooth (ver imagen superior derecha).

373. Debido a que el nombre por defecto desvela el tipo de dispositivo móvil empleado, se recomienda modificarlo por un valor que no revele detalles ni del dispositivo móvil (fabricante o modelo) ni del propietario (evitando tanto referencias al nombre de la persona como de la organización asociadas al mismo), como por ejemplo "bt0001" (Bluetooth móvil 0001).

374. Se recomienda modificar el nombre configurado por defecto (ej. “Nexus One”) con el objetivo de no desvelar información sobre su propietario o la marca y modelo del dispositivo móvil (ej. “bt0001”).

375. En el caso de activar el interfaz Bluetooth para hacer uso de esta tecnología, se recomienda configurar el mismo en modo oculto o no visible, con el objetivo de no desvelar su presencia frente a las operaciones de búsqueda de otros dispositivos Bluetooth.

376. Para ello, desde la ventana de configuración de Bluetooth (accesible a través del menú “Ajustes – Conexiones inalámbricas (y redes) – Ajustes de Bluetooth”) no debe seleccionarse la opción “Visible”. Por defecto, al activar el interfaz Bluetooth éste se encuentra en modo oculto o no visible, opción recomendada desde el punto de vista de seguridad.

377. Al configurar el interfaz Bluetooth en el estado visible, el dispositivo permanecerá en dicho estado únicamente durante los próximos 120 segundos tras seleccionar esta opción, volviendo al modo oculto automáticamente tras ese periodo de tiempo:

378. La versión 4.0 de Android permite configurar los tiempos de visibilidad entre varios valores (2 minutos, 5 minutos, 1 hora o siempre visible). Se recomienda configurar la visibilidad del dispositivo el mínimo tiempo necesario para realizar el emparejamiento.

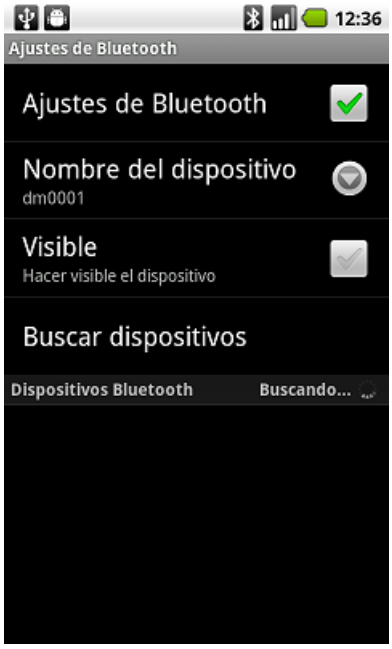
379. Al encontrarse el interfaz Bluetooth del dispositivo móvil en modo oculto, todas las conexiones Bluetooth y operaciones de emparejamiento con otros dispositivos deberán iniciarse desde el dispositivo móvil, siendo necesario que el otro dispositivo Bluetooth se encuentre en modo visible.

Nota: En el caso de requerir, de forma excepcional, disponer del interfaz Bluetooth en modo visible para realizar el emparejamiento con otro dispositivo, la opción de estar visible sólo temporalmente durante 120 segundos es la opción recomendada desde el punto de vista de seguridad, con el objetivo de volver al estado oculto tras la operación de emparejamiento.

Este comportamiento puede variar en futuras versiones de Android, disponiéndose también de la opción para que el dispositivo móvil se encuentre visible de forma permanente [Ref.- 123].

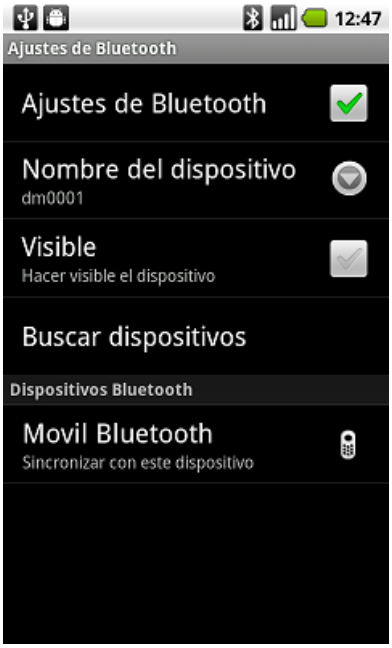
5.12.3 DISPOSITIVOS BLUETOOTH EMPAREJADOS

380. Android lleva a cabo de forma automática y periódica búsquedas de dispositivos Bluetooth visibles, proceso indicado por el texto “Buscando…”, mostrando los mismos bajo la sección “Dispositivos Bluetooth” de la pantalla de configuración de Bluetooth:



381. La operación de búsqueda puede realizarse también de forma manual mediante la opción “Buscar dispositivos”.

382. Mediante la selección de un dispositivo visible de la lista es posible realizar el emparejamiento con el mismo. Android establecerá la comunicación Bluetooth con el otro dispositivo y llevará a cabo el proceso de emparejamiento, solicitando al usuario el PIN o contraseña Bluetooth:



383. Android permite la utilización de PIN o contraseñas Bluetooth formados por caracteres alfanuméricos y símbolos, de hasta 16 caracteres de longitud, durante el emparejamiento con otros dispositivos (tal como define la especificación Bluetooth).

384. La contraseña o PIN Bluetooth se mostrará en la pantalla al ser introducida por el usuario, sin disponer Android de ninguna opción para ocultar su valor, por ejemplo mediante el carácter asterisco ("*"), por lo que debe prestarse especial atención a que nadie, aparte del usuario, disponga de acceso visual a la pantalla durante el proceso de emparejamiento.

385. Se recomienda hacer uso de contraseñas alfanuméricas robustas para el emparejamiento con otros dispositivos Bluetooth (compuestas por números, letras y símbolos, y de al menos 8 caracteres), en lugar de emplear un PIN de cuatro dígitos (valor común por defecto y empleado de forma estándar en el emparejamiento de dispositivos Bluetooth; y en ningún caso utilizar los valores 0000 o 1234 sugeridos por Android).

386. No se han identificado opciones en Android para obtener la dirección Bluetooth (BD_ADDR) de cada dispositivo con el que se ha realizado el emparejamiento, muy útil a la hora de reconocer otros dispositivos asociados al terminal, así como modificar el nombre empleado para identificarlos en el dispositivo móvil y determinar si las conexiones con el dispositivo móvil deben ser autorizadas.

5.12.4 CONFIGURACIÓN AVANZADA DE BLUETOOTH

387. La implementación de Bluetooth de Android, por defecto incluye diferentes perfiles: "PnP Information", "Audio Source", "AVRCP TG", "Voice Gateway", "OBEX Object Push", y "OBEX Phonebook Access Server".

388. No se han identificado en Android opciones de configuración avanzadas que permitan establecer restricciones de conectividad (autentificación, autorización y/o cifrado), obtener información, o configurar opciones de transferencia de archivos, para los diferentes perfiles Bluetooth disponibles.

5.12.5 OBEX FILE TRANSFER (OBEX FTP)

389. Android no ofrece por defecto el perfil estándar de transferencia de archivos de Bluetooth, OBEX File Transfer (u OBEX FTP), sin embargo, algunos fabricantes de dispositivos móviles Android como HTC incluyen su propia implementación de OBEX FTP.

390. Las características y funcionalidades añadidas en ocasiones por los fabricantes de los dispositivos móviles con el objetivo de mejorar las prestaciones del sistema operativo empleado pueden dar lugar a nuevas vulnerabilidades de seguridad.

391. Los dispositivos móviles HTC basados en Android incorporan el servicio HTC Bluetooth OBEX FTP, sobre la pila Bluetooth estándar de comunicaciones de Android, para la transferencia de ficheros a través de Bluetooth.

392. Este servicio permite el acceso y modificación de ficheros, empleando como directorio por defecto en Android la tarjeta de almacenamiento externa conectada al dispositivo móvil.

393. En 2011, una nueva vulnerabilidad de desplazamiento por directorios fue descubierta por Alberto Moreno Tablado para Android 2.1 y 2.2 en dispositivos HTC [Ref.- 122], siendo posible acceder a cualquier fichero del dispositivo móvil, independientemente de su ubicación en el sistema de ficheros, como por ejemplo la base de datos de contactos o los correos de GMail.

394. Desafortunadamente, en 2009, una vulnerabilidad similar de desplazamiento por directorios fue descubierta por el mismo investigador para Windows Mobile 6 y 6.1 en dispositivos HTC (CVE-2009-0244) [Ref.- 1].

395. Pese a que el servicio HTC Bluetooth OBEX FTP sólo está disponible para dispositivos emparejados (proceso que permite obtener privilegios de autentificación y autorización en Bluetooth), debe tenerse en cuenta que existen ataques para la captura de las claves de enlace Bluetooth, y la suplantación de otros dispositivos, que permitirían evitar esta restricción [Ref.- 1].

5.12.6 OBEX OBJECT PUSH

396. Android dispone por defecto de capacidades para el intercambio (o inserción) de objetos, asociadas al perfil Bluetooth estándar OBEX Object Push.

397. El perfil de recepción de objetos (OBEX, Object Exchange) a través de Bluetooth está habilitado por defecto y no se ha identificado ninguna opción de configuración para deshabilitarlo.

398. Cuando otro dispositivo Bluetooth se comunica con este perfil e intenta enviar un objeto, Android solicita autorización por parte del usuario a través de la barra de estado antes de permitir la operación de intercambio:

399. Mediante la selección de dicha notificación, el usuario es informado sobre los detalles de la transferencia, que incluyen el dispositivo Bluetooth remitente, el nombre los datos transferidos, y el tamaño:

400. Si la transferencia de datos a través del perfil OBEX Object Push tiene éxito, tras emplearse los mecanismos de autorización descritos, se indica el resultado al usuario mediante una pantalla de confirmación (imagen superior derecha).

401. El objeto (o fichero) recibido se almacena por defecto en el directorio “bluetooth” de la tarjeta de almacenamiento externa.

402. El perfil OBEX Object Push no dispone del mecanismo de autentificación habilitado por defecto, debido a su modelo de uso, en el que no es necesario emparejarse con el otro dispositivo para transferir datos.

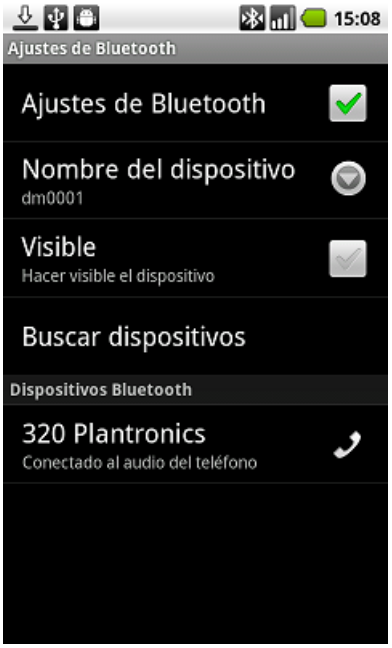
403. El comportamiento de solicitud de autorización al usuario descrito previamente se presenta tanto con dispositivos Bluetooth con los que previamente se ha emparejado Android (es decir, autentificados), como con dispositivos nuevos.

5.12.7 MANOS LIBRES BLUETOOTH

404. El emparejamiento con dispositivos Bluetooth manos libres puede no requerir el introducir ningún PIN o clave de paso, proceso conocido como emparejamiento automático o auto pairing, debido a que Android dispone de conocimiento de los PINs empleados por defecto (no modificables) por los fabricantes de manos libres Bluetooth:

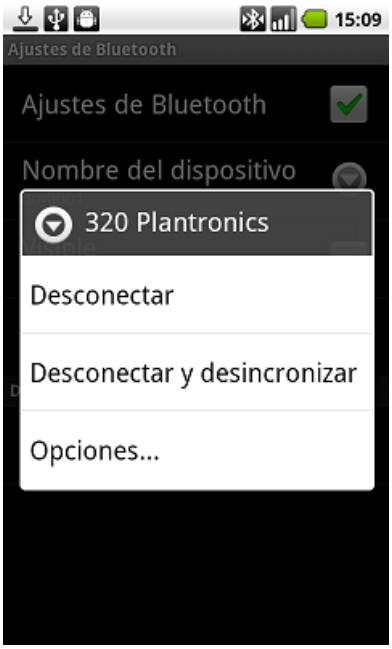
405. El emparejamiento automático se lleva a cabo por ejemplo con dispositivos que emplean valores de PIN como “0000”.

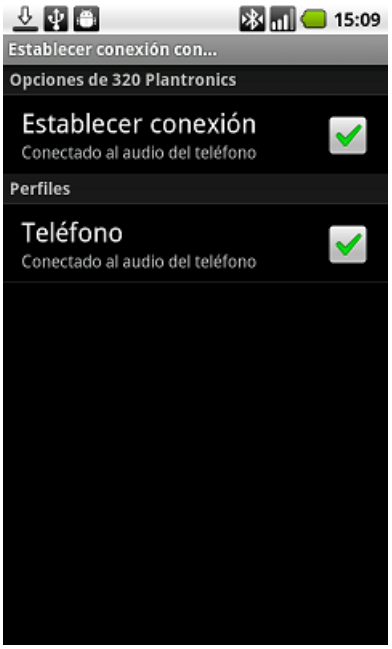
406. El interfaz Bluetooth del dispositivo móvil, una vez es habilitado, intenta establecer automáticamente una conexión con los dispositivos manos libres disponibles en la lista de dispositivos emparejados, proceso conocido como conexión automática o auto connect. Si el dispositivo Bluetooth se encuentra en el rango de alcance del dispositivo móvil, y fueron emparejados previamente, se establecerá la conexión, estado identificado en Android por el icono de estado de Bluetooth en la parte superior (con una doble flecha junto al logotipo de Bluetooth – ver imagen inferior derecha):



407. El proceso de conexión automática no tiene asociada ninguna solicitud de confirmación por parte del usuario ni puede ser deshabilitado mediante opciones de configuración.

408. Una vez se ha establecido la conexión Bluetooth con otro dispositivo (independientemente de su tipo o del perfil empleado), al seleccionarlo se dispone de un menú de “Opciones…”. A través del mismo sólo es posible interrumpir la conexión actualmente establecida o seleccionar los perfiles ofrecidos por el otro dispositivo que se desean utilizar:





409. No se han identificado en Android opciones de configuración avanzadas que permitan configurar los perfiles de Bluetooth asociados a la conexión con dispositivos manos libres.

5.13 COMUNICACIONES WI-FI

5.13.1 DESACTIVACIÓN DE LAS COMUNICACIONES WI-FI

410. La principal recomendación de seguridad asociada a las comunicaciones Wi-Fi (802.11) en dispositivos móviles es no activar el interfaz inalámbrico Wi-Fi salvo en el caso en el que se esté haciendo uso del mismo, evitando así la posibilidad de ataques sobre el hardware del interfaz, el driver o la pila de comunicaciones Wi-Fi [Ref.- 49].

Nota: Durante el proceso de configuración inicial del dispositivo móvil empleado para la elaboración de la presente quía (activado automáticamente la primera vez que se enciende el terminal), si se omite la vinculación del dispositivo móvil a una cuenta de Google, el interfaz Wi-Fi estará deshabilitado.

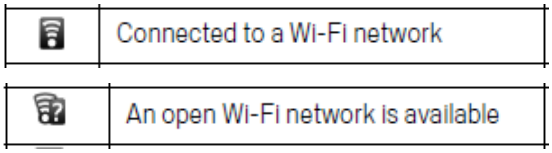
En caso de proceder a vincular el dispositivo móvil a una cuenta de Google, si no se dispone de conexión o servicio de datos a través de las redes de telefonía móvil 2G/3G (primera opción), Android mostrará al usuario un mensaje informativo. El mismo indica que no se dispone de conexión de red, y ofrece al usuario la posibilidad de conectarse a una red Wi-Fi, a través del proceso de configuración de una red Wi-Fi estándar de Android.

Debe tenerse en cuenta que desde el momento que se selecciona el botón “Conectarse a red Wi-Fi” el interfaz Wi-Fi será habilitado (y permanecerá en ese estado incluso aunque posteriormente se interrumpa el proceso de configuración inicial), pudiendo visualizarse en la pantalla de fondo del dispositivo móvil las redes Wi-Fi disponibles en la ubicación actual.

Desde el punto de vista de seguridad se recomienda omitir la vinculación inicial entre el dispositivo móvil y una cuenta de Google y realizar el proceso de configuración inicial posteriormente, salvo que el usuario se encuentre en un entorno seguro y de confianza para poder establecer una conexión a una red Wi-Fi.

411. El interfaz inalámbrico Wi-Fi puede ser desactivado en Android a través del menú "Ajustes – Conexiones inalámbricas (y redes)", mediante el botón de la opción "Wi-Fi (Activar Wi-Fi)":

412. Android proporciona información en la barra superior de estado sobre la disponibilidad de redes Wi-Fi abiertas y si se está o no conectado a una red Wi-Fi actualmente, a través del siguiente conjunto de iconos:



413. La notificación respecto a la disponibilidad de redes Wi-Fi abiertas puede ser configurada a través del menú "Ajustes – Conexiones inalámbricas (y redes) – Ajustes de Wi-Fi", y en concreto mediante la opción "Notificación de red" (habilitada por defecto). Únicamente puede ser modificada una vez el interfaz Wi-Fi ha sido habilitado:

414. Dado que desde el punto de vista de seguridad se desaconseja el establecer conexiones con redes Wi-Fi abiertas, se recomienda desactivar esta opción de notificación.

415. El estado del interfaz Wi-Fi no puede ser verificado de forma rápida y sencilla por el usuario del dispositivo móvil a través de la barra superior de estado. Desafortunadamente, la barra de estado no proporciona información sobre el estado del interfaz Wi-Fi, no siendo posible saber si el mismo está en estado activo o no salvo que el dispositivo móvil esté conectado a una red Wi-Fi actualmente.

416. Android mantiene el estado del interfaz Wi-Fi tras reiniciar el dispositivo móvil, es decir, si el interfaz Wi-Fi estaba activo al apagar el terminal, al encender el dispositivo móvil seguirá activo, incluso con el terminal bloqueado.

417. Igualmente, al salir del modo avión el estado del interfaz Wi-Fi será restaurado, activándose en el caso de haber estado activo previamente (antes de activar el modo avión).

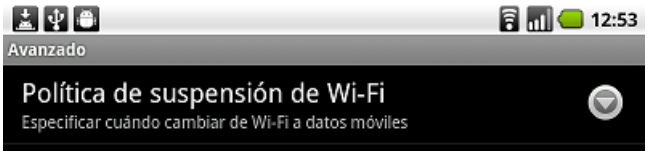
418. Cada 15 segundos, por defecto, el dispositivo móvil genera tramas probe request de tipo broadcast para verificar la disponibilidad de redes Wi-Fi en su zona de alcance.

419. Cuando el dispositivo móvil está conectado a una red, el interfaz Wi-Fi permanece activo durante aproximadamente los siguientes 60 segundos tras pasar al estado de espera o stand-by (desatendido), es decir, el dispositivo móvil está encendido pero con la pantalla apagada y bloqueado. Pasado ese tiempo el dispositivo móvil no genera tráfico pese a que en ningún momento se desconecta de la red Wi-Fi, es decir, al volver a ser utilizado continua sus comunicaciones sin ser necesario autentificarse de nuevo en la red.

420. En caso de no estar conectado a una red Wi-Fi, en el estado de espera el dispositivo móvil no genera ningún tráfico 802.11, ni siquiera las tramas de verificación de disponibilidad de redes Wi-Fi mencionadas previamente. Tan pronto el dispositivo móvil abandona el estado de espera y es utilizado, el interfaz Wi-Fi vuelve a ser activado y genera las tramas de verificación de disponibilidad de redes Wi-Fi.

421. El comportamiento del interfaz Wi-Fi respecto a las operaciones de ahorro de energía del dispositivo móvil puede ser configurado desde el menú “Ajustes – Conexiones inalámbricas (y redes) – Ajustes de Wi-Fi”, a través del botón menú, y mediante la opción “Avanzado”:

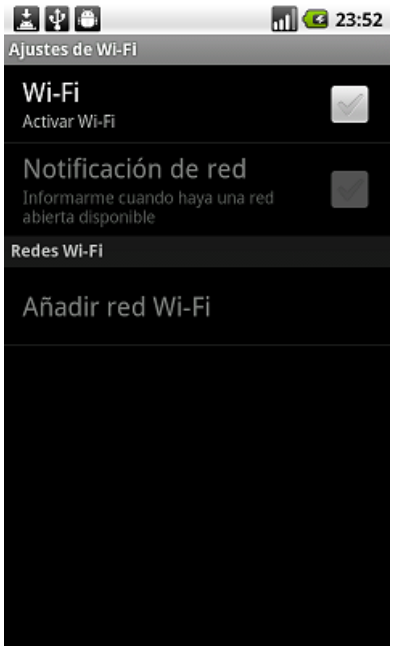
422. La opción “Política de suspensión de Wi-Fi” permite acceder a las diferentes opciones de configuración disponibles: cuando la pantalla se apague (opción por defecto), nunca si se está cargando la batería, o nunca (ver imagen superior derecha).



423. Una vez deshabilitado el interfaz Wi-Fi se hará uso de las capacidades de datos de telefonía móvil (ver apartado "5.13.2. Selección de la red de datos en Android").

424. La configuración detallada de las redes Wi-Fi puede llevarse a cabo a través del menú "Ajustes – Conexiones inalámbricas (y redes) – Ajustes de Wi-Fi".

425. Debe tenerse en cuenta que, al igual que para el interfaz Bluetooth, para poder llevar a cabo la configuración de la pila de comunicaciones Wi-Fi a través del interfaz de usuario del dispositivo móvil es obligatorio activar el interfaz (como se muestra en las dos siguientes imágenes) por lo que se recomienda activar el interfaz y realizar las modificaciones de la configuración en un entorno seguro, para evitar potenciales ataques cuando los mecanismos de seguridad no han sido aún aplicados:



426. La opción "Añadir red Wi-Fi" no está disponible (o habilitada) hasta que el interfaz Wi-Fi no ha sido activado.

427. La dirección del interfaz Wi-Fi está disponible a través del menú "Ajustes – Acerca del teléfono – Estado", y en concreto, en el campo "Dirección MAC de Wi-Fi". La dirección no es visible, se muestra el mensaje "No disponible" en su lugar, si el interfaz Wi-Fi no se encuentra en el estado activo:

Nota: La parte de la dirección Wi-Fi asociada al fabricante (primeros tres *bytes* de la dirección) puede permitir identificar el tipo de dispositivo móvil. En el ejemplo analizado, el valor "90:21:55" está asignado por el IEEE (http://standards.ieee.org/regauth/oui/index.shtml) a "HTC":

```
90-21-55   (hex)        HTC Corporation
902155     (base 16)    HTC Corporation
                        No.23 Xinghua Road
                        Taoyuan City
                        Taoyuan County  330
                        TAIWAN, REPUBLIC OF CHINA
```

428. Es aconsejable comparar la dirección Wi-Fi del dispositivo móvil con su dirección Bluetooth (ver apartado "5.12. Comunicaciones Bluetooth"), con el objetivo de identificar si se trata de direcciones correlativas. En caso afirmativo, un potencial atacante podría obtener la dirección de Bluetooth a partir de la dirección Wi-Fi, con los riesgos que ello conlleva [Ref.- 1], al emplearse la ocultación de la dirección Bluetooth en diferentes escenarios como mecanismo de seguridad.

429. En el caso del dispositivo móvil empleado para la elaboración de la presente guía ambas direcciones comparten el mismo rango del fabricante, pero sin ningún otro elemento común (asignación aleatoria dentro de ese rango).

5.13.2 SELECCIÓN DE LA RED DE DATOS EN ANDROID

Nota: La selección de la red de datos en Android afecta principalmente a la red de datos de telefonía móvil 2G/3G (analizada en el apartado "5.15. Comunicaciones GSM (2G) y UMTS (3G): voz y datos") y al interfaz Wi-Fi (ver este apartado, "5.13. Comunicaciones Wi-Fi").

430. Debido a las múltiples opciones de conectividad de datos disponibles en los dispositivos móviles, como Bluetooth, y principalmente Wi-Fi y 2G/3G, en caso de haber múltiples opciones habilitadas y disponibles, Android gestiona cual es la mejor conexión de datos a

usar en cada momento a través del servicio Connectivity Service [Ref.- 52]. De esta forma evita que el usuario tenga que decidir constantemente que conexión utilizar y proporciona la conectividad necesaria a las aplicaciones que ejecutan en el dispositivo móvil.

431. El Connectivity Service emplea diferentes criterios para seleccionar y mantener la mejor y única opción de conexión de datos, que por defecto da prioridad al interfaz Wi-Fi frente al interfaz de telefonía móvil (2G/3G):

- Si Wi-Fi está activo y se activa 2G/3G, este segundo no llegará a ser habilitado.
- Si 2G/3G está activo y se activa Wi-Fi, la conexión 2G/3G será deshabilitada.
- Si Wi-Fi está activo y se desactiva, el servicio comprobará el estado y la configuración de 2G/3G, y si está disponible, lo habilitará.

432. Los eventos de activación y desactivación de los dos interfaces, Wi-Fi y 2G/3G, pueden ser visualizados a través de los iconos del menú superior de Android.

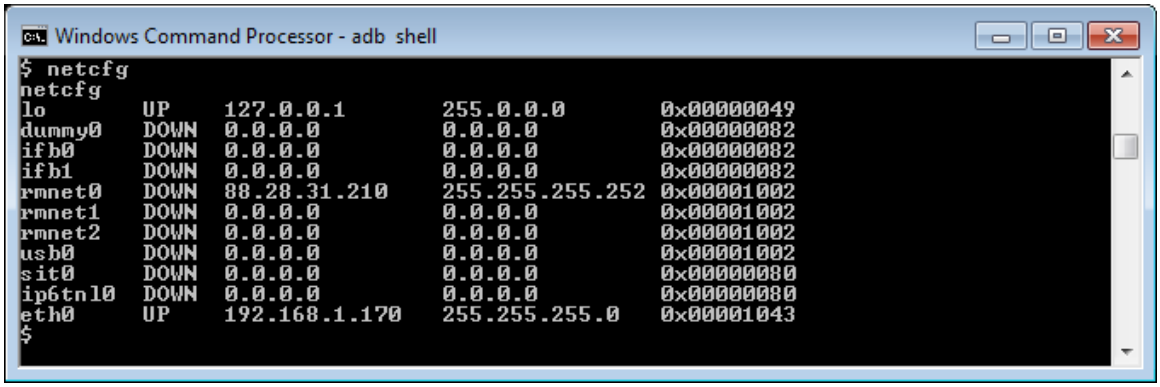
433. El comportamiento del interfaz Wi-Fi, y en consecuencia del interfaz 2G/3G, respecto a las operaciones de ahorro de energía del dispositivo móvil puede ser configurado desde el menú de ajustes de Wi-Fi, tal y como se detalla en el apartado “5.13.1. Desactivación de las comunicaciones Wi-Fi”.

434. El Connectivity Service no permite disponer de varias conexiones activas simultáneamente, opción recomendada desde el punto de vista de seguridad para evitar escenarios dual homing donde la conexión Wi-Fi y la conexión de datos de telefonía móvil (2G o 3G) están activas simultáneamente, con el objetivo de que el dispositivo móvil no actúe de pasarela entre distintas redes.

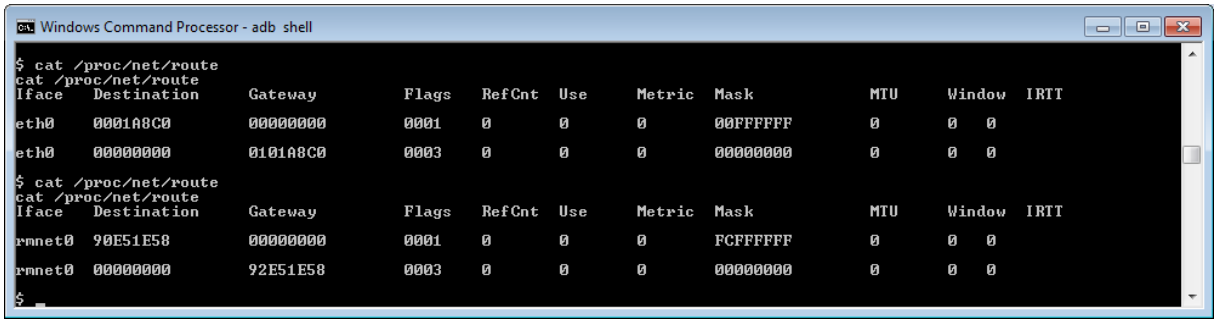
435. Desde el punto de vista de seguridad podría considerarse más seguro cursar todo el tráfico de datos a través de las redes de telefonía móvil (cuando estén disponibles según la cobertura existente) en lugar de a través de redes Wi-Fi, siempre que se fuerce a que la conexión de datos de telefonía móvil empleé tecnologías 3G frente a 2G (ver apartado “5.15. Comunicaciones GSM (2G) y UMTS (3G): voz y datos”). Para ello sería necesario deshabilitar el interfaz Wi-Fi y habilitar las comunicaciones móviles de datos.

436. En el caso contrario, en el que se quiera cursar todo el tráfico de datos a través de redes Wi-Fi se recomienda consultar el apartado “5.15. Comunicaciones GSM (2G) y UMTS (3G): voz y datos”, que contiene información detallada de cómo deshabilitar el interfaz de datos de telefonía móvil.

437. Cuando ambas conexiones de datos han sido activadas, pese a que a través del comando “netcfg” (adb shell) es posible ver la asignación de direcciones IP en ambas redes, Android únicamente utilizará la red de mayor prioridad. En la imagen inferior es posible identificar como el interfaz de la red de telefonía móvil (“rmnet0”) se encuentra en estado DOWN al estar activo el interfaz Wi-Fi (“eth0”), y la dirección IP mostrada para el interfaz “rmnet0” es la correspondiente a la última asignación de DHCP recibida desde la red de telefonía móvil:



438. Adicionalmente, a través de la tabla de rutas ("/proc/net/route") es posible validar el comportamiento descrito. La imagen inferior muestra como el tráfico es dirigido a través del interfaz Wi-Fi ("eth0") al estar ambos interfaces de red activos, empleando el router por defecto 192.168.1.1 (en hexadecimal, y con los valores invertidos, 0x0101A8C0). Posteriormente (segunda ejecución del comando) el tráfico se envía a través del interfaz 2G/3G ("rmnet0") al deshabilitarse el interfaz Wi-Fi, empleando el router 88.30.229.146 (en hexadecimal, y con los valores invertidos, 0x92E51E58):

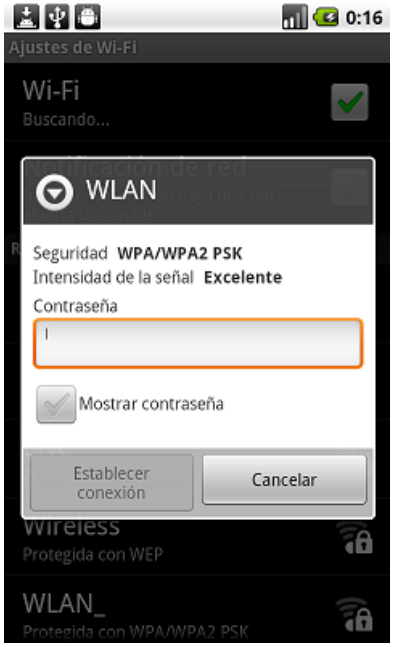


5.13.3 RECOMENDACIONES DE SEGURIDAD PARA LA CONEXIÓN A REDES WI-FI

439. Este apartado proporciona recomendaciones de configuración a través de los diferentes parámetros y opciones disponibles en Android para la conexión segura a redes Wi-Fi.

440. La configuración manual y detallada de las redes Wi-Fi se puede realizar desde el menú "Ajustes – Conexiones inalámbricas (y redes) – Ajustes de Wi-Fi", y en concreto mediante la opción "Añadir red Wi-Fi". Esta opción permite seleccionar todas las opciones de configuración de conexión de una nueva red Wi-Fi, incluyendo el nombre de red (o SSID), el mecanismo de seguridad a emplear (abierta, WEP, WPA/WPA2 PSK o 802.1x EAP), etc. (analizados posteriormente).

441. Adicionalmente, mediante la selección de una de las redes disponibles (listadas en la misma pantalla bajo la sección "Redes Wi-Fi") es posible seleccionar la red Wi-Fi con la que se desea establecer la conexión:



442. Las redes aparecen clasificadas en la lista en orden según la intensidad de señal de cada una de ellas, siendo las redes de la zona superior las de señal de mayor intensidad (de mayor a menor intensidad). La lista permite identificar los mecanismos de seguridad empleados por cada una de la redes.

443. Para establecer la conexión con una red próxima únicamente es necesario introducir la contraseña de acceso a la red (ver imagen superior izquierda) en caso de estar protegida por una contraseña (WEP, WPA/WPA2-PSK). En el caso de redes abiertas únicamente se solicita confirmación por parte del usuario (ver imagen superior derecha).

444. Habitualmente se recomienda hacer uso del mecanismo de configuración manual frente a seleccionar la red Wi-Fi desde el listado de redes disponibles, ya que en este segundo caso, no se dispone de tanta flexibilidad y granularidad para seleccionar los diferentes parámetros de configuración y los mecanismos de seguridad de la red. Sin embargo, en el caso de Android se recomienda añadir la red Wi-Fi desde el listado de redes disponibles (ver apartado “5.13.4. Conexión automática a redes Wi-Fi”).

445. Todas las redes que implementan algún tipo de mecanismo de seguridad, WEP, WPA ó WPA2, aparecen con un candado en el icono de la red, pero Android adicionalmente permite diferenciar el mecanismo de seguridad empleado específicamente desde el listado de redes disponibles, proporcionando los detalles bajo el nombre de la red.

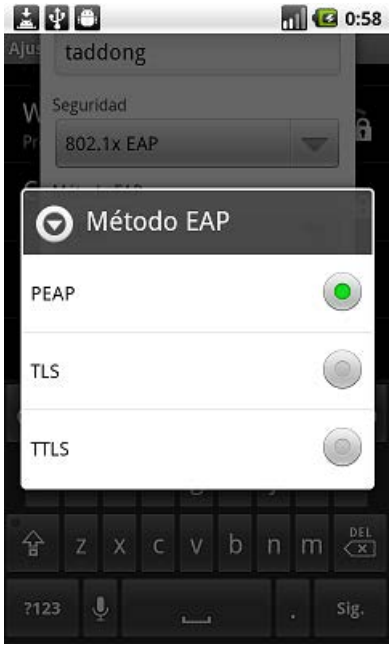
446. Al establecer una primera conexión con una nueva red Wi-Fi, se recomienda agregar la nueva red Wi-Fi de forma automática a través del listado de redes disponibles (debido a una vulnerabilidad descrita posteriormente), pese a que no sea posible visualizar y especificar todas las opciones de configuración disponibles, descritas a continuación.

447. El proceso de configuración de la contraseña puede permitir al usuario no ocultar el texto introducido en pantalla (por ejemplo con el carácter “·”) mediante la opción “Mostrar contraseña” (no habilitada por defecto).

448. En caso de habilitar esta funcionalidad, opción no recomendada, el usuario debe prestar atención a cómo y dónde introduce la contraseña de conexión a la red Wi-Fi para evitar que un potencial atacante la obtenga mediante acceso visual a la pantalla del dispositivo.

449. Dentro de las opciones de configuración de una nueva red Wi-Fi, la primera pantalla de configuración hace posible especificar el nombre de la red (SSID) y el mecanismo de seguridad a emplear: abierta (opción por defecto), WEP, WPA/WPA2 PSK o 802.1x EAP.

450. En caso de seleccionar una red WEP o WPA/WPA2-PSK, es necesario especificar la contraseña de la red (ver imagen inferior izquierda). En el caso de seleccionar una red 802.1x EAP, es necesario especificar el tipo de EAP a emplear: PEAP, TLS o TTLS (ver imagen inferior derecha).



451. Desafortunadamente, Android no permite especificar detalladamente los mecanismos de autentificación y de cifrado de datos, no siendo posible diferenciar entre redes WPA y redes WPA2 (PSK o Enterprise), ni el tipo de cifrado: TKIP, AES o ambos.

452. Por otro lado, tampoco es posible especificar si se permiten conexiones a redes con infraestructura, es decir, puntos de acceso, a redes entre equipos o ad-hoc, o ambas.

453. Android por defecto sigue la recomendación general de seguridad de no permitir conexiones Wi-Fi ad-hoc, permitiendo únicamente conexiones a redes Wi-Fi con infraestructura, es decir, basadas en puntos de acceso. La pantalla que muestra el listado de redes Wi-Fi disponibles directamente no muestra las redes ad-hoc.

Nota: Esta limitación del gestor de conexiones Wi-Fi de Android está implícita en el diseño del sistema y es conocida desde las primeras versiones de Android [Ref.- 40].

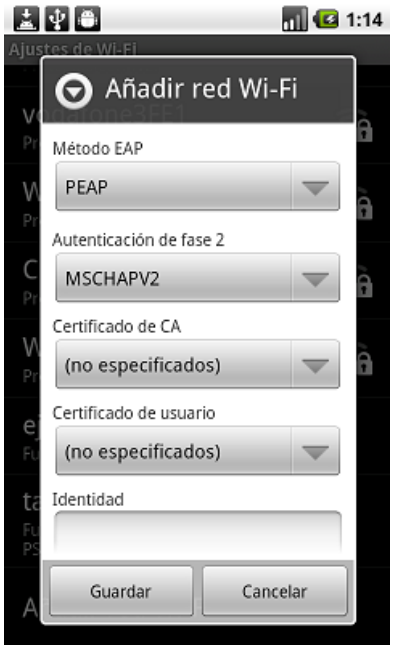
Aunque desde el punto de vista de seguridad se desaconseja modificar este comportamiento, es posible habilitar el soporte para redes *ad-hoc* en dispositivos móviles Android *rooted* a través del interfaz de depuración USB (adb) modificando el fichero "wpa_supplicant" de fábrica [Ref.- 41].

La versiones 2.3 y 4.0 de Android implementen Wi-Fi Direct, un estándar de comunicación Wi-Fi directa entre dispositivos [Ref.- 42] que sustituye a las comunicaciones *ad-hoc*, y añade mejoras de seguridad, facilidad de configuración, rendimiento y consumo.

454. Igualmente, el proceso de configuración de las redes Wi-Fi en Android no permite claramente, y de forma explícita, especificar si la red Wi-Fi es oculta o visible (ver apartado "5.13.4. Conexión automática a redes Wi-Fi").

455. Se recomienda conectarse únicamente a redes que emplean WPA2 (Personal, WPA2-PSK, o Enterprise, WPA2) como mecanismo de autentificación, y AES como mecanismo de cifrado. En su defecto, debería emplearse WPA/TKIP.

456. En caso de emplear WPA2 (o WPA) en su versión Enterprise, es decir, con mecanismos basados en 802.1X/EAP, la pantalla de ajustes permite especificar los parámetros de configuración asociados al tipo de mecanismo EAP empleado:



457. Todos los campos de configuración están disponibles en el interfaz de usuario de Android para los distintos tipos de EAP, lo que puede crear cierta confusión, ya que no todos los tipos de EAP hacen uso de los diferentes campos mostrados.

458. En primer lugar es necesario definir el tipo de autentificación interna (o de fase 2): Ninguno, PAP, MSCHAP, MSCHAPV2 (PEAPv0) o GTC (EAP-GTC, Generic Token Card).

459. Adicionalmente, para PEAP (Protected EAP) debe definirse el certificado digital raíz de la autoridad certificadora (CA) empleada para generar el certificado digital del servidor de autentificación de la red Wi-Fi (RADIUS), mediante el campo "Certificado de CA", que debe haber sido añadido previamente al dispositivo móvil (ver apartado "5.7.1. Certificados digitales y credenciales del usuario"). Asimismo, deben proporcionarse las credenciales del usuario (nombre de usuario y contraseña, y opcionalmente el dominio Windows (por ejemplo "DOMINIO\usuario") en los campos "Identidad" y "Contraseña" (ver imágenes superiores).

460. Por otro lado, para TTLS (conocido como EAP-TTLS) es necesario definir los mismos elementos que para PEAP, pero haciendo uso de la identidad anónima a utilizar para la autentificación externa o de fase 1, mediante el campo "Identidad anónima" (por ejemplo, con el valor estándar "anonymous").

461. Por último, para TLS (conocido como EAP-TLS) es necesario definir los mismos elementos que para PEAP, pero sustituyendo las credenciales tradicionales del usuario (nombre de usuario y contraseña) por un certificado digital cliente personal y que identifica al usuario, mediante el campo "Certificado de usuario", y que debe haber sido añadido previamente al dispositivo móvil (ver apartado "5.7.1. Certificados digitales y credenciales del usuario").

462. En el caso de emplear EAP-TLS siempre es necesario importar un certificado digital personal (en formato PKCS #12) en el dispositivo móvil. Para instalar el certificado personal basta con transferir el fichero del certificado digital personal (.pfx o .p12; en el caso de Android debe emplearse obligatoriamente la extensión .p12) al dispositivo móvil a través de una tarjeta de almacenamiento externa o desde la web (o webmail) (ver apartado "5.7.1. Certificados digitales y credenciales del usuario").

463. Una vez el certificado personal ha sido importado en el dispositivo móvil, estará disponible a través del menú de configuración de la red Wi-Fi 802.1x EAP basada en TLS, desde el campo "Certificado de usuario":

Nota: El certificado digital de usuario es identificado por defecto con un *string* con letras y números si no se modificó su nombre asociado durante el proceso de importación (ver apartado "5.7.1. Certificados digitales y credenciales del usuario"). Android permite importar el mismo certificado digital de usuario con diferentes nombres múltiples veces.

464. Tanto en el caso de autentificación PEAP como TLS o TTLS, es necesario importar previamente en Android el certificado digital de la autoridad certificadora (CA), raíz o intermedia, empleada para generar los certificados digitales asociados al servidor de autentificación de la red Wi-Fi (servidor RADIUS), salvo que se usen certificados emitidos por una de las CAs ya existentes por defecto en Android.

465. Para instalar el certificado basta con transferir el fichero del certificado digital en formato de codificación PEM (obligatoriamente con extensión .crt) al dispositivo móvil, a través de un servidor web [Ref.- 46] o mediante una tarjeta de almacenamiento externa.

466. Una vez se dispone del fichero del certificado digital en la tarjeta de almacenamiento externa, es necesario importarlo a través de el menú "Ajustes – Ubicación y seguridad - Instalar desde la tarjeta SD".

467. En el caso de disponer de varios certificados en el directorio raíz de la tarjeta de almacenamiento (ver imagen inferior izquierda), será necesario seleccionar el que se desea importar, y modificar el nombre con el que será identificado durante su utilización si así se desea (ver imagen inferior derecha):

468. El método de importación de certificados raíz (.crt) es similar el empleado para la importación de certificados de usuario (.p12) (ver apartado "5.7.1. Certificados digitales y credenciales del usuario").

469. El certificado digital importado será eliminado automáticamente de la tarjeta de almacenamiento externa una vez se ha completado la operación de importación.

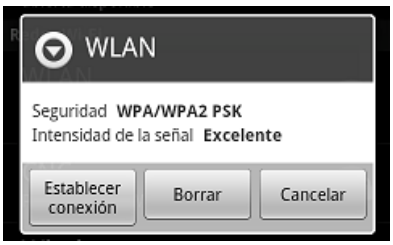
470. Una vez el certificado ha sido importado en el dispositivo móvil, estará disponible a través del menú de configuración de la red Wi-Fi 802.1x EAP basada en PEAP, TTLS o TLS, desde el campo "Certificado de CA":

Nota: Los certificados raíz importados mediante estos métodos sólo afectan a las conexiones Wi-Fi y VPN que hacen uso de certificados digitales, y no a otro tipo de conexiones, como por ejemplo sesiones web mediante HTTPS (ver apartado "5.7.1. Certificados digitales y credenciales del usuario").

471. La lista de redes preferidas (PNL), es decir, a las que se ha conectado previamente el dispositivo móvil o que han sido configuradas en el mismo (ver apartado "5.13.4. Conexión automática a redes Wi-Fi"), puede ser visualizada tras habilitar el interfaz Wi-Fi, desde el menú "Ajustes – Conexiones inalámbricas (y redes) – Ajustes de Wi-Fi", bajo la sección "Redes Wi-Fi" y, en concreto, al final de la lista de redes disponibles, identificadas con el texto "Fuera de rango" (por ejemplo, las redes Wi-Fi "taddong" y "ejemplo" en la imagen inferior izquierda).

472. Las redes existentes en la PNL que están disponibles actualmente aparecerán en la lista de redes disponible con un distintivo que las identifica como redes con las que previamente se ha establecido una conexión, mediante por ejemplo el texto "Recordada" o "Conectada" (por ejemplo, la red "WLAN" en la imagen inferior derecha):

473. Mediante la selección de una red existente en la PNL desde la pantalla con el listado de redes Wi-Fi (con una pulsación sobre la misma), es posible eliminarla de la PNL a través del botón "Borrar" (tanto si no es visible actualmente, imagen izquierda, como si lo es, imagen derecha):



474. Mediante la selección de una red existente en la PNL desde la pantalla con el listado de redes Wi-Fi (con una pulsación sobre la misma continuada), es también posible eliminarla de la PNL o editar sus detalles (como la contraseña de acceso) a través del botón "Modificar red" (tanto si no es visible actualmente, como si lo es):

475. Por defecto, la configuración de TCP/IP empleada para la conexión a las redes Wi-Fi hace uso de una dirección IP dinámica obtenida mediante el protocolo DHCP (ver apartado "5.16. Comunicaciones TCP/IP").

476. En la versión 2.2 y 2.3 es posible fijar una dirección IP estática (junto a la puerta de enlace, la máscara de red, y los servidores DNS primario y secundario) desde el menú "Ajustes – Conexiones inalámbricas (y redes) – Ajustes de Wi-Fi", mediante el botón "Menú", y la opción "Avanzado":

477. Para llevar a cabo la configuración de TCP/IP, o modificaciones en la misma, no es necesario que el interfaz Wi-Fi esté activo.

478. En resumen, desde el punto de vista de seguridad de Android como cliente Wi-Fi, se recomienda hacer uso de redes inalámbricas no ocultas (ver apartado "5.13.4. Conexión automática a redes Wi-Fi"), basadas en WPA2 con cifrado AES, y autentificación de tipo Personal, con una contraseña de acceso (PSK, Personal Shared Key) suficientemente robusta (más de 20 caracteres), o de tipo Enterprise, basada en mecanismos de autentificación 802.1X/EAP, y de tipo EAP-TLS preferiblemente.

Nota: Con el objetivo de proteger el dispositivo móvil y aumentar su nivel de seguridad, se desaconseja el uso de redes inalámbricas públicas y abiertas, con un nivel de seguridad reducido o inexistente (sin mecanismos de autentificación y cifrado), como por ejemplo *hotspots* Wi-Fi disponibles en hoteles, aeropuertos o centros de conferencias [Ref.- 1].

Los riesgos de seguridad asociados a este tipo de entornos incluyen la captura e interceptación del tráfico y datos por parte de un potencial atacante, la posibilidad de inyección de tráfico para la realización de ataques directos y de accesos no autorizados contra el dispositivo móvil, ataques de suplantación de la red, y a ataques de denegación de servicio, entre otros.

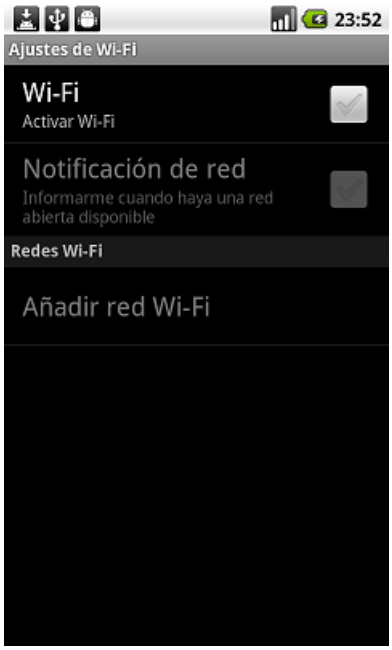
5.13.4 CONEXIÓN AUTOMÁTICA A REDES WI-FI: OCULTAS O VISIBLES

479. Android intenta conectarse automáticamente a las redes Wi-Fi existentes en su lista de redes preferidas (PNL, Preferred Network List). Si alguna de estas redes Wi-Fi está disponible, establecerá la conexión automáticamente.

Nota: No se ha identificado ninguna opción de configuración en el interfaz de usuario de Android para deshabilitar el proceso de conexión automática a redes Wi-Fi si el interfaz Wi-Fi está activo.

480. La lista de redes preferidas (PNL) está disponible a través del menú "Ajustes – Conexiones inalámbricas (y redes) – Ajustes de Wi-Fi", bajo la sección "Redes Wi-Fi". En el caso de redes no disponibles, aparecerán al final de la lista de redes, identificadas con el texto "Fuera de rango". En el caso de redes disponibles, aparecerán a lo largo de la lista de redes (según la intensidad de su señal), identificadas con el texto "Recordada" (temporalmente) o "Conectada" (si se trata de la red a la que está conectado el dispositivo móvil actualmente).

481. La lista de redes preferidas sólo está disponible cuando el interfaz Wi-Fi está habilitado, no siendo posible acceder a ellas (para su borrado o edición) si está deshabilitado:



482. Debe tenerse en cuenta que no existe la opción de desconectarse de la red a la que el dispositivo móvil está conectado actualmente. La única opción disponible es deshabilitar el interfaz Wi-Fi.

483. Las redes Wi-Fi pueden ser configuradas en dos modos: oculto o visible. Las redes ocultas son aquellas que no especifican el nombre de la red (SSID, Service Set Identifier) en las tramas de anuncio de broadcast o beacons, redes también conocidas como nonbroadcast. Las redes visibles son las que sí incluyen el nombre de red en esas tramas.

484. Desde el punto de vista de seguridad, y con el objetivo de proteger a los clientes de la red Wi-Fi, se recomienda no hacer uso de redes ocultas.

485. Aunque en primera instancia puede parecer que el uso de redes Wi-Fi ocultas es una opción más segura, en realidad no es así, ya que es sencillo para un potencial atacante descubrir su existencia e incluso el nombre de esas supuestamente redes ocultas.

486. El uso de una red oculta implica reducir el nivel de seguridad en los clientes Wi-Fi que se conectan a ella, como por ejemplo los dispositivos móviles basados en Android. Si una red está oculta, los clientes Wi-Fi se verán obligados a comprobar de forma explícita si está presente, generando tramas (de tipo probe request) que desvelan el nombre de la red, y lo que es más crítico, que les exponen frente a ataques de suplantación de dicha red por parte de un potencial atacante (especialmente cuando la red no emplea mecanismos de seguridad).

487. Desafortunadamente, Android no implementa ningún mecanismo explícito para definir si una red es oculta o no, por lo que en función de cómo se añada la red Wi-Fi al dispositivo móvil la primera vez, ésta será considerada como una red Wi-Fi oculta o visible.

488. Si la red Wi-Fi es añadida al dispositivo, y en consecuencia a la PNL, seleccionándola de la lista de redes disponibles (situación que sólo se puede presentar si la red es visible), será añadida como red visible (escenario que aporta mayor seguridad a la configuración de Android).

489. Si la red Wi-Fi es añadida al dispositivo, y en consecuencia a la PNL, mediante el botón “Añadir red Wi-Fi” disponible bajo la lista de redes disponibles (situación necesaria a la hora de añadir redes ocultas), será añadida como red oculta (escenario vulnerable desde el punto de vista de Android):

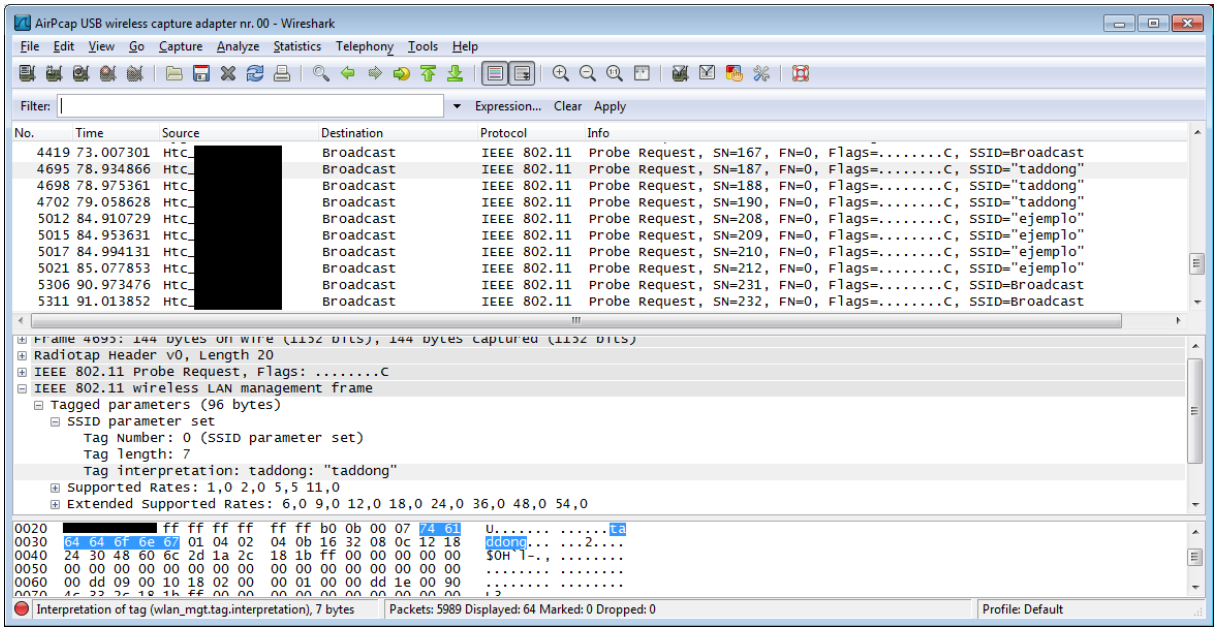
490. Este es el comportamiento más vulnerable (existente y corregido en los sistemas operativos y ordenadores portátiles y de sobremesa hace años), ya que obliga a Android a generar tráfico que desvela la lista de redes Wi-Fi configuradas en el dispositivo móvil (conocida como la PNL, Preferred Network List). Este comportamiento presenta un escenario similar al existente en equipos de escritorio basados en Windows XP sin la actualización de seguridad KB917021 aplicada [Ref.- 50].

491. Adicionalmente, debe tenerse en cuenta que una vez una red Wi-Fi ha sido añadida al dispositivo móvil y está en la PNL, no se dispone de un mecanismo a través del interfaz gráfico de Android para determinar si es considerada oculta o visible.

492. Resumiendo para todas aquellas redes configuradas o añadidas a través del botón "Añadir red Wi-Fi", Android generará tráfico que desvelará estas redes Wi-Fi disponibles en su lista de redes e intentará conectarse a ellas, escenario que puede ser empleado por un potencial atacante para disponer de conectividad con el dispositivo móvil y proceder a explotar vulnerabilidades en el mismo.

493. Por tanto, no se recomienda añadir ninguna red Wi-Fi manualmente al dispositivo móvil a través de este botón, aunque es una práctica común desde el punto de vista de seguridad para disponer de mayor control sobre la configuración de la red a añadir.

494. En la imagen inferior, el dispositivo móvil Android intenta descubrir la presencia de dos redes disponibles en su configuración, "ejemplo" y "taddong", durante el proceso de encendido del terminal, cada vez que se produce la activación del interfaz Wi-Fi y periódicamente una vez el interfaz Wi-Fi ha sido activado, e incluso aunque esté conectado a otra red Wi-Fi diferente:



495. Esta vulnerabilidad de revelación de información en función de cómo han sido añadidas las redes Wi-Fi a Android ha sido confirmada por el Android Security Team (Google), aunque no publicará una actualización para solucionarla [Ref.- 92].

496. Android introducirá modificaciones en el interfaz de usuario empleado para añadir redes Wi-Fi en futuras versiones con el objetivo de solucionar esta vulnerabilidad, dado que se veían afectadas todas las versiones 2.x y 3.x de Android existentes en el momento de su publicación.

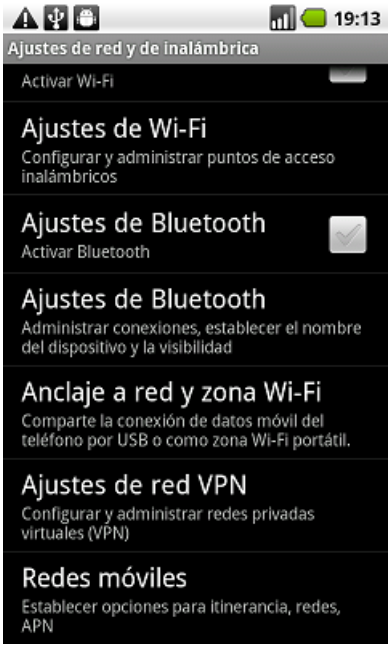
Nota: La versión 2.2 de Android introdujo este cambio en el comportamiento de la pila de comunicaciones Wi-Fi, ya que en versiones previas (incluso versiones previas a 2.2 y la compilación FRF91 empleada para la elaboración de la presente guía) no era posible conectarse con redes Wi-Fi ocultas (tal como identifica el bug 1041 de Android [Ref.- 43]); en el pasado incluso aparecieron aplicaciones en Google Play para añadir esta funcionalidad.

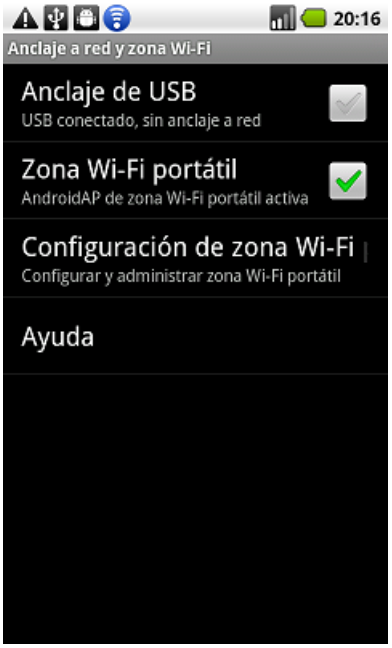
En cualquier caso, siempre antes de poder establecer una conexión con una red Wi-Fi oculta es necesario añadirla al dispositivo móvil de forma manual, para que éste conozca su existencia, y pueda preguntar sobre su disponibilidad (empleando el comportamiento vulnerable descrito previamente).

5.13.5 PUNTO DE ACCESO WI-FI

497. Android dispone de capacidades nativas para actuar como punto de acceso Wi-Fi y router (o enrutador) hacia Internet, proporcionando acceso a múltiples dispositivos (u ordenadores, hasta un máximo de 8) vía Wi-Fi a su conexión de datos de telefonía móvil (2G/3G) [Ref.- 91]. Para ello es necesario habilitar la conexión de datos móviles previamente (ver apartado "5.15. Comunicaciones GSM (2G) y UMTS (3G): voz y datos").

498. Para hacer uso de estas capacidades es necesario acceder al menú "Ajustes – Conexiones inalámbricas (y redes) – Anclaje a red y zona Wi-Fi":

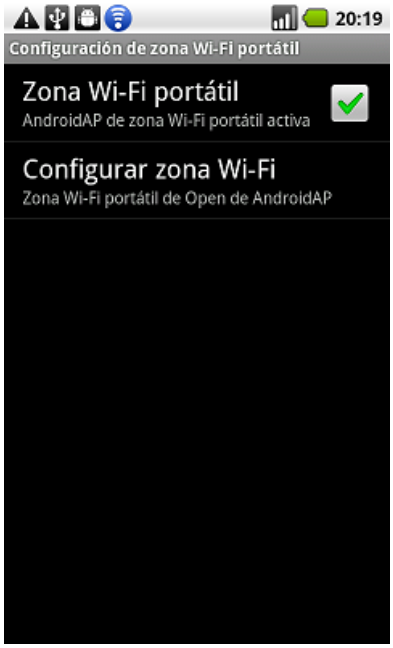




499. A través de la opción "Zona Wi-Fi portátil" es posible habilitar el servicio de punto de acceso Wi-Fi (referido en ocasiones como hotspot Wi-Fi), de forma que otros ordenadores y dispositivos pueda utilizar el dispositivo móvil como punto de acceso Wi-Fi para conectarse a Internet.

500. Debe tenerse en cuenta que, al igual que para el interfaz Wi-Fi (cliente) y Bluetooth, para poder llevar a cabo la configuración del punto de acceso Wi-Fi a través del interfaz de usuario del dispositivo móvil es obligatorio activar esta funcionalidad (como se muestra en las dos siguientes imágenes) por lo que se recomienda activar la funcionalidad y realizar las modificaciones de la configuración en un entorno seguro, para evitar potenciales ataques cuando los mecanismos de seguridad no han sido aún aplicados:

501. Una vez habilitado, mediante la opción "Configuración de zona Wi-Fi", es posible configurar los diferentes ajustes del punto de acceso, incluyendo el nombre de la red Wi-Fi (o SSID) y las características de seguridad:



502. Por defecto, el punto de acceso Wi-Fi que es habilitado es abierto ("Open"), es decir, no implementa ningún mecanismo de seguridad (ver imagen superior derecha). Android permite la creación de puntos de acceso Wi-Fi mediante WPA2-PSK (Pre Shared Key, o WPA2-Personal), basado en el uso de una clave compartida:

503. Cuando el dispositivo móvil actúa de punto de acceso Wi-Fi, las aplicaciones Android no pueden utilizar la conexión Wi-Fi como dispositivo cliente. Si previamente a su activación la conexión Wi-Fi cliente estaba activa, ésta será deshabilitada automáticamente. Igualmente, tras desactivar el punto de acceso Wi-Fi, la conexión Wi-Fi cliente será habilitada de nuevo automáticamente.

504. Se recomienda no habilitar las capacidades de punto de acceso Wi-Fi en el dispositivo móvil salvo que se quiera hacer un uso limitado y controlado de esta funcionalidad. En caso de ser utilizada, la red Wi-Fi asociada debe ser protegida y configurada mediante WPA2-PSK con una contraseña o clave precompartida suficientemente larga (más de 20 caracteres) y difícilmente adivinable [Ref.- 49].

505. El mecanismo de cifrado empleado por defecto por el punto de acceso Wi-Fi si los dispositivos u ordenadores que se conectan a éste lo soportan es AES-CCMP, recomendado desde el punto de vista de seguridad.

506. En caso de activar el punto de acceso Wi-Fi, se recomienda también modificar el nombre de la red Wi-Fi (o SSID) anunciada por el dispositivo móvil por defecto (“AndroidAP”), con el objetivo de no desvelar que se trata de un punto de acceso basado en Android.

507. La red Wi-Fi creada es de tipo punto de acceso (o infraestructura), se anuncia en el canal 6 (de 802.11g), y proporciona incluso capacidades de servidor DHCP para la asignación de direcciones IP a los dispositivos cliente y ordenadores que se conectan a ella:

508. Tras establecerse la conexión de red a través de la red Wi-Fi creada por Android, y tomando Windows 7 como sistema operativo del ordenador de referencia, el interfaz de red Wi-Fi funciona al estar configurado con una dirección IP dinámica (DHCP), asignándose por defecto una dirección IP de clase C (/24), como por ejemplo 192.168.43.123.

509. El dispositivo móvil (por ejemplo, con dirección IP 192.168.43.1) actúa de gateway, router o pasarela por defecto, de servidor DHCP, y de servidor DNS, y es alcanzable mediante ping (ICMP).

Nota: El direccionamiento IP empleado por Android para el punto de acceso Wi-Fi (192.168.43.x) no puede ser modificado salvo en dispositivos móviles *rooted* [Ref.- 96].

510. La dirección MAC asociada al interfaz de red del punto de acceso Wi-Fi tiene asociado un OUI con valor “92:21:55”, qué no está asignado a ningún vendedor públicamente en el momento de elaboración de la presente guía (similar al valor “90:21:55” de HTC).

511. Un análisis de los puertos TCP/IP y servicios disponibles en el interfaz de red empleado para el punto de acceso Wi-Fi del dispositivo móvil permite obtener las siguientes conclusiones:

- El único puerto TCP abierto es el correspondiente al servidor DNS (53/tcp). El servidor DNS es identificado por Nmap como “dnsmasq 2.51”.
- Los únicos puertos UDP abiertos son los correspondientes al servidor DNS (53/udp) y al servidor DHCP (67/udp).

512. Es posible interrumpir la disponibilidad del punto de acceso Wi-Fi deshabilitando la opción “Zona Wi-Fi portátil” habilitada previamente, opción recomendada desde el punto de vista de seguridad una vez no se desea disponer de la conexión de red Wi-Fi.

5.14 COMUNICACIONES GSM (2G) Y UMTS (3G): MENSAJES DE TEXTO (SMS)

513. Las capacidades de mensajería de texto (SMS, *Short Message Service*) de los dispositivos móviles permite el envío de mensajes cortos empleando la infraestructura GSM *(Global System for Mobile communications, o 2G*) o UMTS (*Universal Mobile Telecommunications System, o 3G).*

514. El primer nivel de protección asociado al sistema de mensajería de texto pasa por la concienciación del usuario desde el punto de vista de seguridad, teniendo en cuenta que la implementación de este módulo en los dispositivos móviles actuales proporciona numerosas funcionalidades, y no únicamente la visualización de mensajes de texto.

515. Entre las funcionalidades avanzadas se encuentra la posibilidad de mostrar contenidos de texto, contenidos web (HTML, JavaScript, etc.), gestionar datos binarios, como tonos de llamada, e intercambiar ficheros multimedia (audio, vídeo e imágenes), sobre todo en sus variantes avanzadas: EMS (Enhanced Messaging Service) y MMS (*Multimedia Message Service).*

516. Debido a las diferentes vulnerabilidades asociadas al módulo de mensajería de texto en múltiples dispositivos móviles actuales, incluyendo Android [Ref.- 1], se recomienda que el usuario actúe con prudencia ante la lectura de nuevos mensajes de texto, especialmente los recibidos de fuentes desconocidas.

517. Durante el año 2009 se publicaron diferentes vulnerabilidades de denegación de servicio (DoS) en el módulo SMS de dispositivos Android [Ref.- 1]. El proceso que gestiona los mensajes SMS en Android es una aplicación Java:

518. Se recomienda no abrir ningún mensaje de texto no esperado o solicitado, práctica similar a la empleada para la gestión de correos electrónicos. A la hora de acceder y procesar los contenidos del buzón de entrada de mensajes de texto del dispositivo móvil, el usuario debería seguir las mejores prácticas de seguridad, como por ejemplo:

- No deberían abrirse mensajes de texto recibidos desde números desconocidos, ni ejecutar o permitir la instalación de contenidos adjuntos (configuraciones, binarios o multimedia) asociados a mensajes SMS/MMS no esperados.
- En su lugar, se debería proceder a borrar el mensaje directamente.
- En caso de acceder a los mensajes, debería desconfiarse de su contenido, y tener especial cuidado, por ejemplo, con la utilización de enlaces a sitios web externos.

519. Adicionalmente, es necesario tener en cuenta que los mensajes de texto pueden contener información sensible y confidencial. Por ejemplo, al gestionar el buzón de voz de un usuario, los operadores de telefonía móvil envían todos los detalles de acceso al buzón de voz, incluido el PIN, mediante un mensaje de texto. El acceso a dicho mensaje por parte de un potencial atacante permitiría disponer de control completo del buzón de voz del usuario.

520. Los nuevos mecanismos de autentificación de la banca online también emplean los mensajes de texto para el envío de contraseñas de un solo uso para la realización de operaciones bancarias críticas. El acceso a dicho mensaje por parte de un potencial atacante permitiría completar la operación, como por ejemplo, una transferencia bancaria.

Nota: Existen soluciones propietarias de cifrado de mensajes de texto (SMS), como TextSecure, proporcionadas por terceras compañías de forma gratuita a través de Google Play, que cifran los mensajes de texto tanto durante su almacenamiento en el dispositivo móvil como durante su trasmisión a otros usuarios de la aplicación TextSecure [Ref.- 33]. TextSecure hace uso del protocolo OTR (Off The Record) para cifrar los mensajes de texto.

5.15 COMUNICACIONES GSM (2G) Y UMTS (3G): VOZ Y DATOS

5.15.1 DESACTIVACIÓN DE LAS COMUNICACIONES DE VOZ Y DATOS 2G/3G

521. La principal recomendación de seguridad asociada a las comunicaciones de voz (y SMS) a través de las redes de telefonía móvil en dispositivos móviles es no activar las capacidades de telefonía del terminal salvo que se haga uso de éstas (situación muy habitual, al ser ésta una de las funcionalidades principales de los dispositivos móviles).

Nota: Durante el proceso de configuración inicial del dispositivo móvil empleado para la elaboración de la presente guía (activado automáticamente la primera vez que se enciende el terminal), el interfaz de telefonía móvil para comunicaciones de voz está habilitado, solicitando en primer lugar el PIN de la tarjeta SIM si ésta está insertada.

Se recomienda desactivar el interfaz de telefonía móvil tan pronto finalice el proceso de configuración inicial, para proceder a la aplicación de las medidas de seguridad seleccionadas.

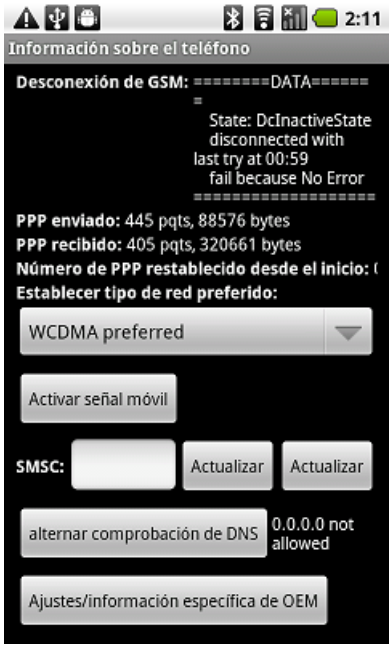
522. Android únicamente permite a través del interfaz de usuario estándar deshabilitar de forma individualizada las capacidades de telefonía móvil (voz y SMS) a través de la opción “Modo avión” del menú “Ajustes – Conexiones inalámbricas (y redes)”.

523. Al activar el modo avión en Android, la conectividad a redes Wi-Fi puede ser habilitada posteriormente y de forma independiente, mientras la conectividad de telefonía móvil sigue deshabilitada. No así la conectividad de Bluetooth, directamente ligada al modo avión, al igual que la conectividad móvil 2G/3G.

524. Adicionalmente, es posible obtener y configurar información avanzada a través del menú de prueba (o testing), disponible en Android tras marcar el siguiente número de teléfono: *#*#4636#*#* (o *#*#info#*#*). Esta funcionalidad permite independizar la desconexión de los diferentes interfaces de comunicaciones inalámbricos, es decir, Bluetooth, Wi-Fi y telefonía móvil 2G/3G.

525. Sin activar el modo avión, y teniendo activados los interfaces Bluetooth y Wi-Fi, mediante la selección de la opción “Información sobre el teléfono” es posible desconectar únicamente el interfaz de telefonía móvil 2G/3G. Para ello es necesario seleccionar el botón “Desactivar señal móvil” en la parte inferior, y como resultado se desactivará

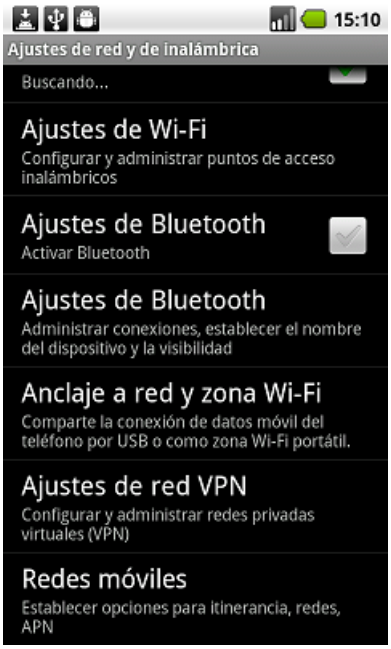
únicamente y por completo (voz y datos) el interfaz de radio de telefonía móvil, permaneciendo los interfaces de Bluetooth y Wi-Fi activos, tal y como denotan los iconos de la barra de estado:



526. Este cambio de configuración no prevalece tras reiniciar el dispositivo móvil, dónde de nuevo el interfaz de radio de telefonía móvil será activado automáticamente tras introducir el PIN.

527. Por otro lado, la principal recomendación de seguridad asociada a las comunicaciones de datos a través de las infraestructuras de telefonía móvil en dispositivos móviles es no activar las capacidades de transmisión y recepción de datos salvo en el caso en el que se esté haciendo uso de éstas, evitando así la posibilidad de ataques sobre el hardware del interfaz, el driver, la pila de comunicaciones móviles y cualquiera de los servicios y aplicaciones disponibles a través de esa red y la conexión a Internet.

528. Las conexiones de datos a través de la red de telefonía móvil (2G/3G), GPRS o UMTS, pueden ser deshabilitadas a través del menú “Ajustes – Conexiones inalámbricas (y redes) – Redes móviles” y en concreto de la opción “Datos habilitados”:



529. La opción “Itinerancia de datos” (o roaming) permite configurar si se desea hacer uso de las capacidades de datos de telefonía móvil del dispositivo cuando se viaja al extranjero y el terminal se encuentra en una red de otro operador al asociado por defecto a su tarjeta SIM.

Nota: Además de la seguridad, una de las preocupaciones de los usuarios de dispositivos móviles sin tarifa plana de conexión de datos son los cargos asociados al uso de las comunicaciones de datos a través de las redes de telefonía móvil (2G/3G), especialmente cuando el contrato tiene gastos asociados por la cantidad de datos transmitidos y/o por tiempo o número de conexiones establecidas, o se viaja internacionalmente (itinerancia o *roaming*). Múltiples aplicaciones en Android pueden iniciar este tipo de conexiones de datos en diferentes momentos del día.

530. Por defecto en Android (configuración de fábrica) el interfaz de datos de telefonía móvil está habilitado (con los APNs que han sido definidos por la tarjeta SIM empleada).

531. Android mantiene el estado del interfaz de telefonía de datos tras reiniciar el dispositivo móvil, es decir, si el interfaz de telefonía de datos estaba activo al apagar el terminal, al encender el dispositivo móvil e introducir el PIN de la tarjeta SIM, seguirá activo.

532. Igualmente, al salir del modo avión el estado del interfaz de datos de telefonía móvil será restaurado, y se activará en el caso de haber estado activo previamente (antes de activar el modo avión).

533. Tras desactivar la conexión de datos, si alguna aplicación requiere disponer de conectividad (por ejemplo, navegación web desde el “Navegador”) la conexión de telefonía de datos no será activada automáticamente.

5.15.2 CONFIGURACIÓN Y SELECCIÓN DE LA RED (VOZ) DE TELEFONÍA MÓVIL

534. Android permite al usuario utilizar la red de telefonía móvil configurada automáticamente a través de la tarjeta SIM, así como seleccionar de forma manual el operador de telecomunicaciones móviles (voz y SMS).

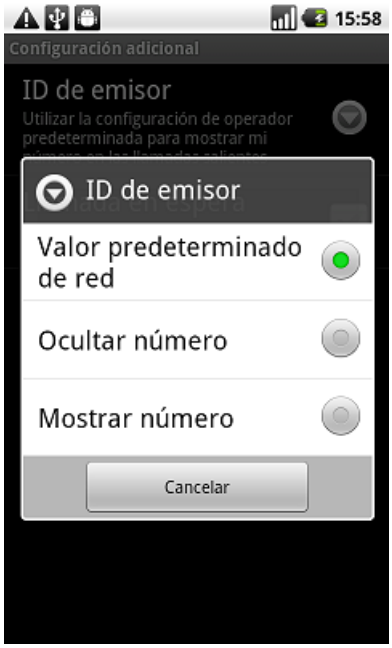
535. Desde el menú de configuración del teléfono (“Ajustes – Conexiones inalámbricas (y redes) – Redes móviles”) y a través de la opción “Operadores de red”, es posible acceder a las opciones para seleccionar el operador de red, ya sea de forma automática como manual.

536. Android llevará a cabo una búsqueda automática de las redes disponibles en la ubicación actual del dispositivo móvil, y mostrará al usuario la lista de operadores de telecomunicaciones identificados:

537. La selección de red permite definir si la red de telefonía será seleccionada de forma automática (opción por defecto) por el dispositivo móvil en función de la tarjeta SIM y de la intensidad de la señal, o sí el usuario puede definir de forma manual la red a la que desea conectarse de la lista de redes disponibles.

538. Con el objetivo de proteger la privacidad del usuario, el módulo de telefonía de Android permite al usuario definir en qué tipo de llamadas se enviará la información de identificación como autor de la llamada: Valor predeterminado de red (opción por defecto), ocultar número (siempre) o mostrar número (para todas las llamadas).

539. Desde el menú “Ajustes – Ajustes de llamada – Configuración adicional”, mediante la opción “ID de emisor”, es posible configurar la opción deseada:



Nota: Existen soluciones propietarias de cifrado extremo a extremo de las comunicaciones y llamadas de voz, como RedPhone, proporcionadas por terceras compañías de forma gratuita a través de Google Play [Ref.- 33]. RedPhone hace uso del protocolo ZRTP para cifrar las comunicaciones de Voz sobre IP (VoIP) entre dos terminales Android, haciendo uso de la infraestructura de los operadores de telefonía móvil, comunicaciones de datos SSL y mensajes SMS cifrados para el establecimiento de las llamadas.

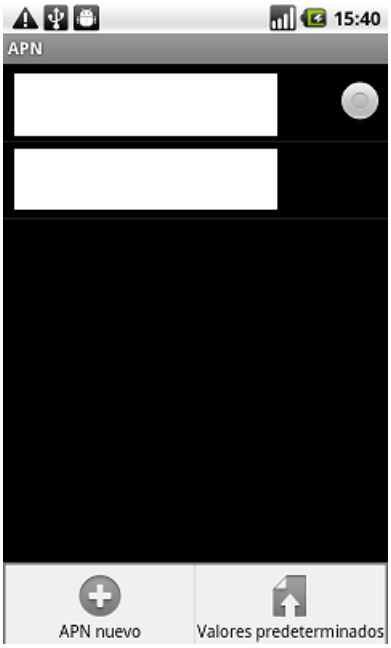
5.15.3 CONFIGURACIÓN DE LA RED DE DATOS DE TELEFONÍA MÓVIL

540. Android permite al usuario, al igual que para la red de telefonía móvil (SMS y voz), utilizar la red de datos configurada automáticamente a través de la tarjeta SIM, así como seleccionar de forma manual tanto el operador de telecomunicaciones móviles como el APN (Access Point Name) para las conexiones de datos.

541. En dispositivos móviles Android como el empleado, al introducir la tarjeta SIM en el dispositivo móvil se lleva a cabo automáticamente el proceso de configuración de las opciones de conectividad de datos asociadas a las redes de telefonía móvil, incluyendo los APNs y su configuración: nombre, APN, proxy y puerto, credenciales (usuario y contraseña), servidor, dispositivos de mensajes multimedia (MMS: MMSC, proxy y puerto MMS), MCC, MNC, tipo de autentificación y tipo de APN (Access Point Name).

542. En función de la tarjeta SIM empleada y de la configuración de datos que ésta tenga asociada, se mostrarán automáticamente los ajustes de conexión disponibles en la lista de APNs, o ningún APN si no dispone de los datos correspondientes (en cuyo caso habrá que añadirlo manualmente).

543. Desde el menú de configuración del teléfono (“Ajustes – Conexiones inalámbricas (y redes) – Redes móviles”) y a través de la opción “APN”, es posible acceder a las opciones para seleccionar el APN para las conexiones de datos, así como añadir o editar la configuración de los APNs, a través del botón de “Menú”:



544. Al definir un nuevo APN deben emplearse los valores proporcionados por el operador de telecomunicaciones. Desde el punto de vista de seguridad, y si el operador admite diferentes protocolos de autentificación, se recomienda seleccionar autentificación mediante CHAP, dentro de las cuatro alternativas disponibles en la opción "Tipo de autenticación" (Ninguno, PAP, CHAP, y "PAP o CHAP"):

545. En este escenario de autoconfiguración existente por defecto, desde el punto de vista de seguridad, cada vez que se cambia la tarjeta SIM se recomienda acceder a la configuración de datos de telefonía móvil y, en concreto, a la lista de APNs para adecuar la configuración a la deseada por el usuario.

5.15.4 SELECCIÓN DE LA RED DE DATOS 2G/3G

546. Las redes de telefonía 2G (o GSM) presentan diferentes vulnerabilidades en la actualidad, como por ejemplo la posibilidad de suplantación de la red por parte de un potencial

atacante debido a debilidades en los mecanismos de autentificación, o la posibilidad de capturar y descifrar el tráfico de voz GSM debido a debilidades en los algoritmos de cifrado, A5/1 [Ref.- 1].

547. 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 la red de telefonía 3G (o UMTS).

548. Android no permite restringir las comunicaciones de telefonía móvil sólo a redes 3G a través del interfaz de usuario estándar (ver menú de prueba o testing posteriormente).

549. A través del menú "Ajustes – Conexiones inalámbricas (y redes) – Redes móviles", y en concreto de la opción "Utilizar sólo redes 2G", es posible indicar que sólo se haga uso de redes 2G (GPRS o EDGE), una opción indicada para disminuir el consumo de batería del terminal, pero desaconsejada desde el punto de vista de seguridad:

550. Se recomienda no activar esta opción, pese a que el dispositivo móvil hará uso automáticamente de redes 2G en zonas dónde no se disponga de suficiente cobertura por parte de las redes 3G.

551. El principal inconveniente de esta configuración (no modificable) es que si el usuario se encuentra en una zona dónde no se dispone de cobertura 3G (o superior, 3.5G), se podrá hacer uso del dispositivo móvil, premiando la disponibilidad del servicio de telefonía (voz y datos) por encima de la seguridad.

552. Android proporciona información en la barra de estado superior sobre las tecnologías de telefonía móvil de datos para las que se dispone de cobertura a través del siguiente conjunto de iconos, que representan la disponibilidad y el estado de la conexión para una red 3G o 3.5G (WCDMA/UMTS o HSPA), 2.75G (EDGE) y 2G (GPRS), respectivamente:

	Connected to the fastest 3G networks (UMTS or HSDPA)
	Connected to the second-fastest network (EDGE)
	Connected to a 2G network (GPRS)
	The more bars are lit, the stronger the wireless signal
	Connected to another wireless service provider's network (roaming)

553. Cuando las flechas asociadas al icono de la conexión de datos están iluminadas, indican que se está trasmitiendo información a través de la red.

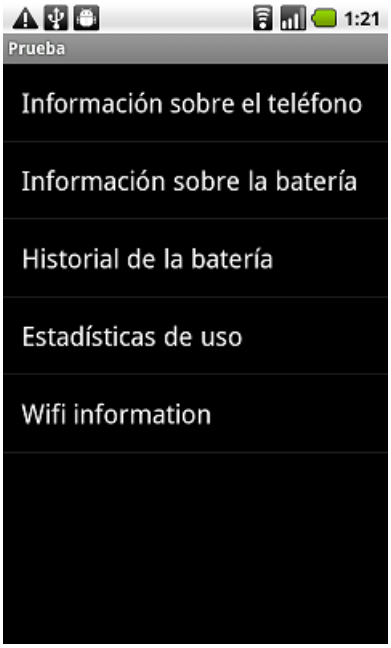
554. La cobertura y conectividad existentes están identificadas por el penúltimo icono, que indica la cobertura existente en función del número de barras activas, o que no se dispone de cobertura si se muestra el siguiente icono:

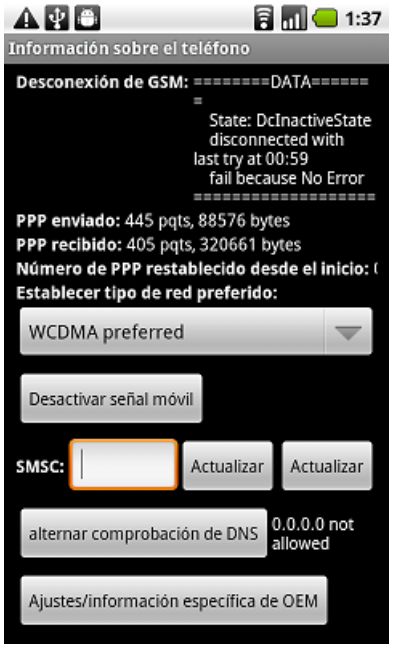
	No signal

555. La configuración por defecto del dispositivo móvil premia la conectividad, permitiendo el uso de redes de telefonía móvil 2G o 3G de forma automática en función de su cobertura y disponibilidad.

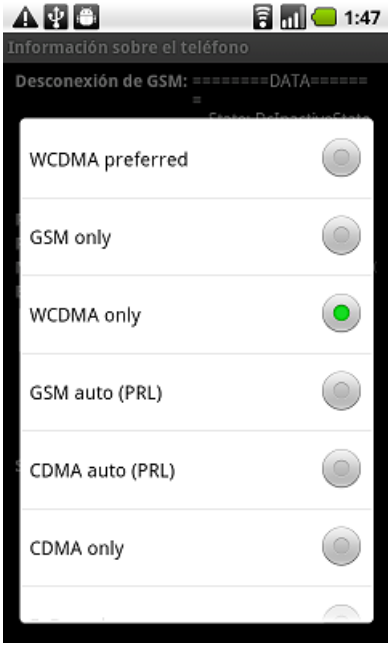
556. Adicionalmente, es posible obtener y configurar información avanzada a través del menú de prueba (o testing), disponible en Android tras marcar el siguiente número de teléfono: *#*#4636#*#* (o *#*#info#*#*).

557. Mediante la selección de la opción “Información sobre el teléfono” se dispone de numerosos detalles de la red de telefonía móvil, siendo posible configurar el tipo de red preferida en la parte inferior de dicha pantalla:





558. De las diferentes opciones disponibles, desde el punto de vista de seguridad se recomienda seleccionar la opción “WCDMA only” para forzar al dispositivo móvil a conectarse únicamente a redes 3G (PRL hace referencia a la “Preferred Roaming List” definida por los operadores de telefonía móvil):



559. Este cambio de configuración prevalece incluso tras reiniciar el dispositivo móvil y fuerza a que el dispositivo móvil sólo hago uso de redes 3G, más seguras que las 2G.

5.16 COMUNICACIONES TCP/IP

560. Esta sección proporciona recomendaciones de seguridad para la pila de comunicaciones TCP/IP del dispositivo móvil, incluyendo recomendaciones generales para TCP/IP (IPv4), SSL/TLS, IPv6 y VPN's.

5.16.1 ADAPTADORES DE RED

561. Los adaptadores de red disponibles en el dispositivo móvil para las diferentes tecnologías de comunicaciones (principalmente Wi-Fi) están disponibles en el menú "Ajustes – Conexiones inalámbricas (y redes) – Ajustes de Wi-Fi", mediante el botón "Menú" y la opción "Avanzado".

562. La pantalla de ajustes avanzados permite seleccionar si se utilizará una dirección IP estática o dinámica (DHCP), en caso de no definirse como estática. Por defecto, la configuración de TCP/IP empleada para la conexión a las redes Wi-Fi hace uso de una dirección IP dinámica obtenida mediante el protocolo DHCP.

563. La configuración de la dirección IP estática permite definir la dirección IP, la puerta de enlace (o router por defecto), la máscara de red, así como los (dos) servidores DNS:

564. La configuración de direccionamiento IP del interfaz Wi-Fi es única para todas las redes Wi-Fi configuradas, en lugar de disponerse de una configuración o perfil de red independiente para cada red Wi-Fi [Ref.- 92].

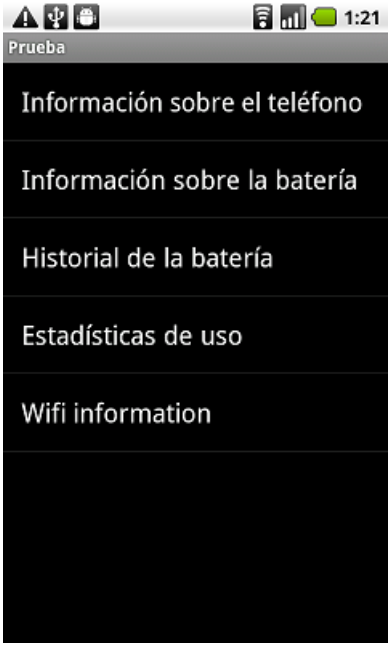
Nota: La versión “Ice Cream Sandwich”, Android 4.0, permite configurar una dirección IP para cada red Wi-Fi.

565. En el caso de emplear una dirección IP asignada dinámicamente por DHCP, es posible obtener información de la misma a través de la entrada de la red inalámbrica con la que se ha establecido la conexión Wi-Fi. Dese el menú “Ajustes – Conexiones inalámbricas (y redes) – Ajustes de Wi-Fi”, se muestra la lista de redes Wi-Fi visibles y aquella a la que estamos conectados.

566. Mediante una pulsación continuada sobre dicha red, “WLAN” en el ejemplo, se mostrará el menú que permite borrar o modificar la red:

567. Mediante la selección de la opción “Modificar red” se dispone de más detalles de la red Wi-Fi, incluyendo la dirección IP que ha sido asignada al dispositivo móvil por el servidor DHCP (ver imagen superior derecha).

568. Adicionalmente, es posible obtener esta información a través del menú de prueba (o testing), disponible en Android tras marcar el siguiente número de teléfono: *#*#4636#*#* (o *#*#info#*#*):



569. La opción “Wifi information – Wifi Status”, mediante el botón “Refresh Stats” en caso de no disponer de datos, proporciona los detalles de conexión a la red Wi-Fi (ver imagen superior derecha).

570. Android no proporciona ningún método a través del interfaz de usuario estándar para consultar la dirección IP asignada de forma dinámica por el operador de telefonía móvil al utilizar las redes de datos 2G/3G.

571. De nuevo, es posible obtener esta información a través del menú de prueba (o testing), disponible en Android tras marcar el siguiente número de teléfono: *#*#4636#*#* (o *#*#info#*#*).

572. Mediante la selección de la opción "Información sobre el teléfono" se dispone de numerosos detalles de la red de telefonía móvil, y en concreto en la sección inferior denominada "Desconexión de GSM" es posible visualizar la dirección IP asignada al dispositivo móvil en el interfaz de datos 2G/3G ("rmnet0"), junto a las direcciones IP del gateway y de los servidores DNS:

573. A través del comando "netcfg" (adb shell) desde un ordenador es también posible ver la asignación de direcciones IP en ambas redes, red Wi-Fi ("eth0") y red de telefonía móvil ("rmnet0").

5.16.2 SEGURIDAD EN TCP/IP

574. Con el objetivo de incrementar el nivel de seguridad de la pila TCP/IP empleada para las conexiones de datos en Android, se recomienda evaluar su comportamiento y modificar ciertos parámetros de configuración que condicionan su funcionamiento.

575. Se recomienda deshabilitar el procesamiento de paquetes de ping, es decir, paquetes ICMP echo request entrantes y sus respuestas asociadas, paquetes ICMP echo response salientes, con el objetivo de limitar el descubrimiento del dispositivo móvil en la red (habilitados por defecto en Android).

Nota: No se ha identificado ningún mecanismo, ni opción de configuración, en Android que permita deshabilitar el procesamiento de *ping*, es decir, la recepción de paquetes *ICMP echo request* y sus respuestas asociadas, *ICMP echo response*.

Igualmente, no se han encontrado mecanismos que permitan modificar los diferentes parámetros de configuración de bajo nivel de la pila TCP/IP mencionados en este apartado.

576. Android no responde a otros tipos de mensajes ICMP de petición y respuesta, como por ejemplo ICMP timestamp o ICMP address subnet mask.

577. La identificación del dispositivo móvil también se puede llevar a cabo a través del protocolo DHCP, ya que en las peticiones DHCP (DHCP Discover y Request) Android incluye varios datos identificativos.

578. Las peticiones de Android añaden la opción 60 de DHCP, identificación del vendedor, con el mensaje "dhcpcd 4.0.15", es decir, hace uso del cliente DHCP estándar de Linux DHCPCD (DHCP Client Daemon), versión 4.0.15.

579. La última versión disponible de dhcpcd para Linux en el momento de elaboración de la presente guía es la 5.2.12 [Ref.- 48].

Nota: En abril de 2011 se encontró una vulnerabilidad de ejecución remota de código en dhcpcd que afectaba a todas las versiones previas a 5.2.12 [Ref.- 53]. Parece que la versión de dhcpcd de Android no es vulnerable por defecto ya que el fichero de configuración "/system/etc/dhcpcd/dhcpcd.conf" no dispone de la opción "host_name" habilitada:

```
# dhcpcd configuration for Android Wi-Fi interface
# See dhcpcd.conf(5) for details.

interface eth0
# dhcpcd-run-hooks uses these options.
option subnet_mask, routers, domain_name_servers
```

La recomendación para evitar ser vulnerable en las versiones 4.x y 5.x de dhcpcd es no disponer de la opción "host_name" en la directiva "options" del fichero de configuración, "dhcpcd.conf", o actualizar a la versión 5.2.12 o superior.

580. Las peticiones también incluyen la opción 12 de DHCP, nombre de equipo, con el valor "android_CÓDIGO", dónde "CÓDIGO" es un string de 16 caracteres hexadecimales correspondiente al ANDROID_ID (correspondiente a la propiedad "net.hostname"; ver apartado "5.9. Configuración por defecto del dispositivo móvil").

581. Adicionalmente, por defecto el dispositivo móvil Android envía peticiones NTP (*Network Time Protocol, UDP/123*) para su sincronización horaria al servidor "europe.pool.ntp.org" en Internet periódicamente. En función de la ubicación geográfica otros servidores NTP podrían ser utilizados, como por ejemplo "north-america." o "ru.".

5.16.3 ESCANEO DE PUERTOS TCP Y UDP

582. A continuación se analiza el comportamiento de la pila TCP/IP de Android frente a intentos de conexión TCP y UDP a través del interfaz Wi-Fi. El análisis se ha realizado en la configuración por defecto del dispositivo móvil, es decir, sin haber realizado ninguna configuración específica o instalación adicional de software.

583. Android responde con un paquete TCP *Reset* a las peticiones de conexión en puertos TCP cerrados.

584. Por defecto, Android no dispone de ningún puertos TCP abierto o filtrado, es decir, los 65.536 puertos TCP están cerrados.

585. Android responde con paquetes ICMP de tipo 3 y código 3 (destino inalcanzable, puerto inalcanzable), limitados a uno por segundo, a las peticiones de conexión en puertos UDP cerrados.

586. Por defecto, Android no dispone de ningún puerto UDP abierto, tanto si DHCP está configurado en el interfaz Wi-Fi como cuando se utiliza una dirección IP estática.

587. El comportamiento por defecto de la pila TCP/IP, la ausencia de mecanismos de filtrado de tráfico (cortafuegos personal) y sus peculiaridades a nivel de TCP y UDP, hacen posible la identificación de los dispositivos móviles basados en Android de forma sencilla.

588. Este tipo de identificación remota a través de la red facilita a un potencial atacante la realización de ataques dirigidos sobre vulnerabilidades conocidas, por lo que se enfatiza la necesidad de mantener el software del dispositivo móvil completamente actualizado en todo momento.

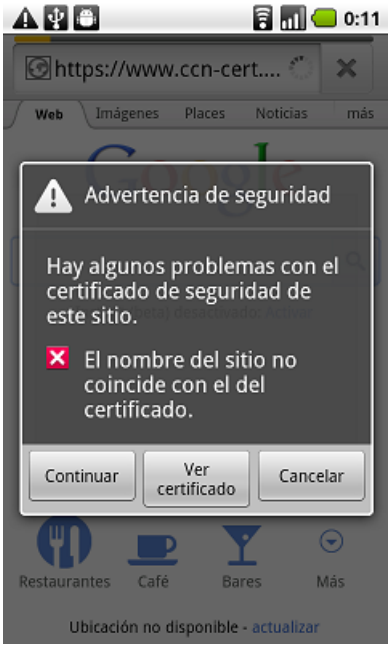
Nota: El comportamiento de la pila TCP/IP frente a escaneos de puertos a través del interfaz de telefonía móvil de datos no puede ser analizado de forma fiable. Este comportamiento a través del interfaz de telefonía móvil de datos está condicionado por la infraestructura de comunicaciones y los mecanismos de filtrado de los operadores de telefonía móvil, que por ejemplo, pueden no permitir comunicaciones mediante ping (*ICMP echo request* y *reply*) o pueden disponer de *proxies* transparentes en la red, por ejemplo para protocolos como FTP o HTTP.

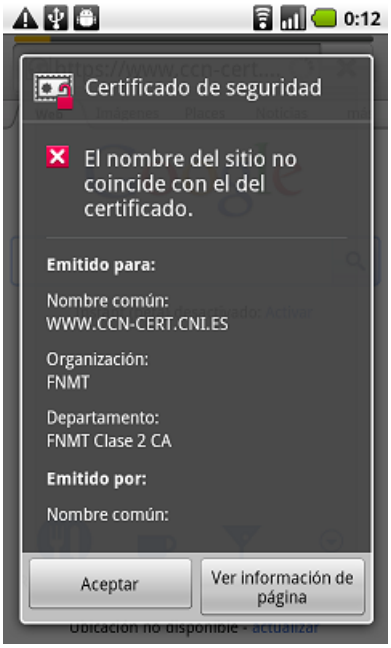
5.16.4 SSL/TLS

589. Android dispone de una implementación de los protocolos SSL, Secure Socket Layer, y TLS, Transport Layer Security, a través del paquete Java denominado “javax.net.ssl”, con soporte para SSL v3.0 y hasta TLS v1.2, basado en la implementación de The Legion of the Bouncy Castle y de OpenSSL [Ref.- 99].

590. Al acceder a un sitio web mediante HTTPS utilizando el navegador web existente en Android por defecto (aplicación “Navegador” versión 2.2), el dispositivo móvil verificará el certificado digital asociado y su cadena de confianza, hasta la autoridad certificadora (CA, Certificate Authority) reconocida correspondiente.

591. En caso de que no sea posible verificar la validez de un certificado, el navegador web de Android generará un mensaje de advertencia, indicando el motivo del error y permitiendo al usuario ver y analizar algunos detalles del certificado digital obtenido (mediante el botón “Ver certificado”):



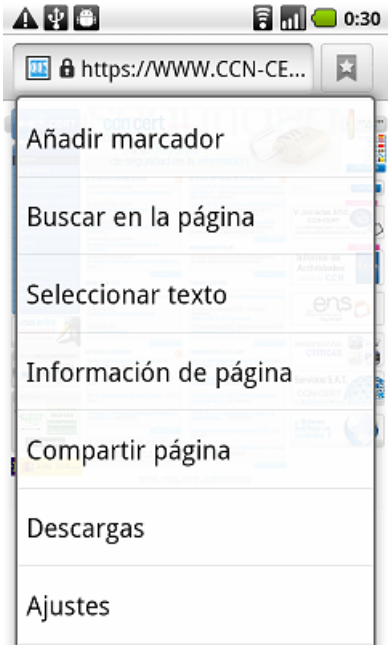


592. Sin embargo, los detalles del certificado digital no incluyen elementos clave para su verificación que sí están disponibles en los navegadores web de los equipos de escritorio, como por ejemplo el número de serie del certificado, las huellas o fingerprints MD5 y SHA-1, los detalles de la cadena o jerarquía de confianza y de las autoridades certificadoras involucradas en su generación, o las extensiones del certificado.

Nota: Como se puede apreciar en las imágenes superiores, el motivo del error del certificado indicado en la advertencia de seguridad no es exacto, ya que indica que se debe a que el nombre del sitio web no coincide con el del certificado, y en realidad el error se debe a otro motivo desconocido. La autoridad certificadora empleada para firmar el certificado del sitio web que ha sido accedido por HTTPS en el ejemplo sí está reconocida por Android (ej. "FNMT Clase 2 CA", alias número 5 del fichero "android_2.2_root_cas.txt" descrito en el apartado "5.7.2. Certificados digitales raíz de Android").

593. Si se acepta un certificado digital, éste será válido hasta que se cierre la instancia (o proceso) actual del navegador web en Android. Esta acción tiene el riesgo asociado de que el certificado digital aceptado, y desconocido, pertenezca a un potencial intruso que se encuentra realizando un ataque de intercepción, MitM (Man-in-the-Middle), sobre el protocolo SSL/TLS y las comunicaciones (supuestamente) cifradas del usuario.

594. Una vez se ha establecido una conexión de confianza mediante HTTPS con un sitio web, es posible ver su certificado digital asociado a través del botón de "Menú" de la aplicación del navegador web, "Navegador", y la opción "Más". Mediante la selección de la opción "Información de página", es posible tener acceso al certificado (botón "Ver certificado"):



595. Como se describe en el apartado "5.7.2. Certificados digitales raíz de Android", el repositorio de certificados raíz no está accesible a través del interfaz de usuario de Android. Por tanto, el usuario confía plenamente en la lista autoridades certificadoras (o CAs, *Certificate Authorities*) que son consideradas como de confianza por Android, y en las modificaciones de dicha lista realizadas por las actualizaciones asociadas a las nuevas versiones de Android.

596. Las carencias descritas asociadas al navegador web de Android 2.2, tanto al mostrarse mensajes de error no exactos como al no disponer de todos los detalles necesarios para verificar un certificado digital, limitan la utilización que se puede hacer del dispositivo móvil para validar el acceso a sitios web mediante HTTPS.

597. Android no soporta la utilización de mecanismos de autentificación web basados en certificados digitales cliente a través del navegador web existente por defecto [Ref.- 117], pese a que sí es posible hacer uso de certificados cliente para la conexión a redes Wi-Fi o VPN (ver apartado "5.7.1. Certificados digitales y credenciales del usuario"). Los certificados digitales clientes guardados en el repositorio de credenciales no están disponibles para el navegador web.

598. Existen otros navegadores web, aplicaciones de terceros (Firefox para Android, SandroB, etc.), que sí disponen de capacidades de autentificación web basada en certificados digitales cliente, ya que definen su propio gestor de certificados cliente (KeyManager) y su propio gestor de confianza (TrustManager, para gestionar sus propias CAs) a través de "javax.net.ssl.SSLContext".

599. La funcionalidad para el uso de certificados digitales cliente en el navegador web ha sido añadida finalmente en Android versión 4.0 [Ref.- 118]. Los cambios introducidos permiten gestionar (visualizar, deshabilitar, habilitar, instalar, eliminar, etc.) las CAs desde el interfaz de usuario de Android y la sección "Ajustes – Seguridad", así como gestionar certificados digitales cliente para el dispositivo móvil y las aplicaciones (como el navegador web o los clientes de correo electrónico) a través de un nuevo KeyChain (o gestor de credenciales y certificados) [Ref.- 119].

5.16.5 IPV6

600. El protocolo IP versión 6 (IPv6) está soportado y activado por defecto en Android para las comunicaciones de datos mediante Wi-Fi, pese a que el usuario no dispone de ninguna opción de configuración disponible relacionada con IPv6 en el interfaz gráfico.

Nota: La disponibilidad de IPv6 para las comunicaciones de datos a través de la infraestructura de telefonía móvil en Android es dependiente no sólo de la versión del sistema operativo, sino también del modelo de dispositivo móvil y del operador de telefonía móvil empleado [Ref.- 54].

601. Durante el proceso de inicialización de conectividad de datos, el dispositivo móvil Android genera peticiones IPv6 de solicitud de vecinos y de router mediante ICMPv6, empleando como dirección origen "fe80::9221:55ff:fe01:0203" (dónde su dirección MAC es 90:21:55:01:02:03), y añadiendo también su dirección MAC como dirección de enlace.

602. La utilización de la dirección MAC en la dirección IPv6 sin hacer uso de las Privacy Extensions de IPv6 (RFC 4941) presenta problemas de seguridad y permite el seguimiento de los dispositivos móviles Android en Internet [Ref.- 55].

603. Adicionalmente, el dispositivo móvil Android envía periódicamente mensajes IPv6 de informes multicast ("Multicast Listener Report Message v2").

604. Para disponer de conectividad IPv6 completa en Android y obtener una dirección IPv6 a través de mensajes RA (Router Advertisement) enviados por un router con soporte de IPv6 es necesario que el interfaz Wi-Fi disponga también de dirección IPv4 (estática o mediante DHCP).

605. Se recomienda deshabilitar la disponibilidad de IPv6 en Android por completo, salvo que se vaya hacer uso de sus capacidades de comunicación, aunque esta opción no está disponible por defecto en la versión analizada (salvo en dispositivos Android rooted).

Nota: No se ha identificado ningún mecanismo, ni opción de configuración, en Android que permita deshabilitar la pila de comunicaciones de IPv6.

5.16.6 VPN

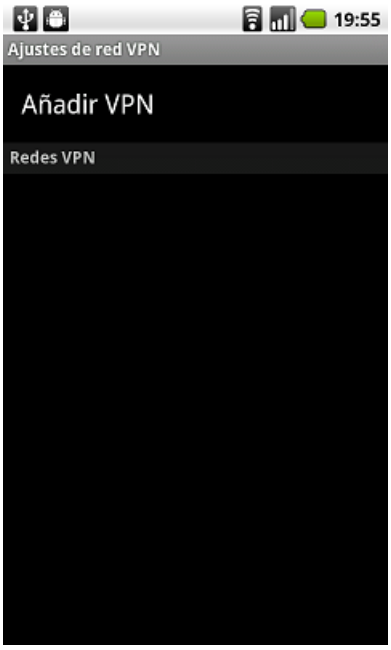
606. Android proporciona soporte para las siguientes tecnologías VPN: Point-to-Point Tunneling Protocol (PPTP; TCP/1723), Layer Two Tunneling Protocol (L2TP; UDP/1701), y L2TP en combinación con Internet Protocol Security (LT2P/IPSec; UDP/500). La opción recomendada desde el punto de vista de seguridad es L2TP/IPsec.

607. Adicionalmente, en el caso de VPN's basadas en IPSec/L2TP, se debe definir el método de autentificación: certificado o clave precompartida.

608. Se recomienda emplear un certificado para la autentificación de IPSec/L2TP al ser un mecanismo más seguro que el establecimiento de una clave precompartida entre el servidor de VPN y el dispositivo móvil (conocida por todos los usuarios de la VPN).

609. Android no dispone de soporte nativo para IPSec (sin L2TP), siendo necesario un cliente VPN de terceros para este tipo de conexiones. Android permite establecer conexiones L2TP/IPSec tanto mediante clave compartida, como mediante certificados.

610. Desde el menú "Ajustes – Conexiones inalámbricas (y redes) – Ajustes de red VPN" es posible añadir una nueva red VPN a través del botón "Añadir VPN":



611. A través de las diferentes opciones es posible configurar la red VPN. Una vez se han establecido las opciones de configuración según el tipo de red (descritas a continuación), mediante el botón "Menú" y la opción "Guardar" es posible almacenar la nueva configuración.

612. Todas las redes VPN, basadas en PPTP, L2TP y L2TP/IPSec, requieren disponer del nombre de la red VPN, del nombre o dirección IP del servidor VPN, y de los dominios DNS.

613. En el caso de redes PPTP, Android permite deshabilitar el cifrado (habilitado por defecto), opción desaconsejada desde el punto de vista de seguridad.

614. En el caso de redes L2TP y L2TP/IPsec, Android permite habilitar un secreto L2TP (deshabilitado por defecto), opción que permite autentificar el propio túnel L2TP mediante un secreto compartido entre el cliente y el servidor (puede ser necesario en función de la configuración del servidor VPN):

615. En el caso de redes L2TP/IPsec, Android permite establecer la clave precompartida para el acceso a la red, o el certificado digital de usuario y de la autoridad certificadora (CA), en función del tipo de red:

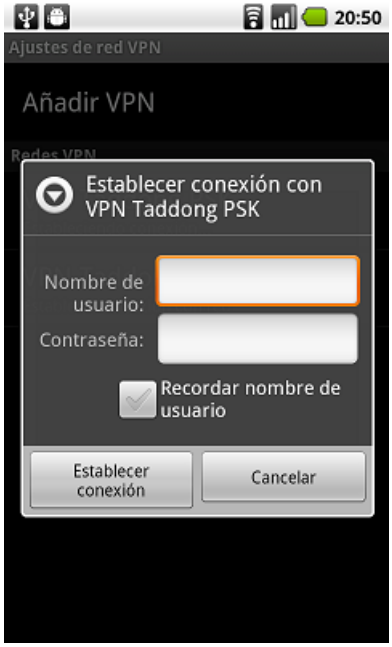
616. El certificado digital necesario para IPSec/L2PT es de tipo personal, y permitirá autentificar al dispositivo móvil y su propietario. Adicionalmente es necesario instalar un certificado raíz (perteneciente a la CA), y asociado a la generación del certificado digital empleado por el servidor de VPN.

617. En el caso de redes L2TP/IPSec basadas en certificados, al seleccionar el certificado del usuario y de la CA, Android mostrará los certificados disponibles en el repositorio de credenciales, previamente importados (ver apartado “5.7.1. Certificados digitales y credenciales del usuario”):

618. Al guardar la nueva configuración de la red VPN, Android solicitará la clave del repositorio de credenciales (ver apartado “5.7.1. Certificados digitales y credenciales del usuario”).

619. Una vez configurada la red VPN, es posible conectarse a la misma seleccionándola de la lista de redes disponibles desde la pantalla “Ajustes – Conexiones inalámbricas (y redes) – Ajustes de red VPN”, mediante la opción “Establecer conexión con red”:

620. Como resultado, Android solicitará al usuario las credenciales de acceso a la VPN, es decir, el nombre de usuario y la contraseña para establecer la conexión con la red VPN seleccionada:



621. Desde el punto de vista de seguridad se recomienda no seleccionar la opción "Recordar nombre de usuario", de forma que cada vez que se establezca una conexión con una red VPN sea necesario proporcionar tanto el usuario como la contraseña.

622. Una vez establecida la conexión con la red VPN, Android restringe las comunicaciones para que todo el tráfico sea cursado a través de la VPN hasta que ésta sea desconectada, es decir, no soporta *split horizon* (conexiones simultáneas directas hacia Internet y a través de la VPN).

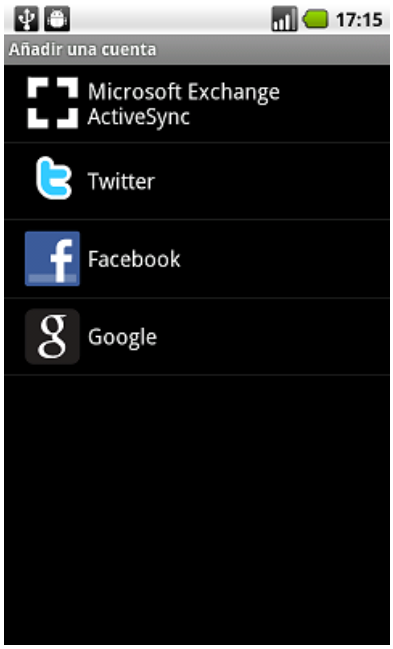
5.17 CUENTA DE USUARIO DE GOOGLE

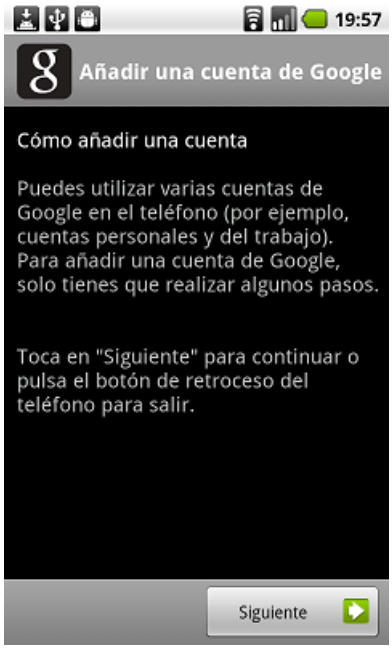
623. Para hacer uso de las aplicaciones de Google en Android (GMail, Google Talk, Google Calendar, etc.), poder descargar aplicaciones de Google Play, hacer copias de seguridad de los datos y la configuración en los servidores de Google, y poder hacer uso de otros servicios de Google desde el dispositivo móvil, es necesario disponer de una cuenta de usuario de Google.

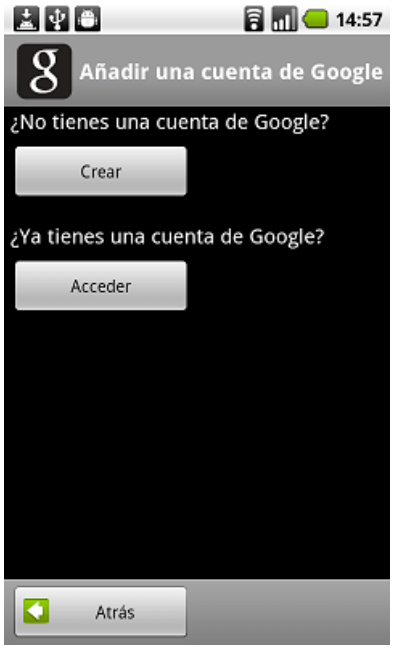
624. Entre otros, los siguientes servicios de Google están disponibles para los usuarios de Android: GMail, YouTube, Google Talk, Google Calendar, Google Docs, Google Maps y Location (ver apartado "5.10.1. Servicio de localización de Google y Google Maps"), copias de seguridad (ver apartado "5.18. Copia de seguridad de datos en los servidores de Google"), Google Play [Ref.- 4] (ver apartado "5.25. Aplicaciones de terceros"), etc.

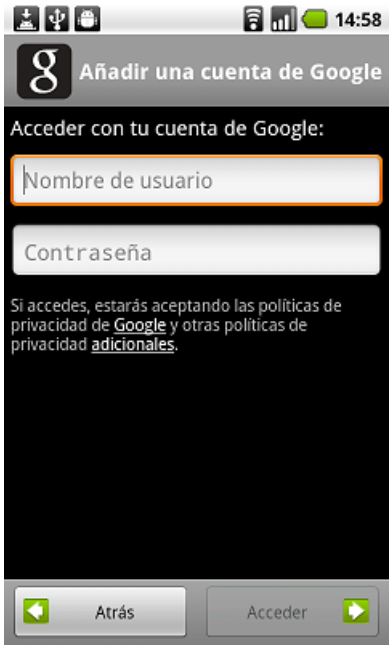
5.17.1 ASIGNACIÓN DE UNA CUENTA DE GOOGLE AL DISPOSITIVO MÓVIL

625. La configuración de una cuenta de Google ya existente y su vinculación al dispositivo móvil Android, o la creación de una nueva cuenta, puede llevarse a cabo desde el menú "Ajustes – Cuentas y sincronización". El botón "Añadir cuenta" permite añadir cuentas de Microsoft Exchange ActiveSync (ver apartado "5.3. Gestión empresarial de dispositivos basados en Android"), Twitter, Facebook y 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 (siendo posible asociar múltiples cuentas):



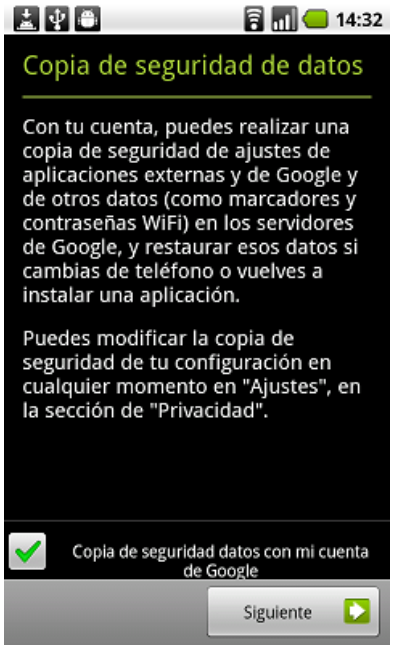


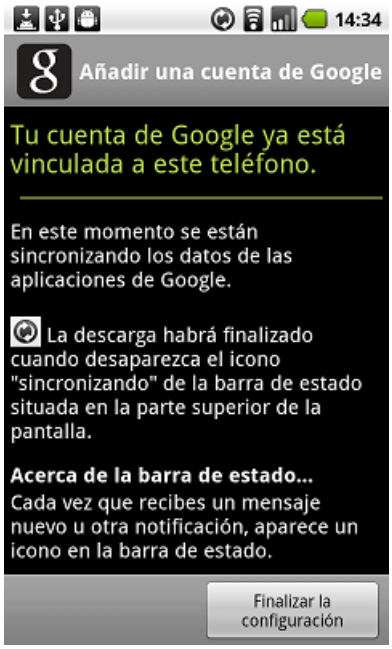




626. Adicionalmente, para configurar otros servicios críticos y relevantes en Android, como por ejemplo el acceso a Google Play, es también necesario disponer de una cuenta de Google (ver apartado “5.25. Aplicaciones de terceros: ”).

627. El proceso de vinculación de una cuenta existente se lleva a cabo mediante una conexión HTTPS con el servidor “android.clients.google.com”. Durante el mismo se solicita confirmación por parte del usuario (ver imagen inferior izquierda) para hacer uso del servicio de copia de seguridad de datos de Android en los servidores de Google, habilitado por defecto (ver apartado “5.18. Copia de seguridad de datos en los servidores de Google”):

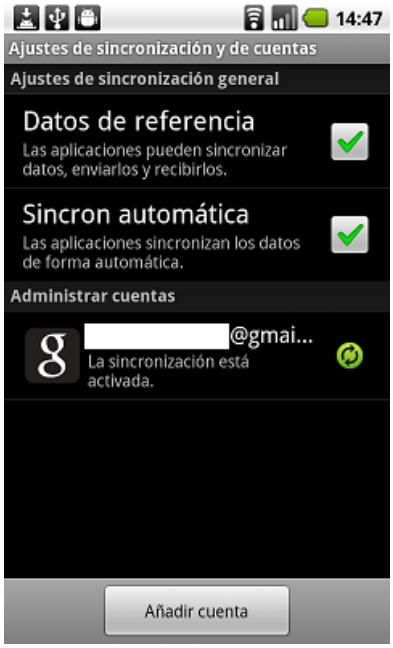


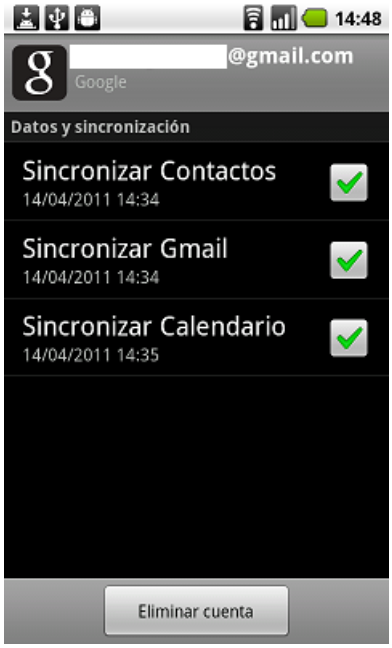


628. Una vez se ha vinculado una cuenta de Google con el dispositivo móvil, se realizará la sincronización automática (ver imagen superior derecha), no siendo posible no llevar a cabo (o cancelar) esta sincronización inicial.

629. 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.

630. Adicionalmente, la cuenta aparecerá en el menú “Ajustes – Cuentas y sincronización”, junto a las opciones generales de sincronización de Android (ver imagen inferior izquierda), que aplican a todas las cuentas disponibles en el dispositivo móvil:





631. Las dos opciones generales de sincronización (ver imagen superior izquierda), “Datos de referencia” y “Sincron automática” están habilitadas por defecto.

632. La primera opción, “Datos de referencia”, permite a las aplicaciones y servicios sincronizar datos (enviar o recibir) incluso cuando no están siendo utilizadas, es decir,

están ejecutando de fondo. Si esta opción no se activa, no es posible recibir nuevos correos en GMail automáticamente o eventos de calendario, siendo necesario refrescar los datos de forma manual en cada aplicación.

633. La segunda opción, “Sincron automática”, permite especificar si los cambios realizados en las aplicaciones y servicios, tanto desde el dispositivo móvil como desde la web, serán sincronizados automáticamente e inmediatamente entre ellos.

634. Si esta opción no se activa es posible sincronizar las aplicaciones manualmente desde cada cuenta, seleccionando la cuenta de la lista de cuentas disponibles, y empleando la opción “Sincronizar ahora” mediante el botón “Menú”.

635. Si se va a hacer uso de las capacidades de sincronización del dispositivo móvil y de las diferentes aplicaciones y servicios, se recomienda utilizar las capacidades de sincronización automática, considerando los posibles riesgos de seguridad detallados a continuación y particulares de cada servicio.

636. Para acceder a los detalles de configuración de una cuenta basta con seleccionarla del listado de cuentas disponibles (ver imagen superior derecha). Las tres opciones de sincronización de las cuentas de Google (Contactos, GMail y Calendario) están todas habilitadas por defecto.

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

638. La sincronización de la información de los diferentes servicios de Google, por ejemplo del calendario, se realiza mediante conexiones HTTP no cifradas, empleando el agente de usuario “User-Agent: Android-GData-Calendar/1.4 (passion FRF91); gzip”, y desvelando en las peticiones la cuenta de Google utilizada (usuario@gmail.com) y en las respuestas (en formato XML) todos los detalles de los datos sincronizados:

```
GET /proxy/calendar/feeds/usuario%40gmail.com HTTP/1.1
Authorization: GoogleLogin auth=DQAA…3vtP
Host: android.clients.google.com
User-Agent: Android-GData-Calendar/1.4 (passion FRF91); gzip

GET       /proxy/calendar/feeds/usuario%40gmail.com/private/full?updated-
min=2011-04-14T12%3A34%3A04.000Z&sortorder=ascending&recurrence-
expansion-end=1970-01-01&max-results=200&recurrence-expansion-start=1970-
01-01&showdeleted=true&orderby=lastmodified&start-max=2012-03-
21T00%3A00%3A00.000Z&requirealldeleted=true HTTP/1.1
...
```

639. Las otras aplicaciones sincronizadas, como por ejemplo los contactos, realizan peticiones similares HTTP sin cifrar con un agente de usuario diferente (pero similar):

```
GET            /proxy/contacts/contacts/usuario@gmail.com/base2_property-
android?sortorder=ascending&max-results=10000&orderby=lastmodified
HTTP/1.1
Authorization: GoogleLogin auth=DQAA…cMVo
GData-Version: 3.0
Host: android.clients.google.com
User-Agent: Android-GData-Contacts/1.3 (passion FRF91); gzip
```

```
POST      /proxy/contacts/groups/usuario@gmail.com/base2_property-android
HTTP/1.1
Authorization: GoogleLogin auth=DQAA…cMVo
GData-Version: 3.0
Content-Type: application/atom+xml
Host: android.clients.google.com
User-Agent: Android-GData-Contacts/1.3 (passion FRF91); gzip
```

640. Este comportamiento de envío de tráfico no cifrado por HTTP es extensible a otros servicios de Google, como algunas de las comunicaciones realizadas entre Android y Google Play (antes Android Market) (ver apartado “5.25. Aplicaciones de terceros: ”), o el servicio de fotos e imágenes Picasa.

641. La sincronización de GMail sin embargo se realiza con el mismo servidor, pero empleando conexiones HTTPS cifradas.

642. Se recomienda no sincronizar el calendario y los contactos con los servicios asociados de Google debido a que la información no es transmitida de forma cifrada y, por tanto, puede ser capturada por cualquiera que se encuentre entre la red de acceso a Internet empleada por el usuario y los servidores de Google.

Nota: Durante la elaboración de la presente guía se identificó este comportamiento diferenciado y vulnerable entre la sincronización del correo de GMail (cifrada con HTTPS) y la sincronización de calendario y contactos (no cifrada a través de HTTP), considerándose erróneamente que se trataba de una decisión de diseño de Google.

Posteriormente se confirmó que esta vulnerabilidad no era voluntaria, por lo que tras la publicación de la misma en Mayo de 2011 [Ref.- 108], Google procedió a reconocer su existencia y a solucionarla mediante el uso de conexiones cifradas con HTTPS, tanto en las versiones de Android actuales como las antiguas. La solución no requiere realizar una actualización de la versión de Android, y se publicó de forma transparente para los usuarios (mediante la modificación por parte de Google de un fichero de configuración del terminal asociado a los servicios de Google), por lo que los usuarios no disponían de información para saber si su dispositivo móvil seguía siendo vulnerable o estaba protegido.

Todas las versiones de Android 2.x hasta la versión 2.3.3 (incluida) eran vulnerables para el servicio de contactos y calendarios. La versión 2.3.4 hace uso de HTTPS:

Use of HTTPS in Android Google Apps:

Android version	Calendar Sync	Contacts Sync	Picasa Sync (Gallery)
3.0	yes	yes	?
2.3.4	yes	yes	no
2.3.3	no	no	no
2.2.1	no	no	n/a
2.2	no	no	n/a
2.1	no	no	n/a

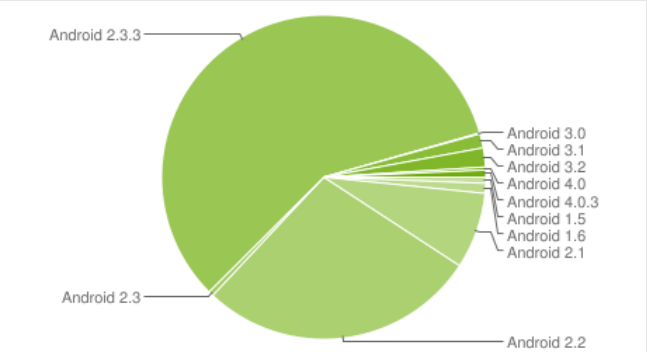
Posteriormente se publicaron actualizaciones para proteger igualmente el servicio Picasa (CVE-2011-2344), a través de una actualización de la aplicación “Galería” (o “Gallery [3D]”) para Android 2.x. Las capacidades de sincronización con Picasa fueron introducidas en “Galería” en la versión 2.3 de Android.

Este comportamiento vulnerable debido al envío de tráfico no cifrado a través de HTTP también afecta a otras aplicaciones de uso común en Android, como Twitter o Facebook [Ref.- 108], según su versión (ver apartado "5.24. Redes sociales"), y es extensible a cualquier otra aplicación instalada por defecto o por el usuario en el dispositivo móvil [Ref.- 109].

La solución para evitar esta vulnerabilidad pasa por hacer uso de las capacidades de Android para establecer conexiones cifradas a través de redes VPN (ver apartado "5.16.6. VPN").

Nota: El impacto real de esta vulnerabilidad, y de vulnerabilidades similares que afectan a los usuarios de Android, puede ser evaluado a través de las estadísticas disponibles y proporcionadas por Google sobre la distribución real (actualizada, e histórica) de las versiones (o niveles de la API) de Android en dispositivos móviles [Ref.- 112].

En el momento de finalización de la elaboración de la presente guía, tomando como fecha las estadísticas del 1 de febrero de 2012, podemos ver como todavía el 40% (aproximadamente) de los dispositivos móviles disponen de una versión de Android igual o inferior a 2.3.3, y por tanto son vulnerables incluso 9 meses después de la publicación de la vulnerabilidad:



Platform	Codename	API Level	Distribution
Android 1.5	Cupcake	3	0.6%
Android 1.6	Donut	4	1.0%
Android 2.1	Eclair	7	7.6%
Android 2.2	Froyo	8	27.8%
Android 2.3 - Android 2.3.2	Gingerbread	9	0.5%
Android 2.3.3 - Android 2.3.7		10	58.1%
Android 3.0	Honeycomb	11	0.1%
Android 3.1		12	1.4%
Android 3.2		13	1.9%
Android 4.0 - Android 4.0.2	Ice Cream Sandwich	14	0.3%
Android 4.0.3		15	0.7%

643. Aunque la vulnerabilidad mencionada asociada a la ausencia de tráfico cifrado afecta directamente a servicios específicos de Google y aplicaciones concretas de Android, potencialmente su impacto podía afectar a cualquier servicio de Google, al hacer todos

ellos uso del protocolo de autentificación ClientLogin [Ref.- 111], que da acceso a todas las interfaces (o APIs) de los servicios de Google.

644. El protocolo de autentificación ClientLogin [Ref.- 108] es empleado por las aplicaciones de Android para obtener un token de autentificación (authToken), mediante el envío de las credenciales válidas (usuario y contraseña) de una cuenta de Google a través de HTTPS. El authToken, denominado "auth", es intercambiado a través de la cabecera "Authorization: GoogleLogin auth=…" de HTTP.

645. El authToken es 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 es válido durante (como máximo) dos semanas (14 días) [Ref.- 110].

646. El riesgo asociado a la vulnerabilidad previamente descrita es que una aplicación Android haga uso del authToken a través de una conexión HTTP no cifrada, desvelando su valor. Si un atacante obtiene un valor válido de authToken podrá hacer uso de los servicios de Google suplantando al usuario asociado a ese authToken.

647. En el caso de que un usuario sea víctima de un ataque de secuestro del valor de su authToken puede invalidarlo mediante la modificación de la contraseña de su cuenta de Google.

648. Finalmente, en el caso de usuarios individuales no asociados a un dominio de Google Apps (ver apartado "5.3. Gestión empresarial de dispositivos basados en Android") es posible acceder a la información de su cuenta a través del Panel de Control de Google, disponible en "https://www.google.com/dashboard/":

649. Dentro de las opciones disponibles asociadas a los dispositivos móviles, y dentro de todos los servicios de Google (GMail, YouTube, etc.), es posible gestionar las aplicaciones instaladas desde Google Play (antes Android Market) (a través de un enlace directo a la cuenta en Google Play: "https://play.google.com/store/account?hl=es/"), así como verificar los datos del dispositivo móvil almacenados por Google (como el IMEI, fecha de registro, etc.):

5.17.2 GESTIÓN DE LAS CREDENCIALES DE LAS CUENTAS DE USUARIO

650. Desde el punto de vista de seguridad, se recomienda no almacenar la contraseña de la cuenta del usuario en el dispositivo móvil, mitigando así el riesgo de que un potencial atacante obtenga acceso al dispositivo móvil, y como consecuencia, a la cuenta de Google del usuario, junto a todos sus servicios asociados, como Google Play.

651. Sin embargo, no se ha identificado ninguna opción en el dispositivo móvil, a través de "Ajustes – Cuentas y sincronización" o "Ajustes – Ubicación y seguridad" (o en la configuración de la aplicación "Play"), para evitar el almacenamiento de la contraseña (o de los tokens de autentificación, authToken) de la cuenta de Google del usuario.

652. Es decir, la contraseña 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 se dispone de acceso directo a la cuenta del usuario y a todos los servicios asociados.

653. 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, dónde la contraseña queda almacenada en el dispositivo no siendo posible evitar que no sea así.

654. La alternativa principal identificada para evitar esta asociación entre cuenta/contraseña y dispositivo es eliminar la cuenta asociada. La pantalla de detalles de una cuenta permite eliminarla del dispositivo móvil mediante el botón "Eliminar cuenta".

655. 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 disponibles en Android.

656. 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 evaluarlo independientemente, y en todo caso, hacer uso del acceso web estándar.

657. 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, desde otro ordenador o desde el propio navegador web del dispositivo móvil Android.

658. Tras acceder a Google (Google Accounts: https://www.google.com/accounts) y modificar la contraseña de la cuenta, la próxima vez que se acceda desde el dispositivo móvil a alguna de las aplicaciones que hacen uso de los servicios de Google (por ejemplo, GMail o Play), y por tanto, de dicha cuenta, Android generará una notificación de error de sincronización (visible desde la barra de estado) y solicitará al usuario la (nueva) contraseña para la cuenta:

Nota: La solicitud de la contraseña asociada a la cuenta del usuario también se puede presentar al cambiar la tarjeta SIM del dispositivo móvil.

659. 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.

660. Por otro lado, debido a que Android está diseñado para trabajar con una cuenta de Google que esté siempre activa, tampoco proporciona capacidades para desconectarse (o cerrar la sesión actual) de la cuenta 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.

661. 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 (como se ha descrito previamente) o utilizar aplicaciones de terceros con este propósito.

662. 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” están 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 en Android 2.x.

5.17.3 ALMACENAMIENTO DE LAS CREDENCIALES DE LAS CUENTAS DE USUARIO

663. El almacenamiento de credenciales en Android se lleva a cabo sin cifrar, es decir, las credenciales de acceso a diferentes servicios son almacenadas en una base de datos SQLite en claro [Ref.- 106], bajo el directorio “/data/data”, que requiere acceso como “root”.

664. Si un atacante obtiene acceso físico al dispositivo móvil, podría seguir el proceso de *rooting* y disponer de acceso a las credenciales.

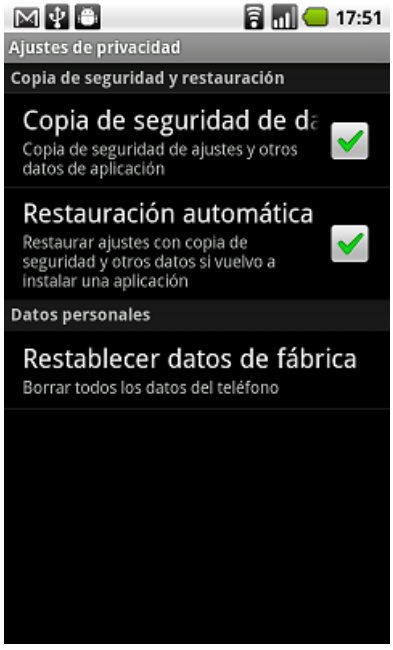
665. Únicamente los mecanismos de cifrado del dispositivo móvil disponibles en Android 3.0+ protegen frente a esta vulnerabilidad (ver apartado “5.6.1. Cifrado del dispositivo móvil”), no existiendo ninguna solución por defecto disponible para Android 2.x.

5.18 COPIA DE SEGURIDAD DE DATOS EN LOS SERVIDORES DE GOOGLE

666. El servicio de copia de seguridad de datos de Google permite almacenar información personal del usuario en los servidores de Google, como los favoritos de navegación web, palabras añadidas al diccionario, una lista de las aplicaciones instaladas, parámetros de configuración de las aplicaciones externas que hacen uso de estas capacidades, contraseñas de las redes Wi-Fi, la mayoría de parámetros de configuración del dispositivo móvil y de los servicios de Google, siendo posible restaurar los datos si fuese necesario reemplazar el dispositivo móvil o reinstalar una aplicación [Ref.- 101].

667. Durante el proceso de creación de una cuenta de Google se solicita confirmación por parte del usuario para activar el servicio de copia de seguridad de datos (ver apartado “5.17. Cuenta de usuario de Google”).

668. El servicio de copia de seguridad de datos en los servidores de Google puede ser activado o desactivado posteriormente a través del menú “Ajustes – Privacidad”, y en concreto, de la opción “Copia de seguridad de datos”:



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

670. Si se reinstala una aplicación externa, el servicio puede almacenar y restaurar los datos asociados a la aplicación. La opción “Restauración automática” permite restaurar la configuración y los datos asociados a una aplicación al instalarla (o reinstalarla) en el dispositivo móvil. Si la aplicación 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 aplicación será recuperada.

671. En caso de reemplazar el dispositivo móvil, este servicio ofrece la posibilidad de restaurar los datos la primera vez que se accede a Google con la cuenta de usuario asociada al servicio.

672. El usuario u organización propietaria del dispositivo móvil Android debe evaluar el nivel de confianza depositado en Google para emplear este servicio y almacenar todos los datos personales y confidenciales del usuario (motivo por el que el mismo se encuentra bajo la sección de privacidad de los ajustes del terminal).

5.19 INSTALACIÓN Y ELIMINACIÓN DE APLICACIONES EN ANDROID

673. Las aplicaciones para Android están desarrolladas en el lenguaje de programación Java y ejecutan sobre una máquina virtual Java ligera denominada Dalvik [Ref.- 16].

674. La máquina virtual Dalvik ha sido optimizada para su utilización en dispositivos móviles, con un consumo eficiente de memoria. Dalvik ejecuta ficheros en formato Dalvik Executable (.dex), o DEX, por lo que en el proceso de desarrollo el código Java (ficheros ".class", Java bytecode) de las aplicaciones de Android es convertido al formato DEX, Dalvik bytecode (mediante la herramienta "dx").

675. Las herramientas de desarrollo de software de Android (Android SDK, Software Development Kit) generan las aplicaciones para Android, o paquetes Android, en un único archivo o contenedor con extensión ".apk".

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

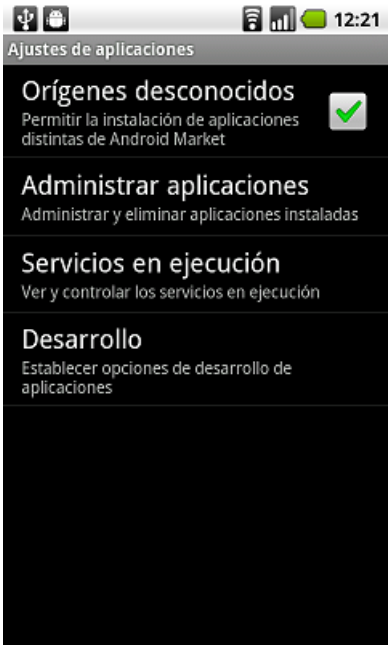
677. Todas las aplicaciones Android deben ser firmadas digitalmente por su desarrollador mediante certificados digitales, siendo por tanto posible identificar al desarrollador de cualquier aplicación oficial.

678. La firma de las aplicaciones es empleada adicionalmente por Android para establecer permisos de operaciones entre aplicaciones y niveles de protección [Ref.- 102] (según el fichero manifest), y para permitir a las aplicaciones compartir su ID.

679. El módulo estándar de instalación de aplicaciones de Android verifica mediante certificados digitales que las aplicaciones oficiales, es decir, que provienen de Google Play, han sido firmadas convenientemente por su desarrollador.

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

681. Para permitir la instalación de cualquier aplicación simplemente es necesario eliminar las comprobaciones de seguridad asociadas en Android mediante la opción "Orígenes desconocidos" del menú "Ajustes – Aplicaciones":



682. Desde el punto de vista de seguridad y con el objetivo de evitar la instalación de aplicaciones de fuentes desconocidas se recomienda no habilitar esta opción, tal como advierte el mensaje mostrado por Android (imagen superior derecha).

5.19.1 INSTALACIÓN REMOTA DE APLICACIONES

683. En mayo de 2010 Google presentó la versión web de Google Play [Ref.- 4], que permite la consulta e instalación de aplicaciones en los dispositivos móviles Android desde otros ordenadores mediante un navegador web, en lugar de emplear la aplicación de acceso a la tienda (Google Play) desde los propios dispositivos móviles.

684. Una vez se adquiere una aplicación a través de la versión web de la tienda, 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.

685. La conexión permanente a través de Internet disponible entre los dispositivos móviles Android y Google se basa en el GTalkService [Ref.- 77]. Para la instalación remota de aplicaciones se emplea el mecanismo (intent) denominado INSTALL_ASSET [Ref.- 78].

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

687. El acceso a Google Play se realiza mediante la cuenta de Google del usuario, por lo que el acceso no autorizado por parte de un atacante a dicha cuenta permitiría la instalación de aplicaciones en el dispositivo móvil asociado del usuario [Ref.- 8]. El proceso de instalación se lleva a cabo automáticamente y conlleva únicamente un aviso en la barra de notificaciones del dispositivo móvil.

688. Alternativamente, podría ser posible la instalación remota de aplicaciones desde la web de Google Play de forma no autorizada si un potencial atacante obtiene los identificadores de sesión empleados en el acceso web a Google Play (antes Android Market) [Ref.- 75].

5.19.2 ELIMINACIÓN REMOTA DE APLICACIONES

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

690. 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 aplicaciones dañinas o maliciosas concretas.

691. En junio de 2010 Google empleó estas capacidades por primera vez [Ref.- 5] [Ref.- 78] para eliminar una aplicación creada como prueba de concepto que pretendía demostrar la facilidad de introducir aplicaciones maliciosas en las tiendas de aplicaciones de varios fabricantes de dispositivos móviles, incluyendo Android Market.

692. Posteriormente, Google ha hecho uso de esta funcionalidad en (al menos) otra ocasión para eliminar otras aplicaciones 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) [Ref.- 6]. Estas aplicaciones hacían uso de vulnerabilidades conocidas en versiones de Android previas a la versión 2.2.2, y específicamente, técnicas empleadas habitualmente en conseguir acceso como "root" a dispositivos móviles Android (proceso conocido como "root", rooted o rooting del dispositivo Android).

693. Esas capacidades permiten a Google no sólo eliminar las aplicaciones maliciosas de Google Play (antes Android Market) y suspender las cuentas de los desarrolladores sospechosos, sino también eliminar las aplicaciones de los dispositivos móviles donde han sido instaladas, notificando al usuario sobre las acciones realizadas.

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

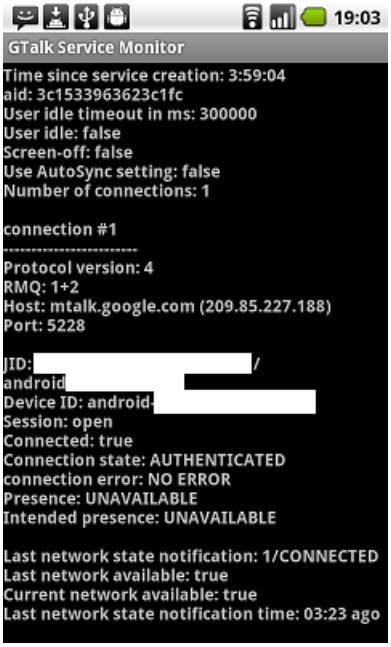
5.19.3 CONEXIÓN GTALKSERVICE

695. La conexión GTalkService [Ref.- 77] [Ref.- 78], 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 (2G/3G) o Wi-Fi.

696. El servicio GTalkService es empleado para el envío de mensajes (intents) desde Google a los dispositivos móviles Android, o para la instalación o eliminación remota de aplicaciones.

697. 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 modificar el trafico intercambiado y, por ejemplo, eliminar o instalar nuevas aplicaciones en el dispositivo móvil.

698. Mediante el código *#*#8255#*#* (o *#*#talk#*#*) de llamada del teléfono en Android es posible ejecutar el GTalk Service Monitor, una aplicación de depuración que permite obtener todos los detalles de ejecución de GTalkService:



699. El *Gtalk Service Monitor* dispone 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>", dónde <CODIGO> es un string de 12 valores hexadecimales) y del "Device ID" (ejemplo, "android-<CODIGO>", dónde <CODIGO> es un string de 16 valores hexadecimales) no están relacionados con el valor del "ANDROID_ID" (ver apartado "5.9. Configuración por defecto del dispositivo móvil").

700. Periódicamente, el dispositivo móvil comprueba que la conexión GTalkService continúa activa (*heartbeat*). Mediante el Gtalk Service Monitor es posible forzar una comprobación o heartbeat (ver imagen superior derecha, botón "Send heartbeat to server").

701. El *heartbeat* requiere tres o cuatro paquetes TCP (un intercambio de datos por cada extremo más las correspondientes confirmaciones) asociados a la sesión existente de GTalkService para realizar la comprobación del estado de la conexión:

```
182 942.984695 192.168.1.170   209.85.227.188   TCP   49831 > hpvroom [PSH, ACK] Seq=659 Ack=261 Win=6912 Len=37 TSV=1485357 TSER=328908344
183 943.056020 209.85.227.188  192.168.1.170    TCP   hpvroom > 49831 [ACK] Seq=261 Ack=696 Win=6784 Len=0 TSV=329808362 TSER=1485357
184 943.056857 209.85.227.188  192.168.1.170    TCP   hpvroom > 49831 [PSH, ACK] Seq=261 Ack=696 Win=6784 Len=37 TSV=329808362 TSER=1485357
185 943.060447 192.168.1.170   209.85.227.188   TCP   49831 > hpvroom [ACK] Seq=696 Ack=298 Win=6912 Len=0 TSV=1485366 TSER=329808362
```

5.20 AUTENTIFICACIÓN DE DOS FACTORES EN GOOGLE APPS

702. El acceso a Google Apps, aplicaciones de Google, puede ser protegido por un mecanismo de verificación en dos pasos más seguro [Ref.- 15]. En lugar de emplearse únicamente las credenciales estándar de acceso del usuario a la cuenta de Google Apps, basadas en un nombre de usuario y una contraseña, la verificación en dos pasos (o autentificación de dos factores) requiere que el usuario introduzca adicionalmente a su contraseña (algo que conoce) un código obtenido mediante su dispositivo móvil (algo que posee).

703. El código de acceso puede ser obtenido en el dispositivo móvil a través de la aplicación Google Authenticator [Ref.- 14], disponible en el Google Play, un mensaje de texto (SMS) o una llamada de teléfono.

704. La generación de los códigos de verificación no requiere disponer de conexión a Internet, servicio de telefonía móvil o plan de datos asociado.

5.21 APLICACIONES EN ANDROID

705. Los siguientes apartados proporcionan breves recomendaciones de seguridad asociadas a las aplicaciones más relevantes existentes por defecto en Android. En ningún caso se pretende realizar un análisis de seguridad exhaustivo de su funcionamiento y de todas las opciones de configuración disponibles en cada aplicación.

Nota: El número de aplicaciones cliente instaladas por defecto por Android (Google), el fabricante del dispositivo móvil o el operador de telefonía móvil, así como la variedad de aplicaciones cliente 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 aplicaciones instaladas, o a instalar, en el dispositivo móvil se recomienda realizar una análisis detallado (similar al efectuado a lo largo de esta guía para algunas de las aplicaciones existentes por defecto en Android), 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, junto a cualquier otra característica de seguridad ofrecida por la aplicación.

5.22 NAVEGACIÓN WEB: NAVEGADOR

706. Una de las tareas más comunes realizadas desde los dispositivos móviles es la de navegación web por Internet. Android incluye por defecto un navegador web, llamado “Navegador” y disponible desde el “Launcher”, basado en el motor de código abierto WebKit y en el motor JavaScript Chrome V8.

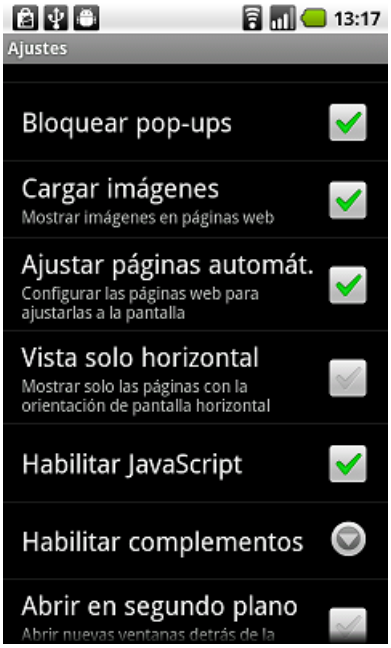
Nota: Algunos fabricantes de dispositivos móviles incluyen otros navegadores web por defecto en sus dispositivos móviles Android, como por ejemplo, Firefox para Android u Opera Mobile o Mini.

707. La versión de “Navegador” disponible por defecto en Android 2.2 es la versión 2.2, manteniendo siempre la misma versión que el sistema operativo.

708. El navegador web de Android presenta limitaciones de seguridad relevantes, como por ejemplo no disponer de soporte para cookies “HttpOnly”, empleadas para proteger la sesión de un usuario frente a ataques de Cross-Site Scripting (XSS) [Ref.- 121].

709. A través del botón “Menú”, cuando la aplicación está siendo ejecutada, es posible acceder mediante la opción “Más - Ajustes” al menú de configuración del “Navegador”, desde dónde se pueden bloquear pop-ups (habilitado por defecto), habilitar o deshabilitar JavaScript y otros complementos (ambos habilitados por defecto), borrar la caché y el historial, permitir el uso de cookies (habilitado por defecto) y borrar las cookies almacenadas actualmente, recordar los datos introducidos en formularios (habilitado por defecto) y borrar los datos almacenados actualmente, así como gestionar las opciones globales de ubicación empleadas por el navegador web, así como las opciones

individualizadas por sitio web (ver apartado “5.10.4.6. Navegador web”). Adicionalmente el navegador web puede mostrar advertencias sobre problemas de seguridad con los sitios web (habilitado por defecto), y recordar las contraseñas empleadas (habilitado por defecto), pudiendo ser eliminadas las que están almacenadas actualmente:



710. 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) y complementos (mediante la opción “A petición” dentro de las tres disponibles), y el uso de cookies en el navegador web, con el objetivo de mitigar los ataques asociados a la ejecución de scripts maliciosos en el navegador y a la privacidad del usuario a través de las cookies. Adicionalmente, el bloqueo de pop-ups y que se muestren las advertencias de seguridad son opciones que deben estar habilitadas, mientras que las opciones de recordatorio de datos de formularios, ubicación, y contraseñas deben deshabilitarse.

711. Esta configuración podría dificultar la visualización de páginas web que utilizan scripts, complementos y cookies en sus contenidos web y para su funcionamiento (la mayoría de páginas web en Internet).

712. Se recomienda borrar de forma frecuente tanto la caché como el historial de navegación web, así como el almacenamiento de cookies, datos de formularios y contraseñas, con el objetivo de proteger la privacidad del usuario.

713. Cada uno de estos elementos puede ser eliminado individualmente mediante el botón “Borrar <elemento>” desde el menú de configuración previamente descrito.

5.22.1 PROVEEDOR DE BÚSQUEDAS AUTOMÁTICO

714. Cuando se introduce un término en la barra de navegación del navegador web, si éste no corresponde con un servidor web, de forma automática se realiza una búsqueda de dicho término a través del buscador de Google (www.google.com).

715. Este comportamiento tiene implicaciones de seguridad relevantes al revelar en Internet la información introducida en la barra de navegación, carácter a carácter según ésta es tecleada, como por ejemplo el nombre de servidores internos de una organización.

716. El agente de usuario empleado por Android para estas búsquedas es el siguiente, desvelando la versión, tipo de terminal (“passion”) y compilación de Android utilizada:

```
Android/1.0 (passion FRF91)
```

717. Adicionalmente, la información del dispositivo móvil se desvela en los parámetros de la URL de “google.com” empleada para las búsquedas, incluyendo sin cifrar mediante HTTP el idioma empleado (“es”), la versión de Android y del navegador web (“2.2”), y el tipo de plataforma móvil (“android”):

```
GET
/m/gne/suggest/v2?q=test&hl=es&gl=es&app=iss&appv=2.2&platform=android&fe
eds=qs,ns HTTP/1.1\r\n
```

5.22.2 IDENTIFICACIÓN DEL NAVEGADOR WEB

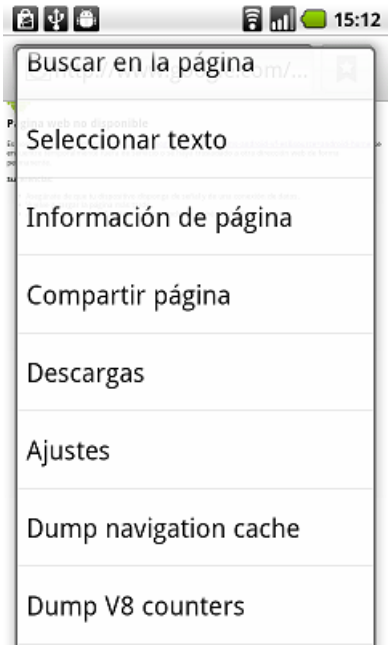
718. Cuando el navegador web accede a Internet, por ejemplo al buscador de Google, la cadena de caracteres que identifica al navegador web o agente de usuario (User-Agent) tiene el siguiente valor, revelando excesivos detalles sobre la versión del navegador web y la plataforma:

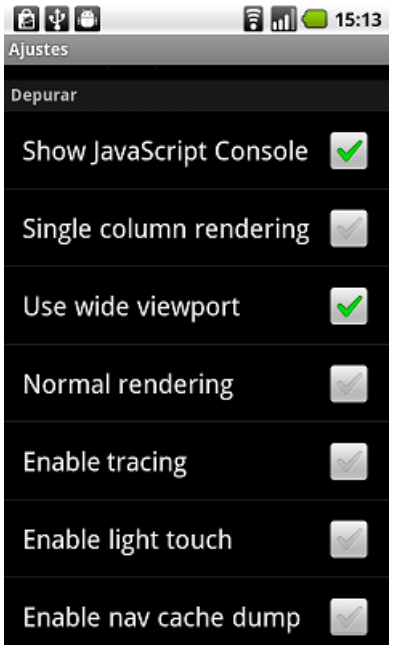
```
Mozilla/5.0 (Linux; U; Android 2.2; es-es; Nexus One Build/FRF91)
AppleWebKit/533.1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1
```

719. Los detalles del dispositivo móvil incluyen la plataforma (“Android”), la versión de Android (“2.2”), el modelo de terminal (“Nexus One”), la versión de compilación de Android (“FRF91”), el idioma empleado (“es-es”), o los detalles del navegador web (incluyendo múltiples versiones de sus componentes).

720. Se recomienda modificar el valor del agente de usuario para que no desvele información adicional. Para ello es necesario activar las capacidades de depuración del navegador web, accediendo desde la barra de dirección a “about:debug”.

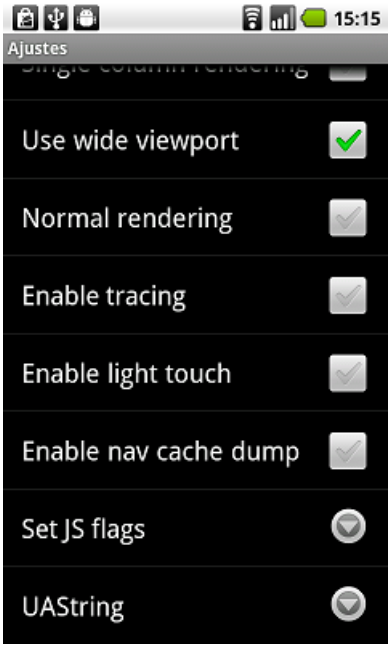
721. Una vez se ha accedido, pese a que el navegador web permanezca en la misma página que estaba previamente, a través del botón “Menú” y de las opciones “Más – Ajustes” se dispondrá de nuevas opciones de configuración avanzadas bajo la sección “Depurar”:





722. Es posible confirmar la activación del modo de depuración del navegador web desde el propio menú “Más”, al aparecer dos nuevas opciones en la parte inferior, bajo “Ajustes” (ver imagen superior izquierda): “Dump <opción>”. El menú “Ajustes” presenta igualmente en su parte inferior numerosas opciones de configuración (ver imagen superior derecha) bajo la nueva sección “Depurar”.

723. En la parte inferior de la sección “Depurar” se encuentra la opción “UAString”, que permite elegir entre el agente de usuario de Android (por defecto), de un equipo de sobremesa (“Desktop”), o de un dispositivo móvil iPhone de Apple (“iPhone”):



724. El agente de usuario recomendado desde el punto de vista de seguridad es el de “Desktop”, ya que emula la utilización del navegador web Safari sobre Mac OS X 10.5.7 (Intel) de Apple, y es lo menos aproximado al dispositivo móvil empleado. El agente de usuario de iPhone emula a un iPhone 3.0, ambos en inglés.

725. La siguiente tabla muestra los agentes de usuario para las dos nuevas opciones, “Desktop” y “iPhone” respectivamente:

```
Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_5_7; en-us)
    AppleWebKit/530.17 (KHTML, like Gecko) Version/4.0 Safari/530.17

Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us)
    AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341
    Safari/528.16
```

726. Se recomienda evaluar si habitualmente se desea realizar la navegación web como equipo de sobremesa (opción recomendada), 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.

727. Debe tenerse en cuenta que la modificación del agente de usuario, y especialmente el valor de la plataforma, podría afectar a la presentación de los contenidos web de ciertos

servidores y aplicaciones que personalizan las respuestas en función de si el cliente es un dispositivo móvil o un ordenador (de sobremesa o portátil).

728. Desafortunadamente, Android 2.2 no permite al usuario seleccionar el agente de usuario a emular. Otras versiones de Android incluyen alternativas de agente de usuario adicionales, como por ejemplo “iPad” o “Froyo-N1” (Android 2.3.6), así como potencialmente la opción de definir el valor, mediante la opción “Manual”.

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 habituales del navegador 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.

729. Algunos módulos de navegación web de Android, como el asociado a la información del GPS, 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#
```

730. El UAProf (*User-Agent Profile*) [Ref.- 84] 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).

731. El perfil contiene 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.

732. 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.

5.22.3 CONTENIDOS ADOBE FLASH

733. Por defecto, Android 2.2 no dispone de un complemento o plugin para la visualización de contenidos Flash asociado al navegador web, pero existe la posibilidad de instalarlo.

734. Al acceder a la página web oficial de Adobe Flash Player (“http://get.adobe.com/flashplayer”), el dispositivo móvil Android (identificado por su agente de usuario) es automáticamente redirigido a Google Play para llevar a cabo la descarga de la aplicación Adobe Flash Player, estando disponible la versión 11 (en concreto 11.1.111.5) en el momento de elaboración de la presente guía:

735. La aplicación Flash Player no requiere permisos especiales para ejecutar en Android.

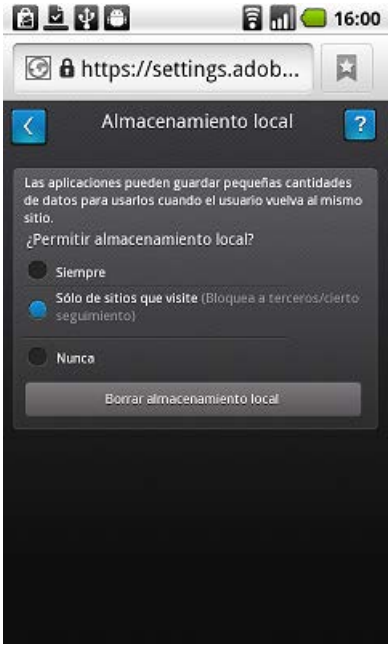
736. Esta aplicación (o *plugin*) es opcional y puede ser proporcionado por defecto en otras versiones de Android, o por el fabricante del dispositivo móvil (integrado en su versión de firmware).

737. La disponibilidad de Flash Player, o capacidades de reproducción Flash, incluida la versión disponible, pueden verificarse accediendo a la siguiente página desde el navegador web de Android: “http://www.adobe.com/software/flash/about”.

738. Debe tenerse en cuenta que las mejoras de seguridad incorporadas en las últimas versiones de Flash Player para los equipos de escritorio, por ejemplo en la versión 11.x, están habitualmente también disponibles en Flash Player para Android. Sin embargo, la correlación del número de versión entre Flash Player para escritorio (Windows, Linux, Mac OS X, etc.) y para Android no coincide, disponiendo normalmente de versiones más actualizadas para la versión de escritorio.

739. Se recomienda siempre actualizar Flash Player a la última versión disponible en Google Play, con el objetivo de eliminar las vulnerabilidades de seguridad conocidas.

740. La instalación de Flash Player en Android añade un icono en el “Launcher”, “Flash Player Settings”, que permite el acceso a la configuración de Flash Player a través del servicio web de Adobe disponible en “https://settings.adobe.com/flashplayer/mobile”:



741. Las opciones de configuración permiten establecer que datos almacenarán localmente las aplicaciones Flash obtenidas de sitios web, permitiéndose siempre este almacenamiento por defecto. Desde el punto de vista de seguridad se recomienda permitir el almacenamiento sólo de los sitios web que se visiten (opción “Sólo de sitios que visite”, en la imagen superior derecha).

742. La versión de Flash Player instalada se puede obtener mediante la verificación de versión estándar para cualquier aplicación en Android (ver apartado “5.26. Actualización de aplicaciones (cliente) en Android”).

5.22.4 CONTENIDOS ADOBE PDF

743. Android dispone por defecto de una aplicación para la lectura de ficheros PDF denominada Quickoffice, versión 2.0.37 (versión 2.0-GEP), siendo también posible instalar el cliente oficial Adobe Reader desde Google Play.

744. Quickoffice no está disponible desde el “Launcher”, y por ejemplo, al acceder a contenidos PDF desde el navegador web, éste descargara el fichero PDF automáticamente y el mismo podrá ser accedido a través de la opción de “Descargas” del navegador web (disponible desde el botón “Menú”, opción “Más – Descargas”).

745. Al seleccionar el fichero PDF, éste será abierto automáticamente mediante Quickoffice.

746. Debido a las numerosas vulnerabilidades de seguridad en las aplicaciones cliente de visualización de ficheros PDF (Adobe Acrobat, Adobe Reader, Foxit, etc.) durante los últimos años, se recomienda mantener actualizada la aplicación de visualización de ficheros PDF a la última versión.

5.23 CORREO ELECTRÓNICO (E-MAIL) Y GMAIL

747. Android proporciona múltiples capacidades para la gestión de correos electrónicos (e-mails) desde el dispositivo móvil, disponibles a través del icono “Enviar correo” desde el “Launcher” (como por ejemplo cuentas de correo de Exchange, cuyo análisis queda fuera del alcance de la presente guía), o desde el icono de “GMail”, dónde es posible configurar una o varias cuentas de correo electrónico (en ambos casos).

Nota: Si se lleva a cabo la configuración de cuentas de correo electrónico mediante Exchange, SMTP, POP3, o IMAP, se recomienda siempre habilitar la opción de hacer uso de conexiones cifradas (SSL), y deshabilitar la opción de aceptar todos los certificados SSL (como aquellos no válidos o autofirmados).

748. Debido a que la vinculación del dispositivo móvil con una cuenta de Google es obligatoria, y a la relación entre esta cuenta y el servicio de correo de Google, GMail, esta funcionalidad estará habilitada normalmente.

749. Desde el punto de vista de seguridad, no se disponen de opciones avanzadas de configuración asociadas a GMail desde el dispositivo móvil Android.

750. Respecto a las credenciales de acceso a GMail, se recomienda seguir las recomendaciones descritas en el apartado "5.17. Cuenta de usuario de Google".

751. Por defecto, al escribir un nuevo mensaje el dispositivo móvil no añade ninguna firma, opción recomendada desde el punto de vista de seguridad para evitar indicar desde dónde se realiza el envío, como por ejemplo "Enviado desde un dispositivo móvil".

752. Se recomienda mantener la configuración por defecto, sin firma, 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. La gestión de las firmas se puede realizar desde el botón "Menú" y la opción "Más – Ajustes – Firma".

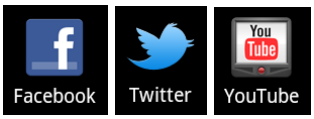
5.24 REDES SOCIALES

753. Android incluye por defecto las siguientes aplicaciones cliente para el acceso a redes sociales en Internet, disponibles en función del fabricante u operador de telefonía móvil del dispositivo móvil:

- Facebook para Android
- Twitter para Android
- YouTube

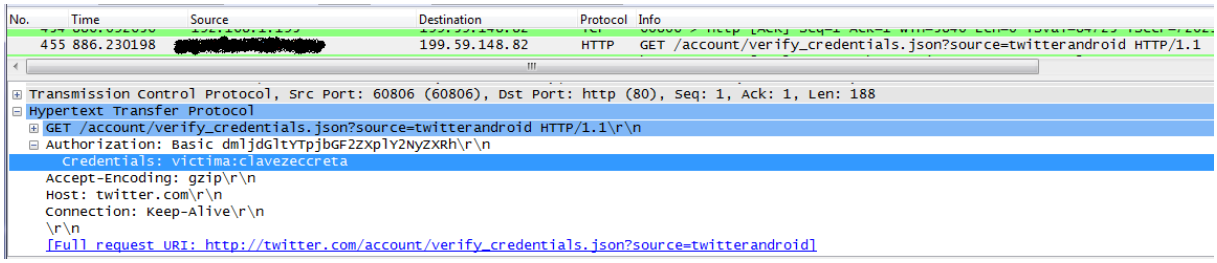
Nota: Otros dispositivos móviles basados en Android, así como otras versiones de Android, incluyen adicionalmente aplicaciones de acceso a otras redes sociales y servicios Web 2.0.

754. La ejecución de las aplicaciones de acceso a las redes sociales está disponible a través del "Launcher" y los iconos de las aplicaciones correspondientes:



755. La aplicación de acceso a Twitter disponible por defecto en Android, "Twitter para Android", versión 1.0.1 (del año 2010), realiza la autentificación con este servicio a través de HTTP en lugar de emplear HTTPS.

756. El método de autentificación empleado es HTTP "Basic", lo que permite a cualquier potencial atacante con capacidades de intercepción del tráfico de red, capturar el intercambio de datos entre el dispositivo móvil y el servicio de Twitter y obtener las credenciales de acceso del usuario, como muestra la siguiente imagen (empleando Wireshark):



757. La versión 3.0.1 de “Twitter para Android” (disponible en enero de 2012) lleva a cabo la autentificación del usuario a través de una conexión cifrada HTTPS.

758. Siempre se recomienda antes de hacer uso de cualquiera de las aplicaciones disponibles por defecto en el dispositivo móvil, o instaladas posteriormente, realizar un análisis de seguridad en profundidad para identificar este tipo de comportamientos vulnerables.

5.25 APLICACIONES DE TERCEROS: GOOGLE PLAY

759. El servicio Google Play (antes Android Market), es empleado por Google para la distribución y venta de aplicaciones y software para la plataforma Android.

760. Android incluye una aplicación, denominada “Play”, disponible desde el “Launcher”, para el acceso a este servicio directamente desde el dispositivo móvil.

761. La primera vez que se utiliza Play, la aplicación solicita al usuario disponer de una cuenta 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 “5.17. Cuenta de usuario de Google”), y aceptar los términos del servicio.

762. La conexión de autentificación empleando la cuenta de Google se realiza a través de HTTPS hacia el servidor “www.google.com”.

763. Teóricamente, la integridad de las aplicaciones de Android se verifica a través de una firma digital asociada al fichero binario (.apk) descargado, pero la ausencia de cifrado abre la puerta a la manipulación de este intercambio de datos, por ejemplo, mediante la sustitución de aplicaciones válidas firmadas digitalmente.

764. Se recomienda actualizar a la última versión de las aplicaciones ya instaladas en el dispositivo móvil (ver apartado “5.26. Actualización de aplicaciones (cliente) en Android”), ya que éstas proporcionarán posibles soluciones disponibles frente a vulnerabilidades de seguridad conocidas.

765. La lista de programas o aplicaciones instaladas desde Google Play es accesible desde la propia aplicación “Play”, o a través del menú “Ajustes – Aplicaciones”, seleccionando la opción “Instaladas” o “Todas” las que han sido instaladas alguna vez en el dispositivo:

Nota: Los desarrolladores interesados en la creación de aplicaciones para Android disponen de todos los detalles e información en el portal para desarrolladores *Android Market Publisher* (http://play.google.com/apps/publish) [Ref.- 7].

766. Debe tenerse en cuenta que la disponibilidad de una aplicación en Google Play no asegura que la misma no sea maliciosa y pueda llevar a cabo acciones desde el dispositivo móvil dónde ha sido instalada que afecten a la seguridad y privacidad del usuario [Ref.- 1].

767. Se recomienda analizar en detalle el contenido y procedencia de una aplicación de terceros antes de instalarla desde Google Play en el dispositivo móvil.

768. Una vez se ha configurado una cuenta de Google en el dispositivo móvil y ambos han sido vinculados (ver apartado “5.17. Cuenta de usuario de Google”), también desde la sección de “Ajustes” de la aplicación web de Android Market (“https://play.google.com/store/account”) es posible gestionar el dispositivo móvil asociado a la cuenta del usuario: modificar su nombre identificativo o alias, si es visible desde los menús (habilitado por defecto), y acceder a todos los detalles del mismo, incluyendo el fabricante, modelo, operador de telefonía móvil, la fecha de actividad reciente y cuando fue registrado.

Nota: Debe tenerse en cuenta que la vinculación del dispositivo móvil con una cuenta de usuario de Google permite por tanto a Google conocer el operador de telefonía móvil empleado en cada momento.

5.26 ACTUALIZACIÓN DE APLICACIONES (CLIENTE) EN ANDROID

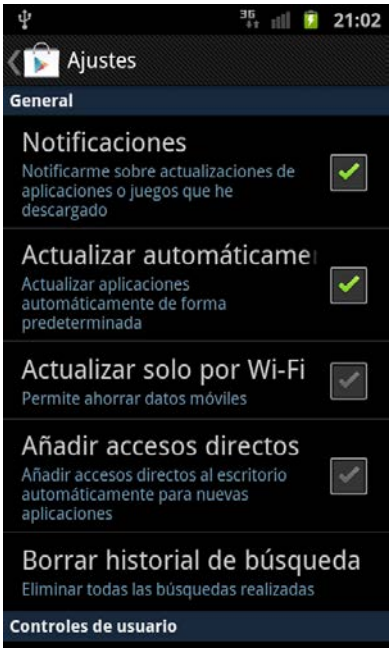
769. El término aplicaciones cliente engloba al conjunto de aplicaciones de terceros que son compatibles con Android y que pueden ser instaladas sobre este sistema operativo.

Nota: Pese a que Android permite la instalación de aplicaciones de terceros no oficiales (ver apartado “5.19. Instalación y eliminación de aplicaciones en Android”), el análisis de las

actualizaciones de aplicaciones cliente en Android se centra en las aplicaciones oficiales disponibles a través de Google Play.

Existen escenarios dónde la aplicación "Play" no puede ser ejecutada si no se dispone de conectividad de datos hacia Internet (Wi-Fi o 2G/3G), mostrándose el siguiente mensaje: "*Atención: Se ha producido un error de red. Inténtalo de nuevo o cancela la operación y vuelve a la pantalla anterior*" o "*Sin conexión*" (según la versión disponible).

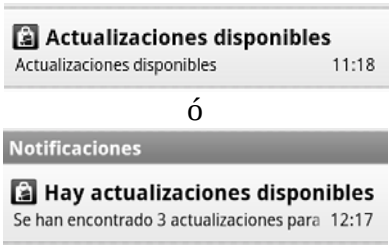
770. Desde la aplicación de Google Play menú "Ajustes" en el apartado "General" es posible configurar como se desea que se produzca el proceso de actualización de las aplicaciones instaladas desde Google Play. Así existe la opción de activar la notificación sobre la actualización de las alicaciones instaladas anteriormente o Actualizar automáticamente las aplicaciones de forma predeterminada, pudiendo configurar que el proceso de descarga de actualizaciones se produzca sólo por red Wi-Fi:



771. En caso de estar interesados en actualizar las aplicaciones tan pronto estén disponibles, tanto a través de redes Wi-Fi como de redes de datos móviles 2G/3G, se recomienda no activar la opción "Actualizar solo por Wi-Fi".

772. El proceso de verificación de actualizaciones se realiza a través de una comunicación HTTPS cifrada con el servidor "android.clients.google.com", aunque las imágenes (PNG, JPG, etc.) se obtienen mediante HTTP desde los servidores "lhX.ggpht.com".

773. La barra de notificaciones de Android mostrará un aviso sobre la disponibilidad de actualizaciones para las aplicaciones cliente, en caso de no haber seleccionado la opción de actualización automática.



774. Mediante la selección de dicha notificación, el usuario puede identificar para qué aplicaciones se dispone de actualización.

775. La pantalla de actualización proporciona detalles sobre las actualizaciones disponibles para las aplicaciones descargadas e instaladas en el dispositivo móvil, así como del resto de aplicaciones instaladas para las que no existe una actualización.

776. Se recomienda dejar habilitada la opción de notificaciones automáticas, y en función del perfil del usuario del dispositivo móvil, habilitar también la opción "Actualizar automáticamente" en el caso de usuario no avanzados. Los usuarios avanzados pueden estar interesados en no habilitar esta opción para poder revisar y analizar las actualizaciones disponibles antes de que éstas sean instaladas.

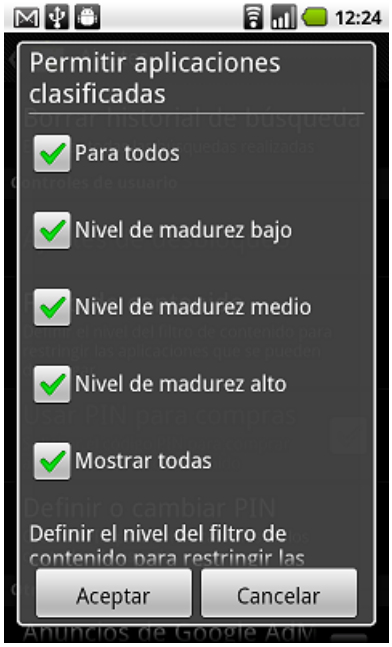
777. Si la funcionalidad de actualizaciones automáticas ha sido habilitada, las nuevas actualizaciones serán aplicadas sin la intervención del usuario si la actualización no modifica los permisos requeridos por la aplicación.

778. En caso de que los permisos hayan cambiado, el proceso de actualización manual mostrará los nuevos permisos requeridos por la nueva versión de la aplicación.

779. El proceso de descarga e instalación de una nueva actualización establece conexiones HTTP no cifradas con el servidor "android.clients.google.com", y en concreto, solicitando el paquete o aplicación a descargar y desvelando numerosos detalles del dispositivo móvil y del software involucrado, como números de versiones, identificadores, cookies, agente de usuario, etc.

780. Debido a que se hace uso de HTTP, y no de HTTPS, para esta comunicación, un posible atacante podría modificar todo el tráfico asociado a la descarga de aplicaciones y actualizaciones en Android.

781. Adicionalmente, Android permite a través de la opción "Filtro de contenido" disponible en los ajustes de "Play" seleccionar el nivel de filtro permitido para la instalación (y navegación por Google Play) de aplicaciones, en función de su nivel de madurez:



782. El nivel de madurez se evalúa en función de los contenidos de la aplicación (violencia – real o fantástica, referencias sexuales, contenido ofensivo, material inadecuado, etc.) y del

tipo de datos del usuario recopilados por la aplicación (ubicación, funciones sociales, compartir datos con otros usuarios, etc.) [Ref.- 104].

783. La opción “Definir o cambiar PIN” permite al usuario establecer un PIN para evitar cambios en los controles de usuario y filtros de contenido por parte de otros usuarios del dispositivo móvil (como por ejemplo menores).

784. El mismo menú de configuración, es decir, desde la aplicación “Play”, a través del botón “Menú”, tras acceder a la opción “Ajustes”, permite la personalización de anuncios mediante la opción “Anuncios de Google AdMob” (deshabilitada por defecto). Se recomienda (por motivos de privacidad) dejar esta opción deshabilitada, ya que permite al dispositivo móvil mostrar anuncios en las aplicaciones del terminal en función de los intereses del usuario.

785. Si la opción se encuentra habilitada, aquellas aplicaciones de Android que muestran anuncios al usuario personalizarán los anuncios en base a los intereses y datos demográficos del usuario. Para ello se emplea el identificador único del dispositivo móvil, tras un proceso de conversión a otro identificador anónimo asociado (según Google).

786. La propia aplicación “Play” se actualiza automáticamente cuando hay disponibles nuevas versiones de sí misma, de forma silenciosa, sin solicitar permiso o notificar al usuario. No se dispone de ninguna opción para que esta actualización no se lleve a cabo. La actualización se lleva a cabo tras ejecutar la aplicación “Play” y acceder a la pantalla principal de Google Play.

787. La versión de la aplicación “Play”, al igual que de cualquier otra aplicación cliente instalada en Android, puede obtenerse desde el menú “Ajustes – Aplicaciones – Administrar aplicaciones”, desde la pestaña “Todas”, seleccionando la aplicación (en el ejemplo inferior, “Play”) de la lista de todas las aplicaciones disponibles (por ejemplo, versión 3.7.13):

788. La pantalla de información de la aplicación cliente permite tanto desinstalar la aplicación (para aplicaciones de terceros), mediante el botón “Desinstalar” (ver imagen superior derecha - deshabilitado), como desinstalar todas las actualizaciones disponibles (para aplicaciones nativas y disponibles por defecto en Android), mediante el botón “Desinstalar

actualizaciones" (ver imagen superior izquierda), ya que estas aplicaciones nativas no pueden ser desinstaladas completamente.

789. Con el objetivo de disponer 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 aplicaciones instaladas, independientemente del desarrollador. La última versión debería solucionar todas las vulnerabilidades de seguridad públicamente conocidas.

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

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

Nota: Adicionalmente existen numerosas aplicaciones cliente o *suites* de software comercial disponibles a través de Google Play o de compañías comerciales cuyo objetivo es aumentar el nivel de seguridad del dispositivo móvil Android, como *suites* o soluciones de seguridad con antivirus, copias de seguridad, bloqueo remoto del terminal, borrado de datos y localización del terminal (ej. AVG Mobilation, Norton Mobile Security, Trend Micro Mobile Security, McAfee WaveSecure, Sophos Mobile, Mobile Defense, Lookout, Autowipe, etc).

6. APÉNDICE A: GUÍA DE SEGURIDAD DE ANDROID 2.3

792. El presente apartado detalla las principales recomendaciones y diferencias de seguridad asociadas a Android versión 2.3 (“Gingerbread”) [Ref.- 9], liberada el 6 de diciembre de 2010, centrándose únicamente en las nuevas funcionalidades y mecanismos de protección disponibles respecto a la versión 2.2 (“Froyo”) de Android (liberada en mayo de 2010, rev. 1.0 y en julio de 2010, rev. 2.0).

Nota: Debe tenerse en cuenta que adicionalmente, a lo largo de la presente guía, se han proporcionado referencias a otras diferencias de seguridad entre Android 2.2 y Android 2.3, o incluso versiones posteriores (Android 3.x y 4.x).

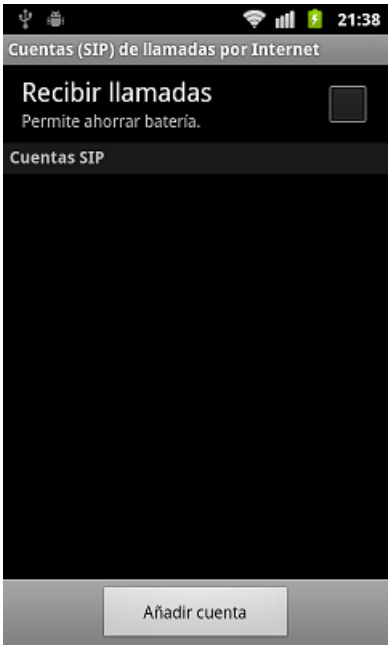
793. La versión 2.3 de Android añade nuevas capacidades respecto a la versión 2.2, incluyendo mejoras en el interfaz de usuario (nuevos temas) y en el teclado táctil, capacidades de copiar y pegar datos, mejoras en la gestión de aplicaciones, un nuevo gestor de descargas web (optimizado para descargas HTTP de mayor tamaño), una nueva aplicación para la cámara y soporte multicámara, soporte para pantallas de mayor tamaño, soporte para nuevos sensores (ej. giroscopio), mejoras en la gestión y consumo de energía, así como soporte para NFC (Near Field Communication) y llamadas de Voz sobre IP (VoIP) mediante SIP (audio y vídeo) [Ref.- 59].

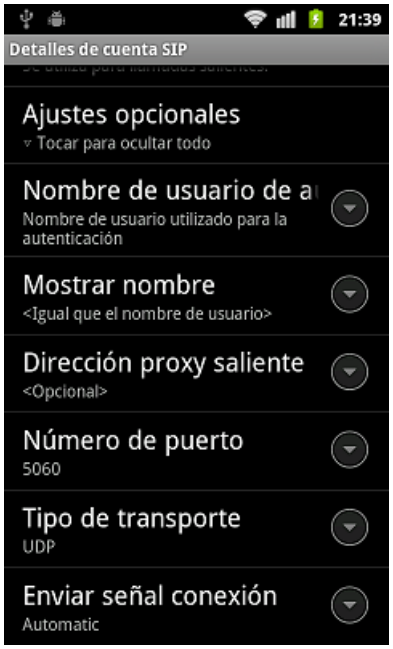
794. La versión del kernel de Linux se ha actualizado de la versión 2.6.32 (Android 2.2) a la versión 2.6.35 (Android 2.3).

795. La guía de usuario de Android 2.3 [Ref.- 25] detalla las principales diferencias generales de esta nueva versión.

796. Android 2.3 permite la instalación de certificados digitales, no sólo desde la tarjeta SD, sino también a través de la conexión USB (en función del modelo de dispositivo móvil), mediante la opción “Ajustes – Ubicación y seguridad – Instalar desde almac USB” (ver apartado “5.7. Gestión de certificados digitales y credenciales en Android”).

797. Android 2.3 permite la configuración de cuentas de Voz sobre IP (VoIP) para realizar llamadas de voz a través de Internet (únicamente a través de redes Wi-Fi) desde el menú “Ajustes – Ajustes de llamadas – Cuentas”, aunque parece no ofrecer capacidades avanzadas de configuración y seguridad, como por ejemplo posibilidad de cifrado de la señalización y contenido de las llamadas de voz mediante los protocolos SIPS y SRTP:

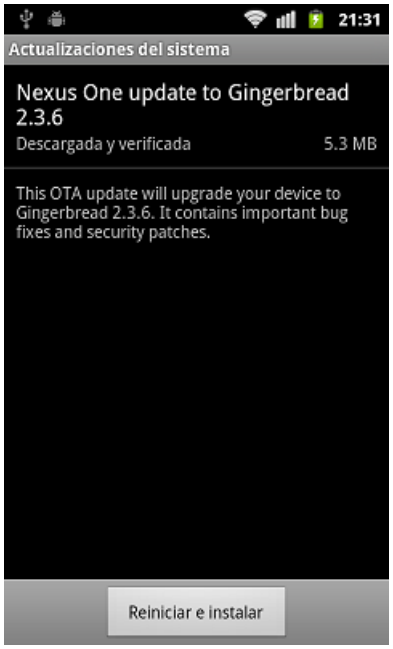




798. Se recomienda deshabilitar las capacidades de NFC (Near Field Communication) de Android 2.3 salvo que se haga uso activo de su funcionalidad. NFC puede ser deshabilitado desde el menú “Ajustes – Conexiones inalámbricas (y redes) – NFC”. Únicamente se mostrará el menú “NFC” en los terminales con capacidades NFC.

799. Si NFC está habilitado, su funcionalidad está disponible en todo momento y el terminal procederá a leer o escanear “etiquetas” NFC (otros dispositivos) tras desbloquear simplemente la pantalla del dispositivo móvil. La gestión de las etiquetas escaneadas se puede realizar desde la aplicación “Etiquetas” disponible desde el “Launcher”.

800. El dispositivo móvil empleado para la elaboración de la presente guía, (HTC) Nexus One, dispone de una actualización a Android 2.3.6 (GRK39F) de septiembre de 2011 [Ref.- 97], disponible de forma automática o para su descarga manual [Ref.- 98] (ver apartado “5.1.2. Actualización manual de Android”):



801. Android 2.3.3 [Ref.- 62] constituye una actualización reducida respecto a la versión 2.3, añadiendo principalmente actualizaciones de la API (API level 10) para los desarrolladores, y ciertas mejoras en NFC y Bluetooth [Ref.- 63].

802. La actualización a la versión 2.3.4 incluye un parche de seguridad (ver apartado “5.17.1. Asignación de una cuenta de Google al dispositivo móvil”), mientras que la versión 2.3.6 incluye múltiples soluciones frente a errores de funcionalidad conocidos y actualizaciones (o parches) de seguridad, por lo que se recomienda su instalación.

7. APÉNDICE B: CAPTURA DE LA PANTALLA EN ANDROID

803. Por defecto Android no proporciona ninguna aplicación para la captura de la pantalla del dispositivo móvil (screenshot). Existen utilidades de terceros que proporcionan esta funcionalidad pero la mayoría de ellas requieren llevar a cabo el proceso de rooting del dispositivo móvil (según el modelo de dispositivo móvil).

804. Sin embargo, es posible realizar capturas de la pantalla del dispositivo móvil Android mediante un ordenador a través del puerto USB haciendo uso de las capacidades de depuración del kit de desarrollo de software (SDK, Software Development Kit) de Android.

805. Las siguientes instrucciones para Windows permiten visualizar la pantalla del dispositivo móvil Android desde un ordenador, siendo posible realizar capturas de la misma.

806. Debido a las capacidades que proporcionan este conjunto de utilidades y acceso para la gestión del dispositivo móvil, se recomienda su utilización para la generación de documentación de seguridad, como por ejemplo, la presente guía.

807. Para poder llevar a cabo capturas de pantalla es necesario instalar diferentes componentes software en el ordenador, incluyendo los drivers USB de acceso al dispositivo móvil Android para Windows [Ref.- 20], el kit de desarrollo de Java (JDK, Java Development Kit) [Ref.- 21] y el kit de desarrollo de software (SDK) de Android [Ref.- 22] para Windows.

808. Para algunos dispositivos móviles basados en Android diferentes al empleado para la elaboración de la presente guía puede ser necesario descargar los drivers USB para Windows desde la propia web del fabricante del dispositivo [Ref.- 20].

809. Como paso previo se recomienda proceder a la instalación del JDK de Java en Windows [Ref.- 21] siguiendo el procedimiento estándar.

810. En el caso del dispositivo empleado para la elaboración de la presente guía, en primer lugar es necesario llevar a cabo la instalación del SDK de Android. Para ello sólo hay que proceder a la instalación estándar ejecutando el fichero de instalación (ej. “installer_r10-windows.exe”) [Ref.- 22], que instalará Android SDK Tools, revisión 10, versión disponible en el momento de elaboración de la presente guía.

811. El SDK de Android para Windows está disponible en un fichero instalable (EXE; opción recomendada), o en un fichero comprimido (ZIP), que sólo requiere descomprimir los contenidos del SDK en una carpeta [Ref.- 22].

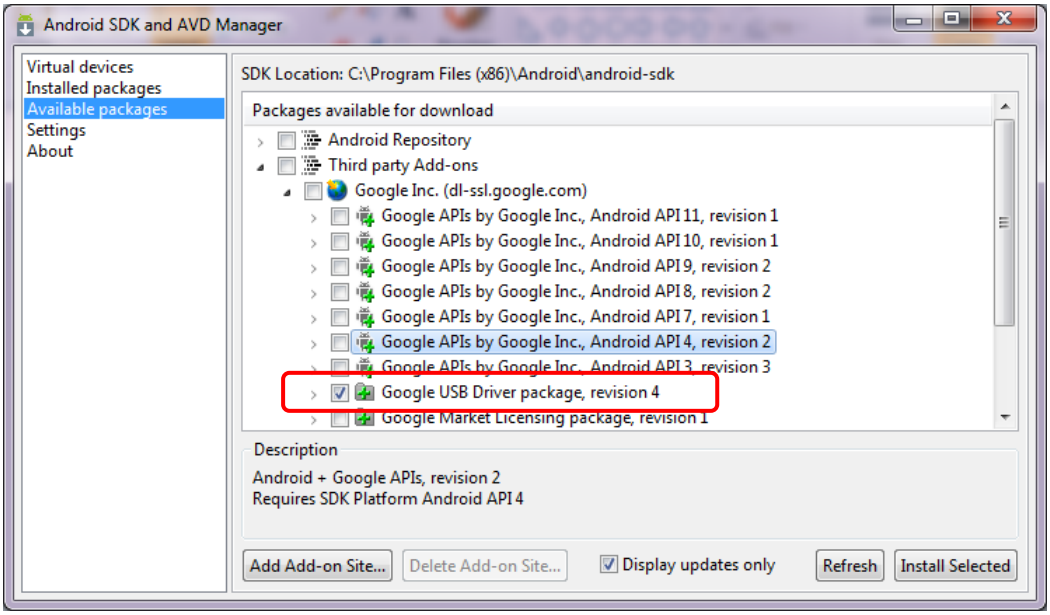
812. Mediante el fichero de instalación, el SDK de Android se instalará (en Windows 7) en la carpeta “C:\Users\<usuario>\AppData\Local\Android\android-sdk” si se instala como usuario no privilegiado, o en “C:\Program Files (x86)\Android\android-sdk” si se instala como administrador (en adelante, carpeta “SDK”). Ambas ubicaciones pueden ser modificadas durante el proceso de instalación.

Nota: Tras la instalación del SDK se comprueba la disponibilidad de actualizaciones de los componentes del kit de desarrollo. Para la captura de la pantalla del dispositivo móvil Android no es necesario instalar o actualizar ningún componente adicional salvo los detallados en el presente apartado, junto al paquete “Android SDK Platform-tools” (revisión 3), al ser recomendable disponer siempre de la última revisión de este componente.

813. Una vez instalado el SDK es necesario instalar los drivers USB de Android para Windows. Los drivers USB están disponibles como un componente opcional del SDK.

814. Para su instalación es necesario emplear la herramienta del SDK denominada “Android SDK and AVD Manager”, asociada al fichero “SDK Manager.exe” que está ubicado en la carpeta “SDK”, y que permite la descarga de otros componentes del kit de desarrollo.

815. Desde la herramienta debe seleccionarse la opción “Available packages”, expandir la categoría “Third party Add-ons” y la subcategoría “Google Inc.” (dl-ssl.google.com), y seleccionar el paquete “Google USB Driver package” (asociado a la última revisión disponible; la número 4 en el momento de aplicación de la presente guía):



Nota: Para disponer de todas las categorías y subcategorías mencionadas puede ser necesario actualizar los componentes disponibles mediante el botón “Refresh” de la sección “Available packages”.

816. Mediante el botón “Install Selected” se llevará a cabo la descarga de los drivers USB, almacenándose en la carpeta “SDK\extras\google\usb_driver”.

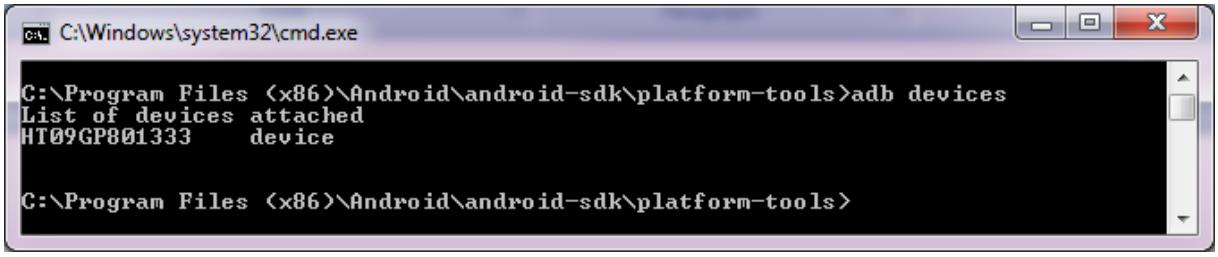
817. Adicionalmente es necesario, a través del menú “Ajustes” (“Settings”) del dispositivo móvil Android y en concreto de la opción “Aplicaciones – Desarrollo” (“Applications – Development”), habilitar la opción “Depuración USB” (“USB debugging”), debiéndose aceptar la confirmación de activación del modo de depuración USB:

818. La instalación de los drivers USB [Ref.- 20] en Windows 7 (en inglés) requiere llevar a cabo los siguientes pasos:

    1. Conectar el dispositivo móvil Android al puerto USB del ordenador.
    2. Pulsar con el botón derecho en “Computer” y seleccionar “Manage”.
    3. Seleccionar “Device Manager” en el panel de la izquierda.
    4. Localizar y expandir la opción “Other devices” en el panel de la derecha, que incluirá el nuevo dispositivo móvil, por ejemplo, “Nexus One”.
    5. Mediante el botón derecho una vez seleccionado el nuevo dispositivo, seleccionar “Update Driver Software…” y la opción “Browse my computer for driver software”.
    6. Debe seleccionarse la carpeta que contiene los drivers USB del SDK, disponibles en “SDK\extras\google\usb_driver”, incluyendo sus subcarpetas.
    7. El proceso confirmará la instalación del driver “Android Composite ADB Interface”, apareciendo en la lista de dispositivos hardware de Windows como “Android Phone”.

819. Android proporciona la herramienta Android Debug Bridge (adb) para la realización de tareas de bajo nivel desde un ordenador [Ref.- 107].

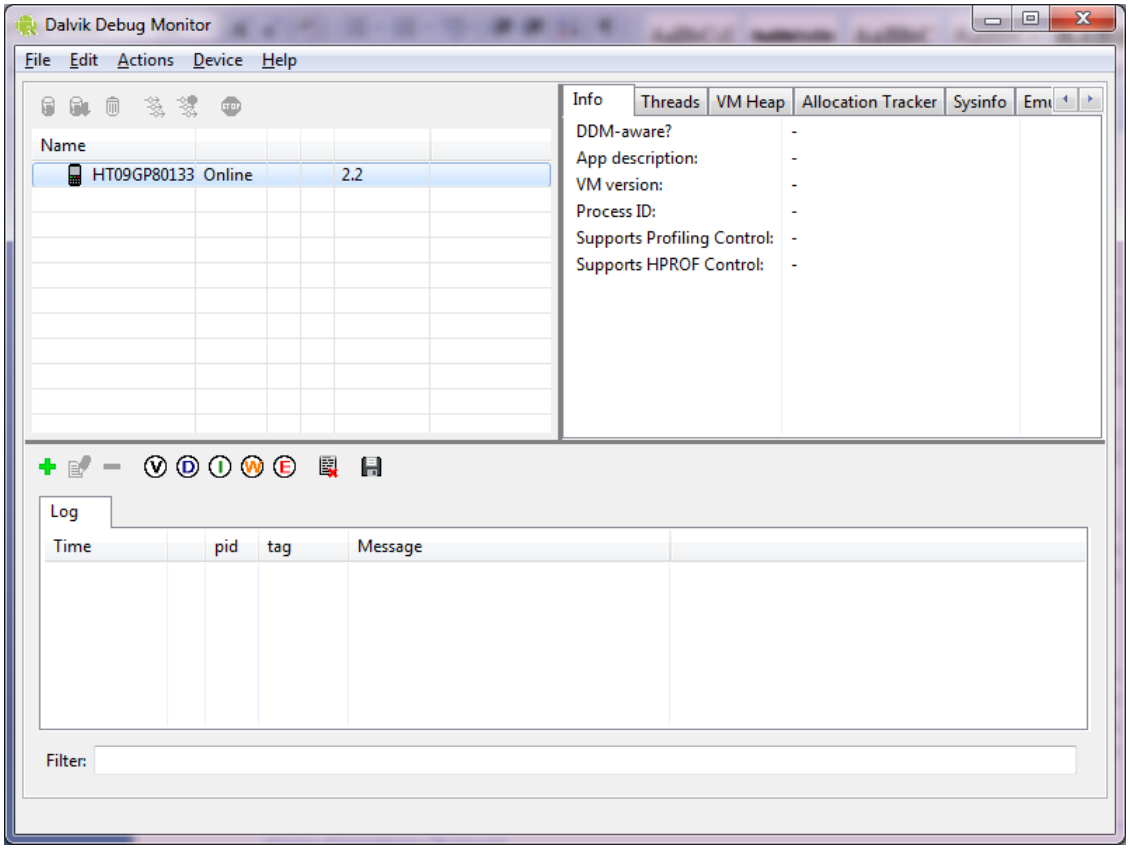
820. Es posible confirmar que el dispositivo ha sido detectado adecuadamente por el ordenador y el SDK de Android mediante el comando “adb devices” disponible desde la carpeta “SDK\platform-tools”:



Nota: El proceso de actualización del driver USB a una nueva revisión, así como el proceso de instalación para Windows XP y Windows Vista, puede diferir del proceso descrito para la instalación inicial de los drivers en Windows 7 [Ref.- 20].

821. Para proceder a la captura de la pantalla del dispositivo móvil Android es necesario conectar el mismo al ordenador a través del puerto USB y ejecutar la utilidad “ddms.bat”, disponible en la carpeta “SDK\tools”.

822. La primera vez que se ejecuta el SDK de Android es posible que se consulte al usuario si desea enviar estadísticas de uso a Google. Una vez el usuario indica su preferencia, la utilidad *Dalvik Debug Monitor* (DDM) se abrirá, mostrando el dispositivo móvil conectado y su versión de Android en la columna de la izquierda:



823. Tras seleccionar el dispositivo móvil, desde el menú “Device – Screen capture…” es posible capturar la pantalla disponible actualmente en el dispositivo móvil. En caso de estar interesado en la captura de otra pantalla, sólo es necesario acceder a la pantalla adecuada en el dispositivo móvil y refrescar la misma en la utilidad de captura a través del botón “Refresh”.

824. Mediante el botón “Save” es posible guardar una captura de la pantalla actual en un fichero gráfico de alta resolución (480 x 800 pixels, 24 bits) en formato PNG (por defecto).

8. REFERENCIAS

La siguiente tabla muestra las fuentes de información a las que se hace referencia a lo largo de la presente guía:

Referencia	Título, autor y ubicación
[Ref.- 1]	"Guía CCN-STIC-450: Seguridad de dispositivos móviles". CCN-CERT. 2010. URL: https://www.ccn-cert.cni.es - Herramientas – Series CCN-STIC
[Ref.- 2]	Android. Google. URL: http://www.android.com
[Ref.- 3]	Google Nexus One. Google. URL: http://www.google.com/phone/detail/nexus-one
[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]	"An Update on Google Play Security". Google. March 2011. URL: http://googlemobile.blogspot.com/2011/03/update-on-android-Play-security.html
[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]	"What is Android?". Google. URL: http://developer.android.com/guide/basics/what-is-android.html
[Ref.- 12]	"Bring Your Phone to Work Day: Managing Android Devices With Google Apps". Octubre 2010. Google. URL: http://googleenterprise.blogspot.com/2010/10/bring-your-phone-to-work-day-managing.html
[Ref.- 13]	"Google Apps Device Policy". Google. URL: https://market.android.com/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 app. Google. URL: https://Play.android.com/details?id=com.google.android.apps.authenticator URL: https://www.google.com/support/accounts/bin/answer.py?answer=1066447
[Ref.- 15]	"Getting started with 2-step verification. How it works". Google Apps. Google. URL:https://www.google.com/support/accounts/bin/static.py?page=guide.cs&guide=1056283&topic=1056284
[Ref.- 16]	"Application Fundamentals". Android Developers. Google. URL: http://developer.android.com/guide/topics/fundamentals.html
[Ref.- 17]	"Security and Permissions". Android Developers. Google. URL: http://developer.android.com/guide/topics/security/security.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
[Ref.- 19]	"API Levels". Android Developers. Google. URL: http://developer.android.com/guide/appendix/api-levels.html
[Ref.- 20]	Android (and OEM) USB Drivers for Windows. Google. URL: http://developer.android.com/sdk/win-usb.html URL: http://developer.android.com/sdk/oem-usb.html
[Ref.- 21]	JDK: Java Development Kit. Java/Sun/Oracle. URL: http://java.sun.com/javase/downloads/

Referencia	Título, autor y ubicación
[Ref.- 22]	Android SDK: Software Development Kit. Google. URL: http://developer.android.com/sdk/index.html URL: http://developer.android.com/sdk/installing.html
[Ref.- 23]	Manifest Permission (Since API Level 1). Google. URL: http://developer.android.com/reference/android/Manifest.permission.html
[Ref.- 24]	"Android 2.2.1 User's Guide". Google. October 23, 2010. URL: http://www.google.com/googlephone/AndroidUsersGuide.pdf
[Ref.- 25]	"Android 2.3 User's Guide". Google. December 13, 2010. URL: http://www.google.com/googlephone/AndroidUsersGuide-2.3.pdf
[Ref.- 26]	"keytool - Key and Certificate Management Tool". Java SE Documentation. Oracle. URL: http://download.oracle.com/javase/6/docs/technotes/tools/solaris/keytool.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]	"Android Encryption". Motorola. 2011. URL: https://motorola-enterprise.custhelp.com/app/answers/detail/a_id/57094
[Ref.- 30]	"Guardian Project". Github. 2010. URL: https://github.com/guardianproject/LUKS/wiki
[Ref.- 31]	"Android 3.0 Platform Highlights". Google. 2011. URL: http://developer.android.com/sdk/android-3.0-highlights.html#enterprise
[Ref.- 32]	WhisperCore. Whisper Systems. 2011. URL: http://www.whispersys.com/whispercore.html
[Ref.- 33]	WhisperCore. Whisper Systems. 2010. URL: http://www.whispersys.com/index.html
[Ref.- 34]	"Android 2.2 Platform Highlights". Google. 2010. URL: http://developer.android.com/sdk/android-2.2-highlights.html
[Ref.- 35]	"Perform a Remote Wipe on a Mobile Phone" (MS Exchange 2010). Microsoft Technet. 2009. URL: http://technet.microsoft.com/en-us/library/aa998614.aspx
[Ref.- 36]	"New Client Access Features in Exchange 2007 SP1". Microsoft Technet. 2008. URL: http://technet.microsoft.com/en-us/library/bb684907%28EXCHG.80%29.aspx
[Ref.- 37]	"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.- 38]	"Microsoft Exchange Information Services and Security Policies Supported by Android 2.2".Google. 2010. URL: www.google.com/help/hc/pdfs/mobile/ExchangeAndAndroid2.2-002.pdf
[Ref.- 39]	"Understanding Exchange ActiveSync Mailbox Policies". Microsoft Technet. 2007. URL: http://technet.microsoft.com/en-us/library/bb123484(EXCHG.80).aspx
[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 Wifi in Android". szym. 2010. URL: http://szym.net/2010/12/adhoc-wifi-in-android/
[Ref.- 42]	"Prospects of Ad-hoc Wifi in Android". szym. 2010. URL: http://szym.net/2010/12/prospects-of-ad-hoc-wifi-in-android/
[Ref.- 43]	"Issue 1041: Hidden SSID Fails to Connect". Android Google Code. 2008. URL: https://code.google.com/p/android/issues/detail?id=1041
[Ref.- 44]	"How can I trust CAcert's root certificate?". CAcert Wiki. URL: http://wiki.cacert.org/ImportRootCert#Android_Phones
[Ref.- 45]	"Issue 11231: Provide support for managing CA and client certificates". Android Google Code. 2008. URL: https://code.google.com/p/android/issues/detail?id=11231
[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: http://roy.marples.name/projects/dhcpcd

Referencia	Título, autor y ubicación
[Ref.- 49]	"Guía CCN-STIC-406: Seguridad en redes inalámbricas". CCN-CERT. URL: https://www.ccn-cert.cni.es - Herramientas – Series CCN-STIC
[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 - Herramientas – Series CCN-STIC
[Ref.- 52]	"ConnectivityManager". Android Developers. URL: http://developer.android.com/reference/android/net/ConnectivityManager.html
[Ref.- 53]	"dhcpcd does not strip or escape shell meta characters". CVE-2011-0996. MITRE. URL: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0996 URL: http://roy.marples.name/archives/dhcpcd-discuss/2011/0326.html
[Ref.- 54]	"Issue 3389: Full IPv6 Android support". Android Google Code. 2009. URL: https://code.google.com/p/android/issues/detail?id=3389
[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: http://www.defcon.org/images/defcon-18/dc-18-presentations/Lineberry/DEFCON-18-Lineberry-Not-The-Permissions-You-Are-Looking-For.pdf
[Ref.- 57]	"Learn How to Find GPS Location on Any SmartPhone, and Then Make it Relevant". Acoustic. 2009. URL: http://www.codeproject.com/KB/windows/DeepCast.aspx
[Ref.- 58]	"New Android 2.2 Software Update for Nexus One phones". Google. 2010. URL: http://googlenexusoneboard.blogspot.com/2010/06/new-android-22-software-update-for.html
[Ref.- 59]	"Difference Between Android 2.2 (Froyo) and Android 2.3 (Gingerbread)". Andrew. 2010. URL: http://www.differencebetween.com/difference-between-android-2-2-froyo-and-android-2-3-gingerbread/
[Ref.- 60]	"Android update from 2.2.1 to 2.2.2". Google. 2010. URL: http://android.clients.google.com/packages/ota/passion/2854b06b22b9.signed-passion-FRG83G-from-FRG83D.2854b06b.zip
[Ref.- 61]	"Issue 9392: SMS are intermittently sent to wrong and seemingly random contact". Google Code. 2010. URL: https://code.google.com/p/android/issues/detail?id=9392
[Ref.- 62]	"Android update from 2.2.2 to 2.3.3". Google. 2010. URL: http://android.clients.google.com/packages/ota/passion/81304b2de707.signed-passion-GRI40-from-FRG83G.81304b2d.zip
[Ref.- 63]	"Difference Between Android 2.3 and Android 2.3.3". olivia. 2010. URL: http://www.differencebetween.com/difference-between-android-2-3-and-vs-android-2-3-3/
[Ref.- 64]	"See your location history dashboard and more with Google Maps 5.3 for Android". Google Mobile Blog. Google. URL: http://googlemobile.blogspot.com/2011/04/see-your-location-history-dashboard-and.html
[Ref.- 65]	"The comprehensive list of update.zip links". Nexus One Forum. Google. 2010. URL: http://www.google.com/support/forum/p/android/thread?tid=7e95404a00a9e232&hl=en
[Ref.- 66]	"Android 2.2.1 Update – New Android Gmail and more". Use My Droid. 2010. URL: http://www.usemydroid.com/android-2-2-1-update/
[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]	"Android Security FAQ". Android Developers. URL: http://developer.android.com/resources/faq/security.html
[Ref.- 70]	"Android Data Stealing Vulnerability". Thomas Cannon. 2010. URL: http://thomascannon.net/blog/2010/11/android-data-stealing-vulnerability/ URL: http://www.h-online.com/open/news/item/Android-vulnerability-permits-data-theft-1141200.html URL: http://vimeo.com/17030639

Referencia	Título, autor y ubicación
[Ref.- 71]	"Mobile Device Security and Android File Disclosure". jduck. Metasploit Blog. 2011. URL: http://blog.metasploit.com/2011/01/mobile-device-security-and-android-file.html
[Ref.- 72]	"Data Leak Vulnerability Haunts Latest Android (Gingerbread)". Matt Shipman. NCSU. 2011. URL: http://web.ncsu.edu/abstract/technology/haunted-android/ URL: http://www.csc.ncsu.edu/faculty/jiang/nexuss.html
[Ref.- 73]	"Reversing Google Play Protocol". Peter Pisljar. 2010. URL: http://peter.pisljar.si/articles/reversing_android_Play_protocol.pdf URL: http://peter.pisljar.si/projects/AMDesktop.zip URL: https://code.google.com/p/android-Play-api/
[Ref.- 74]	"Android Screen Lock Bypass". Thomas Cannon. 2011. URL: http://thomascannon.net/blog/2011/02/android-lock-screen-bypass/ URL: https://Play.android.com/details?id=se.curity.android.screenlockbypass
[Ref.- 75]	"Android Market Security". Thomas Cannon. 2011. URL: http://thomascannon.net/blog/2011/02/android-market-security/
[Ref.- 76]	"How I Almost Won Pwn2Own via XSS". Jon Oberheide. 2011. URL: http://jon.oberheide.org/blog/2011/03/07/how-i-almost-won-pwn2own-via-xss/
[Ref.- 77]	"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.- 78]	"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.- 79]	"Apple. Google Collect User Data". Wall Street Journal. 2011. URL: http://on.wsj.com/gDfmEV
[Ref.- 80]	"Android Map". Samy Kamkar. 2011. URL: http://samy.pl/androidmap/
[Ref.- 81]	Android Open Source Project (AOSP). URL: http://source.android.com
[Ref.- 82]	"Notes on the implementation of encryption in Android 3.0". AOSP. URL: http://source.android.com/tech/encryption/android_crypto_implementation.html
[Ref.- 83]	"Androix X.Y Platform Highlights". Android Developers. URL (2.2): http://developer.android.com/sdk/android-2.2-highlights.html URL (3.0): http://developer.android.com/sdk/android-3.0-highlights.html URL (4.0): http://developer.android.com/sdk/android-4.0-highlights.html
[Ref.- 84]	"Android 2.2 Platform - Revisions". Android Developers. URL: http://developer.android.com/sdk/android-2.2.html
[Ref.- 85]	"Inside the Android Security Patch Lifecycle". Tim Wyatt. Lookout. Agosto 2011. URL: http://blog.mylookout.com/blog/2011/08/04/inside-the-android-security-patch-lifecycle/
[Ref.- 86]	CTS (Compatibility Test Suite). AOSP. URL: http://source.android.com/compatibility/cts-intro.html
[Ref.- 87]	"Researcher Builds Mock Botnet Of 'Twilight'-Loving Android Users". Forbes. Junio 2010. URL: http://www.forbes.com/sites/firewall/2010/06/21/researcher-builds-mock-botnet-of-twilight-loving-android-users/
[Ref.- 88]	"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.- 89]	"Issue 6111: Allow a hostname to be specified". Android. Enero 2010. URL: https://code.google.com/p/android/issues/detail?id=6111
[Ref.- 90]	"Android Devices: Tethering and Portable Wi-Fi Hotspots – USB Tethering with Windows XP". Google Mobile. URL: https://support.google.com/mobile/bin/answer.py?hl=en&answer=182134#wifi
[Ref.- 91]	"Sharing your mobile data connection". Google Mobile. URL: https://support.google.com/mobile/bin/answer.py?hl=en&answer=168932
[Ref.- 92]	"[TAD-2011-003] Vulnerability in Android: To add, or not to add (a Wi-Fi network), that is the question". Raul Siles. Taddong. Mayo 2010. URL: http://blog.taddong.com/2011/05/vulnerability-in-android-to-add-or-not.html

Referencia	Título, autor y ubicación
[Ref.- 93]	"Issue 1215: IP settings for WiFi networks". Android. Noviembre 2008. URL: https://code.google.com/p/android/issues/detail?id=1215
[Ref.- 94]	"Putting Android to work for your business". Official Google Enterprise Blog. Abril 2011. URL: http://googleenterprise.blogspot.com/2011/04/putting-android-to-work-for-your.html
[Ref.- 95]	"Manage my devices". Google Mobile. URL: https://support.google.com/mobile/bin/answer.py?hl=en&topic=1233222&answer=1235372
[Ref.- 96]	"Issue 11855: Support settings change in Android WIFI/USB Tether". Android. Octubre 2010. URL: https://code.google.com/p/android/issues/detail?id=11855
[Ref.- 97]	"Nexus One updated to Android 2.3.6 (GRK39F)". Android Central. Septiembre 2011. URL: http://www.androidcentral.com/nexus-one-updated-android-236-grk39f
[Ref.- 98]	"Android 2.3.6 - Build GRK39F – Nexus One". Google. 2011. URL: http://android.clients.google.com/packages/ota/passion/d323ca384aaa.signed-passion-GRK39F-from-GRJ22.d323ca38.zip
[Ref.- 99]	"Package javax.net.ssl". Android Developers. URL: http://developer.android.com/reference/javax/net/ssl/package-summary.html
[Ref.- 100]	"Official Ice Cream Sandwich for the Nexus One won't happen, Google says". Android Central. Octubre 2011. URL: http://www.androidcentral.com/official-ice-cream-sandwich-nexus-one-wont-happen-google-says
[Ref.- 101]	"Configuración de privacidad". Android Mobile. URL: http://support.google.com/mobile/bin/answer.py?hl=es&answer=168581
[Ref.- 102]	"The AndroidManifest.xml File: <permission>". Android Developers. URL: http://developer.android.com/guide/topics/manifest/permission-element.html#plevel
[Ref.- 103]	"SE Android". SE Linux Project. 2012. URL: http://selinuxproject.org/page/SEAndroid URL: http://selinuxproject.org/~jmorris/lss2011_slides/caseforseandroid.pdf
[Ref.- 104]	"Clasificaciones de contenido de las aplicaciones". Google Play. URL: http://support.google.com/androidPlay/bin/answer.py?hl=es&answer=1075738
[Ref.- 105]	"Updating Google Play". Google Play. URL: http://Play.android.com/support/bin/answer.py?hl=en&answer=190860
[Ref.- 106]	"Issue 10809: Password is stored on disk in plain text". Android. Agosto 2010. URL: https://code.google.com/p/android/issues/detail?id=10809
[Ref.- 107]	"Android Debug Bridge (adb)". Android Developers. URL: http://developer.android.com/guide/developing/tools/adb.html
[Ref.- 108]	"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.- 109]	"Unsecured insights - Safety of apps for Android and iPhone". Christiane Ruetten. Octubre 2010. URL: http://www.heise.de/mobil/artikel/Sicherheit-von-Apps-fuer-Android-und-iPhone-1103681.html (*en Alemán*)
[Ref.- 110]	"Google Data Protocol - FAQ". Google Code. URL: https://code.google.com/apis/gdata/faq.html#clientlogin_expire
[Ref.- 111]	"Authentication and Authorization for Google APIs - ClientLogin for Installed Applications". Google Code. URL: https://code.google.com/apis/accounts/docs/AuthForInstalledApps.html
[Ref.- 112]	"Platform Versions". Android Developers. URL: http://developer.android.com/resources/dashboard/platform-versions.html
[Ref.- 113]	"LOOK-10-007 – TapJacking". Lookout. Diciembre 2010. URL: http://blog.mylookout.com/look-10-007-tapjacking/ URL: http://blog.mylookout.com/blog/2010/12/09/android-touch-event-hijacking/
[Ref.- 114]	"Pimp my android". Sebastián Guerrero. Security by Default. Octubre 2011. URL: http://www.securitybydefault.com/2011/10/pimp-my-android.html

Referencia	Título, autor y ubicación
[Ref.- 115]	"Massive Security Vulnerability In HTC Android Devices (EVO 3D, 4G, Thunderbolt, Others) Exposes Phone Numbers, GPS, SMS, Emails Addresses, Much More". Android Police. Enero 2012 (actualización). URL: http://www.androidpolice.com/2011/10/01/massive-security-vulnerability-in-htc-android-devices-evo-3d-4g-thunderbolt-others-exposes-phone-numbers-gps-sms-emails-addresses-much-more/
[Ref.- 116]	"A Trojan spying on your conversations". Total Defense. Agosto 2011. URL: http://totaldefense.com/securityblog/2011/08/26/A-Trojan-spying-on-your-conversations.aspx
[Ref.- 117]	"Issue 8196: Enhancement: Client Certificate Authentication in Browser". Android. Mayo 2010. URL: https://code.google.com/p/android/issues/detail?id=8196
[Ref.- 118]	"Issue 11231: Provide support for managing CA and client certificates". Android. Septiembre 2010. URL: https://code.google.com/p/android/issues/detail?id=11231
[Ref.- 119]	"KeyChain". Android Developers. URL: http://developer.android.com/reference/android/security/KeyChain.html
[Ref.- 120]	"Issue 4205: When a PPTP VPN is connected, all internet traffic is sent through the VPN". Android. Octubre 2009. URL: https://groups.google.com/group/android-contrib/browse_thread/thread/430149b033c305c2?pli=1 URL: https://code.google.com/p/android/issues/detail?id=4205
[Ref.- 121]	"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.- 122]	"HTC / Android OBEX FTP Service Directory Traversal Vulnerability Advisory". Albero Moreno Tablado. Julio 2011. URL: http://www.securityfocus.com/archive/1/518924 URL: http://seguridadmobile.blogspot.com/2011/07/htc-android-obex-ftp-service-directory.html URL: http://www.seguridadmobile.com/android/android-security/HTC-Android-OBEX-FTP-Service-Directory-Traversal.html
[Ref.- 123]	"Issue 6348: Bluetooth should have the option to be constantly discoverable and not just have a set time limit". Android. Enero 2010. URL: https://code.google.com/p/android/issues/detail?id=6348
[Ref.- 124]	"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
[Ref.- 125]	"Android update from 2.2 to 2.2.1". Google. 2010. URL: (*enlace roto en 02/2012*) URL: http://android.clients.google.com/packages/passion/signed-passion-FRG83-from-FRF91.c8847c98.zip
[Ref.- 126]	"Android 2.3.3 – GRI40 (FULL VERSION)". Google. 2011. URL: http://android.clients.google.com/packages/ota/passion/656099b119f8.signed-passion-ota-102588.656099b1.zip
[Ref.- 127]	"Android update from 2.3.3 to 2.3.4". Google. 2011. URL: http://android.clients.google.com/packages/ota/passion/71d2f9ecd610.signed-passion-GRJ22-from-GRI40.71d2f9ec.zip
[Ref.- 128]	"Android Version History". Wikipedia. URL: https://en.wikipedia.org/wiki/Android_version_history
[Ref.- 129]	"Nexus One: Gingerbread update". Vaidas Sirtautas Blog. Febrero 2011. URL: http://vsshs.com/2011/02/28/nexus-one-gingerbread-update/