GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-455)

Seguridad de dispositivos móviles: iPhone (iOS 7.x)

JULIO 2014

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE LA PRESIDENCIA

NIPO: 002-14-041-07

Fecha de Edición: Julio de 2014

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).

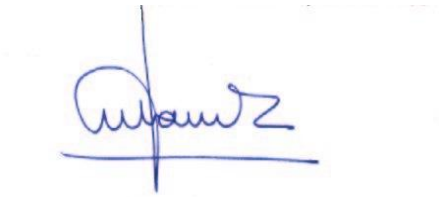
Una de las funciones más destacables que, asigna al mismo, el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información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

Junio 2014



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, iOS de Apple (empleado en dispositivos iPhone, iPad, iPod Touch y Apple TV) [Ref.- 3], en concreto hasta la versión iOS 7.x, con el objetivo de reducir su superficie de exposición frente a ataques de seguridad. Se dispone de documentos independientes de análisis y recomendaciones de seguridad tanto para iPhone como para iPad [Ref.- 127].

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 iOS versión 7.x, y en concreto para dispositivos móviles iPhone de Apple [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 está basada en la versión previa de la misma guía "*Seguridad de dispositivos móviles: iPhone*", centrada en la versión 5.x de iOS y publicada en el año 2013.

8. 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.

9. La serie CCN-STIC-45X, "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

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, y a la gestión empresarial de dispositivos móviles (MDM):

- 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-454 - Seguridad de dispositivos móviles: iPad (iOS 7.x)
- CCN-STIC-455 - Seguridad de dispositivos móviles: iPhone (iOS 7.x)
- CCN-STIC-457 - Gestión de dispositivos móviles: MDM (*Mobile Device Management*) [Ref.- 139]

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. El iPhone es un dispositivo móvil con pantalla táctil capacitiva, diseñado y fabricado por Apple, que proporciona capacidades de telefonía móvil, además de acceso a redes de datos como Internet.

12. La primera versión o generación del iPhone (o iPhone 2G) se distribuyó en EEUU en junio de 2007, comercializándose generaciones (o versiones de hardware) posteriores de este dispositivo móvil en julio de 2008 (iPhone 3G, disponible en múltiples países desde el inicio), junio de 2009 (iPhone 3GS), junio de 2010 (iPhone 4), octubre de 2011 (iPhone 4S), septiembre de 2012 (iPhone 5), y septiembre de 2013 (iPhone 5S y 5C)[1].

13. Las principales diferencias entre las distintas generaciones de iPhone residen en el hardware disponible y en las mejoras de la versión de iOS asociada. Por ejemplo, el iPhone 2G original únicamente disponía de conectividad EDGE (2.75G) y Wi-Fi, añadiéndose en el iPhone 3G conectividad 3G y capacidades de A-GPS (Assisted-GPS). Las versiones posteriores, como 3GS, introducirían una brújula, mejoras en el

[1] https://en.wikipedia.org/wiki/Iphone

rendimiento y en la capacidad de procesamiento, así como en la batería y la cámara, un elemento que se ha ido renovando en todas las generaciones posteriores. Las generaciones 4 y 4S proporcionan mejoras multimedia, de resolución de pantalla, de memoria RAM (512MB), y son las primeras versiones de iOS con capacidades multitarea.

14. Los últimos modelos, iPhone 5, 5C y 5S, incorporan pantallas de mayor tamaño (4" frente a 3,5") y más resolución, y procesadores de mayor capacidad, llegando incluso a la versión 8 de ARM con un procesador Apple A7 de 64 bits en el caso del iPhone 5S, junto a un coprocesador de movimiento (*motion*), denominado M7. Adicionalmente hacen uso de una memoria RAM de 1GB, capacidades Wi-Fi multifrecuencia (802.11a/b/g/n), soporte 4G/LTE empleando una nano SIM, y soporte para Bluetooth 4.0 (al igual que el iPhone 4S).

15. El iPhone 5S incorpora adicionalmente la tecnología Touch ID, un lector biométrico de huella dactilar que ha sido integrado en el botón principal (o Home) del dispositivo móvil (ver apartado "5.4.3. Touch ID").

16. Los dispositivos móviles iPhone se clasifican en distintos modelos dónde sólo cambia su capacidad de almacenamiento, entre 4-16 GB en el modelo original (iPhone 2G) y 16-64 GB en los últimos modelos (iPhone 5, 5C y 5S), y su color, blanco y negro inicialmente, con nuevos colores metalizados (plata, oro, etc) en las últimas versiones, junto a toda una gama de colores (blanco, rosa, amarillo, azul y verde) para el iPhone 5C.

17. iOS (originalmente iPhone Operating System, iOS) es un sistema operativo Unix propietario de Apple, basado en Darwin BSD y heredado de OS X, diseñado para dispositivos móviles.

18. Las nuevas versiones de iOS suelen acompañar al lanzamiento comercial de las nuevas versiones de los dispositivos iPhone de Apple, así la versión iOS 1.x acompañó a la primera generación de iPhone (2G) en junio de 2007[2]. En enero de 2008 se publicó la versión 1.1.3 de iOS con capacidades de geolocalización.

19. iOS 2.x se distribuyó con el iPhone 3G en julio de 2008 y fue la primera versión que disponía de acceso a la App Store y soporte inicial empresarial (compatibilidad con Microsoft Exchange, eliminación de datos remota (*wipe*), y visor de documentos ofimáticos).

20. iOS 3.x se publicó en junio de 2009 (junto al iPhone 3GS), la versión 4.x de iOS se publicó en junio de 2010 (junto al iPhone 4), la versión 5.x de iOS se distribuyó en octubre de 2011 (junto al iPhone 4S), la versión 6.x de iOS se distribuyó en septiembre de 2012 (junto al iPhone 5) y la versión 7.x de iOS se distribuyó en septiembre de 2013 (junto al iPhone 5S y 5C).

21. La versión iOS 7.1.2 fue la última que proporcionaba soporte para el iPhone 4, no estando soportado en la futura versión de iOS 8[3].

22. Los detalles de las versiones de iOS soportadas en cada una de las generaciones de iPhone están disponibles en el apartado "5.1. Actualización del sistema operativo: iOS".

[2] https://en.wikipedia.org/wiki/IOS_version_history

[3] https://www.apple.com/ios/ios8/

23. Uno de los elementos clave para la interacción y gestión de dispositivos móviles basados en iOS recae en el software iTunes para ordenadores de escritorio o portátiles, disponible tanto para OS X como para Windows. Habitualmente, la publicación de una nueva versión de iOS conlleva adicionalmente la publicación de una nueva versión de iTunes, que hace uso de la nueva funcionalidad disponible en iOS.

24. Las primeras generaciones de iPhone (dispositivos móviles iOS) requerían disponer de la versión 7.3 o posterior de iTunes, mientras que iOS 3.x requería iTunes 8.2, la versión 3.1 de iOS estaba asociada a iTunes 9.0, la versión 4.x necesitaba iTunes 9.2 (iPhone 4), y la versión 5.x de iOS requería iTunes 10.5 (iPhone 4S). Posteriormente, la versión 6.x de iOS requería iTunes 10.7 (iPhone 5) y la versión 7.x de iOS estaba asociada a iTunes 11.1 (iPhone 5S y 5C)[4].

25. Los contenidos de esta guía aplican a dispositivos móviles iPhone configurados con el idioma español: "Español". El idioma puede ser seleccionado desde el menú "Ajustes - General - Internacional - Idioma".

26. La guía ha sido probada y verificada (inicialmente) con la versión 7.1.2 del sistema operativo iOS de Apple en un dispositivo iPhone 4S.

Nota: La información general del dispositivo móvil está disponible bajo la opción "Ajustes - General - Información", y en concreto, la información de la versión del sistema operativo se encuentra bajo la categoría "Versión", por ejemplo, 7.1.2 (11D257).

27. Las operaciones que requieren del uso de un ordenador han sido llevadas a cabo mediante OS X Mountain Lion 10.8.5 en inglés, empleando iTunes versión 11.3, y Windows 7 64-bits con iTunes 11.3.

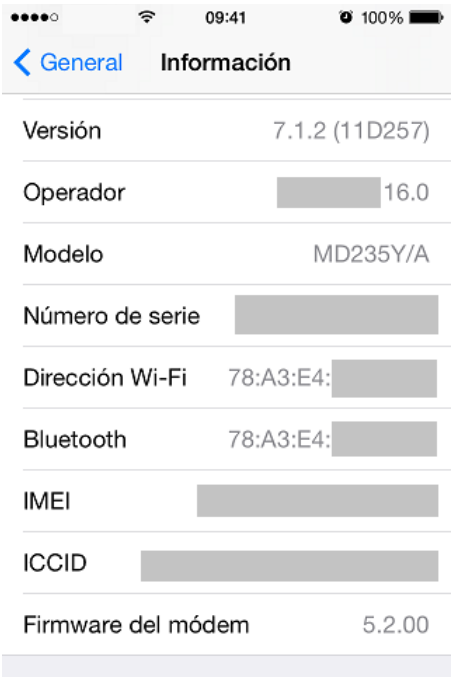
Nota: Para la elaboración de la guía se ha empleado la versión de OS X y Windows 7 en inglés en el ordenador utilizado para la sincronización con el dispositivo móvil, con el objetivo de ejemplificar la compatibilidad de idiomas entre el terminal y el ordenador. La simplicidad de las funciones realizadas 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.

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

    - Dispositivo móvil iPhone 4S 16GB fabricado por Apple (ver imagen inferior) [Ref.- 2]:
        - Versión de iOS: 7.1.2 (tras actualizaciones)
        - Versión de operador: *Carrier* 16.0
        - Modelo: MD235Y/A
        - Versión del firmware del módem: 5.2.00

[4] https://en.wikipedia.org/wiki/ITunes_version_history



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

Nota: Las imágenes incluidas en la presente guía pertenecen principalmente a la versión 7.1.2 de iOS, aunque algunas imágenes pueden corresponder a versiones previas de iOS 7.x. Apple introdujo cambios significativos en el interfaz de usuario en la versión 7.1 de iOS, por lo que algunas capturas de pantalla pueden no ser exactamente iguales entre las versiones 7.1.x y 7.0.x de iOS.

Nota: La guía ha sido diseñada (y aplicada) para dispositivos móviles estándar basados en iOS (iPhone e iPad) en los que no se ha llevado a cabo el proceso de *jailbreak*. Este proceso permite al usuario disponer de control completo sobre el dispositivo móvil y acceder al mismo como "root", o usuario privilegiado, y en concreto, al subsistema Unix subyacente en iOS (basado en Darwin BSD disponible en OS X), eliminando así los controles y/o restricciones establecidos por la plataforma iOS estándar y su fabricante (Apple).

Este proceso permite la instalación de aplicaciones, modificaciones y componentes del sistema no proporcionados a través de la tienda oficial de aplicaciones de Apple, denominada App Store [Ref.- 4]. A diferencia de otras plataformas móviles como Android, en el caso de iOS, este proceso es necesario si el usuario desea ejecutar software no autorizado por Apple, aplicaciones de terceros no oficiales, es decir, no distribuidas a través de la App Store y, por tanto, código no firmado [Ref.- 30].

El proceso de *jailbreak* (que difiere en dispositivos móviles iOS con chip A4, como iPhone 4 e iPad, y dispositivos móviles basados en el chip A5, como iPhone 4S e iPad2, o A5X del iPad de 3ª generación, o versiones posteriores del SoC, System-on-a-Chip, de Apple) permite, además de instalar aplicaciones de terceros, realizar modificaciones y añadir extensiones al

sistema operativo y el sistema de ficheros de iOS, habitualmente a través del cliente de instalación de *software* Cydia (http://cydia.saurik.com). El proceso de *jailbreak* es utilizado por usuarios avanzados para acceder a estas funcionalidades de bajo nivel, pudiendo aplicar correcciones, modificar el interfaz de usuario con nuevas capacidades, y proporcionar acceso al sistema de ficheros y al interfaz de línea de comandos (*shell*).

El proceso de *jailbreak* se lleva a cabo a través de la explotación de vulnerabilidades en el hardware, iOS o alguna de las aplicaciones asociadas. En función del tipo de vulnerabilidad explotada el *jailbreak* permite modificar el entorno de usuario o incluso el proceso de arranque (*boot*) del dispositivo móvil. Por otro lado, en la actualidad existen dos tipos de *jailbreak* en función de los requisitos necesarios para hacer uso del mismo: *tethered* o *untethered*. El primero de ellos, *tethered*, requiere conectar el dispositivo móvil a un ordenador durante su arranque, ya que el *jailbreak* hace uso de código disponible en el ordenador para permitir el arranque y evitar la detección de software no firmado en el terminal. El segundo, *untethered*, es independiente y no requiere conectar el dispositivo móvil a un ordenador durante el arranque, ya que el *jailbreak* modifica el código binario que comprueba y bloquea la existencia de código no firmado.

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

Las particularidades del proceso de actualizaciones en iOS (ver apartado "5.1. Actualización del sistema operativo: iOS"), en algunos casos con relativamente largos periodos de tiempo hasta que una nueva actualización está disponible para los usuarios finales, es uno de los motivos que incentiva a algunos usuarios a realizar el proceso de *jailbreak* para así poder instalar la última versión de ciertos componentes o software en su dispositivo móvil.

Un proceso asociado al *jailbreak*, pero diferente, es el proceso de *unlock* o desbloqueo, que permite al usuario liberar el componente de radio o banda base (*baseband*) del iPhone para poder hacer uso del dispositivo móvil con cualquier operador de telefonía móvil, es decir, utilizando cualquier tarjeta SIM. Este proceso era necesario en las versiones iniciales de iPhone si se quería disponer de libertad para elegir el operador, ya que el modelo de negocio de Apple restringía el uso de iPhone a ciertos operadores de telefonía móvil. El modelo de negocio actual de Apple permite adquirir el iPhone libre, es decir, sin vinculación a un operador de telefonía móvil, no siendo necesario llevar a cabo el proceso de *unlock* por este motivo. Esta funcionalidad aplica a dispositivos móviles iPad con capacidades 2/3/4G/4G.

29. La versión 7.1.2 de iOS empleada en los dispositivos móviles iPhone estuvo disponible desde el 30 de junio de 2014 [Ref.- 142], con notables mejoras de seguridad [Ref.- 143]. La versión previa 7.1.1 de iOS estuvo disponible desde el 22 de abril de 2014 [Ref.- 129].
30. 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.
31. Debe prestarse atención al contrato de telefonía, y en concreto de voz y datos, asociado a la tarjeta SIM (*Subscriber Identity Module*) empleada en el dispositivo móvil iOS.
32. 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 iOS y los diferentes servicios de Apple o de terceros.

4.1 IOS 7

33. iOS 7 [Ref.- 141] introdujo diferencias muy significativas en el diseño, el interfaz de usuario, la disponibilidad de nuevos gestos, las prestaciones generales y en el aspecto visual (iconos, tipos de letra, transiciones, menús, fondo de pantalla, etc) de los dispositivos móviles de Apple respecto a versiones anteriores de iOS, como las versiones 5.x o 6.x:

34. Asimismo, iOS 7 mejora las capacidades multitarea de la plataforma (accesibles mediante una doble pulsación del botón *Home*), optimizaciones en el consumo de batería, incorpora el Centro de Control (accesible al desplazar hacia arriba la parte inferior de la pantalla de iOS), actualiza el Centro de Notificaciones (accesible al desplazar hacia abajo la parte superior de la pantalla de iOS) con una vista diaria, promovió el lanzamiento de iTunes Radio (en USA sólo), la actualización automática de apps, etc.

35. Adicionalmente, iOS7 proporciona nuevas capacidades MDM a nivel empresarial para la gestión tanto de los dispositivos móviles, como de algunas de sus innovadoras capacidades y de los contenidos que estos dispositivos gestionan, así como cientos de nuevas librerías (APIs) para el desarrollo de nuevas apps.

36. Los dispositivos móviles de Apple disponen de otras capacidades más avanzadas en base a la integración entre iOS y el hardware, en concreto, de los últimos modelos como el iPhone 5S y su coprocesador de movimiento M7. Este coprocesador se utiliza en apps como "Mapas" para modificar automáticamente las indicaciones en función de si vamos a

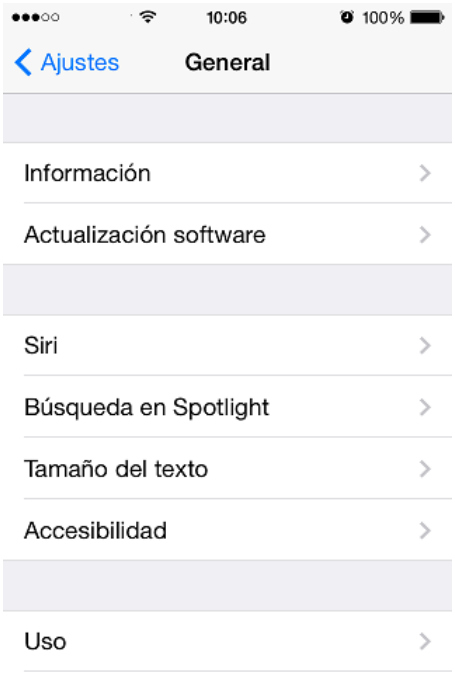
pie o en un vehículo, desactivar la búsqueda de redes Wi-Fi cuando vamos en un vehículo en movimiento, o reducir el consumo del dispositivo mientras dormimos.

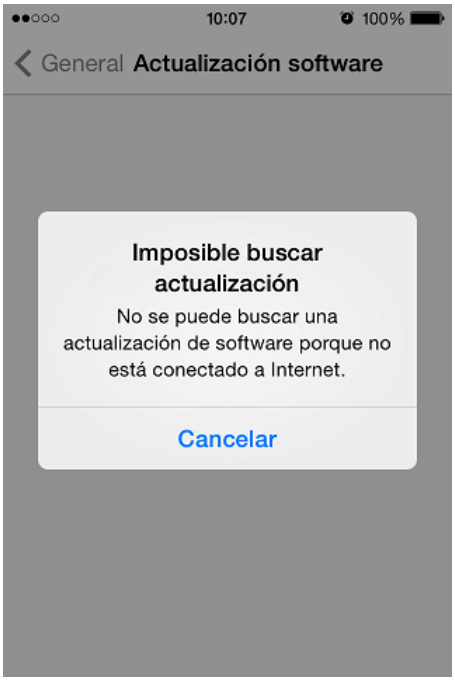
5 CONFIGURACIÓN DE SEGURIDAD DE IPHONE

5.1 ACTUALIZACIÓN DEL SISTEMA OPERATIVO: IOS

37. Los dispositivos móviles iOS, si disponen de conectividad de datos hacia Internet a través de las redes de telefonía móvil (2/3/4G) o de redes Wi-Fi, pueden verificar si existe una nueva versión o actualización del sistema operativo.

38. La opción para llevar a cabo la verificación de la existencia de actualizaciones de iOS está disponible a través del menú "Ajustes - General - Actualización de software", si se dispone de conectividad de datos (en caso contrario se generará un mensaje de error):

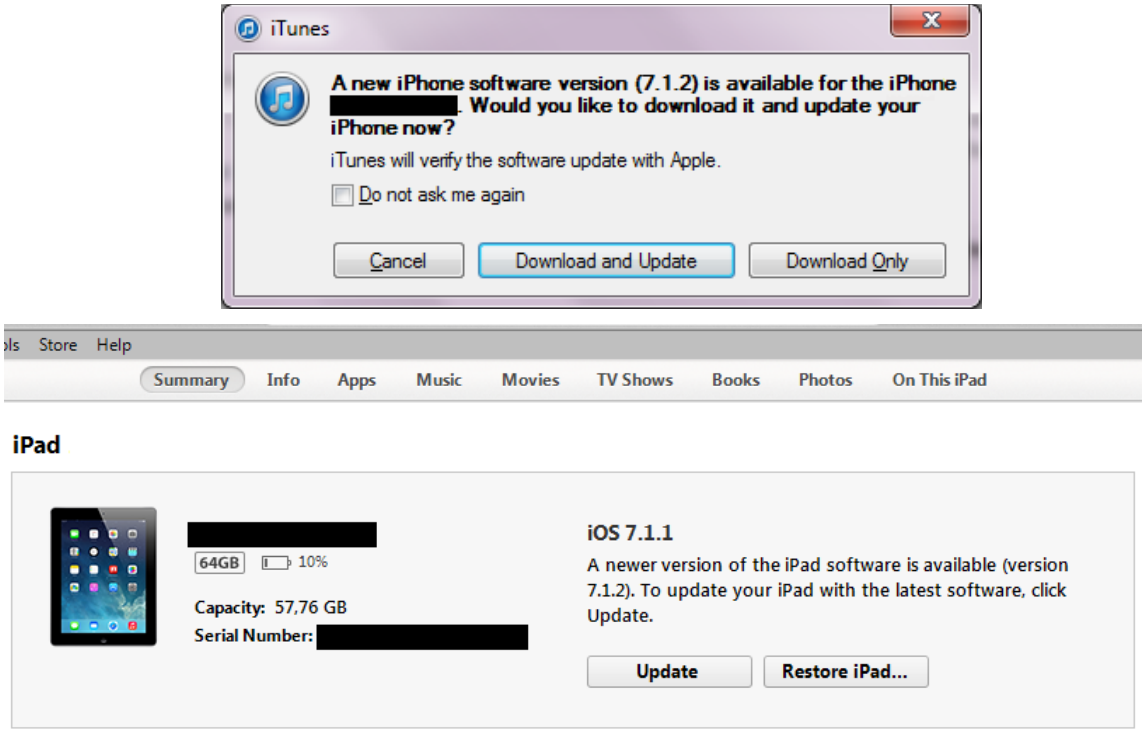




39. Esta funcionalidad, referenciada en ocasiones como actualizaciones OTA (Over-the-Air), está disponible en los dispositivos móviles de Apple únicamente desde la versión 5.0 de iOS, siendo necesario en versiones previas de iOS verificar si existen nuevas versiones del sistema operativo a través del software de ordenador iTunes.

40. En el caso de emplearse iTunes para el proceso de actualización del dispositivo móvil en versiones de iOS previas, es necesario conectar el terminal al ordenador mediante un cable USB para poder llevar a cabo la comprobación e instalación de la nueva versión de iOS.

41. En el caso de disponerse de una nueva versión de iOS, iTunes lo indicará a través de un mensaje que informa de la existencia de la nueva versión, y posteriormente, a través de la pantalla principal asociada al dispositivo móvil en iTunes (ejemplo de iTunes con iPad 3 64GB en iOS 7.1.1 y actualización disponible a iOS 7.1.2):



42. El proceso de actualización empleado también determina el tamaño de las actualizaciones a descargar. En caso de emplearse iTunes se descargará la imagen completa de iOS, que tiene un tamaño de unos 1,2 GB para la versión 7.1.2 de iOS completa para el iPhone 4S (el tamaño de la imagen es aproximado, ya que el mismo varía según el tipo de dispositivo móvil iOS objetivo, por ejemplo, iPhone 4S frente a iPad 3, y también depende de la versión de iOS previa desde la que se lleve a cabo la actualización).

43. En caso de emplearse el dispositivo móvil directamente para llevar a cabo la actualización, se descargará únicamente el fichero correspondiente a la actualización, de mucho menor tamaño, por ejemplo 23 MB, correspondientes solamente a los cambios de la versión 7.1.1 a la 7.1.2 para el iPhone 4S (de nuevo, valores aproximados).

44. La información detallada de cada una de las actualizaciones y descargas disponibles para iOS (incluyendo el tamaño de las mismas) es publicada por Apple en un fichero PLIST en formato XML a través del servidor "http://mesu.apple.com". Este fichero puede ser analizado en detalle mediante la herramienta iCamasu [Ref.- 144].

45. Tanto si la imagen obtenida es completa como si es parcial, todos los datos y configuración del usuario son conservados a través del proceso de backup (o copia de seguridad) disponible mediante iTunes.

46. 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, especialmente si la actualización se realiza directamente desde el dispositivo móvil a través de Wi-Fi sin emplear iTunes.

47. Por otro lado, es importante considerar que ciertos ajustes y estados del dispositivo son restaurados a un valor de fábrica o valor por defecto tras la actualización, independientemente del (y potencialmente diferente al) estado que tenía el dispositivo móvil previamente. Un ejemplo afectado por esta situación a lo largo de diferentes versiones de iOS (incluyendo iOS 7.1.2) es el interfaz de Bluetooth, que siempre aparece

como activo tras llevar a cabo la actualización a una nueva versión de iOS, incluso aunque previamente el interfaz Bluetooth se encontrase en un estado inactivo o apagado.

48. A partir de la versión 5.x de iOS es posible realizar actualizaciones y llevar a cabo la sincronización de datos entre el dispositivo móvil iOS e iTunes (versión 10.5 o superior) empleando una red inalámbrica Wi-Fi, no siendo por tanto imprescindible establecer una conexión física entre ambos dispositivos a través de un cable USB.

49. La funcionalidad para obtener actualizaciones de iOS a través de Wi-Fi (o 2/3/4G) desde el menú "Ajustes - General - Actualización de software" está disponible directamente, sin necesidad de acciones adicionales.

50. La funcionalidad de sincronización de datos con iTunes está disponible desde el menú "Ajustes – General – Sincronizar con iTunes vía Wi-Fi", debiendo haberse habilitado previamente desde iTunes (ver apartado "5.21. Sincronización de datos en iOS").

51. Sin embargo, la sincronización con iTunes a través de una red Wi-Fi no permite llevar a cabo actualizaciones de la versión de iOS en el dispositivo móvil desde el propio iTunes, siendo necesario establecer una conexión por USB para llevar a cabo esta operación mediante iTunes (ejemplo con iOS 5.0.1):

52. iOS también verifica de forma periódica y automática si se dispone de una actualización de software. Para verificar la existencia de una actualización, iOS se conecta al servidor "mesu.apple.com" en el puerto 80/tcp mediante HTTP (conexión no cifrada) y, empleando el método HTTP GET[5], verifica la fecha de modificación del fichero que contiene las versiones de iOS disponibles para actualizaciones OTA:

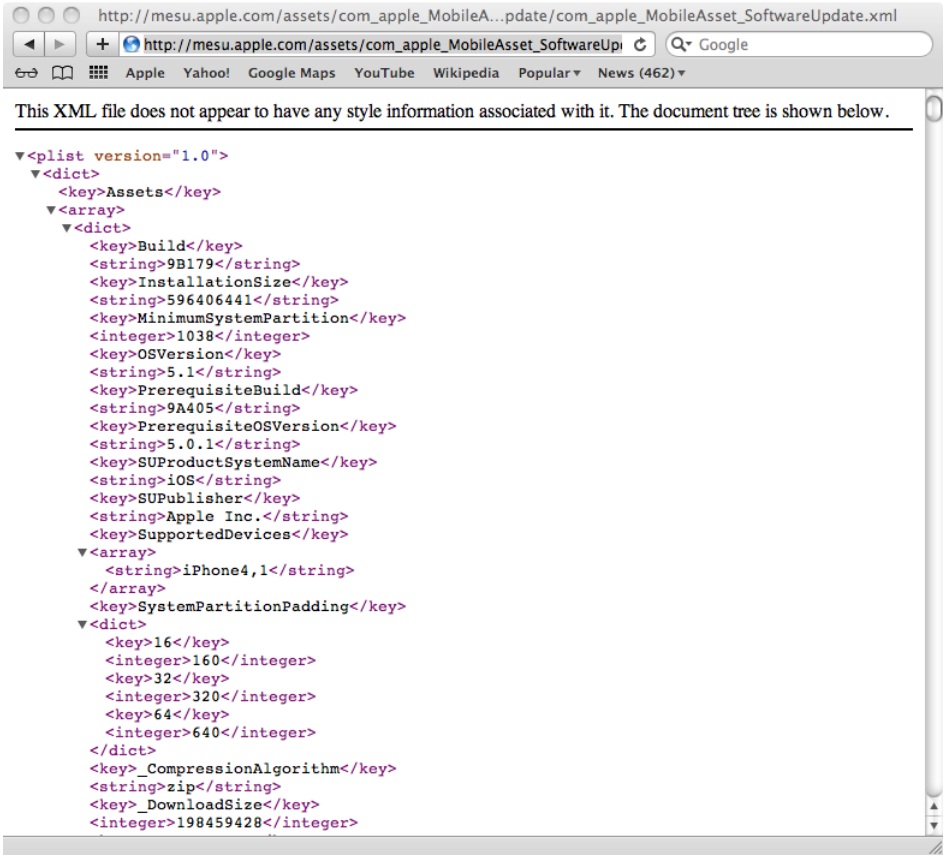
```
/assets/com_apple_MobileAsset_SoftwareUpdate/com_apple_MobileAsset_Software
Update.xml
```

53. El agente de usuario (User-Agent) HTTP empleado por iOS 7.x para identificarse es:

[5] Versiones previas de iOS, como 5.x, hacían uso también del método http HEAD durante el proceso de verificación de actualizaciones.

```
User-Agent: MobileAsset/1.1
```

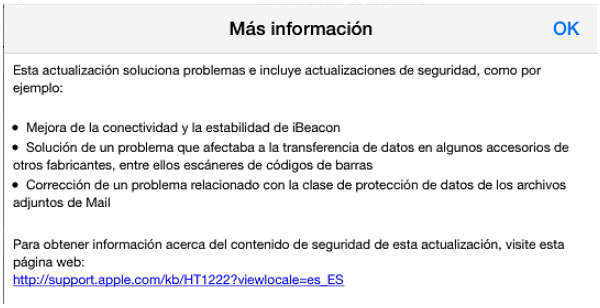
54. Si la fecha del fichero es posterior a la del último fichero disponible en el dispositivo móvil, la respuesta recibida incluye las versiones de iOS disponibles para cada tipo de dispositivo de Apple (iPhone, iPad, iPod…) clasificadas en función de la versión de iOS actualmente instalada, el tamaño de la descarga (fichero comprimido) y de la actualización, y el enlace o URL al fichero de actualización (con extensión .zip):



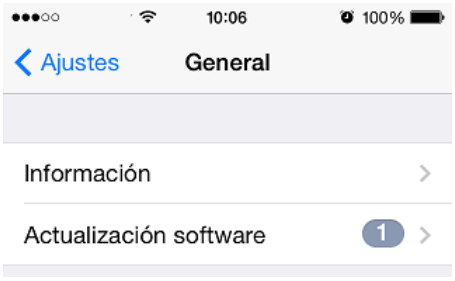
55. El fichero incluye una firma digital en su parte inferior para conservar su autenticidad e integridad (secciones “<key>Certificate</key>” y “<key>Signature</key>”).

56. El proceso de comprobación de disponibilidad de actualizaciones de iOS es similar tanto si se realiza manualmente por el usuario, como si el dispositivo verifica la existencia de una nueva versión automáticamente, en cuyo caso mostrará una notificación asociada (ejemplo de iPad):

57. Si existe una versión disponible, como por ejemplo la actualización a iOS 7.1.2 desde la versión empleada como referencia inicial en la presente guía, iOS 7.1.1, el dispositivo móvil mostrará su disponibilidad y su tamaño, siendo posible obtener los detalles de la actualización a través del botón “Más información”:

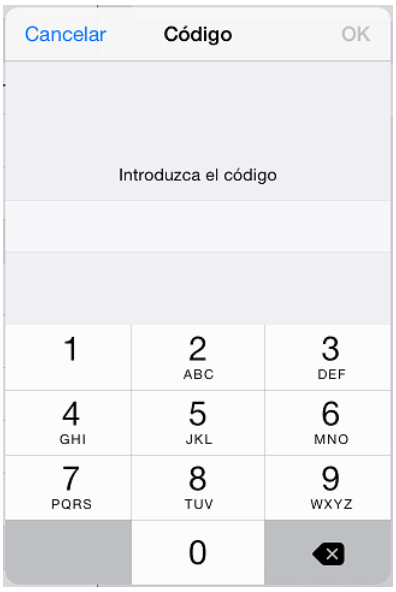


58. Asimismo, si se dispone de una actualización, el dispositivo móvil mostrará en el icono de Ajustes un mensaje indicando que hay una actualización disponible, al igual que en la sección "Ajustes – General":



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

60. Desde la versión 7.1 de iOS, para poder proceder a actualizar el dispositivo móvil vía OTA es necesario introducir el código de acceso (antes incluso de comenzar con la descarga de la actualización para la nueva versión de iOS), al tratarse de una operación administrativa crítica. Adicionalmente, es necesario aceptar los términos y condiciones del software de iOS para proceder a la descarga, instalación y posterior reinicio del dispositivo móvil:



61. Para llevar a cabo la actualización, se establece una conexión HTTP no cifrada con el servidor "appldnld.apple.com" en el puerto 80/tcp mediante el método GET, y si el fichero disponible (en función de su fecha) no ha sido ya descargado, se solicita el fichero indicado en el fichero XML de actualizaciones analizado previamente (a través del método GET HTTP). Por ejemplo:

    - iPhone 4S – iOS 7.1.2 desde la versión 6.0 de iOS:

      ```
      http://appldnld.apple.com/iOS7.1/031-5038.20140630.rHUfi/com_apple_MobileAsset_SoftwareUpdate/ff47fd9537be1993095f5e25295411a8132fc794.zip
      ```

62. El agente de usuario (User-Agent) HTTP empleado por iOS para identificarse a la hora de descargar el nuevo firmware, en función del dispositivo móvil y sus características, es (ejemplo de iPhone 4S con iOS 7.1.1):

```
User-Agent: itunesstored/1.0 iOS/7.1.1 model/iPhone4,1 build/11D202 (6; dt:75)
```

63. Teóricamente, la integridad de las actualizaciones de las nuevas versiones de iOS se verifica a través de una firma digital asociada al fichero de actualización (.zip) descargado, pero la ausencia de cifrado HTTPS podría (teóricamente) abrir la puerta a la manipulación de este intercambio de datos, por ejemplo, mediante la sustitución de la versión entre actualizaciones válidas firmadas digitalmente.

64. 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.

65. El proceso de actualización OTA de iOS desde su introducción en iOS 5.x hasta iOS 7.x inclusive ha sido vulnerable a ataques de manipulación MitM (Man-in-the-Middle), siendo posible para un potencial atacante congelar el dispositivo móvil en su versión de iOS actual. Como resultado, sería posible explotar sobre el dispositivo móvil víctima todas las vulnerabilidades presentes y futuras asociadas a nuevas versiones de iOS (iguales o posteriores a la existente actualmente en el dispositivo) [Ref.- 147].

66. En el caso de iTunes, la verificación de nuevas versiones se lleva a cabo a través de la siguiente URL (primera URL), que proporciona una redirección hacia la lista más actualizada de software de Apple (segunda URL), con las versiones completas de iOS:

```
http://itunes.com/version

(ó http://phobos.apple.com/version, ó https://s.mzstatic.com/version)

http://ax.phobos.apple.com.edgesuite.net/WebObjects/MZStore.woa/wa/com.apple.jingle.appserver.client.MZITunesClientCheck/version/
```

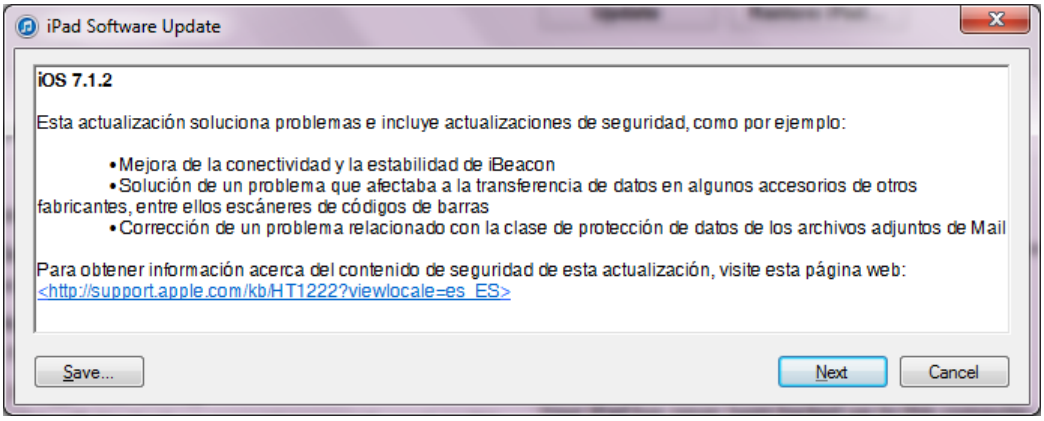
67. En iTunes, tras aceptar el fichero con las novedades de la nueva versión (fichero con extensión ".ipd", *iPhone Documentation*, ver imagen inferior) y los términos y condiciones asociados, la descarga se realiza desde el mismo servidor web, "appldnld.apple.com" en el puerto 80/tcp, pero a través de una ubicación y fichero diferentes (con extensión ".ipsw", *iPhone Software*). Ejemplo:

- iPhone 4S – iOS 7.1.2:

  `http://appldnld.apple.com/iOS7.1/031-4816.20140627.XQbdQ/iPhone4,1_7.1.2_11D257_Restore.ipsw`

  `http://appldnld.apple.com/iOS7.1/031-03364.20140630.VbEDT/iPhoneiTunesUpdateReadMe_7.1.ipd`

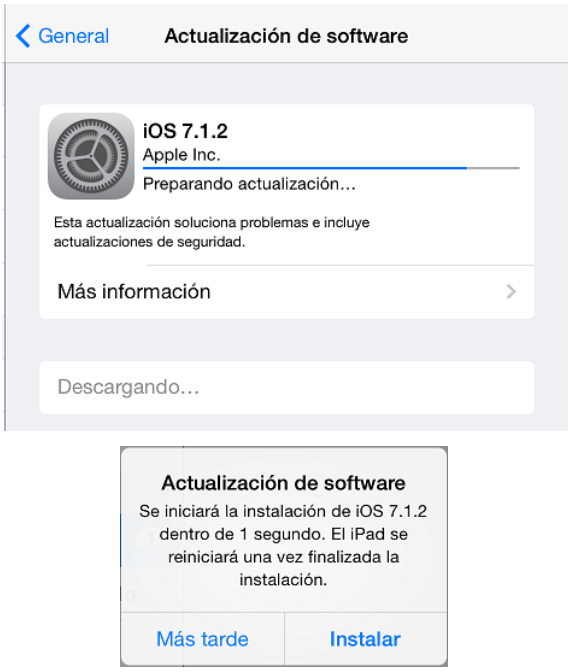
68. El fichero es descargado a la siguiente carpeta, dentro del directorio principal del usuario empleado en OS X: "/Users/<usuario>/Library/iTunes/iPhone Software Updates" para el iPhone, o "iPad Software Updates" en el caso del iPad.



69. Lógicamente, el agente de usuario (User-Agent) HTTP empleado por iTunes para identificarse es diferente al empleado por el dispositivo móvil, y varía entre OS X y Windows:

```
User-Agent: iTunes/11.3 (Macintosh; Intel Mac OS X 10.8.5) AppleWebKit/...
User-Agent: iTunes/11.3 (Windows; Microsoft Windows 7 x64 ... (Build ...))
```

70. Una vez descargada la actualización desde el propio dispositivo móvil (y no desde iTunes), iOS muestra al usuario una notificación de que la nueva versión será instalada en el dispositivo móvil en unos segundos, siendo posible cancelar y posponer su instalación mediante el botón "Más tarde" (ejemplo de iPad):



71. En iOS, si la pantalla de actualización no se encuentra en primer plano o si el usuario desea realizar la instalación posteriormente (mediante el botón "Más tarde" de la imagen previa), es posible llevar a cabo únicamente la descarga de la nueva versión de iOS, y proceder a su instalación en el futuro. Desde la misma pantalla de las actualizaciones de software, se indica que la actualización ya ha sido descargada previamente con el texto "Descargado" bajo el número de versión y con el botón "Instalar ahora", en lugar de "Descargar e instalar":

72. La información detallada de las actualizaciones de seguridad que han sido publicadas por Apple para sus diferentes productos desde enero de 2011, incluyendo las asociadas al iOS del iPhone e iPad, están disponibles en la página web "*Apple Security Updates*" [Ref.- 8].

73. Las actualizaciones correspondientes al año 2010 están disponibles en su propia página web independiente [Ref.- 9], al igual que las correspondientes al periodo entre los años 2008 y 2009 [Ref.- 10], así como las de periodos previos [Ref.- 8] (referencias disponibles al final de dicho documento, y sólo aplicables para iPhone).

74. La política de actualizaciones de seguridad, así como el repositorio oficial de notificaciones con el listado de vulnerabilidades que han afectado a iOS, es gestionado exclusivamente por Apple, único fabricante del dispositivo móvil iPhone o iPad.

75. Por tanto, Apple es quién publicará únicamente actualizaciones para los dispositivos móviles iOS. 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 o no publicadas hasta la fecha.

76. El principal inconveniente de este modelo de actualizaciones de seguridad con una única fuente oficial es que es Apple quién establece cuando estará disponible una actualización, y pese a que se conozca públicamente la existencia de una vulnerabilidad, pueden darse retrasos significativos hasta que se dispone por parte los usuarios finales de una actualización de seguridad que solucione dicha vulnerabilidad, estando los dispositivos móviles desprotegidos durante todo ese tiempo (varias semanas e incluso meses en algunos casos, tal como se detalla a través de algunos ejemplos de la presente guía).

77. Adicionalmente, debe tenerse en cuenta que las soluciones publicadas para corregir vulnerabilidades de seguridad conocidas estarán disponibles únicamente para las últimas versiones de iOS, no existiendo un mecanismo establecido para proporcionar dichas soluciones para versiones previas de iOS que se consideran fuera de soporte y mantenimiento por Apple, por lo que estas versiones, y los dispositivos móviles basados en ellas, serán siempre vulnerables.

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

79. En el caso de disponer de un dispositivo móvil iOS (iPhone o iPad) para el que sí se dispone de una actualización a una versión superior de iOS, por ejemplo 7.x para un terminal basado en iOS 6.x, se recomienda aplicar la actualización sobre el dispositivo con el objetivo de instalar la última versión disponible y protegerlo de vulnerabilidades conocidas.

Nota: Debe tenerse en cuenta que Apple llevó a cabo un cambio muy significativo en la apariencia del interfaz de usuario en iOS 7.x, modificando completamente la usabilidad de los dispositivos móviles, iconos, y aspectos gráficos respecto a versiones anteriores, como iOS 6.x ó 5.x

80. Pese a que existen foros en Internet dónde se distribuyen modificaciones y personalizaciones del sistema operativo iOS (o partes de éste), asociados al proceso de *jailbreak* (como Dev-Team Blog, http://blog.iphone-dev.org), desde el punto de vista empresarial y de seguridad, en ningún caso se recomienda de forma generalizada la instalación o modificación del sistema operativo desde una fuente no oficial.

81. Con el objetivo de mantener el dispositivo móvil siempre actualizado, se recomienda comprobar periódicamente desde el propio dispositivo la disponibilidad de actualizaciones a través del menú “Ajustes - General - Actualización de software”:

82. Desde el punto de vista de seguridad es necesario actualizar igualmente todas las aplicaciones (cliente) instaladas sobre el sistema operativo (ver apartado "5.28. Actualización de aplicaciones (cliente) en iOS").

83. Una de las principales limitaciones asociadas a la actualización de dispositivos móviles basados en iOS se debe a las restricciones comerciales impuestas por Apple respecto a los modelos de dispositivos para los que estará disponible cada versión del sistema operativo.

84. Así por ejemplo, la versión de iOS empleada como referencia para la elaboración de la versión previa de la presente guía, 5.x, y en concreto la última actualización asociada 5.1.1 [Ref.- 5], sólo estaba disponible para los siguientes modelos hardware de dispositivos: iPhone 4S, iPhone 4, iPhone 3GS, iPad 2, iPad, iPod Touch (4ª generación) y iPod Touch (3ª generación).

85. Por otro lado, la versión iOS 7.x, empleada como referencia para la elaboración de la presente guía, y en concreto la actualización asociada 7.1.2 [Ref.- 142], sólo estaba disponible para los siguientes modelos hardware de dispositivos: iPhone 4 o posterior, iPad 2 o posterior, iPad mini, e iPod Touch (5ª generación).

86. El resto de dispositivos móviles asociados, como por ejemplo iPhone 3GS o inferiores, iPad o iPod Touch en sus generaciones previas (de la primera a la cuarta), nunca podrán disponer de las correcciones de seguridad y vulnerabilidades solucionadas por las nuevas versiones de iOS, como por ejemplo, las mejoras de seguridad de la actualización 6.0 [Ref.- 129] (que soluciona 197 vulnerabilidades), 7.0 [Ref.- 130] (que soluciona 80 vulnerabilidades) o 7.1 [Ref.- 145] (que soluciona 41 vulnerabilidades).

87. Igualmente, no todos los contenidos y funcionalidades de la versión 3.x de iOS estaban disponibles en la generación inicial de iPhone (iPhone 2G), ocurriendo algo similar con las funcionalidades de iOS 4.x y el iPhone 3G.

88. La versión 4.x de iOS no dispone de soporte para el iPhone 2G, siendo la versión iOS 3.1.3 la última disponible para este dispositivo móvil.

89. De forma similar, la versión 5.x de iOS no dispone de soporte para el iPhone 3G (o modelos anteriores), siendo la versión iOS 4.2.1 la última versión disponible para este dispositivo móvil.

90. La versión 6.x de iOS no dispone de soporte para el iPad original o de primera generación, siendo la versión iOS 5.1.1 la última versión disponible para este dispositivo móvil [Ref.- 7].

91. La versión 7.x de iOS no dispone de soporte para el iPhone 3GS (o modelos anteriores), siendo la versión iOS 6.1.6 la última versión disponible para este dispositivo móvil.

92. Excepcionalmente, y estando ya fuera del periodo de soporte (es importante considerar que la última actualización de seguridad de iOS 6.x se publicó en marzo de 2013, con la

versión 6.1.3), Apple publicó en febrero de 2014 una actualización para el iPhone 3GS, en concreto la versión 6.1.6 de iOS, con el objetivo de solucionar la vulnerabilidad de HTTPS conocida como "goto fail" y que permitía la aceptación de certificados digitales inválidos como de confianza por parte del dispositivo móvil [Ref.- 131].

93. Debe tenerse por tanto en cuenta que un dispositivo móvil iOS (iPhone o iPad), tras aproximadamente tres años desde su comercialización, deja de estar soportado por Apple y no dispondrá de actualizaciones para las nuevas versiones de iOS, por lo que las vulnerabilidades de seguridad conocidas y existentes en el dispositivo nunca serán solucionadas, con el impacto asociado que esto conlleva en caso de no desecharse el terminal y sustituirlo por un nuevo modelo. Más información en la iOS Support Matrix [Ref.- 96].

94. La importancia de aplicar las últimas actualizaciones de seguridad disponibles se ve también reflejada en el proceso que permite tomar control completo de un dispositivo móvil, denominado *jailbreak* (y descrito previamente) en el caso de iPhone e iPad.

95. La versión de JailbreakMe publicada en agosto de 2010 [Ref.- 46], denominada Star y creada por comex, empleaba una vulnerabilidad en el procesamiento de las fuentes de ficheros PDF, junto a una vulnerabilidad del kernel de iOS (iOSurface) y una debilidad en el proceso de verificación de código firmado.

96. La versión de JailbreakMe 3 publicada en julio de 2011 [Ref.- 42] hacía uso de dos vulnerabilidades, de nuevo en la gestión de las fuentes de ficheros PDF (CVE-2011-0226) y en el kernel de iOS (CVE-2011-0227). Las mismas vulnerabilidades empleadas en este proceso podrían ser utilizadas con fines maliciosos de forma no autorizada para tomar control de los dispositivos de millones de usuarios.

97. Paradójicamente, en este caso concreto, durante el periodo desde la publicación de la vulnerabilidad hasta que Apple publicó la actualización que solucionaba la misma (iOS 4.3.4 [Ref.- 43]), los usuarios que habían realizado el proceso de *jailbreak* estaban protegidos frente a ésta, y no así el resto de usuarios, ya que el proceso solucionaba la misma mediante un parche no oficial denominado PDF Patch 2 [Ref.- 43]:

98. La versión de evasi0n (o evasi0n6) que permitía realizar el proceso de *jailbreak* en iOS 6.x y que fue publicada en febrero de 2013 [Ref.- 146] hacía uso de seis vulnerabilidades y exploits diferentes, reflejando la complejidad actual de este proceso para disponer de control completo del dispositivo móvil iOS. Apple solucionó cuatro de las seis vulnerabilidades con la versión 6.1.3 de iOS en marzo de 2013.

99. La versión de evasi0n7 que permitía realizar el proceso de *jailbreak* en iOS 7.x y que fue publicada inicialmente en diciembre de 2013 [Ref.- 146] hacía uso de cuatro vulnerabilidades y exploits diferentes, reflejando de nuevo la complejidad actual de este proceso para disponer de control completo del dispositivo móvil iOS. Apple solucionó las cuatro vulnerabilidades a lo largo de las múltiples betas de la versión 7.1 de iOS, y finalmente en la versión 7.1 oficial de marzo de 2014.

Nota: A lo largo del tiempo y de las diferentes versiones de iOS y generaciones de dispositivos móviles de Apple se han empleado numerosos exploits que se aprovechaban de diferentes vulnerabilidades de iOS para poder tomar control completo del dispositivo y realizar el proceso de *jailbreak*: http://theiphonewiki.com/wiki/index.php?title=Jailbreak.

5.2 MODELO Y ARQUITECTURA DE SEGURIDAD DE IOS

100. El modelo o arquitectura de seguridad de iOS está basado en el sistema operativo Unix, en concreto en Darwin BSD, heredado de OS X (previamente denominado Mac OS X).

101. La plataforma iOS está compuesta por diferentes componentes, incluyendo los gestores de arranque (*bootloaders*: BootROM, LLB (*Low-Level Bootloader*) e iBoot), el coprocesador criptográfico, el sistema operativo con el kernel [Ref.- 109] y sus extensiones, el software del sistema y las librerías compartidas, el sistema de ficheros con dos particiones HFS+, la de sistema y la de datos de usuario y aplicaciones, las aplicaciones existentes por defecto y las aplicaciones móviles instaladas por el usuario.

102. De manera general, iOS proporciona mecanismos de protección en cuatro áreas diferenciadas [Ref.- 13]: seguridad del propio dispositivo, seguridad de los datos que almacena y de los datos que son enviados a través de las redes de comunicaciones, y seguridad de las aplicaciones.

103. La integridad del proceso de arranque de iOS está protegida frente a posibles manipulaciones, y sólo permite la utilización de iOS en dispositivos móviles validados por Apple, mediante la utilización de componentes que han sido firmados digitalmente por Apple. Cada componente involucrado en el arranque verifica la cadena de confianza del paso previo antes de su ejecución, es decir, comprueba que el código ejecutado previamente ha sido también firmado por Apple.

104. El proceso de arranque seguro, junto a la firma de código, intentan asegurar que los dispositivos móviles basados en iOS sólo ejecutan código y apps de confianza.

105. Al arrancar el dispositivo, el procesador ejecuta código de una memoria de sólo lectura grabada en el proceso de fabricación del dispositivo conocida como BootROM [Ref.- 13].

106. Esta memoria de arranque (BootROM) dispone de un certificado raíz de Apple, que es empleado para verificar la integridad del LLB (*Low-Level Bootloader*) y comprobar que su código también ha sido firmado por Apple. Igualmente, el LLB verifica y ejecuta el siguiente componente, el iBoot, el cual lleva a cabo el mismo proceso hasta ejecutar el kernel de iOS.

107. Los dispositivos móviles de Apple basados en el chip (o SoC) A7 de Apple, como por ejemplo el iPhone 5S, iPad Air o iPad mini [Ref.- 96], disponen adicionalmente de un proceso de arranque que verifica que el software que ejecutará en el coprocesador criptográfico denominado *Secure Enclave* (ver apartado "5.2.2. Security Enclave"), también ha sido firmado por Apple [Ref.- 13].

108. Los dispositivos con capacidades de telefonía móvil, o celular, llevan a cabo un proceso de verificación similar antes de ejecutar el subsistema de banda base que gobierna el módulo de radio para las tecnologías 2/3/4G.

109. Si las verificaciones realizadas durante el proceso de arranque de iOS fallan, se dispone de dos opciones: el modo DFU (*Device Firmware Upgrade*), disponible si el BootROM no puede cargar o verificar la integridad del LLB, y el modo de recuperación, disponible si falla la carga o verificación de cualquiera de los otros componentes, y que permite restaurar el dispositivo a los ajustes de fábrica [Ref.- 132].

110. La seguridad del dispositivo móvil pasa por la utilización de un código de acceso (PIN, contraseña, huella dactilar, etc) para evitar el acceso no autorizado al mismo, junto a políticas de seguridad más granulares para establecer restricciones en el código de acceso y su gestión.

111. De forma complementaria es posible establecer restricciones adicionales en el dispositivo móvil para definir qué aplicaciones y funcionalidades estarán disponibles para el usuario (ver apartado "5.3. Gestión empresarial de dispositivos basados en iOS").

112. La seguridad de los datos almacenados en el dispositivo móvil se basa en las capacidades de cifrado a nivel hardware de todos los datos del dispositivo mediante AES de 256 bits, funcionalidad que no puede ser deshabilitada por el usuario (ver apartado "5.7.1. Cifrado del dispositivo móvil").

113. De forma complementaria es posible hacer uso de las capacidades de protección de datos adicionales de iOS para cifrar los mensajes de correo electrónico y ficheros adjuntos, o los datos de las aplicaciones almacenados en el dispositivo móvil, cuando el dispositivo está bloqueado con un código de acceso (ver apartado “5.7.2. Cifrado de los datos de las aplicaciones”).

114. Adicionalmente las copias de seguridad realizadas a través de iTunes pueden ser cifradas, y se dispone de soporte de S/MIME para el cifrado de correos electrónicos y la posibilidad de restringir el reenvío o movimiento de mensajes entre cuentas de e-mail.

Nota: Un elemento fundamental a tener en cuenta en la protección de los datos almacenados en el dispositivo móvil iOS pasa por la protección de las copias de seguridad creadas a través de iTunes. Si un potencial atacante dispone de acceso al ordenador empleado para la sincronización mediante iTunes, podría acceder a la copia de seguridad que contiene la mayoría de los datos almacenados en el dispositivo móvil.

Se recomienda por tanto cifrar las copias de seguridad de iTunes con una contraseña suficientemente robusta que no sea fácilmente adivinable, debiéndose tener en cuenta que existe software comercial para intentar obtener dicha contraseña empleando ataques de diccionario y fuerza bruta.

En el caso de realizar las copias de seguridad a través de iCloud, opción disponible desde iOS 5.x, Apple protege los datos mediante cifrado, pero debe tenerse en cuenta que Apple dispone

de la contraseña maestra con la que se realiza este proceso de cifrado, pudiendo acceder a todos los datos en el caso de tener que responder a un requerimiento judicial [Ref.- 133].

115. Los datos enviados y recibidos desde el dispositivo móvil pueden ser protegidos mediante tecnologías VPN, incluyendo Cisco IPSec, L2TP/IPSec y PPTP, o mediante VPNs SSL a través de aplicaciones de terceros, como Juniper, Cisco o F5 (ver apartado "5.18.6. VPN").

116. iOS dispone de capacidades de autentificación mediante biometría, a través de Touch ID desde el iPhone 5S, certificados digitales X.509 y funcionalidad para integrarse con soluciones de autentificación de dos factores, como RSA SecurID o CRYPTOCard.

117. Asimismo, proporciona soporte para numerosos estándares de seguridad en redes Wi-Fi, como WEP, WPA, WPA2, tanto personal como empresarial, incluyendo múltiples métodos de autentificación basados en 802.1x y EAP (EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, PEAP v0 y v1, y LEAP), aunque algunos de ellos no pueden ser seleccionados directamente desde el interfaz de usuario (ver apartado "5.14. Comunicaciones Wi-Fi"), sino a través de perfiles de configuración.

118. Por otro lado, las comunicaciones de los servicios y aplicaciones para comunicaciones personales propietarias de Apple, como FaceTime o iMessage, son cifradas extremo a extremo, y emplean un identificador único asignado a cada usuario en función de su Apple ID [Ref.- 13].

119. Por último, la seguridad de las aplicaciones se proporciona mediante un entorno de ejecución restringido o *sandbox* (ver apartado "5.2.2. Sandbox de iOS de Apple"), de forma que una aplicación no pueda acceder a los datos de otra, o a los ficheros y recursos del sistema. La comunicación entre aplicaciones puede realizarse a través de las APIs o librerías que proporciona iOS para este propósito.

120. De forma complementaria, todas las aplicaciones deben haber sido firmadas, con el objetivo de asegurar que no han sido modificadas y que son de confianza (tras seguir el proceso de verificación y aprobación de Apple). Las aplicaciones de sistema proporcionadas con iOS por defecto han sido firmadas por Apple, mientras que las aplicaciones de terceros han sido firmadas por su desarrollador con un certificado emitido previamente por Apple a través del programa de desarrolladores de iOS.

121. iOS verifica en el momento de ejecución de un binario o aplicación que dispone de una firma y que su código ha sido firmado con una firma válida [Ref.- 44], empleándose el formato PKCS#7 para la firma de binarios de la App Store.

122. Si se desea hacer uso de aplicaciones empresariales privadas o propias es necesario utilizar un perfil de aprovisionamiento, que debe ser instalado en el dispositivo móvil para poder ejecutar la aplicación. Estos perfiles pueden ser instalados o revocados a través de las soluciones de gestión empresarial (MDM), para todos los dispositivos de una organización o para dispositivos específicos.

123. Adicionalmente al *sandbox* y a la firma de código, la versión 4 de iOS Apple incorporó otros mecanismos de seguridad al sistema operativo, complementando Data-Execution Protection (DEP), disponible desde la versión iOS 2.x, como Address-Space Layout Randomization (ASLR), técnicas que dificultan parcialmente el proceso de explotación de vulnerabilidades en iOS [Ref.- 110].

124. ASLR fue introducido en la versión 4.3 de iOS [Ref.- 44], aunque para hacer uso de sus mecanismos de protección las aplicaciones para iOS deben ser compiladas con soporte PIE, *Position Independent Executables*. El soporte para PIE está disponible en las aplicaciones incluidas en iOS, pero no en muchas aplicaciones de terceros.

125. Por otro lado iOS proporciona un entorno para el almacenamiento de las credenciales de acceso a aplicaciones y servicios en un repositorio cifrado, denominado *keychain*, y compartimentalizado por aplicación, para evitar que una aplicación acceda a las identidades y credenciales de otra.

126. Adicionalmente, las librerías de desarrollo proporcionan a los programadores de aplicaciones para iOS capacidades criptográficas para cifrar los datos almacenados por la aplicación mediante AES, RC4 o 3DES, incluyendo aceleración hardware para AES y SHA-1 (en iPhone y iPad). Estas capacidades complementan los mecanismos de protección de datos (mencionados previamente) cuando el dispositivo está bloqueado.

127. iOS 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 teóricamente las acciones que una aplicación puede realizar sobre otras aplicaciones, en el sistema o en su interacción con el usuario.

5.2.1 CONTROLES DE ACCESO Y PRIVACIDAD

128. La seguridad más granular de la plataforma se basa en un mecanismo muy básico de permisos que impone restricciones en las operaciones que un proceso (o aplicación) puede llevar a cabo sobre ciertos elementos.

129. Los elementos críticos de la plataforma que requieren de permisos para su acceso debido a que conllevan implicaciones desde el punto de vista de la privacidad del usuario son definidos por Apple y varían en función de la versión de iOS empleada.

130. Para ello, iOS solicita permiso al usuario a través de mensajes y ventanas gráficas (de diálogo) en el momento de hacer uso por primera vez de las funciones (de la API) que requieren acceso a ciertos componentes, como por ejemplo la información de localización (GPS).

131. Al contrario que en otras plataformas móviles como Android, las aplicaciones no deben definir y solicitar permiso para acceder a los recursos y datos compartidos en los que están interesadas en el momento de su instalación, sino que estos se solicitan dinámicamente al usuario durante la ejecución de la aplicación móvil (app).

132. Sin embargo, iOS no proporciona granularidad suficiente para seleccionar únicamente un subconjunto de todos los permisos solicitados por una aplicación y restringir así su funcionalidad.

133. Aunque el número de permisos o controles de acceso se ha ido incrementando en las últimas versiones de iOS, especialmente desde iOS 5.x hasta iOS 7.x, sólo se dispone de controles de acceso para aquellos permisos definidos en la plataforma, quedando otros permisos sin gestionar adecuadamente, como por ejemplo el acceso al número de móvil del usuario o el acceso a la(s) cámara(s).

134. Los controles de privacidad de iOS han evolucionado a lo largo de las últimas versiones. Los permisos existentes en iOS 5.x eran muy limitados, permitiendo la gestión del acceso a la información de localización, las notificaciones *push*, y la integración con (la cuenta

de) Twitter. Sin embargo, no se disponía de permisos para operaciones críticas, como por ejemplo para poder grabar audio a través del micrófono del dispositivo móvil o acceder a la cámara del dispositivo móvil.

135. iOS 6 introdujo el nuevo panel de control de privacidad, con mayor granularidad para controlar el acceso a los servicios de localización (analizados en profundidad en el apartado "5.11. Servicios de localización geográfica"), la posibilidad de compartir datos a través de Bluetooth (opción "Compartir Bluetooth"), y el acceso a los contactos (o agenda), calendarios, recordatorios y fotos. Estos controles permiten restringir el acceso a los datos de todas estas categorías por parte de otras apps.

136. Tal como anunció Apple en febrero de 2012, iOS 6.x solicita finalmente al usuario permiso para el acceso (trasmisión y almacenamiento) a los datos de contactos [Ref.- 31]. Estos datos han sido una de las grandes preocupaciones desde el punto de vista de la privacidad durante años debido a su acceso y utilización por múltiples aplicaciones sin la autorización del usuario.

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

138. iOS 7 extendió los controles de privacidad para gestionar el acceso al micrófono (opción "Micrófono"), y extendió las capacidades de seguimiento a través de publicidad o anuncios (opción "Publicidad" en la parte inferior del menú de privacidad).

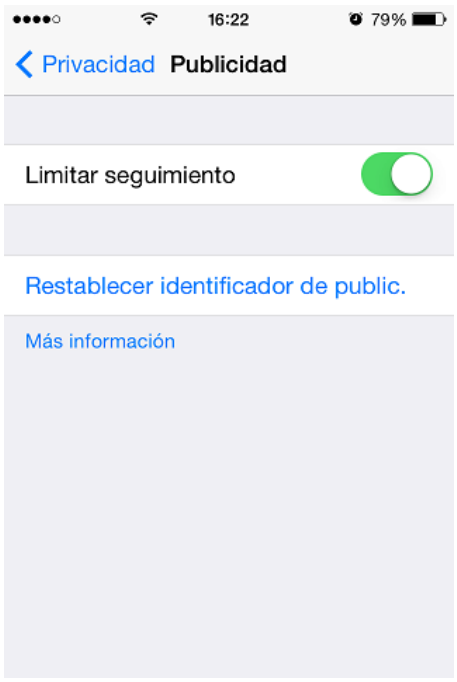
139. Debe prestarse especial atención a las apps que disponen de acceso al micrófono, ya que podrán a través del mismo escuchar todo el sonido y audio existente alrededor del dispositivo móvil, grabarlo y/o enviarlo a través de Internet.

140. Los dispositivos móviles que disponen del coprocesador de movimiento M7 (como por ejemplo los basados en el procesador A7 de Apple: iPhone 5S, iPad Air o iPad mini de 2ª generación) mostrarán adicionalmente el control de "Actividad física" ("Motion Activity"), que permite controlar que apps tendrán acceso a los datos recopilados por dicho procesador y podrán por tanto monitorizar los movimientos del usuario y su dispositivo móvil:

141. Principalmente (pero no en exclusiva), estas capacidades son utilizadas por aplicaciones deportivas, de entrenamiento personal y relacionadas con la salud, pero debe tenerse en cuenta que disponen de información muy detallada y precisa de los movimientos del dispositivo móvil (como ciclos y patrones de sueño, diferencias entre andar y correr, conteo del número de pasos, etc).

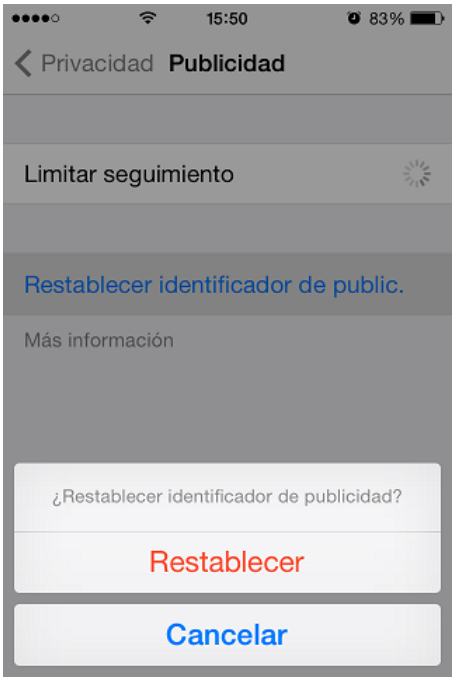
142. iOS 7 añade controles para limitar el acceso a las cuentas del usuario en diferentes redes sociales por parte de otras apps, pudiendo por tanto acceder a los datos publicados o llevar a cabo nuevas publicaciones. Por defecto se dispone de controles para Twitter y Facebook (categorías ya existentes en iOS 6.x), que se extienden en función de su uso también a Flickr o Vimeo.

143. iOS 7 permite limitar el seguimiento del usuario por parte de anunciantes y agencias de publicidad en base a un identificador temporal. Si la opción "Publicidad - Limitar seguimiento" está activa (opción recomendada desde el punto de vista de la privacidad), se evita recibir anuncios de iAd (la red de anuncios y publicidad de Apple asociada a los dispositivos iOS) relacionados con los intereses del usuario [Ref.- 149]:



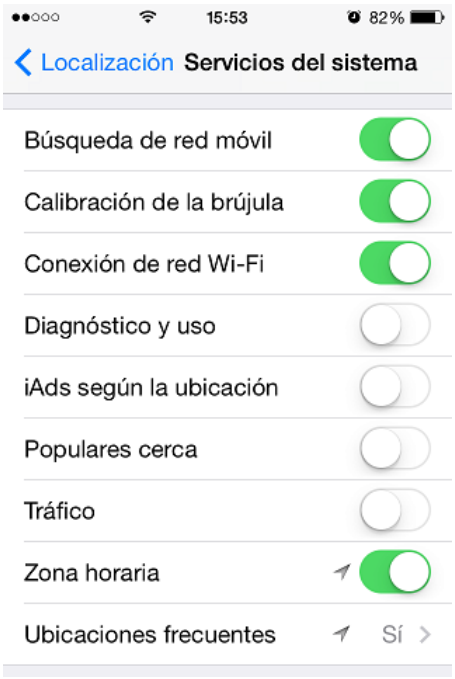
144. Al activar las limitaciones de seguimiento, es posible que se sigan viendo el mismo número de anuncios que antes, pero probablemente serán menos relevantes al no estar basados en los intereses del usuario. Posiblemente se mostrarán anuncios relacionados con el contenido de la app o anuncios basados en otro tipo de información no personal.

145. Adicionalmente, iOS 7 permite desde la sección de publicidad restablecer el identificador de publicidad empleado para ofrecer anuncios personalizados según las preferencias o intereses del usuario, generando un nuevo valor aleatorio y temporal, no asociado al dispositivo móvil, al usuario, o al valor existente previamente:



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

147. Complementariamente, se recomienda deshabilitar que se envíe información de la localización del usuario en las comunicaciones de anuncios de iAd. Para ello se debe deshabilitar el acceso a la localización por parte de iAd desde el menú "Ajustes - Privacidad - Localización - Servicios del sistema" y la opción "iAds según la ubicación":



148. Por último, iOS 8 incorporará finalmente nuevos controles de privacidad para el acceso a la cámara.

149. El siguiente ejemplo muestra la notificación para acceder a la información de localización por parte una aplicación iOS concreta, "Mapas", durante su ejecución, y como el icono de localización de la barra de estado (punta de flecha) muestra que se está accediendo a dicha información una vez ésta acción es permitida por parte del usuario:

150. Para aquellos permisos críticos definidos en la plataforma iOS, es posible ver los mismos desde el menú “Ajustes – Privacidad”, entrando en la opción correspondiente al control a configurar (por ejemplo, "Localización"), y seleccionando la aplicación de la lista:

151. Por defecto, las aplicaciones no disponen de ningún permiso de ubicación si no se activó el servicio de localización durante la configuración inicial del dispositivo móvil iOS. Si durante su ejecución una aplicación solicita permiso, éste será modificado de forma permanente la primera vez que es utilizado y autorizado. Posteriormente es posible volver a deshabilitar dicho permiso a través del menú "Ajustes – Privacidad".

152. Las mismas consideraciones aplican al resto de controles de acceso de privacidad que facilitan el acceso a otros tipos de datos diferentes a la localización, mencionados previamente.

153. En 2012 se identificó una vulnerabilidad en el modelo de permisos implementado por iOS, en el que una aplicación móvil puede únicamente solicitar al usuario permiso para acceder a la información de localización de las fotografías (y vídeos), y como resultado obtener adicionalmente acceso a las propias fotografías (y vídeos), pudiendo transferir las mismas a servidores remotos sin el consentimiento del usuario.

154. La aplicación "PhotoSpy" es una prueba de concepto (no disponible actualmente en la App Store) que muestra esta debilidad en iOS 5.x [Ref.- 112]:

155. Adicionalmente, ser*ía d*eseable disponer de un permiso de acceso a Internet con suficiente granularidad en iOS para poder autorizar a una aplicación a conectarse a Internet sólo a ciertos sitios web, y no a cualquier destino. Por defecto, todas las apps de iOS instaladas en un dispositivo móvil disponen de acceso a Internet, tanto a través de redes Wi-*Fi* como de redes de telefonía móvil 2/3/4G.

156. Desde iOS 7, los desarrolladores de apps para iOS disponen de capacidades a través de las librerías asociadas a los controles de acceso y privacidad para mostrar al usuario un

mensaje personalizado que explique el motivo por el que una determinada app solicita un permiso concreto, a través de un mensaje que describe el propósito de la solicitud.

5.2.2 SECURITY ENCLAVE

157. El *Secure Enclave* es un coprocesador criptográfico disponible en los dispositivos móviles basados en el chip A7 de Apple, como por ejemplo el iPhone 5S, iPad Air o iPad mini de 2ª generación.

158. Dispone de su propio proceso de arranque seguro, memoria cifrada, un generador de números aleatorios *hardware* y de un mecanismo de actualizaciones de software independientes de las del procesador principal [Ref.- 148]. Su función es proporcionar soporte a todas las operaciones criptográficas de los mecanismos de cifrado de iOS, *Data Protection*, incluida la gestión y protección de claves.

159. El generador de números aleatorios (RNG, *Random Number Generator*) disponible en el hardware de los dispositivos móviles iOS se encarga también de la generación de otras claves criptográficas, empleando la entropía del terminal obtenida durante el proceso de arranque y proporcionada también por los sensores internos [Ref.- 148].

160. Durante el proceso de fabricación, a cada *Secure Enclave* se le asigna un identificador único (UID, o Unique ID) que no es accesible para otras partes del sistema y que es desconocido por Apple. Al arrancar el dispositivo, la memoria de trabajo de este coprocesador se cifra con una clave efímera, creada en base a este identificador único.

161. De manera similar, los datos que son almacenados por el *Secure Enclave* en el sistema de ficheros, también son cifrados con una clave similar (basada en el UID), junto a un contador, para evitar ataques de repetición.

162. Complementariamente, este coprocesador es el encargado de procesar los datos biométricos del sensor Touch ID (ver apartado "5.4.3. Touch ID") y verificar si la huella dactilar coincide con una huella previamente registrada [Ref.- 148]. El sensor Touch ID y el *Secure Enclave* se comunican a través de un canal interno cifrado mediante AES empleando una clave de sesión, derivada de una clave compartida, que no permite el acceso a la información intercambiada ni al procesador principal del chip A7 de Apple.

5.2.3 SANDBOX DE IOS DE APPLE

163. Las aplicaciones en iOS ejecutan de forma independiente en su propio entorno de ejecución o *sandbox* [Ref.- 19] [Ref.- 116], denominado Apple XNU Sandbox (previamente “Seatbelt”) o App Sandbox, y basado en TrustedBSD, un entorno MAC (*Mandatory Access Control*) de Unix BSD.

164. Las restricciones del *sandbox* se establecen a través de la definición de políticas o perfiles para cada aplicación (existiendo algunos ya predefinidos), y pueden incluir, entre otros elementos comunicaciones (sockets TCP/IP), lecturas y escrituras (completas o limitadas) en el sistema de ficheros, acceso a recursos del sistema, etc.

165. Las reglas del *sandbox* de iOS son comunes para todas las aplicaciones de terceros descargadas de la App Store, no disponiéndose de granularidad para definir las capacidades de cada una de las aplicaciones en el dispositivo móvil de forma independiente, como por ejemplo ocurre en dispositivos móviles Android.

166. Debe tenerse en cuenta que el sandbox de iOS no limita el acceso a ciertos ficheros y ciertas aplicaciones clave del sistema, como Mobile Safari, pudiendo acceder a estos datos otras aplicaciones de terceros descargadas de la App Store [Ref.- 122].

167. La lista de ficheros legibles en ciertas versiones de iOS incluía ficheros de preferencias (.plist) de aplicaciones, la librería de fotos incluyendo la información de localización, la caché del teclado, las últimas búsquedas en Safari, el histórico de YouTube, información de la cuenta de correo electrónico, el número de teléfono, o el registro de las redes Wi-Fi a las que se ha conectado el dispositivo móvil anteriormente, entre otros.

168. El conjunto de datos disponibles para las aplicaciones móviles de terceros sin restricciones varía entre las diferentes versiones de iOS (ver apartado "5.2.1. Controles de acceso y privacidad").

169. El *sandbox* establece una política de control de acceso granular para cada aplicación o proceso a nivel del sistema operativo, dónde se limita el acceso a ficheros, preferencias, recursos de red, hardware, etc.

170. El objetivo del *sandbox* es evitar que una aplicación pueda disponer de acceso a los datos y recursos de otras aplicaciones o del sistema, ya sea por un mal comportamiento de la misma, o porque sea vulnerable y permita a un potencial atacante o a software malicioso la ejecución de código en el dispositivo móvil.

171. Las aplicaciones ejecutan empleando una cuenta de usuario estándar en Unix (“mobile”).

172. En el momento de su instalación, iOS asigna a cada aplicación su propio *sandbox*. De esta forma, sólo la aplicación tendrá acceso a sus ficheros asociados.

173. El *sandbox* proporciona a la aplicación un contenedor o directorio de trabajo, que en el caso de iOS contiene los documentos del usuario y datos de la aplicación, sus preferencias y la propia aplicación [Ref.- 23] (a diferencia de en OS X).

174. El directorio o contendor del *sandbox* emplea una estructura de subdirectorios definida (Documents, Library, tmp…) [Ref.- 24] y disponible para cada aplicación de iOS.

175. Sin embargo, debe tenerse en cuenta que el entorno de *sandbox* de iOS podría ser vulnerable y permitir operaciones fuera del mismo. Por ejemplo, las actualizaciones de seguridad introducidas en iOS 4 solucionaron una vulnerabilidad que permitía a las aplicaciones acceder directamente a la librería de fotos del usuario, y disponer sin autorización de acceso a las mismas y a la información de localización que éstas pudieran almacenar (CVE-2010-1751) [Ref.- 25].

5.3 GESTIÓN EMPRESARIAL DE DISPOSITIVOS BASADOS EN IOS

176. 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.

177. Las versiones iniciales de iOS presentaban numerosas limitaciones para la integración de dispositivos móviles iPhone es entornos empresariales y de negocio. Las últimas versiones disponen de numerosas funcionalidades para iPhone e iPad cuyo objetivo es proporcionar una integración más sencilla en dichos entornos [Ref.- 15] [Ref.- 69].

178. Apple proporciona capacidades empresariales para la gestión de dispositivos móviles basados en iOS [Ref.- 12] a través de Microsoft Exchange ActiveSync (y otras soluciones de gestión empresarial, MDM) y de la integración con tecnologías corporativas como VPNs, redes Wi-Fi empresariales, servidores LDAP y CalDAV, y la gestión de perfiles, configuraciones y distribución de aplicaciones OTA (Over-the-Air) [Ref.- 54].

179. Alternativamente, Apple proporciona soluciones de gestión para usuarios finales que no requieren del despliegue de servidores dedicados para este propósito, al emplearse los servicios de Apple "en la nube" (iCloud desde la versión 5.x de iOS [Ref.- 53]).

180. El iOS de iPhone e iPad dispone de capacidades para gestionar políticas de seguridad sobre los dispositivos móviles, incluyendo [Ref.- 13] [Ref.- 54]:

- Borrado remoto de los datos del dispositivo móvil (*wipe*), en caso de haber sido perdido o robado (ver apartado "5.9. Eliminación de datos del dispositivo móvil").

  Nota: Este proceso es equivalente a la opción "Borrar contenidos y ajustes" disponible desde el menú "Ajustes - General - Restablecer".

- Forzar la solicitud de un código de acceso al dispositivo móvil.
- Definir si se utilizará para el acceso un PIN (4 dígitos), una contraseña numérica (sólo con dígitos pero de mayor longitud), o una contraseña alfanumérica más robusta compuesta de letras y números.
- Definir si se permite un valor simple para la contraseña, entendiendo como tal secuencias de números o letras habituales, como "1234" o "asdf", o la repetición de caracteres, como "1111".
- Definir la longitud mínima del código de acceso.
- Definir la complejidad de la contraseña de acceso en base a los juegos de caracteres requeridos (números, letras mayúsculas y minúsculas, o símbolos). En concreto la política define el número de caracteres complejos, símbolos distintos a letras y números, que debe tener la contraseña.
- Definir el tiempo de validez del código antes de forzar a su renovación, es decir, su tiempo de expiración.
- Establecer si existe un histórico de contraseñas que evite la reutilización de las mismas, cuyo valor puede estar entre 1 y 50.
- Definir el máximo número de intentos de acceso fallidos. Una vez superado será necesario conectar el dispositivo móvil al ordenador con iTunes con el que está sincronizado para desbloquearlo [Ref.- 135].
- Definir el temporizador tras el cual el dispositivo se suspenderá automáticamente tras un periodo de inactividad.
- Complementariamente, definir la política de bloqueo del dispositivo móvil tras suspenderse (manual o automáticamente), es decir, el periodo de gracia o duración tras el cual será necesario introducir de nuevo el código de acceso para desbloquear el dispositivo.
- Definir si se permite el uso de Touch ID.

181. Adicionalmente, los usuarios de los terminales pueden de forma remota bloquear el dispositivo móvil con un PIN, hacer que suene el dispositivo móvil, mostrar un mensaje en la pantalla, y localizar su ubicación (ver apartado "5.22. Localización del dispositivo móvil: Buscar mi iPhone").

182. Las políticas de seguridad de iOS pueden ser implantadas y distribuidas de forma manual a través de un perfil de configuración (ver apartado "5.3.1. Perfiles de configuración") que los usuarios pueden instalar. Es posible definir que el perfil sólo pueda ser eliminado del dispositivo móvil mediante el uso de una contraseña administrativa, o incluso que para eliminarlo sea necesario restaurar el dispositivo a su configuración de fábrica, eliminando todos los datos que contiene.

183. Adicionalmente, las políticas de seguridad pueden ser distribuidas de forma automática a través de las soluciones de gestión empresarial de dispositivos móviles (MDM) sin la intervención del usuario.

184. Finalmente, si el dispositivo móvil tiene configurada una cuenta de Microsoft Exchange, es también posible distribuir las políticas de seguridad de forma automática y remota (OTA, *Over-the-Air*). Las políticas y funcionalidad disponible dependerá de la versión de Microsoft Exchange (2003, 2007 ó 2010) empleada.

Nota: La gestión empresarial de dispositivos móviles iOS mediante Microsoft Exchange ActiveSync (2003 o superior), incluyendo su implementación, configuración, e integración con las soluciones Microsoft Exchange está fuera del alcance de la presente guía (ver [Ref.-11]).

185. La gestión empresarial de iOS permite establecer restricciones adicionales en el dispositivo móvil para definir que funcionalidad estará disponible para el usuario, como por ejemplo las aplicaciones que hacen uso de la red (Safari, YouTube o iTunes) o la funcionalidad del dispositivo móvil (instalación de aplicaciones o utilización de la cámara).

186. El conjunto de restricciones que pueden ser establecidas en el dispositivo móvil a través de las políticas de seguridad incluye, entre otras:

- Funcionalidad del dispositivo:
  - Permitir: Siri, instalar aplicaciones, utilización de la cámara, FaceTime, capturas de pantallas, sincronización automática en *roaming*, realizar llamadas mediante voz, adquisición de aplicaciones, o utilizar juegos multi-jugador y añadir amigos a Game Center.
- Aplicaciones:
  - Permitir: utilizar YouTube, la tienda iTunes, Safari y poder fijar las preferencias de seguridad de Safari.
- iCloud:
  - Permitir copias de seguridad, sincronización de documentos y claves, y Photo Stream.

- Seguridad y privacidad:
  - Permitir: el envío de datos de diagnóstico a Apple, la aceptación de certificados digitales que no son de confianza y forzar el cifrado de las copias de seguridad a través de iTunes.
- Contenidos:
  - Permitir: contenido explícito (música, podcasts, etc), la región de valoraciones (*ratings*), y establecer el *rating* del contenido permitido.

187. Desde el punto de vista de seguridad, la aplicación para ordenador iTunes también puede ser configurada y gestionada a nivel empresarial, con el objetivo de deshabilitar el acceso a contenido, establecer los servicios disponibles o determinar políticas de actualizaciones específicas [Ref.- 16].

188. Las soluciones de gestión empresarial (MDM) permiten gestionar tanto aplicaciones de terceros de la App Store como aplicaciones privadas corporativas (mediante perfiles de aprovisionamiento). Una aplicación gestionada puede ser eliminada desde el servidor MDM, junto a sus datos, por el administrador del entorno, siendo también posible limitar que se realicen copias de seguridad mediante iTunes o iCloud de los datos sensibles de ciertas aplicaciones.

189. Las aplicaciones gestionadas pueden ser instaladas de forma remota a través del servidor MDM, siendo necesaria la confirmación por parte del usuario del dispositivo móvil [Ref.- 18] o de manera automática y desatendida, según la versión de iOS empleada.

190. En resumen, las soluciones de gestión empresarial de dispositivos móviles, a través del protocolo MDM proporcionado por Apple en iOS, disponen de capacidades para configurar los dispositivos (instalar y eliminar perfiles de configuración y aprovisionamiento), consultar información de los mismos (versiones de software, listas de aplicaciones, etc) y controlarlos remotamente (bloquearlos, eliminar sus datos, etc).

191. El protocolo MDM se integra con las capacidades de notificaciones *push* de iOS (ver apartado "5.18.8. Notificaciones *push*"). El dispositivo móvil dispone de una conexión persistente con uno de los servidores *push* (APNS) de Apple, "courier.push.apple.com", a través del interfaz de telefónica móvil (2/3/4G) o Wi-Fi.

192. A través del servicio *push*, el dispositivo móvil se suscribe al tema asociado al servidor MDM, y el servidor MDM actúa de servidor o proveedor de notificaciones, conectándose a los servidores gateway de Apple disponibles para este servicio, "gateway.push.apple.com". La conexión emplea SSL/TLS con autentificación basada en certificados a través de los puertos 2195/tcp y 2196/tcp.

193. Por otro lado, el servidor MDM ofrece su funcionalidad a través de SSL/TLS. El dispositivo móvil iOS establece una conexión con el servidor MDM tras recibir una notificación *push* para llevar a cabo las acciones oportunas [Ref.- 125].

194. Debe tenerse en cuenta que el protocolo ha presentado algunas debilidades, como la aceptación de cualquier certificado firmado por una autoridad certificadora reconocida, o que el proceso de eliminación remota de datos del dispositivo móvil no emplea ningún mecanismo de autentificación [Ref.- 123].

195. Se dispone de más información sobre la gestión empresarial de dispositivos móviles, incluyendo iOS, en la guía "CCN-STIC-457 - Gestión de dispositivos móviles: MDM (Mobile Device Management" [Ref.- 139].

5.3.1 CAPACIDADES DE GESTIÓN MDM EN IOS7

196. Las capacidades de gestión a través de las soluciones MDM en iOS 7 han sido extendidas respecto a versiones previas, añadiéndose nuevas restricciones, consultas sobre qué funcionalidad está activa en el dispositivo móvil y nuevos comandos de gestión.

197. iOS 7 [Ref.- 150] añade nuevas opciones de configuración, acciones y consultas a través de los mecanismos de gestión empresarial (MDM), como la configuración remota de apps gestionadas, la instalación de fuentes personalizadas, la configuración de opciones de accesibilidad e impresoras vía AirPrint, junto a la gestión de AirPlay y a la definición de destinos permitidos y/o protegidos por contraseña para esta tecnología.

198. Versiones previas de iOS (por ejemplo, iOS 6.x) ya permitían la instalación de apps gestionadas a través de la solución MDM, así como su posterior eliminación, o poder prevenir la realización de copias de seguridad de estas apps a través de iCloud para evitar la fuga de datos corporativos.

199. iOS 7 añade nuevas capacidades para instalar apps silenciosamente en dispositivos móviles supervisados, e incluso configurar las apps remotamente (vía OTA), modificando así su comportamiento. Adicionalmente, la nueva API para las soluciones MDM dispone de comandos para obtener datos del usuario directamente (a través de los protocolos de comunicaciones MDM) de las apps y su *sandbox* asociado (mecanismo denominado *feedback*) [Ref.- 151].

200. Adicionalmente se ha automatizado el proceso de registro en la solución MDM para los dispositivos móviles iOS propiedad de la organización (no válido en entornos BYOD) durante el proceso de activación de los mismos (*streamlined device enrollment*) [Ref.- 151].

201. El nuevo proceso de registro permite a las organizaciones definir previamente como debe realizarse el registro en su solución MDM (pudiendo establecer distintos criterios para diferentes dispositivos) e integrar las configuraciones asociadas (como la URL de registro del servidor MDM) en el proceso estándar de obtención de fábrica y activación de los dispositivos móviles iOS.

202. Estas gestiones se realizan a través de un nuevo servicio de Apple “en la nube” asociado a la compra y registro de dispositivos móviles iOS.

203. Cuando un nuevo dispositivo móvil iOS es recibido por la organización (vía Apple), y es activado por el usuario siguiendo los pasos del proceso de activación estándar, el usuario será preguntado por sus credenciales para proceder automáticamente al proceso de registro en la solución MDM.

204. Es posible incluso establecer que el registro en la solución MDM sea un paso obligatorio que de no ser completado, no permitirá la activación del dispositivo móvil.

205. Apple permite la distribución de apps (o libros) de pago empleando códigos o bonos de pago (*redemption codes*, o URLs) adquiridos a través del *Volume Purchase Program* (VPP) de Apple [Ref.- 152]. Este programa permite la adquisición de apps (y libros) por lotes, asociadas a compras por volumen, junto a apps privadas, personalizadas y

específicas para negocios (B2B) no disponibles en la App Store pública, para su posterior distribución e instalación en los dispositivos móviles de la organización (sin que los usuarios tengan que pagar individualmente por ellas).

206. Previamente a iOS 7, si la organización distribuía la licencia de una app a un empleado, está era asignada al Apple ID del empleado, y no podía ser recuperada y reutilizada por la organización posteriormente (en otro nuevo dispositivo móvil del mismo empleado, o en el dispositivo móvil de otro empleado).

207. Adicionalmente, esta distribución tenía que hacerse por país, debido a las restricciones geográficas del modelo previo, afectando significativamente a la gestión de licencias en organizaciones internacionales con presencia en múltiples países [Ref.- 153].

208. En iOS 7 [Ref.- 150] [Ref.- 151] se permite la asignación temporal y remota (OTA) de apps (y libros) a usuarios a través del VPP, mientras que la organización mantiene la propiedad y el control de las licencias, pudiendo revocar las mismas en todo momento, recuperarlas y/o reasignarlas a otro usuario. Este modelo evita incurrir en pérdidas o gastos innecesarios asociados a la adquisición de apps para la organización e incluso encaja mejor en entornos BYOD.

209. El usuario por tanto obtiene acceso temporalmente a la licencia, y adicionalmente se mantiene la privacidad del usuario, ya que su Apple ID no es revelado a la organización.

210. Se emplea por tanto más el concepto de licencia en lugar de código de pago en iOS 7 (frente a versiones previas), y se puede vincular (si se desea) su uso al proceso de instalación o eliminación de apps a través de la solución MDM.

5.3.2 PERFILES DE CONFIGURACIÓN

211. Los perfiles de configuración de iOS son ficheros XML que contienen las políticas de seguridad del dispositivo móvil, restricciones a aplicar sobre el dispositivo móvil, y otros datos de carácter sensible y confidencial, como por ejemplo la configuración de redes Wi-Fi y VPN, la configuración del APN de telefonía móvil, certificados digitales, las cuentas de usuario de acceso al correo electrónico o las credenciales de acceso a los sistemas de gestión empresariales, como Microsoft Exchange [Ref.- 135].

212. Los ajustes fijados por un perfil de configuración no pueden ser modificados por el usuario. Si un usuario elimina un perfil de configuración (en caso de que esté permitido por el administrador), todos los ajustes asociados serán eliminados. Este modelo permite configurar, por ejemplo, una cuenta de e-mail junto a ciertos requisitos en el código de acceso del dispositivo, no pudiendo accederse a dicha cuenta si no se cumplen dichos requisitos.

213. Los perfiles de configuración pueden ser cifrados (para que su contenido sólo esté disponible para el dispositivo móvil para el que han sido creado), firmados (para asegurar su integridad y que no puedan ser modificados), y bloqueados (para que no puedan ser eliminados de los dispositivos móviles si el usuario no dispone de la contraseña de bloqueo, o de manera permanente).

214. Se recomienda emplear el algoritmo AES de 128 bits para el cifrado de los perfiles de configuración, pese a qué también está disponible el algoritmo 3DES.

215. En caso de no cifrar los perfiles de configuración, las credenciales y contraseñas contenidos en los mismos, por ejemplo empleadas para la conexión a redes Wi-Fi, VPNs,

cuentas de correo electrónico (e-mail), Microsoft ActiveSync, LDAP. CalDAV, etc, podrían almacenarse en claro o en base 64.

216. La primera vez que se distribuye un perfil de configuración éste puede ser instalado a través de una conexión USB y la utilidad de configuración (*iPhone Configuration Utility (IPCU)*, ver apartado "5.3.3. Utilidad de configuración del iPhone"), o mediante *Over-the-Air Enrollment*. En sucesivas distribuciones es posible emplear un adjunto en un correo electrónico, un servidor web, o soluciones de gestión empresariales (MDM).

217. Es posible verificar la existencia y aplicación de un perfil de configuración en el dispositivo móvil desde el menú "General - Ajustes". En el caso de disponer de un perfil existirá una nueva opción "Perfil" entre las opciones "VPN" y "Restablecer" en la parte inferior (o "Perfiles" si hay más de uno):

5.3.3 UTILIDAD DE CONFIGURACIÓN DEL IPHONE (IPCU)

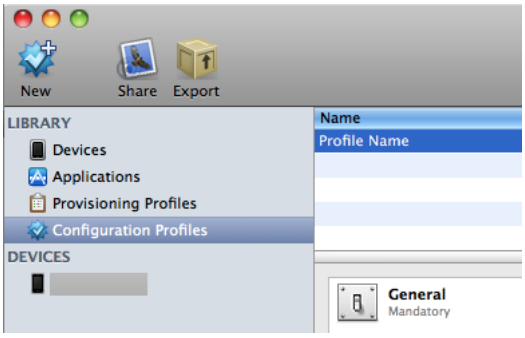
218. La utilidad de configuración del iPhone e iPad (o iOS), en inglés "iPhone Configuration Utility" (en adelante IPCU), está asociada a las capacidades de gestión empresarial de Apple [Ref.- 12] y está disponible tanto para OS X como para Windows [Ref.- 71]:

219. La utilidad IPCU permite crear, gestionar, cifrar e instalar perfiles de configuración en dispositivos móviles iOS, gestionar e instalar perfiles de aprovisionamiento y

aplicaciones autorizadas, y obtener información detallada del dispositivo, incluyendo los logs de la consola.

220. Los perfiles de configuración de iOS son ficheros XML que contienen las políticas de seguridad del dispositivo móvil y numerosos parámetros de configuración (ver apartado "5.3.2. Perfiles de configuración. ").

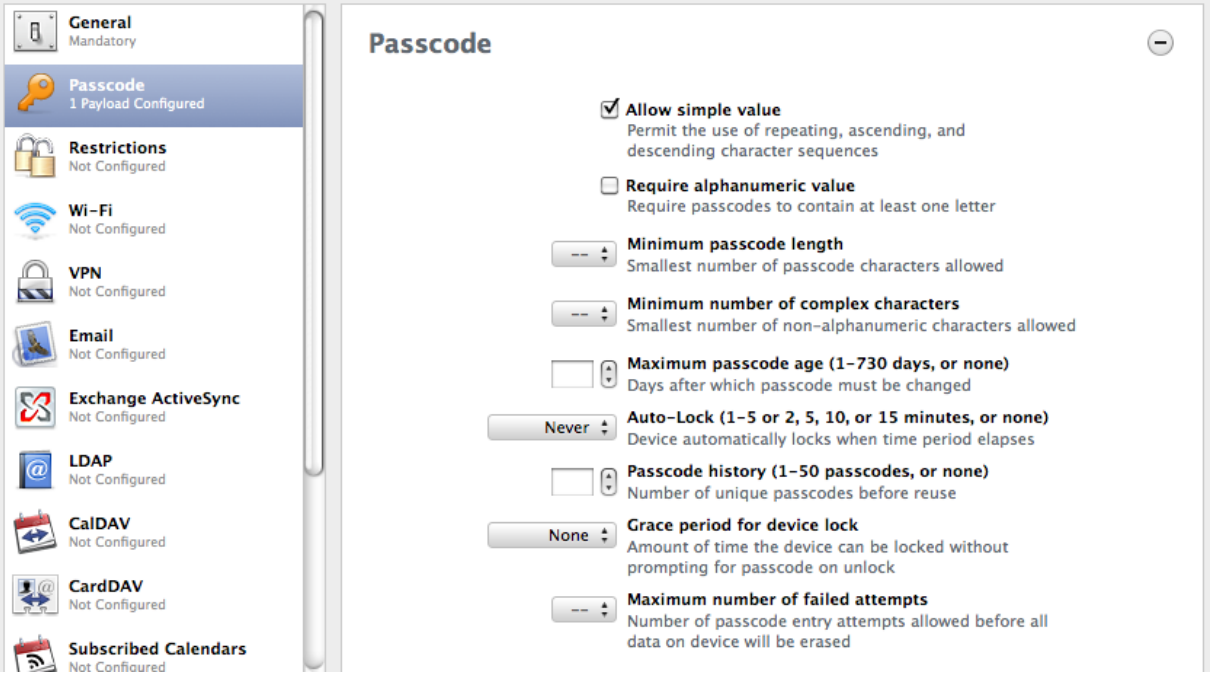
221. Mediante la opción "Configuration Profiles" del menú "Library" de la izquierda es posible crear nuevos perfiles de configuración, empleando para ello el icono "New":



222. La pestaña "General" permite especificar los detalles generales del nuevo perfil de configuración, como por ejemplo el nombre del perfil, un identificador, el nombre de la organización y una descripción. Adicionalmente se debe especificar el nivel de seguridad del perfil, que establece cuando podrá ser eliminado del dispositivo móvil iOS: siempre (opción por defecto), con autorización, o nunca.

Nota: El alcance de la presente guía no contempla el análisis detallado de todas las opciones disponibles a través de la utilidad IPCU para la creación de perfiles de configuración de iOS. A continuación se muestran algunos ejemplos concretos y referencias adicionales para disponer de toda la documentación necesaria.

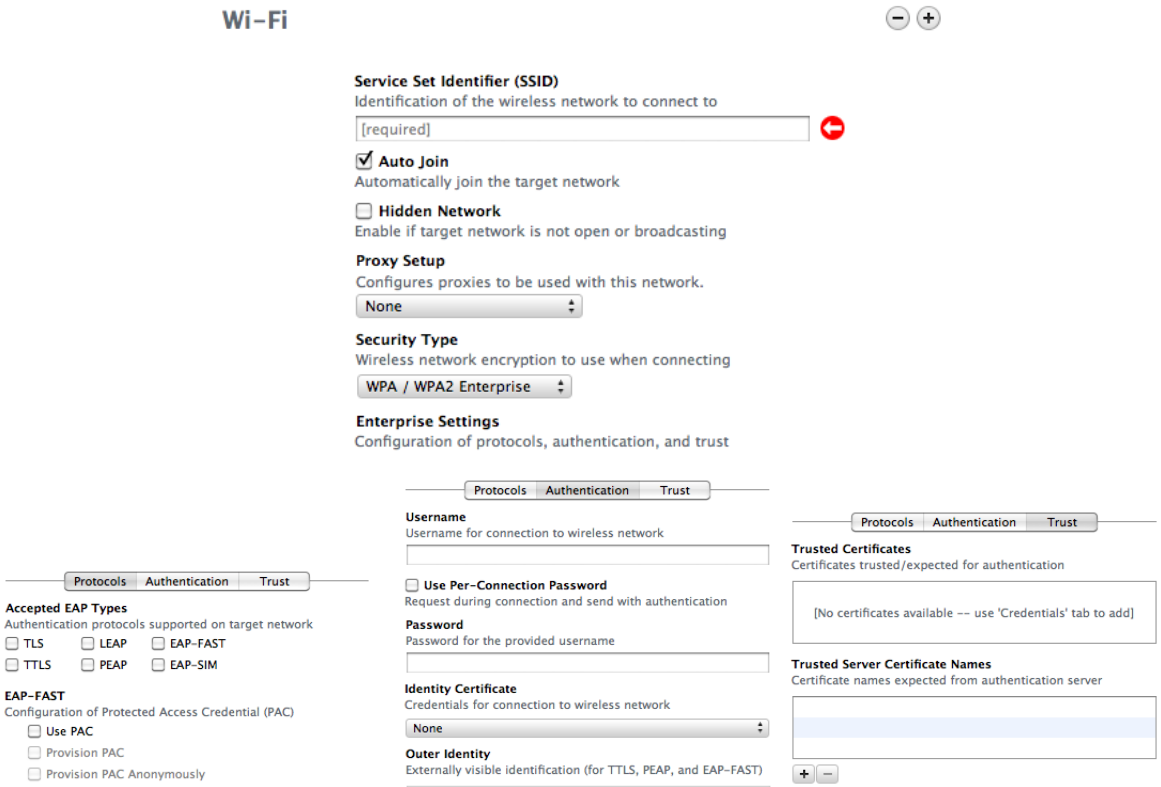
223. Por ejemplo, a través del menú "Passcode" es posible configurar los requisitos asociados al código de acceso del dispositivo móvil y configurar los diferentes ajustes disponibles, como el uso de un código simple, numérico o alfanumérico, su longitud, complejidad y validez, el periodo de autobloqueo del dispositivo (con y sin código de acceso), el histórico de códigos para evitar repeticiones y el número máximo de intentos de acceso permitidos antes de eliminar los datos del dispositivo móvil. El usuario no podrá modificar estos ajustes una vez que se ha instalado el perfil de configuración en el dispositivo móvil:



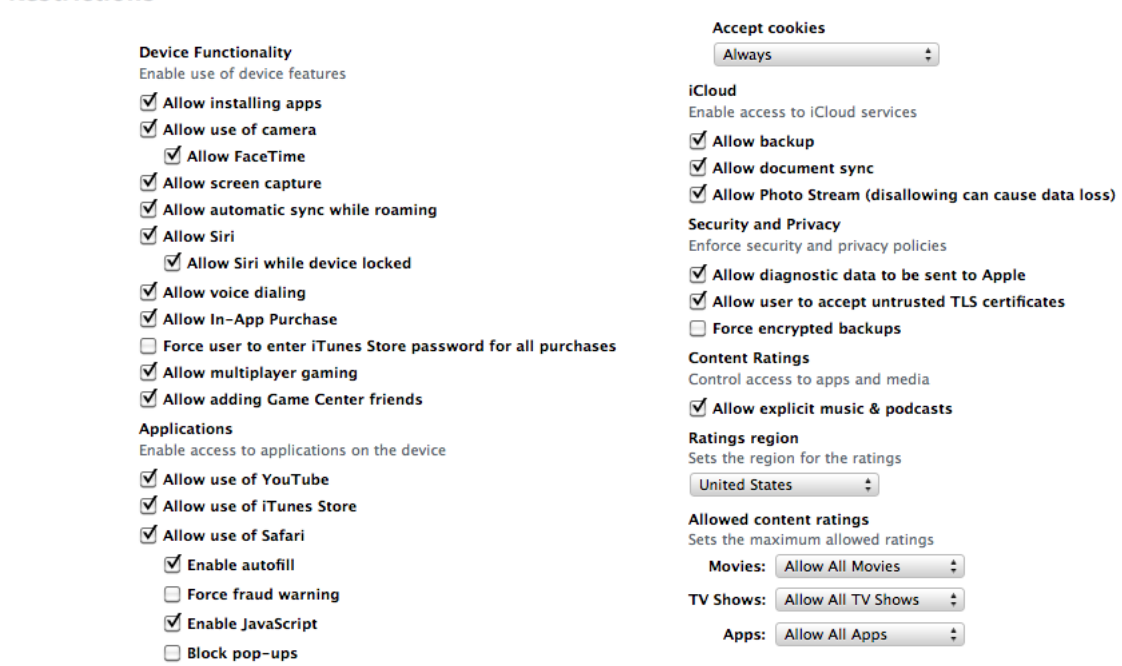
224. Por otro lado, la configuración de un perfil para el acceso a redes Wi-Fi empresariales puede llevarse a cabo desde el menú "Wi-Fi". Previamente a la configuración de la red Wi-Fi es necesario especificar el certificado digital de la autoridad de certificación (Certification Authority, CA) empleada para la generación de certificados de la red Wi-Fi desde el menú "Credentials":

225. Para poder utilizar el certificado digital correspondiente a la CA desde IPCU en OS X basta con disponer de él en un fichero (con extensión .cer o .p12) ubicado en el ordenador asociado, mientras que en Windows debe haber sido importado previamente en el almacén personal de certificados del usuario empleado para ejecutar IPCU.

226. Desde el menú "Wi-Fi" se debe establecer la configuración de la red, especificando el nombre de la red (SSID), si se establecerán conexiones automáticamente con la misma, si es o no una red oculta, la configuración del proxy, los mecanismos de seguridad de la red (como por ejemplo "WPA/WPA2 Enterprise") y todos los parámetros de seguridad asociados, incluyendo los algoritmos EAP, autentificación del usuario (contraseña, certificado digital cliente, etc), y las entidades de confianza, tanto desde el punto de vista de los certificados previamente importados como de los nombres de los servidores de autentificación:



227. Las siguientes imágenes muestran algunas de las restricciones (con los valores por defecto en IPCU) que pueden ser establecidas a través de los perfiles de configuración en los dispositivos móviles iOS, como por ejemplo bloquear la instalación de aplicaciones, el uso de la cámara, de Safari, o de Siri, o la realización de backups mediante iCloud:



228. Una vez el perfil de configuración ha sido creado, mediante el icono "Share" de la opción "Configuration Profiles" del menú "Library" de la izquierda, se procederá a su firma y se generará un mensaje de correo electrónico (e-mail) que incorporará como

adjunto el perfil de configuración (denominado por defecto "Profile Name.mobileconfig"), de forma que pueda ser enviado y abierto desde el dispositivo móvil para su instalación.

229. Adicionalmente a la posibilidad de instalar el perfil de configuración directamente a través de IPCU tras conectar el dispositivo móvil al ordenador mediante cable USB, el icono "Export" de la opción "Configuration Profiles" del menú "Library" de la izquierda, permite exportar en un fichero el perfil creado para su distribución, por ejemplo vía e-mail o a través de la web. El proceso de exportación permite seleccionar el nombre del fichero con el perfil, con extensión ".mobileconfig".

230. El tipo MIME que debe ser configurado en el servidor web empleado para la distribución de perfiles de configuración de iOS, con extensión ".mobileconfig", es "application/x-apple-aspen-config". Por ejemplo, en Apache debe crearse esta asociación en el fichero "mime.conf": AddType application/x-apple-aspen-config .mobileconfig.

231. La utilidad de configuración genera los perfiles de configuración en formato binario tras haber sido firmados, o en formato XML si se selecciona no firmarlos (opción "None"), lo que facilita su análisis y posterior modificación.

232. Una vez el perfil de configuración ha sido instalado en el dispositivo móvil, las acciones o restricciones aplicadas conllevarán que ciertas opciones y menús disponibles en las pantallas de ajuste de configuración del dispositivo móvil iOS aparecerán en color gris, no pudiendo el usuario modificar su configuración.

233. La guía de despliegue de dispositivos iOS a nivel empresarial contiene información más detallada de la parametrización y utilización de la utilidad de configuración de iPhone (IPCU) y de los perfiles de configuración [Ref.- 54] [Ref.- 69].

234. Apple proporciona otra herramienta para la configuración simultánea de múltiples dispositivos móviles iOS, denominada Apple Configurator [Ref.- 117], junto a la disponibilidad de Profile Manager, un servidor MDM para la gestión empresarial de dispositivos móviles en entornos de tamaño reducido, integrado por defecto en OS X Lion Server [Ref.- 124].

235. Esta utilidad sólo está disponible para OS X, puede crear perfiles de configuración al igual que IPCU, pero permite aplicar dichos perfiles y configuraciones a múltiples dispositivos móviles iOS simultáneamente, mientras que IPCU sólo puede trabajar con un dispositivo a la vez [Ref.- 69].

236. Adicionalmente, Apple Configurator permite configurar un dispositivo móvil iOS en modo "supervisado", impidiendo que el dispositivo pueda ser emparejado o asociado con un ordenador con iTunes [Ref.- 69] y proporcionando numerosos controles adicionales, limitaciones de uso y mecanismos de gestión de los dispositivos móviles iOS.

237. La tendencia de Apple para la gestión de dispositivos móviles iOS en entornos de pequeño tamaño pasa por promover Apple Configurator, pero desafortunadamente sólo está disponible para OS X, frente a iPhone Configuration Utility (IPCU), que está disponible tanto para Windows como para OS X.

238. Normalmente, un dispositivo móvil iOS no bloqueado puede ser asociado con cualquier ordenador con iTunes. Sin embargo, en modo "supervisado" sólo puede asociarse con el ordenador que dispone de Apple Configurator y del certificado de supervisión adecuado,

denominado *Supervisory Host Identity Certificate* (SHIC), almacenado en la *keychain* del ordenador OS X con Apple Configurator.

239. Este modo restrictivo o "supervisado" puede ser empleado por ciertas organizaciones para evitar que el usuario del dispositivo móvil iOS pueda sincronizar música y otros contenidos con su ordenador, al igual que evitar que instale aplicaciones o realice copias de seguridad a través de iTunes.

240. Desafortunadamente, otras capacidades críticas sólo pueden ser gestionadas o deshabilitadas desde la solución MDM en dispositivos móviles iOS supervisados, como por ejemplo el restringir el dispositivo móvil a una red Wi-Fi específica, la instalación de apps directamente sin la intervención del usuario, prevenir que el usuario pueda crear o modificar cuentas Apple (Apple ID), deshabilitar iMessages, deshabilitar AirDrop, etc.

5.4 ACCESO FÍSICO AL DISPOSITIVO MÓVIL

241. 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.

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

5.4.1 PIN DE LA TARJETA SIM

243. 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).

Nota: Pese a que los dispositivos móviles iPad no disponen de capacidades de telefonía móvil de voz y SMS, algunos modelos (Wi+Fi+3G y Wi-Fi+Cellular) sí disponen de capacidades de telefonía móvil de datos, empleando igualmente una tarjeta SIM. Por tanto, la presente sección aplica tanto a dispositivos móviles iOS iPhone como iPad, en función de sus capacidades de telefonía.

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

245. Si se ha fijado la restricción de usar PIN en la tarjeta SIM, iOS permite acceder al dispositivo móvil aunque no se disponga del PIN de la tarjeta SIM, pudiendo hacer uso de todos los servicios del terminal, excepto los asociados a las capacidades de telefonía móvil. iOS mostrará tanto en la barra de estado como con un mensaje de notificación que es necesario introducir el código PIN para disponer de acceso a la tarjeta SIM:

246. 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.

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

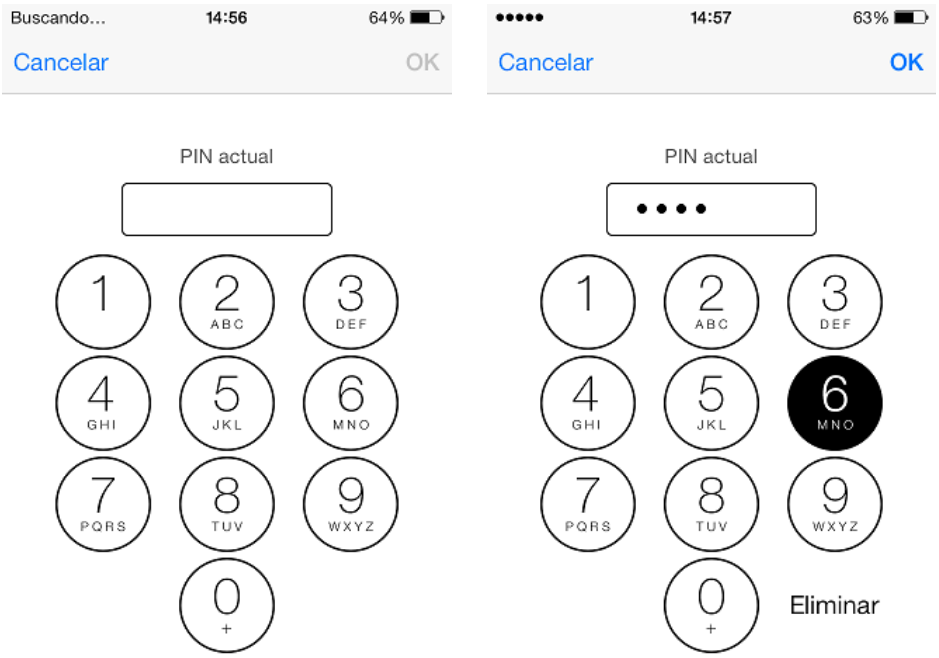
248. iOS permite emplear un PIN de la tarjeta SIM con un valor de 4 a 8 dígitos:

249. 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 (ver imagen superior derecha).

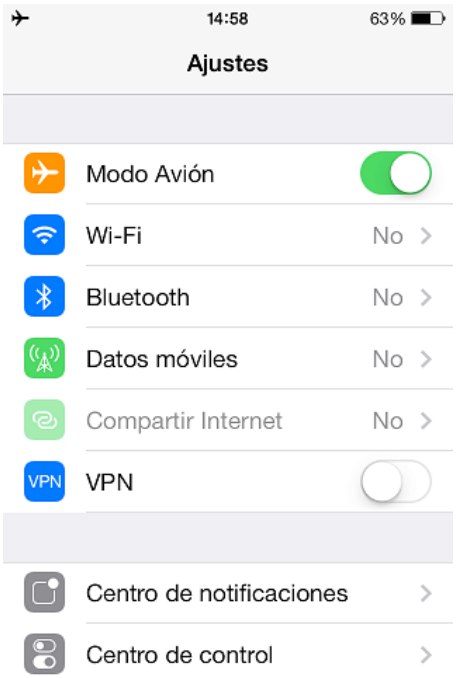
250. El número de intentos restantes es mostrado por iOS en la pantalla de solicitud del PIN. En ese caso, para poder desbloquear la tarjeta SIM es necesario emplear una segunda clave de acceso denominada PUK (*PIN Unlock Key*).

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

252. 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, y preferiblemente empleando 8 dígitos:



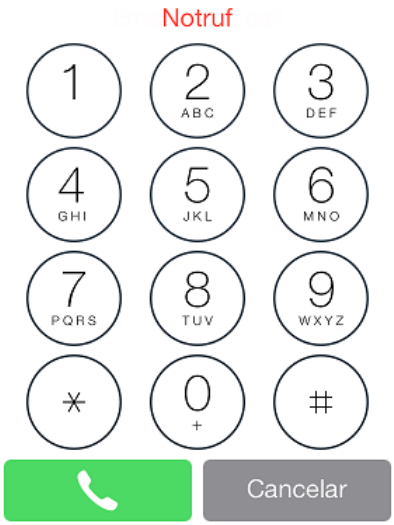
253. Debe tenerse en cuenta que cada vez que el dispositivo móvil sale del "Modo avión" (cuando este modo es desactivado; menú "Ajustes – Modo Avión"), no solicitará el PIN de la tarjeta SIM al usuario, ya que iOS lo almacena en memoria y lo utiliza (en caso de ser necesario) para activar de nuevo los servicios de telefonía móvil:



5.4.2 CÓDIGO DE ACCESO AL DISPOSITIVO MÓVIL

254. El código de acceso (PIN, contraseña, etc) del dispositivo móvil bloquea el acceso no autorizado al terminal, incluyendo sus datos, capacidades de comunicación y aplicaciones.

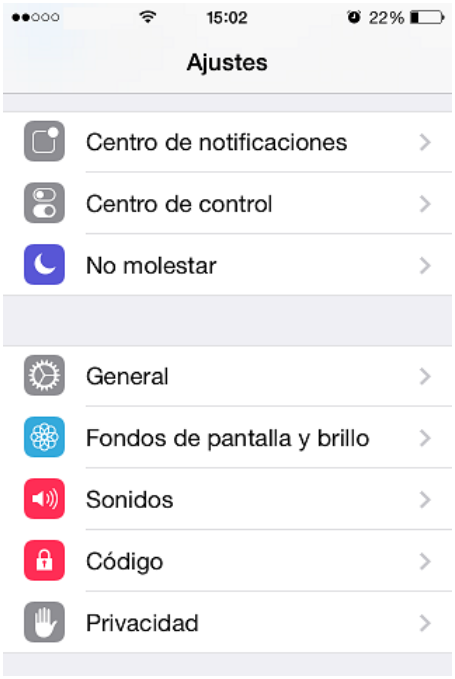
255. Una vez el dispositivo móvil está bloqueado, únicamente se permite la realización de llamadas de emergencia (112) sin el PIN, código o contraseña de acceso al terminal. Para ello es necesario marcar el número de teléfono de emergencias tras deslizar el botón de "Desbloquear" y pulsar el botón “SOS”:



256. 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.

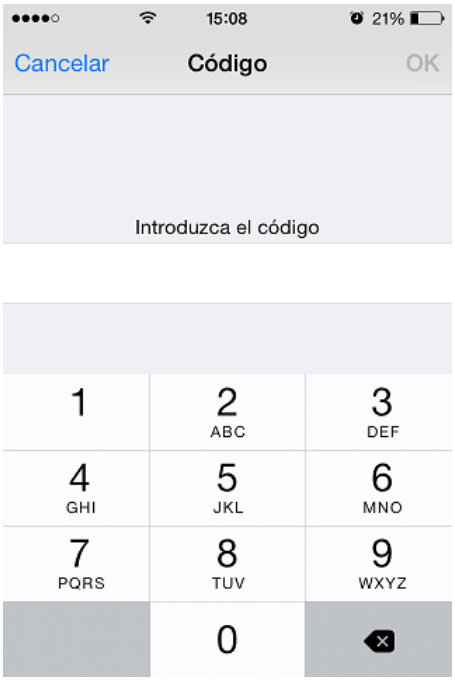
257. Por defecto, los dispositivos móviles basados en iOS no disponen de un código de acceso para bloquear accesos no autorizados al terminal.

258. Se recomienda por tanto establecer el código de acceso al dispositivo móvil a través del menú “Ajustes – Código”:



Nota: El menú con los ajustes de configuración del código de acceso es uno de los elementos asociados al interfaz de usuario (y mencionados al comienzo de la presente guía) que ha cambiado significativamente en la versión 7.1 de iOS respecto a las versiones 7.0.x de iOS y versiones previas (6.x y 5.x). El menú en iOS 7.1 está en "Ajustes - Código" mientras que en iOS 7.0.x estaba en "Ajustes - General - Bloqueo con código".

259. iOS permite establecer dos tipos de contraseña de acceso: un código simple o PIN numérico tradicional (opción “Código simple”), compuesto por cuatro dígitos (0-9), o una contraseña alfanumérica (opción “Código simple” no habilitada):



260. El código simple o PIN impone una restricción implícita en su valor, ya que obligatoriamente debe estar compuesto por cuatro dígitos numéricos.

261. La contraseña, por defecto, no impone restricciones sobre su valor, pudiendo estar compuesta por un único carácter alfanumérico (incluyendo símbolos de puntuación), como por ejemplo "1", "a" o ".".

262. Por tanto, la opción de contraseña, más segura y recomendada que la opción de código simple a priori, debe ser configurada adecuadamente para realmente ser más segura y contener, al menos, cuatro (o preferiblemente más) caracteres alfanuméricos.

263. A través de los perfiles y políticas de configuración, es posible modificar las restricciones asociadas a la contraseña (ver apartado "5.3. Gestión empresarial de dispositivos basados en iOS") y establecer, por ejemplo, una longitud mínima o la complejidad de la misma.

264. Por tanto, el tamaño mínimo en iOS del PIN es de 4 dígitos y el de la contraseña alfanumérica es de 1 dígito o carácter. El tamaño máximo del PIN es también de 4 dígitos y el de la contraseña es superior a 50 dígitos o caracteres.

265. En caso de establecer un código de 4 dígitos, automáticamente iOS activará la opción de configuración de código simple.

266. iOS por defecto 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.

267. Sin embargo, los perfiles y políticas de configuración (ver apartado "5.3. Gestión empresarial de dispositivos basados en iOS") sí permiten definir si se acepta un valor simple para la contraseña, entendiendo como tal secuencias de números o letras habituales, como "1234" o "asdf", o la repetición de caracteres, como "1111".

268. Adicionalmente, en el caso de emplear una contraseña alfanumérica (opción recomendada), por defecto iOS 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.

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

270. De nuevo, los perfiles y políticas de configuración (ver apartado "5.3. Gestión empresarial de dispositivos basados en iOS") sí permiten definir la complejidad de la contraseña de acceso en base a los juegos de caracteres requeridos (números, letras mayúsculas y minúsculas, o símbolos de puntuación).

271. Al emplear un código de acceso la pantalla de bloqueo de acceso de iOS no muestra los valores introducidos mientras se escribe. Sin embargo, en otras pantallas de configuración, como la del cambio del código de acceso, si se muestra temporalmente (durante unos dos segundos) únicamente el último dígito o carácter pulsado.

272. Desde iOS 7, con el objetivo de incrementar la usabilidad, la pantalla de bloqueo resalta los valores introducidos para el código de acceso, lo que facilita su visualización por parte de un tercero:

273. Desde el punto de vista de seguridad se recomienda ser cuidadoso al introducir las contraseñas en estos dos tipos de pantallas, para evitar que alguien con acceso visual al dispositivo móvil durante, por ejemplo, tanto el proceso de autentificación como el proceso de cambio de código, pueda obtener el código de acceso empleado.

274. Pese a la debilidad de un PIN de 4 dígitos frente a ataques de adivinación o fuerza bruta, iOS implementa un mecanismo que hace que sólo sea posible introducir seis PINs o contraseñas incorrectos, debiendo esperar un minuto inicialmente para realizar nuevos intentos de acceso, y aumentando el periodo de tiempo para los intentos posteriores.

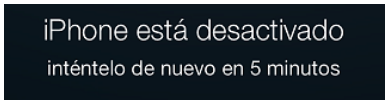
275. Una vez realizados ese número de intentos, el dispositivo no permitirá el acceso durante un minuto:

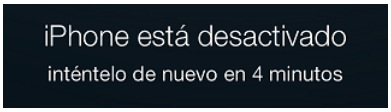
276. Tras introducir de nuevo un PIN o contraseña incorrectos el dispositivo móvil aumenta progresivamente el periodo de tiempo necesario para poder reintentar un nuevo acceso, con el objetivo de dificultar los ataques de fuerza bruta y adivinación del PIN.

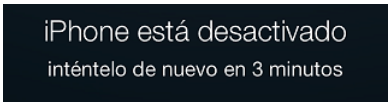
277. El periodo inicial de desactivación del acceso es de 1 minuto, pasando a 5 minutos tras la realización de otro intento de acceso adicional, a 60 minutos en el siguiente intento, y aumentando el tiempo de forma significativa con cada intento de acceso fallido adicional.

278. Si se realiza un número muy elevado de reintentos de acceso fallidos, no será posible realizar el acceso al dispositivo móvil directamente, siendo necesario conectarlo al ordenador con iTunes desde el que se realizó la última sincronización [Ref.- 58].

279. El dispositivo móvil muestra en todo momento al usuario el tiempo restante hasta poder intentar de nuevo el acceso:







280. Los mecanismos de protección frente a fuerza bruta sólo aplican en la interacción de un potencial atacante con la pantalla de bloqueo y acceso del dispositivo móvil (interfaz gráfico de iOS gestionado por *SpringBoard*), existiendo mecanismos para obtener el código de acceso en mucho menos tiempo a través de técnicas en las que se arranca el dispositivo móvil iOS desde una imagen *ramdisk* personalizada (ver apartado "5.7.1. Cifrado del dispositivo móvil").

281. Adicionalmente, los dispositivos móviles de Apple basados en el chip (o SoC) A7 de Apple, como por ejemplo el iPhone 5S, iPad Air o iPad mini [Ref.- 96], disponen de capacidades en el *Secure Enclave* para mitigar ataques de fuerza bruta, ya que éste introduce un retardo de 5 segundos entre intentos fallidos de acceso reiterados (ver apartado "5.2.2. Security Enclave").

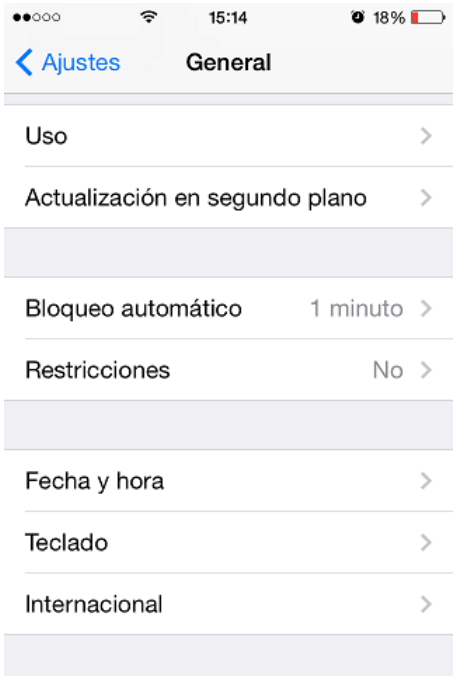
282. Para proceder a modificar el código de acceso al dispositivo móvil, en caso de disponer de un valor ya fijado, es necesario introducir el PIN o contraseña actual.

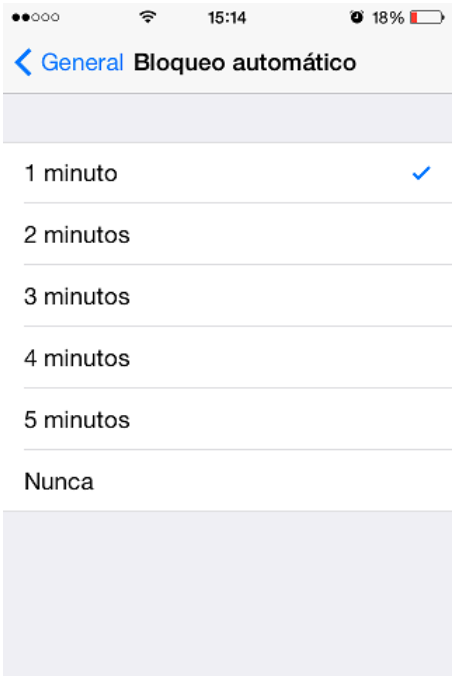
283. Una vez ha sido establecido el código, el dispositivo móvil solicitará al usuario el PIN o contraseña para desbloquear el acceso al terminal cada vez que esté bloqueado, como por ejemplo al encender el terminal o tras un tiempo de inactividad.

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

285. Se recomienda por tanto establecer el bloqueo del dispositivo móvil tras un tiempo de inactividad (primer ajuste), como por ejemplo 1 minuto (no tiene un valor por defecto establecido; opción "Nunca"). 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, pudiendo estar comprendido el valor entre 1 y 5 minutos en incrementos de un minuto.

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



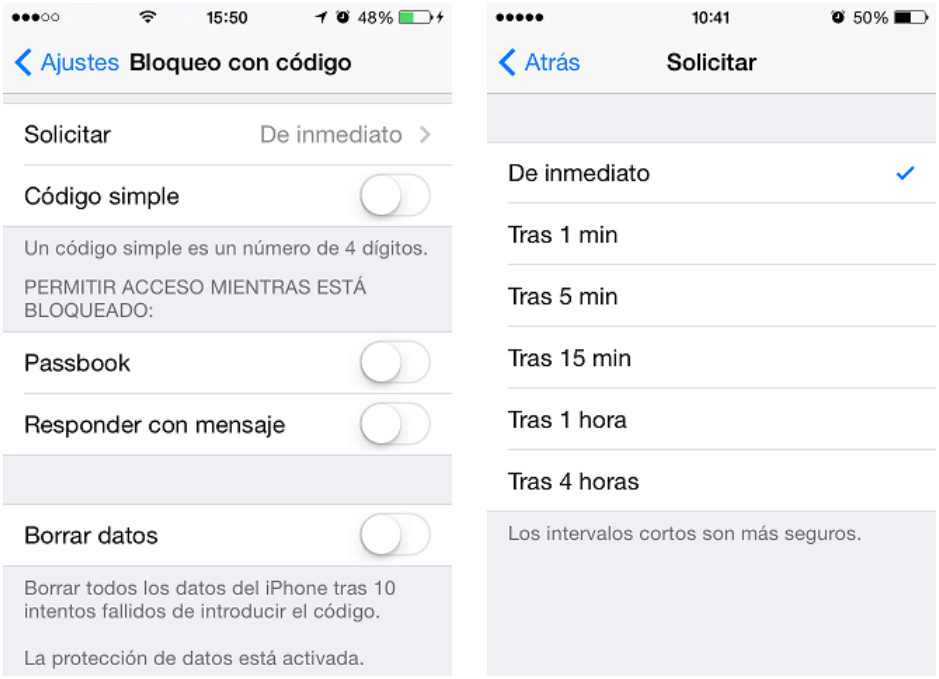


287. Adicionalmente, iOS dispone de una opción que permite que la pantalla nunca se bloquee independientemente del periodo de inactividad (opción desaconsejada desde el punto de vista de seguridad), disponible al seleccionar la opción "Nunca" para el periodo de tiempo.

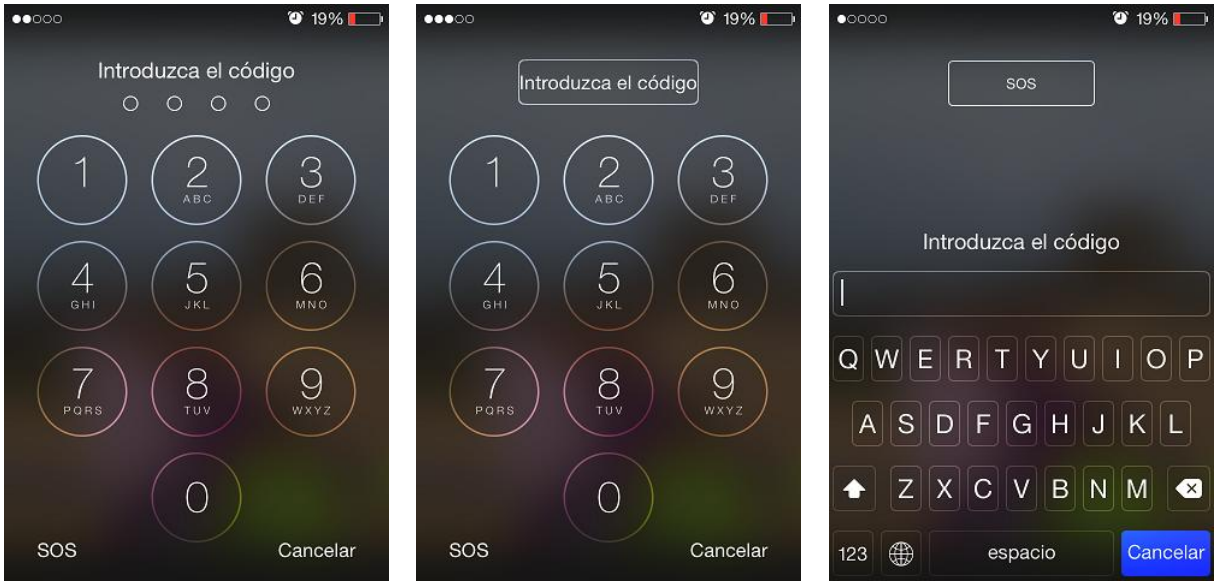
288. Por otro lado, el menú "Ajustes - Código" dispone de la opción "Solicitar", que permite definir cuánto tiempo esperará además el iPhone después de bloquearse para solicitar de nuevo el código de acceso que le permita volver a desbloquearse (segundo ajuste).

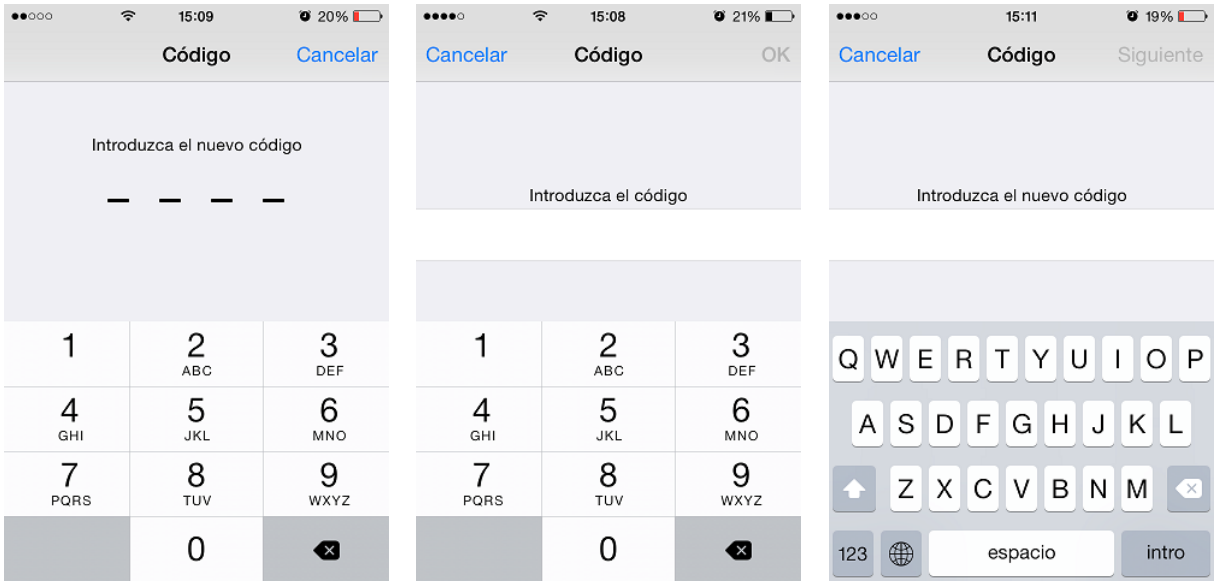
289. iOS permite elegir entre un minuto, 5, 15, una hora y cuatro horas. La opción recomendada desde el punto de vista de seguridad es "De inmediato", de forma que tan pronto se bloquee el dispositivo móvil por falta de actividad, o por haber sido apagada su

pantalla por parte del usuario manualmente, sea necesario introducir el código de acceso para volver a desbloquearlo:



290. Como se puede apreciar en las siguientes imágenes, la pantalla de desbloqueo de iOS permite diferenciar visualmente entre las dos configuraciones de desbloqueo del terminal, PIN (o código simple) y contraseña alfanumérica, lo que puede facilitar a un potencial atacante una primera aproximación al nivel de seguridad existente en el dispositivo móvil (tanto en la pantalla de acceso como en la interior de cambio del código de acceso):





291. Adicionalmente, estas pantallas también permiten diferenciar entre la utilización de un PIN (4 dígitos), al mostrarse únicamente cuatro casillas de entrada, o una contraseña compuesta únicamente por dígitos, por ejemplo 8 dígitos, al mostrarse una línea de entrada pero estar disponible únicamente el teclado numérico, o una contraseña alfanumérica, al mostrarse una línea de entrada y el teclado alfanumérico.

292. Desde el punto de vista de seguridad se recomienda habilitar una contraseña como código de acceso (no un código simple o PIN), que al menos haga uso de caracteres alfanuméricos, y preferiblemente de símbolos de puntuación, con una longitud mínima de al menos 6 u 8 caracteres.

293. 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 iOS (ver apartado “5.3. Gestión empresarial de dispositivos basados en iOS”).

294. Una vez fijados tanto el PIN en la tarjeta SIM como en el dispositivo móvil, al encender el terminal, el dispositivo móvil solicitará el código de acceso del terminal y después el de la tarjeta SIM ("Código PIN"), en este orden:

295. Pese a que la obligatoriedad de introducir dos códigos (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.

296. 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.

297. En caso de llevar a cabo una restauración de los datos del dispositivo móvil iOS de una copia de seguridad realizada previamente, el código de acceso no estará fijado inicialmente. El dispositivo móvil notificará al usuario la primera vez que accede al mismo tras la restauración, ofreciéndole la posibilidad de definir un código en ese instante.

5.4.3 TOUCH ID

298. Apple introduce habitualmente nuevas medidas de seguridad en los nuevos modelos de dispositivos móviles (*hardware*) y versiones de sistema operativo (*software*), como por ejemplo el lector biométrico o sistema de reconocimiento de huella dactilar del iPhone 5S, denominado Touch ID.

299. El lector o escáner de huella digital se encuentra integrado en el botón de "Home" del iPhone, para facilitar su utilización.

300. La representación digital biométrica de la huella dactilar del usuario (o *hash* de la huella) es almacenada en el nuevo coprocesador A7 disponible en estos nuevos modelos de dispositivos móviles, en concreto, en una memoria de sólo escritura. Esos datos no pueden ser supuestamente extraídos de dicho coprocesador debido a las protecciones hardware existentes, y no están accesibles para las apps o iCloud, ya que dicha memoria es empleada solamente para la validación del *hash* de la huella durante el proceso de autentificación.

301. Touch ID puede ser empleado para desbloquear el dispositivo móvil, así como para acceder al *keychain* local y poder hacer uso de este a la hora de realizar compras en la App Store, incluyendo tanto la App Store, como la iTunes Store y la iBooks Store (en lugar de emplear las credenciales asociadas al Apple ID del usuario). Es decir, se establece (por primera vez) una vinculación entre la huella dactilar del usuario (es decir, el mecanismo de autentificación del dispositivo móvil) y su Apple ID.

302. Durante el proceso de registro o configuración, el usuario debe proporcionar adicionalmente a la huella dactilar un código de acceso o desbloqueo de respaldo, que es utilizado en caso de que no sea posible leer la huella dactilar, con el objetivo de proteger el dispositivo móvil frente a distintos escenarios de uso inapropiado.

303. Los escenarios definidos por defecto por Apple imponen la necesidad de introducir el código de desbloqueo la primera vez que el dispositivo móvil arranca, así como después de 48 horas si el dispositivo no ha sido desbloqueado durante ese tiempo. Adicionalmente, si no es posible leer la huella dactilar tras cinco intentos de acceso fallidos, se solicitará al usuario el código de desbloqueo de respaldo. También será

necesario emplear el código de acceso para registrar nuevas huellas dactilares en Touch ID, así como para desbloquear el dispositivo móvil si éste ha sido bloqueado remotamente a través de la solución MDM o de iCloud.

304. En cualquier caso, el usuario puede decidir hacer uso del código de acceso en lugar de la huella dactilar en cualquier momento.

305. Touch ID permite registrar hasta cinco huellas dactilares diferentes para desbloquear el dispositivo móvil [Ref.- 148].

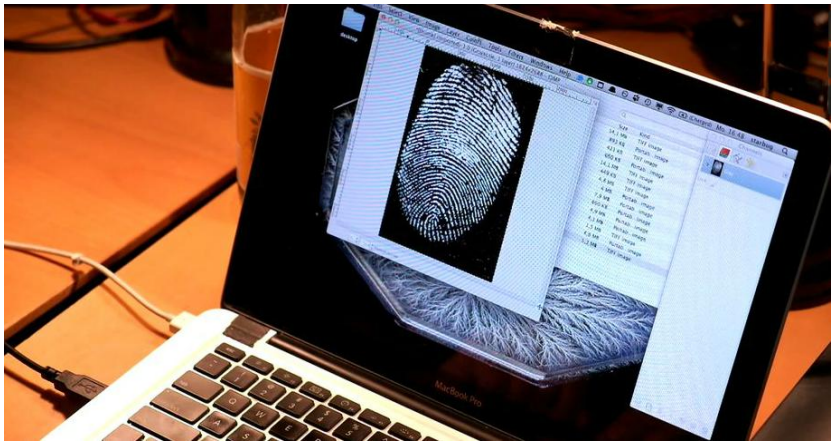
306. El objetivo principal de Touch ID (reflejado en su diseño y restricciones de uso) es promover entre los usuarios la utilización de algún mecanismo de bloqueo del dispositivo móvil, e incrementar su adopción debido a su facilidad de uso, ya que según las estadísticas proporcionadas por Apple durante su anuncio en la conferencia WWDC del año 2013, un 50% de los usuarios no tienen establecido ningún mecanismo de protección de acceso en sus dispositivos móviles.

307. Asimismo, si Touch ID está habilitado el dispositivo móvil se bloqueará automáticamente al entrar en modo reposo o al apagar la pantalla, no aplicando el periodo de gracia configurado en los ajustes para determinar cuándo es necesario introducir de nuevo el código de acceso.

308. Los mecanismos de gestión empresarial de iOS 7, en el caso de dispositivos móviles con Touch ID, como el iPhone 5S, permiten definir una política en la solución MDM para permitir o denegar el uso de Touch ID.

309. Sin embargo, la comunidad de seguridad continua encontrando mecanismos para evitar estas medidas de seguridad, publicando incluso desafíos y premios para motivar o potenciar su investigación. Al día siguiente de la comercialización del iPhone 5S, un investigador del grupo alemán CCC publicó la metodología empleada para saltarse el proceso de autentificación empleando una réplica de la huella dactilar del usuario generada a partir de de las propias huellas existentes en el dispositivo móvil tras su uso habitual [Ref.- 160].

310. El proceso se basa en exponer la huella a polvo de grafito, escanear o tomar una fotografía en alta resolución de la misma, procesar la imagen con un editor gráfico para dejar sólo la huella, en blanco y negro, rotarla en el eje horizontal e invertir sus colores. Posteriormente, se imprime la imagen en una hoja transparente a la escala adecuada, y se usa para cubrir un material fotosensible (PCB, *printed circuit board*). Tras exponer el PCB a luz ultravioleta, se alterará la composición química del material en función de la imagen, creando un molde con relieve con las características y particularidades de la huella. El molde es tratado para que el material pueda ser reutilizado en múltiples ocasiones y tenga propiedades conductivas. Tras aplicar sobre el PCB cola blanca de madera o látex y dejarlo secar, se obtiene una réplica de la huella original que puede ser empleada para suplantar al usuario y desbloquear el sistema Touch ID:



311. Por tanto, no debe depositarse demasiada confianza en los mecanismos de autentificación basados en biometría, y en el caso de ser utilizados a nivel empresarial, deben constituir un complemento a los mecanismos de autentificación tradicionales definidos en la política de seguridad de los dispositivos móviles.

5.4.4 RESTAURACIÓN REMOTA DEL CÓDIGO DE ACCESO

312. A través de las capacidades empresariales para la gestión de dispositivos móviles basados en iOS proporcionadas por Apple, y en concreto a través del servicio "Buscar mi iPhone" (ver apartado “5.22. Localización del dispositivo móvil: Buscar mi iPhone”), en versiones previas de iOS (< 4.x) a través del servicio Mobile Me, si el código de acceso era de 4 caracteres (o menos), era posible de forma remota seleccionar y por tanto restaurar el valor del código de acceso [Ref.- 59].

313. En versiones de iOS 4.x (o posteriores) no es posible llevar a cabo de forma remota la restauración (o restablecimiento) del código de acceso y desbloqueo del dispositivo móvil. Únicamente se puede activar de forma remota el código de acceso ya existente, o en el caso de no disponer previamente de un código de acceso (opción desaconsejada desde el punto de vista de seguridad), fijar el valor de un nuevo código de acceso.

5.4.5 VULNERABILIDADES DE DESBLOQUEO DE IOS

314. iOS ha presentado a lo largo del tiempo y de sus múltiples versiones numerosas vulnerabilidades en la pantalla de desbloqueo, protegida por un código de acceso. A continuación se analizan algunas de las más recientes vulnerabilidades que afectan a la versión de iOS bajo estudio.

315. Durante el 2011 se descubrieron dos nuevas vulnerabilidades relacionadas con el acceso físico al terminal y el desbloqueo no autorizado de iOS, afectando a los últimos modelos de dispositivos móviles de Apple: el iPhone 4S y el iPad 2.

Nota: Esta sección incluye vulnerabilidades que han afectado tanto a dispositivos móviles iOS iPhone como iPad con el objetivo de ejemplificar la criticidad y diversidad de las mismas, pese a disponerse de documentos independientes de seguridad para ambos dispositivos [Ref.- 127] [Ref.- 137].

316. Ambas vulnerabilidades están asociadas a nuevas funcionalidades añadidas por Apple: Siri (sistema de reconocimiento de voz; ver apartado "5.17.3. Siri") [Ref.- 40] y la funda SmartCover del iPad2 [Ref.- 41] (CVE-2011-3440).

317. Si un iPhone 4S está bloqueado y protegido por un código de acceso, Siri aún permite acceder a parte de la funcionalidad del teléfono mediante comandos de voz, y por ejemplo, enviar mensajes de texto o e-mails (a destinatarios existentes en la lista de contactos), realizar llamadas, y acceder al calendario o a los contactos. Una vulnerabilidad, o funcionalidad extendida, similar era conocida desde 2009 en el sistema de control de voz (antecesor de Siri) del iPhone 3GS.

318. Se recomienda por tanto deshabilitar la funcionalidad de Siri cuando el dispositivo móvil está bloqueado, pudiendo hacer uso de Siri tras desbloquear el terminal.

319. Una vez Siri ha sido habilitada (deshabilitada por defecto), esta funcionalidad puede ser deshabilitada en iOS 5.x desde el menú “Ajustes – General – Bloqueo con código”, mediante la opción “Siri" (habilitada por defecto), qué reemplaza a la opción "Marcación por voz” (ver imagen inferior izquierda):

320. En caso de que Siri no haya sido habilitada, el dispositivo móvil no será vulnerable y no se dispondrá de la opción para deshabilitar su uso mientras el dispositivo móvil está bloqueado; en su lugar se muestra la opción de “Marcación por voz” existente en versiones previas de iOS, hasta iOS 7.0.x (ver imagen superior derecha).

321. Por otro lado, si un iPad 2 está bloqueado y se inicia el proceso de apagado, al abrir la SmartCover y cancelar el proceso de apagado, el dispositivo no solicita el código de acceso y permite control completo de la última aplicación en ejecución y de sus datos asociados.

322. Es posible evitar esta vulnerabilidad deshabilitando el desbloqueo mediante SmartCover a través del menú “Ajustes – General – (Des)bloqueo mediante tapa” (habilitado por defecto). La versión 5.0.1 de iOS resolvió la vulnerabilidad de acceso no autorizado mediante SmartCover [Ref.- 6].

323. Estos escenarios permiten a un atacante acceder a información privada simplemente disponiendo de acceso físico temporal al dispositivo móvil, y demuestran los riesgos de

seguridad asociados a las nuevas funcionalidades y tecnologías añadidas a los dispositivos móviles.

324. Adicionalmente, la funcionalidad de acceso rápido a la cámara (disponible desde la pantalla de bloqueo mediante el icono de cámara en la parte inferior derecha) no puede deshabilitarse desde iOS 5.x (y versiones posteriores) y permite realizar fotografías (o vídeos) qué podrían ser comprometedoras cuando el dispositivo móvil está bloqueado y sin necesidad de conocer el código de acceso.

325. El impacto de la realización de fotografías comprometedoras es aún mayor si se tienen en cuenta las nuevas capacidades automáticas de sincronización de fotografías (últimas 1.000 fotos) entre diferentes dispositivos móviles iOS ("photo streaming") a través de iCloud.

326. Para ello una persona con acceso físico al dispositivo móvil bloqueado sólo debe pulsar en la parte inferior derecha de la pantalla de desbloqueo el botón de acceso rápido a la cámara (ver imagen inferior izquierda).

327. Pulsando dicho botón podrá acceder directamente a la aplicación de cámara del dispositivo móvil y realizar fotografías o vídeos. Al estar el dispositivo móvil bloqueado no es posible acceder a las fotografías o vídeos existentes previamente y almacenadas en el mismo, situación indicada por el mensaje de las imágenes inferiores. Únicamente se tiene acceso a las fotografías realizadas mientras el dispositivo está bloqueado:

328. La única opción para bloquear el acceso a la cámara desde la pantalla de desbloqueo en iOS es mediante la opción de imponer restricciones en el uso de la cámara. Desde el menú "Ajustes - General - Restricciones" es posible activar esta protección y no permitir el uso de la cámara, lo que deshabilitará también FaceTime. Al restringir el uso de la cámara, se restringe completamente el acceso a la aplicación asociada (no sólo en la pantalla de desbloqueo), desapareciendo el icono que da acceso a la misma de la pantalla principal del dispositivo móvil.

329. Igualmente, iOS dispone por defecto de la capacidad de actuar como un marco de fotos digital en el caso concreto de dispositivos móviles iPad, siendo posible desde la pantalla de desbloqueo y a través del icono asociado situado en la parte inferior derecha, hacer que el dispositivo móvil muestre una secuencia de las fotos qué contiene.

330. Si la vulnerabilidad detallada anteriormente permitía a alguien con acceso físico al mismo almacenar nuevas fotos en el dispositivo móvil, ésta permite la operación contraria, es decir, acceder a las fotos almacenadas en el dispositivo móvil.

331. La opción puede ser deshabilitada en iOS 5.x e iOS 6.x a través del menú "Ajustes - General - Bloqueo con código", mediante la opción "Marco de fotos" (habilitada por defecto):

332. En iOS 7 la funcionalidad del marco de fotos del iPad ha sido eliminada por Apple, siendo necesario hacer uso de las capacidades de acceso guiado ("Ajustes - General - Accesibilidad - Acceso Guiado", junto al "Pase de diapositivas" de la aplicación de "Fotos") si se quiere emplear el dispositivo móvil como marco de fotos digital.

333. Por otro lado, en febrero de 2012 se publicó una vulnerabilidad que afectaba a iOS 5.0.1 y que permitía a un atacante, con acceso físico al dispositivo móvil, utilizar la aplicación de teléfono de iPhone, con acceso a los números de teléfono favoritos, las llamadas recientes (pérdidas o todas), la lista de contactos, el buzón de voz, etc, e incluso realizar llamadas desde un dispositivo móvil protegido con código de acceso [Ref.- 60].

334. La vulnerabilidad es debida a una condición de carrera (*race condition*) del proceso de desbloqueo del terminal, por ejemplo en el acceso a través de la notificación de una llamada recibida (desde la pantalla de desbloqueo o previsualización) y la búsqueda de la red del operador de telefonía móvil por parte del dispositivo móvil basado en iOS (por ejemplo, tras extraer e insertar la tarjeta SIM).

335. La vulnerabilidad parece ser explotable si la tarjeta SIM no está protegida por un código PIN, ya que en caso contrario será necesario conocer el PIN para que el dispositivo proceda a buscar la red del operador de telefonía móvil.

336. En 2012 también se publicó una nueva vulnerabilidad que afectaba a la pantalla de desbloqueo de iOS 5.0.1 (iPhone) y permitía realizar llamadas mediante FaceTime sin autorización.

337. Para ello el usuario no autorizado sólo debe disponer de acceso físico al dispositivo móvil iOS, acceder a la pantalla de bloqueo, y acceder desde allí a la pantalla para realizar llamadas de emergencia. Desde la misma, y manteniendo pulsado el botón de inicio o "Home" se activará el control por voz.

338. Pese a que el control por voz para la realización de llamadas esté deshabilitado en el menú "Ajustes - General - Bloqueo con código", y en concreto en la opción "Marcación por voz" (disponible al no hacer uso de Siri), era posible iniciar llamadas a través de FaceTime (video conferencia) [Ref.- 111] (ejemplo de la versión iOS 5.x afectada):

339. Adicionalmente esta vulnerabilidad permite a través de los comandos de voz, enumerar la existencia de personas concretas en la lista de contactos del dispositivo móvil.

340. Finalmente, la versión 5.1 de iOS [Ref.- 61] soluciona dos vulnerabilidades diferentes relacionadas con la pantalla de desbloqueo. La primera es debida a una condición de carrera (*race condition*) en el proceso de desbloqueo de iOS (CVE-2012-0644) al realizar el gesto de deslizamiento para realizar una llamada.

341. La segunda permite enviar a cualquier destinatario el mensaje que se encuentra actualmente abierto en la aplicación Mail desde la pantalla de desbloqueo a través de Siri, empleando un comando de voz. Para ello es necesario que la aplicación de Mail esté activa (tras la pantalla de desbloqueo) y disponga de un mensaje seleccionado (CVE-2012-0645). La vulnerabilidad se debe a la ausencia de restricciones de la aplicación Mail para recibir y realizar acciones a través de los mensajes de voz.

342. Los múltiples y diferentes ejemplos de vulnerabilidades que han afectado a la pantalla de desbloqueo de iOS descritos previamente en esta sección sólo constituyen un pequeño subconjunto del conjunto total de vulnerabilidades que han afectado a esta funcionalidad, crítica desde el punto de vista de seguridad, en las últimas versiones de iOS (5.x, 6.x y 7.x) a lo largo de los últimos años.

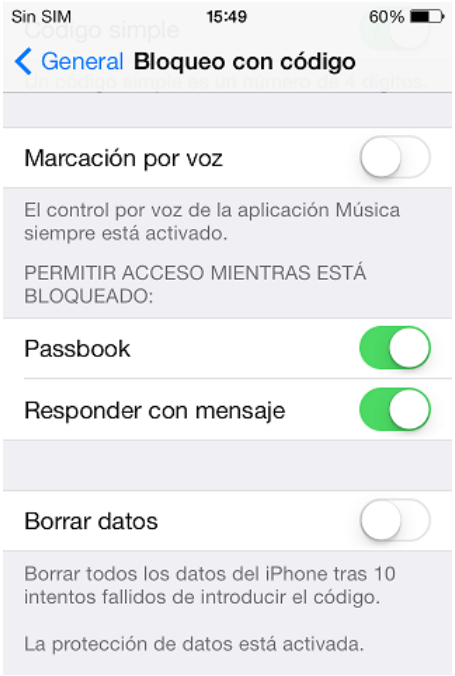
343. Se han contabilizado 9 vulnerabilidades que afectan a la pantalla de desbloqueo en iOS 5.x, 8 vulnerabilidades en iOS 6.x y 10 vulnerabilidades en iOS 7.x.

344. Todo este conjunto de vulnerabilidades refleja la importancia de la seguridad física en los dispositivos móviles, impidiendo el acceso físico no autorizado a terceros, así como la de mantener el dispositivo actualizado a la última versión proporcionada por el fabricante.

5.4.6 MARCACIÓN POR VOZ

345. Algunas de las vulnerabilidades mencionadas sobre la pantalla de desbloqueo de iOS involucran a Siri (ver apartado "5.17.3. Siri") o la funcionalidad previa de marcación por voz.

346. Hasta la versión 7.1 de iOS era posible deshabilitar las capacidades de marcación por voz, incluso en la pantalla de desbloqueo, a través del menú "Ajustes - General - Bloqueo con código" y deshabilitando la opción "Marcación por voz" (ejemplo de iPhone 7.0.x):



347. Una vez deshabilitado, no es posible hacer uso de esta funcionalidad tras mantener pulsado el botón Home durante unos segundos en la pantalla de desbloqueo.

348. A partir de iOS 7.1, la opción de configuración de marcación por voz ha desaparecido del área correspondiente bajo el menú "Ajustes - Código" y, por tanto, esta funcionalidad no puede ser deshabilitada.

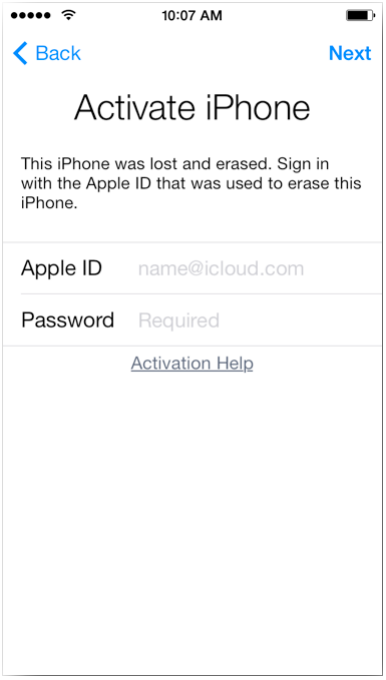
349. La opción de deshabilitar "VoiceOver" a través del menú "Ajustes - General - Accesibilidad" no está relacionada con las capacidades de marcación por voz, e incluso estando desactivada (opción por defecto), la funcionalidad está activa.

350. Esta ausencia de capacidades en la configuración de iOS 7.1.x es complementaria a la carencia previamente mencionada a la hora de deshabilitar el acceso rápido a la cámara desde la pantalla de desbloqueo de iOS, no siendo posible desactivar ambas funcionalidades (en el caso de marcación por voz ni siquiera a través de las restricciones).

5.5 RESTRICCIONES EN EL PROCESO DE ACTIVACIÓN

351. En iOS 7 Apple proporcionó un nuevo proceso de activación de los dispositivos móviles, con el objetivo de disuadir a ladrones interesados en el robo del terminal y en su posterior reventa. El robo y reventa de dispositivos móviles de alta gama, especialmente de Apple, se ha convertido en una actividad delictiva en alza, muy lucrativa y bastante común y frecuente a día de hoy, especialmente en ciertas ciudades a nivel mundial, como por ejemplo Nueva York [Ref.- 154].

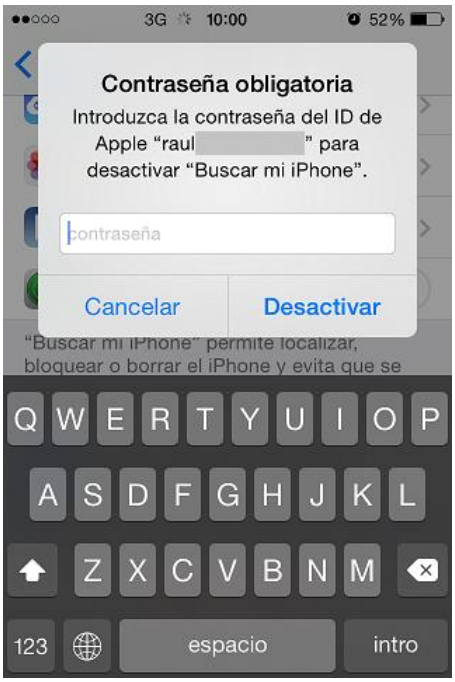
352. Un dispositivo móvil iOS que está bloqueado y ha sido borrado (*wipe*) no puede ser restaurado o reactivado sin las credenciales (Apple ID) de su usuario (previo). Esta protección en el proceso de activación se habilita tanto si el borrado se ha realizado remotamente como si se ha producido tras varios intentos de acceso fallidos:



353. La funcionalidad de bloqueo del proceso de activación se activa automáticamente [Ref.- 155] al habilitar las capacidades de localización del dispositivo a través de la funcionalidad "Find My iPhone" ("Buscar mi iPhone"), disponible desde el menú "Ajustes - iCloud - (Autentificándose) - Buscar mi iPhone" (ver apartado "5.22. Localización del dispositivo móvil: Buscar mi iPhone"):

354. Esta nueva protección evita también que se pueda desactivar la app "Buscar mi iPhone", que se desvincule el dispositivo de iCloud, junto a las restricciones ya mencionadas de que sea borrado y reactivación [Ref.- 156].

355. A la hora de restaurar el dispositivo móvil a sus ajustes de fábrica y eliminar todos los datos existentes, a través del menú "Ajustes - General" y la opción "Restablecer", o a la hora de desactivar la funcionalidad de "Buscar mi iPhone", a través del menú "Ajustes - iCloud" y el botón "Buscar mi iPhone", y también si se intenta borrar la cuenta de iCloud a través del menú "Ajustes - iCloud" y el botón "Eliminar cuenta", se mostrará un mensaje al usuario solicitando la contraseña asociada a su Apple ID. En el caso de no disponer de ella, la acción no podrá ser llevada a cabo:



356. En febrero de 2014 se publicó una vulnerabilidad (CVE-2014-2019) que permitía deshabilitar la funcionalidad de "Buscar mi iPhone" sin conocer las credenciales de iCloud (o Apple ID) del usuario asociado [Ref.- 161].

357. Mediante la modificación de la contraseña de iCloud por un valor incorrecto y la eliminación de la descripción asociada a la cuenta, es posible deshabilitar la funcionalidad "Buscar mi iPhone" e incluso eliminar la cuenta de iCloud.

358. Esta vulnerabilidad fue solucionada por Apple en iOS 7.1. Si el dispositivo móvil está protegido por un código de acceso, no es posible disponer de acceso a los ajustes del terminal para poder explotar dicha vulnerabilidad.

359. Una vez el usuario no dispone del dispositivo móvil físicamente, por haber sido perdido o robado, es necesario ponerlo en modo perdido ("Lost Mode", disponible desde iOS 6.x) a través de "Buscar mi iPhone" desde iCloud [Ref.- 157]. Este proceso bloqueará el dispositivo con un código de acceso (el existente actualmente) y permite mostrar un mensaje de recuperación (incluyendo por ejemplo un número de teléfono del propietario) en la pantalla de bloqueo por si alguien lo encuentra.

360. En el caso de almacenar datos confidenciales en el dispositivo móvil, se recomienda llevar a cabo un borrado remoto (*wipe*) y, pese a haber ejecutado dicha acción, el dispositivo seguirá mostrando el mensaje de recuperación en la pantalla.

361. Pese a que este mecanismo de protección puede hacer que disminuya la amenaza de robo de dispositivos móviles Apple, también podría producir un cambio en el procedimiento empleado para robar el terminal, donde el delincuente puede exigir al propietario del terminal que lo desbloque con su Apple ID antes de perpetrar el robo.

362. En el caso de querer vender o reasignar el dispositivo móvil a otro usuario, y permitir que el nuevo usuario pueda activar y hacer uso del dispositivo, la opción recomendada pasa por restablecer en el dispositivo los ajustes de fábrica, a través del menú "Ajustes - General - Restablecer - Borrar contenidos y ajustes". Este proceso eliminará todos los datos del terminal, deshabilitará la funcionalidad "Buscar mi iPhone", y eliminará la cuenta de iCloud previamente asignada al dispositivo [Ref.- 158].

363. Por tanto, los procesos y procedimientos empresariales establecidos para la devolución de un dispositivo móvil iOS por parte de un empleado (por ejemplo, en el caso de dejar la organización) deben tener en cuenta estas nuevas capacidades y obligar al usuario a restablecer los ajustes de fábrica en el dispositivo móvil antes de devolverlo a la organización para su reutilización por parte de otro empleado.

364. En mayo de 2014, se publicó una solución para llevar a cabo el desbloqueo de los terminales de Apple sin conocer el Apple ID del usuario (previo), denominada doulCi [Ref.- 159], que elude los mecanismos de protección previamente descritos. doulCi permite evitar el bloqueo del proceso de activación mediante un servidor de iCloud alternativo, que debe ser referenciado mediante la modificación de la resolución de nombres hacia el servidor de activación legítimo de Apple, "albert.apple.com", al llevar a cabo la activación del dispositivo móvil mediante iTunes.

365. Las capacidades de bloqueo del proceso de activación están deshabilitadas por defecto únicamente para dispositivos móviles iOS supervisados, pero pueden ser habilitadas de nuevo a través de la solución de gestión empresarial (MDM).

366. En el caso de no querer hacer uso de estas capacidades o funcionalidad en entornos corporativos sin dispositivos supervisados, no hay una alternativa viable, pese a que sí se puede ver si el bloqueo del proceso de activación está o no activo para un dispositivo móvil concreto. Esto obliga a establecer procedimientos detallados para evitar que los dispositivos acaben siendo bloqueados e inútiles si un usuario no proporciona sus credenciales o identificador de Apple (Apple ID).

5.6 PANTALLA DE DESBLOQUEO: PREVISUALIZACIÓN DE DATOS

367. La pantalla de desbloqueo del terminal (*lock screen*) en iOS permite, sin necesidad de introducir el código 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.

368. Adicionalmente, la pantalla muestra las llamadas de teléfono recibidas, siendo posible visualizar el remitente (el número de teléfono del remitente o su nombre si existe en la lista de contactos) e incluso devolver la llamada, sin conocer el código de desbloqueo, deslizando el dedo sobre la notificación de llamada perdida, con las implicaciones de seguridad asociadas que tiene el poder realizar una llamada desde un dispositivo móvil sin autorización, suplantando a su usuario:

369. También la pantalla de previsualización permite visualizar los mensajes de texto (SMS, iMessage, etc) recibidos, incluyendo el texto (casi completo) de los mismos (no únicamente el texto inicial), que en el caso de contener información confidencial, privada o sensible estaría disponible para cualquier persona con acceso físico al dispositivo móvil:

370. En el caso de los mensajes de texto, para acceder a los mismos y poder responderlos, es necesario conocer el código de acceso (a diferencia de como ocurre con las llamadas de voz).

371. Igualmente, si se reciben otras notificaciones posteriormente y no se ha realizado ningún intento de desbloqueo en el dispositivo móvil desde su recepción, se dispondrá de acceso desde la pantalla de previsualización al contenido de todos los mensajes, incluyendo las notificaciones recibidas inicialmente:

372. La información disponible a través de las notificaciones en la pantalla de desbloqueo se extiende a otros elementos y aplicaciones de iOS, como por ejemplo recordatorios,

notificaciones del calendario, mensajes de correo electrónico (incluyendo el asunto y remitente), etc.

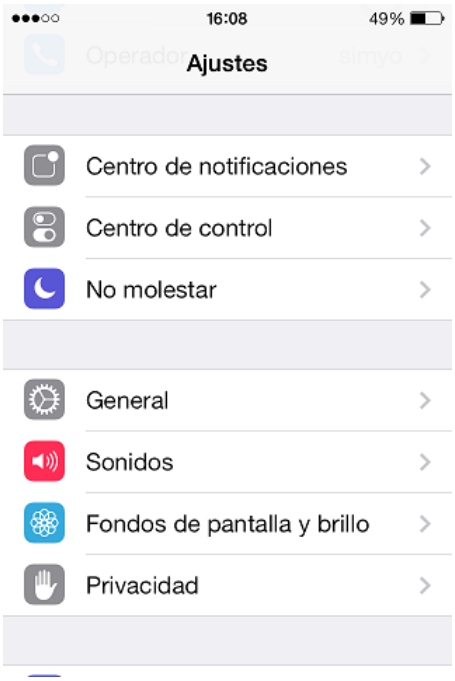
373. La pantalla de desbloqueo puede desvelar por tanto información confidencial a un potencial atacante, ya que esta funcionalidad de previsualización podría permitir a un potencial atacante la lectura de información sensible simplemente con poder tener acceso visual a la pantalla del dispositivo.

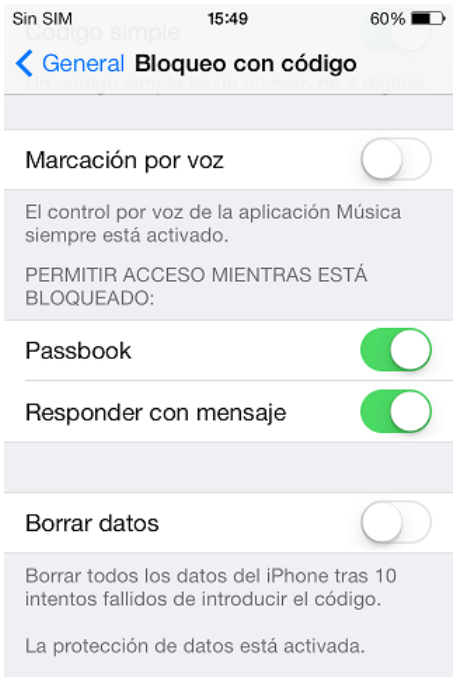
374. La información permanece en la pantalla de desbloqueo o previsualización hasta que se complete con éxito el desbloqueo del dispositivo móvil.

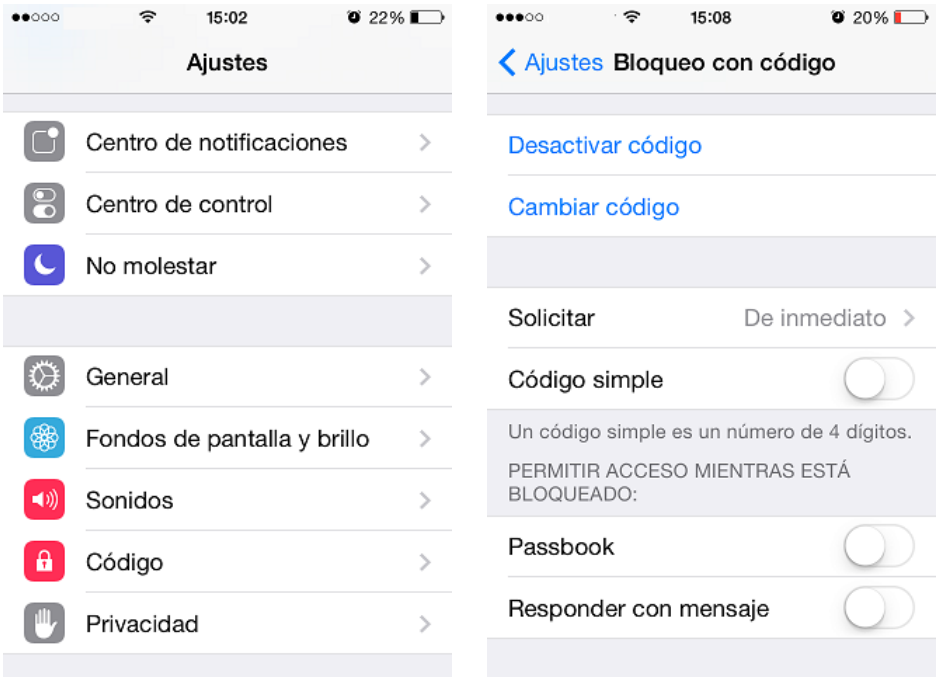
375. Incluso tras haberse desbloqueado el dispositivo móvil al menos en una ocasión, existe la posibilidad en iOS 7 de seguir disponiendo de acceso a dichas notificaciones a través del Centro de Notificaciones (ver apartado "5.6.2. Centro de Notificaciones").

5.6.1 ACCESOS MIENTRAS EL DISPOSITIVO MÓVIL ESTÁ BLOQUEADO

376. En iOS 7, tanto desde el menú "Ajustes - General - Bloqueo con código" de iOS 7.0.x, como desde el menú "Ajustes - Código" de iOS 7.1.x, es posible definir a que aplicaciones y funcionalidad se permitirá el acceso mientras el dispositivo móvil está bloqueado (ejemplos de ambas versiones, iOS 7.0.x e iOS 7.1.x):







377. Por defecto en el caso del iPhone, iOS dispone de dos entradas correspondientes a la app Passbook, y a la posibilidad de responder la recepción de una llamada con un mensaje. Ambas opciones están activas por defecto.

378. Desde el punto de vista de seguridad, si no se desea que un tercero pueda disponer de acceso a Passbook o responder con un mensaje, se recomienda deshabilitar ambas opciones.

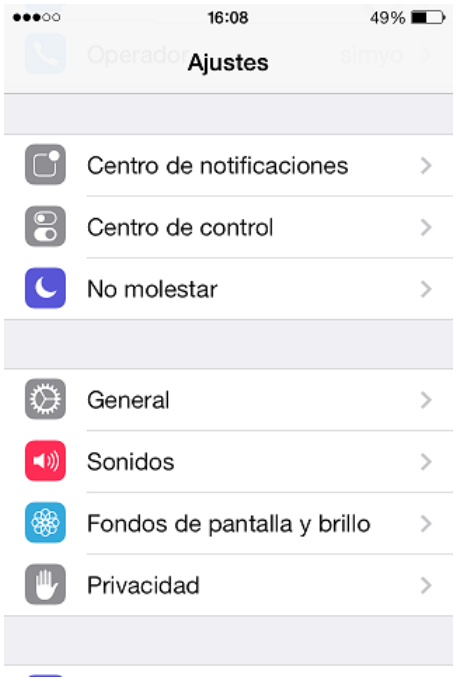
5.6.2 CENTRO DE NOTIFICACIONES

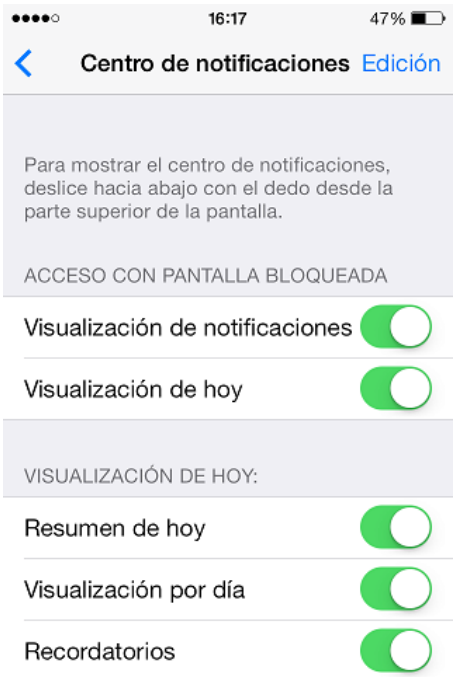
379. El Centro de Notificaciones ya existía en iOS desde la versión 5 como un lugar centralizado para la obtención de mensajes y notificaciones de la plataforma y de las apps, y con capacidades para gestionar qué aplicaciones podían mostrar notificaciones y en qué formato. El nuevo Centro de Notificaciones introducido por Apple en iOS 7 permite disponer de más información, incluso desde la pantalla de desbloqueo, y configurar más aspectos asociados a su funcionamiento.

380. El Centro de Notificaciones desde la versión 7 de iOS está accesible al desplazar hacia abajo la parte superior de la pantalla de iOS, por defecto tanto en la pantalla de bloqueo como una vez el dispositivo móvil ha sido desbloqueado, e incluye tres categorías: Hoy, Todo y No visto.

381. Cada categoría permite acceder a un subconjunto o al conjunto completo de notificaciones, ya visualizadas o pendientes, como su propio nombre indica.

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





383. En primer lugar, se recomienda gestionar si se desea disponer del Centro de Notificaciones en la pantalla de desbloqueo, accesible sin conocer el código de acceso.

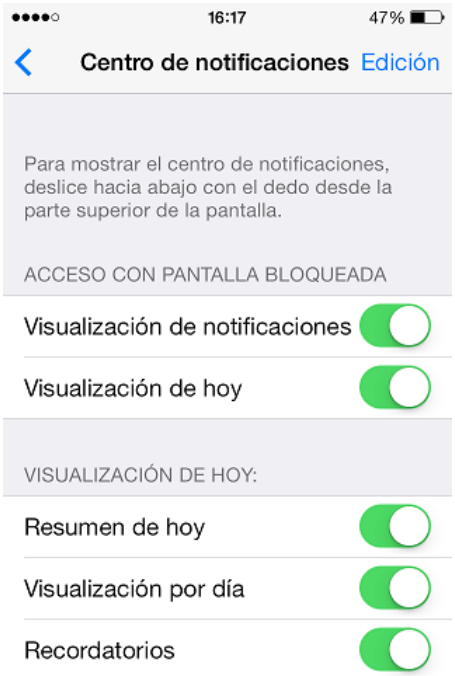
384. Desde el punto de vista de seguridad se recomienda deshabilitar el Centro de Notificaciones si la pantalla está bloqueada a través de la opción "Visualización de notificaciones" desde el menú "Ajustes - Centro de notificaciones".

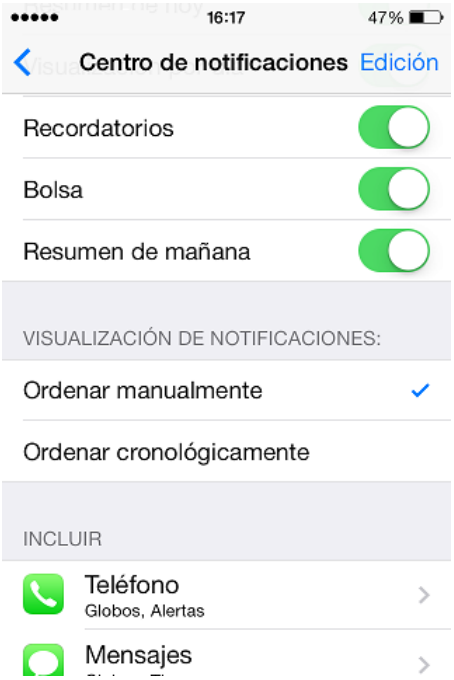
385. Aunque esta configuración afecta a la funcionalidad del dispositivo móvil, evita que un tercero no autorizado pueda acceder a todos los detalles de las notificaciones existentes con sólo disponer de acceso temporal al dispositivo móvil, incluso por un breve espacio de tiempo.

386. Este cambio de configuración afecta a las categorías "Todo" y "No visto", estando aún disponible la información asociada a la categoría "Hoy". Para deshabilitar por completo la información de notificaciones desde la pantalla de desbloqueo es necesario también deshabilitar la opción "Visualización de hoy" del menú "Ajustes - Centro de notificaciones":

387. La ausencia de una pequeña barra horizontal en la parte central y superior de la pantalla de desbloqueo indica visualmente que no se dispone de ningún tipo de acceso al Centro de Notificaciones desde la misma.

388. Por otro lado, los ajustes de configuración del Centro de Notificaciones permiten seleccionar qué componentes o módulos serán mostrados en la pantalla de "Hoy", incluyendo el resumen del día, el siguiente destino, la visualización por día, los recordatorios, la información de bolsa y el resumen del día siguiente, todos ellos habilitados por defecto:

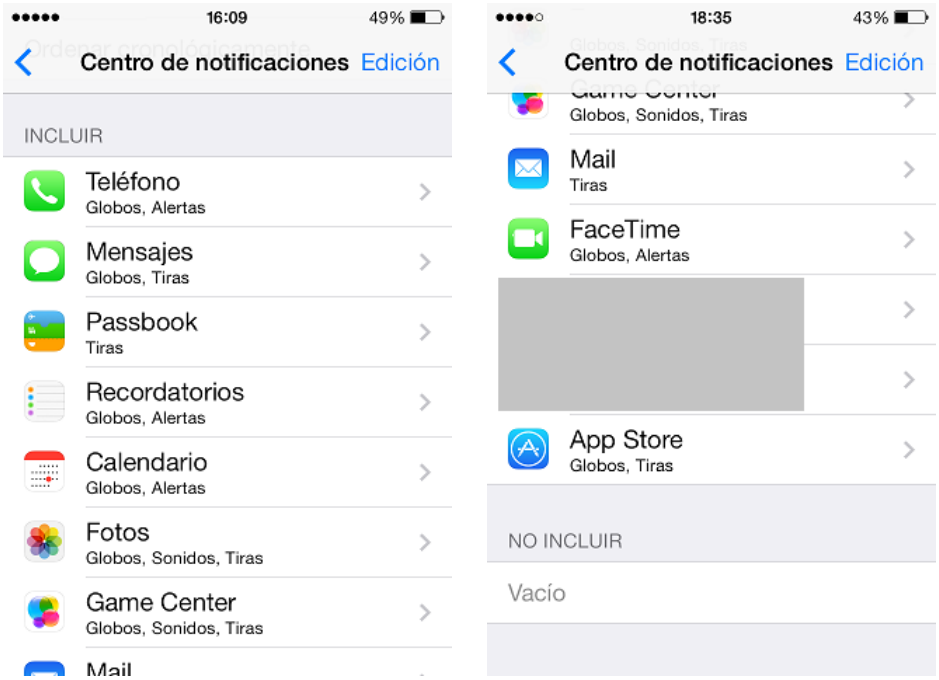




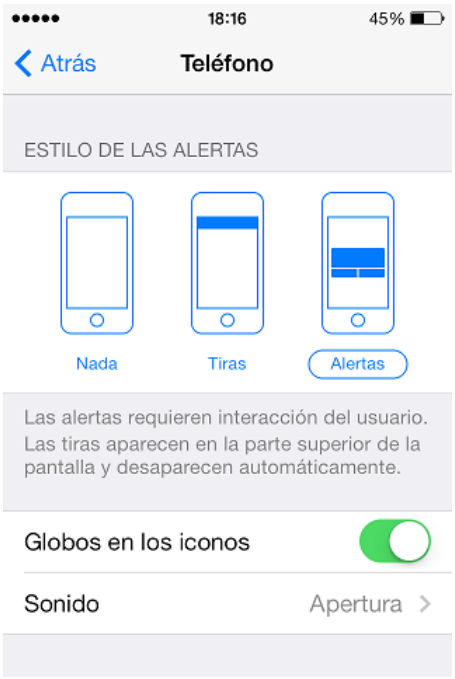
389. Asimismo, las notificaciones pueden ser ordenadas manualmente o cronológicamente.

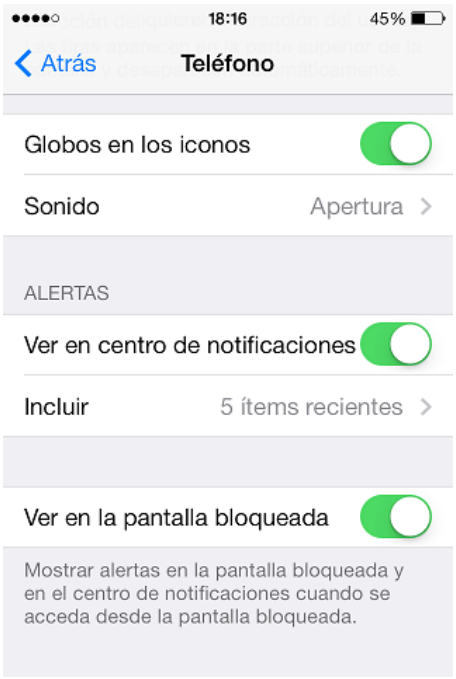
390. Por otro lado, es necesario gestionar de manera granular qué aplicaciones podrán generar notificaciones, y el formato empleado por cada una de éstas.

391. Para cada aplicación que genere mensajes de notificación, tanto nativas de iOS como de terceros (instaladas posteriormente por el usuario desde la App Store), es posible ajustar su configuración, incluyendo si se añade al centro de notificaciones (es decir, si se habilitan sus capacidades de notificación), en cuyo caso aparecerá bajo la sección "Incluir" en el Centro de Notificaciones (o bajo la sección No Incluir" en caso contrario):



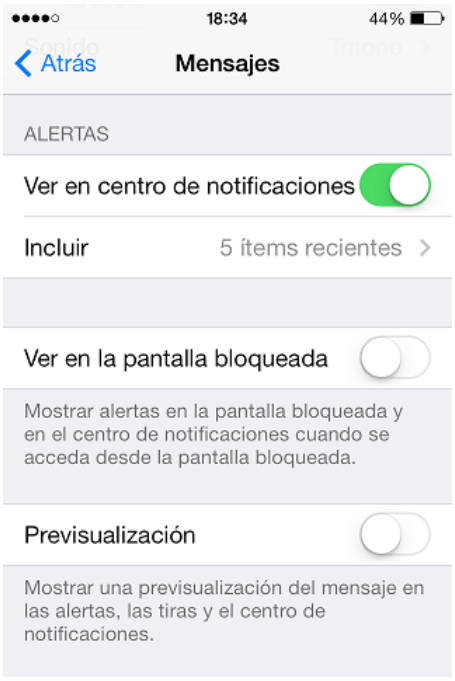
392. Para cada una de las aplicaciones habilitadas en el Centro de Notificaciones es posible configurar diferentes parámetros en función de la aplicación. Por ejemplo, para las aplicaciones de teléfono y mensajes (comentadas previamente al describir la pantalla de desbloqueo), es posible establecer el estilo de las alertas (ninguno, tiras o alertas), si se emplearán globos en el icono de la aplicación para indicar el número de notificaciones pendientes, si se reproducirá un sonido y cuál será, si la información de sus notificaciones asociadas estará disponible en el Centro de Notificaciones, el número de notificaciones recientes que se mostrarán (1, 5 (por defecto) ó 10) y si dichas notificaciones se podrán previsualizar cuando la pantalla del dispositivo móvil está bloqueada, y también cuando se accede al Centro de Notificaciones cuando la pantalla está bloqueada:

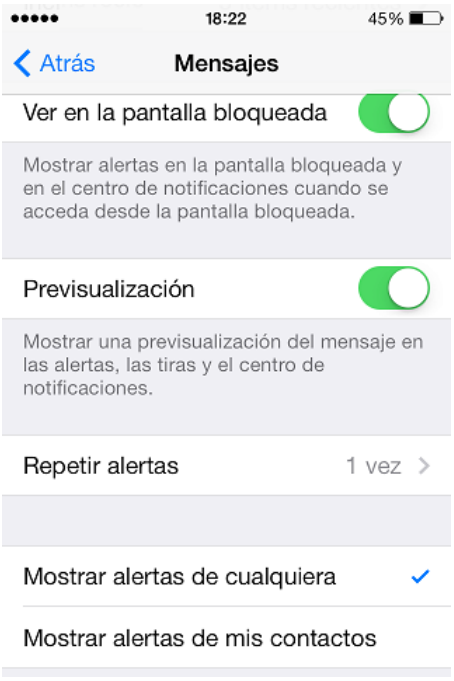




393. Por ejemplo, por defecto, la aplicación de teléfono muestra las últimas 5 notificaciones en forma de alertas, empleando también globos, con un sonido por defecto, permaneciendo disponibles tanto en la pantalla de desbloqueo como en el Centro de Notificaciones (con y sin la pantalla bloqueada).

394. En el caso de la aplicación de Mensajes, se dispone adicionalmente de otras opciones más avanzadas, como la opción que indica si se desea previsualizar el contenido del mensaje en las alertas, las tiras y el Centro de Notificaciones, denominada "Previsualización" y habilitada por defecto, o la opción de repetición de alertas (Nunca, 1, 2, 3, 5 ó 10 veces), y si se mostrarán alertas de cualquiera o sólo las provenientes de los contactos:

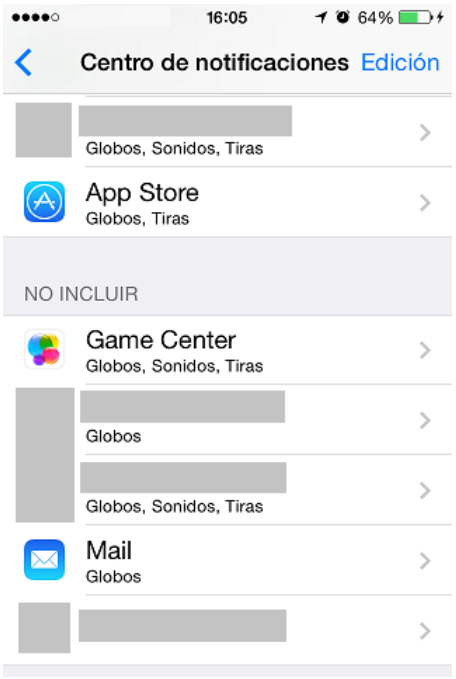




395. Una vez el dispositivo móvil ha sido desbloqueado se dispone de acceso a todas las notificaciones pendientes a través del Centro de Notificaciones desde la barra superior de estado (mediante el gesto ya descrito consistente en deslizar la barra de estado hacia abajo).

396. Desde el punto de vista de seguridad se recomienda recorrer todas las opciones de configuración de las diferentes aplicaciones disponibles en el centro de notificaciones y deshabilitar aquellas de las que no se quiera hacer uso. Las notificaciones de las aplicaciones que gestionan información muy crítica y sensible deberían estar completamente deshabilitadas, mientras que para otras aplicaciones es suficiente con deshabilitar su disponibilidad en la pantalla de desbloqueo (opción "Ver en la pantalla bloqueada" no activa) o las capacidades de previsualización de sus contenidos (opción "Previsualización" no activa), para que, por ejemplo, al recibirse un mensaje SMS (o iMessage) éste no sea previsualizado en la pantalla de desbloqueo del terminal:

397. Adicionalmente, debe tenerse en cuenta que tras la instalación de una nueva aplicación en iOS es necesario acceder al Centro de Notificaciones y ajustar su configuración convenientemente, ya que aparecerá una nueva entrada asociada a la aplicación:



398. En la parte inferior del Centro de Notificaciones se muestran las aplicaciones que disponen de capacidades de notificación pero que han sido deshabilitadas, bajo la sección "No Incluir", que por defecto está vacía.

399. Algunas aplicaciones emplean notificaciones que no hacen uso de capacidades locales del dispositivo, sino que son recibidas desde los servidores de Apple y/o de la aplicación, denominadas notificaciones *push* (ver apartado "5.18.8. Notificaciones *push*").

5.6.3 CENTRO DE CONTROL

400. Complementariamente al Centro de Notificaciones descrito previamente, desde iOS 7 se dispone también del Centro de Control, funcionalidad que permite disponer de accesos directos a los ajustes de configuración más frecuentemente utilizados por los usuarios, incluso desde la pantalla de desbloqueo.

401. Ésta ha sido una de las carencias ampliamente solicitadas por los usuarios en versiones previas de iOS, siendo necesario anteriormente entrar en los ajustes de configuración del dispositivo móvil, y navegar por sus diferentes menús y opciones, para llevar a cabo tareas habituales en el día a día, como por ejemplo activar o desactivar en interfaz Wi-Fi.

402. Sin embargo, los beneficios obtenidos desde el punto de vista de la funcionalidad ofrecida por el Centro de Control desde iOS 7 pueden llevar asociadas contrapartidas desde el punto de vista de la seguridad, especialmente si está disponible también desde la pantalla de desbloqueo.

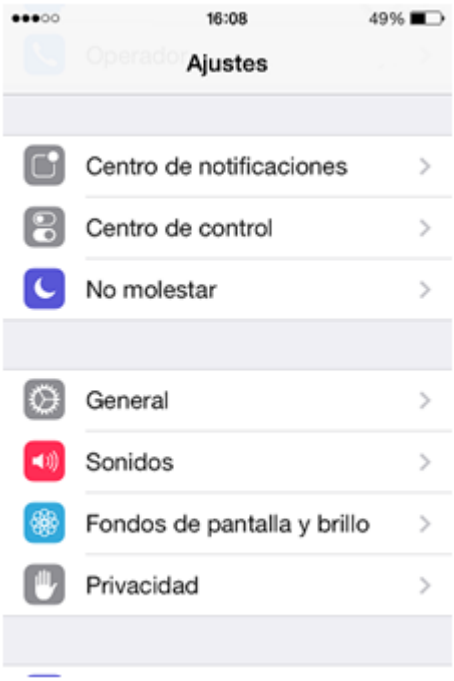
403. El Centro de Control desde la versión 7 de iOS está accesible al desplazar hacia arriba la parte inferior de la pantalla de iOS, por defecto tanto en la pantalla de bloqueo como una vez el dispositivo móvil ha sido desbloqueado.

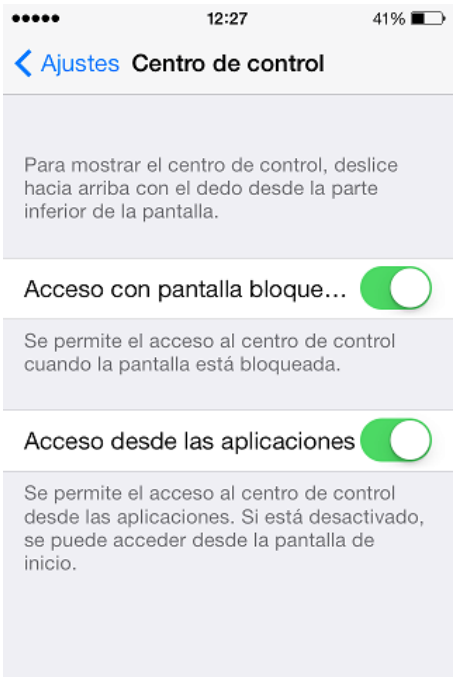
404. El Centro de Control ofrece controles para la reproducción de audio y vídeo, el volumen, acceso a AirDrop y a AirPlay, y el brillo de la pantalla. Adicionalmente, en su parte inferior cuenta con función de linterna a través del *flash* de la cámara, acceso al reloj (en concreto a la funcionalidad que permite fijar un temporizador), a la calculadora y a la

cámara de fotos. En su parte superior proporciona controles para habilitar o deshabilitar el modo vuelo o modo avión, el interfaz Wi-Fi, el interfaz Bluetooth, el modo para no ser molestado y el bloqueo de la orientación de la pantalla:

405. El Centro de Control no puede ser personalizado para eliminar o añadir los controles disponibles, pudiendo hacer uso únicamente de los controles existentes por defecto y definidos por Apple.

406. Desde el punto de vista de seguridad, en el caso de gestionar información sensible y confidencial, se recomienda deshabilitar la posibilidad de acceder al Centro de Control desde la pantalla de desbloqueo del dispositivo móvil mediante el menú "Ajustes - Centro de control". La pantalla asociada pertenece al Centro de Control de iOS y permite configurar tanto el acceso a éste desde la pantalla de bloqueo como desde las aplicaciones:





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

408. En ese escenario, la funcionalidad que permite buscar el iPhone (iPad, o iPod) sería inútil, ya que el dispositivo móvil no dispondrá de capacidades de comunicación de datos (vía Wi-Fi o vía redes móviles 2/3/4G) y, por tanto, no podrá enviar detalles de su ubicación a dicho servicio.

409. Aunque esta configuración afecta a la funcionalidad y facilidad de uso del dispositivo móvil, evita que un tercero no autorizado pueda acceder a las diferentes opciones de configuración existentes con sólo disponer de acceso temporal al dispositivo móvil, incluso por un breve espacio de tiempo.

410. Por otro lado, deshabilitar el acceso al Centro de Control desde las aplicaciones no tiene implicaciones conocidas desde el punto de vista de seguridad, siendo conveniente únicamente para que el Centro de Control no interfiera con el uso habitual de la aplicación, por ejemplo, en el caso de juegos dónde es necesario deslizar el dedo por toda la pantalla.

411. En el caso de deshabilitar ambas opciones, sólo se podrá acceder al Centro de Control desde la pantalla de inicio una vez el dispositivo móvil ha sido desbloqueado.

412. La ausencia de una pequeña barra horizontal en la parte central e inferior de la barra de desbloqueo indica visualmente que no se dispone de ningún tipo de acceso al Centro de Control desde la misma.

5.7 CIFRADO DE DATOS EN IOS

5.7.1 CIFRADO DEL DISPOSITIVO MÓVIL

413. Desde la versión 3GS del iPhone, Apple proporciona capacidades de cifrado hardware del dispositivo móvil (memoria *flash*) mediante un chip criptográfico. Esta funcionalidad está disponible para el iPhone 3GS y modelos posteriores, y para el iPad (en todas sus generaciones) e iPod Touch (desde la 3ª generación), y hace uso de cifrado mediante AES de 256 bits.

414. Las capacidades de cifrado hardware, que implementan tanto el algoritmo AES de 256 bits como SHA-1, permiten aumentar la eficiencia de estas operaciones para que no afecten negativamente a la utilización y el rendimiento del terminal.

415. Sin embargo, pese a implementar capacidades de cifrado hardware, disponiendo de acceso físico al dispositivo móvil es posible acceder al iPhone 3GS y, mediante técnicas similares a las empleadas en el proceso de *jailbreak*, es posible extraer una imagen de disco no cifrada del dispositivo móvil pudiendo acceder a todos los datos.

416. Durante el proceso de extracción de la imagen de disco, el *kernel* de iOS descifra los contenidos transferidos por USB automáticamente, debido a que la clave de cifrado no es dependiente del código de acceso del usuario (al menos hasta la versión iOS 4.2.1 [Ref.- 32]). La clave de cifrado es derivada de datos y material que está almacenado en el dispositivo móvil, y por tanto, disponible para un potencial atacante.

417. En otro escenario similar que también afecta al iPhone 3GS, es posible arrancar el dispositivo móvil desde una imagen *ramdisk* personalizada que elimine el código de acceso, y realizar copias de seguridad no cifradas mediante iTunes, incluso aunque existiera una contraseña de cifrado previamente en iTunes [Ref.- 35].

418. Las capacidades de cifrado de datos de iOS se denominan *Data Protection* [Ref.- 36].

419. iOS cifra el sistema de ficheros (HFS) completo a nivel de bloques mediante una clave denominada FSK, *File System Key*, que se almacena en el dispositivo y es derivada de la clave UID, identificador único del dispositivo móvil, disponible en el hardware del dispositivo móvil, no extraíble y con un valor único para cada terminal [Ref.- 44]. Adicionalmente, el proceso de cifrado emplea una clave GID similar, identificador único de grupo, tipo o modelo de dispositivo móvil, común para todos los terminales de un mismo modelo, como por ejemplo todos los dispositivos que hacen uso del chip A7 de Apple.

420. Tanto el UID (*device Unique IDentifier*) como el GID (*device Group IDentifier*) son claves criptográficas AES de 256 bits que son introducidas en el chip o *hardware* del dispositivo móvil en el momento de su fabricación. El *software* o *firmware* asociado a iOS no dispone de acceso a estas claves, sino únicamente a los resultados de las operaciones criptográficas realizadas con ellas.

421. La vinculación del proceso de cifrado del sistema de ficheros a la clave o identificador único del dispositivo (UID) hace que no sea posible realizar una copia del sistema de ficheros, o incluso extraer los chips de memoria del terminal, y acceder a estos en otro dispositivo móvil similar, ya que su UID será diferente.

422. Debe tenerse en cuenta que la protección de los datos almacenados en los dispositivos móviles iOS es fundamental debido a la gran cantidad de información sensible y privada

que es almacenada por estos, donde caben destacar fotos, e-mails y SMS/iMessages (incluso ya borrados), llamadas realizadas y recibidas, las ubicaciones en las que ha estado el usuario y cuando, rutas y mapas accedidos, así como otra información de localización, la caché y el histórico del navegador web, capturas de pantalla de aplicaciones utilizadas, usuarios y credenciales de acceso a sitios web, la contraseña empleada para las copias de seguridad con iTunes, y prácticamente todo lo que se haya tecleado en el dispositivo móvil (a través de la caché de teclado) [Ref.- 33].

423. El cifrado en el sistema de ficheros de iOS también se realiza a nivel de fichero, y cada fichero es cifrado con su propia clave vinculada al dispositivo móvil en el que está almacenado (la clave se almacena como un atributo extendido del fichero) [Ref.- 34].

424. Adicionalmente, algunos ficheros protegidos (que hacen uso de la funcionalidad de protección de datos descrita posteriormente) están cifrados tanto en función del dispositivo móvil, como del código de acceso del usuario.

425. Este mecanismo aplica por tanto cifrado de dos factores basado en algo que tienes, la clave asociada al dispositivo, implícita al estar los datos almacenados en el propio dispositivo móvil, y algo que conoces, el código de acceso.

426. Los mecanismos de cifrado de iOS han ido evolucionando y mejorando a lo largo del tiempo tanto para las diferentes y nuevas versiones de iOS, como para el hardware de los nuevos dispositivos móviles.

427. Los mecanismos de cifrado de iOS 4 pueden ser vulnerados si se dispone de acceso físico al dispositivo móvil, ya que es posible llevar a cabo una copia del sistema de ficheros completo y extraer las claves de cifrado maestras que están almacenadas (o los datos para calcularlas) en el propio dispositivo móvil [Ref.- 33].

428. Los datos necesarios para obtener dichas claves de cifrado incluyen claves derivadas del UID y del GID (una clave común según el modelo de dispositivo), una clave derivada del código de acceso del usuario, y otras claves custodiadas (*escrow*), generadas y almacenadas por iTunes la primera vez que se conecta el dispositivo móvil al ordenador.

429. En el caso de OS X, las claves intercambiadas en la asociación entre el dispositivo móvil iOS y el ordenador con iTunes, y almacenadas en éste, se encuentran bajo "/private/var/db/lockdown/*.plist".

430. Una vez se dispone de las claves es posible descifrar la mayoría de contenidos existentes en el dispositivo móvil, existiendo herramientas de código abierto [Ref.- 34] y comerciales que proporcionan esta funcionalidad, habitualmente empleadas en el análisis forense de dispositivos móviles iOS.

431. Con el objetivo de mitigar parcialmente la vulnerabilidad mencionada, en la versión 4 de iOS se introdujo la funcionalidad de protección de datos (*Data Protection*) para cifrar mediante hardware algunos datos del usuario almacenados en el dispositivo móvil en función del código de acceso del usuario (ver apartado “5.7.2. Cifrado de los datos de las aplicaciones”), mediante una nueva clave (*passcode key*) [Ref.- 36].

432. Esta funcionalidad emplea el código de acceso del usuario para proteger las claves de cifrado maestras existentes en el dispositivo móvil, y protege los datos almacenados en el dispositivo móvil cuando éste está bloqueado o apagado (no se dispone del código de acceso).

433. La información de las aplicaciones iOS puede ser clasificada en dos grandes grupos: datos, almacenados en el sistema de ficheros, y secretos, almacenados en el *keychain*, como por ejemplo contraseñas o credenciales [Ref.- 69]. El *keychain* se implementa a través de una base de datos SQLite.

434. Las aplicaciones deben especificar una clase de protección para los ficheros y entradas de *keychain* (analizado posteriormente) que quieren proteger con este mecanismo adicional.

435. iOS 5 define cuatro clases de protección tanto para los ficheros como para las entradas del *keychain*, estando los datos disponibles clasificados en categorías (o clases de protección) según cuando son accesibles: cuando el dispositivo está desbloqueado, cuando el dispositivo está bloqueado, tras el primer desbloqueo, o siempre. En iOS 4 sólo se disponía de dos clases de protección, completa o ninguna.

436. Esta jerarquía de clases de protección y claves permite a los dispositivos móviles, por un lado, proteger los datos más sensibles y sólo permitir acceso a los mismos cuando el dispositivo está desbloqueado, y por otro, poder recibir llamadas de teléfono mientras el dispositivo está bloqueado y acceder a todos los ficheros y recursos necesarios.

437. Las entradas del *keychain* pueden adicionalmente especificar en su clase de protección si los datos de la *keychain* pueden ser migrados (o copiados) a otro dispositivo móvil, a través de las clases "ThisDeviceOnly" (sólo para este dispositivo). En caso de emplease este nivel de protección extra, sólo el dispositivo que creó la *keychain* podrá descifrarla.

438. Es el desarrollador de una aplicación iOS quién determina el nivel de protección a aplicar a ciertos datos o secretos, siendo la categoría por defecto aplicada a datos en el sistema de ficheros la de siempre accesibles (sin protección), y la categoría por defecto para entradas en el *keychain* la de accesibles cuando el dispositivo está desbloqueado.

439. En el caso de las aplicaciones de sistema existente por defecto en iOS, es Apple la que determina su criticidad y el nivel de protección para cada una de ellas. La clasificación de los niveles de protección de cada app ha variado también a lo largo de las diferentes versiones de iOS a lo largo del tiempo.

440. La implementación de iOS hace uso de repositorios de claves o *keybags* para ofrecer las diferentes categorías de protección disponibles a nivel del sistema de ficheros, interviniendo en el proceso la clave del dispositivo móvil (disponible únicamente en el módulo hardware criptográfico de los dispositivos móviles iOS o HSM, *Hardware Security Module*), la clave del sistema de ficheros, las claves individuales de cada fichero, y las claves para las diferentes categorías de protección disponibles en el repositorio del sistema (o *System Keybag*), junto al código de acceso del usuario [Ref.- 69].

441. iOS implementa tres repositorios de claves o *keybags* diferentes: sistema (*system*), copias de seguridad (*backup*), y custodia (*escrow*).

442. El *keybag* de sistema es utilizado internamente para proporcionar acceso a los datos del sistema de ficheros y a los secretos del *keychain*. El *keybag* de copias de seguridad se emplea para ofrecer la funcionalidad de copias de seguridad cifradas, enviándose los contenidos cifrados del sistema de ficheros, del *keychain* y este *keybag* a un ordenador remoto, por ejemplo a través de iTunes. Este *keybag* puede ser a su vez protegido por una contraseña en iTunes, y la copia de seguridad potencialmente restaurada en cualquier dispositivo. El *keybag* de custodia es empleado para permitir a un ordenador con iTunes emparejado o asociado con el dispositivo móvil acceder a su sistema de ficheros cuando el dispositivo está bloqueado [Ref.- 69].

443. Las técnicas de descifrado mencionadas previamente siguen siendo válidas excepto para los ficheros protegidos cuyo cifrado depende del código de acceso del usuario.

444. En los dispositivos móviles basados en el chip A7 de Apple, como por ejemplo el iPhone 5S, iPad Air o iPad mini [Ref.- 96], las claves de clase empleadas por *Data Protection* son almacenadas en el *Secure Enclave*.

445. Se dispone de información más detallada sobre el propósito e implementación de cada clase de protección de los ficheros y *keychain*¸ así como del uso de las *keybags*, en el documento oficial de seguridad de iOS [Ref.- 13].

446. Sin embargo, debe tenerse en cuenta que en caso de emplear un PIN de 4 dígitos, su valor también podría ser obtenido mediante técnicas de fuerza bruta por un potencial atacante, y usado para acceder a todos los contenidos, tanto protegidos como no. Las técnicas disponibles permiten conocer el PIN en un iPad en 16 minutos, en un iPhone 4 en 20 minutos y en un iPhone 3GS en 30 minutos [Ref.- 34].

447. El proceso debe realizarse a través del propio dispositivo móvil al emplearse la clave única del dispositivo o UID no extraíble, arrancando el dispositivo móvil desde una imagen *ramdisk* personalizada.

448. Por otro lado, en caso de que se disponga de las claves custodiadas (*escrow*) almacenadas en el ordenador con iTunes con el que se ha sincronizado el dispositivo móvil, también sería posible descifrar todos los contenidos almacenados en el dispositivo móvil, equivalente a disponer del código de acceso.

449. Estas claves custodiadas son empleadas por iTunes para sincronizar los datos y realizar copias de seguridad del dispositivo móvil sin necesidad de introducir el código de acceso. Para ello sólo es necesario que en al menos una ocasión se haya conectado el dispositivo móvil sin bloquear a iTunes. También las emplean las soluciones de gestión empresarial (MDM) para proporcionar la funcionalidad de cambio de contraseña remotamente [Ref.- 34].

450. En iOS 4, como se describe en el apartado “5.7.2. Cifrado de los datos de las aplicaciones”, sólo la aplicación *Mail* nativa hacía uso de *Data Protection* para cifrar los datos a almacenar en el dispositivo móvil.

451. Esta funcionalidad también se emplea para cifrar las capturas de pantalla que son generadas automáticamente cuando el usuario pulsa el botón Home [Ref.- 44].

452. En iOS 5 se ha incrementado la seguridad de los mecanismos de cifrado que requieren conocer el código de acceso del usuario (*Data Protection*), se han introducido nuevas clases de protección (para disponer de acceso a ficheros una vez abiertos si se bloquea el dispositivo móvil), y las claves custodiadas (*escrow*) no pueden ser empleadas para acceder a los datos descifrados sin conocer el código de acceso [Ref.- 45].

453. Adicionalmente a la protección de los ficheros, la seguridad física de los dispositivos móviles continua siendo un elemento clave para su protección, tal como demuestra la vulnerabilidad de seguridad del *keychain* de iOS publicada en febrero de 2011, que permite extraer sin autorización las contraseñas (e-mail, cuentas, aplicaciones, Wi-Fi y VPN) o certificados digitales almacenados en los dispositivos móviles iOS de Apple (iPhone e iPad) con la última versión disponible en el momento del estudio (iOS 4.2.1; también en iOS 5.x posteriormente con ciertas limitaciones) en menos de 6 minutos [Ref.- 32], incluso protegidos por un código de acceso robusto.

454. El repositorio donde se almacenan las credenciales en iOS se denomina *keychain* (ver apartado "5.8.1. Certificados digitales y credenciales del usuario"). Para acceder a sus contenidos, el atacante sólo necesita disponer de acceso físico temporal al dispositivo móvil y tras realizar el proceso de *jailbreak* sobre el mismo, acceder al sistema de ficheros y hacer uso de los mecanismos y funcionalidad de cifrado existentes en iOS, ya que la clave empleada para cifrar el *keychain* se almacena en el propio dispositivo móvil y es independiente del código de acceso.

455. Algunas credenciales son cifradas únicamente con la clave asociada al dispositivo, por lo que están accesibles sin conocer el código de acceso. Otras credenciales, denominadas protegidas, como por ejemplo la contraseña de acceso a sitios web, sin embargo, requieren disponer del código de acceso para poder acceder a su contenido [Ref.- 32].

456. En función de la versión de iOS empleada, el conjunto de credenciales protegidas es diferente. Así por ejemplo en el caso de iOS 3.x todas las entradas del *keychain* son accesibles, al igual que en cualquier versión de iOS si no se ha establecido un código de acceso. En iOS 4.x algunas de las entradas están protegidas, y en iOS 5.x se han introducido mejoras de seguridad, protegiendo por ejemplo las contraseñas de Microsoft Exchange (pero no los certificados digitales cliente), las credenciales de acceso a VPNs o las cuentas de calendario [Ref.- 32]. Estos cambios no han sido documentados oficialmente por Apple ni se dispone de opciones de configuración para clasificar las entradas en el *keychain*.

457. Adicionalmente, en iOS 5.x no sólo las contraseñas (campo *data*) son protegidas en el *keychain*, sino también otros datos (o metadatos) asociados a las credenciales, como el usuario o identificador de la cuenta, o su descripción (campos *account* y *access group*). En el caso de iOS 4.x el *keychain* protegía únicamente las contraseñas.

458. En iOS 7 se habilitaron por defecto y de manera automática los mecanismos de protección de *Data Protection* para las aplicaciones de terceros, protegiéndose los datos almacenados por éstas mientras el dispositivo se encuentra bloqueado.

459. Sin embargo, iOS 7 introdujo una vulnerabilidad (confirmada al menos entre las versiones 7.0.4 y 7.1.1) por la que los ficheros adjuntos a los correos electrónicos (e-mails) no eran cifrados por la aplicación Mail, siendo posible acceder a sus contenidos si se dispone de acceso al sistema de ficheros del dispositivo móvil [Ref.- 134]. Esta vulnerabilidad fue solucionada por Apple en la versión 7.1.2 de iOS.

460. La vulnerabilidad del BootROM (conocida como "limera1n") que permite realizar ataques de fuerza bruta sobre el código de acceso del dispositivo móvil afecta a los dispositivos iOS basados en el chip (o SoC, *System on a Chip*) A4 de Apple, como por ejemplo el iPhone 4 o el iPad 1. En el caso de otros dispositivos como el iPhone 4S y el iPad 2, basados en el chip A5 de Apple, ésta vulnerabilidad no es directamente explotable, por lo que es necesario utilizar en su caso otras vulnerabilidades conocidas, que afectan por ejemplo al kernel de ciertas versiones de iOS, para disponer de acceso completo al sistema y poder ejecutar código no firmado.

461. Aunque esta vulnerabilidad concreta ha sido solucionada en la actualidad en dispositivos móviles de Apple recientes, debe de ser tenida en cuenta, ya que vulnerabilidades similares pueden ser encontradas de nuevo en el futuro y afectar a los nuevos modelos de dispositivos móviles de Apple y, por tanto, también a las versiones más recientes de iOS.

462. La ventaja de las vulnerabilidades del BootROM (encargado del proceso de arranque del dispositivo móvil) para un potencial atacante es que éstas residen en el hardware del propio dispositivo móvil y no pueden, por tanto, ser solucionadas fácilmente por Apple sin reemplazar el dispositivo afectado.

463. A lo largo del tiempo se han descubierto numerosas vulnerabilidades en el proceso de arranque de iOS para diferentes modelos de hardware, afectando tanto al BootROM, LLB, iBoot o al kernel, y que permiten llevar a cabo técnicas de extracción de datos similares a las descritas previamente o el proceso de *jailbreak*, pudiendo ejecutarse código arbitrario no firmado en el dispositivo móvil [Ref.- 46].

Nota: Aunque sólo ciertas entradas del *keychain* sean accesibles sin el código de acceso, el impacto de esta vulnerabilidad es muy elevado teniendo en cuenta que los usuarios reutilizan sus contraseñas entre distintos servicios y aplicaciones, y que, disponiendo de la contraseña de acceso al e-mail (por ejemplo de Microsoft Exchange en iOS 4.x, ya que la contraseña debía estar siempre accesible para preservar la funcionalidad de borrado remoto de datos o *wipe* [Ref.- 44]), es posible recuperar la contraseña de muchos otros servicios que tienen la cuenta de e-mail asociada.

464. En resumen, para evitar ser víctima de las debilidades aún existentes en los mecanismos de cifrado de iOS se recomienda incrementar la seguridad física tanto del dispositivo móvil como del ordenador al que se conecta (evitando que acaben en manos ajenas), disponer de la última versión de iOS en el dispositivo móvil que incluye mejoras significativas, elegir una contraseña de acceso al dispositivo móvil robusta y difícilmente adivinable (al igual que para la contraseña de cifrado de las copias de seguridad mediante iTunes), y no conectar el dispositivo móvil a ordenadores de terceros (para evitar la existencia de copias de seguridad y claves custodiadas en otros ordenadores).

465. Adicionalmente, parece que Apple dispone de capacidades para eliminar el código de acceso de un dispositivo móvil iOS sin conocer su valor si tiene acceso físico al mismo, permitiendo acceso completo al dispositivo móvil y sus datos, procedimiento que sólo se aplica con las correspondiente orden judicial y del que no se han desvelado detalles públicamente [Ref.- 119].

5.7.2 CIFRADO DE LOS DATOS DE LAS APLICACIONES

466. iOS proporciona capacidades de protección adicionales (a través de *Data Protection*, mecanismo analizado y descrito previamente) para cifrar los datos de las aplicaciones almacenados en el dispositivo móvil cuando el dispositivo está bloqueado con un código de acceso.

467. Por defecto, si esta funcionalidad está activa, únicamente los mensajes de correo electrónico y ficheros adjuntos gestionados por la aplicación *Mail* nativa eran cifrados en iOS 5.x al almacenarse en el dispositivo móvil.

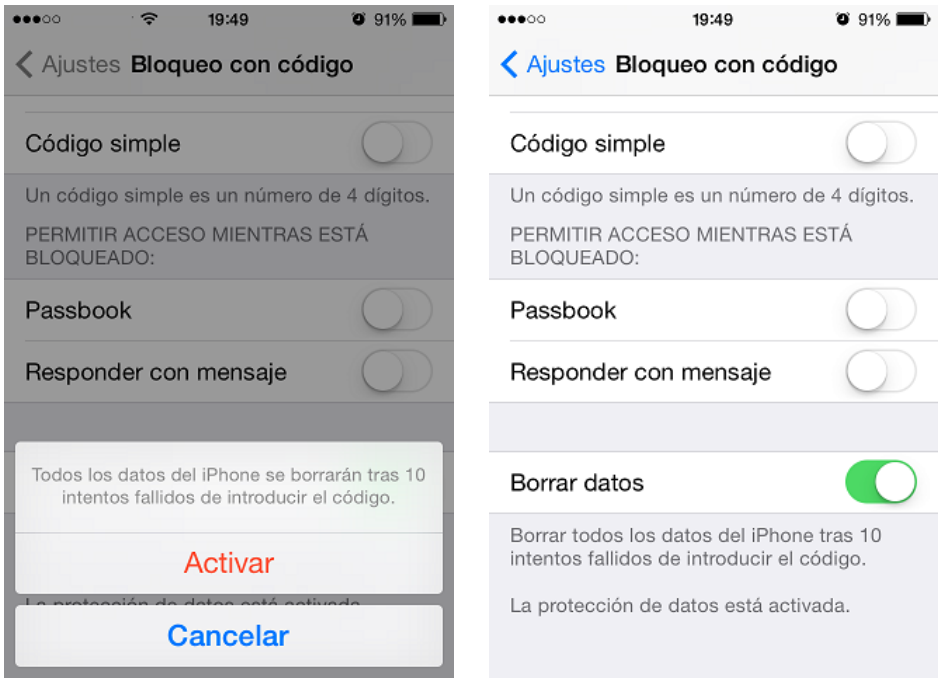
468. En la versión 7 de iOS los mecanismos de protección de datos nativos de iOS mediante cifrado (*Data Protection*) están disponibles automáticamente y por defecto para todas las apps, tanto las apps de sistema como también para las aplicaciones de terceros, con el objetivo de proteger los datos corporativos almacenados por apps de terceros (hasta el primer desbloqueo con el código de acceso tras reiniciar el dispositivo).

469. Los desarrolladores de aplicaciones para iOS también pueden hacer uso de las librerías o APIs de protección de datos para cifrar la información gestionada por sus aplicaciones.

470. Este mecanismo de protección de datos y cifrado se basa en las capacidades hardware de cifrado de iOS (ver apartado “5.7.1. Cifrado del dispositivo móvil”) y en el código de acceso seleccionado por el usuario, de ahí que éste deba ser suficientemente robusto para evitar que sea fácilmente adivinable por parte de un potencial atacante.

471. Los ficheros protegidos con estas capacidades sólo pueden ser accedidos cuando el dispositivo móvil ha sido desbloqueado por el usuario, por lo que se recomienda que el bloqueo del dispositivo se realice de forma automática y lo antes posible (a través de la opción “Ajustes - General - Bloqueo con código - Solicitar: De inmediato”; ver apartado "5.4.2. Código de acceso al dispositivo móvil").

472. Esta funcionalidad se activa tras fijar un código de acceso en el dispositivo móvil y puede ser verificada desde el menú “Ajustes – General – Bloqueo con código” (a través del mensaje “La protección de datos está activada” en la parte inferior de la pantalla) o mediante las soluciones de gestión empresarial (MDM):



5.7.3 BORRADO DE LA MEMORIA DEL DISPOSITIVO

473. Los dispositivos móviles iOS también permiten llevar a cabo el borrado de la memoria interna (almacenamiento de tipo *flash*) de forma segura, especialmente de las claves de cifrado y otra información sensible.

474. Para ello hacen uso de capacidades de gestión de la memoria, denominadas *Effaceable Storage*, que permiten acceder a la memoria a muy bajo nivel y eliminar de la misma las claves de cifrado empleadas para la protección de la memoria principal, haciendo que no sea posible acceder a la información almacenada previamente en la memoria del dispositivo móvil [Ref.- 13].

475. Mediante este método, la información cifrada residente en la memoria del dispositivo móvil no es eliminada, pero se consigue que los datos almacenados sean inaccesibles criptográficamente al eliminar las claves que permitirían descifrarlos, minimizando a su vez el tiempo necesario para borrar completamente los datos del dispositivo.

476. Esta funcionalidad es utilizada, por ejemplo, al restaurar el dispositivo móvil a los ajustes de fábrica a través del menú "Ajustes - General - Restablecer - Borrar contenidos y ajustes".

477. En versiones previas de iOS, el borrado de la memoria se llevaba a cabo mediante la sobreescritura de la misma, proceso que requería mayor dedicación y tiempo (entre 1-4 horas aproximadamente dependiendo del tipo de dispositivo móvil).

5.7.4 CIFRADO DE LAS TARJETAS DE ALMACENAMIENTO EXTERNAS

478. Los dispositivos móviles iOS no tienen capacidades para conectar una tarjeta de almacenamiento externa (ej. tarjeta SD), por lo que la funcionalidad de cifrado no aplica sobre otros elementos externos, sino únicamente sobre el propio dispositivo móvil.

5.8 GESTIÓN DE CERTIFICADOS DIGITALES Y CREDENCIALES EN IOS

5.8.1 CERTIFICADOS DIGITALES Y CREDENCIALES DEL USUARIO (KEYCHAIN)

479. iOS dispone de un contenedor (o almacén) de credenciales y certificados, denominado *keychain*. El *keychain* es un repositorio para el almacenamiento seguro de pequeñas cantidades de información sensible, protegido por mecanismos de cifrado y basado en una base de datos SQLite, dónde se almacenan los certificados digitales, contraseñas y otras credenciales, como por ejemplo las asociadas a redes VPN y redes Wi-Fi. No constituye una solución para el cifrado y almacenamiento generalizado de datos, ya que iOS proporciona otros mecanismos para este propósito empleando ficheros.

480. Las consultas de acceso al *keychain* son restringidas en función del grupo de acceso de la aplicación. Las aplicaciones de sistema acceden al *keychain* a través del grupo de acceso “apple”.

481. El *keychain* es un mecanismo heredado de OS X, y en iOS (3.x), pese a que la clave de cifrado maestra de *keychain* se basa en una clave específica propia del dispositivo móvil que se almacena en una localización inaccesible a las aplicaciones y excluida de las copias de seguridad, disponiendo de acceso físico al dispositivo sus contenidos pueden ser descifrados (ver apartado “5.7.1. Cifrado del dispositivo móvil”).

482. El apartado “5.7.1. Cifrado del dispositivo móvil” detalla la clasificación de diferentes niveles de protección para las entradas del *keychain*, así como la evolución de las mejoras de seguridad del mismo en función de la versión de iOS.

483. El *keychain* de una aplicación se almacena fuera de su *sandbox*. Al realizar una copia de seguridad de los datos del dispositivo móvil, el *keychain* también será copiado.

484. En versiones previas al iOS 4.0 el *keychain* sólo podía ser restaurado desde una copia de seguridad en el mismo dispositivo móvil desde el que se copió, pero sin embargo desde esa versión, el *keychain* es un elemento protegido por contraseña que puede ser restaurado en otro dispositivo (salvo que existan restricciones explícitas para no permitirlo) [Ref.- 24].

485. iOS dispone de capacidades para compartir los datos almacenados en el *keychain* entre aplicaciones, por ejemplo, de un mismo desarrollador, a través de una *shared keychain*, dónde debe definirse qué aplicaciones tienen acceso al mismo (mediante *entitlements*).

486. El *keychain* y su gestión no está directamente accesible para el usuario a través del interfaz gráfico de iOS.

487. iOS permite importar certificados digitales X.509 en formato PKCS#12 que contengan sólo una identidad, desde ficheros con extensión .p12 y .pfx, así como .cer, .crt y .der [Ref.- 62].

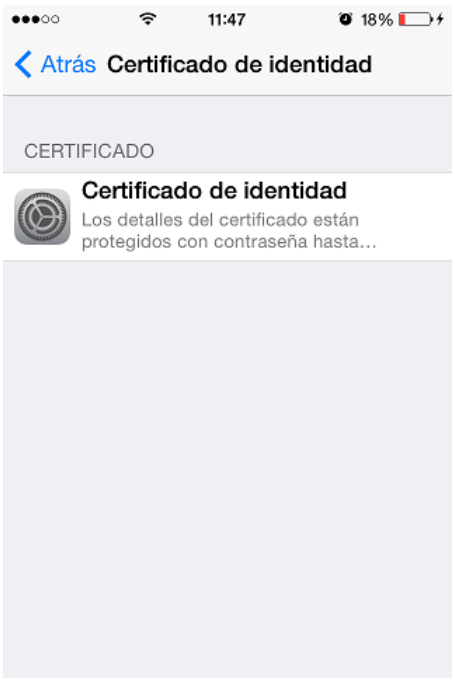
488. Los certificados digitales cliente pueden emplearse para el acceso y autentificación a través de Microsoft Exchange ActiveSync, redes Wi-Fi o conexiones VPN, y desde iOS 5.x para la firma y cifrado de correos electrónicos con S/MIME, y los certificados digitales servidor son empleados para la protección de las comunicaciones, incluyendo las anteriores y, por ejemplo, el acceso a páginas web mediante HTTPS desde Safari (incluyendo soporte para OCSP).

489. Los certificados necesarios para establecer cadenas de confianza pueden ser instalados manualmente o automáticamente a través de perfiles de configuración a través de OTA (Over-the-Air) y el protocolo Simple Certificate Enrollment Protocol (SCEP) [Ref.- 62].

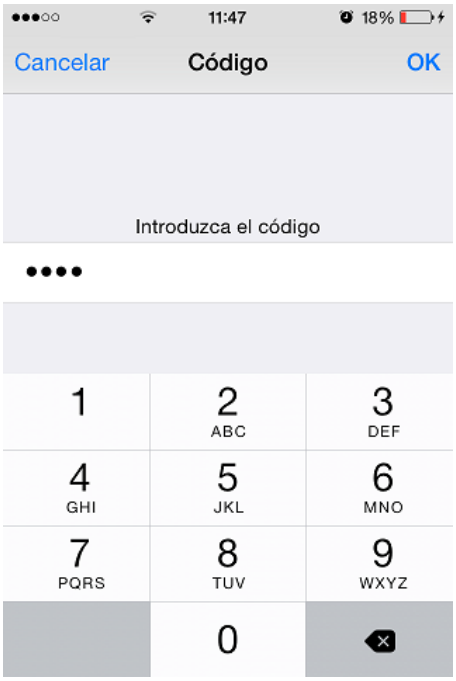
490. Los métodos de distribución e instalación manual de certificados digitales por un usuario, tanto de cliente como de autoridades certificadoras raíz (ver apartado "5.8.2. Certificados digitales raíz de iOS"), incluyen la transferencia a través de un ordenador e iTunes (perfiles de configuración), mediante un fichero adjunto a un correo electrónico, o descargándolo directamente desde una página web mediante Safari.

491. Desde el punto de vista de seguridad, la opción recomendada para la distribución e instalación de certificados en iOS es a través de perfiles de configuración y de la solución de gestión empresarial MDM. En el caso de emplear un servidor web interno a la organización, éste debe hacer uso de mecanismos de autentificación del usuario y de cifrado, para proteger sus comunicaciones. En el caso de emplear un correo electrónico, éste debe hacer uso de mecanismos de cifrado y firma, para permitir la verificación de su autenticidad. Los ejemplos empleados a continuación hacen uso de un correo electrónico para facilitar su visualización.

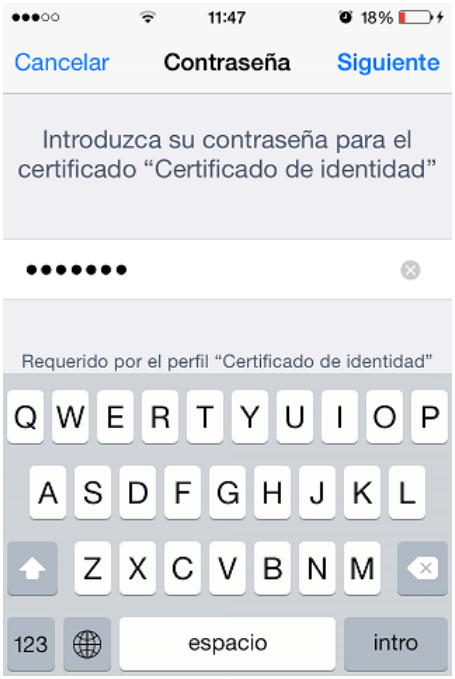
492. Al seleccionar el certificado digital, iOS mostrará al usuario la ventana de instalación de un perfil que incluye un certificado de identidad (o certificado digital cliente), y el usuario mediante el botón "Instalar" puede proceder a su instalación, tras ser notificado de que el perfil modificará los ajustes del dispositivo móvil. El certificado en el ejemplo inferior ha sido recibido por e-mail mediante la app "Mail". El botón "Más detalles" proporciona más información sobre el certificado digital:

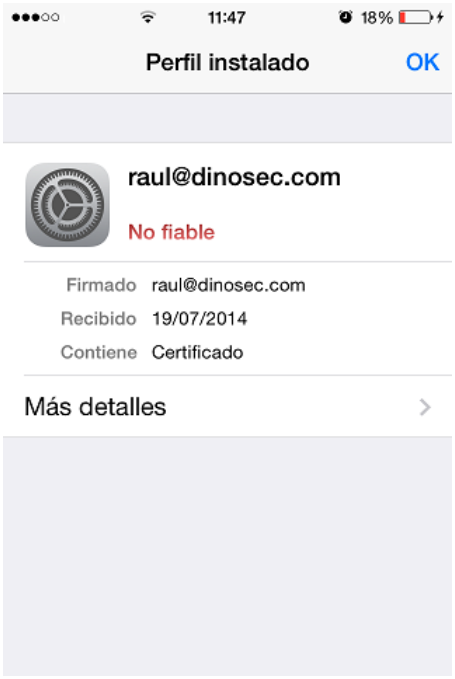


493. Al instalar un certificado digital, iOS solicitará al usuario el código de acceso al dispositivo móvil para proceder a modificar los ajustes del dispositivo:

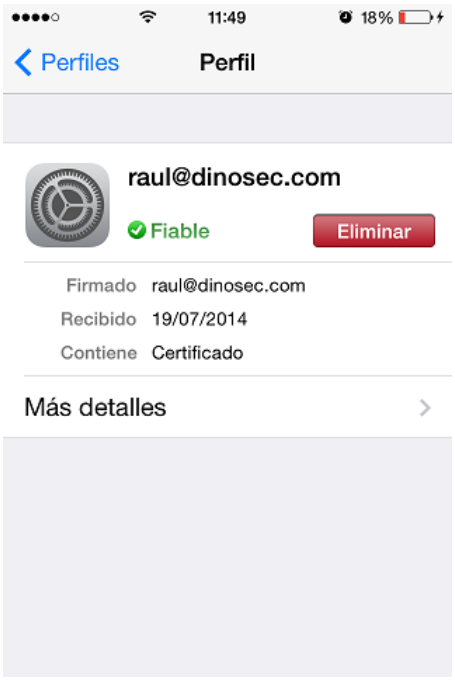


494. Al instalar un certificado digital cliente (denominado certificado de identidad, "Identity Certificate") protegido por una contraseña, iOS solicitará al usuario la misma para proceder a su instalación, confirmándose finalmente si el perfil ha sido o no instalado:

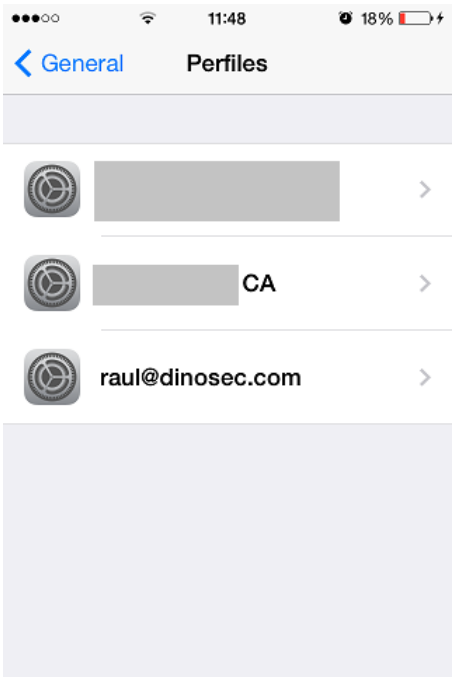


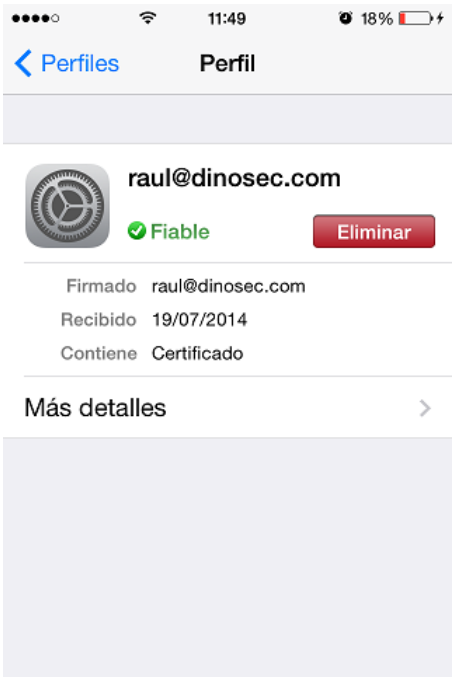


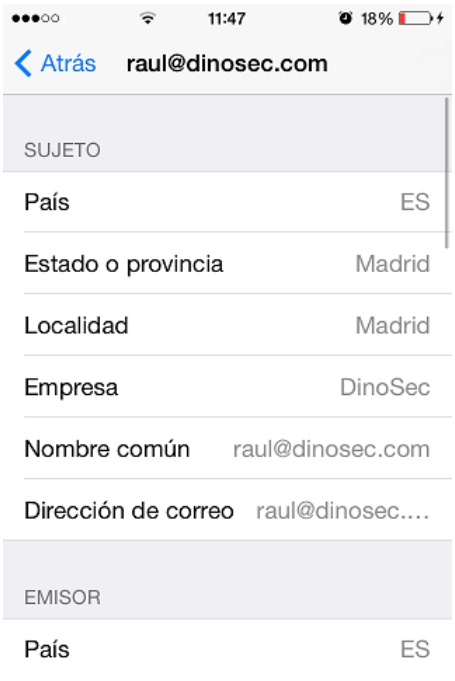
495. La confianza reflejada en el certificado ("No fiable", en la imagen superior) depende de sí iOS dispone de la cadena de confianza completa para dicho certificado, es decir, si también confía en la CA que lo ha emitido. El certificado de dicha CA también deberá ser importado en el dispositivo móvil (ver apartado "5.8.2. Certificados digitales raíz de iOS"), preferiblemente antes de importar los certificados emitidos por ésta. Una vez importada la CA emisora (ver apartado "5.8.2. Certificados digitales raíz de iOS"), el certificado digital cliente será identificado como "Fiable":



496. Es posible acceder a los certificados que han sido instalados previamente a través del menú "Ajustes - General – Perfil (o Perfiles, en caso de existir más de uno)":







497. Desde el mismo menú es posible eliminar un certificado digital previamente instalado a través del botón "Eliminar", así como llevar a cabo esta gestión mediante OTA y las soluciones empresariales de gestión de dispositivos móviles (MDM).

5.8.2 CERTIFICADOS DIGITALES RAÍZ DE IOS

498. En iOS, por defecto, no es posible acceder al listado de autoridades certificadoras (Certificate Authorities, CA) reconocidas por el dispositivo móvil desde el interfaz gráfico de usuario.

499. El conjunto de autoridades raíz de certificación distribuidas por Apple oficialmente y por defecto en el sistema iOS está disponible para iOS 3.x [Ref.- 20], iOS 4.x [Ref.- 21], iOS 5.x e iOS 6.x [Ref.- 22], e iOS 7.x [Ref.- 162].

500. El *Trust Store*, o repositorio de certificados de confianza, de iOS 5.x y 6.x (y versiones previas de iOS) contenía certificados de confianza de autoridades certificadoras (CAs) raíz o intermedias.

501. El *Trust Store*, o repositorio de certificados de confianza, de iOS 7.1.2 dispone de tres categorías de certificados [Ref.- 162]:

- De confianza (*Trusted*), correspondientes a los certificados de confianza de autoridades certificadoras (CAs) raíz o intermedias.
- Siempre preguntar (*Always Ask*), correspondientes a certificados que no son de confianza pero no están bloqueados, por lo que al ser utilizados el usuario será preguntado y decidirá si confía en él y lo acepta o no.
- Bloqueados (*Blocked*), correspondientes a certificados que han sido comprometidos y nunca serán aceptados como de confianza.

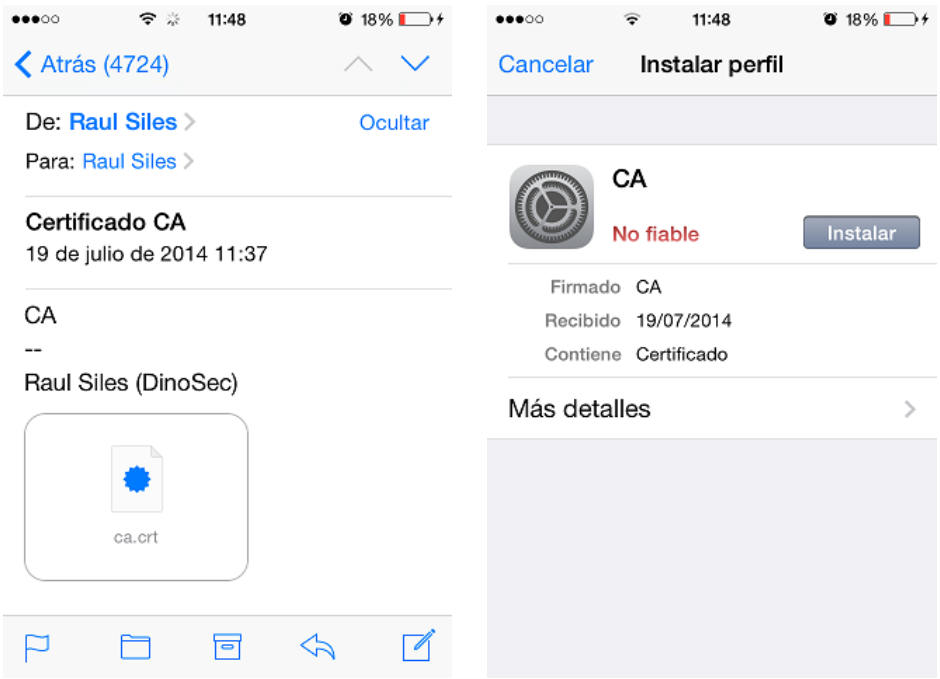
502. Desde las versiones 7.1.x de iOS es posible consultar la versión de la *Trust Store* a través del menú "Ajustes - General - Información" y el apartado "Confiar en la tienda" (*Trust*

Store), con el objetivo de poder consultar la documentación [Ref.- 162] que detalla los certificados que contiene.

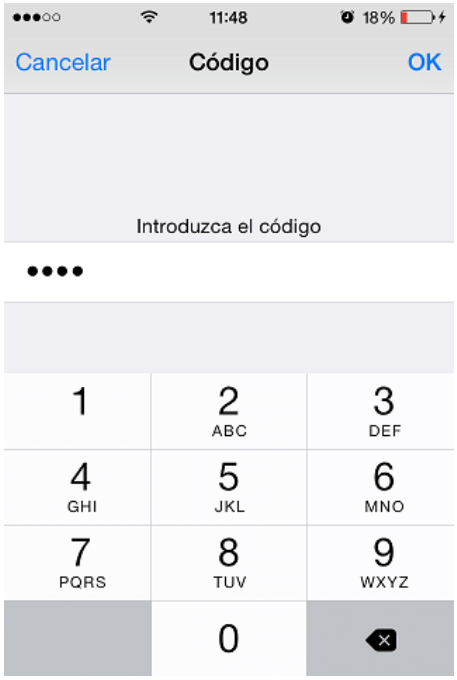
503. Por ejemplo, la versión 2014060300 de la *Trust Store* corresponde a la versión 7.1.2 de iOS:

504. iOS 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 de los métodos de distribución e instalación de certificados detallados en el apartado "5.8.1. Certificados digitales y credenciales del usuario".

505. El proceso es similar al de añadir un certificado de identidad mostrado previamente:

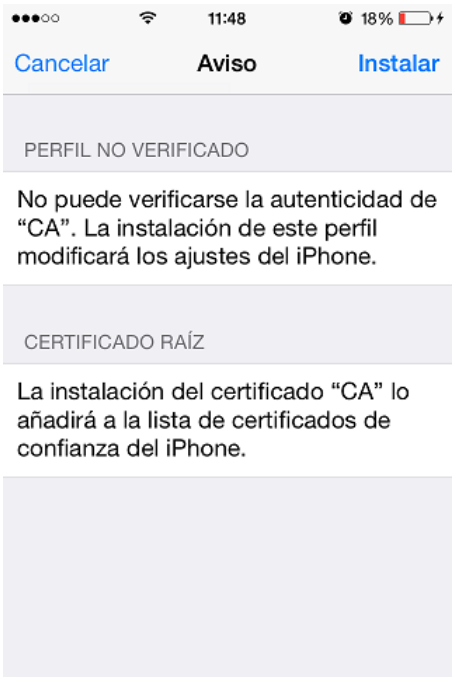


506. Al instalar un certificado digital raíz, iOS solicitará al usuario el código de acceso al dispositivo móvil para proceder a modificar los ajustes del dispositivo:

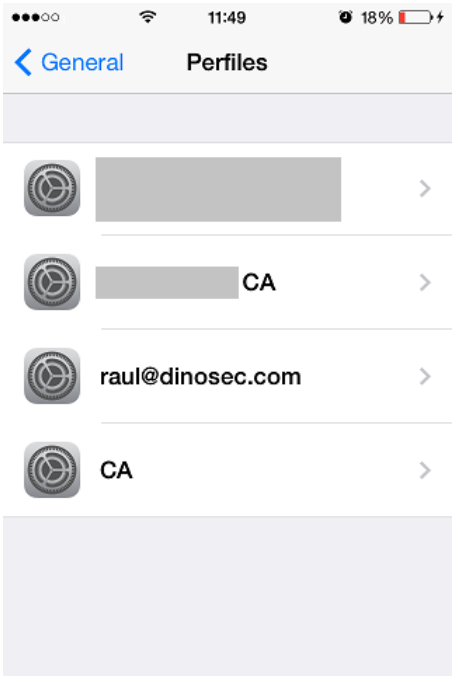


507. El proceso para añadir certificados digitales raíz específicos para su utilización en conexiones Wi-Fi o VPN se detalla en el apartado "5.14.3. Recomendaciones de seguridad para la conexión a redes Wi-Fi".

508. 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:



509. Es posible acceder a los certificados raíz que han sido instalados previamente a través del menú "Ajustes - General – Perfil (o Perfiles, en caso de existir más de uno)":



5.8.3 FIRMA DIGITAL Y VERIFICACIÓN DE APLICACIONES EN IOS

510. Para que una aplicación sea considerada válida y pueda ser distribuida oficialmente a través de la App Store de Apple debe haber sido firmada digitalmente por su desarrollador, mediante un certificado digital válido emitido por Apple y asociado al programa de desarrolladores de iOS.

511. Apple realiza verificaciones adicionales sobre la funcionalidad, estabilidad, diseño, comportamiento, existencia de contenido explícito u ofensivo, y seguridad de la

aplicación, aunque los detalles internos del proceso de verificación de seguridad no han sido publicados por Apple.

512. La guía de revisiones de la App Store [Ref.- 29] (sólo disponible para los desarrolladores de aplicaciones iOS de Apple, tras abonar la cuota correspondiente al programa de desarrolladores de iOS [Ref.- 27]) proporciona los detalles del tipo de contenido, funcionalidad y calidad esperado en las aplicaciones iOS.

513. La firma digital de las aplicaciones iOS no evita que las mismas contengan vulnerabilidades de seguridad o código malicioso, pero permite vincular la aplicación a su desarrollador, y asegurar su integridad frente a modificaciones [Ref.- 28].

514. Los binarios de las aplicaciones de iOS emplean el formato MACH-O, empleándose SHA-1 para la generación de *hashes* que son firmados para asegurar su procedencia e integridad. Los *hashes* de los binarios del sistema están cacheados en el propio kernel de iOS [Ref.- 46].

515. La vinculación entre la aplicación y el desarrollador no ofrece fiabilidad desde el punto de vista de seguridad; ésta viene proporcionada a través del proceso de verificación de aplicaciones de Apple antes de su aceptación, aprobación y publicación.

Nota: Los desarrolladores interesados en la creación de aplicaciones para iOS disponen de todos los detalles e información en el portal para desarrolladores de Apple, iOS Dev Center [Ref.- 27] y en la librería de documentación asociada [Ref.- 14].

Inicialmente Apple no proporcionó un entorno de desarrollo (SDK, *Software Development Kit*) para terceros, aunque de forma temporal anunció un entorno web ("AJAX SDK"), que finalmente se materializó en el SDK actual, liberado en marzo de 2008 y revisado y actualizado en octubre de 2008, junto a su integración junto a la App Store.

Adicionalmente, en junio de 2014 Apple anunció la disponibilidad de Swift, un nuevo lenguaje de programación para el desarrollo de apps de iOS (y OS X) a partir de la versión 8 de iOS, futuro sustituto de Objective-C: https://developer.apple.com/swift/.

516. El proceso de verificación de aplicaciones de Apple antes de su publicación se centra en analizar los contenidos y la funcionalidad de la aplicación, principalmente a través de la utilización que ésta hace de las librerías (APIs) del sistema. Sin embargo, este proceso no es infalible, habiéndose presentado diferentes casos en los que los desarrolladores han introducido funcionalidad oculta en aplicaciones que han sido aprobadas por Apple.

517. Por ejemplo, en el 2009 la aplicación Lyrics incluyó funcionalidad oculta que no había sido aprobada previamente por Apple, demostrando las debilidades e inconsistencia del proceso manual de verificación y revisión de aplicaciones [Ref.- 37].

518. Una vulnerabilidad publicada en octubre de 2011 y que afectaba al módulo de firma y verificación de código de los dispositivos iOS de Apple (iPhone, iPad, etc – iOS 4.3) demostró la posibilidad de publicar aplicaciones benignas en el App Store que posteriormente descargarán código dañino, extendiendo así su funcionalidad dinámicamente.

519. Charlie Miller demostró este problema de seguridad a través de la aplicación Instastock, qué fue publicada oficialmente por Apple en el App Store [Ref.- 38].

520. La versión 5.0.1 de iOS resolvió esta vulnerabilidad, de ahí la importancia de mantener siempre los dispositivos móviles actualizados a la última versión proporcionada por el fabricante [Ref.- 6].

521. La aplicación que contiene el código oculto puede permanecer temporalmente en la App Store, ya que Apple puede eliminarla tan pronto sea consciente de su comportamiento no autorizado.

522. Adicionalmente a la posibilidad de eliminar una aplicación de la App Store, los dispositivos móviles basados en iOS disponen potencialmente de capacidades por parte del vendedor, Apple, para deshabilitar aplicaciones de los mismos de forma remota (funcionalidad conocida como "*kill switch*"), pudiendo crear una lista negra (*blacklist*) de aplicaciones no autorizadas [Ref.- 39].

523. iOS dispone de una URL en el módulo CoreLocation que refleja el listado de aplicaciones no autorizadas: https://iphone-services.apple.com/clbl/unauthorizedApps.

524. En el momento de elaboración de la presente guía su contenido está vacío:

```
{ "Date Generated" = "2011-10-26 22:04:09 Etc/GMT"; "BlackListedApps" = {}; }
```

525. 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.

526. Estas capacidades permiten a Apple no sólo eliminar las aplicaciones maliciosas de la App Store y suspender las cuentas de los desarrolladores sospechosos, sino también eliminar las aplicaciones de los dispositivos móviles donde han sido instaladas (se desconoce si el mecanismo notificaría al usuario sobre las acciones realizadas).

527. No se tiene constancia de que Apple haya empleado estas capacidades en ninguna ocasión para eliminar una aplicación en los dispositivos móviles de los usuarios.

5.8.4 ENTERPRISE SINGLE SIGN ON (SSO)

528. Previamente a iOS 7, únicamente las apps que provenían de un mismo desarrollador tenían la capacidad de compartir un mismo keychain (*Shared Keychain*) y como resultado podían almacenar, intercambiar y reutilizar información de credenciales para acceder a servicios remotos sin necesidad de solicitar las credenciales de nuevo al usuario.

529. iOS 7 proporciona una solución de autentificación única empresarial, denominada *Enterprise Single Sign On* (SSO), para compartir y reutilizar las credenciales del usuario entre diferentes apps, incluso provenientes de distintos desarrolladores. El modelo de integración empleado previamente en iOS 6 para compartir las credenciales de acceso a Twitter y Facebook se ha extendido a lo largo de toda la plataforma móvil y de todas las apps.

530. Las credenciales para los distintos servicios son almacenadas en un repositorio único del sistema (*keychain*), desde el que pueden ser reutilizadas por diferentes apps, siendo posible definir su uso en base a prefijos de URLs e identificadores de apps concretos.

531. Los perfiles de configuración de iOS deben especificar la identidad o localización del KDC, y establecer relaciones entre los servicios o URLs que deben ser accedidos, y las apps que pueden reutilizar las credenciales del usuario para acceder a estos.

532. El proceso de autentificación es gestionado por iOS, no por las apps individualmente, y mediante Kerberos y la asignación de tickets de Kerberos, o tokens SPNEGO [Ref.- 148], iOS permite su reutilización entre distintas apps.

533. Sin embargo, para que SSO funcione, el servicio accedido debe soportar autentificación mediante Kerberos, y el Kerberos KDC (*Key Distribution Center*) debe estar accesible tanto para los usuarios como para los servicios, lo que implica que normalmente se accede mediante SSO a servicios empresariales dentro de la organización (ya que el KDC habitualmente no estará expuesto públicamente en Internet).

534. El usuario sólo necesita autentificarse una única vez con sus credenciales, y éstas serán automáticamente reutilizadas por el resto de apps corporativas designadas con los permisos necesarios para hacer uso de dichas credenciales [Ref.- 153].

535. Las capacidades de SSO están disponibles por defecto en Mobile Safari, y en cualquier otra app de terceros que haga uso de las librerías (APIs) de comunicaciones estándar de iOS.

5.8.5 ICLOUD KEYCHAIN

536. En iOS 7, Apple proporcionó nuevas capacidades centralizadas de almacenamiento de credenciales, almacenadas en el repositorio denominado *keychain* (llavero), a través de iCloud, similares a la funcionalidad ofrecida por otros gestores de contraseñas o credenciales. En concreto esta funcionalidad fue introducida en iOS 7.0.3.

537. El keychain es una base de datos o repositorio de información protegido para el almacenamiento de credenciales (identificador de cuenta y contraseña), tanto de sitios web como de apps, contraseñas de redes Wi-Fi, e información de tarjetas de crédito (sin el código CVV).

538. iCloud Keychain permite almacenar el keychain local existente en iOS y OS X en iCloud, de manera supuestamente segura [Ref.- 165] mediante la utilización de cifrado basado en AES de 256 bits, y permite su utilización y compartición desde diferentes dispositivos Apple, tanto móviles (iOS 7 o superior) como tradicionales (OS X Mavericks o superior).

539. iCloud Keychain sólo sincroniza aquellos elementos del *keychain* del usuario que han sido identificados con el atributo que permite su sincronización entre dispositivos, es decir, que no son únicos para cada dispositivo. Por ejemplo, las identidades de redes VPN no son sincronizadas y compartidas, mientras que las credenciales empleadas por Mobile Safari o las contraseñas de redes Wi-Fi sí lo son.

540. Por defecto, los elementos añadidos al *keychain* por las apps de terceros están identificados como no sincronizables, debiendo el desarrollador de la app modificar el atributo si desea que sea compartido entre diferentes dispositivos.

541. La versión de Mobile Safari disponible en iOS 7, al igual que la versión de Safari de OS X 10.9 y versiones posteriores, se integran directamente con iCloud Keychain, permitiendo el almacenamiento de credenciales y tarjetas de crédito, su reutilización, e incluso la generación y almacenamiento de nuevas contraseñas (a través del nuevo generador de contraseñas).

542. Esta funcionalidad en Safari y Mobile Safari se complementa con capacidades para autocompletar formularios web, de forma que el usuario puede tanto sincronizar sus contraseñas a través de iCloud Keychain entre OS X 10.9+ e iOS 7+, como generar

nuevas contraseñas desde Safari y/o Mobile Safari, y hacer uso directo de las mismas desde estos navegadores web y sus capacidades automáticas para autocompletar formularios web.

543. La versión 7.1 de iOS amplió el número de países con soporte para iCloud Keychain.

544. La funcionalidad de iCloud Keychain puede ser habilitada en iOS 7 desde el menú "Ajustes - iCloud" y la opción "Llavero" (*Keychain*):

545. Adicionalmente, Apple proporciona un servicio de recuperación del *keychain* (*Keychain Recovery*) en el caso de que el usuario pierda su *keychain* local y no disponga de una copia de seguridad. Este escenario es aún más crítico al emplear las nuevas capacidades de generación de contraseñas aleatorias de Mobile Safari, que potencialmente sólo estarán disponibles en el *keychain* del usuario.

546. Para ello Apple proporciona un nuevo servicio de depósito o fidecomiso (*escrow*) del *keychain*, pero supuestamente sin disponer de acceso a sus contenidos. Para ello se emplea un segundo factor de autentificación, y se cifra el *keychain* con una contraseña supuestamente robusta. Esta contraseña a su vez es empleada para proteger la contraseña aleatoria que realmente protege el almacenamiento del *keychain*.

547. Desafortunadamente, por defecto, los requisitos existentes respecto al código de seguridad de iCloud que debe establecer el usuario al activar iCloud Keychain durante el proceso de configuración sólo requieren emplear un código de 4 dígitos. Este escenario permitiría a Apple, o a un tercero que haya comprometido el entorno de iCloud de Apple, realizar ataques de fuerza bruta y acceder de manera trivial a los contenidos del *keychain* del usuario.

548. Se recomienda emplear en su lugar como código de seguridad de iCloud una frase de paso suficientemente larga y robusta, ya que la misma está protegiendo uno de los elementos, sino el elemento, más sensible almacenado por el dispositivo móvil, el *keychain*.

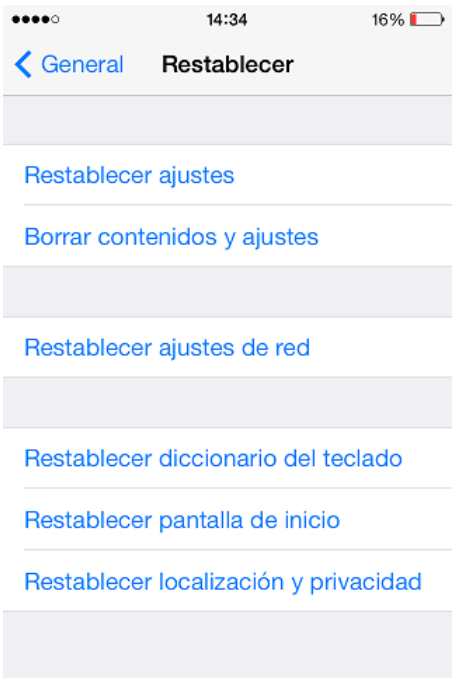
549. Otra opción posible es hacer uso de las capacidades de generación de un código criptográfico aleatorio para proteger el keychain por parte de iOS durante el proceso de configuración, pero en este caso, el almacenamiento del *keychain* se llevará a cabo directamente y únicamente en base al este valor (sin hacer uso de un registro basado en datos de los que sólo dispone el usuario, *iCloud Escrow Record*) [Ref.- 165].

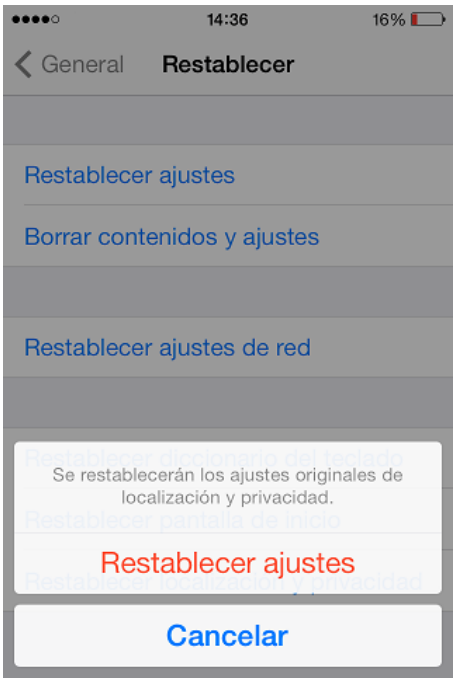
550. El proceso de recuperación del *keychain* emplea el código de seguridad de iCloud y adicionalmente el número de teléfono del usuario, al hacer uso de un desafío enviado mediante un mensaje SMS, junto a las credenciales de la cuenta del usuario en iCloud [Ref.- 148].

5.9 ELIMINACIÓN DE DATOS DEL DISPOSITIVO MÓVIL

551. iOS proporciona capacidades locales para la eliminación de todos los datos almacenados en el dispositivo móvil a través de la opción “Borrar contenidos y ajustes” disponible desde el menú “Ajustes - General - Restablecer”. Para poder restablecer los ajustes es necesario introducir el código de acceso del dispositivo móvil.

552. El proceso de restablecimiento eliminará todos los datos del teléfono, incluyendo cuentas de iCloud e iTunes, configuración y datos de aplicaciones y del sistema, y de aplicaciones previamente descargadas. No se eliminará el software del sistema operativo ni las actualizaciones de sistema ya aplicadas, es decir, la versión existente del propio iOS:





553. La opción "Borrar contenidos y ajustes" elimina los ajustes (los ajustes se restaurarán a sus parámetros de fábrica) y la información del usuario, junto a la clave de cifrado de los datos. Según el tipo de dispositivo móvil y la versión de iOS el tiempo que conlleva este proceso puede variar significativamente, siendo únicamente de unos minutos en los últimos dispositivos compatibles con iOS 5.x (y versiones posteriores de iOS) que emplean cifrado por hardware [Ref.- 63].

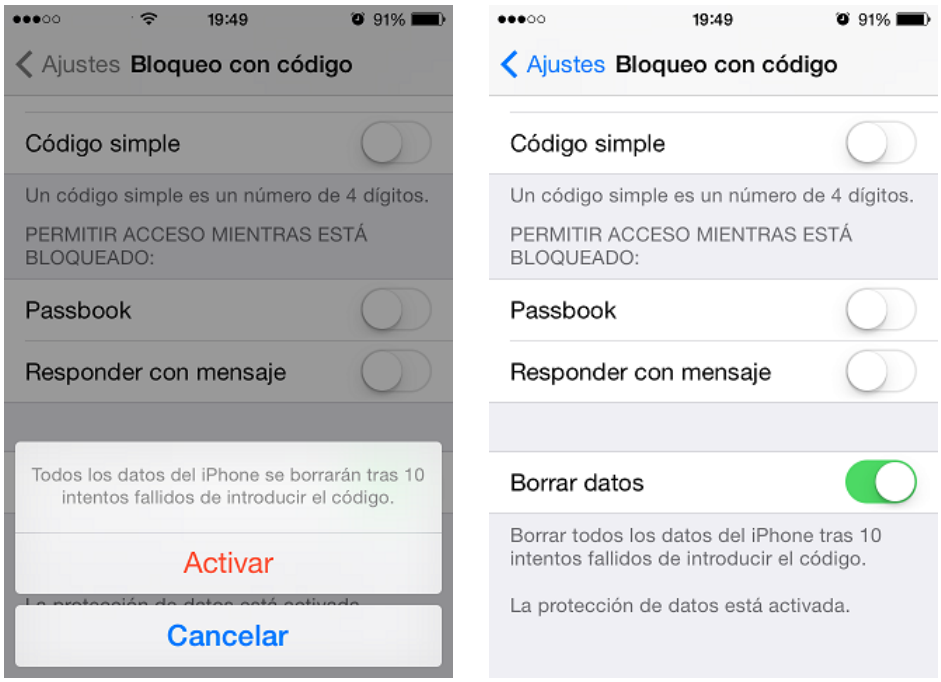
554. Por otro lado, la opción "Restablecer ajustes" o "Restablecer ajustes de red" (así como las opciones de restablecimiento de la zona inferior de la pantalla), permiten restaurar todos

los ajustes, o los asociados a las redes de comunicaciones respectivamente, a los parámetros de fábrica, sin actuar sobre los datos del usuario.

555. Estas capacidades de borrado de datos local también pueden ser activadas tras llevarse a cabo un número determinado de intentos de acceso fallidos, pudiendo activarse esta funcionalidad de forma manual o a través de las políticas de seguridad de los mecanismos de gestión empresariales de dispositivos móviles iOS (ver apartado "5.3. Gestión empresarial de dispositivos basados en iOS").

556. El número máximo de intentos fallidos de acceso por defecto en iOS es de 10. Este valor máximo también puede ser modificado mediante las políticas de seguridad a través de los perfiles de configuración, las soluciones de gestión empresariales (MDM) o de Microsoft Exchange ActiveSync.

557. Puede verificarse si esta funcionalidad ha sido activada a través del menú "Ajustes - Código – Borrar datos":



558. Adicionalmente iOS proporciona 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).

Nota: Debe tenerse en cuenta que para que esta funcionalidad sea operativa el dispositivo móvil debe estar conectado a una red de datos, por lo que una de las primeras acciones que un atacante interesado en los datos almacenados en el terminal realizará es la extracción de la tarjeta SIM.

iOS no dispone de funcionalidad de emergencia existente en otros terminales, como BlackBerry, para eliminar los datos que contiene el dispositivo móvil si éste no ha estado conectado a la red y a la solución MDM durante un periodo de tiempo determinado.

559. Tal y como se mencionaba en el apartado "5.3. Gestión empresarial de dispositivos basados en iOS", a través de las soluciones de gestión empresariales (o MDM), o del servicio iCloud (ver apartado "5.22. Localización del dispositivo móvil: Buscar mi

iPhone"), los usuarios (o administradores) disponen de capacidades para borrar de forma remota los datos del dispositivo móvil (*wipe*), en caso de haber sido perdido o robado.

560. Adicionalmente, mediante Microsoft ActiveSync en el caso de disponer de una cuenta de Microsoft Exchange configurada en el dispositivo móvil, los administradores pueden hacer uso de las capacidades de borrado remotas (*wipe*) a través de la *Exchange Management Console* (Exchange Server 2007) o de la herramienta *Exchange ActiveSync Mobile Administration Web Tool* (Exchange Server 2003 o 2007), o los usuarios directamente a través de *Outlook Web Access* (Exchange Server 2007).

561. El proceso de borrado o *wipe* en el iPhone e iPhone 3G sobrescribe los datos del dispositivo móvil, por lo que conlleva aproximadamente una hora por cada 8GB de memoria. En el caso del iPhone 3GS o el iPad (o dispositivos posteriores), el proceso simplemente elimina la clave de cifrado empleada por el dispositivo móvil, por lo que es una operación casi inmediata [Ref.- 63].

562. 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 las aplicaciones instaladas, los datos y las configuraciones realizadas por el usuario.

563. Cuando un dispositivo móvil iOS se conecta (empareja o asocia) a un ordenador con iTunes, se establece una relación de confianza entre ambos.

564. Si se desea realizar un borrado completo de datos de un dispositivo móvil iOS, incluyendo tanto los datos y los ajustes de configuración como las relaciones de confianza existentes entre el dispositivo móvil y ordenadores con iTunes, es necesario emplear una restauración completa desde el modo DFU (*Device Firmware Update*) [Ref.- 69].

565. Este procedimiento permitiría la reutilización del dispositivo móvil iOS por parte de otro empleado, por ejemplo, dentro de la misma organización, como si se tratara de un dispositivo nuevo.

566. Para ello se debe conectar el dispositivo móvil iOS a un ordenador con iTunes, mantener pulsado los botones de encendido/apagado (u "On/Off") e inicio (o "Home") durante 10 segundos, soltar el botón de encendido/apagado manteniendo pulsado en botón de inicio, y soltar el botón de inicio una vez iTunes genera un mensaje de error indicando que el dispositivo está en modo recuperación ("recovery mode").

567. No es necesario que el ordenador con iTunes empleado disponga de una relación de confianza previa, ni disponer de la clave de acceso o PIN del dispositivo móvil iOS. Sin embargo, desde iOS 7 se deben tener en cuenta las restricciones existentes en el proceso de activación (ver apartado "5.5. Restricciones en el proceso de activación").

5.10 CONFIGURACIÓN POR DEFECTO DEL DISPOSITIVO MÓVIL

568. El dispositivo móvil está configurado por defecto con valores fijados por el fabricante del sistema operativo y del hardware, Apple en este caso, y ligeramente por el operador de telefonía móvil en función del perfil de configuración de iOS asociado a la tarjeta SIM. Estos valores pueden desvelar detalles del terminal o de su propietario.

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

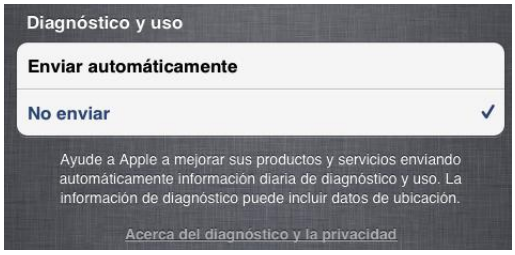
570. El nombre del dispositivo móvil iOS por defecto suele estar fijado a un valor asociado tanto al usuario como al tipo de dispositivo móvil, como por ejemplo "*Usuario iPhone 4s*" (igualmente con dispositivos iPad), aunque depende del sistema operativo empleado en el ordenador con iTunes y del usuario empleado en dicho ordenador.

571. En el caso de realizar la instalación, configuración y activación del dispositivo móvil a través de una red Wi-Fi sin emplear iTunes, el nombre empleado por defecto por iOS refleja el tipo de dispositivo móvil, como por ejemplo "iPhone" o "iPad".

572. El proceso de configuración inicial del dispositivo móvil iOS desde los ajustes de fábrica permite seleccionar el idioma, el país o región, y ajustar la configuración de los servicios de localización, habilitar la conexión a una red Wi-Fi (o conectarse mediante iTunes y cable USB) para proceder a la activación del dispositivo móvil, y aceptar los términos y condiciones de licencia de iOS. Sin embargo, no permite seleccionar o modificar el nombre del dispositivo móvil.

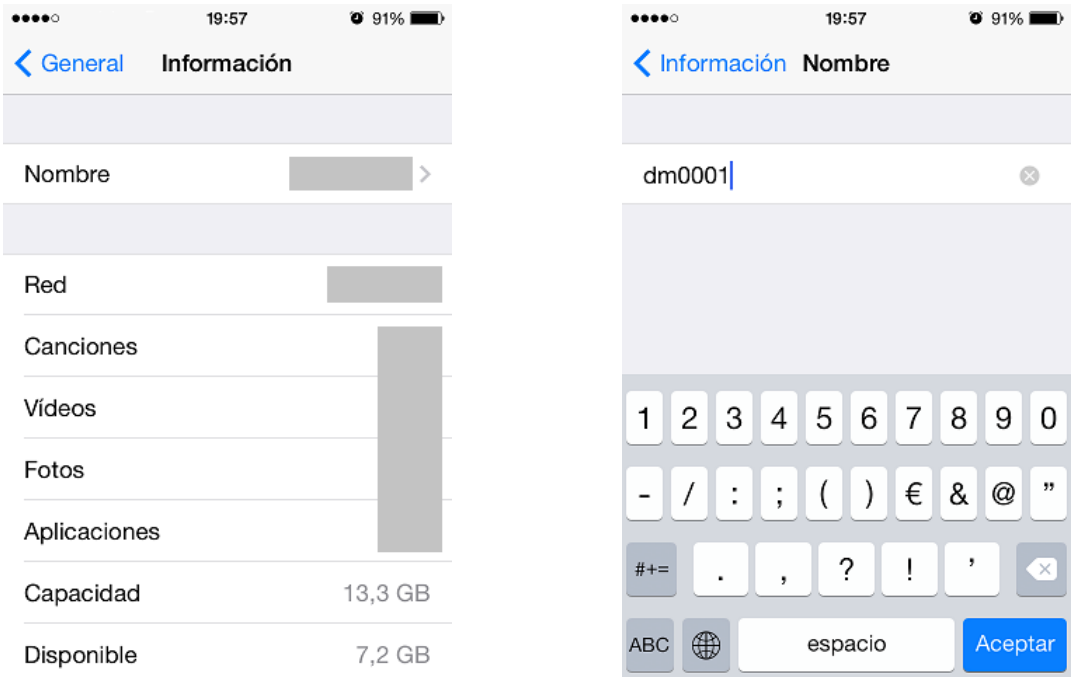
573. Por tanto, el valor por defecto más habitual es el menos recomendado desde el punto de vista de seguridad, ya que desvela información tanto de su propietario como del tipo de dispositivo móvil, por lo que se recomienda modificarlo lo antes posible.

574. Adicionalmente, durante el proceso de configuración inicial iOS solicita al usuario la posibilidad de remitir a Apple información de diagnóstico y uso del dispositivo móvil, incluyendo datos de su ubicación (ejemplo de iOS 5.x):



575. Se recomienda no permitir el envío de dicha información a Apple para evitar revelar detalles privados del uso y la ubicación del dispositivo móvil: opción "No enviar".

576. Los dispositivos móviles iOS permiten la modificación del nombre del dispositivo móvil a través del menú "Ajustes - General - Información", y en concreto de la opción "Nombre":



577. En caso de desvelarse el nombre del dispositivo en sus comunicaciones, como por ejemplo en el tráfico DHCP (donde se desvela el valor del nombre en el campo 12 de DHCP, "Host Name"; ver apartado "5.18.2. Seguridad en TCP/IP"), éste podría revelar detalles tanto del fabricante del dispositivo móvil, como por ejemplo el modelo de 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.

578. iOS emplea también el nombre del dispositivo móvil al hacer uso de diferentes servicios y tecnologías, como por ejemplo Bluetooth (ver apartado "5.13. Comunicaciones Bluetooth"), no disponiendo de otras opciones de configuración o ajustes para modificar su valor.

579. Desde el punto de vista de seguridad 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).

5.11 SERVICIOS DE LOCALIZACIÓN GEOGRÁFICA

580. Las capacidades o servicios de localización geográfica del dispositivo móvil (o geolocalización) a través de GPS (*Global Positioning System*), o de las redes de datos (telefonía móvil 2/3/4G y Wi-Fi), pueden ser activadas y desactivadas por el usuario en función de su utilización.

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

582. Diferentes aplicaciones integradas en iOS, como Mapas, la cámara (app Cámara), Safari en su acceso a sitios y aplicaciones web, así como otras aplicaciones de Apple y de terceros, pueden hacer uso de los servicios de localización geográfica.

583. El uso de los servicios de localización recientemente en el dispositivo móvil iOS viene reflejado por un icono en forma de punta de flecha en la barra superior de estado:

Nota: El dispositivo GPS (junto al resto de servicios de localización) en iOS está activo únicamente cuando se está haciendo uso de una aplicación con capacidades de localización, es decir, que hace uso del GPS.

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

585. En el caso de habilitar los servicios de localización, se hará automáticamente uso del módulo GPS (en caso de disponer de uno el dispositivo móvil iOS, como en el iPhone), si se dispone de cobertura suficiente para recibir la señal de los satélites GPS.

586. Si adicionalmente se dispone del interfaz Wi-Fi activo, se hará uso de la información recopilada de las redes Wi-Fi visibles y existentes en la ubicación actual en la que se encuentra el dispositivo móvil. En caso de no disponer del interfaz Wi-Fi activo y hacer uso de una aplicación que requiere capacidades de localización, iOS notificará al usuario del posible aumento de precisión al ser activado el interfaz Wi-Fi a la hora de determinar la ubicación actual (ver imagen inferior izquierda):

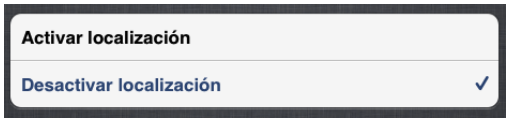
587. Adicionalmente, si además se tiene activado el interfaz de telefonía móvil del teléfono (en caso de disponer de éste el dispositivo móvil iOS; por ejemplo, iPhone), se hará uso de la información recopilada de las torres de telefonía móvil 2/3/4G existentes en la ubicación actual en la que se encuentra el dispositivo móvil (adicionalmente a las comunicaciones de datos).

588. Únicamente los dispositivos móviles iOS iPad con capacidades 3G (o 4G, celulares) disponen tanto de capacidades de telefonía móvil como de un módulo GPS interno. Por tanto, los modelos celulares de iPad hacen uso de ambas tecnologías para aumentar la precisión en la localización respecto a los modelos que sólo disponen de capacidades Wi-Fi. Todos los dispositivos móviles iPhone recientes (desde el iPhone 3G, incluido) disponen tanto de capacidades de telefonía móvil como de módulo GPS.

589. La ubicación se obtiene a través de la información de localización disponible sobre torres de telefonía móvil 2/3/4G y redes Wi-Fi, y la señal recibida en cada momento por el dispositivo móvil para ambas tecnologías (telefonía móvil y Wi-Fi), junto a la información más precisa proporcionada por el dispositivo o módulo GPS.

590. Los servicios de localización se habilitan o no durante el proceso inicial de configuración del dispositivo móvil iOS, por lo que no tienen asociado un valor por defecto.

591. Durante el proceso de configuración inicial asociado al dispositivo móvil empleado para la elaboración de la presente guía, iOS solicita al usuario si desea usar los servicios de localización: "Activar o desactivar localización" (ejemplo de iOS 5.x):



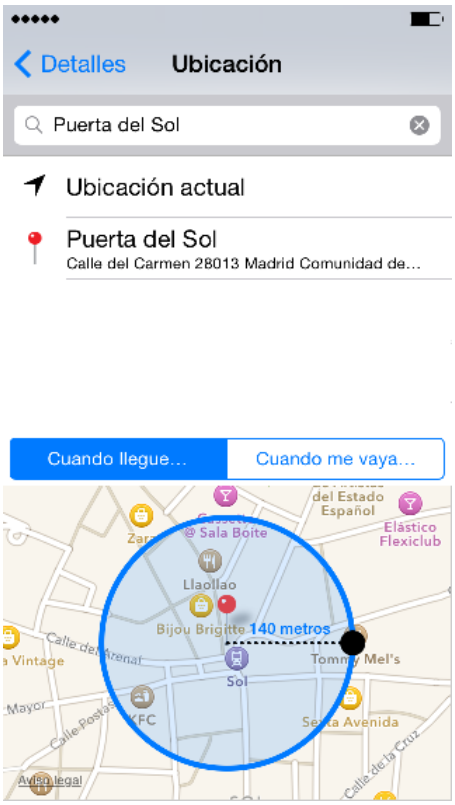
592. Se recomienda desactivar la localización durante el proceso inicial de configuración y habilitarla posteriormente y de forma más personalizada únicamente para ciertas aplicaciones.

593. En caso de no activar dichos servicios, iOS notifica al usuario que Mapas y otras aplicaciones no podrán hacer utilizar la ubicación aproximada del usuario, pero que pueden ser habilitados posteriormente desde el menú "Ajustes".

594. El centro de control de los servicios de localización de iOS (bajo la sección "Privacidad" desde iOS 7) permite gestionar de forma individual estas capacidades para cada una de las aplicaciones que pueden hacer uso de las mismas.

595. Este centro de localización proporciona información detallada, a través del icono de localización de color violeta descrito previamente, para cada una de las aplicaciones existentes, indicando si está haciendo uso de estos servicios actualmente o si ha hecho uso de estos durante las últimas 24 horas (si el icono de localización es de color gris).

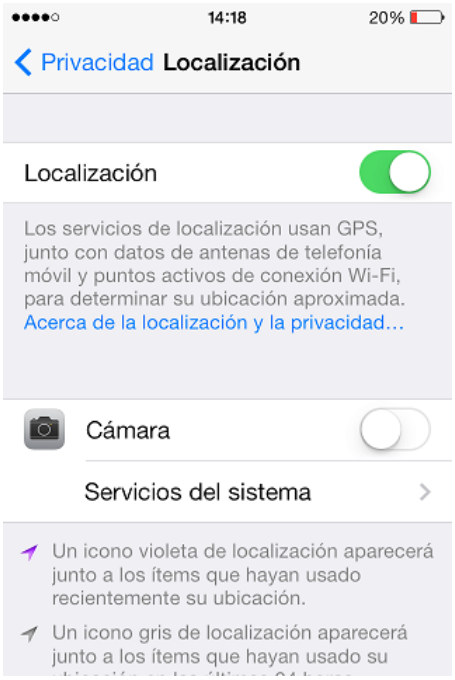
596. Si el icono de localización muestra únicamente el contorno (de color violeta), indica que la app está haciendo uso de una geocerca (*geofence*). Una geocerca es un perímetro virtual alrededor de una ubicación geográfica, y algunas aplicaciones, como por ejemplo Recordatorios, hacen uso de estas geocercas para generar notificaciones cuando el usuario se aproxima o aleja de dicha ubicación:

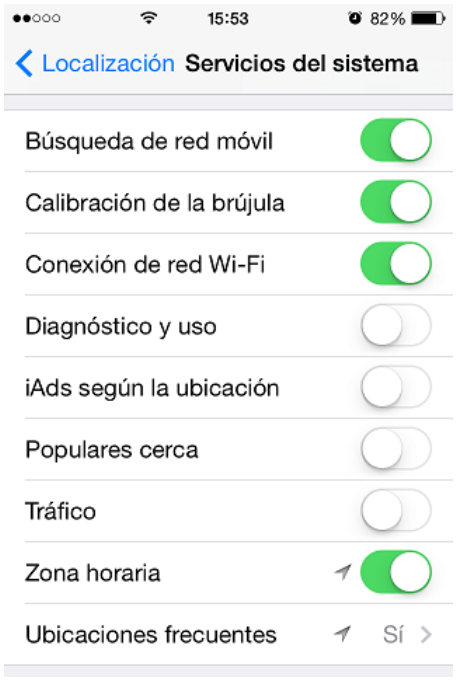


597. El usuario debe por tanto habilitar de forma global las capacidades o servicios de localización de iOS, y por otro, dar permiso de forma individual a las aplicaciones (o sitios web) que desea dispongan de la información de su ubicación actual. Esta granularidad es la más conveniente desde el punto de vista de seguridad. Para ello muestra una lista con todas las apps instaladas que disponen de capacidades asociadas a los servicios de localización y que han solicitado en algún momento utilizarlas.

598. Por otro lado, desde el menú “Ajustes - Privacidad - Localización”, y en concreto a través de la opción “Servicios del sistema”, es posible configurar qué servicios de iOS (Búsqueda de red móvil, Calibración de la brújula, Zona horaria, etc) dispondrán de

acceso a los servicios de localización. Por defecto, todos los servicios del sistema disponen de estos permisos:





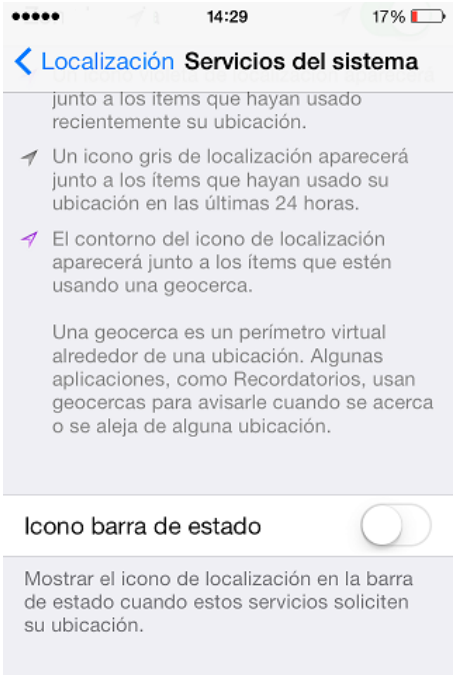
599. Por ejemplo, la opción "Zona horaria" es utilizada para el ajuste automático del reloj del dispositivo móvil en función de la zona horaria donde se encuentre el usuario, asociado a la opción de reloj disponible en "Ajustes - General - Fecha y hora - Ajuste automático" (y "Zona horaria").

600. A modo de resumen, la opción "Búsqueda de red móvil" permite localizar más rápidamente redes de telefonía móvil a la hora de conectarse a ellas, la opción "Calibración de la brújula" es auto-descriptiva, la opción "Conexión de red Wi-Fi" obtiene información de redes Wi-Fi cercanas y la envía a Apple para actualizar la base de

datos de redes Wi-Fi y su localización a nivel mundial, la opción "Diagnóstico y uso" remite a Apple información sobre el uso de estos servicios de localización, la opción "iAds según la ubicación" ha sido analizada en el apartado "5.2.1. Controles de acceso y privacidad", la opción "Populares cerca" permite obtener recomendaciones de sitios cercanos al usuario, la opción "Tráfico" proporciona información sobre las condiciones del tráfico a la aplicación de "Mapas" y la opción "Ubicaciones frecuentes" es analizada posteriormente.

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

602. Adicionalmente, la opción "Icono barra de estado" (deshabilitada por defecto) situada en la parte inferior de la pantalla permite visualizar en la barra superior de estado si los servicios de sistema están haciendo uso de los servicios de localización:



603. Se recomienda, por un lado, deshabilitar los servicios de localización para todos aquellos servicios del sistema que no sean utilizados, y especialmente, aquellos complementarios o que pueden afectar a la privacidad del usuario como "Diagnóstico y uso" o "iAds según la ubicación".

604. Por otro lado, se recomienda habilitar el icono de localización en la barra de estado para que el usuario pueda ser consciente de las actividades del dispositivo móvil y, en concreto, de cuando se hace uso de los servicios de localización por parte de los servicios del sistema.

Nota: Existen estudios publicados en abril de 2011 que reflejan que la información de localización y los desplazamientos del usuario con el dispositivo móvil recopilada por iOS, en concreto en base a las torres de telefonía móvil, es almacenada en el dispositivo móvil y en la copia de seguridad asociada en iTunes, sin cifrar. Esta funcionalidad está disponible en iOS desde la versión 4.0 y es empleada como parte de los servicios de localización de iOS.

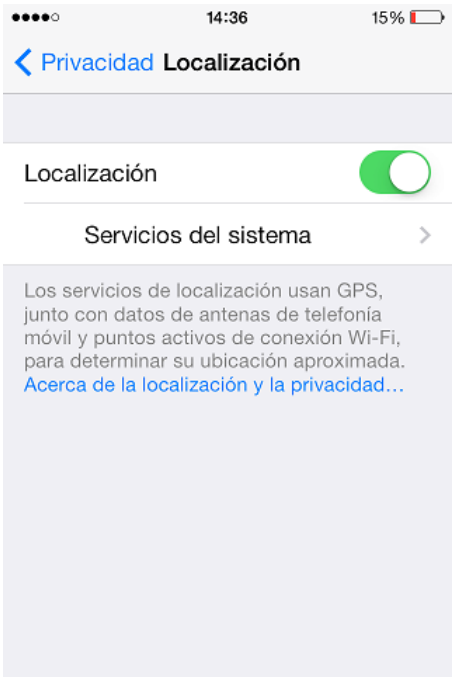
Existe una aplicación, iPhone Tracker (http://petewarden.github.com/iPhoneTracker/) para OS X, o para Windows (http://huseyint.com/iPhoneTrackerWin/), que permite acceder a la información almacenada y visualizar los datos recopilados.

Apple incorporó mejoras en la actualización de iOS 4.3.3 [Ref.- 108] para reducir el tamaño de la base de datos (o caché) almacenada en el dispositivo ("consolidated.mdbd"), evitando su almacenamiento en las copias de seguridad realizadas a través de iTunes del dispositivo móvil, y eliminando los datos del fichero al desactivar los servicios de localización.

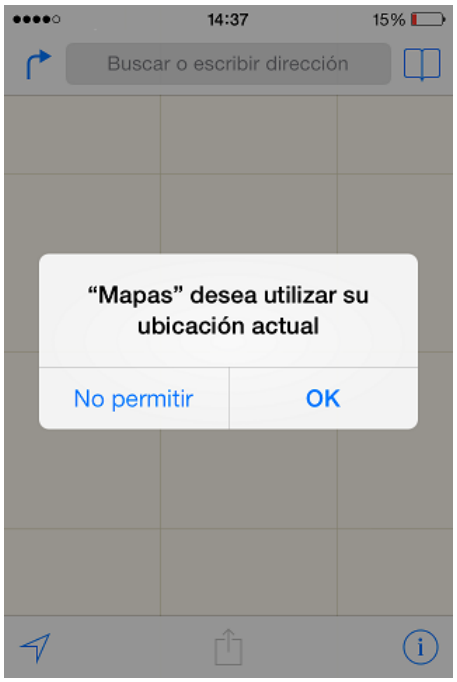
Este hecho ratifica la necesidad de cifrar tanto los contenidos del dispositivo móvil como las copias de seguridad en iTunes con el objetivo de evitar que un tercero pueda disponer de acceso no autorizado a esta información, vulnerando la privacidad del usuario.

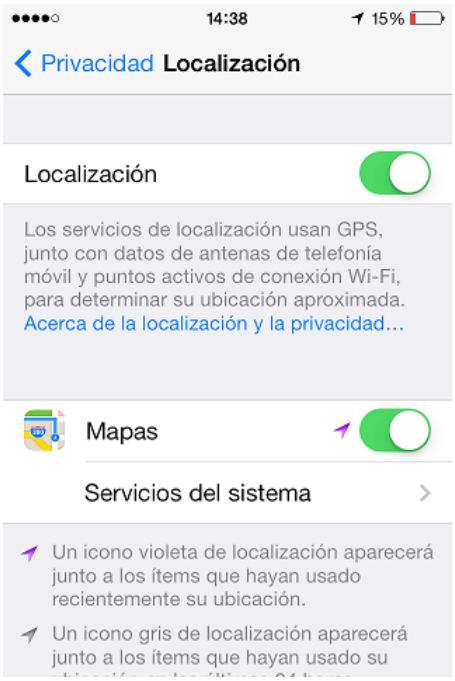
605. Adicionalmente, en iOS es posible restablecer todos los ajustes de los avisos de localización de las diferentes aplicaciones a los valores por defecto de fábrica, es decir ninguna configuración previa, a través del menú "Ajustes - General - Restablecer" y la opción "Restablecer localización y privacidad":

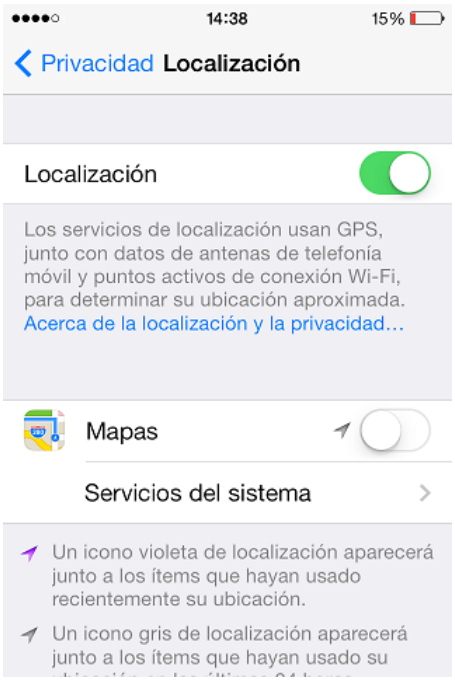
606. Tras seleccionar esa opción, introducir el código de acceso para proceder a modificar los ajustes, y confirmar la acción, iOS eliminará todas las aplicaciones de los servicios de localización (excepto la funcionalidad de búsqueda del iPhone), y éstas serán añadidas progresivamente según sean utilizadas de nuevo, soliciten y hagan uso de estos servicios:



607. Cada vez que una aplicación solicita acceso a los servicios de localización, ésta es añadida al centro de gestión de estos servicios. Si no se permite el acceso, aparecerá como desactivada, y si sí se permite dicho acceso, estará activada en el centro de gestión:







608. Se recomienda deshabilitar los servicios de localización del dispositivo móvil salvo que se esté haciendo uso explícito de esta funcionalidad, tanto de forma global como independiente para las diferentes aplicaciones (de usuario y de sistema) disponibles, y habilitarlos únicamente en función de su uso.

5.11.1 UBICACIONES FRECUENTES

609. Al igual que con otros mensajes de autorización relacionados con la privacidad, al comenzar a utilizar iOS 7 se le preguntará al usuario si permite al dispositivo móvil recabar información sobre las rutas y lugares que se visitan.

610. Bajo la sección "Ubicaciones frecuentes" del menú "Ajustes - Privacidad - Localización - Servicios del sistema" se dispone de información de los lugares que son visitados frecuentemente por el dispositivo (tras aceptar el mensaje que solicita el acceso a estos datos) o historial. Esta información es almacenada en el dispositivo móvil, y se emplea para proporcionar información útil en base a la ubicación, y es transmitida a Apple de manera anónima para la mejora de la apps de Mapas:

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

612. Los ajustes de configuración permiten la activación individualizada de la utilización de los datos de las ubicaciones frecuentes para mejorar la apps de Mapas, y por tanto, del envío de esta información a Apple.

613. Si no se desea que Apple obtenga información sobre las ubicaciones frecuentes, y realice la correlación de éstas con la dirección postal asociada al Apple ID del usuario para la

mejora de los Mapas, se recomienda deshabilitar esta funcionalidad desde el punto de vista de la privacidad.

5.11.2 ASSISTED GPS (A-GPS)

614. Todos los dispositivos móviles iOS con módulo GPS (iPhone e iPad celular) hacen uso de una tecnología conocida como *Assisted* GPS o A-GPS (AGPS o aGPS) [Ref.- 65].

615. *Assisted GPS* es un sistema de ayuda para mejorar la obtención de información de localización mediante GPS, que utiliza tanto datos sobre la localización actual de los satélites GPS, como datos de las torres de telefonía móvil 2/3/4G e información de las redes Wi-Fi cercanas, para disponer de una estimación de la ubicación del dispositivo móvil más rápidamente.

616. La funcionalidad de datos de A-GPS, y de localización geográfica en general de iOS, envía tráfico cifrado de datos hacia los servidores de Apple denominados "gs-loc.apple.com" y "gspN-ssl.apple.com" (dónde N es un número de un dígito), empleando el puerto 443/tcp (HTTPS). También se hace uso del servidor "iphone-ld.apple.com" para la realización de consultas.

617. Si los servicios de localización están activos, esta comunicación es empleada también por iOS de forma periódica, supuestamente anónima y cifrada, para enviar a Apple información sobre redes Wi-Fi y torres de telefonía en diferentes ubicaciones y alimentar así las bases de datos de geolocalización utilizadas por este servicio [Ref.- 64].

618. iOS 7 emplea el siguiente "User-Agent" (ejemplo de iOS 7.0.4; similar en función de la versión de iOS empleada) para proporcionar los datos de localización de las redes Wi-Fi:

```
User-Agent: locationd/1613.5.1 CFNetwork/672.0.8 Darwin/14.0.0
```

619. Adicionalmente, si los servicios de localización están activos y el dispositivo móvil iOS dispone de GPS, enviará información de las coordenadas y la velocidad de desplazamiento (al viajar por ejemplo en coche) para recopilar datos de tráfico y carreteras [Ref.- 64].

Nota: El alcance de la presente guía no contempla la realización de un análisis de seguridad detallado de los protocolos de comunicaciones internos protegidos mediante HTTPS (o SSL/TLS) y empleados entre los dispositivos móviles iOS y los servidores de Apple para ofrecer diferentes servicios, como por ejemplo los servicios de localización.

620. Los dispositivos móviles iOS no emplean la infraestructura estándar A-GPS. Habitualmente, los servidores A-GPS pueden ser proporcionados por los operadores de telefonía móvil (“agps.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” (“supl.operador.es”).

Nota: Debido a que el tráfico entre el dispositivo móvil y los servidores de Apple está cifrado, sin realizar un análisis detallado, se desconoce si la implementación de A-GPS de iOS, con el objetivo de agilizar el proceso de localización de coordenadas del GPS y su precisión, emplea gpsOneXTRA (también conocida como QuickGPS en otras plataformas móviles). Esta funcionalidad típicamente se conecta mediante HTTP (80/tcp) 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. Una vez conocida la situación actual de los satélites, el módulo GPS puede identificar la localización del dispositivo más rápidamente y con mayor precisión. La documentación de Apple parece indicar que su módulo A-GPS también hace uso de la información de la localización actual de los satélites GPS [Ref.- 140].

621. Debe tenerse en cuenta que pese a que el dispositivo móvil disponga de módulo de GPS, hay escenarios en los que no es posible obtener señal de GPS (por ejemplo, en el interior de edificios), por lo que las aplicaciones harán uso de las capacidades de localización de iOS sin GPS si estás han sido habilitadas (interfaz Wi-Fi y de telefonía móvil).

622. iOS no permite deshabilitar la funcionalidad A-GPS en caso de no querer hacer uso explícito de estas capacidades, por ejemplo, con el objetivo de usar únicamente el módulo GPS y evitar desvelar información de la ubicación del dispositivo móvil (por ejemplo y potencialmente, la torre de telefonía a la que está asociado o las redes Wi-Fi cercanas) a través del tráfico de datos destinado a los servidores A-GPS.

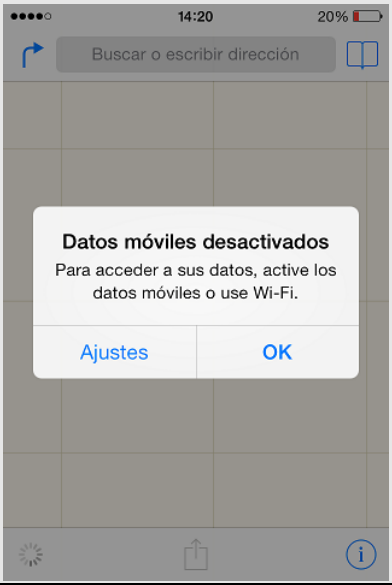
623. La única forma de impedir dicho tráfico es deshabilitando tanto el interfaz Wi-Fi como el interfaz de datos de telefonía móvil, aunque debe tenerse en cuenta que en el caso de iOS, el tráfico de datos que contiene esa información es cifrado entre el dispositivo móvil y los servidores de Apple previamente enumerados.

5.11.3 SERVICIO DE LOCALIZACIÓN DE MAPAS

624. Los servicios de localización con o sin GPS son utilizados, entre otros, por la aplicación oficial de mapas, asociada al servicio de mapas de Apple, que en el caso de iOS, está disponible como aplicación por defecto a través del icono “Mapas”.

Nota: Desde la versión iOS 6 la aplicación de mapas disponible por defecto pertenece a Apple. En versiones previas de iOS, como iOS 5, se incluía Google Maps como aplicación de mapas predeterminada. Google Maps puede ser aún instalada en iOS a través de la App Store.

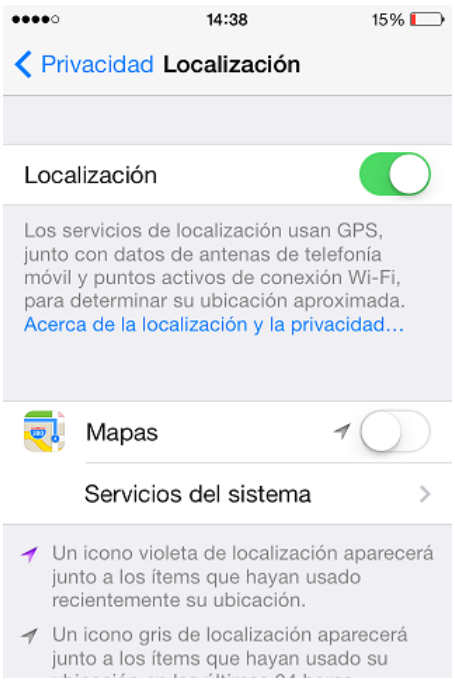
La aplicación "Mapas" requiere de una conexión de datos (telefonía móvil o Wi-Fi) para funcionar y acceder a la información cartográfica de los mapas. En caso de no disponer de conexión, iOS notificará al usuario:



625. La aplicación oficial de "Mapas" desde iOS 6 dispone de capacidades de navegación paso a paso por voz, integración con Siri, información de tráfico en tiempo real, visualización de los mapas en 3D (*flyover*), etc. Algunas de estas características, como por ejemplo la navegación paso a paso o *flyover*, sólo están disponibles para ciertos modelos de dispositivos móviles (como por ejemplo el iPhone 4S, iPad2 o superiores).

626. Desde "Mapas" es posible hacer uso de la información y servicios de localización, en concreto, a través del icono previamente descrito en forma de flecha y disponible en la parte inferior izquierda, que centrará el mapa en la localización o ubicación actual del usuario (identificada por una bola azul).

627. Como ejemplo y tal y como se ha descrito previamente, es posible deshabilitar el servicio de localización de iOS en cualquier momento desde el menú “Ajustes - Privacidad - Localización”, y en concreto mediante la opción asociada a la aplicación "Mapas" (ver imagen inferior izquierda):



628. En caso de haber deshabilitado los servicios de localización para la aplicación, iOS notificará al usuario de la necesidad de activar esa funcionalidad para poder hacer uso de ella (ver imagen superior derecha).

629. Al hacer uso de aplicaciones que requieren conocer la ubicación del usuario, como "Mapas", si los servicios han sido habilitados 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 la información de localización disponible sobre torres de telefonía móvil y redes Wi-Fi.

630. El servicio de ubicación de "Mapas" de Apple (desde iOS 6.x) emplea conexiones HTTP (no cifradas) desde el dispositivo móvil hacia “gspa*19*.ls.apple.com” (“/tile.vf?”), enviando a Apple numerosos parámetros GET relativos a la ubicación. Estas peticiones son respondidas con imágenes JPEG asociadas a los mapas.

631. Este tipo de peticiones HTTP también desvelan la app del dispositivo móvil en su cabecera "User-Agent":

```
User-Agent: com.apple.Maps
```

632. Los datos intercambiados en las peticiones HTTP adicionalmente revelan la ubicación y el idioma empleados (“ES”), en concreto hacia el servidor "gsp1.apple.com", así como información del módulo cliente en el dispositivo móvil:

```
User-Agent: Mapas/1.0 CFNetwork/672.1.15 Darwin/14.0.0
```

633. En resumen, estas peticiones de información no cifradas hacia Apple desvelan información de la ubicación 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, también contienen información de la ubicación estimada del dispositivo móvil.

634. Sin embargo, la información más detallada de localización, que podría incluir detalles de las redes, Wi-Fi y de telefonía, existentes en el área de cobertura del dispositivo móvil, es intercambiada mediante tráfico cifrado con servidores específicos de Apple.

635. Se recomienda limitar el uso del servicio de localización en la aplicación "Mapas", y específicamente su utilización empleando el interfaz Wi-Fi y de telefonía móvil (además del 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 en el tráfico de red.

5.11.4 OTRAS APLICACIONES QUE HACEN USO DE LA LOCALIZACIÓN

636. Diferentes aplicaciones y funcionalidad disponible por defecto en iOS puede hacer uso de los servicios de localización, como Mapas, App Store, Cámara, Safari, Twitter, Brújula, Tiempo o "Buscar mi iPhone" (y otras, añadidas dinámicamente al ser utilizadas), tal como refleja el centro de gestión asociado ("Ajustes - Privacidad - Localización"). A continuación se analizan algunas de estas aplicaciones, centrándose en la utilización de los servicios de localización:

5.11.4.1 *Tiempo*

637. La aplicación "Tiempo", asociada al icono "Tiempo", proporciona información meteorológica empleando los servicios de Yahoo sobre diferentes ubicaciones (o ciudades) predefinidas por el usuario, pero también puede proporcionar información sobre el tiempo local en función de la ubicación del usuario.

638. Cada una de las ubicaciones predefinidas por el usuario dispone de su pantalla asociada (indicadas por una serie de puntos en la parte inferior central).

639. El icono de punta de flecha situado en la parte inferior central de la pantalla de la app "Tiempo" (ver imagen inferior derecha) permite hacer uso de los servicios de localización para obtener la ubicación actual del usuario (local) y sus datos meteorológicos (empleada por defecto):

Nota: La aplicación "Tiempo" requiere de una conexión de datos (telefonía móvil o Wi-Fi) para funcionar y acceder a la información meteorológica actual. En caso de no disponer de conexión, iOS notificará al usuario. "Tiempo" hace uso de los servicios de meteorología de Yahoo, con numerosas peticiones HTTP hacia servidores de "yahooapis.com".

640. iOS establece conexiones con Yahoo (http://apple-mobile.query.yahooapis.com) mediante HTTP, sin cifrar, y en concreto al recurso "/v1/yql?", empleando el agente de usuario (User-Agent) "Tiempo/1.0 CFNetwork/672.0.8 Darwin/14.0.0" (por ejemplo para iOS 7.0.4) y un conjunto de cabeceras HTTP "X-..." (no estándar) que desvelan detalles del dispositivo móvil, más los parámetros ("env" y "q") para realizar la consulta de información meteorológica a través de SQL. El agente de usuario permite identificar la aplicación empleada, el tipo de dispositivo iOS y la versión de iOS. Esta información es complementada por las cabeceras HTTP "X-...", incluyendo un UUID y autentificación mediante OAuth.

641. Este UUID es un identificador, qué no corresponde con el UDID (Unique Device IDentifier) de los dispositivos móviles Apple (ver apartado "5.27. Aplicaciones de terceros: App Store").

642. Los intercambios de datos entre la aplicación y el servicio de Yahoo mediante HTTP se realizan en formato XML para todas las ubicaciones predefinidas por el usuario simultáneamente.

643. Se recomienda no hacer uso de este tipo de servicios que desvelan información detallada de la ubicación (o los intereses) 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.

5.11.4.2 *Redes sociales*

644. 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:

645. La opción de configuración para habilitar o deshabilitar la gestión de la ubicación del usuario en Twitter se realiza igualmente desde el centro de gestión de la localización de iOS (ver imagen superior derecha).

646. Esta funcionalidad estará disponible en la aplicación de la red social si el servicio de ubicación está habilitado en el dispositivo móvil y por ejemplo, en el caso de Twitter, permite añadir la ubicación del usuario a la hora de publicar un mensaje (o *tweet*) mediante el botón de ubicación situado en la parte inferior izquierda del mensaje:

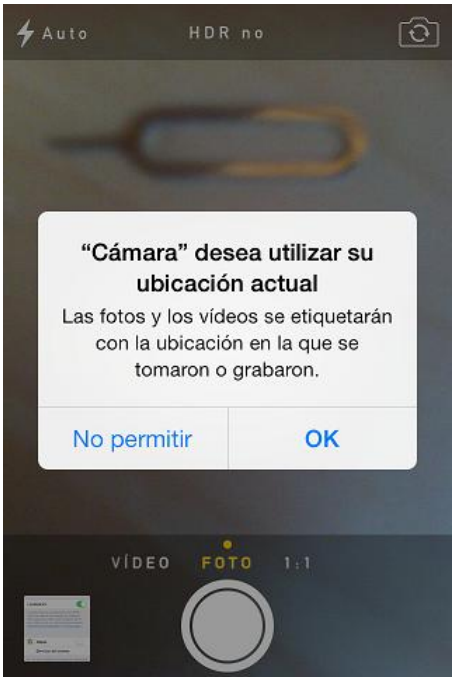
647. Para que la ubicación del usuario sea compartida a través de Twitter, el usuario debe activar esta funcionalidad explícitamente a través del botón destinado a tal efecto (descrito previamente) a la hora de escribir un nuevo mensaje o *tweet* (opción desaconsejada desde el punto de vista de seguridad).

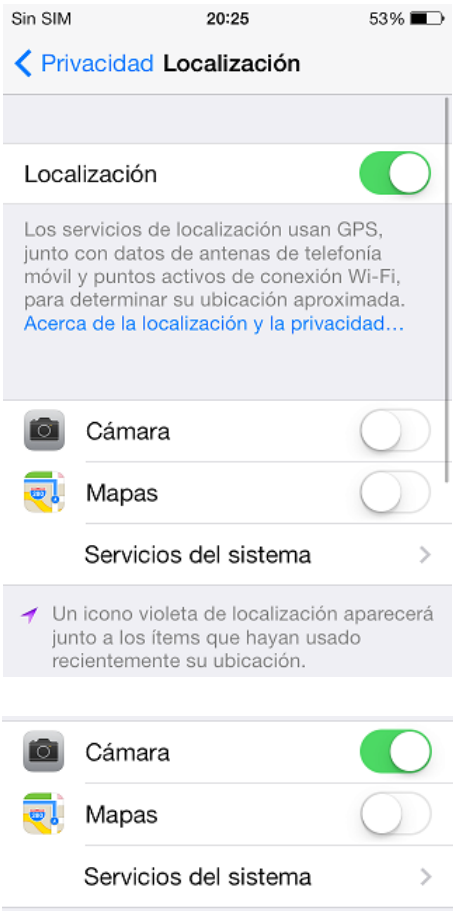
648. Se recomienda no hacer pública la ubicación en la que se encuentra el usuario en redes sociales o servicios similares con el objetivo de proteger su privacidad.

5.11.5 INFORMACIÓN GEOGRÁFICA EN FOTOGRAFÍAS

649. iOS permite añadir información de la localización geográfica a las fotografías realizadas con la cámara del dispositivo móvil, información conocida como geoetiquetas (o *geotags*). Al realizar la fotografía se añaden las coordenadas GPS en el momento de tomar la instantánea a la cabecera EXIF de la imagen.

650. Por defecto, iOS no tiene definido si la información de localización se incorporará a las fotografías tomadas con el dispositivo móvil. La primera vez que se hace uso de la cámara, iOS solicita permiso al usuario para incorporar la información de localización a las fotografías (ver imagen inferior izquierda):

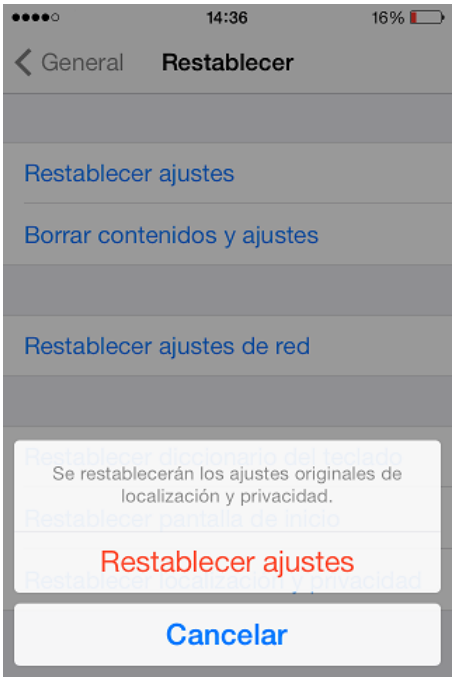




651. Esta funcionalidad es utilizada automáticamente por iOS una vez la aplicación "Cámara" ha sido añadida al centro de gestión de localización de iOS (ver imagen superior derecha, ejemplo mostrando que la funcionalidad puede ser deshabilitada de nuevo).

652. A través del menú de configuración del centro de gestión de localización es posible habilitar o deshabilitar la incorporación de esta información a las fotografías que se realicen con la cámara.

653. Si se desea que el usuario vuelva a ser preguntado acerca de dicho acceso, es necesario restablecer los avisos de localización a los valores por defecto de fábrica, a través del menú "Ajustes - General - Restablecer" y la opción "Restablecer localización y privacidad":



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

5.12 COMUNICACIONES USB

655. La conexión USB del dispositivo móvil a un ordenador proporciona dos funcionalidades o tipos de conexiones diferentes:

- Unidad de disco, para compartir la capacidad o memoria de almacenamiento del dispositivo móvil con el ordenador.
- Conexión de telefonía móvil de datos, o *tethering*, para compartir la conexión de datos de telefonía móvil (2/3/4G) o Wi-Fi del dispositivo móvil con el ordenador.

656. iOS no permite utilizar los dispositivos móviles de Apple como unidad de disco USB externa independiente, salvo en aquellos dispositivos dónde se haya aplicado el proceso de *jailbreak* y mediante aplicaciones de terceros.

657. A través de la utilización de aplicaciones específicas desde el ordenador, como i-FunBox (disponible para Windows y OS X respectivamente), DiskAid o iExplorer [Ref.- 100], es posible acceder al sistema de ficheros (con ciertas limitaciones si no se ha realizado el proceso de *jailbreak*).

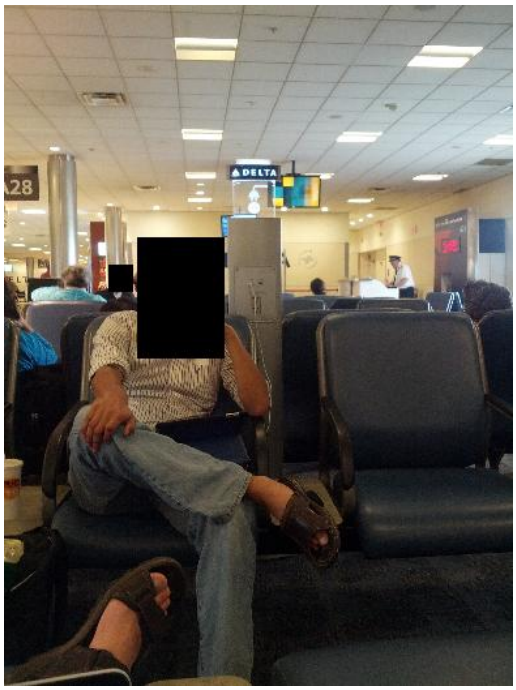
658. Las capacidades de *tethering* de iOS sólo permiten compartir la conexión de datos de telefonía móvil (2/3/4G) del dispositivo móvil con el ordenador, y no así la conexión Wi-Fi a través de USB o Bluetooth.

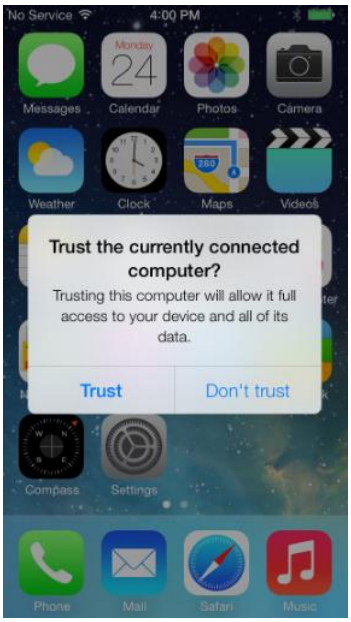
659. Apple denomina las capacidades de *tethering* desde el iPhone 3GS (o superior) con el término *Personal Hotspot* [Ref.- 67].

5.12.1 RELACIONES DE CONFIANZA EN LAS CONEXIONES MEDIANTE USB

660. Durante el año 2013, unos investigadores de Georgia Tech (GTISC) demostraron la posibilidad de instalar apps maliciosas en iOS sin la intervención del usuario, y extraer información del dispositivo móvil, a través de la utilización de un cargador de electricidad malicioso (denominado Mactans [Ref.- 163]), vulnerabilidad que afectaba a las últimas versiones de iOS 6.x disponibles en ese momento.

661. Una tarea diaria tan habitual como la carga de la batería del dispositivo móvil, debido a las capacidades de transmisión tanto de corriente eléctrica como de datos del puerto USB, puede volverse muy peligrosa en el caso de hacer uso de cargadores que no sean confiables. Apple solucionó el problema en iOS 7 notificando al usuario de la existencia de una conexión de datos al conectar su dispositivo a un periférico externo:





662. Este nuevo mecanismo de seguridad introducido en iOS 7 requiere que se establezca una relación de confianza entre el dispositivo móvil y el ordenador de sobremesa (PC o Mac) al llevar a cabo una conexión mediante el puerto USB:

663. Para poder aprobar desde el dispositivo móvil el establecimiento de esta relación de confianza con el ordenador a través de USB es necesario disponer del código de acceso y desbloquear previamente el dispositivo.

5.12.2 CONEXIÓN DE RED USB (*TETHERING*)

664. La opción de conexión compartida, o *tethering*, permite compartir la conexión de datos de telefonía móvil (2/3/4G) del dispositivo móvil con el ordenador a través de USB, Bluetooth o Wi-Fi.

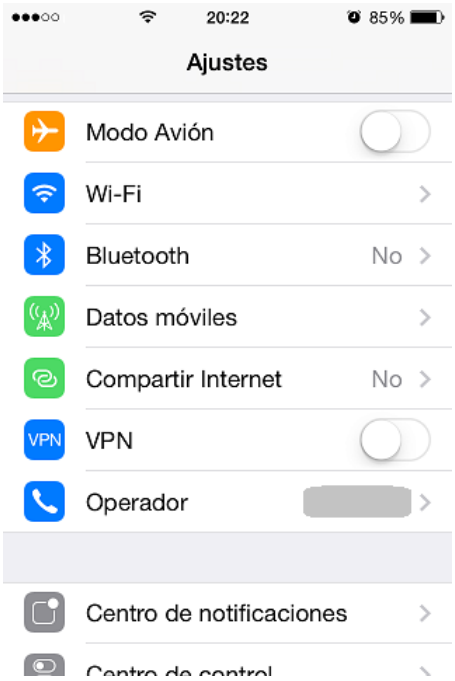
665. Desde el punto de vista de seguridad se recomienda hacer uso de *tethering* mediante cable USB, en lugar de mediante Bluetooth. Los detalles de la conexión compartida de datos a través del interfaz Wi-Fi se analizan en el apartado "5.14.7. Punto de acceso Wi-Fi".

666. El icono de notificación empleado por iOS para la conexión de *Personal Hotspot* en la barra superior de estado, tanto por USB, Bluetooth o Wi-Fi, corresponde a dos anillos entrelazados:

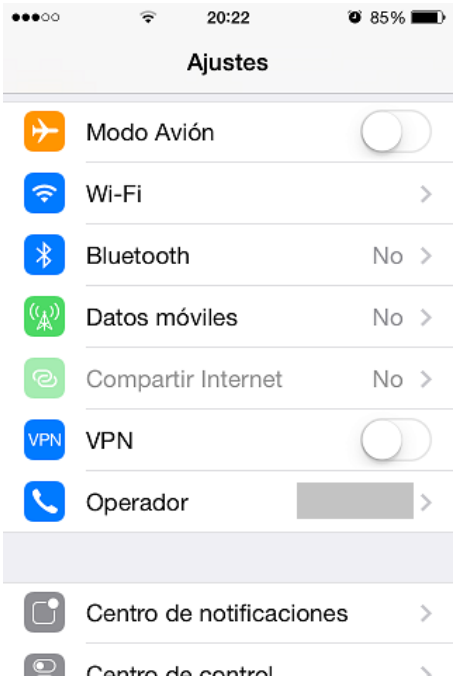
667. Las capacidades de *Personal Hotspot* por USB y por Wi-Fi (ver apartado “5.14.7. Punto de acceso Wi-Fi”) pueden ser utilizadas simultáneamente en iOS, proporcionando conexión de red a otros dispositivos u ordenadores simultáneamente tanto por USB como por Wi-Fi.

668. iOS proporciona capacidades nativas de *tethering* o *Personal Hotspot* mediante USB para Windows XP SP3 (o posterior) y OS X 10.5.8+, siendo necesario disponer de iTunes 9.2 (o posterior) instalado en el ordenador (o al menos de ciertos componentes como AppleApplicationSupport.msi y AppleMobileDeviceSupport.msi en Windows) [Ref.-67].

669. Para hacer uso de estas capacidades es necesario conectar el dispositivo móvil al ordenador mediante USB y acceder al menú “Ajustes - Compartir Internet" [Ref.- 68]:



670. La opción "Compartir Internet" está únicamente habilitada tras activar la conexión de datos de telefonía móvil (2/3/4G) desde el menú “Ajustes - Datos móviles" (sino aparecerá en color gris o sombreado, como en la imagen inferior):



671. En caso de activar los datos móviles y no disponer aún de dicha opción, se debe a que la configuración del operador de telefonía móvil empleado no permite *tethering*. Para habilitar la opción será necesario actualizar la configuración del operador de telefonía móvil en iOS, o emplear un operador de telecomunicaciones diferente [Ref.- 70].

672. A través del botón “Compartir Internet” es posible habilitar el servicio de *tethering*, de forma que el ordenador utilice el dispositivo móvil como su conexión principal de red:

Nota: Al habilitar la conexión compartida de red o *tethering*, si los interfaces de Bluetooth y Wi-Fi de iOS están deshabilitados, la conexión sólo estará disponible por defecto a través de USB (ver imagen superior derecha, opción "Sólo USB").

673. Tras establecerse la conexión de red, y tomando OS X como sistema operativo del ordenador de referencia, se crea automáticamente un interfaz de red configurado con una dirección IP dinámica (DHCP) con máscara /28 (255.255.255.240), como por ejemplo 172.20.10.2.

674. La configuración de este interfaz de red toma todos los valores por defecto existentes en el sistema operativo del ordenador. 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.

675. El dispositivo móvil (por ejemplo, con dirección IP 172.20.10.1) actúa de *gateway*, *router* o pasarela por defecto, de servidor DHCP, y los servidores DNS asignados mediante DHCP corresponden a los servidores DNS públicos obtenidos por iOS en la conexión de datos de telefonía móvil (2/3/4G), y es alcanzable mediante ping (ICMP).

Nota: El direccionamiento IP empleado por iOS para el acceso *tethering* por cable USB (172.20.10.x/28) no puede ser modificado.

676. 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 “AC:DE:48” (podría variar entre distintas versiones de iOS), qué está reservado por el IEEE, y por tanto no asignado a ningún vendedor. El valor completo no parece corresponder con el valor de la dirección MAC del interfaz Bluetooth o Wi-Fi del dispositivo móvil.

677. Un análisis de los puertos TCP/IP y servicios disponibles en el interfaz de red del dispositivo móvil empleado para el acceso por USB a través del dispositivo móvil permite obtener un perfil similar al del punto de acceso Wi-Fi (ver apartado "5.14.7. Punto de acceso Wi-Fi").

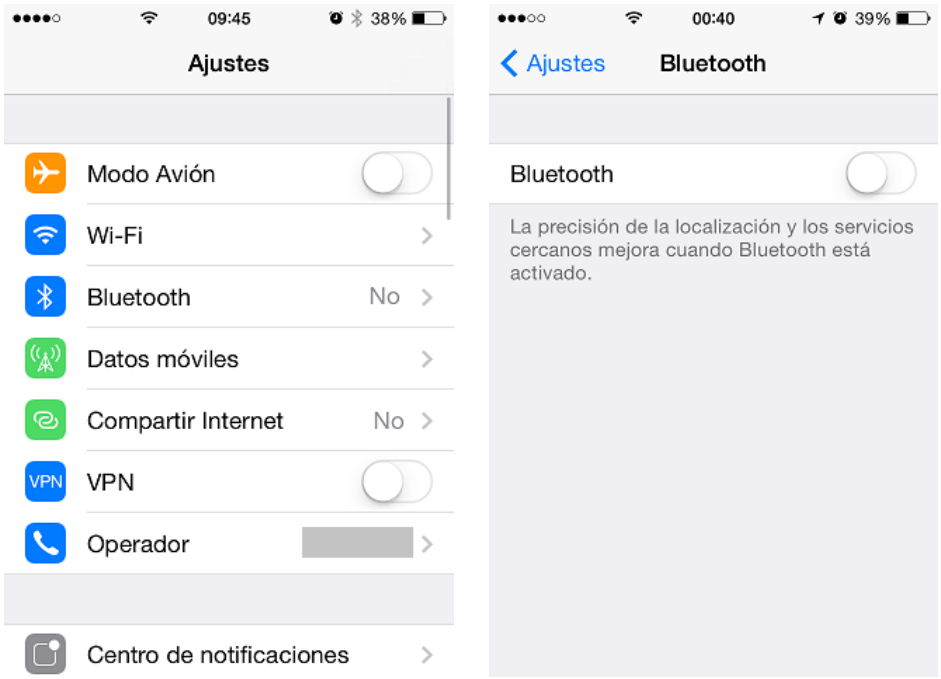
678. Es posible finalizar la conexión compartida de datos deshabilitando la opción “Compartir Internet” habilitada previamente, opción recomendada desde el punto de vista de seguridad una vez no se desea disponer de la conexión de red por USB.

5.13 COMUNICACIONES BLUETOOTH

5.13.1 DESACTIVACIÓN DE LAS COMUNICACIONES BLUETOOTH

679. 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.- 82].

680. El interfaz inalámbrico Bluetooth puede ser desactivado en iOS, situación por defecto, a través del menú “Ajustes - Bluetooth”, mediante el botón “Bluetooth”:



681. 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 y el siguiente icono:

682. iOS 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.

683. Adicionalmente, tras aplicar la actualización de una nueva versión de iOS, el interfaz Bluetooth será activado, independientemente de cuál era su estado antes de la

actualización. Se recomienda por tanto deshabilitar el interfaz Bluetooth tras cada actualización de iOS.

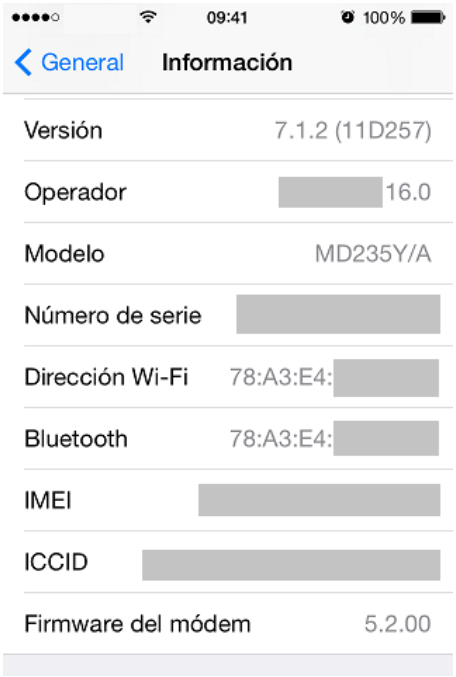
684. La activación inicial del interfaz Bluetooth se llevará a cabo tan pronto el dispositivo móvil se haya reiniciado, incluso aunque aún no haya sido desbloqueado por primera vez tras encenderlo (al igual que el interfaz Wi-Fi; ver apartado "5.14. Comunicaciones Wi-Fi").

685. 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).

686. Debe tenerse en cuenta que tras proceder a la activación del modo avión, iOS permite la activación independiente del interfaz Bluetooth (al igual que ocurre con el interfaz Wi-Fi), no disponiéndose de capacidades de comunicación a través del interfaz de telefonía móvil, pero sí a través del interfaz Bluetooth (o Wi-Fi).

687. 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/o bloqueado (suspendido).

688. La dirección del interfaz Bluetooth, BD_ADDR (*Bluetooth Device Address*) está disponible a través del menú "Ajustes - General - Información", y en concreto, en el campo "Bluetooth", visible tanto si el interfaz Bluetooth se encuentra en el estado activo como si no:



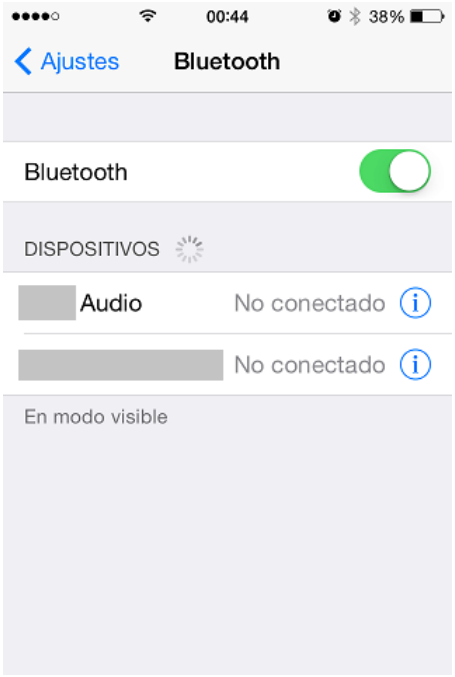
Nota: La parte de la dirección Bluetooth (BD_ADDR) asociada al fabricante, NAP+UAP (primeros tres *bytes* de la dirección) puede permitir identificar el tipo de dispositivo móvil. En el ejemplo analizado, el valor "78:A3:E4" está asignado por el IEEE (http://standards.ieee.org/regauth/oui/index.shtml) a "Apple":

```
78-A3-E4    (hex)        Apple, Inc.
78A3E4      (base 16)    Apple, Inc.
```

```
1 Infinite Loop
Cupertino  CA 95014
UNITED STATES
```

5.13.2 CONFIGURACIÓN GENERAL DE BLUETOOTH

689. 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 iOS 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:



690. La pantalla de configuración (ver imagen superior derecha) permite llevar a cabo acciones muy limitadas, como habilitar y deshabilitar el interfaz Bluetooth, visualizar la lista de dispositivos actualmente emparejados o buscar otros dispositivos Bluetooth con los que conectarse (dispositivos Bluetooth visibles en la ubicación actual).

691. El nombre del dispositivo Bluetooth corresponde al nombre del dispositivo móvil iOS y sólo puede ser modificado cambiando el nombre del propio dispositivo.

692. Debido a que el nombre puede desvelar el tipo de dispositivo móvil empleado o información del propietario, 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 0001).

693. 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 [Ref.- 51].

694. Sin embargo, iOS no dispone de opciones para configurar el modo del interfaz de Bluetooth a través del interfaz de usuario. Mientras el dispositivo móvil se encuentre en la pantalla de Bluetooth (o en las pantallas de detalles de los dispositivos ya emparejados), el dispositivo móvil permanecerá en el estado visible. Al salir de éstas, pasará al estado oculto.

695. Por tanto, por defecto, al activar el interfaz Bluetooth (desde la pantalla Bluetooth) éste se encuentra en modo visible, opción no recomendada desde el punto de vista de seguridad. Si no se desea este comportamiento, se recomienda salir de esa pantalla lo antes posible.

696. Si el dispositivo móvil está suspendido no se encuentra en estado visible (aunque el interfaz sí está activo), pese a estar en la pantalla de Bluetooth, y permanece oculto al ser encendido posteriormente pero encontrarse en la pantalla de bloqueo del terminal protegida por el código de acceso. Al desbloquear el dispositivo y entrar de nuevo a la pantalla de Bluetooth volverá a estar en modo visible.

697. 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, o que el otro dispositivo conozca de antemano la dirección Bluetooth del dispositivo móvil iOS.

698. iOS 7 añade soporte para más perfiles Bluetooth LE (Low Energy), y compatibilidad con los nuevos dispositivos Bluetooth de bajo consumo que están viendo la luz, incorporando además un sencillo método de configuración similar a NFC pero compatible con los dispositivos móviles iOS con soporte para Bluetooth 4.0.

699. iOS 7 también introduce nuevas capacidades Bluetooth 4.0 (o LE) a través de iBeacon, es decir, micro geolocalización o la posibilidad de obtener coordenadas de localización a través de Bluetooth con más precisión que las habituales, incluso en interiores (dónde no llega la señal GPS, o de las torres de telefonía y redes Wi-Fi), como por ejemplo museos, comercios y aeropuertos.

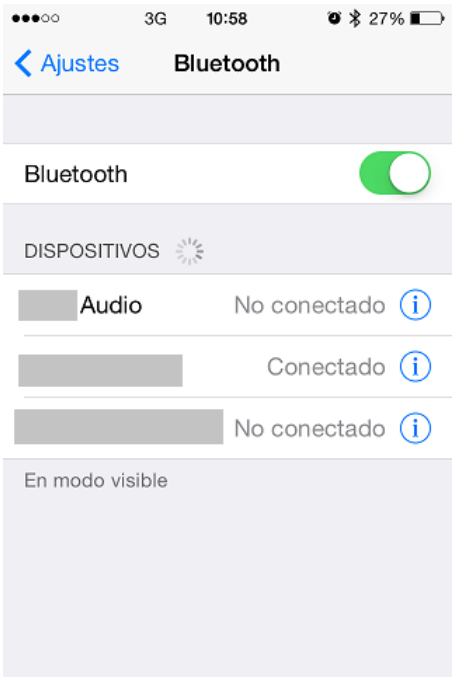
700. Estas capacidades permitirán todo un nuevo conjunto de aplicaciones, posibilidades y soluciones para el seguimiento, monitorización y detección de proximidad en interiores, incluyendo el concepto de definición de vallas o límites geográficos (*geofence*).

701. Bluetooth 4.0 (o LE) dispone de capacidades de detección de proximidad a través de la intensidad de la señal Bluetooth, lo que permite por ejemplo configurar automáticamente los dispositivos Apple TV (desde la versión 6.0) mediante un dispositivo móvil basado en iOS 7 [Ref.- 164], o bloquear un ordenador tradicional al alejarnos de él con el dispositivo móvil y no detectarse su presencia próxima.

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 se gestiona permaneciendo en la pantalla de Bluetooth. Se recomienda permanecer en ésta el menor tiempo posible, ya que en dicha pantalla el dispositivo móvil nunca volverá al estado oculto (mientras esté encendido, no suspendido), opción no recomendada desde el punto de vista de seguridad.

5.13.3 DISPOSITIVOS BLUETOOTH EMPAREJADOS

702. iOS lleva a cabo de forma automática y periódica búsquedas de dispositivos Bluetooth visibles al permanecer en la pantalla de Bluetooth, proceso indicado por un icono circular en movimiento a la derecha del texto “Dispositivos”, mostrando los mismos bajo la sección “Dispositivos” de la pantalla de configuración de Bluetooth:



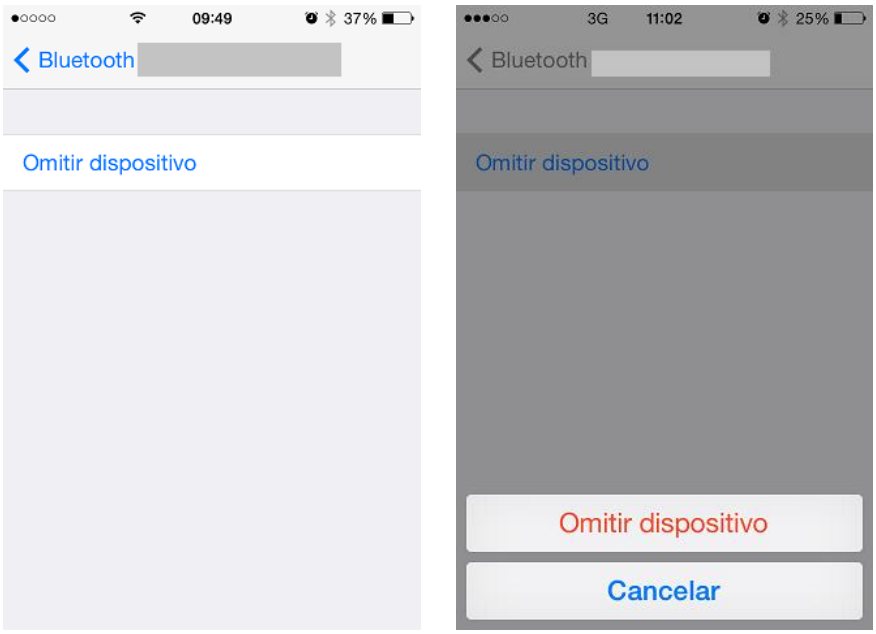
703. iOS siempre muestra los dispositivos que han sido emparejados previamente con el dispositivo móvil y su estado: "No conectado" o "Conectado" (ver imagen superior izquierda). Si en la zona de cobertura se descubren nuevos dispositivos Bluetooth visibles, estos serán añadidos a la lista de dispositivos (ver imagen superior derecha).

704. El método para diferenciar si un dispositivo Bluetooth que aparece en un momento dado en la lista de dispositivos Bluetooth disponibles está ya emparejado con el dispositivo móvil, requiere analizar el texto mostrado a la derecha del nombre del dispositivo. Si el texto indica "No conectado" se trata de un dispositivo previamente emparejado (salvo que el dispositivo móvil esté actualmente conectado a un dispositivo de la lista, indicado por el texto "Conectado"), mientras que si indica "No enlazado" se trata de un dispositivo con el que previamente no se ha emparejado (o enlazado):

705. En iOS 7 se han identificado escenarios dónde dispositivos que no habían sido emparejados previamente con iOS aparecen con el texto "No conectado", en lugar de "No enlazado".

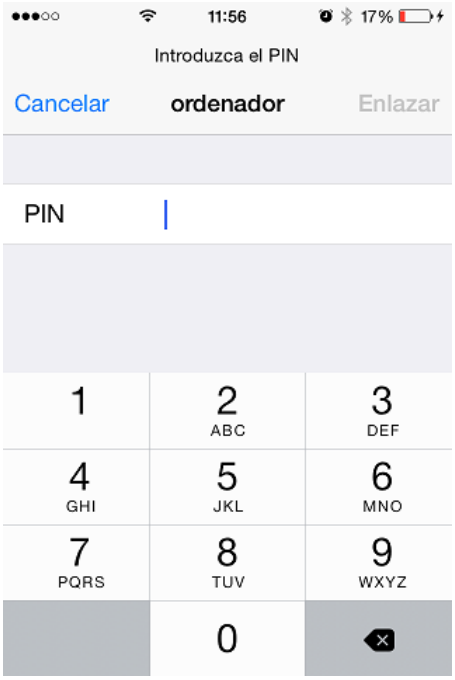
706. Adicionalmente, si el usuario accede de forma manual a cada uno de los dispositivos de la lista mediante el icono de información (i) asociado a cada dispositivo Bluetooth, sólo disponible para los dispositivos ya emparejados, se visualizará el botón "Omitir dispositivo".

707. Este botón indica que ese dispositivo ha sido previamente emparejado con el dispositivo móvil y permite eliminar el emparejamiento en el dispositivo móvil, siendo necesario volver a realizar todo el proceso de emparejamiento Bluetooth, incluida la verificación del PIN, si se desea establecer una conexión con ese dispositivo de nuevo en el futuro:



708. iOS no dispone de ninguna opción manual en el interfaz de usuario para realizar la operación de búsqueda de otros dispositivos Bluetooth visibles.

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



710. iOS 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).

711. iOS no proporciona capacidades para desconectarse de un dispositivo con el que hay actualmente una sesión o conexión Bluetooth activa, salvo apagando el otro dispositivo o deshabilitando por completo el interfaz Bluetooth en el dispositivo móvil iOS.

712. 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, o similares, ampliamente conocidos).

713. No se han identificado opciones en iOS 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 y evitar ataques de suplantación, así como modificar el nombre empleado para identificarlos en el dispositivo móvil y determinar si las conexiones con el dispositivo móvil deben ser autorizadas.

5.13.4 CONFIGURACIÓN AVANZADA DE BLUETOOTH

714. La implementación de Bluetooth de iOS, por defecto, incluye un número reducido de perfiles (*Profiles*) Bluetooth según el tipo y modelo de dispositivo móvil (iPhone o iPad) [Ref.- 82], en comparación a todos los disponibles en la especificación oficial: Perfil

"Manos libres (Hands-Free, HFP)", "Acceso a la agenda telefónica (Phone Book Access, PBAP)", "Distribución de audio avanzado (Advanced Audio Distribution, A2DP)", "Control remoto de audio/vídeo (Audio/Video Remote Control, AVRCP)", "Red de área personal (Personal Area Network, PAN)", "Dispositivo de interfaz humana (Human Interface Device, HID)" y "Acceso a mensajes (MAP)"[6].

Dispositivo	Perfil de manos libres (HFP 1.6)	Perfil de acceso a la agenda telefónica (PBAP)	Perfil de distribución de audio avanzado (A2DP)	Perfil de control remoto audio/vídeo (AVRCP 1.4)	Perfil de red de área personal (PAN)	Perfil de dispositivo de interfaz humana (HID)	Perfil de acceso a mensajes (MAP)
iPhone 4 y posterior	✓	✓	✓	✓	✓	✓	✓
iPhone 3GS	✓	✓	✓	✓	✓	✓	–
iPhone 3G	✓	✓	✓	✓	✓	–	–
iPhone original	✓	✓	–	–	–	–	–
iPad 2 y posterior	✓	–	✓	✓	✓	✓	–
iPad (1.ª generación)	–	–	✓	✓	✓	✓	–
iPod touch (4.ª generación y posterior)	✓	–	✓	✓	✓	✓	–
iPod touch (2.ª y 3.ª generación)	–	–	✓	✓	✓	✓	–

715. La disponibilidad de los diferentes perfiles Bluetooth depende del dispositivo móvil iOS, estando todos ellos implementados en el iPhone 4 y versiones posteriores.

716. No se han identificado opciones de configuración avanzadas en el interfaz de usuario de iOS que permitan establecer restricciones de conectividad (autentificación, autorización y/o cifrado), obtener información, o configurar opciones de transferencia de datos, para los diferentes perfiles Bluetooth disponibles.

717. Supuestamente [Ref.- 82][Ref.- 82], todas las conexiones Bluetooth establecidas por iOS hacen uso de cifrado a nivel de enlace, por lo que es necesario que el otro dispositivo Bluetooth también soporte cifrado.

718. Únicamente, tras haber realizado el emparejamiento con ciertos dispositivos Bluetooth que implementan perfiles específicos, al acceder a la información (i) detallada de dichos dispositivos es posible obtener opciones extra de configuración (ejemplo para el perfil PBAP):

[6] La letra "P" al final de la abreviatura de cada perfil Bluetooth corresponde al término "Profile".

719. El iPhone 4S y el iPad de 3ª generación, y modelos posteriores, incorporan la especificación Bluetooth 4.0 (incluyendo BLE o BTLE, *Bluetooth Low Energy*).

720. Desafortunadamente, no se dispone públicamente de información detallada sobre los perfiles Bluetooth LE soportados por los dispositivos móviles iOS (al menos similar a la documentación existente para los perfiles Bluetooth estándar [Ref.- 82]).

721. Para más información es necesario acceder a la sección de Bluetooth del programa de desarrolladores para iOS de Apple [Ref.- 174], o al programa MFi, *Made For iPhone* [Ref.- 175], pero que desafortunadamente no es de aplicación si los dispositivos se comunican únicamente con iOS a través de Bluetooth o Bluetooth LE.

722. El emparejamiento con dispositivos Bluetooth manos libres requiere introducir el PIN o clave de acceso, ya que iOS no implementa el proceso conocido como emparejamiento automático o *auto pairing*, basado en el uso de valores de PIN conocidos, como 0000.

5.13.5 RED DE ÁREA PERSONAL (PAN)

723. El dispositivo móvil iOS dispone del perfil de red de área personal (PAN, *Personal Area Network*) para establecer conexiones TCP/IP con otros dispositivos a través de Bluetooth, y en concreto, para compartir su conexión de Internet móvil (2/3/4G).

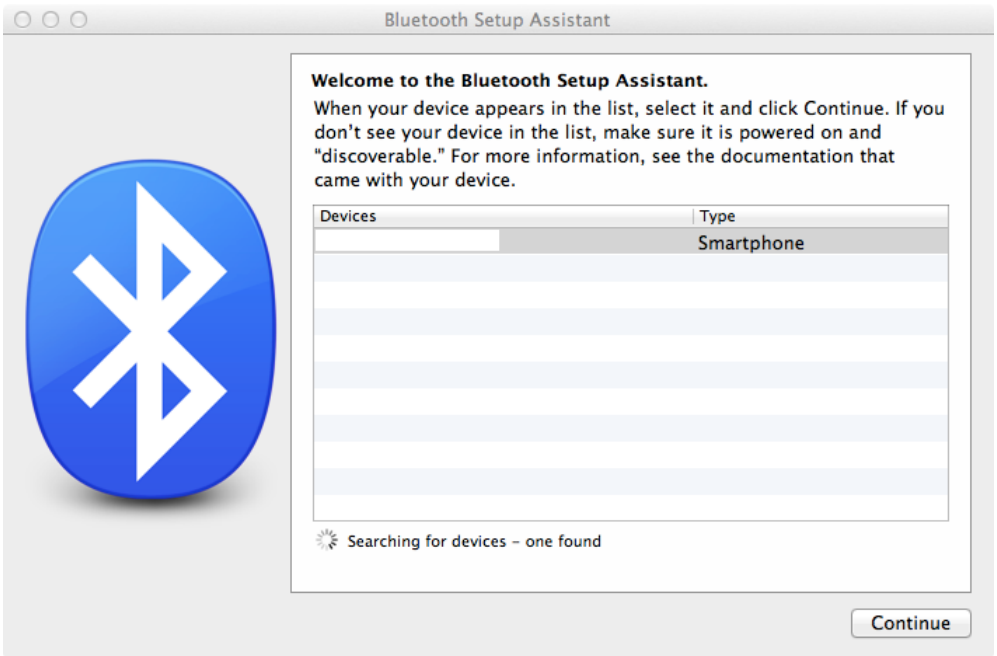
724. iOS permite compartir la conexión de Internet o *Personal Hotspot* a través del interfaz Bluetooth (ver apartado "5.12.2. Conexión de red USB (*Tethering*)"), opción desaconsejada desde el punto de vista de seguridad frente a la utilización de un cable USB.

725. Para hacer uso de estas capacidades es necesario establecer una conexión Bluetooth entre el dispositivo móvil y el ordenador mediante Bluetooth y acceder posteriormente al menú “Ajustes - Compartir Internet":

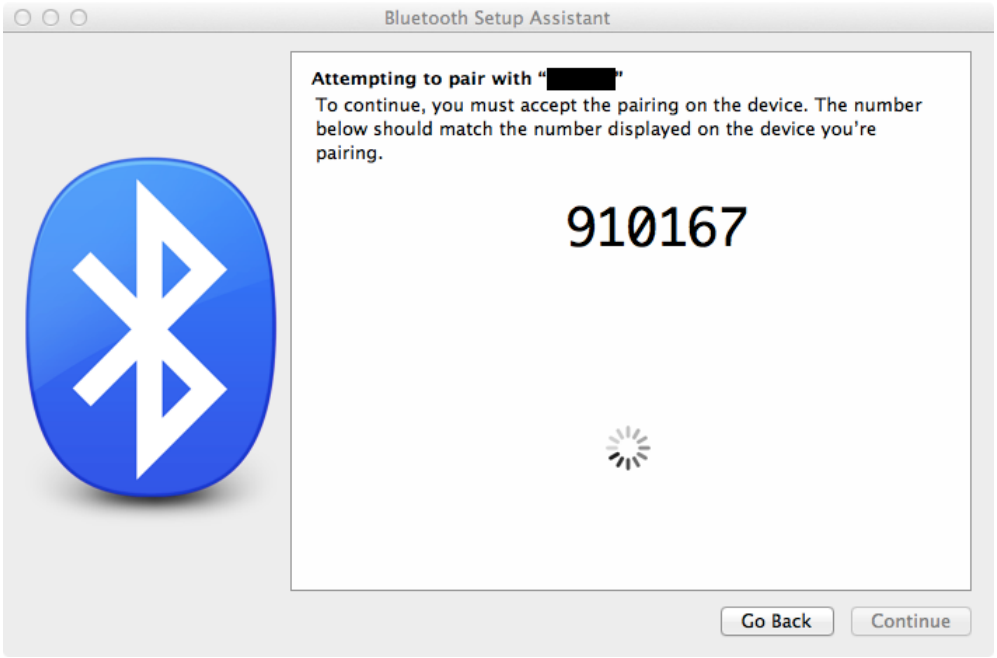
726. La conexión Bluetooth de iOS para *Personal Hotspot* hace uso de la especificación Bluetooth 2.0 (o posterior) y es compatible con Windows XP SP3, Windows Vista/7 y OS X 10.4.11+ [Ref.- 67], y versiones posteriores.

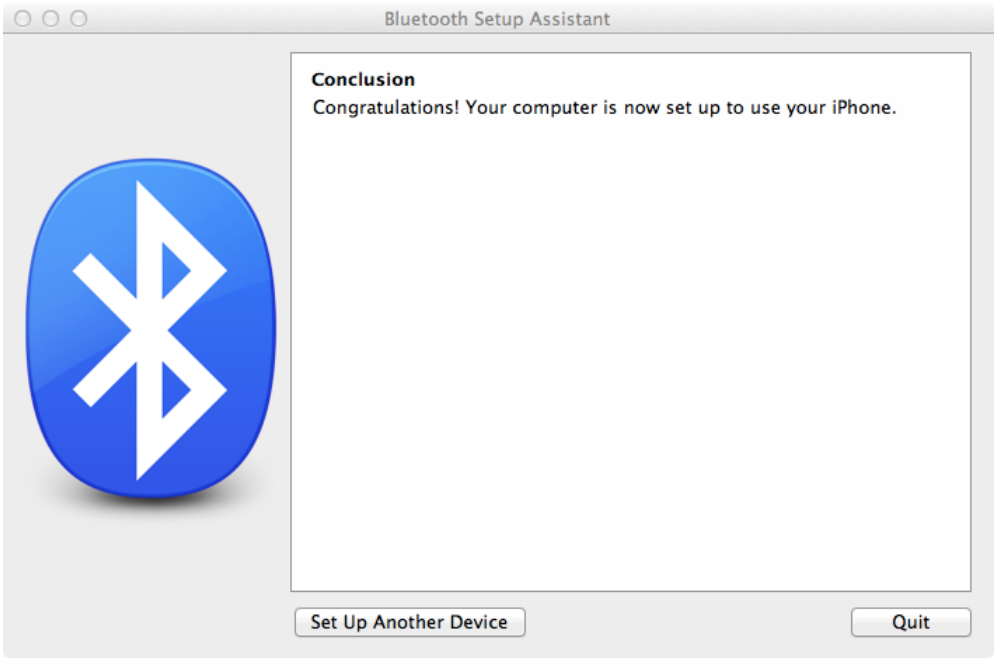
727. Tomando OS X como sistema operativo del ordenador de referencia, y tras habilitar el interfaz de Bluetooth en iOS ("Ajustes - Bluetooth", activando el botón "Bluetooth"), debe realizarse el emparejamiento desde el ordenador a través "System Preferences - Bluetooth (On) - Set Up New Device...".

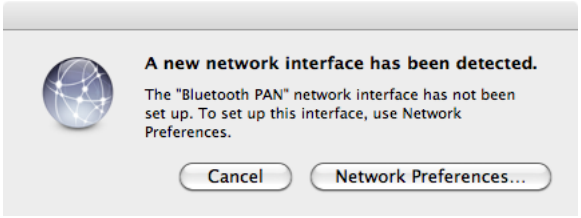
728. El dispositivo móvil iOS será descubierto por el ordenador al estar en modo visible, pudiéndose realizar el emparejamiento entre ambos dispositivos:



729. El proceso de emparejamiento Bluetooth permite desde el ordenador confirmar el código o PIN Bluetooth generado automáticamente, así como que el proceso se ha completado satisfactoriamente, junto a la creación de un nuevo interfaz de red "Bluetooth PAN":

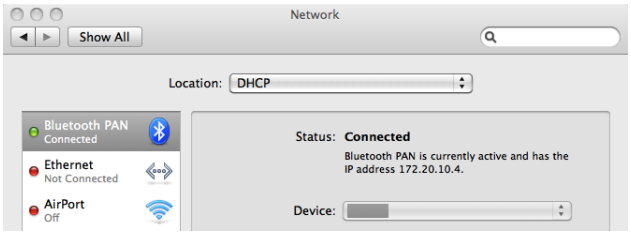




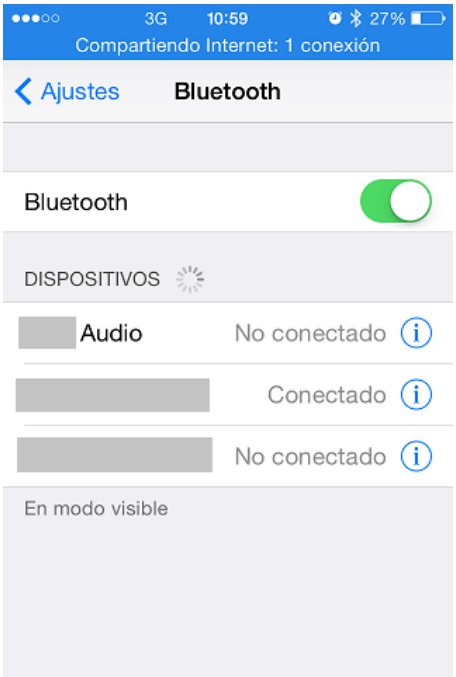


730. En el dispositivo móvil se visualizará el intento de emparejamiento, que deberá ser aceptado por el usuario, tras confirmar el valor del PIN:

731. Una vez establecida la conexión Bluetooth entre ambos dispositivos, desde el ordenador es posible hacer uso de la conexión de red empleando el enlace Bluetooth PAN:



732. En el dispositivo móvil se reflejará la conexión por parte del ordenador, haciendo uso de la funcionalidad de conexión compartida de Internet o *Personal Hotspot*:



733. Tras establecerse la conexión de red a través de la conexión Bluetooth creada por iOS, y tomando OS X como sistema operativo del ordenador cliente de referencia, el interfaz de red Bluetooth PAN funciona al estar configurado con una dirección IP dinámica (DHCP), asignándose por defecto una dirección IP con máscara /28 (255.255.255.240), como por ejemplo 172.20.10.4.

734. El dispositivo móvil (por ejemplo, con dirección IP 172.20.10.1) actúa de *gateway, router* o pasarela por defecto, de servidor DHCP, y los servidores DNS asignados mediante DHCP corresponden a los servidores DNS públicos obtenidos por iOS en la conexión de datos de telefonía móvil (2/3/4G), y es alcanzable mediante ping (ICMP).

Nota: El direccionamiento IP empleado por iOS para la conexión compartida de Internet mediante Bluetooth (172.20.10.x/28) no puede ser modificado.

735. La dirección MAC asociada al interfaz de red Bluetooth del dispositivo móvil tiene asociado un OUI con valor "AC:DE:48", qué está reservado por el IEEE, y por tanto no asignado a ningún vendedor. El valor completo no parece corresponder con el valor de la dirección MAC del interfaz Bluetooth o Wi-Fi del dispositivo móvil.

736. Un análisis de los puertos TCP/IP y servicios disponibles en el interfaz de red empleado para el acceso por Bluetooth (PAN) del dispositivo móvil permite obtener un perfil similar al del punto de acceso Wi-Fi (ver apartado "5.14.7. Punto de acceso Wi-Fi").

737. Es posible interrumpir la disponibilidad de la conexión compartida de Internet deshabilitando la opción "Compartir Internet" habilitada previamente, opción recomendada desde el punto de vista de seguridad una vez no se desea disponer de la conexión a través de Bluetooth.

5.14 COMUNICACIONES WI-FI

5.14.1 DESACTIVACIÓN DE LAS COMUNICACIONES WI-FI

738. 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), iOS ofrece al usuario la posibilidad de activar el interfaz Wi-Fi y conectarse a una red Wi-Fi, a través del proceso de configuración de una red Wi-Fi estándar de iOS, para completar el proceso de activación.

Curiosamente, si la red Wi-Fi no dispone de servicio DHCP para asignar una dirección IP de forma dinámica al dispositivo móvil iOS, no será posible establecer la conexión, ya que ésta es la opción de configuración por defecto y no se dispone de ninguna opción para modificarla y configurar una dirección IP fija durante el proceso de configuración inicial. La otra opción disponible pasa por llevar a cabo la configuración inicial a través de una conexión a iTunes mediante un cable USB (opción "Conectarse a iTunes" disponible en la pantalla de redes Wi-Fi). Se recomienda por tanto deshabilitar el interfaz Wi-Fi del dispositivo móvil tan pronto finaliza el proceso inicial de configuración con el objetivo de llevar a cabo la configuración personalizada del dispositivo antes de establecer conexiones de datos adicionales.

Debe tenerse en cuenta que desde el momento que se selecciona la opción de conectarse a una red Wi-Fi, el interfaz Wi-Fi será habilitado y permanecerá en ese estado tras la activación inicial. Desde el punto de vista de seguridad se recomienda omitir la conexión inicial a una red Wi-Fi y realizar el proceso de configuración inicial mediante un ordenador con iTunes, salvo que el usuario se encuentre en un entorno seguro y de confianza para poder establecer una conexión segura a una red Wi-Fi.

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

740. iOS proporciona información en la barra superior de estado sobre si se está o no conectado a una red Wi-Fi actualmente, a través del siguiente icono (el número de barras refleja la intensidad de la señal Wi-Fi):

741. 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.

742. iOS 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.

743. Hasta que el dispositivo móvil no es desbloqueado, únicamente genera tráfico de comprobación de las redes Wi-Fi visibles (ver abajo), y una vez es desbloqueado establece la conexión con la red Wi-Fi de preferencia.

744. 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).

745. Debe tenerse en cuenta que tras proceder a la activación del modo avión, iOS permite la activación independiente del interfaz Wi-Fi (al igual que ocurre con el interfaz de Bluetooth), no disponiéndose de capacidades de comunicación a través del interfaz de telefonía móvil, pero sí a través del interfaz Wi-Fi (o Bluetooth):

746. Cuando el dispositivo móvil está conectado a una red, el interfaz Wi-Fi permanece activo incluso tras pasar al estado de espera o *stand-by* (suspendido), es decir, el dispositivo móvil está encendido pero con la pantalla apagada y/o bloqueado. El dispositivo móvil genera tráfico de datos continuamente y de forma periódica y 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.

747. Al estar conectado a una red Wi-Fi el dispositivo móvil no genera tráfico 802.11 correspondiente a tramas de verificación de disponibilidad de redes Wi-Fi (*probe requests*, analizadas a continuación), salvo que se encuentre en la pantalla de "Redes Wi-Fi", dónde se generan esté o no conectado a una red en la actualidad.

748. En caso de no estar conectado a una red Wi-Fi, en estado activo, cada 8-11 segundos aproximadamente, el dispositivo móvil genera tramas *probe request* de tipo *broadcast* para verificar la disponibilidad de redes Wi-Fi en su zona de alcance.

749. En estado suspendido (o estado de espera) el dispositivo móvil también genera tráfico 802.11 correspondiente a tramas de verificación de disponibilidad de redes Wi-Fi (analizado en el apartado "5.14.6. Conexión automática a redes Wi-Fi").

750. iOS no proporciona opciones de configuración avanzadas para determinar el comportamiento del interfaz Wi-Fi respecto a las operaciones de ahorro de energía del dispositivo móvil.

751. Una vez deshabilitado el interfaz Wi-Fi se hará uso de las capacidades de datos de telefonía móvil (ver apartado “5.14.2. Selección de la red de datos en iOS”), en caso de estar disponibles.

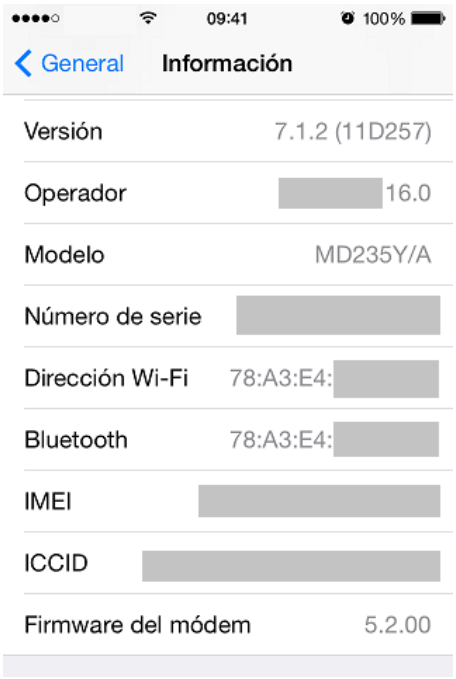
752. La configuración detallada de las redes Wi-Fi puede llevarse a cabo a través del menú "Ajustes – Wi-Fi" y en concreto, a través del icono de información (i), disponible a la derecha de cada red Wi-Fi, o mediante la opción "Otra..." situada al final de la lista de redes Wi-Fi disponibles:

753. 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:

754. La opción “Otra...” que permite añadir una nueva red Wi-Fi manualmente no está disponible (o habilitada) hasta que el interfaz Wi-Fi no ha sido activado.

755. Los dispositivos móviles iOS no disponen de capacidades para evitar que el usuario se conecte a cualquier red Wi-Fi insegura, o habilite y deshabilite el interfaz Wi-Fi.

756. La dirección del interfaz Wi-Fi está disponible a través del menú “Ajustes - General - Información”, y en concreto, en el campo “Dirección Wi-Fi”, visible tanto si el interfaz Wi-Fi se encuentra en el estado activo como si no:



Nota: La parte de la dirección Wi-Fi asociada al fabricante (primeros tres *bytes* de la dirección) puede permitir identificar el tipo de dispositivo móvil. En el ejemplo analizado, el valor “78:A3:E4” está asignado por el IEEE a “Apple“ (http://standards.ieee.org/regauth/oui/index.shtml):

```
78-A3-E4    (hex)        Apple, Inc.
78A3E4      (base 16)    Apple, Inc.
                         1 Infinite Loop
                         Cupertino  CA 95014
                         UNITED STATES
```

757. Por defecto, iOS se conecta de forma automática a las redes conocidas, no disponiéndose de ninguna opción para deshabilitar este comportamiento.

758. La opción "Preguntar al conectar" (habilitada por defecto) establece si iOS preguntará al usuario en caso de necesitar disponer de una conexión de datos y no detectar la existencia de una actualmente, por ejemplo, porque una aplicación genere tráfico de datos.

759. Al identificarse que es necesario disponer de una conexión y no existir ninguna activa, por ejemplo al no existir ninguna red Wi-Fi conocida en el alcance del dispositivo móvil, tras generar la notificación de datos móviles desactivados, iOS muestra al usuario una lista de redes Wi-Fi disponibles en la ubicación actual, y le pregunta si desea acceder a una red Wi-Fi abierta nueva dentro del alcance (ejemplo de iOS 5.x):

760. Desde el punto de vista de seguridad, y siendo muy restrictivos, se puede desactivar esta opción de notificación, de forma que en lugar de mostrarse al usuario la lista de redes Wi-Fi disponibles, sea el usuario el que tenga que ir a la pantalla de ajustes de "Redes Wi-Fi" de forma manual e intencionada y establecer la conexión con una de ellas.

761. Es aconsejable comparar la dirección Wi-Fi del dispositivo móvil con su dirección Bluetooth (ver apartado "5.13. 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.

762. En el caso de los dispositivos móviles de Apple, y en concreto los basados en iOS como el empleado para la elaboración de la presente guía, ambas direcciones son correlativas, con el riesgo de seguridad asociado [Ref.- 72], siendo trivial para un atacante capturar el tráfico Wi-Fi del dispositivo móvil y derivar inmediatamente la dirección Bluetooth.

5.14.2 SELECCIÓN DE LA RED DE DATOS EN IOS

Nota: La selección de la red de datos en iOS afecta principalmente a la red de datos de telefonía móvil 2/3/4G (analizada en el apartado "5.16. Comunicaciones GSM (2G), UMTS (3G) y LTE (4G): voz y datos") y al interfaz Wi-Fi (ver este apartado, "5.14. Comunicaciones Wi-Fi").

763. Debido a las múltiples opciones de conectividad de datos disponibles en los dispositivos móviles, como Bluetooth, y principalmente Wi-Fi y 2/3/4G, en caso de haber múltiples opciones habilitadas y disponibles, iOS gestiona cual es la mejor conexión de datos a usar en cada momento. 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.

764. iOS emplea diferentes criterios para seleccionar y mantener la mejor y única opción de conexión de datos, que por defecto da prioridad al interfaz Wi-Fi frente al interfaz de telefonía móvil (2/3/4G).

765. Si una aplicación requiere acceso a Internet, iOS empleará la conexión Wi-Fi existente. En el caso de no disponer de ella, intentará conectarse a las redes Wi-Fi disponibles y conocidas, y de no encontrar ninguna, mostrará la lista de redes Wi-Fi disponibles (ver imagen inferior para iOS 5.x). Si no hay ninguna red Wi-Fi disponible o si el usuario elige no conectarte a ninguna red Wi-Fi (botón "Cancelar"), iOS se intentará conectar a Internet a través de la red de datos de telefonía móvil (2/3/4G) [Ref.- 73]:

766. En caso de no disponer de ningún interfaz de red activo generará un mensaje de error.

767. Desde el punto de vista de la activación y desactivación de los interfaces de red (Wi-Fi y telefonía móvil de datos, 2/3/4G), el comportamiento de iOS es el siguiente:

- Si Wi-Fi está activo y se activa 2/3/4G, este segundo interfaz no llegará a ser habilitado.
- Si 2/3/4G está activo y se activa Wi-Fi, la conexión 2/3/4G será deshabilitada.
- Si Wi-Fi está activo y se desactiva, iOS comprobará el estado y la configuración de 2/3/4G, y si está disponible, lo habilitará y hará uso de él.

768. Los eventos de activación y desactivación de los dos interfaces, Wi-Fi y 2/3/4G, pueden ser visualizados a través de los iconos de la barra de estado de iOS a través de sus respectivos iconos.

769. iOS no permite disponer de varias conexiones activas simultáneamente, salvo en el caso de actuar como punto de acceso Wi-Fi (ver apartado "5.14.7. Punto de acceso Wi-Fi".), opción recomendada desde el punto de vista de seguridad para evitar escenarios *dual homing* donde la conexión Wi-Fi y la conexión de datos de telefonía móvil (2/3/4G) están activas simultáneamente, con el objetivo de que el dispositivo móvil no actúe de pasarela entre distintas redes.

770. 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 3/4G frente a 2G (opción no disponible en iOS, ver apartado "5.16. Comunicaciones GSM (2G), UMTS (3G) y LTE (4G): voz y datos"). Para ello sería necesario deshabilitar el interfaz Wi-Fi y habilitar las comunicaciones de datos móviles.

771. 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 "5.16. Comunicaciones GSM (2G), UMTS (3G) y LTE (4G): voz y datos", que contiene información detallada de cómo deshabilitar el interfaz de datos de telefonía móvil.

772. En el caso de que el dispositivo móvil iOS identifique varias redes Wi-Fi conocidas a las que se podría conectar, éste se conectará a la última red a la que estuvo previamente conectado.

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

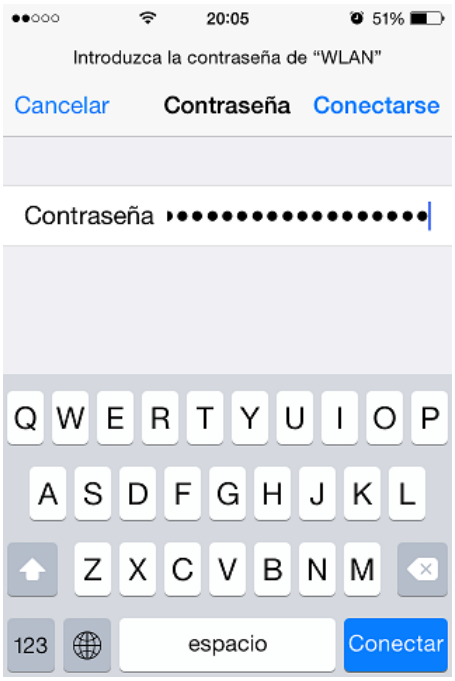
773. Este apartado proporciona recomendaciones de configuración a través de los diferentes parámetros y opciones disponibles en iOS para la conexión segura a redes Wi-Fi.

774. La configuración manual y detallada de las redes Wi-Fi puede realizarse desde el menú "Ajustes – Wi-Fi ", y en concreto, a través del icono de información (i) de cada red Wi-Fi (únicamente para los ajustes de direccionamiento IP, pero no para los ajustes Wi-Fi), o mediante la opción "Otra..." situado al final de la lista de redes Wi-Fi disponibles.

775. Esta opción de configuración es la opción documentada para establecer una conexión con una red Wi-Fi oculta (ver apartado "5.14.6. Conexión automática a redes Wi-Fi").

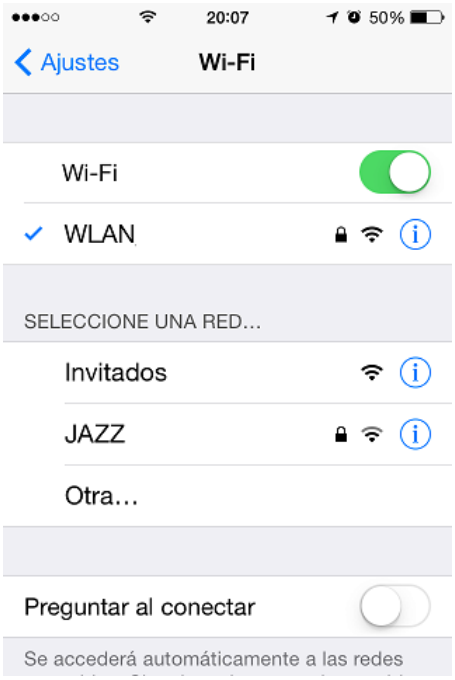
776. Esta última opción es la única que permite seleccionar todas las opciones de configuración de conexión de una nueva red Wi-Fi, incluyendo el nombre de red (o SSID), y el mecanismo de seguridad a emplear (abierta o ninguna, WEP, WPA/WPA2 Personal, PSK, o 802.1x EAP, Empresa), analizado posteriormente.

777. Adicionalmente, mediante la selección de una de las redes disponibles (listadas en la misma pantalla sobre la opción "Otra...") es posible seleccionar la red Wi-Fi con la que se desea establecer la conexión, para lo que se solicitará únicamente la contraseña (caso de requerir una):



778. Las redes Wi-Fi aparecen clasificadas en la lista en orden alfabético. La lista no permite identificar los mecanismos de seguridad empleados por cada una de la redes, ya que el único indicativo de que se hace uso de algún mecanismo de seguridad es indicado con un icono de un candado. No es por tanto posible saber si la red hace uso de WEP, WPA, WPA2, personal o empresarial.

779. Para establecer la conexión con una red próxima únicamente es necesario introducir la contraseña de acceso a la red (ver imagen superior derecha) en caso de estar protegida por una contraseña (WEP o WPA/WPA2-PSK). En el caso de redes abiertas directamente se establece la conexión con la red Wi-Fi:

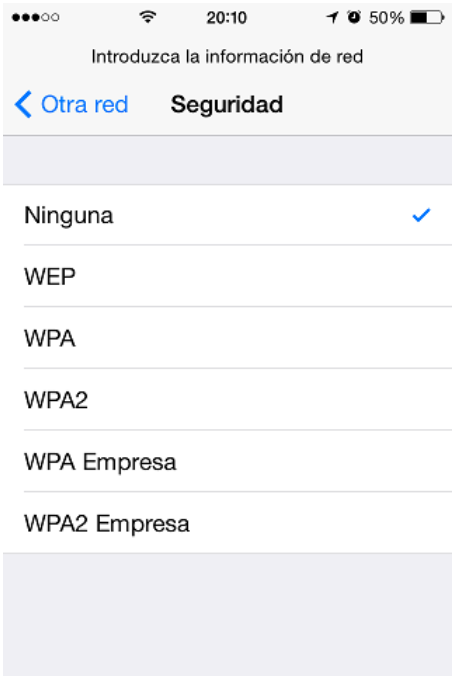


780. Habitualmente se recomienda hacer uso del mecanismo de configuración manual frente a seleccionar la red Wi-Fi desde el listado de redes disponibles, ya que en este segundo caso, no se dispone de tanta flexibilidad y granularidad para seleccionar los diferentes parámetros de configuración y los mecanismos de seguridad de la red. Sin embargo, en el caso de iOS se recomienda añadir la red Wi-Fi desde el listado de redes disponibles (ver apartado “5.14.6. Conexión automática a redes Wi-Fi”) y no a través de la opción "Otra...".

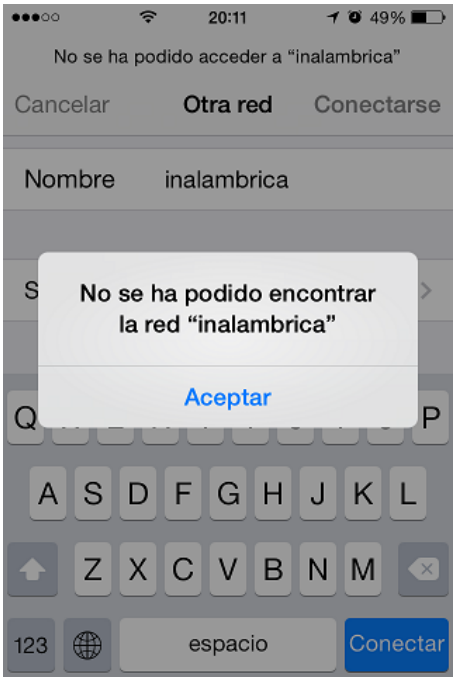
781. Es decir, al establecer una primera conexión con una nueva red Wi-Fi, se recomienda agregar la nueva red Wi-Fi de forma automática a través del listado de redes disponibles (debido a una vulnerabilidad descrita posteriormente), pese a que no sea posible visualizar y especificar todas las opciones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

782. 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.

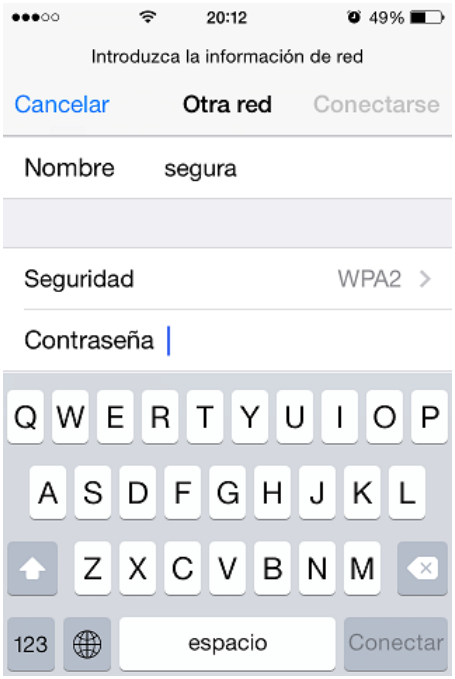
783. Dentro de las opciones de configuración de una nueva red Wi-Fi, la primera pantalla de configuración hace posible especificar el nombre de la red (SSID) y el mecanismo de seguridad a emplear: ninguna o abierta (opción por defecto), WEP, WPA ó WPA2 (ambas opciones referencian a la versión personal o PSK), WPA Empresa y WPA2 Empresa (estas dos últimas referencian a la versión empresarial empleando 802.1x/EAP):



784. Para poder añadir la nueva red es necesario que la misma esté disponible en la zona de cobertura y poder establecer una conexión a través del botón "Conectarse". En caso contrario iOS notificará al usuario mediante un mensaje de error indicando que la red Wi-Fi no está disponible y ésta no será añadida al dispositivo móvil:



785. En caso de seleccionar una red WEP, WPA o WPA2, es necesario especificar la contraseña de la red (ver imagen inferior izquierda). En el caso de seleccionar una red WPA Empresa o WPA2 Empresa (802.1x/EAP), es necesario especificar el nombre de usuario y la contraseña (ver imagen inferior derecha), así como el modo o tipo de EAP a emplear: Automático o EAP-TLS (analizados posteriormente):



786. Desafortunadamente, iOS no permite especificar detalladamente los mecanismos de cifrado de datos de WPA o WPA2, no siendo posible diferenciar el tipo de cifrado: TKIP, AES (CCMP) o ambos.

787. 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.

788. iOS por defecto permite el establecimiento de conexiones Wi-Fi *ad-hoc*, además de 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* en versiones previas de iOS, no siendo posible diferenciarlas inicialmente de las redes con infraestructura.

789. El único método que existía para diferenciar si una red Wi-Fi que aparece en un momento dado en la lista de redes Wi-Fi disponibles es una red *ad-hoc* o no (con infraestructura), requiere que el usuario acceda de forma manual a cada una de las redes de la lista.

790. Mediante el icono de información (i) asociado cada red Wi-Fi, si el botón "Conexión automática" está disponible, significa que la red es de tipo *ad-hoc*. En caso contrario, si no aparece dicho botón, es que es una red Wi-Fi con infraestructura.

791. En iOS 7 la red Wi-Fi a la que está conectado el dispositivo móvil aparece en la parte superior junto al botón de activación del interfaz Wi-Fi, con el objetivo de diferenciarla del resto de redes Wi-Fi disponibles en el área de cobertura actual.

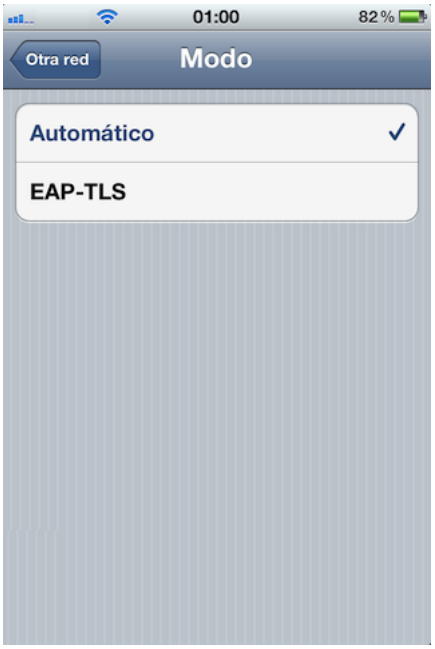
792. En iOS 7, igualmente, las redes Wi-Fi de tipo *ad-hoc* aparecen de manera separada en su propia lista bajo la categoría "Dispositivos", en lugar de bajo la categoría "Seleccione una red...", con el objetivo de diferenciarlas del resto de redes Wi-Fi basadas en una infraestructura o punto de acceso:

793. Se recomienda no establecer conexiones con redes *ad-hoc*, salvo que los requisitos de seguridad asociados sean equivalentes a los de una red con infraestructura segura.

794. Igualmente, el proceso de configuración de las redes Wi-Fi en iOS no permite claramente, y de forma explícita, especificar si la red Wi-Fi es oculta o visible (ver apartado “5.14.6. Conexión automática a redes Wi-Fi”).

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

796. En caso de emplear WPA2 (o WPA) en su versión Empresa, es decir, con mecanismos basados en 802.1X/EAP, la pantalla de ajustes de iOS 7 no permite especificar los parámetros de configuración asociados al modo o tipo de mecanismo EAP a emplear: Automático (opción por defecto) o EAP-TLS (pese a que estas opciones si estaban disponibles por ejemplo en iOS 5.x, ver imágenes inferiores).



797. La documentación de Apple especifica que iOS proporciona soporte para los siguientes métodos de autentificación EAP: EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, PEAPv0, PEAPv1, and LEAP [Ref.- 74].

798. El modo automático de iOS referencia a diferentes tipos EAP (como por ejemplo PEAP, *Protected EAP*), y hace uso por defecto de usuario y contraseña para las credenciales del usuario (ver imagen superior izquierda). Por tanto, deben proporcionarse las credenciales

del usuario (nombre de usuario y contraseña, y opcionalmente el dominio Windows (por ejemplo “DOMINIO\usuario”) en los campos “Nombre de usuario” y “Contraseña” (ver imágenes superiores).

799. El interfaz de usuario de iOS no proporciona acceso a la configuración de todos los tipos de métodos EAP soportados, ni a todas las opciones de configuración disponibles para cada método EAP. Para poder fijar otros tipos EAP, así como opciones de configuración más avanzadas, es necesario hacer uso de los perfiles de configuración de iOS (ver apartado "5.3.2. Perfiles de configuración").

800. Adicionalmente, tanto para PEAP o EAP-TTLS, como para EAP-TLS, 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 (servidor RADIUS), empleando los perfiles de configuración de iOS (ver apartado "5.3.2. Perfiles de configuración"). El certificado asociado debe haber sido añadido previamente al dispositivo móvil (ver apartado “5.8.1. Certificados digitales y credenciales del usuario”).

801. El modo EAP-TLS (o TLS) en iOS 5.x modifica el campo "Contraseña" por el campo "Identidad", ya que 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 “Identidad”, y que debe haber sido añadido previamente al dispositivo móvil (ver apartado “5.8.1. Certificados digitales y credenciales del usuario”).

802. 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) al dispositivo móvil a través de los métodos soportados por iOS (ver apartado “5.8.1. Certificados digitales y credenciales del usuario”).

803. Una vez el certificado personal ha sido importado en el dispositivo móvil, estará disponible en iOS 5.x a través del menú de configuración de la red Wi-Fi WPA/WPA2 Empresa basada en EAP-TLS, desde el campo “Identidad”.

804. En el caso de iOS 7, el interfaz de usuario ha sido simplificado y no se dispone de ninguna de las opciones de configuración avanzadas mencionadas previamente para iOS 5.x. iOS seleccionará de manera automática en método EAP a emplear en función de los ofrecidos por la red Wi-Fi empresarial.

805. Por tanto, y con mayor razón en iOS 7, la configuración de redes Wi-Fi WPA o WPA2 Empresa debe llevarse a cabo a través de un perfil de configuración, empleando por ejemplo la utilidad de configuración de iPhone (ver apartado "5.3.3. Utilidad de configuración del iPhone"), que debe incluir 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 iOS.

806. En el momento de establecer la primera conexión con una red Wi-Fi WPA2 Empresa, iOS solicitará al usuario verificar la identidad del servidor de autentificación (RADIUS) al que se está conectando a través de su certificado digital.

807. Se recomienda aceptar el certificado digital del servidor tras verificar exhaustivamente sus detalles y confirmar que pertenece al servidor RADIUS al que pretendemos

conectarnos, ya que en caso contrario las credenciales de acceso, usuario y contraseña, serían enviadas a otro servidor potencialmente controlado por un atacante.

808. El método de importación de certificados raíz (.crt) es similar el empleado para la importación de certificados de usuario (.p12) (ver apartado "5.8.1. Certificados digitales y credenciales del usuario").

809. En el año 2013 se publicaron múltiples vulnerabilidades que afectaban a la mayoría de dispositivos móviles y sistemas operativos de diferentes fabricantes, incluyendo iOS, y en concreto, que facilitaban la suplantación de redes Wi-Fi Empresariales [Ref.- 173].

810. Por defecto, las verificaciones y comprobaciones que llevan a cabo los dispositivos móviles iOS a la hora de identificar una red Wi-Fi Empresarial como legítima no son suficientes, por lo que un atacante puede suplantar a la red legítima y forzar a que el dispositivo móvil iOS víctima se conecte a la red del atacante automáticamente.

811. Desafortunadamente, los mensajes de verificación del certificado del servidor RADIUS empleados por iOS por defecto a la hora de conectarse a una red Wi-Fi Empresarial son exactamente iguales tanto al conectarse a la red Wi-Fi legítima como a la red Wi-Fi suplantada por el atacante.

812. Una vez que el dispositivo móvil iOS intenta conectarse a la red Wi-Fi Empresarial, llevará a cabo el proceso de autentificación, desvelando potencialmente las credenciales del usuario (usuario y contraseña).

813. En el caso de hacer uso del método EAP más común, PEAP, el proceso de autentificación desvelará el desafío y la respuesta asociados a MSCHAPv2, lo que permitiría al atacante llevar a cabo ataques de diccionario o fuerza bruta para obtener las credenciales del usuario. Debe tenerse en cuenta que existen actualmente servicios de pago en Internet que permiten obtener la contraseña del usuario a partir del desafío y la respuesta de MSCHAPv2 con un 100% de efectividad.

814. Adicionalmente, el atacante puede rebajar el tipo de método EAP empleado por la red Wi-Fi y utilizar en su lugar EAP-GTC, empleando PAP, lo que indicará al dispositivo móvil que lleve a cabo el proceso de autentificación facilitando las credenciales en claro, sin cifrar y sin emplear ningún mecanismo de protección adicional.

815. En este tipo de ataque, apodado EAP *Dumb-Down*, el atacante no debe llevar a cabo ninguna acción adicional, ya que dispondrá directamente del nombre de usuario y contraseña empleado por el dispositivo móvil víctima.

816. Debe tenerse en cuenta que las credenciales empleadas por el dispositivo móvil para conectarse a la red Wi-Fi Empresarial normalmente no sólo se emplean para la conexión a la red Wi-Fi, sino que también constituyen las credenciales del usuario en el dominio de la organización, permitiendo igualmente el acceso a la cuenta de correo, a los entornos Windows, a servidores web internos o a los concentradores VPN de la organización.

817. Así mismo, una vez el atacante dispone de las credenciales del usuario, puede suplantar completamente a la red Wi-Fi Empresarial legítima y forzar a que el dispositivo móvil iOS víctima se conecte a la red suplantada para llevar a cabo cualquier otro tipo de ataque, ya que a partir de ese momento, víctima y atacante compartirán la red Wi-Fi.

818. Este tipo de vulnerabilidades, aún no solucionadas en iOS 7, pueden ser mitigadas mediante una exhaustiva y minuciosa configuración de las redes Wi-Fi Empresariales en iOS a través de un perfil de configuración, dónde se verifique tanto el certificado de la

autoridad de certificación (CA) empleada en la red Wi-Fi (recomendándose hacer uso de una CA privada en lugar de una pública), el nombre del servidor RADIUS (desafortunadamente éste es un parámetro opcional dentro de los perfiles de configuración), y se defina de manera restrictiva el tipo de método EAP a emplear por la red Wi-Fi[7]. Otra alternativa es hacer uso de EAP-TLS, método de autentificación de los dispositivos móviles y usuarios basado en certificados digitales cliente, y que no permite por tanto exponer el usuario y contraseña de la víctima.

819. En resumen, desde el punto de vista de seguridad de iOS como cliente Wi-Fi, se recomienda hacer uso de redes inalámbricas no ocultas (ver apartado "5.14.6. 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 Empresa, basada en mecanismos de autentificación 802.1X/EAP, y de tipo EAP-TLS preferiblemente, con todos los ajustes de certificados y del servidor RADIUS minuciosamente configurados a través de un perfil de configuración..

820. Adicionalmente, iOS 7 añade soporte para Wi-Fi HotSpot 2.0 [Ref.- 141], también conocido como HS2 o *Wi-Fi Certified Passpoint*[8], un estándar que permite al dispositivo móvil conectarse a una red Wi-Fi pública (*Wi-Fi hotspot*) de forma automática sin intervención del usuario, empleando WPA2 como mecanismo de seguridad.

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 ataques de denegación de servicio (DoS), entre otros.

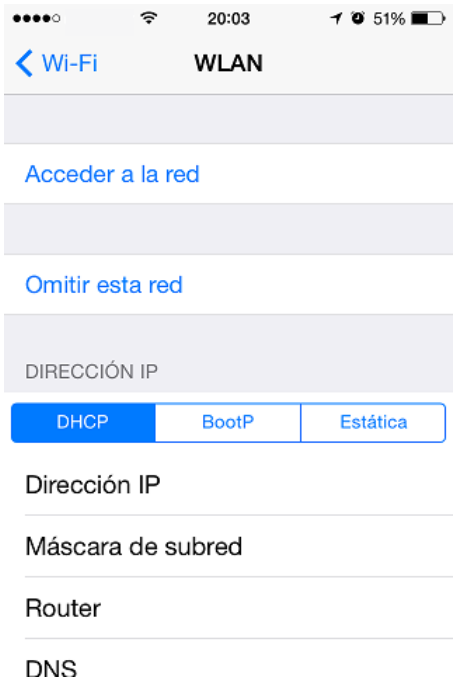
5.14.4 LISTA DE REDES PREFERIDAS (PNL)

821. La lista de redes preferidas (PNL, *Preferred Network List*), es decir, las redes Wi-Fi a las que se ha conectado previamente el dispositivo móvil o que han sido configuradas en el mismo (ver apartado "5.14.6. Conexión automática a redes Wi-Fi"), no puede ser visualizada en los dispositivos móviles iOS, una limitación con implicaciones relevantes desde el punto de vista de seguridad.

822. 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 "Omitir esta red" , tanto si se está conectado a ella actualmente como si no:

[7] Incluso en este caso, iOS empleará el método EAP sugerido por la red Wi-Fi a la que se intenta conectar.

[8] http://www.wi-fi.org/discover-wi-fi/wi-fi-certified-passpoint



823. Una limitación de iOS relevante desde el punto de vista de seguridad es que sólo permite eliminar una red Wi-Fi si actualmente el dispositivo móvil se encuentra en su rango de alcance o cobertura, no siendo posible en otro caso [Ref.- 83].

824. Aquellas redes Wi-Fi a las que el dispositivo móvil se haya conectado en alguna ocasión, y que por tanto habrán sido añadidas a la PNL, permanecerán en la PNL de forma oculta y sólo serán visibles cuando el dispositivo móvil vuelva a estar bajo su rango de cobertura. En ese momento el usuario podría proceder a su eliminación.

825. Como resultado, numerosas redes Wi-Fi permanecerán en la PNL y no podrán ser eliminadas por el usuario, ya que el dispositivo no volverá a estar bajo su rango de

alcance, y el usuario desconocerá en muchos casos que las mismas residen en la configuración Wi-Fi interna del dispositivo móvil.

826. Este comportamiento se presenta independientemente de si la red Wi-Fi es visible u oculta (ver apartado “5.14.6. Conexión automática a redes Wi-Fi”).

827. Como resumen, iOS no permite conocer las redes Wi-Fi configuradas en el dispositivo móvil salvo cuando se está en su rango de alcance y éstas son mostradas, e incluso en ese caso, no es sencillo diferenciar cuales de las redes disponibles en la lista de redes Wi-Fi ya están configuradas en el dispositivo móvil (por haberse conectado previamente a ellas) y cuáles no (salvo que el dispositivo esté actualmente conectado a una de estas redes Wi-Fi, indicado por un símbolo de confirmación o "*tick*").

828. El único método para diferenciar si una red Wi-Fi que aparece en un momento dado en la lista de redes Wi-Fi disponibles pertenece a la PNL del dispositivo móvil o no, requiere que el usuario acceda de forma manual a cada una de las redes de la lista.

829. Mediante el icono de información (i) asociado a cada red Wi-Fi, si el botón "Omitir esta red" está disponible, significa que la red se encuentra en la PNL y está configurada en el dispositivo móvil. En caso contrario, si no aparece dicho botón, es que no se encuentra en la PNL.

830. La herramienta iStupid, *indescreet SSID tool (for the) unknown PNL (on) iOS devices*, ha sido diseñada específicamente para facilitar la eliminación de redes Wi-Fi de la PNL de los dispositivos móviles iOS [Ref.- 171].

831. Esta herramienta permite simular la existencia de una red Wi-Fi, incluso sin encontrarse en el área de cobertura de la misma, conociendo su nombre o SSID.

832. Adicionalmente, permite especificar el tipo de seguridad de la red Wi-Fi original, único parámetro junto con el SSID necesario para suplantar la red original y poder proceder a su eliminación en iOS a través de la opción "Omitir esta red". En caso de no disponer de la información del tipo de seguridad empleado por la red Wi-Fi original, iStupid permite iterar automáticamente por los distintos tipos de mecanismos de seguridad disponibles en las redes Wi-Fi para identificar cuál era el empleado por la red original y poder así eliminarla de la PNL.

5.14.5 CONFIGURACIÓN TCP/IP DEL INTERFAZ WI-FI

833. 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 “5.18. Comunicaciones TCP/IP”), información disponible mediante el icono de información (i) asociado a cada red Wi-Fi de la lista, y en concreto, de la red a la que el dispositivo móvil está actualmente conectado:

834. Es posible fijar una dirección IP estática (junto a la máscara de subred, router, los servidores DNS primario y secundario, los dominios de búsqueda y el uso de un proxy HTTP) desde la opción "Estática" de los detalles de direccionamiento IP de la red Wi-Fi seleccionada de la lista de redes disponibles:

835. Para llevar a cabo la configuración de TCP/IP de una red Wi-Fi, o modificaciones en la misma, es necesario que el interfaz Wi-Fi esté activo, para poder seleccionar así la red Wi-Fi de la lista de redes disponibles.

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

836. iOS 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 dispone de ninguna opción de configuración en el interfaz de usuario de iOS para deshabilitar el proceso de conexión automática a redes Wi-Fi si el interfaz Wi-Fi está activo. Una vez que iOS se haya conectado a una red Wi-Fi, se conectará automáticamente a ella siempre que esté en su radio de alcance. Si hay más de una red Wi-Fi anteriormente utilizada dentro del radio de alcance, iOS se conectará a la ultima red Wi-Fi empleada.

837. Como se ha mencionado previamente, la lista de redes preferidas (PNL) no está disponible a través del interfaz gráfico de usuario de iOS.

838. Adicionalmente, la posibilidad de gestión de redes Wi-Fi conocidas sólo está disponible cuando el interfaz Wi-Fi está habilitado, no siendo posible acceder a ellas (para su borrado o edición) si el interfaz Wi-Fi está deshabilitado, y sólo además cuando el dispositivo móvil están en el rango de alcance de la red que se desea gestionar.

839. 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.

840. 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 *non-broadcast*. Las redes visibles son las que sí incluyen el nombre de red en esas tramas.

841. 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.

842. 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.

843. 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 iOS. Si una red está oculta, los clientes Wi-Fi se verán obligados a comprobar de forma explícita si la red Wi-Fi 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).

844. Desafortunadamente, iOS 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.

845. 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 iOS).

846. Como es lógico, iOS (al igual que muchos otros clientes Wi-Fi) no permite visualizar las redes Wi-Fi ocultas en la lista de redes disponibles, siendo necesario añadirlas manualmente.

847. Si la red Wi-Fi es añadida al dispositivo manualmente, y en consecuencia a la PNL, mediante el botón “Otra...” 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 iOS [Ref.- 172]):

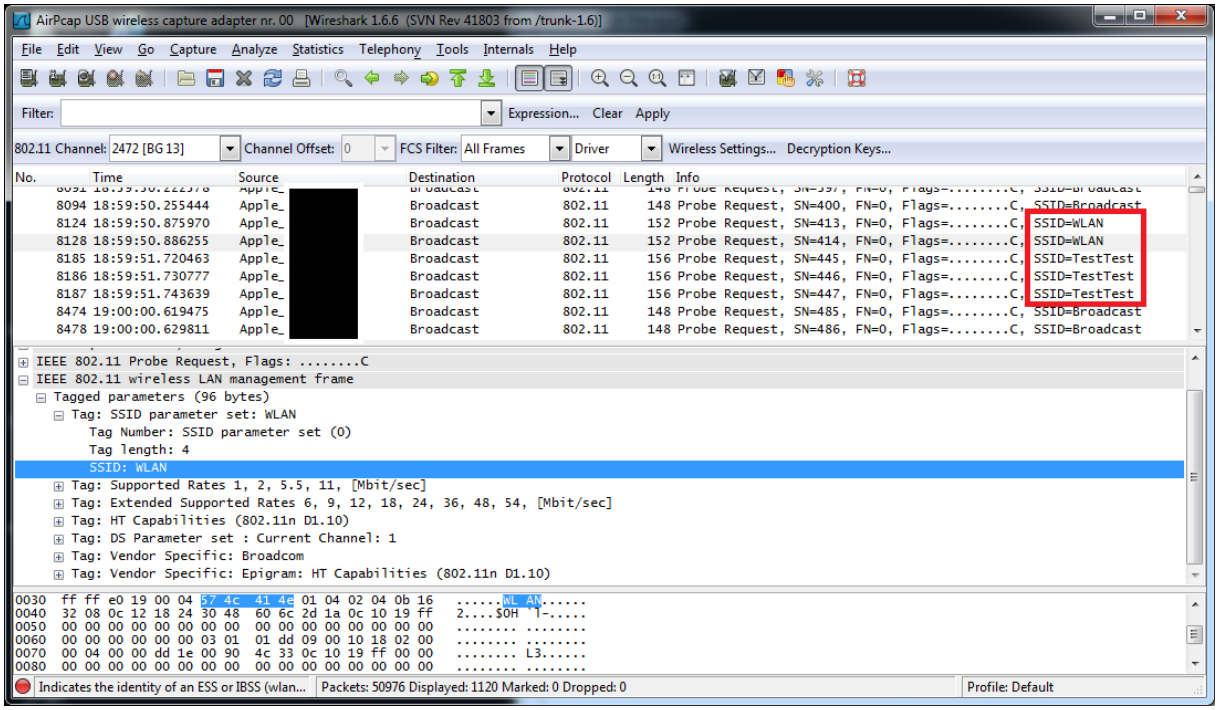
848. Este es el comportamiento más vulnerable (existente y corregido en los sistemas operativos y ordenadores portátiles y de sobremesa hace años), ya que obliga a iOS a generar tráfico que desvela la lista de redes Wi-Fi configuradas en el dispositivo móvil (conocida como la PNL, *Preferred Network List*). Este comportamiento presenta un escenario similar al existente en equipos de escritorio basados en Windows XP sin la actualización de seguridad KB917021 aplicada, de enero de 2007 [Ref.- 77].

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

850. Resumiendo, para todas aquellas redes configuradas o añadidas a través del botón “Otra...”, independientemente de si la red añadida es oculta o visible, iOS generará tráfico que desvelará estas redes Wi-Fi disponibles en su lista de redes preferidas e intentará conectarse a ellas, escenario que puede ser empleado por un potencial atacante para disponer de conectividad con el dispositivo móvil y proceder a explotar vulnerabilidades en el mismo [Ref.- 172].

851. Por tanto, no se recomienda añadir ninguna red Wi-Fi manualmente al dispositivo móvil a través del botón "Otra...", aunque es una práctica común desde el punto de vista de seguridad para disponer de mayor control sobre la configuración de la red Wi-Fi a añadir y, en concreto, los ajustes de los mecanismos de seguridad de la red Wi-Fi.

852. En la imagen inferior, el dispositivo móvil iOS intenta descubrir la presencia de dos redes añadidas manualmente a través del botón "Otra..." y disponibles en su configuración o PNL, "WLAN" y "TestTest", durante el proceso de búsqueda de redes Wi-Fi:



5.14.7 PUNTO DE ACCESO WI-FI

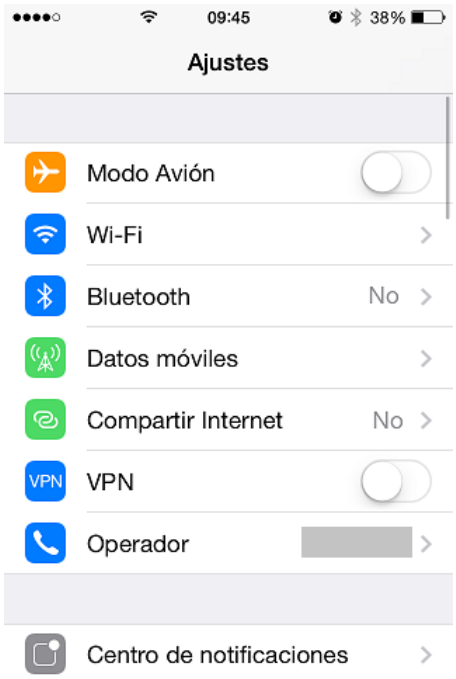
853. iOS dispone de capacidades nativas para actuar como punto de acceso Wi-Fi y *router* (o enrutador) hacia Internet (referido por Apple como *Personal Hotspot* o Compartir Internet), proporcionando acceso a múltiples dispositivos u ordenadores vía Wi-Fi a su conexión de datos de telefonía móvil (2/3/4G) [Ref.- 67].

854. La funcionalidad de *Personal Hotspot* a través de Wi-Fi (frente a las opciones a través de USB o Bluetooth, ver apartado "5.12.2. Conexión de red USB (*Tethering*)") está disponible sólo desde iPhone 4, o posterior, y únicamente a partir del iPad de 3ª generación Wi-Fi+Cellular (o 4G) y del iPad mini Wi-Fi+Cellular.

855. El límite máximo de equipos cliente que pueden conectarse simultáneamente para compartir la conexión de datos de telefonía móvil (2/3/4G) está limitado por el tipo de dispositivo móvil (el modelo concreto de iPhone, iPad o iPad mini), la versión de iOS y por el perfil asociado al operador de telefonía móvil [Ref.- 68].

856. En primer lugar es necesario habilitar la conexión de datos móviles desde el menú "Ajustes - Datos móviles" (ver apartados "5.16. Comunicaciones GSM (2G), UMTS (3G) y LTE (4G): voz y datos" y "5.12.2. Conexión de red USB (*Tethering*)").

857. Para hacer uso de estas capacidades es necesario acceder al menú "Ajustes - Compartir Internet" [Ref.- 68]:



858. A través del botón "Compartir Internet", y teniendo el interfaz Wi-Fi activo en iOS, es posible habilitar el servicio de punto de acceso Wi-Fi, de forma que otros ordenadores y dispositivos puedan utilizar el dispositivo móvil como punto de acceso Wi-Fi para conectarse a Internet.

859. Si el interfaz Wi-Fi no está activo en el momento de compartir la conexión de datos de telefonía móvil, iOS solicitará al usuario su activación (junto al interfaz Bluetooth):

860. El interfaz Wi-Fi de iOS no puede ser usando en modo cliente a la vez que está habilitada la funcionalidad de *Personal Hotspot*. Por tanto, cuando el dispositivo móvil actúa de punto de acceso Wi-Fi, las aplicaciones iOS no pueden utilizar la conexión Wi-Fi como dispositivo cliente, sino que harán uso de la conexión de datos de telefonía móvil

(2/3/4G). Si previamente a su activación la conexión Wi-Fi cliente estaba activa, ésta será deshabilitada automáticamente y desconectada de la red Wi-Fi a la que estaba conectado. Igualmente, tras desactivar el punto de acceso Wi-Fi, la conexión Wi-Fi cliente será habilitada de nuevo automáticamente.

861. En concreto, mientras no se haya establecido ninguna conexión por parte de un cliente Wi-Fi al punto de acceso proporcionado por iOS, el dispositivo móvil puede seguir haciendo uso de su conexión Wi-Fi como cliente (en caso de existir y estar establecida).

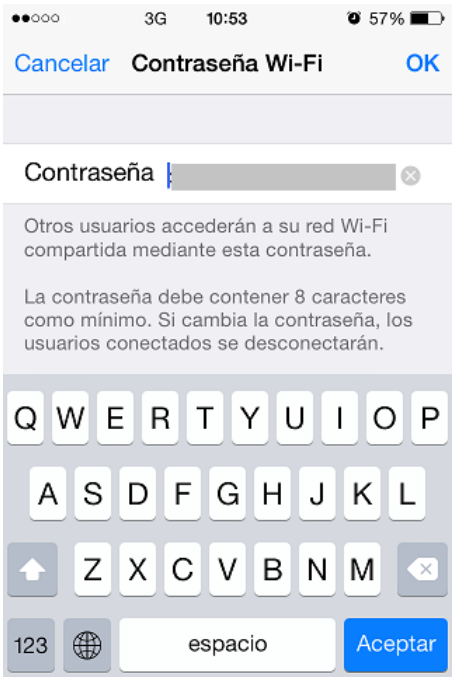
862. Al volver a la pantalla disponible desde el menú "Ajustes - Compartir Internet", el dispositivo móvil dejará de hacer uso de su conexión Wi-Fi como cliente y volverá a anunciar la presencia del punto de acceso Wi-Fi.

863. En cuanto se abandona dicha pantalla o si el dispositivo móvil pasa al estado de reposo, si no hay ningún cliente Wi-Fi conectado, inmediatamente deja de anunciarse la presencia del punto de acceso. Supuestamente, el punto de acceso sólo es anunciado durante 90 segundos (al menos en la versión 5.x de iOS), tiempo disponible para que los clientes Wi-Fi establezcan una conexión [Ref.- 68], siendo necesario reactivarlo si no se ha conectado ningún cliente.

864. El tiempo en el que está disponible el punto de acceso creado y los escenarios cuando éste es activado y desactivado al hacer uso del dispositivo móvil si aún no se ha conectado ningún cliente varía entre distintas versiones de iOS. Por ejemplo, en iOS 7 el punto de acceso permanece activo durante periodos más largos de tiempo incluso sin haber recibido conexiones de clientes Wi-Fi, y su estado puede cambiar si el dispositivo entra en estado suspendido o está específicamente en la pantalla de "Compartir Internet".

865. Debe tenerse en cuenta que, a diferencia de 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 no es obligatorio activar esta funcionalidad antes de completar su configuración. Por tanto, se recomienda realizar las modificaciones de la configuración en primer lugar, tal como establecer la contraseña o el nombre de la red Wi-Fi, y activar la funcionalidad de conexión compartida posteriormente, para evitar potenciales ataques cuando los mecanismos de seguridad no han sido aún aplicados.

866. Mediante el menú "Ajustes - Compartir Internet" y a través de la opción “Contraseña Wi-Fi”, es posible configurar la contraseña Wi-Fi asociada al punto de acceso. El nombre de la red Wi-Fi (o SSID) corresponderá al nombre del dispositivo móvil y las características de seguridad de la red Wi-Fi no pueden ser modificadas, empleándose una red Wi-Fi 802.11g/n con seguridad basada en WPA2:



867. El nombre del dispositivo móvil, y por tanto de la red Wi-Fi, puede ser configurado desde el menú "Ajustes - General - Información" y el campo "Nombre".

868. El punto de acceso Wi-Fi que es habilitado implementa mecanismos de seguridad basados en WPA2-PSK (*Pre Shared Key*, o WPA2-Personal), basado en el uso de una clave compartida (PSK).

869. 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 una contraseña o clave precompartida suficientemente larga (más de 20 caracteres) y difícilmente adivinable [Ref.- 49].

870. En junio de 2013, un estudio de investigación confirmó que las contraseñas generadas automáticamente por iOS 6.x para la funcionalidad de punto de acceso Wi-Fi (o *Personal Hotspot*), y en concreto empleadas como valor de la clave compartida (PSK) del mecanismo de seguridad WPA2-PSK, son susceptibles frente a ataques de fuerza bruta.

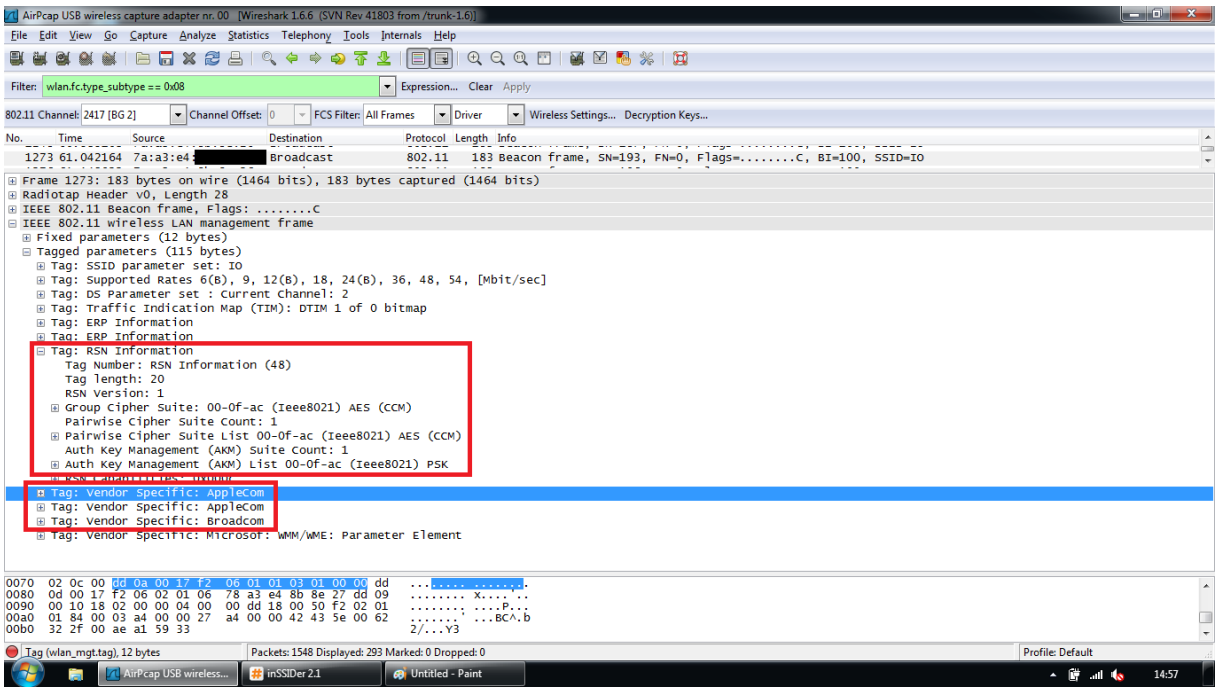
871. Pese a que la contraseña generada por defecto automáticamente por iOS puede parecer suficientemente aleatoria, con hasta 10 caracteres alfanuméricos (de 4 a 6 letras, seguidas de 4 dígitos), el estudio reveló que su aleatoriedad está limitada [Ref.- 170], al generarse a partir de un diccionario de 1.842 entradas. Adicionalmente, el proceso de selección de palabras dentro de ese diccionario tampoco es suficientemente aleatorio, por lo que es posible adivinar la contraseña utilizada por iOS en menos de 50 segundos.

872. En iOS 7 el algoritmo de generación de contraseñas ha sido modificado por Apple (CVE-2013-4616), empleándose 12 caracteres alfanuméricos. Pese a eso, se recomienda seleccionar una contraseña propia y personalizada de más de 20 caracteres y no confiar en la generada automáticamente por el dispositivo móvil.

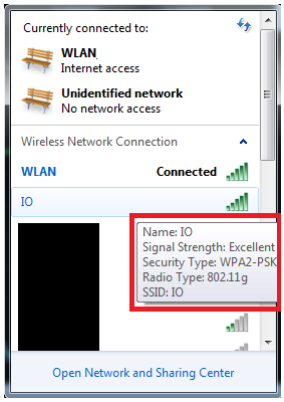
873. El mecanismo de cifrado para WPA2-PSK empleado por defecto por el punto de acceso Wi-Fi proporcionado por iOS es AES-CCMP, opción recomendada desde el punto de vista de seguridad.

874. 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 (nombre del propio dispositivo móvil), con el objetivo de no desvelar que se trata de un punto de acceso basado en un dispositivo móvil iOS o datos de su propietario.

875. Sin embargo, debe tenerse en cuenta que las tramas de anuncio (o *beacon*) del punto de acceso creado por iOS incluyen etiquetas propietarias de Apple que desvelan, al menos, el fabricante del dispositivo ("AppleCom"):

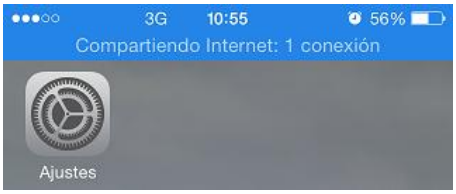


876. La red Wi-Fi creada es de tipo punto de acceso (o infraestructura), se anuncia en el canal 2 (por ejemplo, de 802.11g), y proporciona incluso capacidades de servidor DHCP para la asignación de direcciones IP a los dispositivos cliente y ordenadores que se conectan a ella:



877. Tras establecerse la conexión de red a través de la red Wi-Fi creada por iOS, y tomando como referencia Windows 7 como sistema operativo del ordenador cliente, el interfaz de red Wi-Fi funciona al estar configurado con una dirección IP dinámica (DHCP), asignándose por defecto una dirección IP con máscara /28 (255.255.255.240), como por ejemplo 172.20.10.3:

878. La barra de estado del dispositivo móvil iOS pasará a ser de color azul e indicará el número de conexiones activas, es decir, el número de clientes conectados al dispositivo móvil, en cada momento. Este comportamiento de la barra de estado es visible desde cualquier pantalla del dispositivo móvil:



879. El dispositivo móvil (por ejemplo, con dirección IP 172.20.10.1) actúa de *gateway*, *router* o pasarela por defecto, de servidor DHCP, y los servidores DNS asignados mediante DHCP corresponden a los servidores DNS públicos obtenidos por iOS en la conexión de datos de telefonía móvil (2/3/4G), y es alcanzable mediante ping (ICMP).

Nota: El direccionamiento IP empleado por iOS para el punto de acceso Wi-Fi (172.20.10.x/28) no puede ser modificado.

880. La dirección MAC asociada al interfaz de red del punto de acceso Wi-Fi tiene asociado un OUI con valor "7A:A3:E4" (podría variar entre distintas versiones de iOS), qué no está asignado a ningún vendedor públicamente en el momento de elaboración de la presente guía. El valor corresponde exactamente con el valor de la dirección MAC del interfaz Wi-Fi del dispositivo móvil, dónde únicamente varía el valor del segundo carácter hexadecimal (de "78" a "7A"), siendo la dirección MAC del interfaz Wi-Fi en este ejemplo "78:A3:E4:01:02:03".

881. 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:

- Los únicos puertos TCP abiertos son los correspondientes al servidor FTP (21/tcp) y al servicio de sincronización de iOS con iTunes (62078/tcp). El

supuesto servidor FTP permite establecer una conexión mediante TCP pero no se recibe ninguna respuesta posterior para acceder a este servicio.

- Los únicos puertos UDP abiertos son los correspondientes al servidor mDNS (o zeroconf) (5353/udp) y al servidor DHCP (67/udp).

882. 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 puntos de acceso implementados por los dispositivos móviles basados en iOS de forma sencilla una vez conectados a ellos.

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

5.14.8 INTEGRACIÓN CON AIRDROP

884. AirDrop es un servicio propietario de Apple (similar al estándar *Wi-Fi Direct*) que permite compartir o transferir ficheros y datos entre equipos con OS X o dispositivos móviles iOS de manera inalámbrica, sin tener por tanto que hacer uso del correo electrónico, iMessage/MMS, un dispositivo de almacenamiento o servicios de almacenamiento "en la nube".

885. iOS 7 introduce soporte para AirDrop, previamente sólo disponible en OS X 10.7.x (Lion) o superior, integrando en esta plataforma móvil las capacidades de transferencia de datos inalámbricas, incluyendo el intercambio de ficheros, fotos, vídeos, sitios web, localizaciones, etc.

886. Por defecto AirDrop permite el intercambio de fotos (desde la app de "Fotos"), tarjetas de visita (desde "Contactos"), notas (desde "Notas"), URLs (desde "Mobile Safari"), tarjetas de Passbook, listados de apps (desde la "AppStore"), listados multimedia (desde "iTunes"), y estaciones de radio (desde "iTunes Radio"), entre otros. Otras apps de terceros también pueden integrar la funcionalidad de AirDrop para compartir otro tipo de datos.

887. En el caso de OS X, AirDrop hace uso de tecnologías Wi-Fi propietarias de Apple, mientras que en el caso de iOS, AirDrop emplea tanto tecnologías Wi-Fi como Bluetooth LE (BTLE o 4.0), debiendo ambos interfaces estar activos para poder hacer uso de las capacidades de AirDrop. Por tanto, los servicios AirDrop de OS X y de iOS son incompatibles, no siendo posible las transferencias entre dispositivos móviles y equipos tradicionales.

888. AirDrop está soportado únicamente a partir del iPhone 5 en adelante, y a partir del iPad de 4ª generación, o el iPad mini, en adelante.

889. Las capacidades de AirDrop [Ref.- 166] están disponibles en iOS 7 a través del Centro de Control (ver apartado "5.6.3. Centro de Control"). Desde el menú disponible al seleccionar AirDrop es posible apagarlo, permitir únicamente comunicaciones con los contactos (para lo que es necesario que ambos usuarios dispongan de una cuenta iCloud activa a la que estén conectados, y que el Apple ID del otro usuario esté en la lista de contactos), opción configurada por defecto, o permitir conexiones con cualquier usuario. En este último caso, el dispositivo móvil iOS estará visible para cualquier usuario cercano con capacidades de AirDrop:

890. Las apps con capacidades de AirDrop (Fotos, Mobile Safari, Contactos, Mapas, Notas, iTunes (Radio), etc) permiten el intercambio de datos a través del icono de compartir información: (un cuadrado con una flecha en la parte superior).

891. El emisor anuncia su intención de compartir datos empleando Bluetooth LE, tecnología que también se utiliza para descubrir la existencia de otros dispositivos cercanos y para que posteriormente, el receptor, responda con la identidad del usuario (mediante un *hash* identificativo).

892. Si el emisor identifica la existencia de un usuario válido y permitido (en base a la lista de contactos sincronizada con iCloud), acepta la comunicación con dicho usuario y crea una red Wi-Fi *ad-hoc* (o *peer-to-peer*) y anuncia la existencia de la conexión AirDrop mediante el servicio de descubrimiento multicast DNS (*Bonjour*).

893. AirDrop posteriormente emplea TLS para la transferencia de datos, llevando a cabo la verificación de ambos extremos en base a los certificados de iCloud de ambos usuarios.

894. Al activarse AirDrop se genera una identidad en el dispositivo móvil basada en certificados de clave pública y privada. Adicionalmente se emplea un *hash* de la identidad del usuario, en base a la dirección de e-mail y el número de teléfono asociado al Apple ID del usuario.

895. El destinatario de la transferencia obtendrá un mensaje de alerta, teniendo que aceptar (o rechazar) la conexión AirDrop antes de que ésta se lleve a cabo, y los datos recibidos se abrirán en la app asociada.

896. En el caso de únicamente permitir comunicaciones con los contactos del usuario, opción recomendada en el caso de hacer uso de AirDrop, se lleva a cabo un proceso de verificación más exhaustivo, e incluso visualmente se identifica al otro extremo de la comunicación con su imagen y nombre existente en la lista de contactos del dispositivo móvil.

897. En el caso de permitir comunicaciones con cualquiera, y no disponer de una entrada para el otro usuario en la lista de contactos, se mostrará una silueta y el nombre configurado en el otro dispositivo móvil iOS, lo que abre la posibilidad a ataques de ingeniería social suplantando a otros usuarios mediante la manipulación del nombre del dispositivo.

898. AirDrop, pese a hacer uso de TLS, es potencialmente vulnerable en ciertos escenarios a ataques de interceptación o Man-in-the-Middle (MitM), ya que puede emplear certificados anónimos disponibles en la librería *CFNetwork* de Apple[9].

899. Las capacidades de AirDrop pueden ser deshabilitadas a través de un perfil de configuración mediante la solución de gestión empresarial (MDM), pero únicamente para dispositivos móviles iOS supervisados, lo que limita notablemente poder deshabilitar esta funcionalidad en muchos entornos corporativos sin dispositivos supervisados.

900. Por este motivo, se recomienda incrementar la concienciación del usuario respecto a esta tecnología, si se hará uso de ella, y en qué escenarios.

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

901. 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), o incluso LTE (*Long Term Evolution*, 4G).

902. 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.

903. 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*).

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

905. Durante el año 2009 se publicaron diferentes vulnerabilidades de denegación de servicio (DoS) en el módulo SMS de dispositivos móviles, incluyendo iOS [Ref.- 1].

906. Una vulnerabilidad en dispositivos iPhone (CVE-2009-2204) afectaba a la decodificación de mensajes SMS. Un atacante podía enviar un mensaje SMS malicioso y provocar una denegación de servicio en el terminal víctima, o incluso tomar control del mismo mediante la ejecución remota de código. Este ataque sólo necesitaba que el teléfono estuviera encendido, no requiriendo ninguna intervención por parte del usuario y éste sólo se percataría de la recepción de un SMS anormal, con un único carácter.

907. Esta vulnerabilidad obligó a Apple a distribuir una nueva actualización del sistema operativo del iPhone, iOS versión 3.0.1, qué afectaba al módulo de telefonía del terminal. Este tipo de amenazas reflejan la importancia que mantener los dispositivos actualizados frente a las últimas vulnerabilidades descubiertas y con la última versión facilitada por el fabricante.

[9] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1800

908. El proceso CommCenter del iPhone se encarga de gestionar los mensajes SMS y las llamadas de teléfono. Debido a que ejecuta como root y no está confinado a un entorno de ejecución restringido (*sandbox*), una vulnerabilidad en el mismo (como la mencionada) permitía disponer de control completo del dispositivo.

909. Adicionalmente, en agosto de 2012, pod2g publicó la posibilidad de suplantar el remitente de cualquier mensaje corto (SMS) en cualquier versión de iOS desde la 1.x hasta la 6beta4 mediante la modificación de la cabecera UDH (*User Data Header*) "reply-to", con las implicaciones de seguridad asociadas, debido al uso masivo de los SMS por los usuarios y a emplearse hoy en día los SMS como mecanismo de autentificación de dos factores en transacciones financieras [Ref.- 176].

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

- No deberían abrirse mensajes de texto recibidos desde números desconocidos, ni ejecutar, abrir o permitir la instalación de contenidos adjuntos (configuraciones, enlaces web (URLs), 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.

911. 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.

912. Los nuevos mecanismos de autentificación de la banca (y muchos otros servicios) online también emplean los mensajes de texto para el envío de contraseñas de un solo uso para la realización de operaciones bancarias críticas o como parte del proceso de autentificación mediante dos factores. El acceso a dicho mensaje por parte de un potencial atacante permitiría completar la operación, como por ejemplo, una transferencia bancaria, o disponer de las credenciales de autentificación:

Nota: En iOS 5.x Apple ha introducido un nuevo servicio de mensajería denominado iMessage [Ref.- 78], disponible sólo entre dispositivos móviles basados en iOS 5.x y OS X (Mountain Lion, y opcionalmente Lion). Este servicio integra en los dispositivos móviles iOS, y en una única aplicación ("Mensajes"), las capacidades de mensajería tradicionales de los operadores de telefonía móvil, a través de mensajes de texto (SMS) y MMS, y las capacidades de mensajería instantánea (IM, *Instant Messaging* o *chat*) propias de Internet y TCP/IP (empleando las comunicaciones Wi-Fi o 2/3/4G del dispositivo), similares a las de otros servicios como Jabber, AIM, Google Talk o WhatsApp.

iMessage permite el envío de texto, fotos, vídeos, ubicaciones y contactos, así como mensajería en grupo, y dispone de la posibilidad de generar acuses de recibo y de lectura (ver apartado "5.17.1. iMessage").

5.16 COMUNICACIONES GSM (2G), UMTS (3G) Y LTE (4G): VOZ Y DATOS

5.16.1 DESACTIVACIÓN DE LAS COMUNICACIONES DE VOZ Y DATOS 2/3/4G

913. La principal recomendación de seguridad asociada a las comunicaciones de voz (incluyendo 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 o configurar minuciosamente los ajustes asociados al interfaz de telefonía celular.

914. Desafortunadamente, el uso de las capacidades de telefonía en teléfonos móviles como el iPhone es una situación extremadamente habitual, al ser ésta una de las funcionalidades principales de los dispositivos móviles, por lo que no es posible aplicar la primera de las recomendaciones y deshabilitarlas frecuentemente.

915. Desafortunadamente, la segunda de las recomendaciones tampoco puede ser aplicada fácilmente, ya que los ajustes de telefonía existentes son muy limitados en la plataforma móvil bajo estudio.

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, o la utilización de una tarjeta SIM sin código PIN.

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.

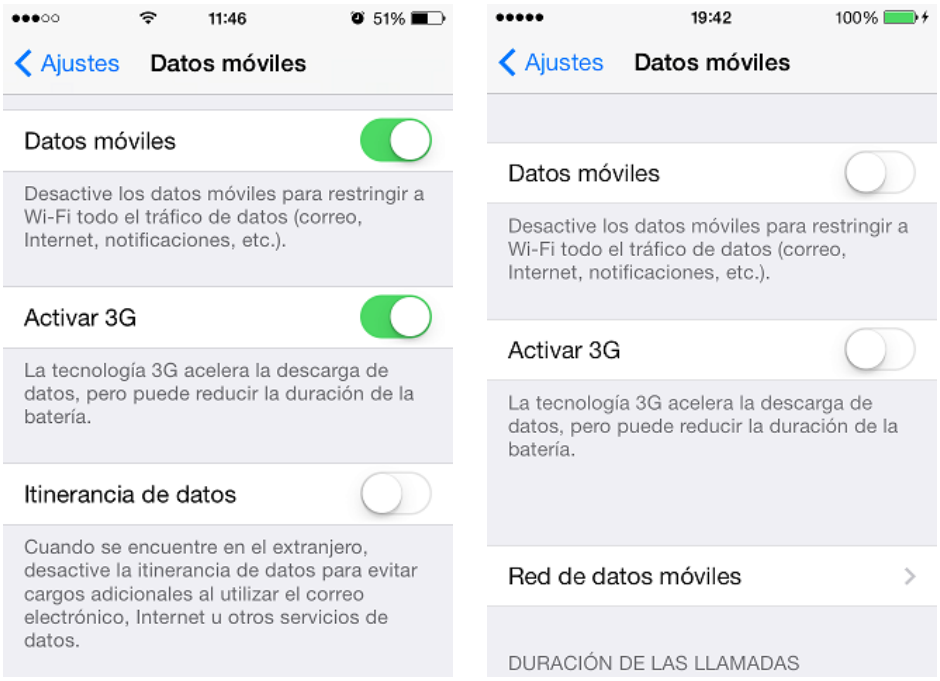
916. iOS únicamente permite a través del interfaz de usuario estándar deshabilitar de forma individualizada las capacidades de telefonía móvil (voz y SMS) a través de la opción "Modo Avión" del menú "Ajustes".

917. Al activar el modo avión en iOS, la conectividad a redes Wi-Fi o Bluetooth puede ser habilitada posteriormente y de forma independiente, mientras que la conectividad de telefonía móvil sigue deshabilitada. No así la conectividad de datos móviles 2/3/4G, directamente ligada al modo avión.

918. Pese a que iOS permite habilitar los datos móviles tras activar el modo avión, el interfaz de telefonía móvil no estará disponible ni para voz y SMS, ni para datos, hasta que no se deshabilite el modo avión.

919. 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.

920. Las conexiones de datos a través de la red de telefonía móvil (2/3/4G), GPRS, UMTS o LTE (referenciadas como 2/3/4G en adelante por simplificar), pueden ser deshabilitadas a través del menú "Ajustes - Datos móviles" y en concreto del botón "Datos móviles", siendo posible desconectar únicamente el interfaz de datos de telefonía móvil 2/3/4G, mientras es aún posible emplear las capacidades de voz y SMS:



921. Una vez activado el interfaz, 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 (2/3/4G), especialmente cuando el contrato tiene gastos asociados por la cantidad de datos transmitidos y/o por tiempo o número de conexiones establecidas, o se viaja internacionalmente (itinerancia o *roaming*). Múltiples aplicaciones en iOS pueden iniciar este tipo de conexiones de datos en diferentes momentos del día (ver apartado "5.16.5. Utilización selectiva de la red de datos 2/3/4G").

922. Por defecto en iOS (configuración de fábrica) el interfaz de voz y datos de telefonía móvil está habilitado (tras desbloquear la tarjeta SIM en caso de estar protegida por un PIN), con los APNs que han sido definidos en iOS por el perfil de configuración asociado al operador de telefonía de la tarjeta SIM empleada.

923. Se recomienda por tanto deshabilitar el interfaz de telefonía del dispositivo móvil tan pronto finaliza el proceso inicial de configuración con el objetivo de llevar a cabo la configuración personalizada del dispositivo antes de establecer conexiones adicionales.

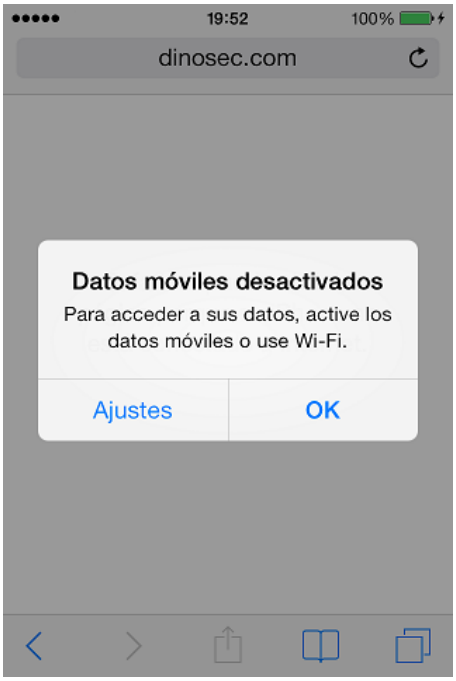
924. iOS mantiene el estado del interfaz de telefonía de datos tras reiniciar el dispositivo móvil, es decir, si el interfaz de telefonía de datos estaba activo al apagar el terminal, al encender el dispositivo móvil e introducir el PIN de la tarjeta SIM, seguirá activo.

925. 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).

926. Los dispositivos móviles iOS disponen de capacidades para que el usuario habilite o deshabilite el interfaz de radio de telefonía móvil (a través del modo avión) o las

capacidades de datos de dicho interfaz (a través de "Datos móviles"), no siendo posible evitarlo.

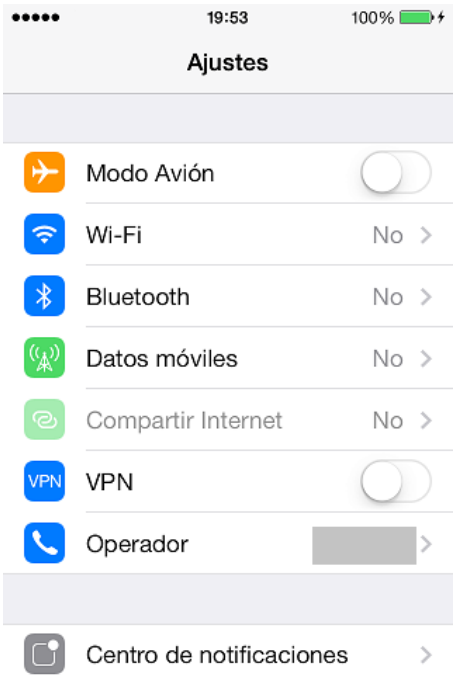
927. Tras desactivar la conexión de datos, si alguna aplicación requiere disponer de conectividad (por ejemplo, navegación web desde “Safari”), y no se dispone de conectividad a través de redes Wi-Fi, la conexión de telefonía de datos no será activada automáticamente, notificándose al usuario de la ausencia de conectividad para que proceda a su activación de forma manual desde el menú "Ajustes":



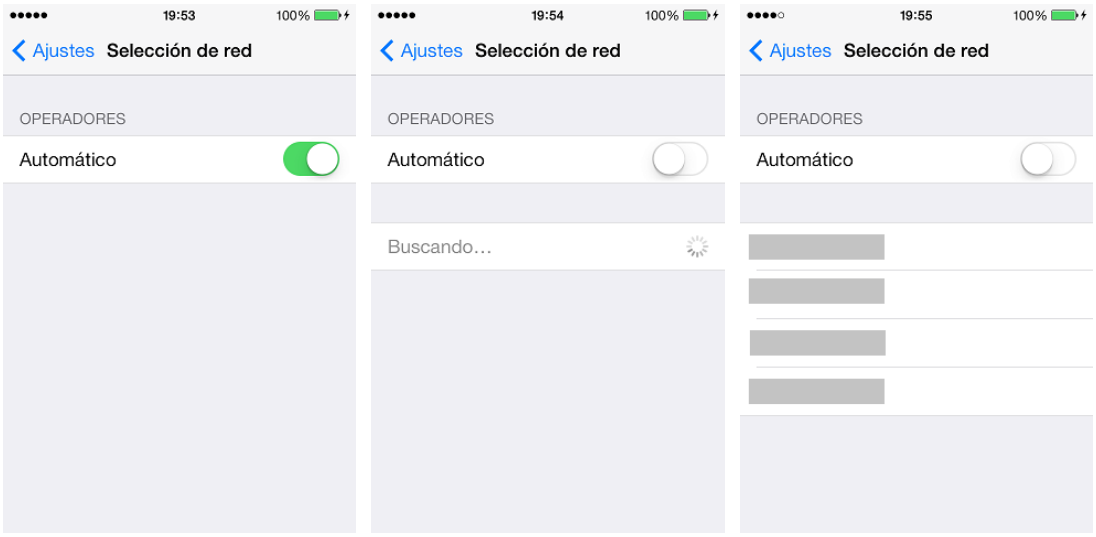
5.16.2 SELECCIÓN DE LA RED DE VOZ Y DATOS DE TELEFONÍA MÓVIL

928. iOS 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).

929. Desde el menú de configuración del teléfono “Ajustes - Operador”, mediante la desactivación del botón "Automático" (habilitado por defecto), el dispositivo móvil realizará la búsqueda de operadores de telefonía móvil en la zona de cobertura:



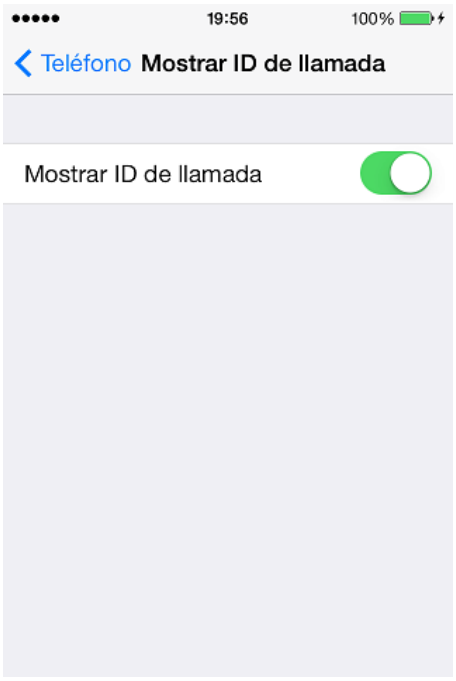
930. Como resultado mostrará al usuario la lista de operadores de telecomunicaciones identificados, siendo posible seleccionar manualmente el operador deseado:



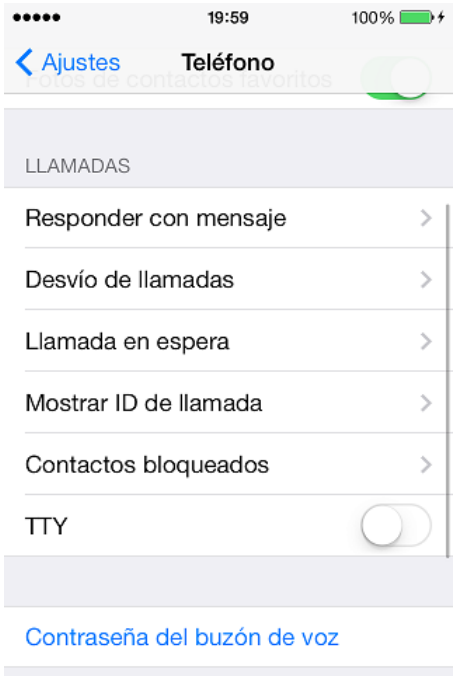
931. La selección de red permite definir si la red de telefonía será seleccionada de forma automática (opción por defecto) por el dispositivo móvil en función de la tarjeta SIM y de la intensidad de la señal, o sí el usuario puede definir de forma manual la red a la que desea conectarse de la lista de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

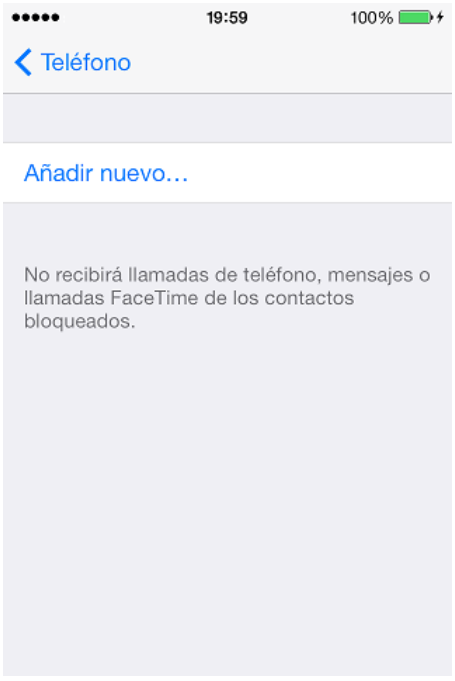
932. Por otro lado, y con el objetivo de proteger la privacidad del usuario, el módulo de telefonía de iOS permite al usuario definir si se enviará la información de identificación como autor de la llamada, disponiendo de la opción de ocultar siempre el número o mostrar el número para todas las llamadas.

933. Desde el menú “Ajustes – Teléfono", mediante la opción “Mostrar ID de llamada”, es posible configurar la opción deseada:



934. Adicionalmente, desde iOS 7 la plataforma proporciona capacidades para filtrar comunicaciones con ciertos usuarios. A través de la opción "Contactos bloqueados" del menú "Ajustes - Teléfono" es posible crear una lista negra de contactos (seleccionándolos de la lista de contactos del dispositivo móvil) de los que no se desea recibir llamadas de teléfono, mensajes (SMS/MMS, iMessage...) o llamadas de FaceTime:





935. En las redes 2/2.5G, tanto en GSM como en GPRS/EDGE, las comunicaciones son cifradas habitualmente mediante el algoritmo A5/1 (que presenta debilidades de seguridad ampliamente conocidas), mecanismo que es seleccionado por la red del operador de telefonía al establecerse la comunicación con el terminal.

936. Existen otros algoritmos de cifrado disponibles, como A5/0, en el que no se realiza ningún cifrado de las comunicaciones, es decir, éstas viajan en claro sin cifrar. Este algoritmo es empleado en algunos países de acuerdo a las leyes locales, como India.

937. Los dispositivos móviles iOS no notifican al usuario cuando se hace uso del algoritmo A5/0 (independientemente de las restricciones existentes en la tarjeta SIM) y, por tanto, cuando sus comunicaciones pueden ser interceptadas al no estar cifradas. Este algoritmo puede ser empleado por un potencial atacante para interceptar las comunicaciones de los usuarios a través de una estación base falsa GSM [Ref.- 97].

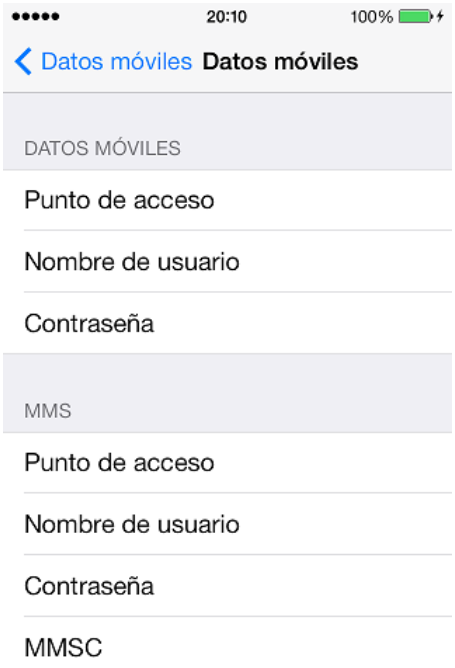
Nota: Existen soluciones propietarias de cifrado extremo a extremo de las comunicaciones y llamadas de voz, como CellCrypt Mobile, proporcionadas por terceras compañías de forma gratuita (únicamente la aplicación móvil) a través de la App Store y asociadas a un servicio de pago [Ref.- 84]. CellCrypt Mobile hace uso de cifrado FIPS 140-2 para comunicaciones de Voz sobre IP (VoIP) entre dos terminales compatibles, haciendo uso de redes IP (Wi-Fi o móviles, 2/3/4G) para las llamadas.

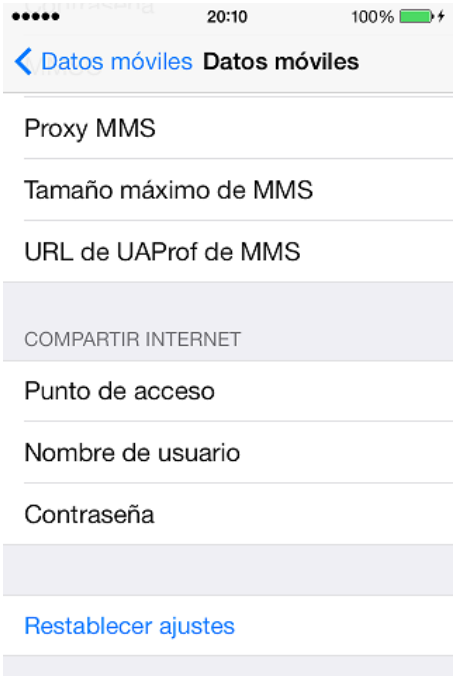
5.16.3 CONFIGURACIÓN DE LA RED DE DATOS DE TELEFONÍA MÓVIL

938. iOS permite al usuario, al igual que para la red de telefonía móvil (voz y SMS), 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*) o punto de acceso para las conexiones móviles de datos.

939. En dispositivos móviles iOS como el iPhone, al introducir la tarjeta SIM en el dispositivo móvil se lleva a cabo automáticamente (a través del perfil de configuración de iOS asociado al operador de telefonía) el proceso de configuración de las opciones de conectividad de datos asociadas a las redes de telefonía móvil, incluyendo los APNs y su configuración: APN o punto de acceso y credenciales (usuario y contraseña) tanto para datos móviles como para las capacidades de compartir Internet (ver apartado "5.12.2. Conexión de red USB (*Tethering*)"). Adicionalmente, la configuración incluye la configuración de mensajes multimedia (MMS): punto de acceso, credenciales (usuario y contraseña), MMSC, proxy MMS, tamaño máximo de MMS y URL de UAProf de MMS.

940. 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 el apartado de "Red de datos móviles" del menú "Ajustes - Datos móviles", menú que permite acceder a las opciones de configuración descritas previamente, o ningún punto de acceso (o APN) si no dispone de los datos correspondientes a dicho operador de telefonía (en cuyo caso habrá que añadirlos manualmente):





941. Al definir un nuevo APN deben emplearse los valores proporcionados por el operador de telecomunicaciones.

942. 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.

943. El botón "Restablecer ajustes" permite restaurar la configuración de datos móviles a la asociada por defecto al operador de telefonía móvil utilizado según la tarjeta SIM.

944. Debe tenerse en cuenta que, salvo emplearse un perfil de configuración, las modificaciones realizadas manualmente sobre la configuración de datos móviles se

perderán al actualizar la versión de iOS, siendo necesario modificarla de nuevo tras cada nueva actualización [Ref.- 80].

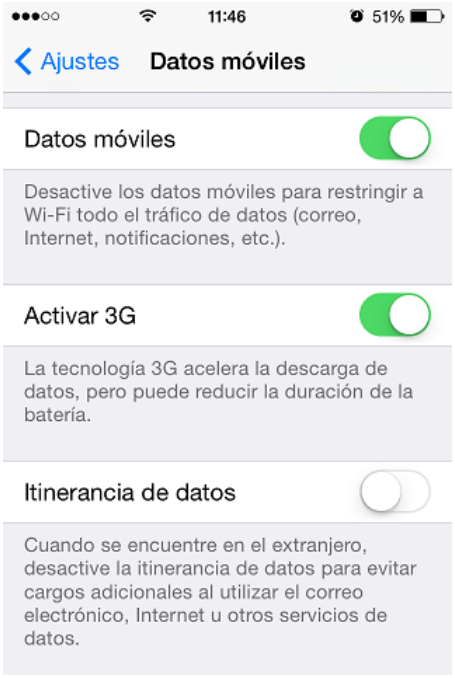
5.16.4 SELECCIÓN DEL TIPO DE RED DE DATOS 2/3/4G

945. 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].

946. 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) o 4G (LTE).

947. iOS no permite restringir las comunicaciones de telefonía móvil sólo a redes 3G ó 4G a través del interfaz gráfico de usuario estándar.

948. Sin embargo, iOS sí permite establecer que el dispositivo móvil sólo haga uso de redes 2G (GPRS o EDGE) para las comunicaciones de datos a través de las redes de telefonía, una opción disponible para disminuir el consumo de batería del terminal y de los gastos asociados al consumo de datos, pero desaconsejada desde el punto de vista de seguridad, a través del menú “Ajustes - Datos móviles”, y en concreto de la opción “Activar 3G”:



949. 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 ó 4G de los operadores de telefonía móvil.

950. El principal inconveniente de esta configuración en la que sí se han activado las capacidades 3G ó 4G es que si el usuario se encuentra en una zona dónde no se dispone de cobertura 3G (o superior, 3.5G o 4G), se podrá hacer uso del dispositivo móvil a

través de 2G, premiando la disponibilidad del servicio de telefonía (voz y datos) por encima de la seguridad.

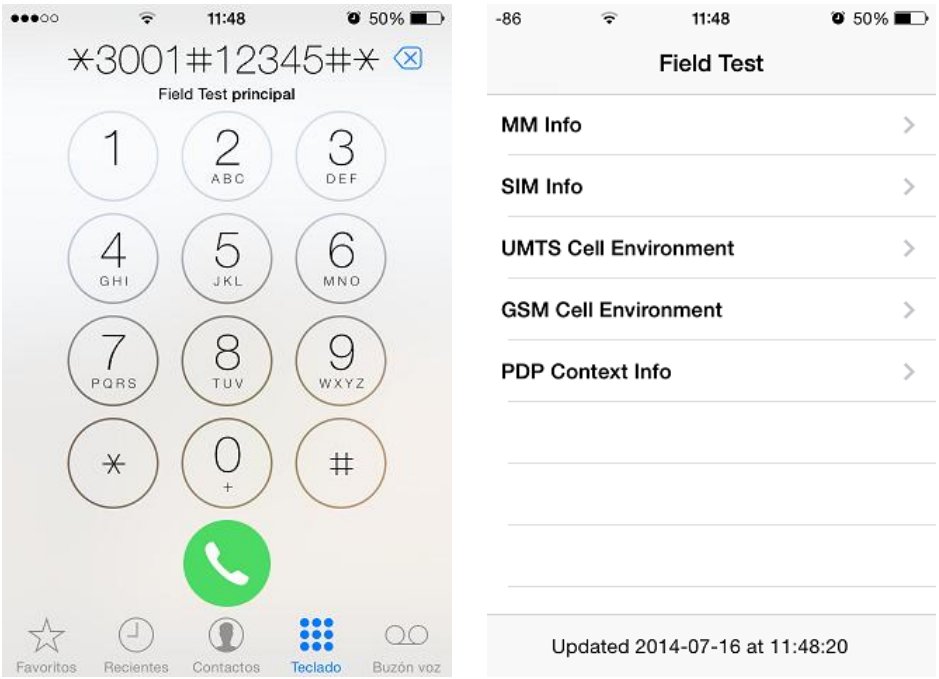
951. iOS proporciona información en la barra de estado superior sobre las tecnologías de telefonía móvil de datos para las que se dispone de cobertura de datos a través del siguiente conjunto de símbolos, que representan la disponibilidad y el estado de la conexión para una red "4G" (LTE, *Long Term Evolution* - UMTS), "3G" (3G o 3.5G, WCDMA/UMTS o HSPA), "E" (2.75G o EDGE) y "●" (2G o GPRS), respectivamente [Ref.- 79].

952. La posibilidad de conexión 4G (o LTE) está disponible sólo en el iPhone 5 o el iPad Wi-Fi+Cellular o Wi-Fi+4G (iPad de 3ª generación) y modelos posteriores. Adicionalmente a las redes GSM indicadas, el iPhone dispone de soporte para redes CDMA (1xRTT y EV-DO) en diferentes países.

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

954. La configuración por defecto del dispositivo móvil premia la conectividad, permitiendo el uso de redes de telefonía móvil 2/3/4G de forma automática en función de su cobertura, intensidad de señal y disponibilidad.

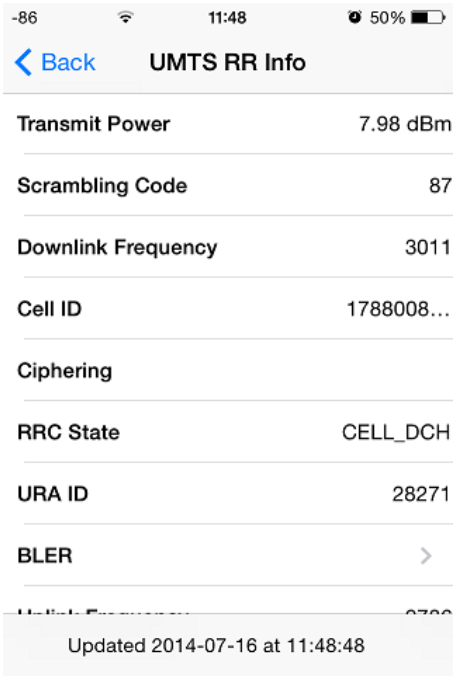
955. Adicionalmente, es posible obtener y configurar información avanzada a través del menú del modo de prueba (o *Field Test*), disponible en iOS tras marcar el siguiente número de teléfono, *3001#12345#*, y pulsar la tecla de llamada:



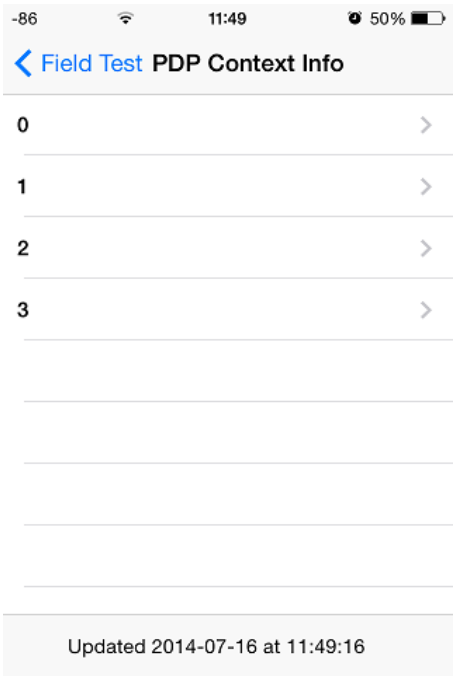
956. El modo de prueba indica la intensidad de la señal de telefonía móvil en la barra superior de estado mediante un valor numérico, más preciso que las barras de cobertura.

957. Este modo proporciona adicionalmente numerosos detalles relacionados con las redes de telefonía móvil y el interfaz de radio del dispositivo móvil, como por ejemplo intensidad

de diferentes parámetros de la señal y frecuencias empleadas, o la celda de servicio y celdas vecinas actualmente tanto para UMTS como para GSM [Ref.- 85]:



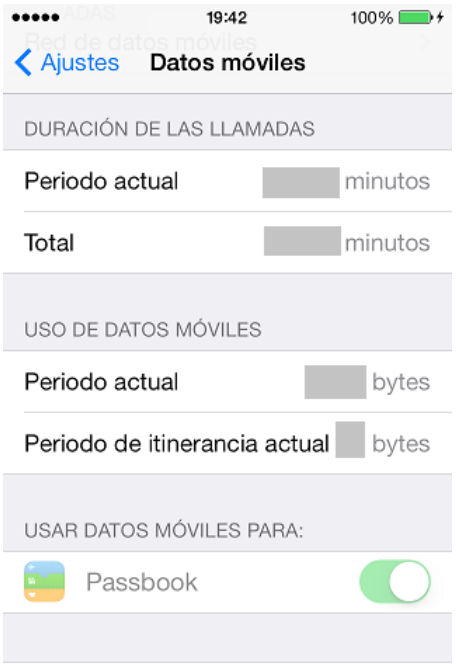
958. Por ejemplo, mediante la selección de la opción “PDP Context Info”, y del primero de los nodos disponibles, "0", se dispone de los detalles de la dirección IP obtenida a través del interfaz de datos móviles (2/3/4G) y de la red de telefonía móvil, junto al punto de acceso (APN). Esta dirección IP no está disponible a través del interfaz gráfico de usuario de iOS:



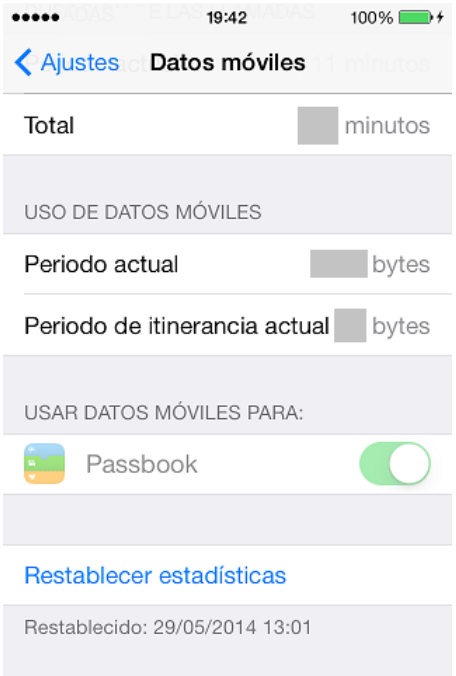
959. El modo de prueba permite obtener muchos detalles de operación del interfaz de radio del dispositivo móvil, pero no permite modificar los parámetros disponibles.

5.16.5 UTILIZACIÓN SELECTIVA DE LA RED DE DATOS 2/3/4G

960. Desde iOS 7, el menú de "Ajustes - Datos móviles" proporciona adicionalmente información de uso del interfaz de telefonía móvil, incluyendo la duración de las llamadas de voz (en minutos) y el consumo (en bytes) de los datos móviles en el periodo actual:



961. El periodo actual está reflejado en la parte inferior de dicho menú, con la fecha y la hora en la que las estadísticas fueron restablecidas por última vez. El botón "Restablecer estadísticas" permite comenzar un nuevo periodo:



962. Por otro lado, la sección "Usar datos móviles para:" permite definir de manera granular qué apps de sistema o instaladas posteriormente en el dispositivo móvil pueden hacer uso

de las capacidades de transmisión de datos a través de las redes de telefonía móvil, pudiendo el usuario en todo momento activar o desactivar estas capacidades para cada app de manera individual.

963. Por defecto todas las apps disponen de capacidades para hacer uso del interfaz de telefonía móvil 2/3/4G, pero a través del menú "Ajustes - Datos móviles" (en la parte inferior: "Usar datos móviles para:") es posible configurar selectivamente qué apps podrán solo hacer uso de comunicaciones a través de redes Wi-Fi (es decir, no podrán usar las redes de telefonía para las transferencias de datos).

964. Adicionalmente, esta configuración granular es aplicable a los servicios del sistema. Mediante la opción "Servicios del sistema" (en la parte inferior, tras todas las apps disponibles) del menú "Ajustes - Datos móviles" es posible visualizar el consumo de cada uno de los servicios del sistema, pero no es posible deshabilitar los mismos.

5.17 COMUNICACIONES PROPIETARIAS DE APPLE

965. Los dispositivos móviles basados en iOS disponen de diferentes capacidades de comunicación propietarias de Apple, como por ejemplo iMessage, para mensajería instantánea, o FaceTime, para llamadas de videoconferencia.

Nota: El alcance de la presente guía no contempla la realización de un análisis de seguridad detallado de iMessage [Ref.- 136]o FaceTime [Ref.- 138] y sus protocolos de comunicaciones asociados, y en particular, del tráfico cifrado.

5.17.1 IMESSAGE

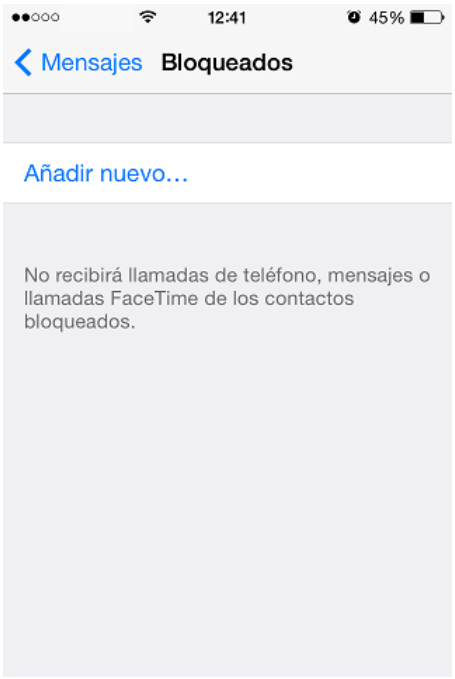
966. iMessage es el servicio propietario de Apple para el envío de mensajes de texto, tanto instantáneos a través de TCP/IP como SMS (o MMS), a través de las redes de los operadores de datos de telefonía móvil, junto a imágenes, vídeos, contactos, localizaciones, etc, disponible desde iOS 5.x.

967. Al contrario que otros servicios de mensajería, iMessage encola durante un periodo de hasta 7 días los mensajes en el caso de que los dispositivos móviles destino no estén disponibles (*offline*), para su posterior envío.

968. La configuración de iMessage se realiza desde el menú "Ajustes - General - Mensajes", y la aplicación de acceso al servicio disponible por defecto en iOS se denomina "Mensajes".

969. Por defecto el servicio no está activo, pudiendo ser habilitado a través del botón "iMessage" disponible en el menú de configuración previamente indicado:

970. Adicionalmente, desde iOS 7 la plataforma proporciona capacidades para filtrar comunicaciones con ciertos usuarios. A través de la opción "Contactos bloqueados" del menú "Ajustes - Mensajes" o "Ajustes - Facetime" es posible crear una lista negra de contactos (seleccionándolos de la lista de contactos del dispositivo móvil) de los que no se desea recibir llamadas de teléfono, mensajes (SMS/MMS, iMessage...) o llamadas de FaceTime:



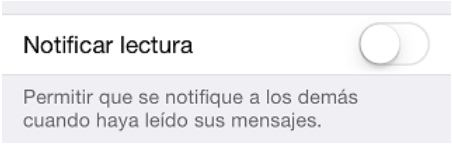
971. La activación del servicio iMessage se establece a través del servidor "service.ess.apple.com" mediante HTTPS en el puerto 443/tcp. También se hace uso de conexiones cifradas al servidor "service1.ess.apple.com" (y similares, como "service2", "static", "init", etc, y "setup.icloud.com") en el puerto 443/tcp.

972. También se llevan a cabo conexiones HTTP (80/tcp) no cifradas contra el servidor "init.ess.apple.com", lo que potencialmente podría dar lugar a ataques de manipulación de dicho tráfico al no estar cifrado, para intercambiar una firma ("<key>signature</key>"), información de certificados digitales codificados en base64 ("<key>certs</key>") y una "bag" o fichero XML ("<key>bag</key>") que contiene detalles de las operaciones y parámetros asociados al servicio, y en concreto hacia el recurso "/WebObjects/VCInit.woa/wa/getBag?ix=1", empleando el siguiente agente de usuario que revela la versión de iOS, el tipo y modelo de dispositivo móvil:

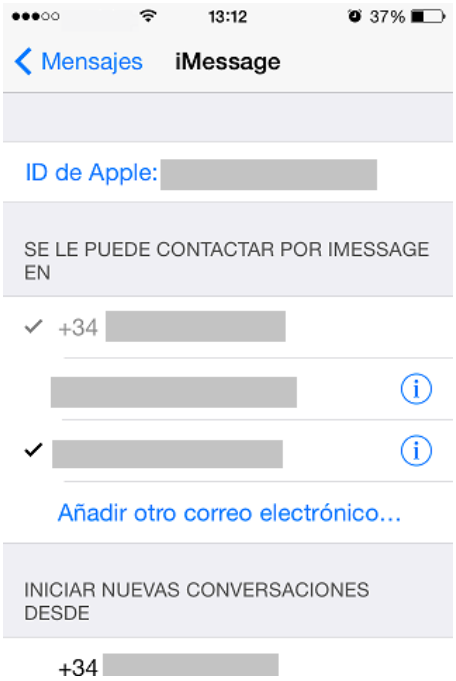
```
User-Agent: server-bag [iPhone OS,7.1.2,11D257,iPhone4,1]
```

973. Los diferentes servicios disponibles en el dominio "*.ess.apple.com" se emplean como canal de comunicación para el intercambio de mensajes de gestión, como los asociados al proceso de autentificación, administración, intercambio de claves y contactos [Ref.- 136].

974. Las opciones de configuración de iMessage permiten notificar al resto de usuarios de la lectura de los mensajes ("Notificar lectura"), opción desaconsejada dese el punto de vista de la privacidad, y enviar los mensajes como SMS en caso de no estar iMessage disponible (en el caso del iPhone), opción que puede tener implicaciones en la confidencialidad de los mensajes si está habilitada y se hace uso de redes 2G:



975. Por defecto y tras completar el proceso de validación, la activación del servicio iMessage se asigna a dos direcciones en los dispositivos móviles iPhone, tanto a la dirección (o e-mail) del usuario en iCloud (identificador de Apple o Apple ID), referenciado en la sección "Enviar y recibir" (ver imágenes superiores), y empleado en la configuración de iMessage en iOS, como al número de teléfono móvil del dispositivo móvil (iPhone). Este último es un identificador obligatorio en el caso de iPhone que no puede ser desvinculado del servicio para la recepción de mensajes (por lo que aparece sombreado en color gris):



976. En el caso de dispositivos móviles iPad, al no disponer éstos de capacidades de telefonía móvil de voz y SMS/MMS, ni por tanto de un número de teléfono, es necesario asociar el servicio de iMessage a un identificador de Apple (Apple ID) y su dirección de e-mail asociada.

977. Los mensajes son enviados a través del servicio APNS, cifrados mediante TLS empleando el puerto 5223/tcp, hacia los servidores "rand<N>-courier.push.apple.com" (dónde "N" es un valor entre 0 y 255) y haciendo uso de autentificación cliente mediante certificados digitales.

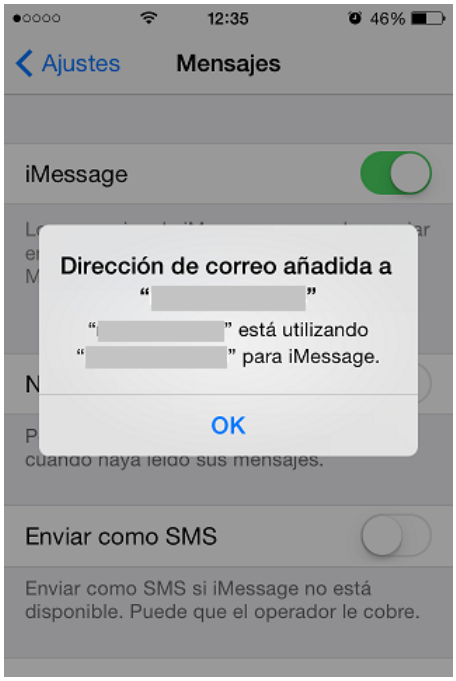
978. Al enviar un mensaje a un destinatario desde iMessage, si el destinatario también hace uso del servicio el botón de envío es de color azul y el mensaje se envía a través del servicio de datos TCP/IP (iCloud), mientras que si no dispone del servicio, el botón de envío es de color verde y el mensaje se envía a través de SMS (o MMS):

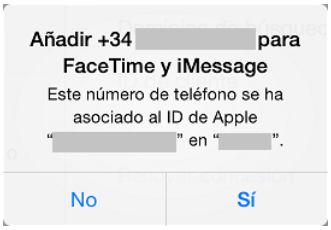
979. Para disponer del servicio iMessage es necesario asociar una cuenta de iCloud al dispositivo móvil. Las capacidades de sincronización de iCloud hacen que los mensajes intercambiados a través de iMessage aparezcan de manera sincronizada en todos los dispositivos móviles iOS asociados al mismo identificador de usuario (Apple ID o cuenta) en iCloud.

980. El servicio iMessage hace un uso extensivo de APNS empleando cifrado extremo a extremo entre los dispositivos Apple, empleando para ello dos pares de claves privadas y públicas, una para cifrado y otra para firma.

981. Las claves privadas son almacenadas en el *keychain* del dispositivo móvil. Las claves públicas son enviadas al servicio de directorio de Apple (IDS, *iMessage Directory Service*), dónde se asocian al identificador del usuario (número de teléfono o e-mail) y a la dirección del dispositivo móvil. El proceso se repite para cada nuevo dispositivo, número de teléfono o e-mail añadidos por el usuario, notificándose a través de un mensaje de alerta la existencia de un nuevo registro en todos los dispositivos previamente

registrados. En el caso de mensajes en grupo, el proceso se repite de nuevo para cada dispositivo móvil de cada destinatario del grupo:





982. Estas claves públicas son obtenidas a través del IDS por el dispositivo llamante para poderse comunicar con el destinatario, cifrando mediante AES de 128 bits individualmente la comunicación para cada uno de los dispositivos móviles del usuario destino. Los metadatos de la comunicación, como información de tiempos y enrutamiento, no son cifrados [Ref.- 13].

983. En el caso de enviarse mensajes de texto extensos u otros contenidos multimedia, estos son cifrados con una contraseña aleatoria y almacenados en iCloud, para posteriormente distribuir dicha contraseña y la ubicación del contenido hacia el dispositivo móvil destino de forma segura.

984. Debe tenerse en cuenta que dado que no existe ningún tipo de vinculación entre las claves públicas descritas y la identidad del usuario, salvo la existente en IDS, Apple tendría la capacidad de modificar dicha asociación en IDS y disponer de acceso a los contenidos de cualquier usuario [Ref.- 136]. Igualmente, la implementación de iMessage abre la posibilidad de sufrir diferentes ataques MitM una vez se confía en los certificados emitidos por una supuesta CA legítima.

985. Los dispositivos iOS, en caso de ser extraviados o robados, son vulnerables a que el nuevo usuario que tiene acceso a los mismos disponga de acceso a los mensajes de iMessage pasados y futuros del usuario víctima, ya que incluso tras el borrado remoto del dispositivo móvil, no se elimina la vinculación del servicio iMessage a través de la cuenta de iCloud (Apple ID) y el dispositivo móvil [Ref.- 98].

986. La vinculación del identificador de Apple del usuario se realiza internamente en el dispositivo móvil, y no es eliminada tras llevar a cabo el borrado remoto del dispositivo móvil, cambiar la contraseña asociada al identificador de Apple, o cambiar el terminal a un nuevo número de teléfono, por lo que su nuevo propietario puede tanto enviar como recibir mensajes, suplantando al usuario previo.

5.17.2 FACETIME

987. FaceTime es el servicio propietario de Apple para el establecimiento de llamadas de videoconferencia, disponible desde iOS 4.x en el iPhone 4. Posteriormente, desde la versión 7 de iOS, FaceTime también permite realizar sólo llamadas de audio a través de las redes de datos, tanto Wi-Fi como móviles (2/3/4G). Durante el transcurso de una llamada es posible cambiar de video a audio y viceversa.

988. Al igual que con iMessage, el establecimiento de llamadas mediante FaceTime hace un uso extensivo del servicio APNS, empleándose cifrado extremo a extremo entre los participantes.

989. FaceTime hace uso del protocolo ICE (*Internet Connectivity Establishment*) para establecer la conexión inicial entre los dispositivos, y de SIP (*Signaling Initiation Protocol*) para el establecimiento de la comunicación, verificación de los certificados y generación de una clave de sesión. Los contenidos de la llamada son intercambiados mediante SRTP (*Secure Real Time Protocol*) y cifrados con AES de 256 bits.

990. El servicio de FaceTime puede ser activado de manera similar a iMessages a través del menú "Ajustes - FaceTime", teniendo asignados identificadores similares a los descritos previamente para el servicio de iMessages:

5.17.3 SIRI

991. Siri es el sistema de reconocimiento de voz y lenguaje natural introducido por Apple en el iPhone 4S, con la versión 5 de iOS [Ref.- 56], que permite al usuario realizar multitud

de tareas mediante comandos de voz, como por ejemplo enviar mensajes SMS, realizar llamadas de voz, crear citas en el calendario, añadir recordatorios, etc, convirtiéndose en un asistente personal electrónico.

992. Originalmente, la funcionalidad de Siri no estaba disponible en el iPad [Ref.- 57] debido a su integración directa con el núcleo y servicios de iOS, y a la ausencia de ciertas capacidades hardware en el iPad en comparación con el iPhone (4S), necesarias para la funcionalidad de Siri, como por ejemplo las capacidades de telefonía móvil, o el GPS (no disponible en algunos modelos de iPad).

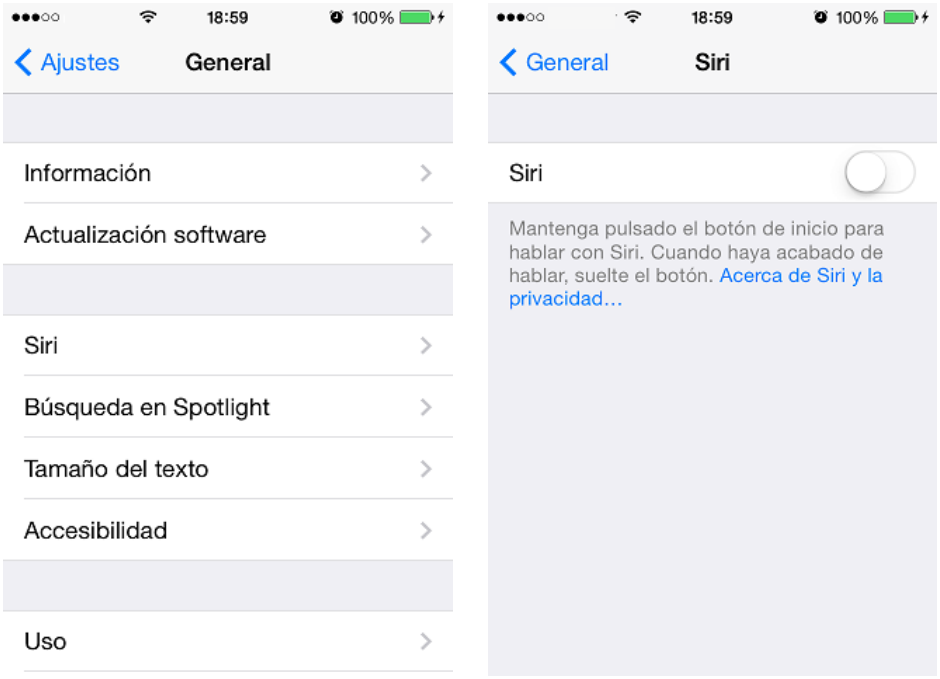
993. Desde la versión 6 de iOS, Apple proporcionó soporte para Siri también en el iPad, en concreto, a partir del iPad con pantalla retina (iPad de 3ª generación) o el iPad mini. Para más detalles ver la "Guía CCN-STIC-454 - Seguridad de dispositivos móviles: iPad (iOS 7.x)" [Ref.- 137].

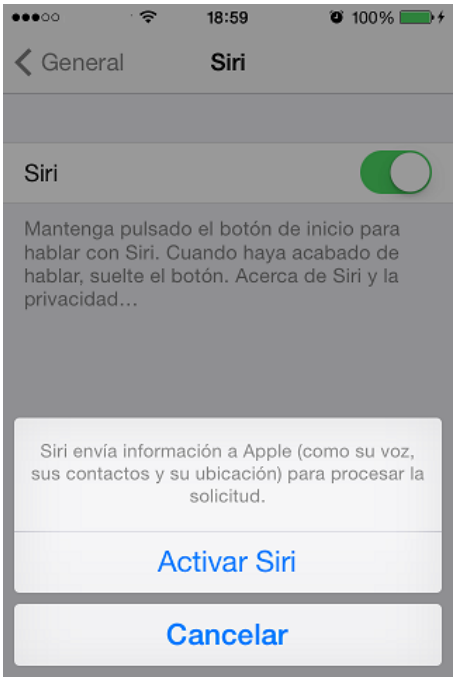
994. Siri procesa los comandos y mensajes de voz dictados por el usuario y los convierte en fonemas (unidades de sonido). Los fonemas son grabados por el dispositivo y enviados a los servidores de Apple de procesamiento de voz, y una vez procesados, estos servidores devuelven a Siri su respuesta en forma de comandos para el asistente (denominados "Ace" por el método HTTP personalizado empleado, "ACE"), con los que Siri llevará a cabo las acciones identificadas e invocará a la aplicación de iOS necesaria para cada acción: Teléfono, Reloj, Safari, Calendario, Música, etc.

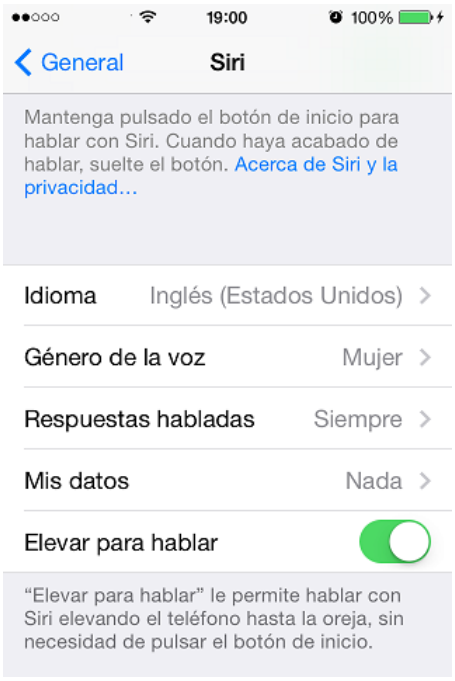
995. La comunicación entre Siri y los servidores de Apple puede llevarse a cabo tanto a través de redes Wi-Fi como de telefonía móvil (2/3/4G).

996. En la versión 5 de iOS Siri sólo disponía de soporte para los siguientes idiomas: inglés, francés, alemán y japonés. En la versión 6 de iOS se añadió soporte para español en Siri.

997. Siri es activado tras mantener pulsado el botón "Home" del iPhone, o el botón de llamada en dispositivos manos libres Bluetooth, habiéndose activado previamente su utilización desde el menú "Ajustes - General - Siri" (deshabilitado por defecto):







998. Debe tenerse en cuenta que (según indica Apple) con el objetivo de mejorar y personalizar el funcionamiento de Siri y sus capacidades de reconocimiento de voz para que entienda y reconozca mejor al usuario, el iPhone no sólo enviará a los servidores de Apple los fonemas extraídos de la información dictada por el usuario, sino también detalles de la lista de contactos del usuario, las relaciones (por ejemplo, de parentesco o amistad) de estos con el usuario, nombres de las listas de recordatorios, o detalles de su colección o librería de música, como por ejemplo los nombres de las canciones, artistas, listas de reproducción, etc.

999. Adicionalmente Siri puede hacer uso de los servicios de localización de iOS para emplear el servicio de recordatorios cuando el usuario llega a una ubicación concreta, o para proporcionar información detallada sobre ubicaciones cercanas a la localización actual del usuario.

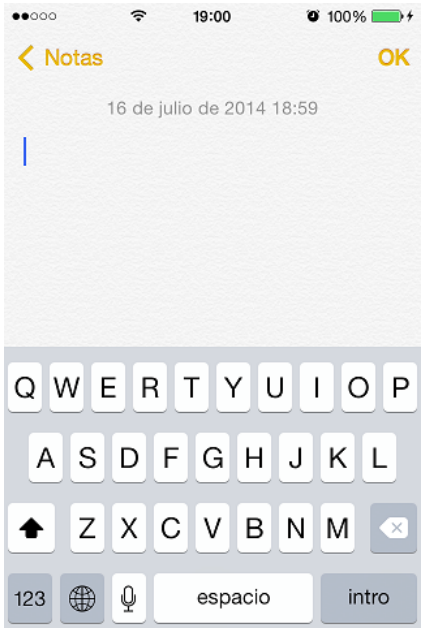
1000. La comunicación entre el dispositivo móvil y los servidores Siri de Apple se basa en unos identificadores aleatorios generados por el dispositivo móvil al activar Siri. Si se desactiva Siri y vuelve a ser activado de nuevo, estos identificadores aleatorios cambiarán.

1001. A través del menú "Ajustes - General - Siri", deshabilitando y habilitando Siri de nuevo, es posible (teóricamente) eliminar toda la información que Siri hubiera almacenado previamente sobre el usuario:

1002. Las comunicaciones entre el dispositivo móvil y Siri se llevan a cabo mediante HTTPS [Ref.- 13]. Al iniciarse una sesión con Siri, el dispositivo envía el nombre y apellidos y la localización aproximada del usuario, para que estos puedan ser empleados por Siri como parte de su funcionalidad. En caso de ser necesario, Siri puede solicitar posteriormente acceso a información de localización más precisa.

1003. Supuestamente, la información de la sesión es descartada tras 10 minutos de inactividad. Las grabaciones de la voz del usuario son almacenadas durante un periodo de 6 meses para que puedan ser utilizadas por el sistema de reconocimiento de voz de Siri.

1004. Al activar Siri se activan adicionalmente las capacidades de dictado de iOS en todas las aplicaciones que hacen uso del teclado, estando disponibles a través del icono del micrófono existente en el teclado:



1005. Debe analizarse detalladamente si se desea hacer uso de Siri considerando las implicaciones desde el punto de vista de la privacidad que tiene el transferir a Apple todos esos datos del usuario y sus actividades diarias.

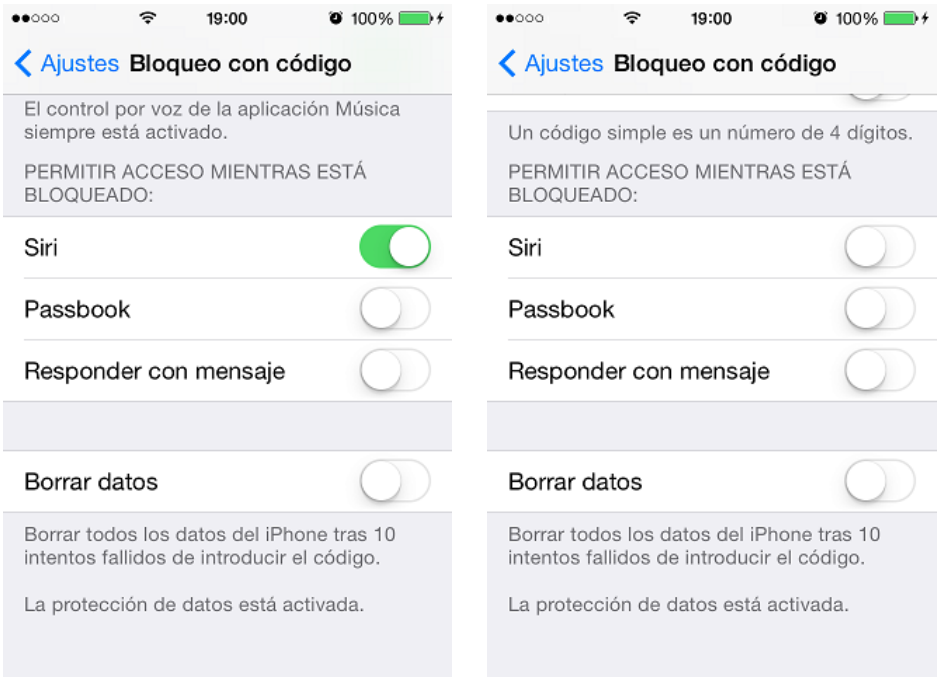
1006. Los detalles de cómo son procesados los comandos e instrucciones (como por ejemplo dictar e-mails o mensajes de texto) emitidos por los usuarios de dispositivos móviles iOS a través de Siri, y como estos datos (junto al resto de información de contactos y otros datos de usuario mencionados previamente) son almacenados y procesados se desconocen y no han sido publicados por Apple.

1007. En el caso de estar concienciado con la privacidad y confidencialidad de las actividades realizadas a través de iOS, se recomienda deshabilitar su uso individualmente. Adicionalmente, una organización podría filtrar el acceso a los servidores de Siri a través de las redes corporativas de la organización, lo que no evitaría que los usuarios siguieran haciendo uso del servicio a través de otras redes, como por ejemplo las redes de telefonía 2/3/4G.

1008. En el caso de desear deshabilitar Siri a nivel empresarial, se recomienda hacer uso de las capacidades de gestión de las soluciones MDM y emplear un perfil de configuración que determine que Siri no estará disponible en los terminales de los usuarios.

1009. Siri está disponible para su uso por defecto desde la pantalla de desbloqueo del dispositivo móvil, aunque es posible configurar a través de un perfil de configuración que sólo pueda ser utilizado una vez el terminal ha sido desbloqueado (opción recomendada desde el punto de vista de seguridad), o incluso desde el interfaz de usuario.

1010. Una vez Siri ha sido habilitado, desde el menú "Ajustes - Código", bajo la sección "Permitir acceso mientras está bloqueado:", es posible deshabilitar Siri a través de su botón de activación asociado:



Nota: El alcance de la presente guía no contempla la realización de un análisis de seguridad detallado de Siri y sus protocolos de comunicaciones.

5.18 COMUNICACIONES TCP/IP

1011. 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, VPNs y per-app VPNs.

1012. iOS 7 añade soporte de TCP multiruta, constituyéndose como el primer sistema operativo móvil con soporte para esta nueva extensión del protocolo TCP, que permite realizar conexiones a través de varias interfaces como LTE, Wi-Fi y Bluetooth al mismo tiempo. En la práctica, esta funcionalidad implica que si se está viendo un vídeo en YouTube a través de la conexión Wi-Fi de la oficina y se sale de su alcance, la reproducción no se detendrá sino que continuará a través de 3G/LTE sin incidencias.

5.18.1 ADAPTADORES DE RED

1013. Los adaptadores de red disponibles en el dispositivo móvil para las diferentes tecnologías de comunicaciones (principalmente, Wi-Fi y 2/3/4G) están disponibles en el menú correspondiente, como por ejemplo “Ajustes - Wi-Fi” o “Ajustes - Datos móviles”, mediante las opciones descritas en sus apartados asociados, “5.14. Comunicaciones Wi-Fi” y “5.16. Comunicaciones GSM (2G), UMTS (3G) y LTE (4G): voz y datos”.

1014. En el caso del interfaz Wi-Fi se dispone de ajustes avanzados para seleccionar si se utilizará una dirección IP estática o dinámica (DHCP), junto a la máscara de subred, router, los servidores DNS primario y secundario, los dominios de búsqueda y el uso de un proxy HTTP.

1015. La configuración de direccionamiento IP del interfaz Wi-Fi es independiente para cada una de las redes Wi-Fi configuradas.

1016. En el caso del interfaz móvil 2/3/4G no se dispone de opciones de configuración avanzadas.

1017. 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. Desde el menú “Ajustes – Wi-Fi”, se muestra la lista de redes Wi-Fi visibles y aquella a la que estamos conectados.

1018. Mediante una pulsación sobre el icono de información (i) asociado a la red Wi-Fi en la lista, se mostrará el menú que permite visualizar la configuración TCP/IP de la red obtenida por DHCP, desde la pestaña con el mismo nombre (ver apartado “5.14. Comunicaciones Wi-Fi”):

1019. iOS 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 2/3/4G (salvo a través del modo de prueba (o *Field Test*), ver apartado "5.16. Comunicaciones GSM (2G), UMTS (3G) y LTE (4G): voz y datos").

5.18.2 SEGURIDAD EN TCP/IP

1020. Con el objetivo de incrementar el nivel de seguridad de la pila TCP/IP empleada para las conexiones de datos en iOS, se recomienda evaluar su comportamiento y modificar ciertos parámetros de configuración que condicionan su funcionamiento.

1021. iOS no proporciona opciones de configuración avanzadas a través del interfaz de usuario que permitan modificar el comportamiento de la pila TCP/IP utilizada.

1022. 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 iOS).

Nota: No se ha identificado ningún mecanismo, ni opción de configuración, en iOS 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, por tanto las siguientes recomendaciones son teóricas y permiten únicamente analizar el comportamiento de la pila TCP/IP de iOS, pero no modificarlo.

1023. iOS no responde a otros tipos de mensajes ICMP de petición y respuesta, como por ejemplo *ICMP timestamp* o *ICMP address subnet mask*.

1024. La identificación del nombre del dispositivo móvil también se puede llevar a cabo a través del protocolo DHCP, ya que en las peticiones DHCP (*DHCP Discover y Request*)

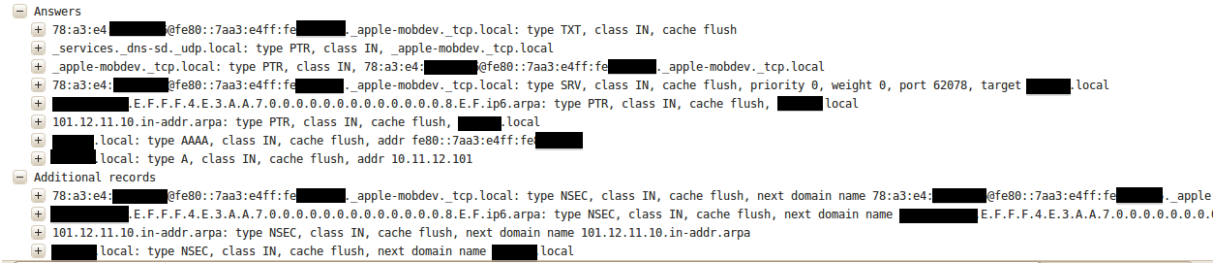
iOS incluye la opción 12 de DHCP, nombre de equipo, con el valor correspondiente al nombre del dispositivo móvil.

1025. Adicionalmente, el dispositivo móvil iOS envía periódicamente peticiones NTP (*Network Time Protocol*, 123/udp) para su sincronización horaria al servidor "time.apple.com" en Internet.

1026. Podría entenderse que la funcionalidad de cliente NTP de iOS está asociada a la opción "Ajuste automático" disponible desde el menú "Ajustes - General - Fecha y hora", sin embargo, incluso con esa opción deshabilitada se llevan a cabo las peticiones NTP. Aparentemente no se dispone de ninguna opción por parte del usuario para deshabilitar el uso de NTP una vez se dispone de conectividad de datos.

1027. Periódicamente iOS genera informes IGMP (v3) multicast (224.0.0.22) de pertenencia al grupo 224.0.0.251, correspondiente a mDMS (multicast DNS).

1028. Adicionalmente, iOS es fácilmente identificable mediante el tráfico mDNS (multicast DNS, 5353/udp) qué genera, incluyendo información asociada a "_apple-mobdev._tcp.local" (registros DNS de tipo TXT y SRV), consultas de tipo "QU" y "QM", así como respuestas de tipo PTR y desvelando tanto su dirección MAC como su dirección IPv6, IPv4 y el nombre del dispositivo móvil:



1029. Este tráfico mDNS es generado tanto mediante IPV4 (con destino 224.0.0.251) como mediante IPv6 (ver apartado "5.18.5. IPv6").

1030. Apple proporciona un listado actualizado de los diferentes puertos TCP/IP (TCP y UDP) empleados por los sistemas operativos y aplicaciones disponibles en sus productos. Aunque dicha información no hace referencia explícita a los dispositivos móviles iOS, es posible obtener los detalles de numerosos servicios y aplicaciones de iOS al ser comunes en los sistemas operativos de los ordenadores de Apple (OS X) [Ref.- 99] [Ref.- 118] [Ref.- 69].

5.18.3 ESCANEO DE PUERTOS TCP Y UDP

1031. A continuación se analiza el comportamiento de la pila TCP/IP de iOS 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.

1032. iOS responde con un paquete *TCP Reset* a las peticiones de conexión en puertos TCP cerrados.

1033. Por defecto, iOS sólo dispone de un puerto TCP abierto, es decir, los restantes 65.535 puertos TCP están cerrados. El puerto abierto, 62078/tcp, corresponde al servicio de sincronización de iOS con iTunes.

1034. iOS responde con paquetes ICMP de tipo 3 y código 3 (destino inalcanzable, puerto inalcanzable), limitados para evitar una congestión excesiva de la red, a las peticiones de conexión en puertos UDP cerrados.

1035. Por defecto, iOS únicamente dispone del puerto 5353/udp abierto, correspondiente a multicast DNS (mDNS o zeroconf).

1036. 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 iOS de forma sencilla.

1037. Este comportamiento y el perfil de puertos abiertos en iOS 7 es similar al existente en las primeras versiones de iOS, como por ejemplo iOS 1.x en el iPhone 2G original [Ref.- 89].

1038. Los dispositivos móviles iOS no disponen de un cortafuegos personal (o *firewall*) para bloquear las comunicaciones TCP/IP.

1039. 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.

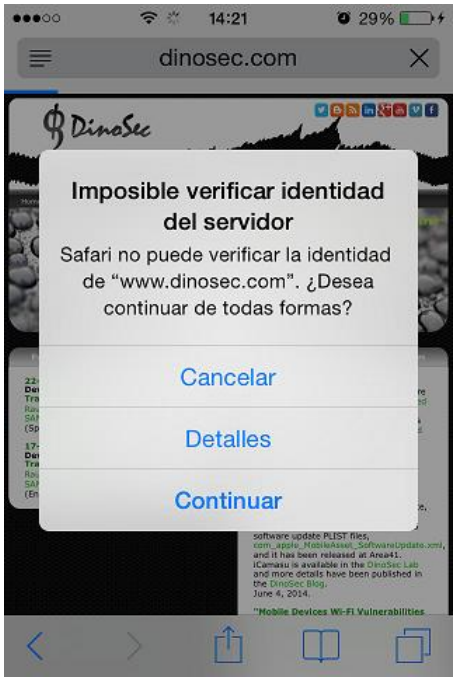
5.18.4 SSL/TLS

1040. iOS dispone de una implementación de los protocolos SSL, *Secure Socket Layer*, y TLS, *Transport Layer Security*, denominada *SecureTransport* bajo licencia APSL (*Apple Public Source License*), con soporte para SSL v3.0 y TLS v1.0, con SSL v2.0 deshabilitado por defecto (opción recomendada desde el punto de vista de seguridad), y con soporte adicional para DTLS v1.0, TLS v.1.1 y v1.2 desde iOS 5.0 [Ref.- 88].

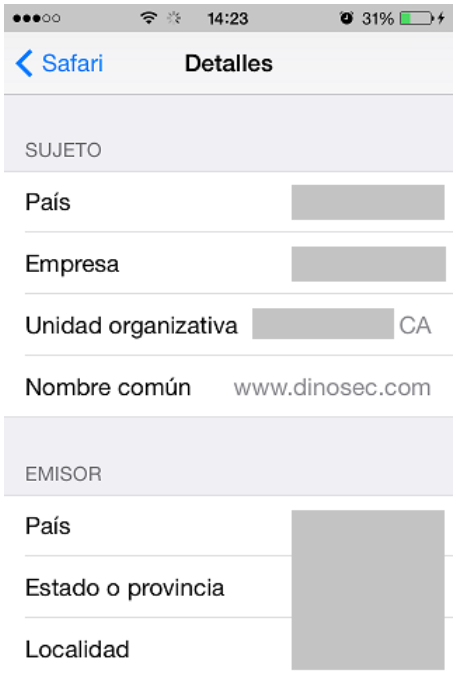
1041. Por tanto, iOS proporciona soporte para SSL versión 3 y para TLS en sus versiones 1.0, 1.1 y 1.2. Aplicaciones cliente como Safari, Calendario o Mail hacen uso de estos protocolos si el acceso al servidor correspondiente solicita su utilización.

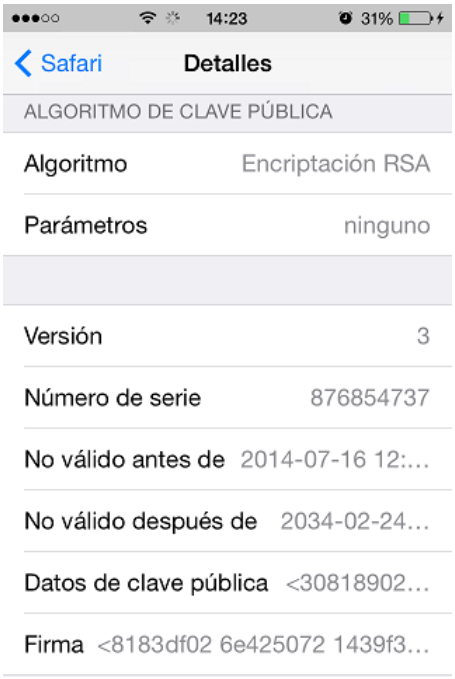
1042. Al acceder a un sitio web mediante HTTPS (y por tanto HTTP sobre SSL/TLS) utilizando el navegador web existente en iOS por defecto (aplicación “Safari” (Mobile)), el dispositivo móvil verificará el certificado digital asociado y su cadena de confianza, hasta la autoridad certificadora (CA, *Certificate Authority*) reconocida correspondiente.

1043. En caso de que no sea posible verificar la validez de un certificado, el navegador web de iOS 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 “Detalles”):

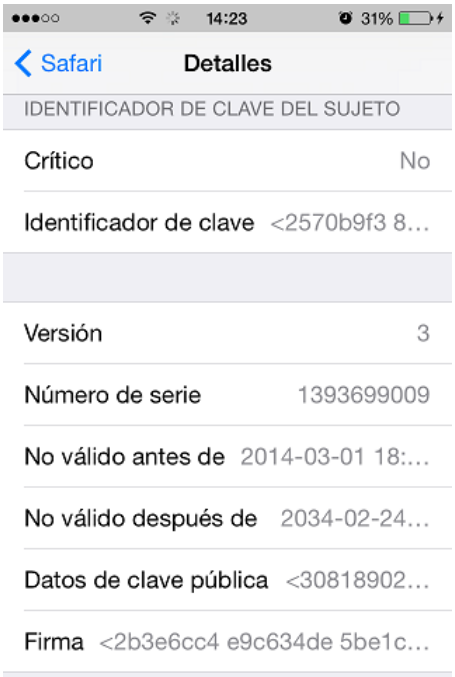


1044. Los detalles del certificado digital (disponibles a través del botón "Más detalles") incluyen elementos clave para su verificación al igual que en los navegadores web de los equipos de escritorio, como por ejemplo el número de serie del certificado, las huellas o *fingerprints* MD5 y SHA-1, los detalles de la cadena o jerarquía de confianza y de las autoridades certificadoras involucradas en su generación, o las extensiones del certificado:





1045. Sin embargo, las limitaciones del tamaño de pantalla de iOS y la ausencia de capacidades para visualizar el contenido completo de los campos del certificado, hacen que sólo sea posible ver el valor inicial del contenido de los diferentes campos, lo que no permite su correcta y completa verificación[10]:



1046. Por otro lado, iOS presenta una vulnerabilidad desde las versiones iniciales de este sistema operativo. Si se acepta un certificado digital, éste será válido de forma permanente, incluso si se cierra la instancia (o proceso) actual del navegador web Safari en iOS, e incluso tras reiniciar el dispositivo móvil.

1047. Mediante la eliminación de los datos únicamente del sitio web accedido (a través del menú "Ajustes - Safari - Avanzado - Datos de sitios web" y el botón "Edición"), o mediante el borrado del historial y de todas las cookies y datos de Safari (a través del menú "Ajustes - Safari" y los botones "Borrar historial" y "Borrar cookies y datos"), no se puede eliminar la validez del certificado aceptado por el usuario.

Nota: Durante el proceso de elaboración de la presente guía en 2011 Apple fue notificado de este comportamiento vulnerable, acrecentado por el hecho de no poder gestionar o verificar los certificados considerados como de confianza por el dispositivo móvil en cualquier momento (ver apartado "5.8.1. Certificados digitales y credenciales del usuario (Keychain)").

En el momento de elaboración de la presente guía no existe ningún procedimiento en la última versión de iOS disponible, 7.1.2, para eliminar un certificado digital aceptado por el usuario en el pasado.

1048. La acción de aceptar un certificado no verificado tiene el riesgo asociado de que el certificado digital aceptado, y desconocido, pertenezca a un potencial intruso que se

[10] La versión 8 de iOS permitirá finalmente acceder a todos los detalles de los certificados digitales X.509 desde el interfaz de usuario.

encuentra realizando un ataque de intercepción, MitM (*Man-in-the-Middle*), sobre el protocolo SSL/TLS y las comunicaciones (supuestamente) cifradas del usuario.

1049. Una vez se ha establecido una conexión de confianza mediante HTTPS con un sitio web, no se dispone de ninguna opción en el interfaz de usuario de Safari o iOS para poder ver el certificado digital asociado, lo que facilita la realización de ataques de suplantación sobre los certificados SSL/TLS e imposibilita que el usuario realice ninguna verificación.

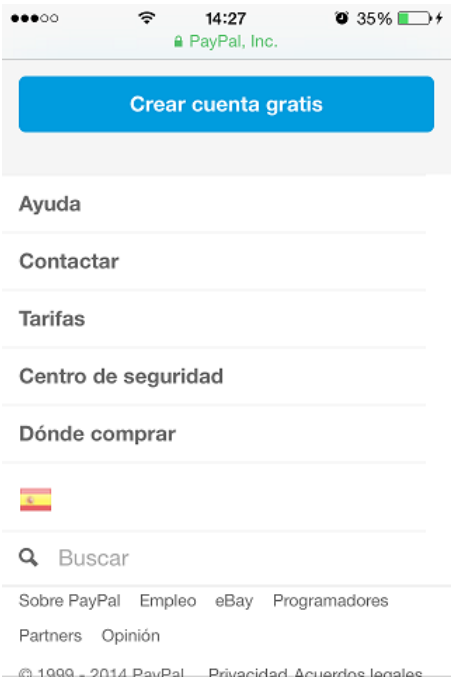
1050. Como se describe en el apartado “5.8.2. Certificados digitales raíz de iOS”, el repositorio de certificados raíz no está accesible a través del interfaz de usuario de iOS. Por tanto, el usuario confía plenamente en la lista autoridades certificadoras (o CAs, *Certificate Authorities*) que son consideradas como de confianza por Apple, y en las modificaciones de dicha lista realizadas por las actualizaciones asociadas a las nuevas versiones de iOS.

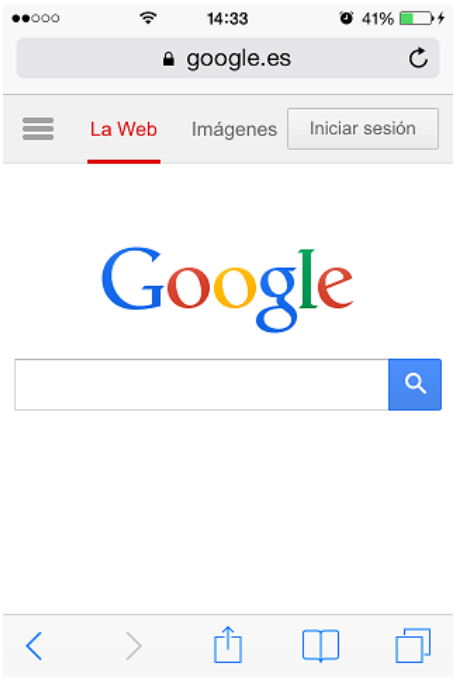
1051. Los perfiles de configuración de iOS disponen de un ajuste que posibilita configurar el dispositivo móvil para no permitir al usuario aceptar certificados digitales que no son de confianza ("*Allow user to accept untrusted certificates*").

1052. Se recomienda hacer uso de este ajuste de configuración para limitar los riesgos asociados a permitir comunicaciones con un servicio remoto que emplea un certificado digital que no es de confianza.

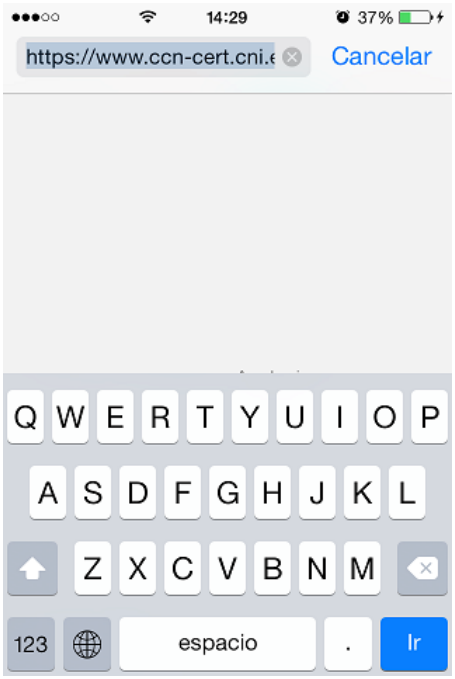
1053. Las carencias descritas asociadas al navegador web Safari en iOS, tanto al mostrarse mensajes de error incompletos, como al no disponer de todos los detalles necesarios para verificar un certificado digital una vez establecida la conexión mediante HTTPS, como en la gestión y eliminación de certificados aceptados y considerados de confianza en un momento dado, limitan significativamente la utilización que se puede hacer del dispositivo móvil para validar el acceso a sitios web mediante HTTPS.

1054. Por otro lado, iOS presenta notables limitaciones a la hora de gestionar y notificar al usuario sobre la existencia de diferentes escenarios relacionados con HTTPS y la gestión de certificados digitales. La verificación de certificados digitales con validación extendida sólo se muestra a través del color de las letras y el candado asociado al título de la página, que será de color verde si se trata de un certificado con validación extendida (ver imagen inferior izquierda) y negro o gris si no lo es (ver imagen inferior derecha):





1055. En el caso de páginas web que combinan tráfico HTTPS cifrado con tráfico HTTP no cifrado, el usuario podrá ver la indicación de "https://" en la barra de dirección de Safari, pero el candado asociado al uso de HTTPS no aparecerá en el título de la página, indicando que cierto tráfico es intercambiado de forma no cifrada (no siendo notificado el usuario mediante ningún otro mensaje de aviso):



1056. Las versiones 4.2.10 y 4.3.5 de iOS (CVE-2011-0228) introdujeron mejoras para solventar una vulnerabilidad en la verificación de la cadena de certificados (que afectaba por ejemplo a iOS 4.3.3), donde cualquier certificado válido podía ser utilizado para firmar nuevos certificados, actuando como un certificado raíz. La vulnerabilidad se debía a la ausencia de verificaciones en iOS de los campos de restricciones ("Basic

Constraints") de los certificados digitales X.509, que determinan si un certificado pertenece a una CA o no [Ref.- 87].

1057. Por otro lado, durante el año 2011 múltiples autoridades de certificación (*Certification Authorities*, CA) consideradas de confianza por parte de la industria, y por tanto de Apple y los dispositivos móviles iOS, fueron comprometidas en diferentes incidentes de seguridad, como por ejemplo DigiNotar o Comodo.

1058. La revocación de los certificados digitales de confianza de Comodo fue proporcionada en las actualizaciones correspondientes a las versiones 4.3.2 (http://support.apple.com/kb/HT4606) y 4.2.7 de iOS.

1059. La revocación de los certificados digitales de confianza de DigiNotar fue proporcionada en la actualización correspondiente a la versión 5.0 de iOS (http://support.apple.com/kb/HT4999).

1060. El proceso de actualizaciones de iOS para eliminar dichas CAs de confianza de los dispositivos móviles tuvo asociado un retraso considerable por parte de Apple (de varias semanas), periodo durante el cual todos los dispositivos móviles eran vulnerables a ataques de interceptación de tráfico cifrado hacia destinos que hicieran uso de certificados emitidos por dichas CAs.

1061. Adicionalmente, iOS no proporciona ninguna opción a través del interfaz de usuario para visualizar la lista de CAs de confianza aprobadas por Apple, ni revocar manualmente ninguna de ellas (la lista está disponible únicamente en los documentos oficiales de Apple: ver apartado "5.8.2. Certificados digitales raíz de iOS").

1062. Al igual que con las vulnerabilidades utilizadas por JailBreakMe 3 (descritas previamente), los usuarios que habían realizado el proceso de *jailbreak* disponían de la herramienta iSSLFix a través de Cydia para estar protegidos frente a estas dos vulnerabilidades (verificación correcta de certificados y eliminación de CAs comprometidas, a través de diferentes versiones de iSSLFix [Ref.- 101]).

1063. En febrero de 2014 Apple anunció una vulnerabilidad crítica en la implementación de SSL/TLS de los dispositivos móviles iOS (CVE-2014-1266), afectando tanto a las versiones 7.x como 6.x, y obligando a la publicación de una nueva actualización para ambas versiones, iOS 7.0.6 e iOS 6.1.6 (incluso para solucionar el problema en el iPhone 3GS, pese a llevar algún tiempo fuera de soporte) [Ref.- 169].

1064. La vulnerabilidad en la implementación *SecureTransport* de Apple se debía a la existencia de una sentencia "goto fail" de más en el código fuente de la librería, lo que le otorgó el nombre a esta vulnerabilidad (conocida como "goto fail"), y que provocaba que bajo ciertas circunstancias (al hacer uso de los algoritmos de cifrado DHE y ECDHE) no se llevara a cabo una validación correcta de los certificados digitales [Ref.- 168].

1065. Como resultado, un atacante podía llevar a cabo un ataque de MitM, interceptar el tráfico de los dispositivos móviles iOS (y OS X) víctima, y disponer de acceso a todo el tráfico cifrado sin que se generase ningún error de validación del certificado.

1066. Finalmente, iOS soporta la utilización de mecanismos de autentificación web basados en certificados digitales cliente a través del navegador web Safari [Ref.- 94], al igual que es posible hacer uso de certificados cliente para la conexión a redes Wi-Fi o VPN (ver apartado “5.8.1. Certificados digitales y credenciales del usuario”) o a Microsoft Exchange ActiveSync.

1067. Tras establecer la conexión HTTPS con el sitio web y éste solicitar un certificado al cliente para la autentificación, Safari solicita al usuario que seleccione el certificado cliente que desea usar de la lista de certificados disponibles.

5.18.5 IPV6

1068. El protocolo IP versión 6 (IPv6) está soportado y activado por defecto en iOS para las comunicaciones de datos mediante Wi-Fi (desde la versión 4 de iOS), pese a que el usuario no dispone de ninguna opción de configuración disponible relacionada con IPv6 o su configuración en el interfaz gráfico de iOS.

Nota: La disponibilidad de IPv6 para las comunicaciones de datos a través de la infraestructura de telefonía móvil en iOS es dependiente no sólo de la versión del sistema operativo, sino también del operador de telefonía móvil empleado.

1069. iOS hace uso de una pila TCP/IP dual, donde conviven tanto IPv4 como IPv6 simultáneamente, sin embargo la información de direccionamiento de IPv6 no está disponible a través del interfaz de usuario de iOS, siendo necesario hacer uso de aplicaciones de terceros (como por ejemplo "IPv6 Toolkit" o "Ip6config", disponibles en la App Store) para acceder a esa información.

1070. Durante el proceso de inicialización de conectividad de datos, el dispositivo móvil iOS genera peticiones IPv6 de solicitud de vecinos y de router mediante ICMPv6, empleando como dirección origen "fe80::**7aa3:e4**ff:fe**01:0203**" (*Link-Local Address*, FE80::/10, dónde su dirección MAC es 78:a3:e4:01:02:03), y añadiendo también su dirección MAC como dirección de enlace.

1071. La utilización de la dirección MAC en la dirección IPv6 global (EUI-64: "2001::/16") sin hacer uso de las *Privacy Extensions* de IPv6 (RFC 4941, antes RFC 3041) al emplear SLAAC (*stateless address autoconfiguration*) presenta problemas de seguridad y permite el seguimiento de los dispositivos móviles iOS en Internet.

1072. Esta vulnerabilidad fue solucionada con la actualización de seguridad de iOS 4.3 [Ref.- 86], mediante el uso de direcciones temporales aleatorias para las conexiones salientes. Adicionalmente, desde la versión 4.3.1 de iOS se dispone de soporte para DHCPv6 con estado y un servidor DHCPv6 (o sin estado (SLAAC) desde la versión 4 de iOS).

1073. Adicionalmente, el dispositivo móvil iOS envía periódicamente mensajes IPv6 de informes *multicast* ("Multicast Listener Report Message v2" - ICMPv6).

1074. Se recomienda deshabilitar la disponibilidad de IPv6 en iOS por completo, salvo que se vaya hacer uso de sus capacidades de comunicación, aunque esta opción no está disponible por defecto en la versión de iOS analizada.

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

5.18.6 VPN

1075. iOS proporciona soporte para las siguientes tecnologías VPN: Cisco *IP Security* (IPSec), *Point-to-Point Tunneling Protocol* (PPTP; 1723/tcp), y *Layer Two Tunneling Protocol* (L2TP; 1701/udp) en combinación con *Internet Protocol Security* (LT2P/IPSec;

500/udp). La opción recomendada desde el punto de vista de seguridad pasa por emplear IPSec o L2TP/IPsec.

1076. Adicionalmente, iOS permite la conexión a redes VPN SSL empresariales a través de aplicaciones cliente propietarias de Juniper, Cisco o F5 [Ref.- 102], y en concreto de dispositivos Juniper SA Series, Cisco ASA, y servidores F5 BIG-IP Edge Gateway SSL VPN. Las VPNs SSL permiten realizar la autentificación de los usuarios con todos los métodos detallados a continuación.

1077. iOS dispone de capacidades de autentificación del usuario mediante contraseña (MSCHAPv2 para L2TP/IPSec y PPTP), autentificación de dos factores (RSA SecurID o CRYPTOCard), y certificados digitales, soportando las extensiones .der, .cer, y .crt.

1078. La autentificación entre equipos en L2TP/IPSec se realiza únicamente mediante clave compartida (*shared secret*), opción disponible también en Cisco IPSec, (en ésta última) junto a la opción de emplear certificados digitales.

1079. En todos los casos (Cisco IPSec, L2TP/IPSec y PPTP), la autentificación del usuario puede realizarse mediante contraseña o autentificación de dos factores.

1080. iOS proporciona capacidades VPN en modo *split tunneling* para separar el tráfico entre/desde redes públicas y privadas, en función de cómo se defina la política de seguridad asociada.

1081. En el caso de VPNs basadas en autentificación cliente mediante certificados, iOS soporta VPN *On Demand*, solución en la que se establecerá automáticamente la VPN al acceder a ciertos dominios o direcciones IP preconfiguradas.

1082. Las opciones de configuración disponibles en *On Demand* permiten establecer una VPN para cualquier dirección de un dominio, nunca establecer la VPN para ciertos dominios (aunque en el caso de estar previamente establecida se hará uso de ella), o bajo demanda, estableciéndose la VPN para ciertas direcciones de un dominio si la resolución de nombres falla.

1083. Esta funcionalidad puede ser empleada no sólo por aplicaciones de sistema existentes por defecto en iOS, como por ejemplo Mail o Mobile Safari, sino también por aplicaciones de terceros que hacen uso de las librerías (API) de comunicaciones estándar, *CFStream* y *CFSocketStream* (frente al uso de *sockets raw*).

1084. La opción que permite emplear un certificado para la autentificación de IPSec/L2TP entre equipos, 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), no está disponible en iOS. Únicamente está disponible para VPNs Cisco IPSec.

1085. El proceso para añadir certificados digitales raíz específicos para su utilización en conexiones Wi-Fi o VPN se detalla en el apartado “5.14.3. Recomendaciones de seguridad para la conexión a redes Wi-Fi”.

1086. Finalmente, iOS permite configurar las opciones de proxy para conectarse a través de redes VPN de forma manual, o mediante los protocolos PAC y WPAD.

1087. La configuración de redes VPN en iOS puede realizarse de forma manual o a través de los perfiles de configuración.

1088. Desde el menú “Ajustes - General - VPN” es posible añadir una nueva red VPN a través del botón “Añadir configuración VPN...”, así como acceder a las configuraciones de redes VPN existentes y activar su utilización mediante el botón "VPN" superior:

1089. En iOS 7 el uso de una red VPN también puede activarse directamente, una vez configurada, desde "Ajustes - VPN".

1090. La red VPN seleccionada (indicado mediante un *tick* a la izquierda del nombre) será empleada por defecto al activar el servicio de VPN de iOS.

1091. A través del icono de información (i) disponible a la derecha de cada red VPN, es posible acceder y modificar los ajustes de configuración de la red.

1092. Todas las redes VPN, basadas en PPTP, L2TP y L2TP/IPSec, requieren disponer de la descripción o nombre de la red VPN, del nombre o dirección IP del servidor VPN, y de la cuenta de usuario que permite autentificarse en la VPN (ver imágenes posteriores).

1093. En el caso de redes PPTP, iOS permite deshabilitar el cifrado (habilitado por defecto a la opción automática), opción desaconsejada desde el punto de vista de seguridad:

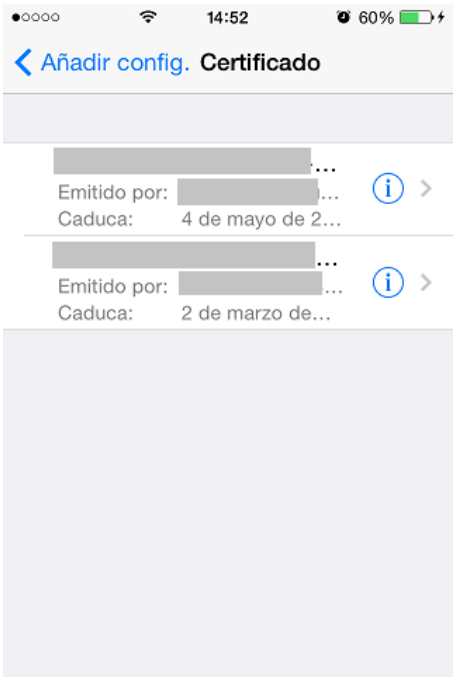
1094. En el caso de redes L2TP/IPsec (reflejadas como "L2TP"), iOS permite configurar el secreto L2TP o clave precompartida para el acceso a la red, opción que permite autentificar el propio túnel L2TP mediante un secreto compartido entre el cliente y el servidor (puede ser necesario en función de la configuración del servidor VPN):

1095. Como se puede ver en la imagen superior, la configuración tanto para PPTP como para L2TP/IPSec, permite especificar si se hará uso de autentificación mediante contraseña o a través de dos factores mediante RSA SecurID (deshabilitado por defecto), así como definir si se enviará todo el tráfico a través de la red VPN (en lugar de hacer uso de *split tunneling*), mediante la opción "Enviar todo el tráfico" (habilitada por defecto), configuración recomendada desde el punto de vista de seguridad.

1096. Una vez establecida la conexión con la red VPN, en iOS el usuario (junto al servidor de VPN) es quién puede restringir las comunicaciones para que todo el tráfico sea cursado a través de la VPN hasta que ésta sea desconectada, es decir, no usando *split tunneling u horizon* (conexiones simultáneas directas hacia Internet y a través de la VPN).

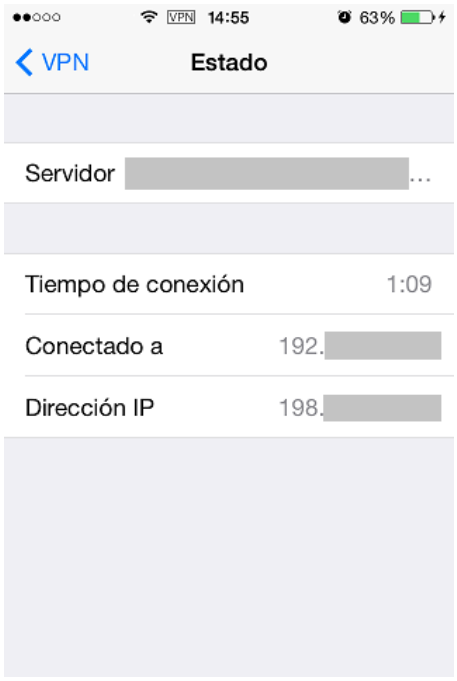
1097. En el caso de redes Cisco IPsec, iOS permite establecer el secreto o clave precompartida para el acceso a la red, el nombre de grupo IPSec, así como si se hará uso de un certificado digital para la autentificación del dispositivo móvil:

1098. En caso de emplear un certificado digital (ver imagen superior derecha), las opciones de "Nombre grupo" y "Secreto" serán reemplazadas por la opción "Certificado", que permite seleccionar el certificado digital cliente de la lista de certificados disponibles (ver apartado “5.8.1. Certificados digitales y credenciales del usuario”) importados previamente a través de los perfiles de configuración:



1099. El certificado digital necesario para Cisco IPSec es de tipo personal, y permitirá autentificar al dispositivo móvil y a 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 o concentrador de VPN.

1100. Una vez configurada la red VPN, es posible conectarse a la misma seleccionándola de la lista de redes disponibles desde la pantalla “Ajustes - General - VPN”. iOS reflejará el tiempo de duración de la conexión actual e información sobre el direccionamiento IP a través de la opción "Estado", así como la existencia de la conexión a través del icono VPN en la barra superior de estado:



1101. Las contraseñas de las redes VPN pueden quedar almacenadas por defecto en los ajustes de configuración de la red, no siendo necesario por parte del usuario introducir las credenciales de acceso a la VPN, por ejemplo el nombre de usuario y la contraseña, para establecer la conexión con la red VPN seleccionada. Desde el punto de vista de seguridad no se recomienda permitir este comportamiento.

1102. La única opción que proporciona iOS a través del interfaz de usuario para no almacenar la contraseña, de forma que cada vez que se establezca una conexión con una red VPN sea necesario proporcionarla, pasa por dejar en blanco dicho campo en la configuración de la red VPN. En ese caso, el campo quedará marcado como "Preguntar cada vez" (en color gris), frente a otros campos que son obligatorios (indicado pro el texto "Obligatorio").

1103. En el caso de introducir la contraseña en la configuración de la red VPN, si un potencial atacante dispusiera de acceso no autorizado al dispositivo móvil podría establecer conexiones con la red VPN automáticamente, salvo que la red VPN haga uso de autentificación de dos factores, para lo que sería necesario adicionalmente disponer del token de generación de contraseñas de un sólo uso asociado.

1104. La configuración de proxy, con las opciones "No", "Manual" (servidor, puerto y autentificación - usuario y contraseña) o "Automát." (URL) está disponible en la parte inferior de los ajustes de configuración de cada red VPN.

1105. Los dispositivos móviles iOS no disponen de un mecanismo por defecto para disponer de conectividad únicamente a través de redes VPN, no permitiendo ningún tráfico en cualquier otro caso, estando en manos del usuario o de las capacidades *On Demand* (sólo para ciertas direcciones o dominios) el establecimiento de la conexión VPN, además de las posibles desconexiones de la VPN cuando el dispositivo móvil es suspendido por falta de actividad.

5.18.7 VPN POR APP (PER-APP VPN)

1106. iOS 7 incorpora la posibilidad de establecer una conexión VPN por app en lugar de disponer de una VPN global para todo el sistema, de forma que cuando la app gestionada es iniciada, se establece automáticamente una conexión VPN hacia la organización para la transmisión de los datos corporativos, contribuyendo así a la separación y protección de la transmisión de datos corporativos y personales.

1107. Las nuevas extensiones de gestión de dispositivos móviles (MDM) de iOS 7 permiten la configuración y utilización de manera transparente al usuario de VPNs (o redes privadas virtuales) para aplicaciones móviles (apps) específicas, denominadas "per-app VPN" por Apple.

1108. Las per-app VPNs son independientes y/o complementarias a la configuración de VPNs genéricas para todas las comunicaciones del dispositivo móvil.

1109. Estas capacidades permiten proteger los datos intercambiados por una app específica a través de la red mediante las capacidades de autentificación y cifrado proporcionadas por las VPNs, de forma que todo el tráfico enviado y recibido por la app haga uso de la VPN.

1110. iOS 7 permite la definición de diferentes perfiles de VPN, únicamente a través de una solución MDM y no directamente en los dispositivos móviles, de forma que diferentes apps, tanto de sistema como por ejemplo Mobile Safari (pese a no ser una app gestionada), como de terceros como por ejemplo apps corporativas, puedan emplear VPNs diferentes.

1111. Una vez se ha establecido una VPN específica para una app, otras apps no pueden enviar su tráfico a través de dicha VPN.

1112. Estas capacidades de per-app VPN complementan las capacidades de VPN *On Demand* ya existentes en versiones previas de iOS. Un perfil de configuración de iOS definido en la solución MDM puede por tanto disponer de reglas para la activación de una VPN global al dispositivo bajo demanda (VPN *On Demand*) cuando se accede a ciertos dominios a proteger (con relaciones entre dominios objetivos y los perfiles VPN a emplear), así como una serie de reglas para la activación de una per-app VPN específica para una app cuando ésta es arrancada (con relaciones entre las apps gestionadas y los perfiles per-app VPN a emplear) [Ref.- 167].

1113. Desde el punto de vista de las apps, no es necesario llevar a cabo desarrollos específicos para que hagan uso de la funcionalidad de per-app VPN, aunque se recomienda hacer uso de las librerías (API) genéricas de comunicaciones, *NSURLConnection* y *NSURLSession*.

5.18.8 NOTIFICACIONES *PUSH*

1114. Apple proporciona el servicio APNS, *Apple Push Notification Service*, para el envío de notificaciones, como por ejemplo la actualización de la etiqueta asociada a un icono de una aplicación, la reproducción de un sonido, o la generación de un mensaje de texto, para las aplicaciones y servicios de los dispositivos móviles iOS.

1115. Las notificaciones *push*, introducidas en iOS 3.x, permiten el envío de notificaciones y mensajes a aplicaciones que no están ejecutando actualmente. Para ello se emplea una nueva API y servicios web proporcionados por servidores web remotos de Apple y del

desarrollador de la aplicación. La autentificación mutua entre el dispositivo móvil y el servicio *push* se realiza mediante certificados digitales [Ref.- 26].

1116. Las aplicaciones que emplean notificaciones, y que no hacen uso de capacidades locales del dispositivo, sino que son recibidas desde los servidores de Apple y/o de la aplicación, denominadas notificaciones *push*, requieren disponer de conectividad de datos en el dispositivo móvil y acceso no filtrado hacia el puerto 5223/tcp de los servidores de *push* de Apple ("NN-courier.push.apple.com", donde "NN" es un número de uno o dos dígitos).

1117. La comunicación entre el dispositivo móvil y los servidores de Apple en el puerto 5223/tcp emplea un protocolo propietario basado en XMPP (ej. Jabber) y cifrado mediante SSL/TLS y un certificado emitido por Entrust para "courier.push.apple.com", pero en la negociación inicial es posible identificar que el cliente corresponde a un dispositivo Apple iPhone (ver el ejemplo inferior; con el mismo texto independientemente de la versión de iOS empleada, ej. 5.x ó 7.x):

```
.
Apple Inc.1.0...U....Apple iPhone1.0...U....Apple iPhone Device CA0..
```

1118. La conexión entre el dispositivo móvil iOS y los servidores push de Apple emplea autentificación mutua, con certificados cliente y servidor, y un protocolo de comunicaciones que ha evolucionado desde el empleado en iOS 4.x [Ref.- 103].

1119. A través del servicio *push*, el dispositivo móvil iOS se suscribe a los temas específicos asociados a las aplicaciones que hacen uso de este servicio. Los servidores propios de cada aplicación actúan de servidor o proveedor de notificaciones, conectándose a los servidores gateway de Apple disponibles para este servicio, "gateway.push.apple.com".

1120. La conexión entre el servidor *push* de la aplicación y los servidores gateway de Apple emplea SSL/TLS con autentificación basada en certificados a través del puerto 2195/tcp y el puerto 2196/tcp para el servicio de *feedback* [Ref.- 125]. Las notificaciones son enviadas en formato JSON dentro de un protocolo binario propietario.

1121. Este tipo de aplicaciones y sus notificaciones asociadas generan tráfico de datos desde el dispositivo móvil a intervalos periódicos, al igual que otras aplicaciones que solicitan datos de forma frecuente a través de las conexiones de datos (Wi-Fi o de telefonía móvil), como por ejemplo "Mail".

1122. Las aplicaciones con capacidades *push* incluyen el cliente de correo o "Mail", las comunicaciones con los servidores MDM, y aplicaciones iOS que pueden ejecutar de fondo, como clientes de voz sobre IP (VoIP) o aplicaciones que hacen uso de la localización.

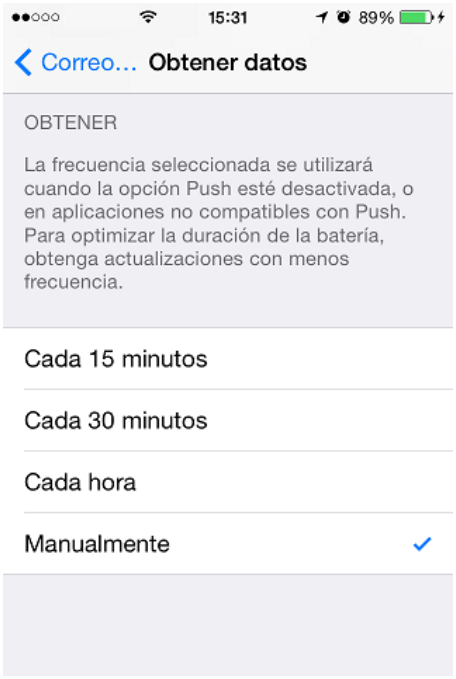
1123. Si se desea deshabilitar por completo las comunicaciones de datos se deben desactivar los interfaces de red, tanto Wi-Fi como de comunicaciones de datos móviles (2/3/4G).

1124. Por un lado, desde el menú "Ajustes - Centro de notificaciones" es posible deshabilitar para cada app individualmente los mensajes de notificaciones seleccionando la opción "Nada" para el tipo de alerta (y adicionalmente deshabilitando el resto de opciones de notificación; ver apartado "5.6.2. Centro de Notificaciones").

1125. Esta configuración debe aplicarse de forma individual para cada aplicación que hace uso de notificaciones *push*, asociadas a las actividades mientras las aplicaciones no están abiertas o en uso. Una vez una aplicación está en uso, ésta puede establecer conexiones de datos en función de sus necesidades [Ref.- 76].

1126. Por otro lado, desde el menú "Ajustes - General - Actualización en segundo plano" es posible permitir que las apps usen los servicios de localización o actualicen sus contenidos en segundo plano, cuando no son la aplicación activa actualmente (ver apartado "5.18.9. Actualizaciones en segundo plano").

1127. Adicionalmente, desde el menú "Ajustes - Correo, contactos, calend.", mediante la opción "Obtener datos" es posible restringir las comunicaciones de datos periódicas deshabilitando la opción "Push" (habilitada por defecto) y fijando la frecuencia de obtención de datos a "Manualmente" (de forma que no se obtengan datos con ninguna periodicidad prefijada):



1128. Este ajuste es global y afecta al correo, contactos y calendarios con soporte para notificaciones push (si la opción "Push" está habilitada) o sin soporte (si la opción "Push" no está habilitada), definiéndose la periodicidad de manera global.

1129. La opción "Manualmente" permite que la aplicación obtenga datos únicamente cuando esté en uso.

1130. A través de las entradas existentes en la parte superior es posible determinar la política de obtención de datos de forma individual para cada cuenta de correo disponible o iCloud, pudiendo elegir entre las opciones "Push" (únicamente si la cuenta dispone de estas capacidades), "Obtener" (para hacer uso de la frecuencia de obtención de datos definida de forma global previamente: cada 15 minutos, 30 minutos o cada hora) o "Manual" (para obtener datos sólo cuando la aplicación esté en uso"):

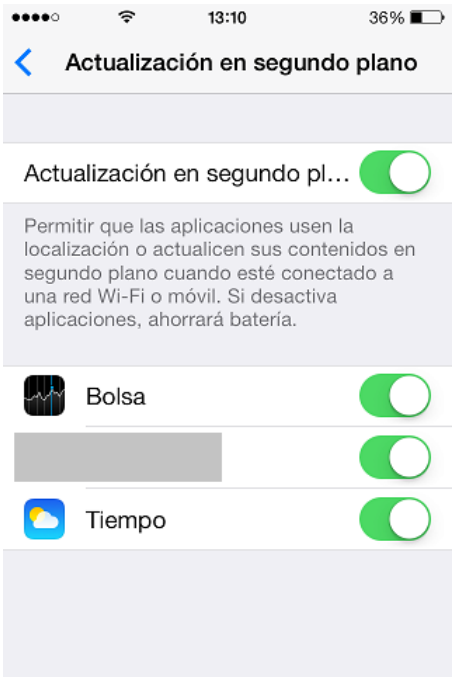
1131. Desde el punto de vista de seguridad se recomienda establecer una política general restrictiva de obtención de datos, y definir posteriormente configuraciones personalizadas en función de las aplicaciones y cuentas disponibles.

5.18.9 ACTUALIZACIONES EN SEGUNDO PLANO

1132. Las nuevas capacidades de multitarea introducidas en iOS 7 permiten adicionalmente a las apps actualizar sus datos en segundo plano, es decir, cuando están en ejecución pero no son la app activa.

1133. Las actualizaciones de datos se llevan a cabo por iOS teniendo en cuenta múltiples factores, como por ejemplo el tipo de conexión de red, la hora del día, y las notificaciones *push*, y con el objetivo de minimizar el impacto en el consumo de la batería.

1134. A través del menú "Ajustes - General" y de la opción "Actualización en segundo plano" se dispone de capacidades para activar o desactivar por completo esta funcionalidad, o para hacerlo de forma granular por aplicación:



5.19 CUENTA DE USUARIO DE APPLE

1135. Para hacer uso de los servicios y las aplicaciones de Apple en iOS (iCloud, App Store, iTunes, etc), como por ejemplo poder descargar aplicaciones de App Store, hacer copias de seguridad de los datos y la configuración en los servidores iCloud de Apple, y poder hacer uso de otros servicios de Apple desde el dispositivo móvil iOS, es necesario disponer de una cuenta de usuario o identificador de Apple, denominado Apple ID.

1136. Este Apple ID, habitualmente asociado a una tarjeta de crédito para realizar las transacciones de los servicios de pago, es empleado adicionalmente durante el proceso de activación y de configuración inicial del dispositivo móvil.

1137. El Apple ID de un usuario no tiene porqué estar asociado a una tarjeta de crédito si no se requiere llevar a cabo compras o pagos a través del dispositivo móvil iOS, como por ejemplo únicamente para la adquisición de aplicaciones móviles gratuitas [Ref.- 115].

1138. iOS ofrece la opción al usuario de iniciar sesión con un Apple ID existente, o de crear un nuevo Apple ID de manera gratuita. Mediante la opción "Omitir este paso" es posible continuar con el proceso de activación del dispositivo móvil sin proporcionar un Apple ID válido en este momento (ejemplo de iOS 5.x):

1139. En caso de no vincular el dispositivo móvil con un Apple ID durante el proceso de configuración inicial, iOS notifica al usuario que no podrá hacer uso de la App Store, iTunes Store, iCloud y otros servicios (ejemplo de iOS 5.x):

1140. Apple proporciona información y detalles del Apple ID y de todas las tareas de gestión asociadas (creación de un identificador, modificación de los datos asociados, restauración de la contraseña, etc) a través de la web "My Apple ID" ("Mi ID de Apple") [Ref.- 104].

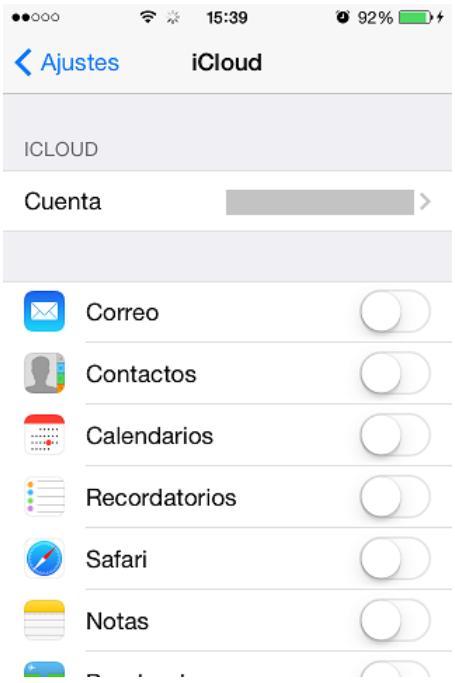
1141. El Apple ID puede emplearse adicionalmente para el acceso a servicios de Apple no relacionados directamente con los dispositivos móviles, como por ejemplo Apple Retail Stores o Mac App Store. Entre otros, los siguientes servicios de Apple están disponibles para los usuarios de iOS: iCloud, iTunes, iMessage, FaceTime, (iOS) App Store, etc.

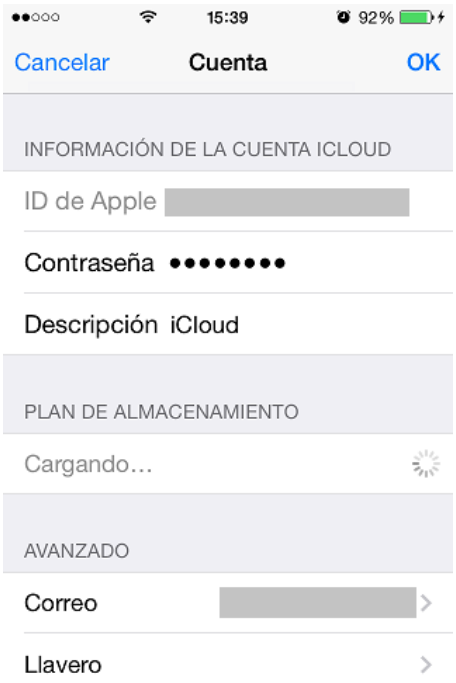
5.19.1 ASIGNACIÓN DE UNA CUENTA DE APPLE AL DISPOSITIVO MÓVIL

1142. La configuración de una cuenta de Apple (o Apple ID) ya existente y su vinculación al dispositivo móvil iOS, o la creación de una nueva cuenta, puede llevarse a cabo desde diferentes menús en función de los servicios que se desean asociar a dicho Apple ID.

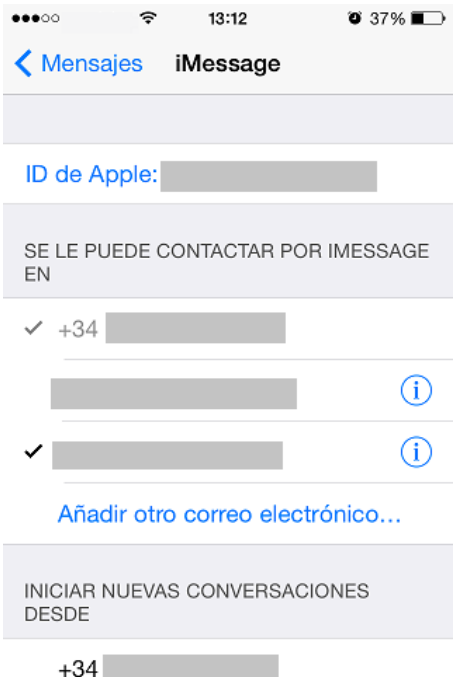
1143. Los diferentes menús de ajustes de la configuración permiten llevar a cabo la creación de una nueva cuenta si no se dispone de un Apple ID.

1144. Desde el menú "Ajustes - iCloud - Cuenta" es posible establecer el Apple ID para los servicios de iCloud. La contraseña es almacenada por defecto junto al Apple ID para hacer uso de estos servicios de forma periódica y automática:





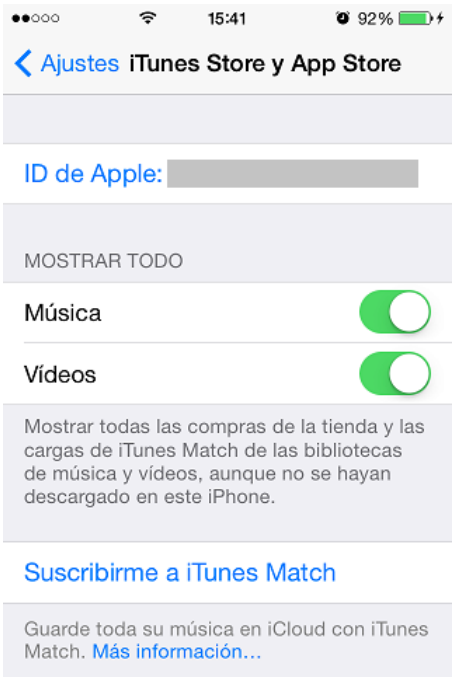
1145. Desde el menú "Ajustes - FaceTime" es posible establecer el Apple ID para los servicios de videoconferencia de FaceTime (ver imagen inferior izquierda). La contraseña es almacenada por defecto junto al Apple ID para hacer uso de estos servicios de forma periódica y automática:

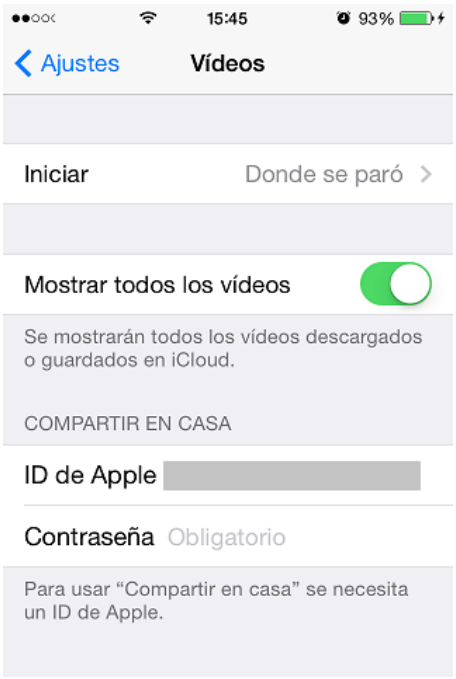


Nota: El alcance de la presente guía no contempla el análisis detallado del servicio y protocolos empleados por FaceTime [Ref.- 126].

1146. Desde el menú “Ajustes - Mensajes - Enviar y recibir” es posible establecer el Apple ID para los servicios de iMessage (ver imagen superior derecha). La contraseña es almacenada por defecto junto al Apple ID para hacer uso de estos servicios de forma periódica y automática.

1147. Desde el menú “Ajustes - iTunes Store y App Store” es posible establecer y gestionar el Apple ID para los servicios de la App Store (ver imagen inferior izquierda). La adquisición de nuevas aplicaciones, o su actualización, a través de la App Store siempre solicita al usuario introducir la contraseña asociada al Apple ID vinculado a la aplicación:





1148. Desde el menú "Ajustes - Videos - Compartir en casa" es posible establecer el Apple ID para los servicios de compartición de contenido multimedia (ver imagen superior derecha), que permiten acceder a la biblioteca de iTunes de un ordenador desde un dispositivo móvil iOS de forma remota.

1149. La mayoría de servicios y aplicaciones que hacen uso de un Apple ID almacenan y hacen uso automáticamente de la contraseña asociada, excepto App Store (al requerir autorización a la hora de realizar nuevos pagos), opción desaconsejada desde el punto de vista de seguridad, ya que el acceso no autorizado al dispositivo móvil iOS permitiría adicionalmente el acceso a todos los servicios asociados al Apple ID (ver siguiente apartado).

5.19.2 GESTIÓN DE LAS CREDENCIALES DE LAS CUENTAS DE USUARIO

1150. Desde el punto de vista de seguridad, se recomienda no almacenar la contraseña de la cuenta del usuario de Apple, o Apple ID, 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 Apple del usuario, junto a todos sus servicios asociados.

1151. Sin embargo, no se ha identificado ninguna opción general en los dispositivos móviles iOS para forzar este comportamiento y evitar el almacenamiento de la contraseña, dependiendo el comportamiento de cada uno de los servicios y aplicaciones que hacen uso del Apple ID (tal como se ha detallado previamente).

1152. Es decir, la contraseña asociada a la cuenta del usuario puede quedar almacenada automáticamente en el dispositivo móvil para ciertos servicios, no siendo posible evitar su almacenamiento. Como resultado, tras encender el dispositivo se dispone de acceso completo y directo a la cuenta del usuario y a todos los servicios asociados.

1153. 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 Twitter o Facebook, dónde la contraseña queda almacenada en el

dispositivo no siendo posible evitar que no sea así (tal como indica el texto "Obligatorio"), ya que es obligatorio proporcionar un valor para la contraseña y éste valor es verificado antes de abandonar la pantalla de configuración de la cuenta:

1154. La alternativa principal identificada para evitar esta asociación entre cuenta/contraseña y dispositivo es eliminar la cuenta asociada. Sin embargo, esta práctica no puede ser empleada en el proceso de utilización habitual del dispositivo móvil y sus servicios asociados.

1155. La pantalla de detalles de una cuenta ("Ajustes - iCloud") permite eliminarla del dispositivo móvil mediante el botón “Eliminar cuenta” disponible en color rojo en la parte inferior.

1156. iOS no proporciona capacidades para modificar la contraseña de la cuenta principal de Apple asociada al dispositivo móvil e iCloud, ni para modificar las contraseñas de otros servicios disponibles en iOS.

1157. Únicamente desde “Ajustes - iTunes Store y App Store”, seleccionando el Apple ID, se puede obtener acceso al servicio iForgot, disponible cuando no se recuerda la contraseña asociada a un Apple ID.

1158. Las siguientes recomendaciones aplican tanto a la cuenta principal de Apple (Apple ID) para iCloud 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 a dichos servicios.

1159. Para invalidar la contraseña almacenada para la cuenta principal de Apple asociada al dispositivo móvil e iCloud, 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 iOS.

1160. Tras acceder a Apple ("My Apple ID": https://appleid.apple.com [Ref.- 104]) y modificar la contraseña de la cuenta (Apple ID), la próxima vez que se acceda desde el dispositivo móvil a alguna de las aplicaciones que hacen uso de los servicios de Apple

(ya sea de forma manual, o de forma automática, por ejemplo, iMessage o FaceTime), y por tanto, de dicha cuenta, iOS generará una notificación de error y solicitará al usuario la (nueva) contraseña asociada al Apple ID.

1161. Como resultado del cambio de contraseña, algunos servicios (como por ejemplo iMessage) eliminará automáticamente el Apple ID previo de los ajustes de configuración de iOS, siendo necesario llevar a cabo de nuevo el proceso de activación de la cuenta en el servicio (ver apartado "**¡Error! No se encuentra el origen de la referencia.**. **¡Error! No se encuentra el origen de la referencia.**").

1162. 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, junto a las acciones detalladas en el apartado "5.5. Restricciones en el proceso de activación".

1163. Por otro lado, debido a que iOS está diseñado para que múltiples de los servicios existentes trabajen con un Apple ID que está siempre activo, tampoco proporciona capacidades para desconectarse (o cerrar la sesión actual) de la cuenta de Apple, 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.

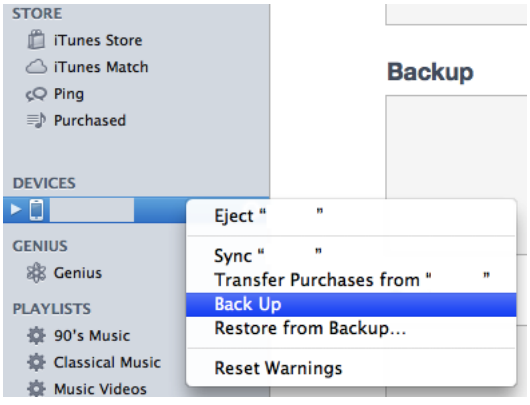
1164. El método disponible para forzar esta desconexión, sin tener que eliminar la cuenta del dispositivo móvil y/o resetear el mismo, pasa por cambiar la contraseña (como se ha descrito previamente).

5.20 COPIA DE SEGURIDAD DE DATOS EN IOS

1165. Apple proporciona dos alternativas para realizar una copia de seguridad de (la mayoría de) los datos almacenados en los dispositivos móviles basados en iOS: iTunes e iCloud.

1166. La información que se almacena en la copia de seguridad incluye, entre otros, la música, programas de televisión, aplicaciones y libros adquiridos (los productos de la iTunes y App Store), fotos y vídeos, los ajustes del dispositivo móvil (por ejemplo, favoritos del teléfono y fondos de pantalla, cuentas de correo, contactos o calendario), datos de las aplicaciones, organización de la pantalla de inicio y de las aplicaciones, mensajes (iMessage, SMS y MMS), tonos, etc [Ref.- 48] [Ref.- 50].

1167. iTunes puede llevar a cabo una copia de seguridad del dispositivo móvil durante el proceso de sincronización de datos. Adicionalmente, el usuario puede forzar la realización de una copia de seguridad tras conectar el dispositivo a iTunes (a través de USB o de Wi-Fi), seleccionando el dispositivo móvil de la lista de dispositivos de iTunes, mediante la opción "Copia" ("Back Up"; disponible a través del botón derecho del ratón):



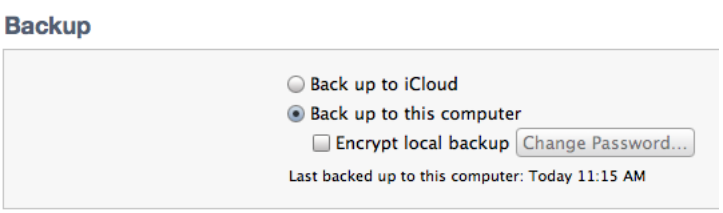
1168. Las copias de seguridad de iTunes incluyen los datos mencionados previamente, aunque los mismos varían entre diferentes versiones de iOS [Ref.- 50].

1169. El contenido de las copias de seguridad puede ser protegido y cifrado mediante una contraseña, siendo ésta necesaria en el proceso de restauración de los datos. Se recomienda seleccionar una contraseña suficientemente robusta y difícilmente adivinable por un potencial atacante que disponga de acceso a los ficheros del ordenador donde se almacena la copia de seguridad.

1170. Debe tenerse en cuenta que existen herramientas, como por ejemplo IGPRS [Ref.- 114], que permiten auditar la fortaleza de la contraseña empleada para proteger las copias de seguridad de iOS 4.x y 5.x realizadas mediante iTunes, y que pueden descifrar su contenido en caso de emplearse una contraseña débil.

1171. Para versiones posteriores de iOS, como 6.x y 7.x, y versiones 11.x de iTunes existen numerosas herramientas comerciales que permiten la recuperación de la contraseña de las copias de seguridad de iTunes mediante ataques de diccionario o fuerza bruta, como por ejemplo iPhone Backup Unlocker, iTunes Backup Password Recovery o Elcomsoft Phone Password Breaker.

1172. El cifrado de las copias de seguridad puede ser habilitado desde la pantalla de resumen del dispositivo móvil en iTunes, mediante la opción "Cifrar copia de seguridad local" (deshabilitada por defecto; en inglés en la imagen inferior "Encrypt local backup"):



1173. Las copias de seguridad son almacenadas en el ordenador en una ubicación diferente en función del sistema operativo:

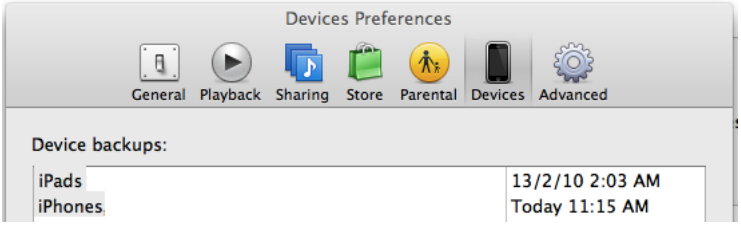
- OS X:

  ~/Library/Application Support/MobileSync/Backup/

- Windows 8, 7 y Vista:

  C:\Users\<usuario>\AppData\Roaming\Apple Computer\MobileSync\Backup\

1174. A través del menú de preferencias de iTunes, desde la sección de "Dispositivos" ("Devices"), es posible verificar la existencia de copias de seguridad locales:



5.20.1 COPIAS DE SEGURIDAD EN ICLOUD: ICLOUD BACKUP

1175. Desde la versión 5.0 de iOS, adicionalmente, es posible realizar copias de seguridad a través del servicio iCloud (http://icloud.com) de Apple [Ref.- 53], un servicio de almacenamiento que permite realizar copias de seguridad de los datos "en la nube" y sincronizar dichos datos entre todos los dispositivos móviles iOS del usuario, con almacenamiento ilimitado para las compras de la App Store y 5 GB de espacio gratuito para el resto de datos.

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 iOS y el servicio iCloud de Apple, ni para la funcionalidad de copias de seguridad, ni para el resto de servicios ofrecidos por esta plataforma.

1176. En el caso de habilitar las capacidades de copia de seguridad mediante iCloud no será posible realizar copias de seguridad mediante iTunes con el ordenador local. Ambas soluciones no son compatibles en la actualidad.

1177. iCloud no sólo permite almacenar los datos del usuario (música, fotos, aplicaciones, calendarios, documentos, etc), sino también sincronizarlos entre los diferentes dispositivos iOS (o OS X Lion o superior) del usuario. Adicionalmente, las capacidades de copia de seguridad (*backup*) de iCloud permiten almacenar la configuración del dispositivo móvil, los datos de las aplicaciones y los mensajes (de texto o SMS, multimedia o MMS, o iMessage) a diario a través de redes Wi-Fi [Ref.- 52].

1178. iCloud realiza automáticamente una copia de seguridad de los datos del dispositivo móvil una vez habilitada la opción de copia de seguridad a través del menú "Ajustes - iCloud - Almacenamiento y copia":

1179. El servicio de copia de seguridad de datos de iCloud permite almacenar información personal del usuario en los servidores de Apple, incluyendo los datos mencionados

previamente, y siendo posible para los datos de las aplicaciones seleccionar qué aplicaciones se incluirán en las copias de seguridad y el espacio empleado por cada una de ellas.

1180. Desde el menú "Ajustes - iCloud - Almacenamiento y copia", mediante la opción "Gestionar almacenamiento", es posible seleccionar el dispositivo a gestionar y acceder a toda esa información.

1181. La copia se ejecutará a diario siempre que el dispositivo móvil esté conectado a Internet mediante Wi-Fi, también esté conectado a una fuente de alimentación y tenga la pantalla bloqueada [Ref.- 48]. El servicio almacena las tres copias de seguridad más recientes del dispositivo móvil para su futura restauración.

1182. Adicionalmente es posible realizar una copia de seguridad manualmente siempre y cuando el dispositivo esté conectado a Internet mediante Wi-Fi a través de la opción "Realizar copia de seguridad ahora" disponible desde "Ajustes - iCloud - Almacenamiento y copia":

1183. Los datos almacenados por las copias de seguridad de iCloud incluyen información sobre contenidos adquiridos en la App Store (y otras tiendas online de Apple), como música, películas, apps, libros, etc (pero no los propios contenidos), fotos y vídeos en el Carrete, los ajustes de configuración del dispositivo, los datos de las apps, la organización de las apps en la pantalla principal, mensajes (SMS, MMS e iMessage), tonos de llamada y el buzón de voz visual.

1184. Los servicios de iCloud cifran las comunicaciones durante el intercambio de datos mediante HTTPS (SSL/TLS), al igual que los datos que son almacenados en este servicio [Ref.- 17] mediante AES de 128 bits.

1185. La información de metadatos de los ficheros almacenados en iCloud, junto a las claves de cifrado, es almacenada por Apple en la cuenta de iCloud del usuario. Los contenidos de los ficheros son almacenados por Apple, sin ninguna vinculación con el usuario, en servicios de almacenamiento de terceros, como Amazon S3 o Windows Azure [Ref.- 13].

1186. Debe tenerse en cuenta que el objetivo de los mecanismos de cifrado de los datos almacenados por los usuarios pretenden evitar el acceso a dichos datos privados entre distintos usuarios del servicio, sin embargo, tal como especifican los términos y condiciones del servicio, Apple dispone de la posibilidad de acceder a los datos de todos los usuarios [Ref.- 107], hecho que debe ser cuidadosamente evaluado antes de utilizar iCloud para el almacenamiento de información sensible y confidencial.

1187. La comunicación entre el dispositivo móvil y los servidores de iCloud, "keyvalueservice.icloud.com" (o "pNN-keyvalueservice.icloud.com", dónde "NN" es un número de dos dígitos), se lleva a cabo mediante el puerto 443/tcp (HTTPS), empleando un certificado comodín proporcionado por Entrust para "*.icloud.com".

1188. Adicionalmente a la funcionalidad de copia de seguridad de iCloud, esta solución ofrece otros servicios. Los diferentes servicios disponibles en iCloud, como *Photo Stream* (sincronización de fotos en tiempo real entre dispositivos Apple), y la sincronización de documentos y copias de seguridad, pueden ser (des)habilitados de forma independiente a través de los perfiles de configuración y las soluciones MDM.

1189. La política de contraseñas actual asociada a los identificadores de Apple (Apple ID) necesarios para el uso de los servicios de iCloud y App Store requiere emplear al menos 8 caracteres, incluyendo un número, una letra mayúscula y una letra minúscula.

1190. Sin embargo, si el usuario ya disponía de un Apple ID creado con anterioridad al momento en que se introdujo dicha política de contraseñas por parte de Apple, podrá mantener una contraseña que no cumple dicha política mientras no la cambie.

1191. Se recomienda evaluar en detalle la importancia y confidencialidad de cada uno de los datos a almacenar en iCloud, considerando que la información privada almacenada en el dispositivo móvil podría ser accedida por un potencial atacante en caso de que disponga de acceso al servicio iCloud como el usuario y/o a sus servidores asociados.

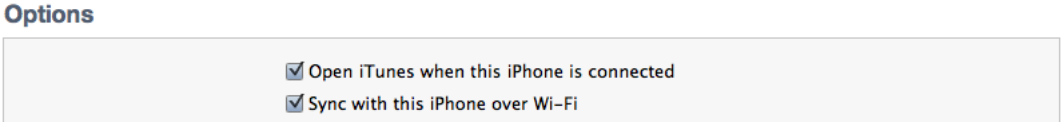
5.21 SINCRONIZACIÓN DE DATOS EN IOS

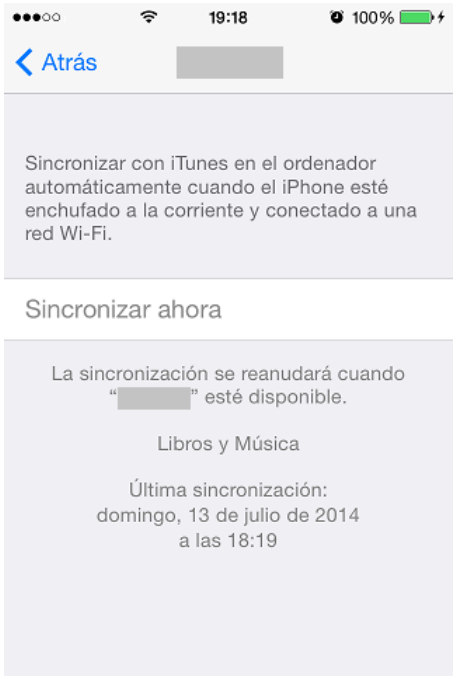
1192. Adicionalmente a las capacidades de realización de copias de seguridad (ver apartado "5.20. Copia de seguridad de datos en iOS"), iOS permite llevar a cabo la sincronización de otros datos del usuario, tanto a través de iTunes como de iCloud.

1193. A partir de la versión 5.x de iOS es posible llevar a cabo la sincronización de datos entre el dispositivo móvil y un ordenador con iTunes (versión 10.5 o superior) empleando tanto una conexión física entre ambos dispositivos a través de un cable USB (opción disponible también previamente), como una red inalámbrica Wi-Fi.

1194. La opción para habilitar la funcionalidad de sincronización a través de Wi-Fi está disponible desde el propio dispositivo móvil, en el menú “Ajustes – General – Sincronizar con iTunes vía Wi-Fi” (ver imágenes inferiores).

1195. Sin embargo, para poder hacer uso de esta funcionalidad es necesario activarla inicialmente desde iTunes. La activación debe llevarse a cabo mediante la opción "Sincronizar a través de Wi-Fi" ("Sync with this iPhone over Wi-Fi") disponible en la pantalla resumen del dispositivo en iTunes, debiendo estar conectado el dispositivo móvil al ordenador con iTunes a través de un cable USB en el momento de la activación:

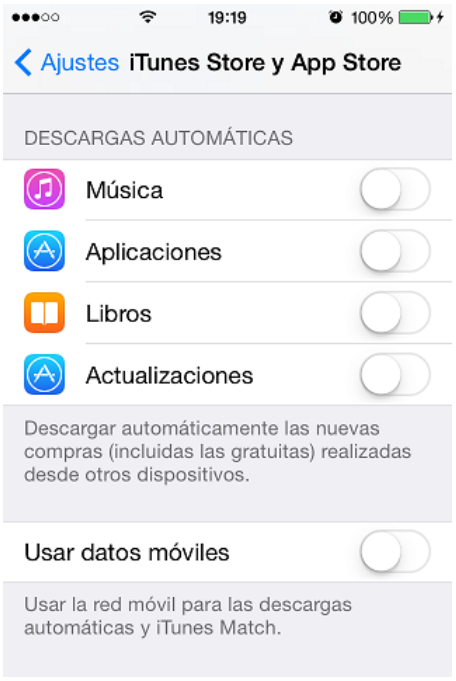




1196. Para llevar a cabo la sincronización con iTunes a través de Wi-Fi el ordenador con iTunes y el dispositivo móvil deben estar conectados a la misma red Wi-Fi [Ref.- 47].

1197. Es posible transferir las compras o contenidos adquiridos en la tienda iTunes (iTunes Store) y la App Store seleccionando el dispositivo móvil en iTunes, y la opción "Transferir compras" (disponible a través del botón derecho).

1198. Para transferir automáticamente los contenidos adquiridos, incluso desde otros dispositivos iOS, en la iTunes Store y la App Store, tanto de pago como gratuitos, es necesario hacer uso de las opciones bajo la sección "Descargas automáticas" del menú "Ajustes - iTunes Store y App Store":



1199. Las descargas automáticas están divididas en "Música", "Aplicaciones", "Libros" y "Actualizaciones" de forma independiente, siendo posible seleccionar si se hará uso únicamente de redes Wi-Fi para dicha descarga o también de redes de telefonía móvil (2/3/4G), mediante la opción inferior "Usar datos móviles" (ver imagen superior).

1200. Las capacidades de sincronización permiten transferir las fotos realizadas desde el dispositivo móvil iOS al ordenador, así como los contactos, calendarios, favoritos y notas [Ref.- 55], todos ellos disponibles desde las diferentes pestañas de información del dispositivo móvil iOS en iTunes.

1201. Los ajustes de las cuentas de correo electrónico se pueden sincronizar desde el ordenador al dispositivo móvil iOS, pero no al contrario.

1202. Se recomienda evaluar en detalle la importancia y confidencialidad de cada uno de los tipos de datos a sincronizar con iCloud (e iTunes), considerando que la información privada almacenada en el dispositivo móvil podría ser accedida por un potencial atacante en caso de que disponga de acceso al servicio iCloud (o al ordenador con iTunes) como el usuario y/o a sus servidores asociados.

5.22 LOCALIZACIÓN DEL DISPOSITIVO MÓVIL: BUSCAR MI IPHONE

1203. El servicio "Buscar mi iPhone" (“Find My iPhone”, o iPad), integrado en iCloud, permite a los usuarios de dispositivos móviles iOS (y OS X Lion) localizar la ubicación del dispositivo móvil si éste ha sido extraviado o sustraído.

1204. Pese a denominarse "Buscar mi iPhone", es un servicio disponible para la localización de los distintos tipos de dispositivos móviles basados en iOS de Apple, como por ejemplo el iPhone y el iPad.

1205. Adicionalmente, el servicio proporciona capacidades para bloquear de forma remota el dispositivo móvil con un código de acceso, ejecutar un borrado de datos remoto (*wipe*; ver apartado "5.9. Eliminación de datos del dispositivo móvil"), hacer que suene el dispositivo móvil, mostrar un mensaje en la pantalla, o recibir un correo electrónico

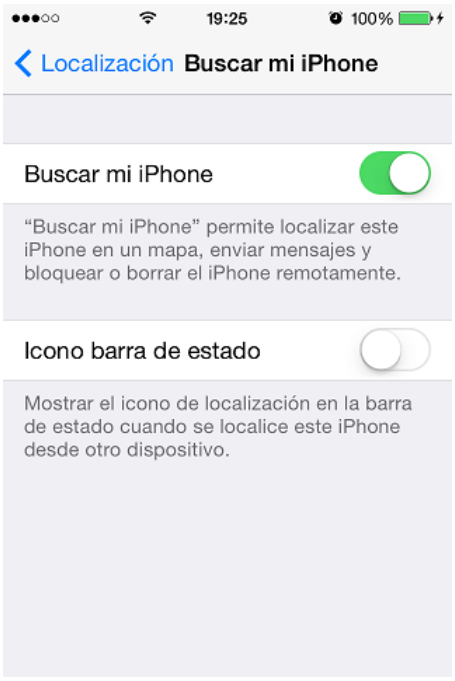
cuando el dispositivo móvil no ha podido ser localizado por falta de conectividad y vuelve de nuevo a disponer de conexión a Internet (vía Wi-Fi o 2/3/4G).

1206. Los usuarios de iCloud requieren hacer uso de iOS 5.x o OS X Lion, o versiones posteriores. El servicio "Buscar mi iPhone" está también disponible para los usuarios de MobileMe, con la versión 3.1.3 o superior de iOS (servicio que fue sustituido por iCloud en iOS 5.x).

1207. El acceso al servicio está disponible desde la web de iCloud (https://www.icloud.com) o MobileMe (https://www.me.com), o desde otros dispositivos iOS mediante la aplicación "Buscar mi iPhone" ("Find My iPhone") disponible en la App Store (http://itunes.apple.com/us/app/find-my-iphone/id376101648?mt=8):

1208. Para poder hacer uso de este servicio desde iOS 5.x, y en versiones posteriores, es necesario disponer de una cuenta en iCloud (o en MobileMe en versiones previas de iOS) y la funcionalidad debe ser activada a través del menú “Ajustes - iCloud - Buscar mi iPhone”:

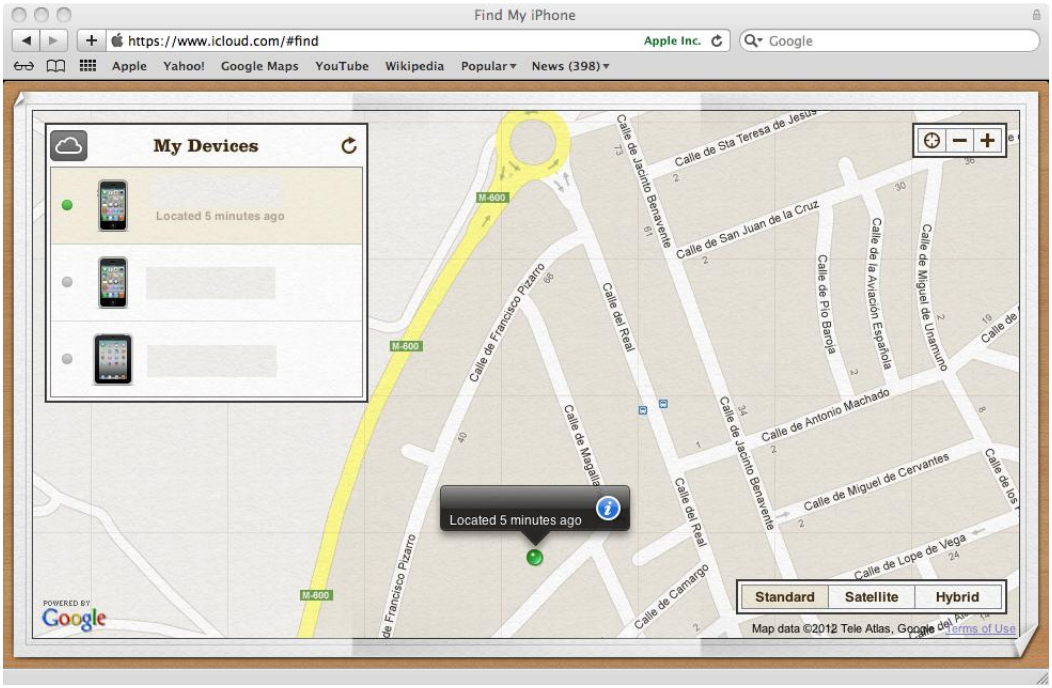
1209. Adicionalmente, la opción "Buscar mi iPhone" en iOS del menú "Ajustes - Privacidad - Localización" activa o desactiva la misma funcionalidad (ofreciendo dos formas de interactuar con el servicio). Adicionalmente, desde este menú, es posible definir si se permite al usuario ver el icono de los servicios de localización en la barra de estado cuando el dispositivo móvil está siendo localizado a través de la opción "Icono barra de estado":



1210. Desde el punto de vista de seguridad y con el objetivo de no alertar al usuario que haya podido sustraer el dispositivo móvil, no se recomienda activar esta funcionalidad, de forma que el dispositivo móvil pueda ser localizado desde otro dispositivo de forma transparente al usuario no autorizado que lo pueda poseer en un momento determinado.

1211. El acceso al servicio web de iCloud (https://www.icloud.com) está protegido mediante usuario y contraseña, asociados a una cuenta de usuario de Apple o Apple ID, y puede ser utilizado para gestionar los dispositivos móviles vinculados a dicha cuenta desde cualquier ordenador conectado a Internet. Adicionalmente el servicio puede ser accedido desde un dispositivo móvil empleando cualquier conexión de datos a Internet o a través de la aplicación "Buscar mi iPhone" desde un dispositivo móvil iOS.

1212. iCloud, y el servicio "Buscar mi iPhone", permiten sincronizar la localización actual del dispositivo móvil con el objetivo de poder obtener a través del interfaz web del servicio, en caso de pérdida, la ubicación del terminal la última vez que realizó la sincronización:

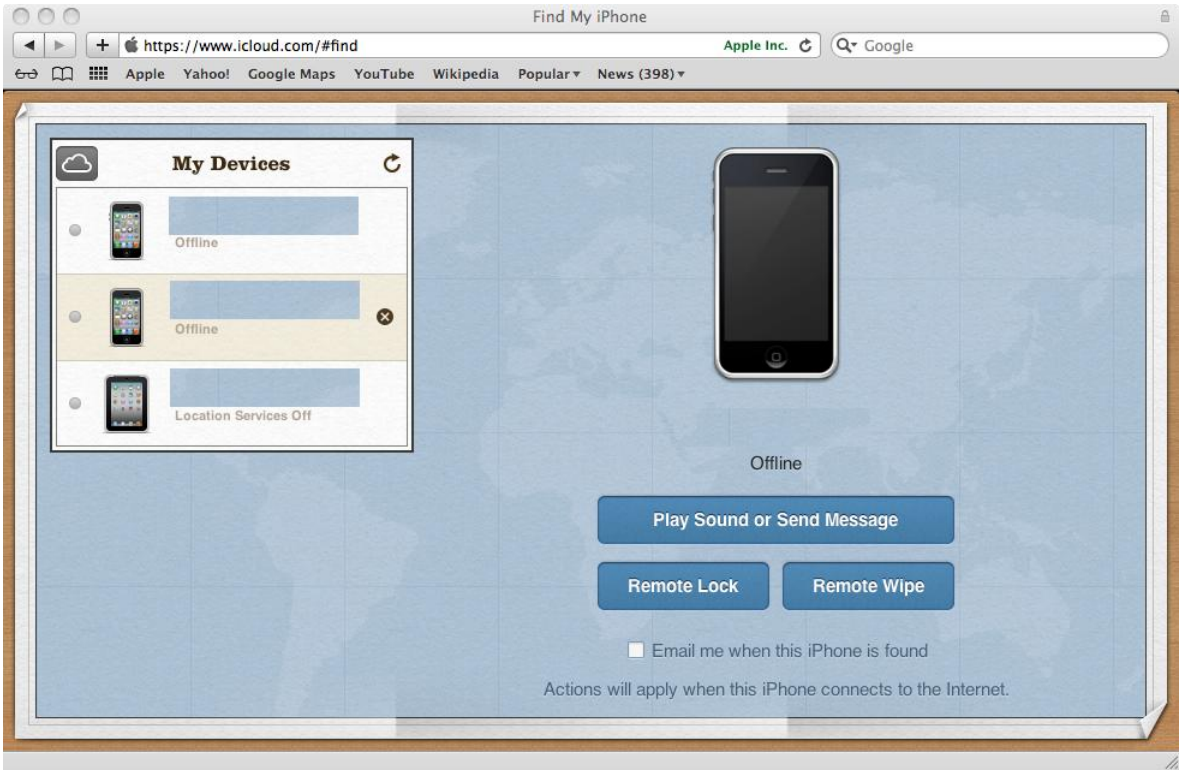


1213. La localización del dispositivo móvil sólo se transmite a los servidores de Apple en el momento que es solicitada, y no de forma periódica, el temporizador relativo de sesión por falta de actividad (tanto desde la web como desde la aplicación móvil) es de 15 minutos, y la última localización disponible es almacenada de forma cifrada en sus servidores un máximo de 24 horas [Ref.- 17].

1214. Asimismo, la plataforma iCloud permite acceder al resto de servicios para hacer que el teléfono suene para localizarlo tras su pérdida, mostrar un mensaje en la pantalla, y proteger la información que almacena mediante el bloqueo del terminal o incluso mediante la eliminación de los datos almacenados en el dispositivo móvil:

1215. El acceso al servicio "Buscar mi iPhone" dentro de iCloud requiere que el usuario vuelva a autentificarse con la contraseña asociada a su Apple ID registrado en iCloud:

1216. El servicio proporciona acceso a todos los dispositivos asociados al Apple ID del usuario, ofreciendo la funcionalidad de búsqueda. En caso de que el dispositivo móvil esté "offline" (no disponible y desconectado de Internet en estos momentos), la aplicación muestra la funcionalidad que permite recibir un e-mail cuando el dispositivo vuelva a conectarse a Internet (disponible en la parte inferior de la pantalla):



1217. Esta funcionalidad también está disponible si el dispositivo móvil fue localizado recientemente pero vuelve a estar "offline":

1218. El mensaje de correo electrónico, o e-mail, será enviado a la dirección de e-mail del usuario asociada a la cuenta de iCloud o Apple ID.

1219. Una vez localizada la ubicación del dispositivo móvil también es posible acceder a los diferentes servicios disponibles (salvo al de envío de un e-mail al ser localizado):

1220. Al hacer sonar el teléfono remotamente (durante 120 segundos en el volumen más alto), el dispositivo móvil puede mostrar un mensaje personalizado, por ejemplo, indicando que su propietario está buscando el terminal. Tanto la funcionalidad de hacer sonar un sonido como de mostrar un mensaje son opcionales. En su defecto, si no se escribe ningún mensaje, mostrará el texto "Find My iPhone Alert" (ejemplo con iOS 5.x):

1221. El mensaje enviado permanecerá visible en la pantalla del terminal, tanto tras intentar desbloquearlo sin éxito, como una vez desbloqueado:

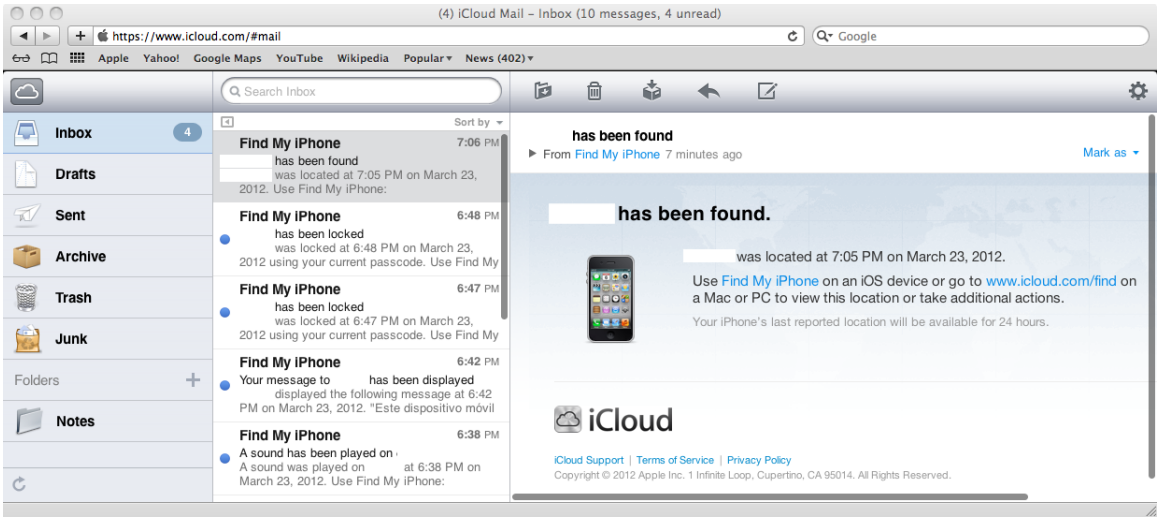
1222. La funcionalidad de bloqueo remoto del dispositivo móvil utilizará el código de acceso o PIN existente, en caso de disponer de uno, para proceder a bloquear el dispositivo. En caso de que no hubiera un código de acceso establecido previamente, permitirá establecer el valor del código de acceso o PIN a emplear para bloquear el dispositivo.

1223. En versiones previas de iOS a través del servicio Mobile Me, si el código de acceso era de 4 caracteres (o menos), era posible seleccionar el valor de dicho código remotamente y cambiar el existente [Ref.- 59], sin embargo desde iOS 4.x no es posible modificar el código existente (que sería la opción recomendada desde el punto de vista de seguridad; ver imagen inferior izquierda). Por tanto, si la persona que dispone de acceso no autorizado al dispositivo móvil ha obtenido el valor del código de acceso, su propietario no podrá de forma remota impedir el acceso al dispositivo móvil:

1224. La funcionalidad de borrado remoto de datos (*wipe*), ver imagen superior derecha, eliminará todos los datos del dispositivo (ver apartado "5.9. Eliminación de datos del

dispositivo móvil"), imposibilitando la localización del dispositivo móvil pero evitando que un potencial atacante consiga acceso a los datos que contiene.

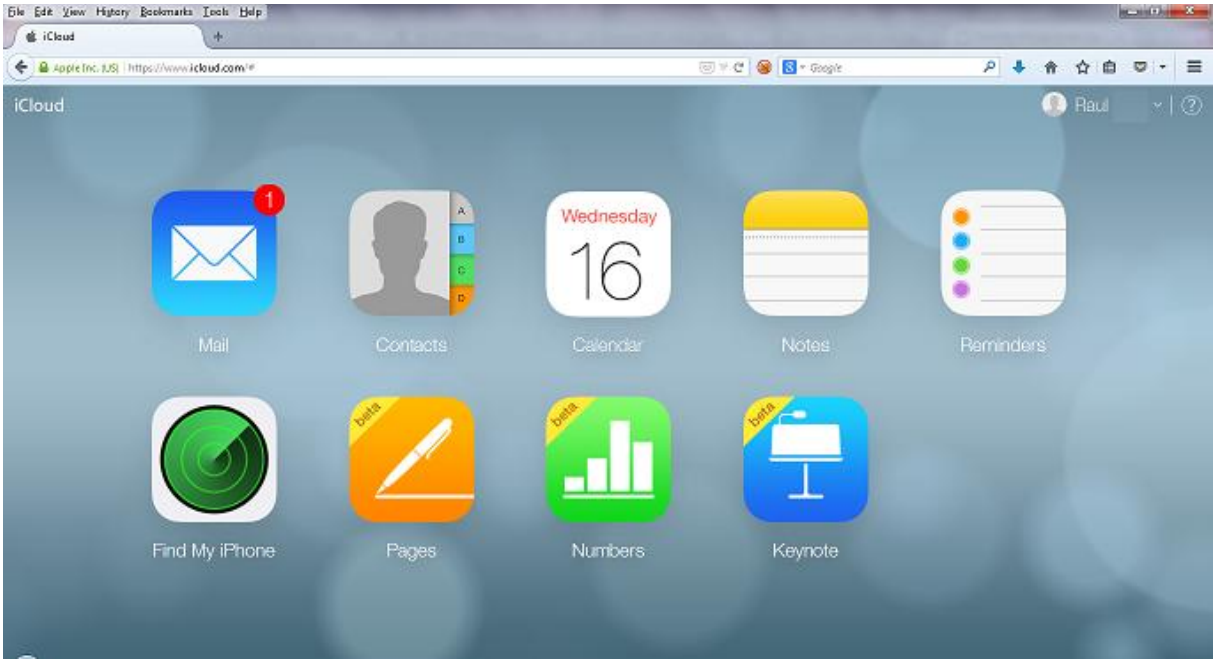
1225. Toda las acciones asociadas al servicio "Buscar mi iPhone" generan e-mails que son enviados al usuario de iCloud, con el objetivo de disponer de un registro con las diferentes operaciones realizadas sobre el dispositivo móvil a través del servicio:

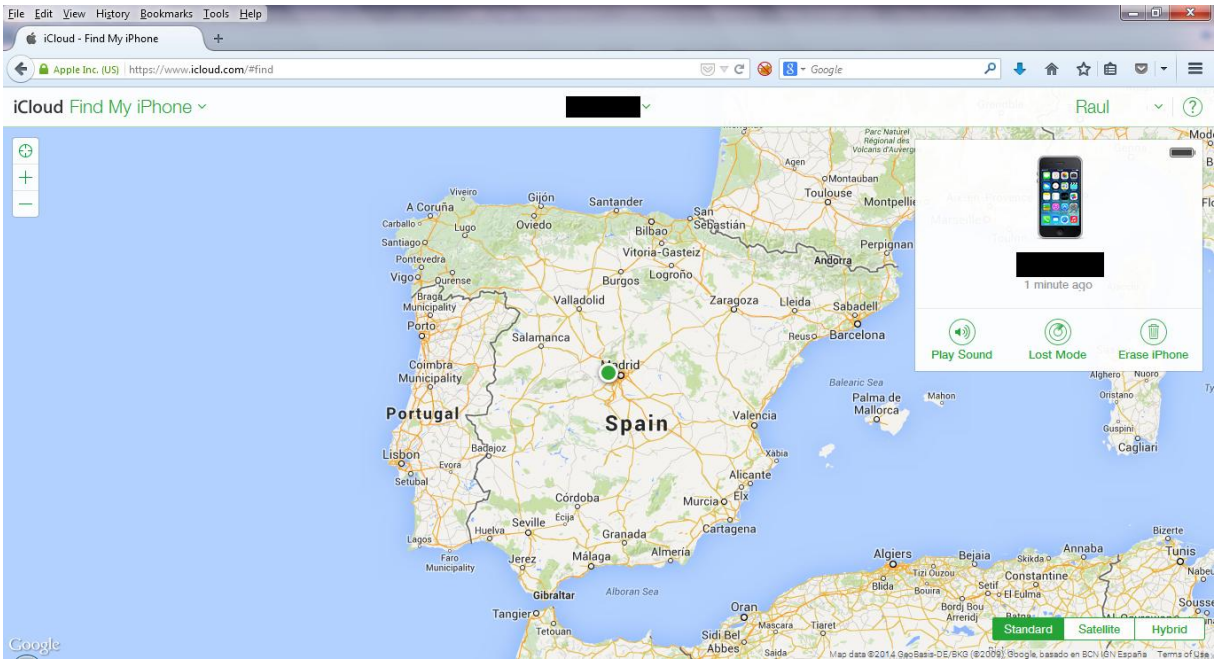


1226. Con el objetivo de recuperar un dispositivo móvil perdido se recomienda hacer uso de las capacidades del servicio iCloud en el siguiente orden: localizar la ubicación del teléfono, bloquear el teléfono para evitar su uso, hacerlo sonar para notificar su búsqueda y, finalmente, borrar los datos del mismo.

1227. En el caso de que el objetivo principal no sea la recuperación del dispositivo móvil sino la eliminación de sus datos, debido a su carácter confidencial y privado, se puede proceder a la operación de borrado directamente tras intentar obtener su ubicación.

1228. Adicionalmente, desde iOS 7 se dispone de capacidades a través del servicio de "Buscar mi iPhone" desde iCloud para activar la funcionalidad de dispositivo móvil perdido, "Lost Mode" (ver apartado "5.5. Restricciones en el proceso de activación"):





5.23 APLICACIONES EN IOS

1229. Las aplicaciones para iOS están desarrolladas en el lenguaje de programación Objective-C[11] y en la API de programación gráfica Cocoa y Cocoa Touch, y ejecutan sobre el sistema operativo iOS. Por tanto, las aplicaciones iOS son susceptibles de ser vulnerables a los fallos de programación tradicionales existentes en el lenguaje C, como desbordamientos de memoria (*buffer or integer overflows*), o *format strings* [Ref.- 26].

[11] Adicionalmente, Apple introdujo el lenguaje de programación Swift a partir de iOS 8.

1230. Las aplicaciones iOS son compiladas mediante el entorno de programación Xcode. Cada aplicación incluye un identificador único, el ejecutable, los "derechos" (*entitlements*), las preferencias y metadatos (en formato Objective-C Property List o .plist, como por ejemplo "Info.plist"), la firma digital de su desarrollador y los ficheros multimedia asociados.

1231. El fichero "Info.plist", entre otros, declara los requisitos de la aplicación por motivos de compatibilidad, pero no para la definición de permisos requeridos por la misma.

1232. Los *entitlements* describen los permisos (o "derechos") asociados a la aplicación, como si es posible hacer uso de un depurador, el grupo de acceso a la *keychain*, o el perfil de *sandbox* a utilizar. Para ello se emplea un documento XML firmado que es incluido en el paquete software de la aplicación [Ref.- 46].

1233. El modelo de seguridad de iOS sólo permite la ejecución de aplicaciones firmadas por Apple y que por tanto han seguido el modelo de desarrollo establecido por Apple para los desarrolladores oficiales de aplicaciones móviles para iOS.

1234. La gestión de aplicaciones en iOS se puede realizar directamente a través del dispositivo móvil y la aplicación "Store", que permite el acceso a la App Store, o a través de iTunes, gestionando el acceso a la App Store a través de un ordenador y realizando la sincronización entre éste y el dispositivo móvil.

1235. Las aplicaciones móviles para iOS están vinculadas en la App Store al Apple ID del usuario, y podrán ser instaladas y actualizadas en todos los dispositivos móviles iOS de los que es propietario el usuario, al introducir en todos ellos las credenciales asociadas a ese Apple ID.

1236. Los siguientes apartados proporcionan breves recomendaciones de seguridad asociadas a las aplicaciones más relevantes existentes por defecto en iOS. En ningún caso se pretende realizar un análisis de seguridad exhaustivo de su funcionalidad y de todas las opciones de configuración disponibles en cada aplicación.

Nota: El número de aplicaciones cliente instaladas por defecto por Apple (iOS), variable en función de la versión de iOS, así como la variedad de aplicaciones cliente de otras compañías que pueden ser instaladas posteriormente manualmente o desde App Store, 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 iOS), 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 funcionalidad y seguridad ofrecida por la aplicación.

5.23.1 GESTIÓN DE COMPARTICIÓN DE CONTENIDOS ("MANAGED OPEN IN")

1237. iOS 7 ha comenzado la adopción de un modelo para poder compartimentalizar la parte profesional y personal del dispositivo móvil, y su adecuación a entornos BYOD, basado en proteger los datos corporativos y no permitir acceso a estos desde apps no aprobadas por la organización.

1238. Para ello, iOS 7 permite definir a través de las soluciones de gestión empresarial (MDM) qué tipo de documentos y contenidos pueden ser abiertos por qué apps, con el

objetivo de encontrar un equilibrio entre el acceso a contenidos corporativos y privados desde dispositivos móviles, y la protección de dichos contenidos.

1239. iOS 7 emplea la tecnología denominada “Managed Open In” (o gestión de compartición de contenidos) que permite controlar qué apps y cuentas gestionadas pueden emplearse para abrir documentos, contenidos y ficheros adjuntos corporativos, y que éstos no puedan ser accedidos desde apps no autorizadas (o no gestionadas).

1240. Pese a que el objetivo principal de "Managed Open In" es bloquear el acceso a contenidos privados y corporativos por parte de apps no autorizadas (más asociado a la filtración de información privada hacia el exterior de la organización, común en las soluciones DLP, *Data Loss Prevention*), también proporciona suficiente flexibilidad para bloquear contenidos personales hacia apps corporativas (más asociado a la introducción de contenidos no deseados o maliciosos desde el exterior hacia el interior de la organización).

1241. La diferenciación, o los entornos de compartición, se establecen a partir de la identificación de qué cuentas (por ejemplo de correo electrónico) y qué apps son gestionadas, y por tanto autorizadas, por la organización a través de la solución MDM. El conjunto de cuentas y apps gestionadas constituyen el entorno empresarial o corporativo dentro del dispositivo móvil iOS (en contraposición al resto de elementos de la plataforma, asociados al entorno personal del usuario). Así por ejemplo, un fichero adjunto recibido a través de una cuenta gestionada de correo electrónico sólo podrá ser abierto a través de las capacidades de compartición de iOS en las apps gestionadas permitidas para ese tipo de documento.

1242. Las capacidades de compartición de datos (o formalmente "Open In") de iOS están disponibles a través del icono de compartir información,  , de cada una de las apps existentes.

1243. Las apps declaran en su fichero de configuración general (info.plist) qué tipo de contenidos o ficheros pueden gestionar, identificados por su UTI (*Uniform Type Identifier*). La funcionalidad "Open In" identifica el listado de apps disponibles para un tipo de fichero determinado y las muestra a la hora de compartirlo.

1244. "Managed Open In" filtra o limita el número de apps que aparecen listadas como posibles destinatarios a la hora de intentar compartir un contenido con otros destinos vía la funcionalidad de "Open In" de la plataforma iOS para cada app.

1245. Estas restricciones son aplicadas habitualmente a la funcionalidad local que permite enviar o compartir un documento o datos desde una app hacia otra app en el mismo dispositivo móvil, o capacidades de la plataforma móvil, como la impresión de dichos datos.

1246. Debe tenerse en cuenta que otras capacidades de compartición de datos, como AirDrop (ver apartado "5.14.8. Integración con AirDrop"), no están restringidas por las políticas de "Managed Open In", al igual que tampoco lo están las capacidades de compartir o enviar datos a Twitter o Facebook (ambos servicios plenamente integrados en la plataforma móvil de Apple en iOS 7) si las apps gestionadas empleadas tienen capacidades (es decir, hacen uso de las librerías) de compartición con estos servicios. Por tanto, "Managed Open In" sólo mitiga uno de los posibles vectores de ataque centrados en la filtración de datos corporativos desde el dispositivo móvil.

1247. Tampoco aplican las restricciones establecidas por "Managed Open In" a otros tipos de datos diferentes a documentos, como por ejemplo a la información de contactos o calendario, que debe ser gestionada a través del panel de control de privacidad de iOS.

1248. Por otro lado, la compartición o integración de otras apps con otros servicios o repositorios de datos de Apple (iCloud), o de terceros, tampoco está protegidas por "Managed Open In", ya que no hacen uso de la funcionalidad nativa de compartición de datos de iOS (denominada formalmente "Open In"), o por ejemplo, el reenvío a través de correo electrónico de un fichero.

1249. "Managed Open In" no proporciona por tanto una solución contenedora completa como la existente en algunas de las soluciones MDM disponibles en la industria, por lo que es necesario complementarla con otras protecciones frente a los diferentes escenarios descritos previamente.

5.24 NAVEGACIÓN WEB: SAFARI

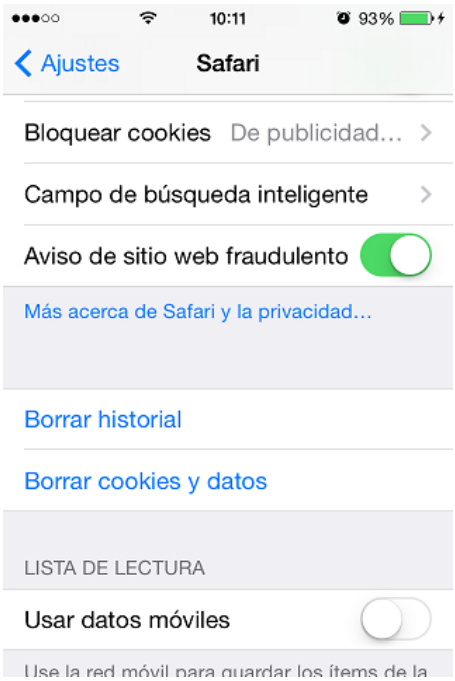
1250. Una de las tareas más comunes realizadas desde los dispositivos móviles es la de navegación web por Internet. iOS incluye por defecto un navegador web, referenciado como “Safari”, y correspondiente a la versión móvil (o Safari Mobile o Mobile Safari) del navegador web Safari, basado en el motor de código abierto WebKit (con modificaciones por parte de Apple, AppleWebKit).

1251. La versión genérica de Safari disponible por defecto en iOS 7.1.2 es la versión 7.0, y en concreto "Safari/9537.53" /según el valor de la cabecera HTTP "User-Agent").

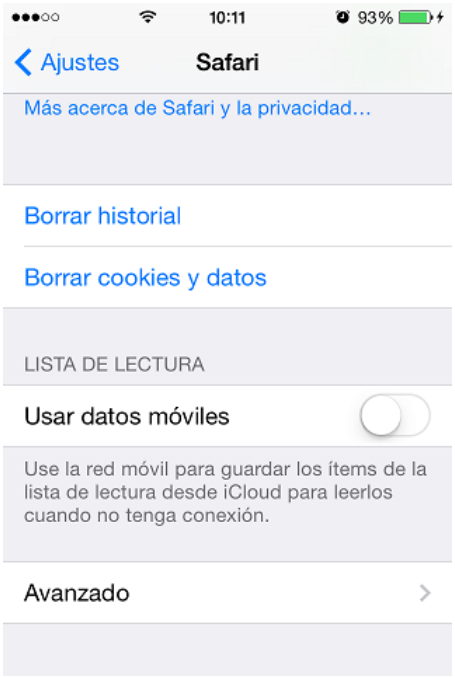
1252. La versión 6 de iOS introdujo nuevas capacidades de integración entre Safari e iCloud, añadiendo la posibilidad de sincronizar las pestañas abiertas entre diferentes dispositivos Apple (basados en iOS 6 o OS X Mountain Lion, o versiones posteriores), o la creación de listas de lectura offline, para cuando no se dispone de conexión a Internet.

1253. El navegador web Safari de iOS presenta limitaciones de seguridad relevantes, como por ejemplo las ya mencionadas relativas a la validación y almacenamiento de los certificados SSL/TLS (ver apartado "5.18.4. SSL/TLS"). Sin embargo, sí dispone de soporte para cookies "secure", empleadas para proteger la sesión de un usuario en conexiones HTTPS cifradas, o "HttpOnly", empleadas para proteger la sesión de un usuario frente a ataques de Cross-Site Scripting (XSS) [Ref.- 121] [Ref.- 120].

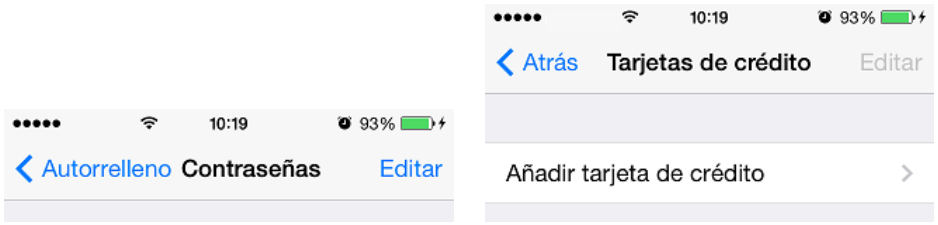
1254. A través del menú “Ajustes - Safari”, es posible acceder a los ajustes de configuración del navegador web, desde dónde se recomienda (buscando un equilibrio entre seguridad y usabilidad del navegador web) no habilitar las opciones de "Contraseñas y autorelleno" para completar los campos de formularios HTML (deshabilitadas por defecto), permitir el uso de cookies proporcionadas sólo por las páginas web visitadas (opción habilitada por defecto: "Bloquear cookies - De publicidad y terceros"), dejar habilitada la opción de "Aviso de sitio web fraudulento" (activa por defecto), dejar habilitada la opción "Bloquear ventanas" para evitar la generación de pop-ups (activa por defecto), habilitar la opción "No rastrear" (deshabilitada por defecto) para evitar el seguimiento de agencias de publicidad (descrita posteriormente), y habilitar o deshabilitar JavaScript en función de las preferencias del usuario, disponible en la sección "Avanzado - JavaScript" (activa por defecto):



1255. Adicionalmente los ajustes permiten borrar el historial, a través del botón "Borrar historial", y borrar las cookies y los datos (caché) almacenados actualmente, a través del botón "Borrar cookies y datos", tanto de forma global para todo el navegador web, como los datos de manera individualizada para cada sitio web, a través de la opción "Avanzado - Datos de sitios web" y el botón "Edición":



1256. Adicionalmente, a través de la opción "Contraseñas y autorelleno", es posible configurar si el navegador web puede completar automáticamente en páginas web los datos de contacto del usuario a partir de una entrada de la agenda de contactos, así como recordar los nombres de usuario y contraseñas (credenciales) empleados en páginas y formularios web, junto a la información de tarjetas de crédito, todos ellos deshabilitados por defecto (opción recomendada desde el punto de vista de seguridad), pudiendo ser eliminadas las que están almacenadas actualmente mediante el botón "Editar" dentro de cada categoría (analizadas en detalle posteriormente):



1257. Para una navegación web más segura, pero muy restringida desde el punto de vista de su funcionalidad, se recomienda deshabilitar la ejecución de scripts mediante la opción "JavaScript", y el uso de cookies en el navegador web (mediante la opción "Bloquear cookies: Siempre"), con el objetivo de mitigar los ataques asociados a la ejecución de scripts maliciosos en el navegador web y a la privacidad del usuario a través de las cookies. Adicionalmente, el bloqueo de ventanas o pop-ups es una opción que debe permanecer habilitada.

1258. Esta configuración podría dificultar la visualización de páginas web que utilizan scripts y cookies en sus contenidos web y para su correcto funcionamiento (desafortunadamente, la mayoría de páginas web en Internet).

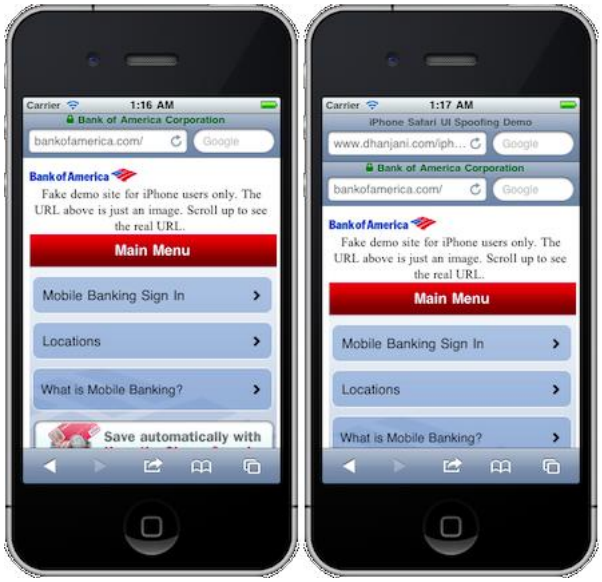
1259. Se recomienda borrar de forma frecuente tanto el historial de navegación web, como el almacenamiento de cookies y datos (caché), y los datos de formularios, contraseñas y tarjetas de crédito (en caso de ser almacenados), con el objetivo de proteger la privacidad del usuario.

1260. Cada uno de estos elementos puede ser eliminado individualmente mediante los botones correspondientes previamente analizados.

1261. El navegador web de iOS, Safari (Mobile), fue vulnerable a ataques de suplantación de la barra de direcciones o navegación (*Address Bar Spoofing*) en la versión 4.x de iOS [Ref.- 90].

1262. Esta vulnerabilidad en concreto se debía a fallos de diseño en el módulo UIWebView empleado por las aplicaciones iOS para la optimización de los contenidos en la reducida pantalla de los dispositivos móviles, haciendo que la barra de direcciones o navegación desaparezca de la pantalla (o zona visible por el usuario), no siendo posible validar de un vistazo la dirección o URL de la página actual.

1263. Un atacante puede hacer desaparecer la barra de direcciones original, e incluso añadir la suya propia, haciéndose pasar por otro sitio web:



1264. En resumen, este tipo de ataques permite hacer creer al usuario que la página web en la que se encuentra pertenece a un sitio web, cuando en realidad pertenece a otro, técnica empleada por ejemplo en ataques de *phishing*.

1265. De nuevo, la versión iOS 5.1 (y versiones iOS 5.x previas) es vulnerable a este tipo de ataques debido a un fallo en la función windows.open() de Javascript en AppleWebKit/534.46 con Safari/7534.48.3 [Ref.- 91]:

Nota: En el momento de elaboración de la primera versión de la presente guía, esta vulnerabilidad afectaba a las últimas versiones de iOS disponibles (5.x, incluida 5.1) y a todos los últimos modelos de dispositivos móviles iOS, como iPhone4, iPhone4S, iPad2 e iPad3, y no se disponía de solución para la misma. La versión 5.1.1 [Ref.- 96] de iOS publicada a principio de mayo de 2012 finalmente solucionó esta vulnerabilidad.

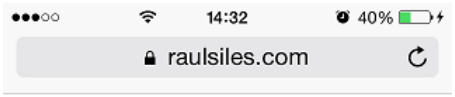
1266. Adicionalmente, versiones previas de iOS (4.x) eran vulnerables a la gestión de esquemas asociados a las URLs, o esquemas de recursos en Internet [Ref.- 93].

1267. Los esquemas de URLs definen que aplicaciones serán invocadas por el navegador web Safari en el momento de procesar una URL perteneciente a un protocolo diferente a los que el gestiona ("http:", "https:",...), como por ejemplo "tel:", que lanzaría la aplicación del "Teléfono".

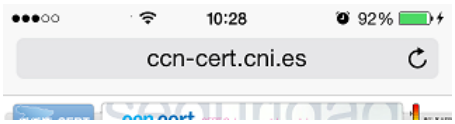
1268. Una URL o enlace de tipo "tel:" ("<iframe src=”tel:34-911234567”></iframe>") solicitará autorización por parte del usuario antes de lanzar la aplicación "Teléfono" y realizar la llamada al número de teléfono del destinatario indicado.

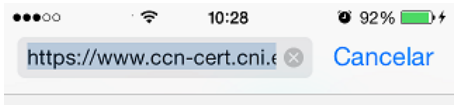
1269. Sin embargo, si el usuario dispone de Skype en el dispositivo móvil iOS, una URL o enlace de tipo "skype:" ("<iframe src=”skype://34911234567?call”></iframe>") inicia la llamada inmediatamente a través de Skype sin solicitar autorización al usuario:

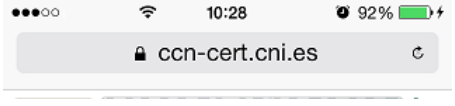
1270. En el caso de iOS 7, con el objetivo de mejorar la usabilidad y disponer de más espacio para el contenido de las páginas web, Mobile Safari oculta por defecto los detalles del sitio web visitado, mostrando únicamente el nombre del servidor web:

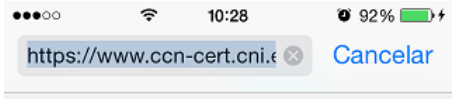


1271. Este comportamiento dificulta al usuario tanto la visualización del protocolo empleado (http o https), teniendo en cuenta (como puede verse en las imágenes) que el uso del icono del candado es inconsistente, especialmente en páginas que hacen uso tanto de contenidos http como https simultáneamente, como la verificación de los parámetros GET empleados en la URL, lo que facilita la realización de ataques web sobre los dispositivos móviles basados en iOS:



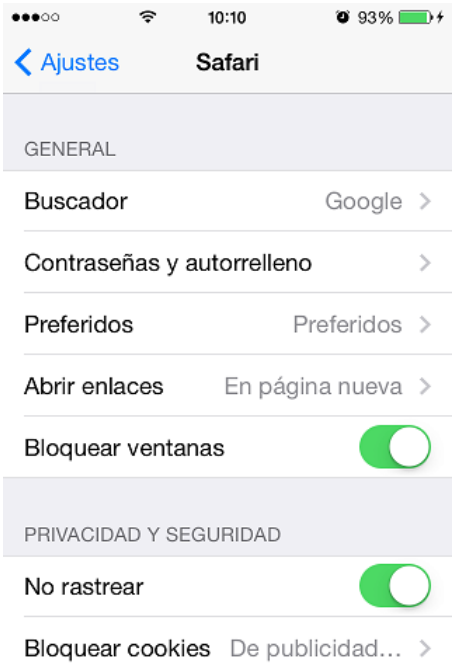






1272. La versión de Mobile Safari de iOS 7 añade la posibilidad de establecer la cabecera HTTP "Do Not Track" ("DNT") con el objetivo de que el usuario pueda especificar a los sitios web que visita que no quiere que se haga seguimiento de sus actividades.

1273. "Do Not Track" puede ser habilitado a través del menú "Ajustes - Safari - Privacidad y Seguridad" y la opción "No rastrear":



1274. Por otro lado, las capacidades de navegación privada (*Private Browsing*) de Mobile Safari en iOS 7, para evitar que se almacene en el dispositivo el histórico de navegación o las cookies, o que se sincronicen otros datos de navegación con otros dispositivos, son más accesibles, estando disponibles en la propia app de Safari.

1275. Es posible activar la navegación privada a través de la opción "Nav. privada" existente en la esquina inferior izquierda al abrir una nueva pestaña vacía. En versiones de iOS previas estas capacidades tenían que ser habilitadas desde la sección de ajustes:

1276. En el caso del iPhone (y no del iPad), el acceso a la navegación privada está también disponible desde el icono de favoritos situado en la parte inferior de Mobile Safari (con forma de libro abierto):

1277. En iOS 6 era posible hacer uso de las capacidades de Safari para autocompletar datos en formularios web, como por ejemplo información de contacto del usuario o contraseñas. En iOS 7, la configuración de Safari permite de manera granular ver y editar los datos almacenados para cada sitio web, e incluso forzar el uso de estas capacidades incluso para sitios web que intentan deshabilitarlas (no recomendado desde el punto de vista de seguridad).

1278. Esta información está disponible en el menú "Ajustes - Safari - Contraseñas y autorelleno". Las diferentes opciones disponibles permiten habilitar de manera independiente el autorelleno de los datos de contacto del usuario (opción "Usar datos de contacto", obtenidos directamente del registro del usuario en la aplicación "Contactos"), de credenciales (opción "Nombres y contraseñas") y de tarjetas de crédito (opción "Tarjetas de crédito").

1279. Para estas dos últimas categorías es posible visualizar tanto las contraseñas como las tarjetas de crédito guardadas por Mobile Safari (analizadas previamente).

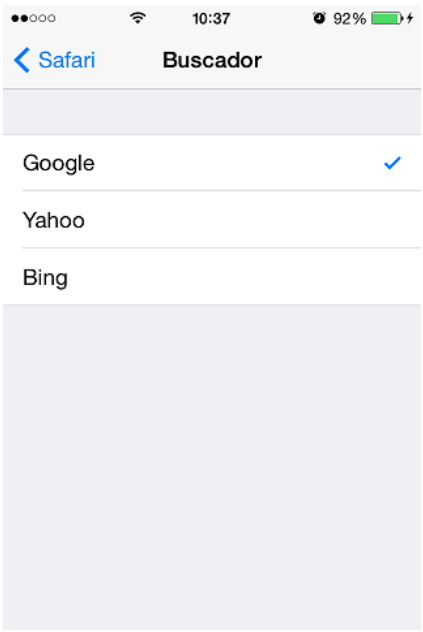
1280. Desde el punto de vista de seguridad, si se desea disponer de mayor control sobre los datos enviados a través de formularios web al hacer uso de Mobile Safari, se recomienda deshabilitar todas las opciones de autorelleno.

5.24.1 PROVEEDOR DE BÚSQUEDAS AUTOMÁTICO

1281. 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 utiliza el término como nombre de dominio (con extensión .com) y se establece una conexión con el servidor web "www.<termino>.com".

1282. Es decir, iOS no proporciona un proveedor de búsquedas por defecto en el navegador web móvil, y no realiza una búsqueda automática de dicho término a través del buscador por defecto de Safari, Google (www.google.com).

1283. Las opciones de buscadores disponibles desde el menú "Ajustes - Safari - Buscador" son Google (opción por defecto), Yahoo y Bing:



1284. En iOS 7, el menú "Campo de búsqueda inteligente" permite habilitar sugerencias del motor de búsqueda y precargar el mejor resultado, ambas opciones activas por defecto.

5.24.2 IDENTIFICACIÓN DEL NAVEGADOR WEB

1285. Cuando el navegador web accede a Internet, 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 móvil:

```
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 7 1 2 like Mac OS X)
AppleWebKit/537.51.2 (KHTML, like Gecko) Version/7.0 Mobile/11D257
Safari/9537.53
```

1286. Los detalles del dispositivo móvil incluyen la plataforma y tipo de terminal (“iPhone”), la versión de iOS (“7.1.2”), el modelo de terminal y versión de iOS concretas (“Mobile/11D257”), y la versión y los detalles del navegador web (incluyendo múltiples versiones de sus componentes), como la versión del motor WebKit ("537.51.2"), la versión de la familia genérica de Safari ("7.0") o la versión específica de Safari ("9537.53") [Ref.- 66].

1287. Se recomienda modificar el valor del agente de usuario para que no desvele información adicional, aunque iOS no proporciona ninguna funcionalidad para modificar el agente de usuario. Únicamente a través de aplicaciones de terceros disponibles en la App Store, o para dispositivos sobre los que se ha aplicado el proceso de *jailbreak*, es posible la modificación de su valor.

1288. 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.

1289. 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).

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.

1290. Los módulos de navegación web de iOS no añaden la cabecera WAP estándar que permite identificar el tipo de terminal (fabricante y modelo) y que sí es añadida por otros dispositivos móviles, "x-wap-profile". Es decir, iOS se comporta más como un dispositivo de escritorio.

1291. El UAProf (*User-Agent Profile*) es un documento XML que contiene información sobre las características y capacidades de un dispositivo móvil, estándar definido por OMA, *Open Mobile Alliance*. El documento está especificado en las cabecera HTTP "x-wap-profile" (o "Profile"), apuntando normalmente a una web del fabricante del terminal (repositorio de perfiles).

1292. 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*.

1293. En el caso de iOS no se añade la cabecera "x-wap-profile" a su tráfico HTTP y por tanto no se referencia ningún perfil, evitando desvelar detalles particulares del terminal aparte de los ya mencionados sobre el agente de usuario.

5.24.3 CONTENIDOS ADOBE FLASH

1294. Por defecto, los dispositivos móviles iOS no permiten la ejecución de contenidos Flash, política establecida originalmente en iOS por Apple [Ref.- 95], por lo que no hay soporte para esta tecnología web en el navegador web Safari y no existe la posibilidad de instalar el complemento o *plugin* para la visualización de contenidos Flash en el navegador web.

1295. Los contenidos que hacen uso de tecnologías Flash deben ser visualizados en iOS a través de aplicaciones de terceros o en otros formatos, como por ejemplo contenidos basados en tecnologías HTML5 o vídeos H.264.

1296. Adobe introdujo una excepción a esta situación con el lanzamiento de Adobe Flash Media Server 4.5 y Adobe Flash Access 3.0, siendo posible para los desarrolladores crear aplicaciones basadas en Flash para dispositivos móviles iOS, ya que las mismas harán uso de vídeos en formato HTTP Live Streaming (soportado por iOS) en lugar del formato previo, F4F.

5.24.4 CONTENIDOS ADOBE PDF

1297. iOS permite por defecto visualizar de forma nativa ficheros PDF desde el navegador web Safari (Mobile). Alternativamente, Apple proporciona una aplicación para iOS para la gestión de ficheros PDF denominada iBooks que permite la lectura de este tipo de ficheros almacenados localmente en el dispositivo móvil y no a través de un servidor web. Adicionalmente, es posible desde octubre de 2011 instalar en iOS el cliente oficial Adobe Reader desde la App Store.

1298. Debido a las numerosas vulnerabilidades de seguridad en las aplicaciones cliente de visualización de ficheros PDF durante los últimos años, se recomienda mantener actualizada la aplicación de visualización de ficheros PDF a la última versión, independientemente de si se utilizan las capacidades nativas de iOS, iBooks, Adobe Reader u otras aplicaciones de terceros.

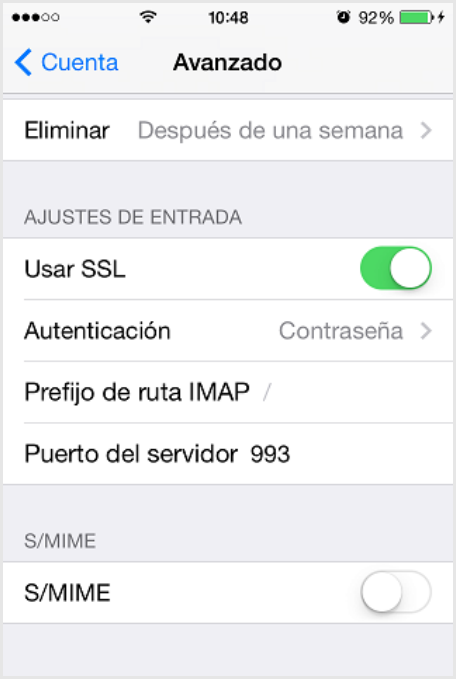
5.25 CORREO ELECTRÓNICO (E-MAIL)

1299. iOS proporciona capacidades para la gestión de correos electrónicos (e-mails) desde el dispositivo móvil, disponibles a través de la aplicación "Mail".

1300. Desde el menú “Ajustes - Correo, contactos, calend.” es posible añadir nuevas cuentas de correo a través de la opción "Añadir cuenta", como por ejemplo cuentas de iCloud, cuentas de correo de Exchange, GMail (Google Mail), Yahoo!, Aol, Outlook.com u otras generales (SMTP, IMAP, POP3...), cuyo análisis queda fuera del alcance de la presente guía.

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/TLS). Los puertos empleados por defecto para las conexiones cifradas de correo son: IMAPS (993/tcp), POP3S (995/tcp) y SMTPS (465/tcp).

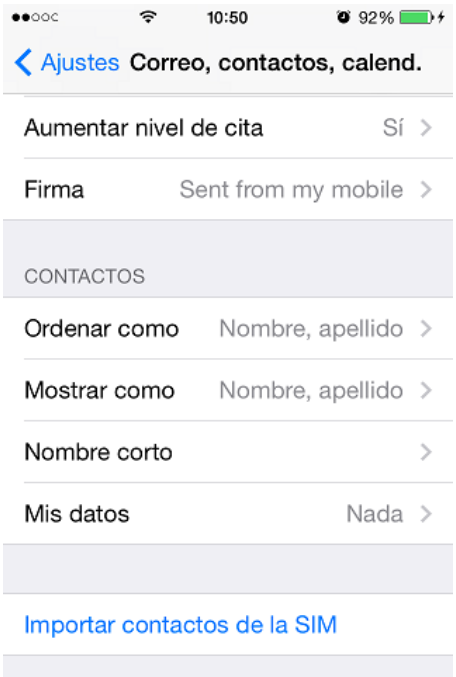
La opción está disponible para la consulta del buzón de correo (web, IMAP(S), POP3(S), etc) a través del menú "Ajustes - Correo, contactos, calend.", seleccionando la cuenta de correo y accediendo a la opción "Cuenta", mediante el botón "Avanzado". El botón "Usar SSL" debe estar habilitado para cifrar todas las comunicaciones al recibir correos electrónicos:



Adicionalmente, se dispone de la misma opción para la obtención de correos (SMTP(S)) a través del menú "Ajustes - Correo, contactos, calend.", seleccionando la cuenta de correo y accediendo a la opción "Cuenta", mediante el botón "SMTP". Seleccionando el servidor SMTP desde la opción "Servidor principal", es posible acceder al botón "Usar SSL", que de nuevo debe estar habilitado para cifrar todas las comunicaciones al enviar correos electrónicos:

1301. Respecto a las credenciales de acceso a los servidores de correo electrónico, tal como se describe en el apartado "5.19.2. Gestión de las credenciales de las cuentas de usuario", la contraseña es almacenada junto a la configuración de la cuenta para disponer de acceso inmediato y permanente al buzón de correo, no disponiéndose de ninguna opción para no almacenarla (escenario desaconsejado desde el punto de vista de seguridad).

1302. Por defecto, al escribir un nuevo mensaje de correo el dispositivo móvil iOS añade una firma que desvela el tipo de dispositivo empleado y el modelo, como por ejemplo "Enviado desde mi iPhone" o "Enviado desde mi iPad", opción desaconsejada desde el punto de vista de seguridad al revelar detalles innecesarios del dispositivo móvil:



1303. Se recomienda modificar la configuración por defecto, a través del menú "Ajustes - Correo, contactos, calend. - 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 para evitar indicar desde dónde se realiza el envío, como por ejemplo “Enviado desde mi dispositivo móvil” (ver imagen superior, en inglés).

1304. La aplicación cliente disponible por defecto, "Mail", para la gestión de correos electrónicos (e-mails) en iOS presenta diferentes debilidades de seguridad que deben ser tenidas en cuenta por los usuarios y organizaciones.

1305. Por defecto, la aplicación tiene habilitada la carga de imágenes contenidas en correos electrónicos en formato HTML. Esta funcionalidad permitiría a un potencial atacante enviar a un usuario víctima un correo electrónico con una imagen incluida (etiqueta "<img>" HTML) y automáticamente el dispositivo móvil iOS al proceder a la visualización del e-mail, solicitaría la imagen (a través de una petición HTTP GET estándar).

1306. Si la imagen referencia al servidor web del atacante, éste obtendrá la dirección IP de la víctima, su posible ubicación en base a la misma, así como los detalles del dispositivo móvil, como por ejemplo modelo y versión de iOS, a través de la cabecera HTTP "User-Agent" (ver apartado "5.24.2. Identificación del navegador web"). Todos esos detalles estarían directamente vinculados al usuario víctima al haber sido éste identificado por su dirección de e-mail.

1307. Al igual que para cargar una imagen, esta funcionalidad puede ser empleada para forzar al usuario víctima a realizar cualquier petición web empleando el método HTTP GET a través de la etiqueta "<img>".

1308. A través del menú "Ajustes - Correo, contactos, calend." es posible deshabilitar la carga automática de imágenes mediante la desactivación del botón "Cargar imágenes":

1309. En general, se recomienda modificar la configuración del cliente de correo empleado en iOS para minimizar la información desvelada a terceras partes sobre el dispositivo móvil.

5.26 REDES SOCIALES

1310. iOS 5 incluyó por defecto integración para el acceso a redes sociales en Internet con las siguientes aplicaciones cliente:

- Twitter para iOS
- YouTube

1311. En iOS 6, la aplicación por defecto de YouTube fue eliminada por Apple (parece que por un motivo de licencias), pese a estar disponible a través de la App Store posteriormente. Asimismo, iOS 6 añadió capacidades de integración con Facebook.

1312. La integración nativa de la plataforma iOS con Twitter y Facebook (a través de autentificación mediante OAuth) facilita la publicación de tweets (Twitter) y cambios de estado (Facebook) desde otras apps, como "Calendario", "Fotos", "Mapas" o "Contactos", junto al Centro de Notificaciones.

1313. En iOS 7 la integración con las redes sociales se amplió a Flickr y Vimeo desde "Fotos" (el carrete de fotografías y vídeos) o "Contactos". Estos dos servicios aparecen como opciones válidas al intentar compartir una foto en iOS 7.

1314. La ejecución de las aplicaciones de acceso a las redes sociales está disponible a través de los diferentes iconos disponibles en la pantalla principal del dispositivo móvil o a través de los ajustes de configuración.

Nota: Es posible disponer de acceso a otras redes sociales a través de las aplicaciones de terceros disponibles en la App Store, como por ejemplo Google+ (Hangouts), LinkedIn, Pinterest, Vine, etc.

5.26.1 TWITTER

1315. La aplicación de acceso a Twitter disponible por defecto en iOS, denominada “Twitter”, e integrada por completo desde iOS 5, realiza la autentificación con este servicio y el intercambio de información a través de HTTPS, y en concreto en el momento de elaboración de la versión inicial de la presente guía, mediante el protocolo TLS v1.2.

1316. La comunicación se establece con el servidor "api.twitter.com" a través de HTTPS (puerto 443/tcp), tanto para la autentificación como para el intercambio de datos, aunque se han identificado conexiones HTTP (80/tcp) sin cifrar hacia los servidores "mobile.twitter.com", "pbs.twimg.com", "abs.twimg.com", etc.

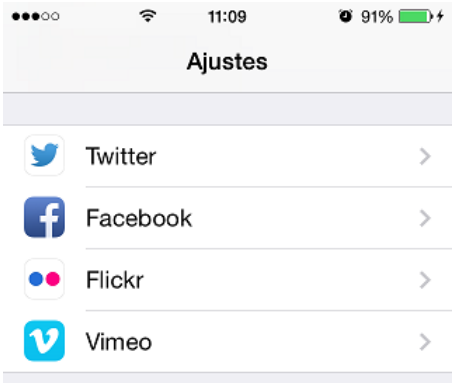
1317. El cliente de Twitter emplea el siguiente agente de usuario, desvelando tanto la versión de la aplicación Twitter como los datos del dispositivo móvil iOS:

```
User-Agent: Twitter/6.8.1 CFNetwork/672.1.15 Darwin/14.0.0
```

1318. Los accesos a los otros servidores mencionados ("*.twimg.com") solicitan imágenes, y datos en formato JSON, también cifrados empleando el mismo agente de usuario.

5.26.2 FACEBOOK, FLICKR Y VIMEO

1319. El acceso a Facebook, Flickr y Vimeo no dispone de ninguna aplicación por defecto en iOS 6 (o posterior), pese a que se dispone de la app correspondiente en la App Store, denominada "Facebook" y a su integración a través de los ajustes de configuración (donde incluso se ofrece un acceso directo para la instalación de la app desde la App Store):



5.26.3 OTRAS APPS

1320. 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 posibles comportamientos y comunicaciones vulnerables.

1321. La seguridad de las aplicaciones móviles, incluso de proveedores de servicios de referencia como Facebook, Dropbox [Ref.- 106] (PIN de acceso [Ref.- 105]), LinkedIn [Ref.- 106], o aplicaciones de entidades financieras, presentan aún en la actualidad notables debilidades y vulnerabilidades asociadas, como por ejemplo en el almacenamiento inseguro de datos confidenciales o sensibles.

1322. Por ejemplo, en abril de 2012 un investigador reportó que la aplicación móvil para iOS de Facebook almacenaba las credenciales de OAuth necesarias para el acceso al servicio sin cifrar en los ficheros (.plist) asociados a la aplicación en iOS [Ref.- 106]. Un atacante sólo requiere disponer de acceso físico temporal a un dispositivo para acceder a dichos ficheros y obtener las credenciales, lo que le permitiría suplantar al usuario en Facebook.

1323. En otros casos, la existencia de (potenciales) vulnerabilidades en aplicaciones, ha llevado a que Apple retire temporalmente de la App Store versiones concretas de aplicaciones, como por ejemplo WhatsApp.

5.27 APLICACIONES DE TERCEROS: APP STORE

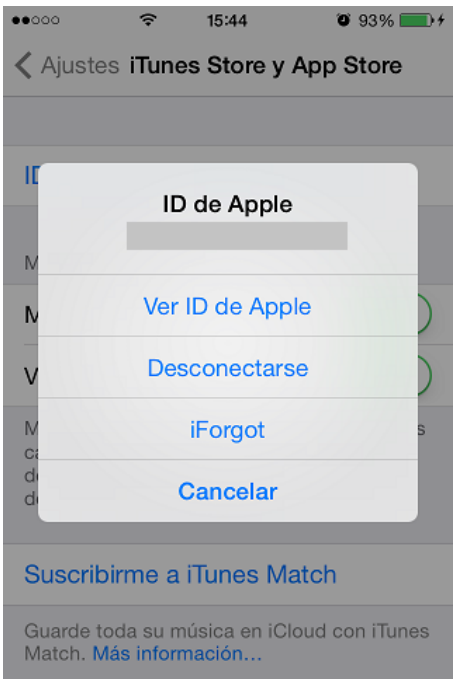
1324. La plataforma App Store [Ref.- 4] es empleada por Apple para la distribución y comercialización de aplicaciones móviles y software para los dispositivos móviles iOS.

1325. iOS incluye una aplicación, denominada "App Store", disponible desde la pantalla principal del dispositivo móvil, para el acceso a este servicio directamente desde el dispositivo, lo que permite la instalación de aplicaciones Over-the-Air (OTA) a través de redes Wi-Fi o 2/3/4G:

1326. Adicionalmente es posible llevar a cabo la instalación de aplicaciones en dispositivos móviles iOS a través de iTunes, ya sea mediante Wi-Fi o a través de su conexión con un ordenador vía cable USB.

1327. La primera vez que se utiliza App Store es necesario asociar un Apple ID (si no se ha configurado uno todavía en el dispositivo móvil), disponiendo el usuario de opciones para dar de alta o crear un identificador nuevo, tras aceptar los términos del servicio.

1328. Posteriormente, desde el menú "Ajustes - iTunes Store y App Store" es posible identificar en la parte superior el Apple ID asociado para el acceso a la App Store, así como ver la información para dicho identificador (tras introducir la contraseña asociada), desconectar el uso de dicho identificador del dispositivo móvil, o invocar el proceso de restauración de la contraseña (denominado iForgot):



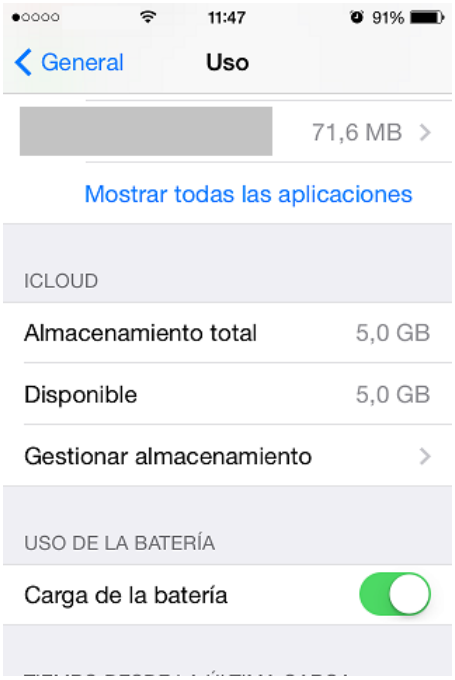
1329. La obtención de información de la cuenta, así como otras gestiones, se realiza mediante HTTPS hacia los servidores "configuration.apple.com", "metrics.apple.com" y "itunes.apple.com". Adicionalmente se establecen conexiones HTTP no cifradas hacia "ax.init.itunes.apple.com" (recurso "/bag.xml?ix=2&dsid=..."), para solicitar información adicional ("bag"; ver apartado "**¡Error! No se encuentra el origen de la referencia.**. **¡Error! No se encuentra el origen de la referencia.**").

1330. La conexión de autentificación hacia la App Store empleando el Apple ID se realiza a través de HTTPS, pero las consultas de información en App Store, por ejemplo al visualizar las aplicaciones disponibles o ver los detalles y descripción de una aplicación, emplean conexiones HTTP no cifradas para la carga de imágenes principalmente contra los servidores "a*N*.mzstatic.com", empleando el agente de usuario de la aplicación "iTunes", que desvela una vez más numerosos detalles del dispositivo móvil:

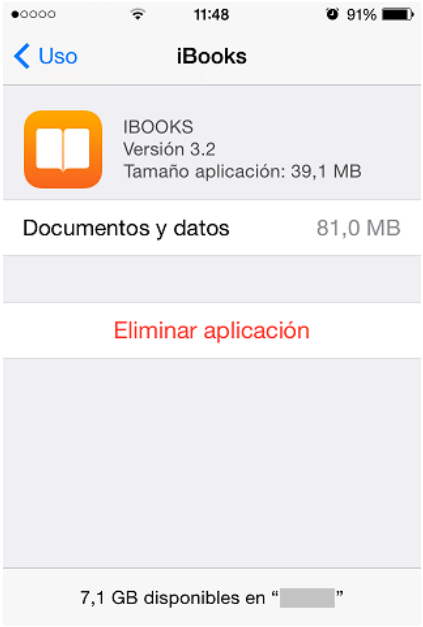
```
User-Agent: AppStore/2.0 iOS/7.1.2 model/iPhone4,1 build/11D257 (6;
dt:78)
```

1331. Se recomienda actualizar a la última versión de las aplicaciones ya instaladas en el dispositivo móvil (ver apartado “5.28. Actualización de aplicaciones (cliente) en iOS”), ya que éstas proporcionarán posibles soluciones disponibles frente a vulnerabilidades de seguridad conocidas.

1332. La lista de programas o aplicaciones instaladas desde la App Store es accesible desde el menú "Ajustes - General - Uso", bajo la sección "Almacenamiento", incluyendo el espacio de almacenamiento utilizado por cada una de ellas. Adicionalmente, mediante la opción "Mostrar todas las aplicaciones" es posible acceder al listado completo de aplicaciones instaladas en el dispositivo móvil iOS:



1333. Seleccionando cualquiera de las aplicaciones es posible obtener los detalles de almacenamiento utilizados por la propia aplicación, y por sus documentos y datos:



1334. La información de las aplicaciones del usuario también está disponible directamente desde un ordenador con iTunes, a través de "Library - Apps" o de "Store - iTunes Store - Historial de compras (Ver el repertorio)". En este caso la lista de aplicaciones mostradas está vinculada a la librería de iTunes, a través de uno o varios Apple IDs, y sólo se dispone de los detalles de qué aplicación está actualmente instalada en qué dispositivo móvil iOS cuando se establece una conexión de sincronización entre el dispositivo móvil e iTunes.

1335. Debe tenerse en cuenta que la disponibilidad de una aplicación en la App Store 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, pese a haber sido revisada por Apple mediante su proceso de aceptación y publicación de nuevas aplicaciones. Apple ya ha retirado múltiples aplicaciones de la App Store por este motivo [Ref.- 1].

1336. En algunos casos, la utilización de una aplicación móvil propietaria para el acceso a un servicio web presenta ciertas ventajas frente al acceso estándar a través del navegador web, Mobile Safari en el caso de iOS, considerando que ha sido desarrollada de forma segura y que no presenta vulnerabilidades.

1337. Por ejemplo, la aplicación propietaria ejecutará dentro de su propio *sandbox*, disponiendo de un mayor control y gestión sobre los datos de los que hace uso, y no compartiendo datos con otros servicios web, por ejemplo a través de la caché de Safari. Por otro lado la aplicación puede forzar el cifrado local de todos sus datos, o hacer uso de datos cuando no se dispone de conectividad (*offline*).

1338. El uso de este tipo de aplicaciones en entornos móviles muy restringidos podría permitir incluso deshabilitar la utilización de Safari en iOS.

1339. Se recomienda analizar en detalle el contenido y procedencia de una aplicación de terceros antes de instalarla desde la App Store en el dispositivo móvil.

1340. El UDID es un identificador único del dispositivo móvil (hardware) asociado a cada dispositivo móvil iOS, de 40 caracteres, similar a un número de serie, y que puede ser obtenido desde iTunes, seleccionando el dispositivo y pulsando sobre el campo del

número de serie, o a través de la utilidad de configuración del iPhone (ver apartado "5.3.3. Utilidad de configuración del iPhone").

1341. Este identificador (UDID) es empleado, por ejemplo, para el control en la distribución de aplicaciones móviles en fase beta o de pruebas. Con el objetivo de proteger la privacidad de los usuarios, en 2012 Apple comenzó a bloquear el acceso al mismo desde las aplicaciones móviles, evitando así las actividades de seguimiento de los usuarios realizadas por algunas aplicaciones y compañías [Ref.- 113].

5.27.1 CONFIGURACIÓN REMOTA DE APPS GESTIONADAS

1342. iOS 7 proporciona capacidades de gestión empresarial (MDM) para la configuración remota, centralizada y a gran escala de apps gestionadas en los dispositivos móviles de Apple.

1343. Las apps gestionadas son aquellas apps provisionadas a través de un App Store empresarial o corporativo, y son gestionadas desde una solución MDM, pudiendo hacer uso de las capacidades extendidas de gestión introducidas en iOS 7, como Per-app VPNs, Managed Open In o Feedback.

1344. Estas capacidades permiten configurar y personalizar una app gestionada dentro de una organización en función de la región, el departamento, o incluso el usuario individual o dispositivo móvil específico.

1345. Se recomienda por tanto, siempre que sea posible, tratar las apps como apps gestionadas o de negocio e instalarlas desde el App Store corporativo para poder aprovechar todas las capacidades de gestión disponibles, frente a realizar su instalación como app personal desde el App Store oficial y público.

1346. En aquellos casos dónde ya existan apps personales instaladas en los dispositivos de los usuarios que vayan a ser utilizadas como apps empresariales o de negocio, se recomienda llevar a cabo su despliegue como apps gestionadas y la migración correspondiente.

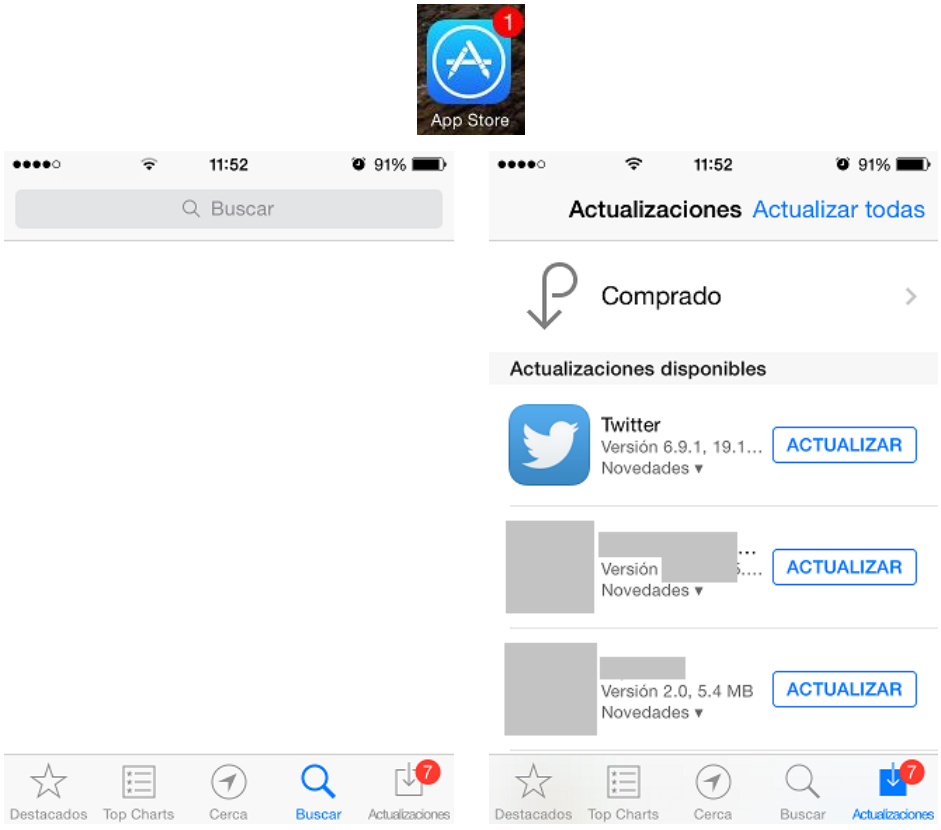
5.28 ACTUALIZACIÓN DE APLICACIONES (CLIENTE) EN IOS

1347. El término aplicaciones cliente engloba al conjunto de aplicaciones de terceros que son compatibles con iOS y que pueden ser instaladas sobre este sistema operativo.

Nota: Apple únicamente permite la instalación de aplicaciones de terceros oficiales en dispositivos móviles iOS desde la App Store.

La aplicación "App Store" no puede ser utilizada si no se dispone de conectividad de datos hacia Internet (Wi-Fi o 2/3/4G), mostrándose los siguientes mensajes de error:

1348. Una vez el dispositivo móvil establece conexión con la App Store a través de la aplicación "App Store", iOS comprueba automáticamente la última versión disponible de las aplicaciones instaladas en el dispositivo móvil, la compara con la versión instalada en el terminal, y ofrece al usuario instalar la nueva versión a través de una notificación en la sección "Actualizar" (y en el icono de "App Store"):



1349. El menú "App Store - Actualizaciones" permite disponer de acceso a las nuevas versiones de las aplicaciones que ya están instaladas en el dispositivo móvil.

1350. Desde la versión 6 de iOS es posible llevar a cabo la actualización de aplicaciones directamente desde el dispositivo móvil empleando la app "App Store" (“App Store - Actualizaciones”) en segundo plano, mientras se hace uso del dispositivo móvil para otras tareas, y además no se solicitará al usuario la contraseña de su Apple ID en la App Store a la hora de actualizar aplicaciones ya instaladas (tal y como ocurría en versiones previas de iOS, como 5.x), sino únicamente para llevar a cabo la instalación de nuevas apps.

1351. Para llevar a cabo las actualizaciones se utilizan comunicaciones HTTPS cifradas hacia los servidores “itunes.apple.com” y “client-api.itunes.apple.com”, que además hacen uso de técnicas de *certificate pinning* para evitar la intercepción del tráfico de red.

1352. Únicamente se hace uso de HTTP para el envío de peticiones no cifradas correspondientes a las imágenes de las apps en la App Store a través de los servidores "a*N*.mzstatic.com".

1353. Teóricamente, la integridad de las aplicaciones de iOS se verifica a través de una firma digital asociada al fichero binario (.ipa, "iPhone App") descargado, que se complementa con la utilización de cifrado mediante HTTPS para evitar la manipulación de este intercambio de datos.

1354. El acceso "Comprado" del menú "App Store - Actualizaciones" permite acceder al histórico, y a la potencial descarga, de apps compradas previamente por el usuario en el pasado:

1355. Adicionalmente, es posible llevar a cabo la desinstalación de una aplicación desde el menú "Ajustes - General - Uso", tras seleccionarla de la lista de aplicaciones instaladas, mediante el botón “Eliminar aplicación”.

1356. Alternativamente las aplicaciones pueden ser eliminadas manteniendo pulsado su icono asociado en la pantalla principal del dispositivo móvil, mediante el botón que muestra una cruz.

1357. 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.

1358. La información respecto a las actualizaciones de software y descargas disponibles para las aplicaciones de iOS está disponible en la App Store.

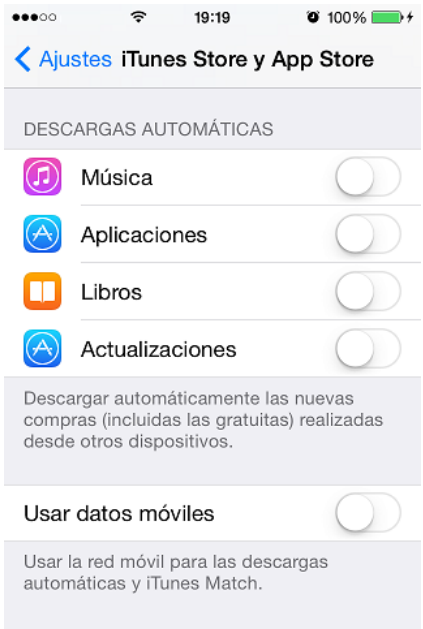
1359. La instalación de actualizaciones de software y aplicaciones en iOS, ya que todas las aplicaciones se han obtenido a través de la App Store, conlleva un proceso homogéneo, facilitando el proceso de actualización para usuarios no experimentados y aumentando el nivel de seguridad de los dispositivos móviles al agilizar el proceso de sustitución de software vulnerable.

1360. Los dispositivos supervisados basados en iOS7 tienen la capacidad de recibir actualizaciones de las apps de manera silenciosa, sin requerir la autorización por parte del usuario. Se considera que los dispositivos móviles supervisados pertenecen a la organización y no requieren por tanto de la autorización explícita del usuario para su gestión.

1361. Estas capacidades aplican tanto a apps publicas como corporativas. Sin embargo, en el caso de las apps públicas, el usuario será consciente de la actualización ya que le será solicitado su Apple ID.

1362. Por otro lado, y de manera complementaria tanto para dispositivos gestionados como no, iOS 7 permite al usuario configurar el dispositivo para que lleve a cabo actualizaciones automáticas tan pronto se identifique que existe una nueva versión de una app, sin que el usuario tenga que intervenir en el proceso de actualización.

1363. Desde el menú "Ajustes - iTunes Store y App Store" y la opción "Descargas automáticas - Actualizaciones" es posible habilitar la descarga automática de actualizaciones para las apps ya instaladas en el dispositivo móvil sin solicitar la autorización del usuario:



1364. La opción inferior "Usar datos móviles" permite determinar si la descarga automática de actualizaciones para las apps se realizará únicamente cuando se disponga de conectividad a través de una red Wi-Fi, o también a través de las redes de telefonía móvil 2/3/4G (con los posibles gastos de tráfico de datos asociados).

1365. Esta funcionalidad, aunque puede ser muy conveniente desde el punto de vista de seguridad para usuarios finales, al automatizar y facilitar la aplicación de actualizaciones, debe ser gestionada adecuadamente en entornos empresariales.

1366. En entornos empresariales se recomienda que antes de permitir la instalación y utilización en producción de una nueva versión de una app, ésta sea analizada y probada convenientemente para evaluar si la nueva funcionalidad introduce debilidades o vulnerabilidades de seguridad no permitidas por la organización.

1367. La información detallada de qué apps han sido actualizadas, ya sea manual o automáticamente, está disponible a través del Centro de Notificaciones (categoría "Todo"), o desde la app "App Store - Actualizaciones", mostrándose un histórico reciente de actualizaciones ordenadas cronológicamente por fecha (de más a menos reciente).

Nota: Adicionalmente existen numerosas aplicaciones cliente o *suites* de software comercial disponibles a través de la App Store cuyo objetivo es aumentar el nivel de seguridad del dispositivo móvil iOS, como *suites* o soluciones de seguridad con antivirus o antimalware (ej. Intego VirusBarrier iOS, LookOut Mobile Antivirus, etc) , aunque las mismas no disponen de la funcionalidad de un antivirus (AV) tradicional, ya que por política Apple no permite la coexistencia de AV en iOS.

6 APÉNDICE B: CAPTURA DE LA PANTALLA EN IOS

1368. Por defecto iOS 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 *jailbreak* del dispositivo móvil.

1369. Sin embargo, iOS dispone de capacidades nativas para capturar la pantalla. Mediante la pulsación de las teclas de encendido/apagado ("On/Off" o "Power") y el botón de inicio ("Home") simultáneamente en el dispositivo móvil, se llevará a cabo una captura de la pantalla del dispositivo y se almacenará junto al resto de las fotos de la cámara.

7 REFERENCIAS

La siguiente tabla muestra las fuentes de información a las que se hace referencia a lo largo de la presente guía:

NOTA: A todas las referencias mostradas a continuación con el formato "http://support.apple.com/kb/NNNN" se les puede añadir el parámetro "?viewlocale=es_ES" para traducirlas del inglés al español (si están disponibles). Debe tenerse en cuenta que la versión en español podría no estar tan actualizada como la versión en inglés.

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]	iPhone. Apple. URL: http://www.apple.com/iphone/
[Ref.- 3]	iOS. Apple. URL: http://www.apple.com/iphone/ios/
[Ref.- 4]	App Store. Apple. URL: http://www.itunes.com/appstore/ (requiere iTunes) URL: http://itunes.apple.com/us/genre/mobile-software-applications/id36?mt=8 (no requiere iTunes)
[Ref.- 5]	"iOS 5.1.1 Software Update". Apple. Mayo 2012. URL: http://support.apple.com/kb/DL1521
[Ref.- 6]	"About the security content of iOS 5.0.1 Software Update". Apple. Noviembre 2011. URL: http://support.apple.com/kb/HT5052
[Ref.- 7]	"About the security content of iOS 5.1.1 Software Update". Apple. Mayo 2012. URL: http://support.apple.com/kb/HT5278
[Ref.- 8]	"Apple Security Updates". Apple. 2011-2012. URL: http://support.apple.com/kb/HT1222
[Ref.- 9]	"Apple security updates (2010)". Apple. 2010. URL: http://support.apple.com/kb/HT5165
[Ref.- 10]	"Apple security updates (15-Jan-2008 to 03-Dec-2009)". Apple. 2008-2009. URL: http://support.apple.com/kb/HT4218
[Ref.- 11]	"Exchange ActiveSync and iOS 5 Devices". Apple. URL: http://help.apple.com/iosdeployment-exchange/ URL: http://images.apple.com/iphone/business/docs/iOS_EAS.pdf
[Ref.- 12]	"iPhone Support – Enterprise". Apple. URL: http://www.apple.com/support/iphone/enterprise/
[Ref.- 13]	"Deploying iPhone and iPad - Security Overview". Apple URL: http://images.apple.com/iphone/business/docs/iOS_Security.pdf
[Ref.- 14]	iOS Developer Library. Apple. URL: https://developer.apple.com/library/ios/navigation/
[Ref.- 15]	"iPhone in Business" (& Resources). Apple. URL: https://www.apple.com/iphone/business/ URL: https://www.apple.com/iphone/business/resources/
[Ref.- 16]	"Deploying iTunes for iOS Devices". Apple. URL: http://help.apple.com/iosdeployment-itunes/
[Ref.- 17]	"iCloud: iCloud security and privacy overview". Apple. URL: http://support.apple.com/kb/HT4865
[Ref.- 18]	"Mobile Device Management Overview". Apple. URL: http://www.apple.com/business/mdm
[Ref.- 19]	"The Apple Sandbox". Dionysus Blazakis. Independent Security Evaluators. Enero 2011. URL: http://securityevaluators.com/files/papers/apple-sandbox.pdf
[Ref.- 20]	"iOS 3.x: List of available trusted root certificates". Apple. URL: http://support.apple.com/kb/HT3580 URL: https://support.apple.com/kb/HT2185 (iOS 2.x)
[Ref.- 21]	"iOS 4.x: List of available trusted root certificates". Apple. URL: https://support.apple.com/kb/HT4415

Referencia	Título, autor y ubicación
[Ref.- 22]	"iOS 5 and iOS 6: List of available trusted root certificates". Apple. URL: http://support.apple.com/kb/HT6167
[Ref.- 23]	"App Sandbox Design Guide". 2012-02-16. Apple. URL: http://developer.apple.com/library/mac/documentation/Security/Conceptual/AppSandboxDesignGuide/AppSandboxDesignGuide.pdf
[Ref.- 24]	"iOS App Programming Guide". 2012-03-07. Apple. URL: http://developer.apple.com/library/ios/documentation/iphone/conceptual/iphoneosprogrammingguide/iphoneappprogrammingguide.pdf
[Ref.- 25]	"About the security content of iOS 4". Apple. Noviembre 2011. URL: https://support.apple.com/kb/HT4225
[Ref.- 26]	"Mobile Application Security". Himanshu Dwivedi, Chris Clark, David Thiel. McGraw-Hill. ISBN: 0071633561. 2010. URL: http://www.mhprofessional.com/product.php?isbn=0071633561
[Ref.- 27]	"iOS Dev Center". Apple. URL: http://developer.apple.com/iphone/ URL: https://developer.apple.com/programs/ios/
[Ref.- 28]	"iOS Code Signing Setup, Process, and Troubleshooting (Technical Note TN2250)". iOS Developer Library. Apple. URL: https://developer.apple.com/library/ios/#technotes/tn2250/_index.html
[Ref.- 29]	"App Store Review Guidelines". Apple. URL: https://developer.apple.com/appstore/guidelines.html
[Ref.- 30]	"Bypassing iPhone Code Signatures". Jay Freeman (saurik). URL: http://www.saurik.com/id/8
[Ref.- 31]	"Apple: App Access to Contact Data Will Require Explicit User Permission". All Things D. Febrero 2012. URL: https://allthingsd.com/20120215/apple-app-access-to-contact-data-will-require-explicit-user-permission/ URL: http://www.imore.com/2012/02/12/path-apps-accessing-contacts-inspiration-android/
[Ref.- 32]	"Lost iPhone? Lost Passwords!. Practical Consideration of iOS Device Encryption Security". Fraunhofer SIT. Febrero 2011. URL: http://sit.sit.fraunhofer.de/studies/en/sc-iphone-passwords.pdf URL: http://sit4.me/iphone-keychain-faq URL: http://www.youtube.com/watch?v=uVGiNAs-QbY
[Ref.- 33]	"ElcomSoft Breaks iPhone Encryption, Offers Forensic Access to File System Dumps". ElcomSoft. Mayo 2011. URL: http://blog.crackpassword.com/2011/05/elcomsoft-breaks-iphone-encryption-offers-forensic-access-to-file-system-dumps/ URL: http://blog.crackpassword.com/2011/05/extracting-the-file-system-from-iphone-ipad-ipod-devices/
[Ref.- 34]	"iPhone Data Protection In-Depth". Sogeti/ESEC. 2011. URL: http://esec-lab.sogeti.com/dotclear/public/publications/11-hitbamsterdam-iphonedataprotection.pdf URL: https://code.google.com/p/iphone-dataprotection/
[Ref.- 35]	"Bypassing iPhone 3G[s] Encryption". Jonathan Zdziarski. Julio 2009. URL: http://www.zdziarski.com/blog/?p=516
[Ref.- 36]	"iOS: Understanding data protection". Apple. Octubre 2011. URL: http://support.apple.com/kb/HT4175
[Ref.- 37]	"Want to Fool Apple's App Store? Plant an Easter Egg". Wired. Mayo 2009. URL: http://www.wired.com/gadgetlab/2009/05/appstoreeasteregg/
[Ref.- 38]	"iPhone Security Bug Lets Innocent-Looking Apps Go Bad". Forbes. 2011. URL: http://www.forbes.com/sites/andygreenberg/2011/11/07/iphone-security-bug-lets-innocent-looking-apps-go-bad/
[Ref.- 39]	"Secret URL May Allow Apple to Delete Your iPhone Apps Remotely". Wired. Agosto 2008. URL: http://www.wired.com/gadgetlab/2008/08/secret-url-allo/ URL: http://www.wired.com/gadgetlab/2008/08/apple-sells-60/

Referencia	Título, autor y ubicación
[Ref.- 40]	"Bad Siri! She'll let anyone use a locked iPhone 4S". CNet. Octubre 2011. URL: http://news.cnet.com/8301-27080_3-20122632-245/bad-siri-shell-let-anyone-use-a-locked-iphone-4s/
[Ref.- 41]	"Anyone with a Smart Cover can break into your iPad 2". 9 to 5 mac. Octubre 2011. URL: http://9to5mac.com/2011/10/20/anyone-with-a-smart-cover-can-break-into-your-ipad-2/ URL: http://bringyourownit.com/2011/10/24/consumerization-and-mobile-security/
[Ref.- 42]	JailbreakMe. Comex. URL: http://www.jailbreakme.com URL: http://esec-lab.sogeti.com/post/Analysis-of-the-jailbreakme-v3-font-exploit
[Ref.- 43]	"About the security content of iOS 4.3.4 Software Update". Apple. Julio 2011. URL: http://support.apple.com/kb/HT4802 URL: https://github.com/comex/pdfpatch2 (parche no oficial)
[Ref.- 44]	"Apple iOS 4 Security Evaluation". Dino A. Dai Zovi. Trails of Bits LLS. URL: http://www.trailofbits.com/resources/ios4_security_evaluation_slides.pdf URL: http://www.trailofbits.com/resources/ios4_security_evaluation_paper.pdf
[Ref.- 45]	"iOS 5 data protection updates". Sogeti ESEC Lab. Octubre 2011. URL: http://esec-lab.sogeti.com/post/iOS-5-data-protection-updates
[Ref.- 46]	"iPhone security model & vulnerabilities". Sogeti / ESEC. HITB SecConf 2010. 2010. URL: http://esec-lab.sogeti.com/dotclear/public/publications/10-hitbkl-iphone.pdf
[Ref.- 47]	"iOS: Syncing with iTunes". Apple. Noviembre 2011. URL: https://support.apple.com/kb/HT1386 URL: https://support.apple.com/kb/TS4062
[Ref.- 48]	"iOS: cómo realizar una copia de seguridad". Apple. Octubre 2011. URL: https://support.apple.com/kb/HT1766?viewlocale=es_ES
[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]	"iTunes: acerca de las copias de seguridad de iOS". Apple. Marzo 2012. URL: http://support.apple.com/kb/HT4946?viewlocale=es_ES
[Ref.- 51]	"Guía CCN-STIC-418: Seguridad en Bluetooth". CCN-CERT. URL: https://www.ccn-cert.cni.es - Herramientas – Series CCN-STIC
[Ref.- 52]	"iCloud: información general sobre copias de seguridad y restauraciones". Apple. Octubre 2011. URL: http://support.apple.com/kb/HT4859?viewlocale=es_ES
[Ref.- 53]	"iCloud". Apple. URL: https://www.apple.com/icloud/
[Ref.- 54]	"iPhone OS Enterprise Deployment Guide" (Second Edition, for version 3.2 or later). Apple. 2010. URL: http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf
[Ref.- 55]	"iOS: cómo sincronizar o transferir contenidos a tu ordenador". Apple. Octubre 2011. URL: https://support.apple.com/kb/HT1296?viewlocale=es_ES
[Ref.- 56]	"Siri". Apple. 2011. URL: http://www.apple.com/iphone/features/siri.html URL: http://www.apple.com/iphone/features/siri-faq.html
[Ref.- 57]	"Waiting for Siri: Why Apple's Personal Assistant Isn't on the iPad (Yet)". Apple. Marzo 2012. URL: http://www.informit.com/articles/article.aspx?p=1854712
[Ref.- 58]	"iOS: Wrong passcode results in red disabled screen". Apple. 2011. URL: http://support.apple.com/kb/ht1212
[Ref.- 59]	"MobileMe: Troubleshooting Find My iPhone". Apple. 2012. URL: http://support.apple.com/kb/TS2734
[Ref.- 60]	"iOS 5 Security Flaw Allows Access To Contacts List, Recent Calls & Text Messages Without Passcode". iPhoneIslam. Febrero 2012. URL: http://www.cultofmac.com/147700/ios-5-security-flaw-allows-access-to-contacts-list-recent-calls-text-messages-without-passcode/
[Ref.- 61]	"About the security content of iOS 5.1 Software Update". Apple. Marzo 2012. URL: http://support.apple.com/kb/HT5192
[Ref.- 62]	"Deploying iPhone and iPad: Digital Certificates". Apple. Marzo 2012. URL: http://images.apple.com/ipad/business/docs/iOS_Certificates_Mar12.pdf

Referencia	Título, autor y ubicación
[Ref.- 63]	"iOS: ¿cómo funciona "Borrar contenidos y ajustes"?". Apple. Marzo 2012. URL: http://support.apple.com/kb/ht2110?viewlocale=es_ES
[Ref.- 64]	"iOS 5: Understanding Location Services". Apple. 2011. URL: http://support.apple.com/kb/HT4995 (iOS 5) URL: http://support.apple.com/kb/HT1975 (iOS 4)
[Ref.- 65]	"Assisted GPS (A-GPS)". Wikipedia. 2012. URL: http://en.wikipedia.org/wiki/Assisted_GPS
[Ref.- 66]	"Optimizing Web Content". Apple. URL: https://developer.apple.com/library/safari/#documentation/AppleApplications/Reference/SafariWebContent/OptimizingforSafarioniPhone/OptimizingforSafarioniPhone.html
[Ref.- 67]	"iOS: System requirements for Personal Hotspot". Apple. 2012. URL: http://support.apple.com/kb/HT3574
[Ref.- 68]	"iOS: Understanding Personal Hotspot". Apple. 2012. URL: http://support.apple.com/kb/HT4517 URL: http://support.apple.com/kb/TS2756
[Ref.- 69]	"iOS Hardening Configuration Guide: For iPod Touch, iPhone and iPad running iOS 5.1 or higher". DoD Australian Government. March 2012. URL (5.x): http://dsd.gov.au/publications/iOS5_Hardening_Guide.pdf URL (4.x): http://dsd.gov.au/publications/iOS_Hardening_Guide.pdf URL (iOS 7.0.6+): http://www.asd.gov.au/publications/iOS7_Hardening_Guide.pdf
[Ref.- 70]	"iOS: Updating your carrier settings" & "iPhone: Locating wireless carriers". Apple. 2012. URL: http://support.apple.com/kb/ht1970 & URL: http://support.apple.com/kb/ht1937
[Ref.- 71]	"iPhone Configuration Utility (IPCU)". Apple. URL: http://support.apple.com/kb/DL1465 (OS X) URL: http://support.apple.com/kb/DL1466 (Windows)
[Ref.- 72]	"Busca las diferencias en las direcciones inalámbricas - WiFi y BlueTooth - de tus dispositivos Apple (2 partes)". Raúl Siles. Seguridad Apple. Abril 2011. URL: http://www.seguridadapple.com/2011/04/busca-las-diferencias-en-las.html URL: http://www.seguridadapple.com/2011/05/busca-las-diferencias-en-las.html
[Ref.- 73]	"iOS: conexión a Internet". Apple. Marzo 2012. URL: http://support.apple.com/kb/HT1695?viewlocale=es_ES
[Ref.- 74]	"Despliegue del iPhone y el iPad: Wi-Fi". Apple. 2011. URL: http://images.apple.com/es/iphone/business/docs/iOS_WiFi.pdf
[Ref.- 75]	"iPhone OS: Guía de integración en empresas" (segunda edición). Apple. 2010. URL: http://manuals.info.apple.com/es_ES/Guia_de_integracion_en_empresas.pdf
[Ref.- 76]	"iOS: About cellular data usage". Apple. 2011. URL: http://support.apple.com/kb/HT4146
[Ref.- 77]	"Description of the Wireless Client Update for Windows XP with Service Pack 2". Microsoft. 2010. URL: http://support.microsoft.com/kb/917021
[Ref.- 78]	"iMessage". Apple. 2011. URL: http://www.apple.com/iphone/built-in-apps/messages.html
[Ref.- 79]	"iOS: Descripción de las redes de datos móviles". Apple. 2012. URL: http://support.apple.com/kb/HT1976?viewlocale=es_ES
[Ref.- 80]	"iOS: acerca de los ajustes de red de datos móviles (cómo ver o editar el APN)". Apple. 2011. URL: http://support.apple.com/kb/HT2283?viewlocale=es_ES
[Ref.- 81]	"Gestión insegura de redes WiFi en iOS". Seguridad Apple. Junio 2011. URL: http://www.seguridadapple.com/2011/06/gestion-insegura-de-redes-wifi-en-ios.html
[Ref.- 82]	"iOS: perfiles de Bluetooth compatibles". Apple. Octubre 2013. URL: http://support.apple.com/kb/HT3647?viewlocale=es_ES
[Ref.- 83]	"Wi-Fi (In)Security - All Your Air Are Belong To...". Raúl Siles. GOVCERT. 2010. URL: http://www.taddong.com/docs/Wi-Fi_(In)Security_GOVCERT-2010_RaulSiles_Taddong_v1.0_2pages.pdf
[Ref.- 84]	"CellCrypt Mobile for iPhone". CellCrypt. 2011. URL: http://www.cellcrypt.com/cellcrypt-mobile-iphone

Referencia	Título, autor y ubicación
[Ref.- 85]	"Hacking y seguridad en comunicaciones móviles GSM/GPRS/UMTS/LTE ". David Pérez y José Picó. Taddong. 2011. URL: http://www.informatica64.com/libros.aspx?id=hmoviles
[Ref.- 86]	"Acerca del contenido de seguridad de iOS 4.3". Apple. 2011. URL: http://support.apple.com/kb/HT4564?viewlocale=es_ES
[Ref.- 87]	"CVE-2011-0228". Apple. 2011. URL: http://support.apple.com/kb/HT4824 URL: http://blog.recurity-labs.com/archives/2011/07/26/cve-2011-0228_ios_certificate_chain_validation_issue_in_handling_of_x_509_certificates/index.html URL: https://issl.recurity.com/ URL: https://www.trustwave.com/spiderlabs/advisories/TWSL2011-007.txt
[Ref.- 88]	"Technical Note TN2287 - iOS 5 and TLS 1.2 Interoperability Issues". Apple. 2011. URL: http://developer.apple.com/library/ios/#technotes/tn2287/_index.html URL: http://www.opensource.apple.com/source/libsecurity_ssl/
[Ref.- 89]	"iPhone - Security 101". Raúl Siles. RaDaJo. Febrero 2008. URL: http://www.radajo.com/2008/02/iphone-security-101.html
[Ref.- 90]	"UI Spoofing Safari on the iPhone ". Nitesh Dhanjani. Noviembre 2010. URL: http://www.dhanjani.com/blog/2010/11/ui-spoofing-safari-on-the-iphone-.html URL: http://www.dhanjani.com/ios-safari-ui-spoofing/
[Ref.- 91]	"[MajorSecurity-SA-2012-014]Apple Safari on iOS 5.1 - Adressbar spoofing vulnerability". David Vieira-Kurz. MajorSecurity. Marzo 2012. URL: http://www.majorsecurity.net/safari-514-ios51-advisory.php URL: http://majorsecurity.net/html5/ios51-demo.html
[Ref.- 92]	"[TAD-2011-003] Vulnerability in Android: To add, or not to add (a Wi-Fi network), that is the question". Raúl Siles. Taddong. Mayo 2010. URL: http://blog.taddong.com/2011/05/vulnerability-in-android-to-add-or-not.html
[Ref.- 93]	"Insecure Handling of URL Schemes in Apple's iOS". Nitesh Dhanjani. Noviembre 2010. URL: http://www.dhanjani.com/blog/2010/11/insecure-handling-of-url-schemes-in-apples-ios.html
[Ref.- 94]	"Client Certificate Support Across Mobile Platforms – A Summary". MobilityDojo. Diciembre 2010. URL: http://mobilitydojo.net/2010/12/28/client-certificate-support-across-mobile-platforms-a-summary/
[Ref.- 95]	"Thoughts on Flash". Apple. Abril 2010. URL: http://www.apple.com/hotnews/thoughts-on-flash/
[Ref.- 96]	iOS Support Matrix. URL: http://iossupportmatrix.com
[Ref.- 97]	"Does your phone warn you when it is not encrypting your calls?". David Pérez, José Picó. Taddong. Febrero 2011. URL: http://blog.taddong.com/2011/02/does-your-phone-warn-you-when-it-is-not.html
[Ref.- 98]	"Stolen iPhone? Your iMessages may still be going to the wrong place". Jacqui Cheng. Diciembre 2011. URL: http://arstechnica.com/apple/2011/12/stolen-iphone-your-imessages-may-still-be-going-to-the-wrong-place/
[Ref.- 99]	"Well known TCP and UDP ports used by Apple software products". Apple. Octubre 2011. URL: http://support.apple.com/kb/ts1629
[Ref.- 100]	Aplicaciones de transferencia de datos entre iOS y un ordenador: - i-FunBox (disponible para Windows y OS X respectivamente) - URLs: http://www.i-funbox.com y http://ifunboxmac.com - DiskAid - URL: http://www.digidna.net/products/diskaid - iExplorer- URL: http://www.macroplant.com/iexplorer/
[Ref.- 101]	"iSSLFix (CVE-2011-0228 fix for older idevices/firmwares)". jan0. URL: https://github.com/jan0/isslfix/ URL (DigiNotar): https://github.com/jan0/isslfix/blob/master/diginotar.h
[Ref.- 102]	"Deploying iPhone and iPad - Virtual Private Networks". Apple. 2012. URL: https://www.apple.com/iphone/business/docs/iOS_VPN_Mar12.pdf
[Ref.- 103]	"Pushproxy". meee. 2012. URL: https://github.com/meeee/pushproxy

Referencia	Título, autor y ubicación
[Ref.- 104]	"My Apple ID". Apple. URL: https://appleid.apple.com URL (FAQ): http://support.apple.com/kb/he37
[Ref.- 105]	"Tu contraseña, en un archivo en texto claro". Alejandro Ramos. Security by Default. Marzo 2012. URL: http://www.securitybydefault.com/2012/03/tu-contrasena-en-un-archivo-en-texto.html
[Ref.- 106]	"Facebook Plist Mobile Security Hole Allows Identity Theft". Gareth Wright. Abril 2012. URL: http://garethwright.com/blog/facebook-mobile-security-hole-allows-identity-theft URL (Dropbox): http://thenextweb.com/mobile/2012/04/06/security-hole-in-facebook-ios-app-doesnt-require-jailbreak-or-theft-and-dropbox-has-it-too/ URL (Linked-in): http://blog.scoopz.com/2012/04/07/linkedin-ios-app-also-vulnerable-to-plist-identity-theft/
[Ref.- 107]	"Apple holds the master decryption key when it comes to iCloud security, privacy". Ars Technica. Abril 2012. URL: http://arstechnica.com/apple/2012/04/apple-holds-the-master-key-when-it-comes-to-icloud-security-privacy/
[Ref.- 108]	"iOS 4.3.3 Software Update". Apple. Mayo 2011. URL: http://support.apple.com/kb/DL1358
[Ref.- 109]	"Targeting the iOS Kernel". Stefan Esser. SyScan 2011. Abril 2011. URL: http://www.syscan.org/index.php/download/get/0c66aaae8becc39e75baa9e51e4ffb0c/Day1_Speaker_02_Stefan_Esser.zip
[Ref.- 110]	"Antid0te 2.0 – ASLR in iOS". Stefan Esser. HitB 2011. Mayo 2011. URL: http://conference.hitb.org/hitbsecconf2011ams/materials/D1T1%20-%20Stefan%20Esser%20-%20Antid0te%202.0%20-%20ASLR%20in%20iOS.pdf
[Ref.- 111]	"More fun with a locked iPhone 4". Ade Barkah. Febrero 2012. URL: http://peekay.org/2012/02/05/more-fun-with-locked-iphone-4/
[Ref.- 112]	"Apple Loophole Gives Developers Access to Photos". Nick Bilton. NYT. Febrero 2012. URL: http://bits.blogs.nytimes.com/2012/02/28/tk-ios-gives-developers-access-to-photos-videos-location/
[Ref.- 113]	"Apple reportedly rejecting apps that access UDIDs". Apple Insider Marzo 2012. URL:http://www.appleinsider.com/articles/12/03/25/apple_begins_blanket_rejections_of_apps_that_access_udids.html
[Ref.- 114]	"Ivan Golubev's Password Recovery Suite (IGPRS)". Ivan Golubev. 2012 URL: http://www.golubev.com/igprs/
[Ref.- 115]	"Creating an iTunes Store, App Store, iBookstore, and Mac App Store account without a credit card". Apple. 2012 URL: http://support.apple.com/kb/HT2534
[Ref.- 116]	"A Sandbox Odyssey". Vicenzo Iozzo. 2012. URL: http://prezi.com/lxljhvzem6js/a-sandbox-odyssey-infiltrate-2012/
[Ref.- 117]	"Apple Configurator". Apple. 2012. URL: http://help.apple.com/configurator/mac/1.0/?lang=es
[Ref.- 118]	"iTunes for Windows: Connection issues when using Internet filters, accelerators, or firewalls". Apple. Diciembre 2009. URL: http://support.apple.com/kb/ts1379
[Ref.- 119]	"iOS Forensic Analysis for iPhone, iPad, and iPod touch". Sean Morrissey. APress. URL: http://www.apress.com/9781430233428
[Ref.- 120]	"HTTpOnly cookies support". OWASP. URL: https://www.owasp.org/index.php/HttpOnly
[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]	"iPhone Privacy". N. Seriot. Julio 2010. URL: http://www.seriot.ch/resources/talks_papers/iPhonePrivacy.pdf
[Ref.- 123]	"Strengths and Weaknesses in Apple's MDM System". Intrepids Group. Agosto 2011. URL: http://intrepidusgroup.com/insight/2011/08/apple-mdm-talk/ URL: https://github.com/intrepidusgroup/imdmtools/
[Ref.- 124]	"Lion Server Support - Profile Manager". Apple. 2012. URL: http://www.apple.com/support/lionserver/profilemanager/

Referencia	Título, autor y ubicación
[Ref.- 125]	"iOS Hacker's Handbook". Charlie Miller, Dion Blazakis, Dino DaiZovi, Stefan Esser, Vincenzo Iozzo, Ralf-Philip Weinmann. Wiley. 2012. URL: http://eu.wiley.com/WileyCDA/WileyTitle/productCd-1118204123.html
[Ref.- 126]	"Special Look: Face Time (three parts)". Joshua Wright. Packestan. 2010. URL: http://www.packetstan.com/2010/07/special-look-face-time-part-1.html URL: http://www.packetstan.com/2010/07/special-look-face-time-part-2-sip-and.html URL: http://www.packetstan.com/2010/07/special-look-face-time-part-3-call.html
[Ref.- 127]	"Guía CCN-STIC-454 - Seguridad de dispositivos móviles: iPad". CCN-CERT. 2012. "Guía CCN-STIC-455 - Seguridad de dispositivos móviles: iPhone". CCN-CERT. 2012. URL: https://www.ccn-cert.cni.es - Herramientas – Series CCN-STIC URL: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/454-Seguridad_iPad/454-Seguridad-de-dispositivos%20moviles-iPad-may13.pdf URL: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/455-Seguridad_iPhone/455-Seguridad-de-dispositivos-moviles-iPhone-may13.pdf
[Ref.- 128]	"About the security content of iOS 7.1.1". Apple. Abril 2014. URL: http://support.apple.com/kb/HT6208
[Ref.- 129]	"About the security content of iOS 6". Apple. Septiembre 2012. URL: http://support.apple.com/kb/HT5503
[Ref.- 130]	"About the security content of iOS 7". Apple. Septiembre 2013. URL: http://support.apple.com/kb/HT5934
[Ref.- 131]	"About the security content of iOS 6.1.6". Apple. Febrero 2014. URL: http://support.apple.com/kb/HT6146
[Ref.- 132]	"If you can't update or restore your iOS device". Apple. URL: http://support.apple.com/kb/HT1808
[Ref.- 133]	"Apple iCloud master decryption key". Ars Technica. April 2012. URL: http://arstechnica.com/apple/2012/04/apple-holds-the-master-key-when-it-comes-to-icloud-security-privacy/
[Ref.- 134]	"What Apple Missed to Fix in iOS 7.1.1". Andreas Kurtz. April 2014. URL: http://www.andreas-kurtz.de/2014/04/what-apple-missed-to-fix-in-ios-711.html
[Ref.- 135]	"Configuration Profile Key Reference". Apple. URL: https://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/
[Ref.- 136]	"iMessage Privacy". pod2g & gg. Quarkslab. HITB. October 2013. URL: http://blog.quarkslab.com/static/resources/2013-10-17_imessage-privacy/slides/iMessage_privacy.pdf
[Ref.- 137]	"Guía CCN-STIC-454 - Seguridad de dispositivos móviles: iPad (iOS 7.x)". CCN-CERT. 2014. "Guía CCN-STIC-455 - Seguridad de dispositivos móviles: iPhone (iOS 7.x)". CCN-CERT. 2014. URL: https://www.ccn-cert.cni.es - Herramientas – Series CCN-STIC
[Ref.- 138]	"Special Look: Face Time" - (part 1: Introduction) (part 2: SIP and Data Streams) (part 3: Call Connection Initialization). Joshua Wright. Packetstan. URL: http://www.packetstan.com/2010/07/special-look-face-time-part-1.html URL: http://www.packetstan.com/2010/07/special-look-face-time-part-2-sip-and.html URL: http://www.packetstan.com/2010/07/special-look-face-time-part-3-call.html
[Ref.- 139]	"CCN-STIC-457: Gestión de dispositivos móviles: MDM (Mobile Device Management)". CCN-CERT. Noviembre 2013. URL: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/457/457-Gestion_dispositivos_moviles_MDM-nov13.pdf
[Ref.- 140]	"iOS 7: Cómo funciona Localización". Apple. URL: http://support.apple.com/kb/HT5594?viewlocale=es_ES
[Ref.- 141]	"iOS 7". Apple. Sep 2013. URL: http://support.apple.com/kb/DL1682
[Ref.- 142]	"iOS 7.1.2". Apple. Junio 2014. URL: http://support.apple.com/kb/DL1750

Referencia	Título, autor y ubicación
[Ref.- 143]	"About the security content of iOS 7.1.2". Apple. Junio 2014. URL: http://support.apple.com/kb/HT6297
[Ref.- 144]	"iCamasu". Raúl Siles. DinoSec. Junio 2014. URL: http://blog.dinosec.com/2014/06/icamasu.html
[Ref.- 145]	"About the security content of iOS 7.1". Apple. Marzo 2014. URL: http://support.apple.com/kb/HT6162
[Ref.- 146]	"evasi0n6 & evasi0n7". evad3rs. URL: http://evasi0n.com
[Ref.- 147]	"iOS: Back to the Future". Raúl Siles. DinoSec. Junio 2014. URL: http://blog.dinosec.com/2014/06/ios-back-to-future.html
[Ref.- 148]	"iOS Security". Apple. February 2014. URL: http://images.apple.com/ipad/business/docs/iOS_Security_Feb14.pdf
[Ref.- 149]	"Cómo cancelar la recepción de anuncios basados en intereses de iAd". Apple. 2013. URL: http://support.apple.com/kb/HT4228?viewlocale=es_ES
[Ref.- 150]	"iOS 7 and business". Apple. URL: https://www.apple.com/ios/ios7/business/
[Ref.- 151]	"Managing Apple Devices" (session 300). Apple. WWDC 2013. Julio 2013. URL: https://developer.apple.com/wwdc/videos/ URL: https://developer.apple.com/wwdc/videos/index.php?id=300
[Ref.- 152]	"Volume Purchase Program (VPP)". Apple. 2013. URL: https://www.apple.com/business/vpp/ URL: https://help.apple.com/iosdeployment-apps/ URL: https://www.apple.com/iphone/business/it-center/apps.html
[Ref.- 153]	"iOS 7 Mobile App Management Features (MAM)". MobileIron. URL: http://www.mobileiron.com/en/solutions/ios-7/ios7-mobile-application-management-features-mam-vpp-sso-vpn
[Ref.- 154]	"NY authorities trying to stop smartphone thefts". 2013. URL: http://appleinsider.com/articles/13/05/13/new-york-authorities-ask-apple-google-to-help-stop-smartphone-thefts URL: http://appleinsider.com/articles/12/09/25/rate_of_apple_product_theft_rising_in_new_york_city_accounts_for_over_14_of_all_major_crime
[Ref.- 155]	"iCloud: Activation Lock". Apple. URL: http://support.apple.com/kb/PH13695
[Ref.- 156]	"iCloud: Find My iPhone Activation Lock in iOS 7". Apple. URL: http://support.apple.com/kb/ht5818
[Ref.- 157]	"Buscar mi iPhone en iCloud". Apple. URL: https://www.icloud.com/#find
[Ref.- 158]	"Find My iPhone Activation Lock: Removing a device from a previous owner's account". Apple. URL: http://support.apple.com/kb/TS4515
[Ref.- 159]	"doulCi". doulCi Team. URL: http://doulci.net
[Ref.- 160]	"Chaos Computer Club breaks Apple TouchID". CCC. September 2013. URL: http://ccc.de/en/updates/2013/ccc-breaks-apple-touchid URL: http://vimeo.com/75324765 URL: http://istouchidhackedyet.com
[Ref.- 161]	"Security flaw in Find My iPhone iCloud Lock BYPASS. Activation Lock Bypass". Bradley Williams. (CVE-2014-2019). Febrero 2014. URL: https://www.youtube.com/watch?v=QnPk4RRWjic
[Ref.- 162]	"iOS 7: List of available trusted root certificates". Apple. URL: http://support.apple.com/kb/HT5012
[Ref.- 163]	"Mactans: Injecting Malware into iOS Devices via Malicious Chargers". GTISC. BlackHat USA 2013. August 2013. URL: https://media.blackhat.com/us-13/US-13-Lau-Mactans-Injecting-Malware-into-iOS-Devices-via-Malicious-Chargers-Slides.pdf URL: https://media.blackhat.com/us-13/US-13-Lau-Mactans-Injecting-Malware-into-iOS-Devices-via-Malicious-Chargers-WP.pdf
[Ref.- 164]	"Apple TV (3rd generation): Using an iOS device to set up your Apple TV". Apple. URL: http://support.apple.com/kb/ht5900

Referencia	Título, autor y ubicación
[Ref.- 165]	"iCloud Keychain and iOS 7 Data Protection". Andrey Belenko. Viaforensics. December 2013. URL: https://viaforensics.com/articles-presentations/icloud-keychain-ios-7-data-protection-passwords-13.html
[Ref.- 166]	"iOS: Use AirDrop to wirelessly share content". Apple. URL: http://support.apple.com/kb/ht5887
[Ref.- 167]	"Configuration Profile Key Reference". Apple: URL: https://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/Introduction/Introduction.html#//apple_ref/doc/uid/TP40010206
[Ref.- 168]	"Apple's SSL/TLS bug". Adam Langley. Febrero 2014. URL: https://www.imperialviolet.org/2014/02/22/applebug.html
[Ref.- 169]	"Apple 'goto fail' vulnerability". Apple. URL: http://support.apple.com/kb/HT6147 URL: http://support.apple.com/kb/HT6146
[Ref.- 170]	"Mobile Hotspots". Department Informatik. TF. Junio 2013. URL: https://www1.cs.fau.de/hotspot
[Ref.- 171]	"iStupid: indescreet SSID tool (for the) unknown PNL (on) iOS devices". Raúl Siles. DinoSec. Mayo 2013. URL: http://www.dinosec.com/es/lab.html#iStupid
[Ref.- 172]	"Preferred Network List (PNL) disclosure in iOS 1.x-6.x when adding Wi-Fi networks manually". Raúl Siles. DinoSec. Marzo 2013. URL: http://blog.taddong.com/2013/04/how-to-add-wi-fi-networks-to-mobile.html
[Ref.- 173]	"Wi-Fi: Why iOS (Android & others) Fail inexplicably". Raúl Siles. DinoSec. Marzo 2013. URL: http://www.dinosec.com/es/lab.html#Rooted2013WiFi
[Ref.- 174]	"Bluetooth for Developers". Apple. 2014. URL: https://developer.apple.com/bluetooth/ URL: https://developer.apple.com/hardwaredrivers/bluetoothdesignguidelines.pdf URL: https://developer.apple.com/library/ios/documentation/NetworkingInternetWeb/Conceptual/CoreBluetooth_concepts/AboutCoreBluetooth/Introduction.html URL: https://www.bluetooth.org/tpg/QLI_viewQDL.cfm?qid=20230
[Ref.- 175]	"MFi". Apple. 2014. URL: https://developer.apple.com/programs/mfi/ URL: https://mfi.apple.com/MFiWeb/getFAQ.action#4-2
[Ref.- 176]	“Never trust SMS: iOS text spoofing”. Pod2g. Agosto 2012. URL: http://www.pod2g.org/2012/08/never-trust-sms-ios-text-spoofing.html