GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

CCN
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 455D

Guía práctica de seguridad en dispositivos móviles: iPhone (iOS 12.x)

Octubre 2018

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2018.10.31 13:41:56 +01'00'

NIPO: 083-19-039-8
Fecha de Edición: octubre de 2018
Mónica Salas y Raúl Siles (DinoSec) han colaborado en la elaboración del presente informe.

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

PRÓLOGO

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

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

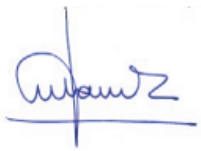
Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad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

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

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

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

Octubre de 2018



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN

La creciente utilización de dispositivos móviles tanto en el plano profesional como personal, unida al incremento en el número y tipo de amenazas que afectan a los mismos, requiere poner en marcha todos los mecanismos disponibles de cara a la protección de la información que se transfiere y almacena en estos dispositivos, que cada vez es mayor y más sensible.

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

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

El presente documento realiza un análisis general de los mecanismos y la configuración de seguridad recomendados para el sistema operativo iOS de Apple (empleado en dispositivos iPhone, iPad, y iPod Touch, en sus diferentes variantes) [Ref.- 1] [Ref.- 2], y, en concreto, está centrado en la versión 12.x, con el objetivo de reducir su superficie de exposición frente a ataques de seguridad.

2. OBJETO

El propósito del presente documento es proporcionar una lista de recomendaciones de seguridad para la protección de los datos, comunicaciones e información que almacenan los dispositivos móviles basados en el sistema operativo iOS versión 12.x, y en concreto para dispositivos móviles iPhone [Ref.- 1] y iPad [Ref.- 2] de Apple.

El presente informe proporciona los detalles específicos de aplicación e implementación de las recomendaciones de seguridad y buenas prácticas necesarias para la prevención de los riesgos, amenazas, y vulnerabilidades de seguridad a las que están expuestos los dispositivos móviles basados en iOS en la actualidad, y se ha redactado considerando como requisito la necesidad de encontrar un equilibrio entre seguridad y funcionalidad en relación a las capacidades disponibles en los dispositivos móviles a proteger, con el objetivo de poder hacer uso de la mayoría de características disponibles en los mismos de forma segura.

Adicionalmente, se recomienda la lectura de las guías CCN–CERT asociadas a otros sistemas operativos y versiones de plataformas móviles, en caso de ser necesaria su aplicación en otros terminales, y a la gestión empresarial de dispositivos móviles (MDM):

- CCN–STIC–450 – Seguridad de dispositivos móviles [Ref.- 400]
- CCN–STIC–451 – Seguridad de dispositivos móviles: Windows Mobile 6.1
- CCN–STIC–452 – Seguridad de dispositivos móviles: Windows Mobile 6.5
- CCN–STIC–453C – Seguridad de dispositivos móviles: Android 5.x [Ref.- 405]
- CCN–STIC–453D – Seguridad de dispositivos móviles: Android 6.x [Ref.- 406]
- CCN–STIC–453E – Seguridad de dispositivos móviles: Android 7.x [Ref.- 407]
- CCN–STIC–454(A) – Seguridad de dispositivos móviles: iPad (iOS 7.x) [Ref.- 409]
- CCN–STIC–455(A) – Seguridad de dispositivos móviles: iPhone (iOS 7.x) [Ref.- 410]

- CCN–STIC–456 – Cuenta de Usuario Servicios Aplicaciones Google para Dispositivos Móviles Android [Ref.- 408]
- CCN–STIC–457 – Gestión de dispositivos móviles: MDM (Mobile Device Management) [Ref.- 403]
- CCN–CERT BP–03/16 – Buenas Prácticas. Dispositivos móviles" [Ref.- 404]

3. ENTORNO DE APLICACIÓN DE ESTA GUÍA

El iPhone[1] es un dispositivo móvil de tipo *smartphone* con pantalla táctil capacitiva basado en el sistema operativo iOS, diseñado y fabricado por Apple, que proporciona capacidades de telefonía móvil, además de acceso a redes de datos como Internet. La primera versión o generación del iPhone (2G) se distribuyó en EEUU en junio de 2007, comercializándose desde entonces y hasta la fecha, posteriores generaciones del iPhone cada año.

Las principales diferencias entre las distintas generaciones de iPhone residen fundamentalmente en el tipo de hardware disponible, la funcionalidad proporcionada por el mismo y las mejoras de la versión de iOS asociada. Entre otras características hardware, los modelos más recientes ya cuentan con pantalla Retina, GPS y servicios de geolocalización, múltiples sensores (como brújula digital, acelerómetro, giroscopio, barómetro, etc., varias cámaras (traseras y frontales)), procesador ARM de 64 bits, capacidades Wi-Fi multi-frecuencia en 2,4 y 5 GHz (802.11a/b/g/n/ac), soporte de telefonía móvil o celular 4G/LTE empleando una tarjeta nano SIM, soporte para Bluetooth 4.x o 5.x, tecnología "Touch ID" (un lector biométrico de huella dactilar que ha sido integrado en el botón principal, o Home, del dispositivo móvil; ver apartado "10.2. Touch ID"), tecnología "Face ID" (un sistema de autentificación biométrica mediante reconocimiento facial que ha sido integrado en la cámara frontal del dispositivo móvil; ver apartado "10.3. Face ID"), conector *lightning*[2], capacidades de carga inalámbrica, módulo NFC para poder hacer uso de las capacidades de pago desde el dispositivo móvil a través de Apple Pay, entre otros.

El iPad[3] es un dispositivo móvil de tipo tableta, o *tablet*, con pantalla táctil capacitiva cuyo sistema operativo también es iOS, que, como principal diferencia con el iPhone, ofrece un tamaño de pantalla mayor y carece de capacidades de telefonía móvil de voz y SMS/MMS. Comenzó a comercializarse en EEUU en abril de 2010 y, a fecha de elaboración del presente documento, se ofrece en tres variantes: iPad Pro, iPad o iPad Air, e iPad mini, diferenciadas fundamentalmente por el tamaño de la pantalla. Los modelos disponibles actualmente cuentan con pantalla Retina, tecnología "Touch ID", dos cámaras (trasera y frontal), capacidades Wi-Fi multi–frecuencia con soporte hasta para 802.11ac y Bluetooth 4.2 o 5.x, conector *lightning*, múltiples sensores, entre otros. Opcionalmente, es posible adquirir los modelos de iPad con módulo GPS y soporte de telefonía móvil o celular 4G/LTE empleando una tarjeta nano–SIM, disponible para establecer comunicaciones de datos móviles.

4. IOS

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

[1] https://es.wikipedia.org/wiki/IPhone
[2] https://es.wikipedia.org/wiki/Lightning_(conector)
[3] https://es.wikipedia.org/wiki/IPad

Las nuevas versiones de iOS suelen acompañar al lanzamiento comercial de las nuevas versiones hardware de los dispositivos de Apple (normalmente del iPhone, liberándose nuevas subversiones de iOS en el caso de nuevas versiones hardware del iPad). Así, la versión iOS 1.0 acompañó a la primera generación de iPhone (2G) en junio de 2007, mientras que la versión iOS 12.0 se liberó en septiembre de 2018 junto a los iPhone XR, XS y XS Max.

A fecha de elaboración del presente informe (octubre de 2018), la tasa de adopción de iOS 12 en dispositivos móviles de Apple, tras su publicación en octubre de 2018, es del 53%[4].

Las principales funcionalidades introducidas por iOS 12[5] son:

- Mejoras en el rendimiento, tanto de las apps, la cámara, el teclado y el menú "Compartir", no solo para los nuevos dispositivos móviles, sino también para modelos más antiguos (alargando potencialmente la vida de uso de éstos).
- FaceTime permite llamadas de grupo de hasta 32 personas simultáneamente, con cifrado extremo a extremo tanto en llamadas individuales como de grupo.
- Se incorpora la capacidad "Tiempo de Inactividad", que permite establecer periodos durante los cuales se bloquearán las apps y las notificaciones.
- Se añaden herramientas para conocer el "Tiempo de Uso" del dispositivo, así como la generación de "Informes de actividad" diarios.
- Las capacidades de "Tiempo de Uso" permiten definir restricciones en el uso de apps y en el acceso a sitios web en base a los identificadores de usuario (ID de Apple, o *Apple ID*) asociados a los miembros de una misma familia.
- Mayor granularidad en el control de las notificaciones, permitiendo establecer excepciones para recibir notificaciones críticas incluso con la opción "No Molestar" activa, agrupación de notificaciones, respuesta abreviada manteniendo pulsada una notificación y modificación de ajustes de la notificación instantáneos.
- Se añade la opción de "Actualización de software automática", para que las actualizaciones de software del sistema operativo iOS se descarguen e instalen sin intervención del usuario durante la noche.
- Características relevantes desde el punto de vista de la seguridad:
  - Servicio de comprobación de contraseñas repetidas si se hace uso de "llavero de iCloud".
  - Capacidades para autocompletar los códigos de seguridad asociados a un segundo factor de autentificación (2FA) recibidos por SMS dentro de las apps y de las páginas web.
  - Mejoras en la gestión de las opciones de compartición de Safari, que impiden la recopilación de información sobre los identificadores del dispositivo móvil para su uso en publicidad personalizada.

Los detalles asociados a cada actualización pueden consultarse en "Ajustes – General – Actualización de software – Más información", una vez hay disponible una actualización para la versión de iOS actual del dispositivo (ver apartado "20. Actualización del sistema operativo iOS").

[4] https://developer.apple.com/support/app-store/
[5] https://www.apple.com/es/ios/ios-12/features/

5. DISPOSITIVO MÓVIL EMPLEADO

El dispositivo móvil empleado en la elaboración del presente informe es el iPhone SE, que comparte muchas de las prestaciones de modelos de gama más alta, con pantalla de 4", procesador Apple A9 (y coprocesador de movimiento M9), cámara trasera de 12MP con capacidades de grabación de vídeo en 4K y tecnología Touch ID, entre otros.

La mayor parte de las recomendaciones de seguridad proporcionadas son aplicables al resto de dispositivos móviles iPhone e iPad que soporten la versión iOS 12, pero puede que algunas de ellas no sean de aplicación directa en modelos que no dispongan de los componentes hardware implicados.

La versión concreta de iOS empleada en la elaboración del presente informe es la 12.0, primera versión de iOS 12 publicada por Apple, en septiembre de 2018.

Nota: Al finalizar la elaboración del presente informe, se liberó la versión de iOS 12.0.1, que resuelve dos vulnerabilidades descubiertas en la pantalla de bloqueo de su predecesora, iOS 12.0, y que permiten acceder a contenidos del dispositivo sin que éste se encuentre desbloqueado [Ref.- 25], por lo que se recomienda actualizar a iOS 12.0.1 tan pronto resulte posible (consultar apartado "20. Actualización del sistema operativo iOS" para ver el mecanismo de actualizaciones).

6. PROCESO DE ACTIVACIÓN DEL DISPOSITIVO MÓVIL

Una vez se arranca el dispositivo móvil por primera vez mediante la pulsación del botón de encendido, es preciso realizar el denominado "proceso de activación", que requiere introducir una tarjeta SIM, y que establecerá una configuración por defecto con los valores fijados por Apple (y/o seleccionados por el usuario durante este proceso), junto a los ajustes del operador de telefonía móvil en función del perfil de configuración móvil de iOS asociado a la tarjeta SIM y al operador.

El proceso de activación mostrará el mensaje "Pulsa el botón de inicio para abrir", al que sigue una pantalla con identificadores en la que se muestra información sobre el número de serie y el IMEI del dispositivo móvil, y el ICCID de la tarjeta SIM, entre otros. Tras pulsar el botón "Inicio" ("*Home*"), se indicará que la tarjeta SIM está bloqueada y, al pulsar en "*Unlock*" ("Desbloquear"), se solicitará el PIN de la tarjeta SIM.

Nota: El iPhone no ofrece la posibilidad de tomar capturas de pantalla durante el proceso de activación, por lo que las imágenes asociadas a este proceso se omitirán.

La correcta introducción del PIN de la tarjeta SIM activa la vinculación del dispositivo móvil a una tarjeta SIM y número de teléfono, junto a las capacidades de comunicación de datos móviles, y permite continuar con la activación, que se inicia con la selección de idioma y región. El proceso de activación ofrece la posibilidad de iniciar sesión acercando otro dispositivo móvil de Apple (funcionalidad conocida como "Inicio rápido"). Si se opta por la opción "Configurar manualmente", se activará el interfaz Wi-Fi, se escanearán las redes Wi-Fi cercanas y se mostrará una lista con las redes encontradas, ordenada alfabéticamente, para facilitar la conexión a una red Wi-Fi. Al final de la lista se dispone de la opción para configurar

una red Wi-Fi manualmente (opción "Seleccionar otra red")[6], o de emplear la conexión de datos móviles para el proceso de activación (opción "Usar conexión móvil").

La introducción de la contraseña de la red Wi-Fi debe realizarse de forma que se impida el acceso visual a la pantalla por parte de terceros no autorizados, ya que los caracteres se muestran momentáneamente en claro durante su introducción. Una vez se verifica la contraseña, se reflejará que se ha establecido una conexión a esa red Wi-Fi mediante un símbolo de validación ("√") a la izquierda de su nombre. Al pulsar "Siguiente", se mostrará un mensaje informando de que el proceso de activación está en curso.

La siguiente pantalla informa al usuario de que se va a obtener información personal, junto a los aspectos de privacidad asociados, y propone la activación de la función "Touch ID" (identificación por huella). Se recomienda configurar dicha funcionalidad con posterioridad a completar el proceso de activación (ver apartado "10.2. Touch ID"), seleccionando "No usar".

Si se opta por "No usar", se presentará la pantalla de configuración de bloqueo de la pantalla, que, por defecto, solicita la introducción de un código de acceso (o PIN) de 6 dígitos, pero que también ofrece el menú "Opciones de código" (ver apartado "10.1. Código de acceso del dispositivo móvil ") con otras alternativas. Desde el punto de vista de seguridad, se recomienda seleccionar, bien un código "alfanumérico personalizado" de al menos 8 caracteres, bien un código "numérico personalizado" de al menos 8 dígitos. Si se optase por "No usar código" (opción totalmente desaconsejada desde el punto de vista de seguridad), se mostrará un mensaje de aviso.

El siguiente paso consiste en seleccionar si se desea realizar la configuración inicial a partir de una copia de seguridad (desde iCloud o iTunes; consultar el apartado "19. Copias de seguridad y restauración"), transferir los datos desde un dispositivo móvil Android o configurar como un nuevo iPhone (opción documentada en el presente informe), para la cual se ofrece la posibilidad de utilizar un identificador de usuario o ID de Apple (*Apple ID*) ya existente o crear uno nuevo, en cuyo caso se solicitará la fecha de nacimiento para permitir o inhabilitar el acceso a determinados servicios.

Para indicar el ID de Apple, se solicitará la introducción de una dirección de correo electrónico o la creación de una nueva cuenta de usuario en iCloud, que se utilizará como ID de Apple:

- En caso de no desear asociar el dispositivo móvil a un ID de Apple, se empleará la opción "Configurar más tarde en Ajustes". La asociación entre el dispositivo móvil y un ID de Apple es necesaria para la utilización de ciertos servicios de Apple, como "Buscar mi iPhone" (ver apartado "9.1.1. Buscar mi iPhone").
- En caso de querer realizar la vinculación del dispositivo móvil con un ID de Apple (opción documentada a continuación), la misma cuenta de usuario se empleará tanto para acceder a los servicios de iCloud, como a la iTunes Store y a la App Store. La contraseña ha de teclearse en un lugar seguro y fuera del alcance visual de terceros, ya que los caracteres aparecen brevemente en claro en la pantalla durante su introducción.

Nota: Es muy importante destacar que, pese a que se muestra un mensaje informando de que la vinculación entre la dirección de e-mail seleccionada como ID de Apple y el dispositivo móvil no puede cambiarse posteriormente, la realidad es que esto sí es posible, como se documenta en el apartado "9. Cuentas asociadas al dispositivo móvil".

[6] A través de "Seleccionar otra red" se puede escoger una red Wi-Fi oculta, aunque el uso de este tipo de redes se desaconseja desde el punto de vista de seguridad.

La cuenta de usuario proporcionada en este paso se empleará por defecto tanto para los servicios de iCloud como para el acceso a la iTunes Store y a la App Store, tanto si se crea nueva como si se añade una ya existente. Sin embargo, una vez concluido el proceso de activación, será posible configurar distintas cuentas de usuario para el acceso a estos servicios.

Para validar el ID de Apple durante el proceso de activación, si dicho ID de Apple dispone de un segundo factor de autentificación (2FA) configurado[7], debe seleccionarse entre dos mecanismos para recibir el código de verificación: "SMS" (utilizado por defecto) y "Llamada telefónica", y pulsar "Siguiente". En caso de emplearse "SMS", el código de verificación se rellenará automáticamente una vez recibido el mensaje (si no es así, se puede teclear manualmente). Finalmente, se deberán aceptar los términos y condiciones del servicio.

Se solicitará al usuario permiso para activar los servicios de localización. Se recomienda seleccionar "Desactivar localización" y seguir a posteriori las recomendaciones del apartado "14. Servicios de localización". También se ofrecerá la posibilidad de configurar los métodos de pago para el uso del servicio "Apple Pay", el cual queda fuera del alcance del presente informe, y cuyo uso se desaconseja desde el punto de vista de seguridad, y del denominado "Llavero de iCloud", un servicio de almacenamiento de credenciales y métodos de pago en la nube para su compartición entre los diferentes dispositivos móviles (iOS) y tradicionales (macOS) asociados a una misma cuenta de usuario de iCloud (ver apartado "9.5. Llavero de iCloud").

Por último, se presenta la pantalla de activación del asistente personal digital Siri, recomendándose desde el punto de vista de seguridad posponer a más tarde su configuración (ver apartado "11.5.3. Siri"), y se solicita al usuario permiso para compartir con Apple la información sobre el uso y datos de los distintos servicios y productos asociados al dispositivo móvil y a la cuenta de iCloud. Desde el punto de vista de privacidad, se recomienda seleccionar la opción "No compartir".

El proceso de instalación concluye con un mensaje de bienvenida, tras el cual se mostrará la pantalla de inicio.

- Durante la activación, se asignará al dispositivo móvil iOS un nombre, el cual se puede consultar a través de "Ajustes – General – Información – Nombre" y que, cuando no se emplea iTunes durante el proceso de activación, por defecto corresponde a:
- Un nombre genérico que corresponde al tipo de dispositivo, como "iPhone" o "iPad", si no se ha establecido vinculación con una cuenta de usuario de iCloud durante el proceso de activación (ver imagen derecha de la <Figura 1>, basada en iOS 11.4.1, similar en iOS 12).
- Un nombre genérico que corresponde al tipo de dispositivo seguido del nombre del usuario, el cual se toma de los campos nombre y apellidos configurados en la cuenta de usuario de iCloud, si se realizó la vinculación durante el proceso de activación (ver imagen izquierda de la <Figura 1>.

[7] Cuando se crea el ID de Apple durante la activación del dispositivo, como éste tiene que disponer de una tarjeta SIM, se activa automáticamente la cuenta de usuario con el segundo factor de autentificación.

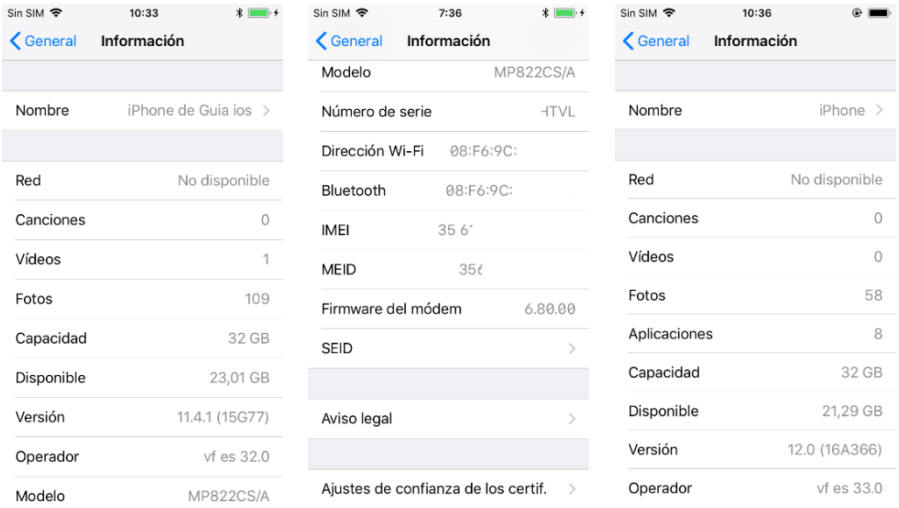


Figura 1 – Información sobre el dispositivo móvil: nombre del dispositivo.

Desde el punto de vista de seguridad, ***se recomienda cambiar el nombre del dispositivo móvil a través de "Ajustes – General – Información – Nombre – [nombre actual] >" por uno que no revele detalles ni del dispositivo móvil (fabricante o modelo) ni del usuario (evitando tanto referencias al nombre de la persona como de la organización asociados al mismo)***, ya que este nombre se intercambia en múltiples comunicaciones, como las conexiones Bluetooth y el tráfico DHCP.

Una vez completada la activación, el dispositivo móvil abrirá la pantalla de inicio (o "*Home*"). En ese momento, dispondrá por un lado de los ajustes de configuración seleccionados por el usuario durante el proceso de activación, y por otro, de los ajustes por defecto fijados por Apple en función de otros parámetros, como la versión concreta de iOS o las características hardware del terminal. Se recomienda, a continuación, proceder a aplicar las recomendaciones ofrecidas en los siguientes apartados del presente informe.

7. PANTALLA DE INICIO ("HOME")

La pantalla de inicio (o "Home") se muestra al desbloquear el dispositivo móvil tras el proceso de arranque y también al pulsar el botón inicio o "Home" desde cualquier otra pantalla. Se encuentra dividida en varias secciones, que se describen a continuación.

En realidad, la pantalla de inicio consta de tantas subpantallas como puntos aparecen sobre la barra de iconos de acceso rápido, la cual se encuentra en la parte más inferior de la pantalla. Es posible deslizarse entre pantallas desplazando el dedo a derecha o izquierda desde cualquier punto de la pantalla actual.

La pantalla principal contiene los iconos de las principales apps incluidas en iOS; la pantalla situada más a la izquierda incorpora la función de búsqueda mediante texto y voz (en la parte superior) y la zona de "widgets", descritos respectivamente en los apartados "7.3. Búsqueda mediante texto y voz" y "7.4. Today View".

7.1 BARRA SUPERIOR DE ESTADO

La barra de estado en iOS está compuesta por una serie de iconos de estado, que permiten consultar de forma rápida algunos de los ajustes principales:

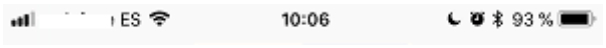


Figura 2 – Barra superior de estado.

La parte izquierda de la barra muestra el estado de la conectividad de datos móviles (en el extremo izquierdo) y de redes inalámbricas (icono que sigue al nombre del operador de telefonía móvil). El icono formado por 4 barras de tamaño creciente indica que se está dentro del alcance de una red móvil y el nivel de cobertura (a mayor número de barras marcadas, mejor cobertura), y viene acompañado del nombre del operador de la red y, eventualmente, del tipo de red disponible (GPRS, E, 3G, 4G, LTE). Si se está haciendo uso de una conexión de datos compartida (ver apartado "11. Conexiones inalámbricas y redes"), se mostrará un símbolo formado por dos eslabones enlazados.

La parte central de la barra de estado ofrecerá la hora si el dispositivo está desbloqueado, y mostrará un candado cerrado si se encuentra bloqueado.

En la parte derecha de la barra, por defecto se presenta solo el estado de la carga de la batería. El icono de Bluetooth, presente hasta iOS 11 por defecto si el interfaz Bluetooth se encuentra activo (hubiese o no establecida una conexión Bluetooth con otro dispositivo), no se muestra en iOS 12 hasta que exista una conexión [Ref.- 4].

Adicionalmente, y según las funcionalidades activas, se podrá mostrar el símbolo de "No molestar", alarma, conexión a auriculares, y otros iconos adicionales. La lista completa puede consultarse en la página de soporte oficial de Apple [Ref.- 3].

Es importante destacar que la barra superior de estado puede aparecer coloreada para informar de otras situaciones:

- Verde: existe una llamada telefónica en curso.
- Rojo: se está grabando sonido o imágenes (o vídeo) del dispositivo.
- Azul: se está compartiendo la conexión de datos (ver apartado "11.6. Personal Hotspot"), indicándose además el número de dispositivos que están conectados actualmente por este medio. Desde el punto de vista de seguridad, es importante prestar atención al número de conexiones activas por si, estando activo el servicio, se estuvieran estableciendo conexiones no deseadas.

No existe ninguna opción conocida que permita personalizar los iconos que se muestran en la barra superior de estado (a menos que el dispositivo se haya sometido a un proceso de *jailbreak*, escenario totalmente desaconsejado desde el punto de vista de seguridad).

7.2 CENTRO DE CONTROL

El Centro de control ("Control center") es una característica rediseñada en iOS 11, y permite un acceso rápido a funciones concretas mediante una serie de iconos.

El Centro de control se muestra en iPhone desplazando un dedo hacia arriba desde la parte inferior de la pantalla (en iPhone X y modelos posteriores, deslizando el dedo hacia abajo desde la esquina superior derecha de la pantalla)[8].

[8] Para acceder al Centro de control desde un iPad en iOS 12, es preciso deslizar el dedo hacia abajo desde la esquina superior derecha de la pantalla.

Figura 3 – Centro de control.

El Centro de color está formado tanto por ajustes (individuales o de grupo) como por accesos directos a aplicaciones. Un grupo se identifica por un recuadro gris oscuro que alberga un conjunto de iconos, como en el caso de los ajustes de red o comunicaciones.

El Centro de control es un elemento crítico desde el punto de vista de seguridad, pues permite activar/desactivar elementos relacionados con la conectividad del dispositivo móvil (por ejemplo, el modo avión, o los interfaces de comunicaciones Wi-Fi, Bluetooth y de red móvil o celular). Un potencial atacante con acceso al Centro de control podría desactivar las capacidades de comunicación de datos (Wi-Fi y móviles 2/3/4G), impidiendo que la funcionalidad "Buscar mi iPhone" pudiese localizar el dispositivo (consultar el apartado "9.1.1. Buscar mi iPhone" para más información.

Por ello, ***se recomienda deshabilitar el Centro de control cuando la pantalla se encuentre bloqueada por un método de acceso desactivando el interruptor "Ajustes – Touch ID y código – [Permitir acceso al estar bloqueado] Centro de control"*** (tercera imagen de la <Figura 3>):

Para obtener más detalles y desplegar los ajustes adicionales relativos a un grupo de ajustes concreto, se puede pulsar prolongadamente sobre uno de los iconos del grupo[9]. En el ejemplo de la segunda imagen de la <Figura 3>, se ha desplegado el grupo correspondiente a los ajustes de red o comunicaciones, vista que proporciona más detalles e información sobre cada uno de los iconos del grupo.

La descripción exacta de los diferentes ajustes se puede consultar en la página de soporte oficial de Apple sobre el Centro de control [Ref.- 5].

Es posible personalizar las apps que integran el Centro de control desde "Ajustes – Centro de control – Personalizar controles", pulsando el símbolo " " sobre los controles que se desea añadir y el símbolo " " sobre los que se desea eliminar. No es posible eliminar del Centro de control los ajustes de red, el "modo nocturno", brillo, volumen, duplicar pantalla, reproducción de música o rotación de pantalla.

[9] Este comportamiento está disponible solo desde iPhone 6s y modelos posteriores.

7.3 BÚSQUEDA MEDIANTE TEXTO Y VOZ

La búsqueda de iOS, disponible en el campo superior "Buscar" de la pantalla situada a la izquierda de la pantalla de inicio, está estrechamente ligada a la funcionalidad del asistente digital personal Siri (ver apartado "11.5.3. Siri"), y también es conocida como "Spotlight". Para acceder a ella se puede deslizar el dedo de izquierda a derecha desde la pantalla de inicio (con la pantalla bloqueada o desbloqueada), lo cual da acceso además a la zona de "widgets" y a la "Vista de hoy", o también deslizar el dedo desde el centro de la pantalla de inicio hacia abajo (sólo con pantalla desbloqueada).

Figura 4 – Menú "Buscar" con pantalla bloqueada.

Al pulsar dentro del campo superior "Buscar", iOS proporcionará sugerencias que se actualizan en tiempo real a medida que se introduce el texto y que concuerden con el término proporcionado según varios criterios, los cuales dependerán de si el dispositivo móvil está bloqueado o desbloqueado y de los ajustes del menú "Ajustes – Siri y Buscar – [Nombre app] Sugerencias de Siri y Buscar".

Si la pantalla está bloqueada (<Figura 4>), se mostrarán:

- Una lista de resultados de las primeras coincidencias asociadas al término de búsqueda.
- Los nombres de las apps instaladas en el dispositivo móvil coincidentes con la cadena de caracteres introducida. Este resultado puede constituir un problema desde el punto de vista de seguridad si un potencial atacante tuviese acceso temporal al dispositivo (sin conocer el código de acceso) y quisiera conocer si una determinada app, que por ejemplo tenga una vulnerabilidad explotable, se encuentra instalada en el dispositivo móvil. Sin ni siquiera introducir ningún texto, ya se muestran las apps más relevantes sugeridas por Siri.
- La entrada de la app "Diccionario" para ese texto.
- Las acciones "Buscar en Internet/App Store/Mapas", aunque se muestran, solicitarán el desbloqueo de la pantalla para lanzar las búsquedas correspondientes.

Adicionalmente, si la pantalla está desbloqueada (<Figura 5>), por defecto se obtendrá el resultado de:

- Los contenidos de las apps instaladas en el dispositivo coincidentes con la cadena de caracteres introducida, incluyendo los ajustes que contienen el texto (ver imagen derecha de la <Figura 5>). Este resultado puede plantear problemas de seguridad si se permite a un tercero acceso temporal al dispositivo con objeto de mostrarle una información concreta (escenario totalmente desaconsejado), pues de forma rápida puede consultar contenidos específicos (mensajes, contactos, e–mails…) sin necesidad de recorrer diferentes pantallas.

Figura 5 – Menú "Buscar" con la pantalla desbloqueada.

El comportamiento del menú "Buscar" se controla a través de "Ajustes – Siri y Buscar" (ver <Figura 6>). Para evitar que el contenido de una app se muestre en los resultados de búsqueda, es preciso desactivar el campo "Búsquedas, sugerencias y atajos" correspondiente a dicha app (por ejemplo, la imagen derecha de la <Figura 6> ilustra este aspecto para la app "Teléfono".

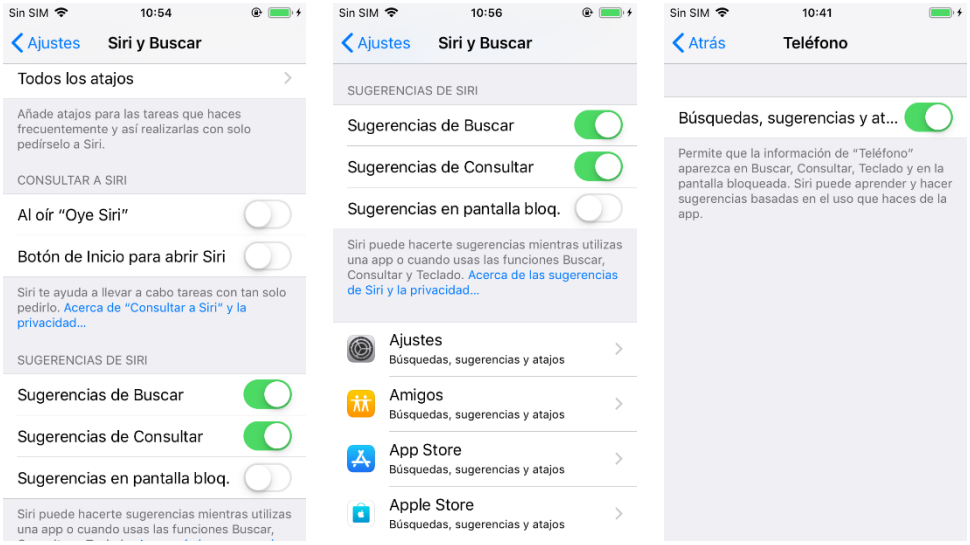


Figura 6 – Menú "Siri y Buscar".

Por defecto, tras realizar la activación del dispositivo móvil, todas las apps tienen este ajuste activo, por lo que iOS hará uso de todos los contenidos durante las búsquedas.

Al desactivar este ajuste, aparecerá en la pantalla uno nuevo denominado "Mostrar app", que controla si la app en cuestión aparecerá en las sugerencias de apps de la función "Siri y Buscar". Es importante destacar que, si se desactiva el ajuste "Búsquedas, sugerencias y atajos", si el asistente de voz Siri se encuentra activo, Siri ignorará la app correspondiente de cara a mostrar resultados asociados a ella durante las búsquedas, pero seguirá utilizando internamente los datos de dichas apps (y enviándole estadísticas y datos a Apple de forma cifrada) para seguir aprendiendo y proporcionando sugerencias personalizadas. Si se desea evitar también este comportamiento, es preciso deshabilitar adicionalmente los ajustes bajo la sección "Sugerencias de Siri": "Sugerencias de Buscar", "Sugerencias de Consultar" y "Sugerencias en pantalla bloqueada" (ver imagen izquierda de la <Figura 6>). Para más información, se recomienda seleccionar el texto "Acerca de 'Consultar a Siri' y la privacidad" de esta sección.

Por tanto, ***desde el punto de vista de seguridad, se recomienda al usuario valorar qué contenidos no desea que se muestren en las búsquedas y desactive el ajuste "Búsquedas, sugerencias y atajos", para cada app individualmente. Adicionalmente, si no se desea enviar contenidos a Apple, se recomienda desactivar todos los ajustes de la sección "Sugerencias de Siri" dentro de "Ajustes – Siri y Buscar".***

El campo "Buscar" permite también búsquedas por voz, funcionalidad que se invoca presionando sobre el icono de micrófono situado a la derecha de la barra de búsqueda superior; la primera vez que se pulse el micrófono, iOS solicitará el permiso para "Activar Dictado", el cual envía datos a Apple (incluyendo voz, contactos y ubicación) durante las tareas de reconocimiento de voz. Se desaconseja el uso de esta funcionalidad por cuestiones de privacidad. Sin embargo, se constata que es posible conceder el permiso de activar la función de dictado para este propósito, incluso con el dispositivo móvil bloqueado, lo que activa el ajuste disponible en "Ajustes – General – Teclado – Activar dictado" hasta que el usuario lo desactive accediendo a dicho menú. Para más información, se recomienda seleccionar el texto "Acerca de dictado y la privacidad…" de esta sección. Este comportamiento resulta inconveniente si el usuario del dispositivo no desea hacer uso de la búsqueda por voz, pero un tercero consigue acceso físico momentáneo al dispositivo y concede dicho permiso:

Figura 7 – Solicitud del permiso "Activar dictado".

Una vez el usuario deshabilita intencionadamente las capacidades de dictado desde el menú de ajustes indicado previamente, no es posible habilitarlo de nuevo desde el menú superior de búsqueda (esté la pantalla bloqueada o desbloqueada).

La función de dictado permite la introducción de texto mediante voz a través del teclado, en lugar de mediante la pulsación de las teclas, incluso sin conexión a Internet para los lenguajes disponibles. Estas capacidades, junto a las de búsqueda, pueden ser ampliadas a través del asistente digital personal Siri (ver apartado "11.5.3. Siri"), para disponer de capacidades de interacción por voz avanzadas con el dispositivo móvil.

Todo lo que se registre a través de esta funcionalidad, denominada "Consultar a Siri", se enviará a Apple, incluyendo datos personales como contactos, dispositivos asociados al usuario, relaciones entre éste y sus contactos, nombres de álbumes de fotos, etc. (todos los detalles se pueden obtener a través del enlace "Acerca de 'Consultar a Siri' y la privacidad…").

Desde el punto de vista de privacidad, se aconseja desactivar las opciones "Al oír 'Oye Siri'" y "Botón de Inicio para abrir Siri" del menú "Ajustes – Siri y Buscar"[10] **y "Ajustes – General – Teclado – Activar dictado"** (ver imagen izquierda de la <Figura 6>).

7.4 TODAY VIEW

La "Vista de hoy" ("Today View") es una vista de la pantalla de inicio, a la que se accede deslizando el dedo de izquierda a derecha. Está formada por una serie de "widgets", que proporcionan una vista rápida a contenidos de apps, tanto con la pantalla bloqueada como desbloqueada:

Figura 8 – Today View.

Es posible personalizar esta vista mediante el botón "Editar", que solicitará el código de acceso si se invoca con la pantalla bloqueada. Al "Editar", se abrirá el menú "Añadir widgets", que permite suprimir mediante "⊖" y añadir mediante "⊕". Para modificar el orden de presentación en la pantalla "Today", se debe pulsar de forma sostenida en el símbolo de líneas horizontales y desplazarlo a la posición deseada (ver <Figura 9>).

[10] En iPhone X y modelos posteriores, al no disponer de botón de inicio (y Touch ID), las opciones a desactivar son "Pulsar el botón lateral para abrir Siri" y "Al oír 'Oye Siri'".

Figura 9 – Personalización de los elementos ("widgets") de la "Vista de hoy".

Desde el punto de vista de privacidad, ***se recomienda no incluir "widgets" en la "Vista de hoy" cuyos contenidos puedan revelar información sensible del usuario (por ejemplo, "Notas" o "Próximamente").***

Para inhabilitar completamente la funcionalidad "Vista de hoy" en la pantalla de bloqueo, se debe desactivar" el interruptor "Ajustes – Touch ID y código – [Permitir acceso al estar bloqueado] Visualización Hoy" (tercera imagen de la <Figura 9>).

7.5 CENTRO DE NOTIFICACIONES

El denominado "Centro de Notificaciones" es un panel que se presenta al deslizar el dedo de arriba a abajo desde cualquier pantalla, y en el que se visualizan las notificaciones y la "Vista de hoy", y cuya apariencia es igual a la de la pantalla de bloqueo (salvo por el icono de candado cerrado que se muestra en la barra de estado para esta última).

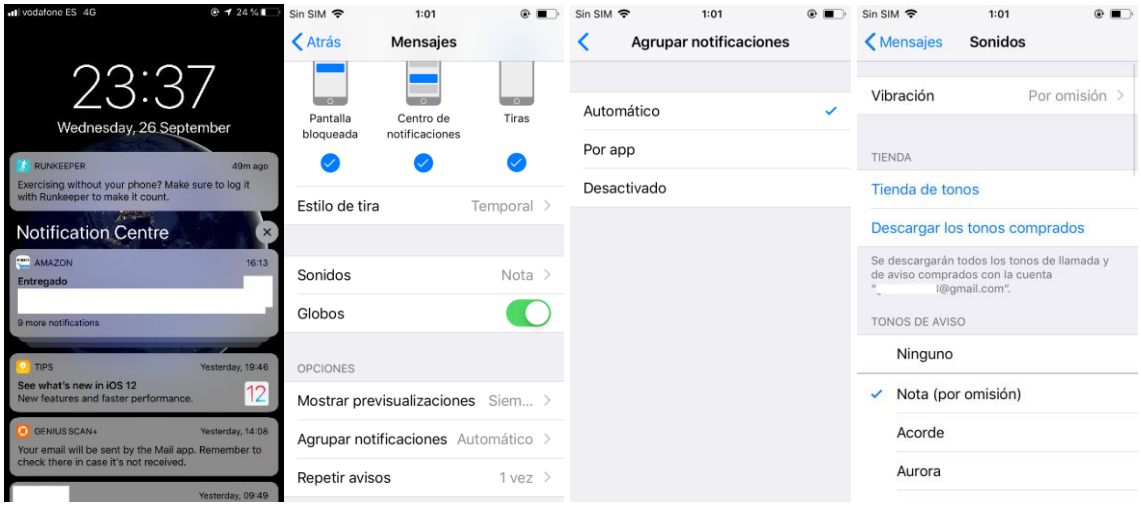


Figura 10 – Centro de notificaciones y sus pantallas de ajustes.

Las notificaciones se ordenan cronológicamente, apareciendo las más recientes y que no se han visto aún en la parte superior de la pantalla, seguidas de las recibidas hoy que se han visto pero no se han procesado y, por último, de las recibidas en días previos.

La aparición de las notificaciones en la pantalla de bloqueo puede controlarse desde el interruptor "Ajustes – Touch ID y código – [Permitir acceso al estar bloqueado] Notificaciones recientes" (ver <Figura 10>). ***Se desaconseja desde el punto de vista de seguridad y privacidad deshabilitar esta opción, que, aunque afecte 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 visual al dispositivo móvil***.

La sección "Ajustes – Notificaciones" permite una gestión más granular de las notificaciones. El ajuste general "Mostrar previsualizaciones" (que se puede fijar a "Siempre", "Si está desbloqueado" o "Nunca") establece el comportamiento por defecto del Centro de Notificaciones. Sin embargo, es posible controlar el comportamiento de una app en relación a las notificaciones seleccionando la entrada de dicha app en la sección "Estilo de notificación" y marcando/desmarcando el "🔵" bajo "Pantalla bloqueada" (imagen 2 de la <Figura 10>) y seleccionando "Mostrar previsualizaciones – Si está desbloqueado". Desde el punto de vista de seguridad, ***se recomienda aplicar esta recomendación especialmente para las apps de contenido potencialmente sensible*** (por ejemplo, Mensajes). Si se utilizan apps que comunican eventos de seguridad, como apps de banca, la recomendación es habilitar "Ver en la pantalla bloqueada", pues suelen informar de pagos realizados mediante las tarjetas de crédito asociadas o de operaciones realizadas desde la cuenta corriente, lo que permite detectar usos no autorizados.

Una de las novedades de iOS 12 es la posibilidad de agrupar las notificaciones procedentes de una misma app en una pila, que permite procesarlas o eliminarlas individualmente o en conjunto, a través del ajuste "Ajustes – Notificaciones – [Nombre de la app] – [Opciones] Agrupar notificaciones"[11]. Adicionalmente, las notificaciones de algunas apps pueden acompañarse de un sonido y/o una vibración, pero se permite al usuario controlar este comportamiento a través de los ajustes "Sonidos – Vibración" y "Sonidos – Tonos de aviso" (ver <Figura 10>). Las notificaciones denominadas "Discretas" (aquéllas para las que no se defina un sonido ni se habilite la vibración) no se presentarán en la pantalla de bloqueo, sino únicamente en el Centro de notificaciones.

Al deslizar el dedo de izquierda a derecha sobre una notificación (o una pila de notificaciones), se mostrarán tres opciones: "Gestionar", "Ver" y "Borrar". La opción "Gestionar" permite cambiar los ajustes de la notificación, por ejemplo, para que se desactive o se convierta en una notificación discreta (ver imagen derecha de la <Figura 11>). La pulsación corta sobre la notificación invoca una acción asociada a la misma, como puede ser devolver una llamada, o responder brevemente a un mensaje.

[11] No todas las apps soportan la agrupación de notificaciones (por ejemplo, "Mail"), por lo que no dispondrán de la opción de configuración "Agrupar notificaciones".

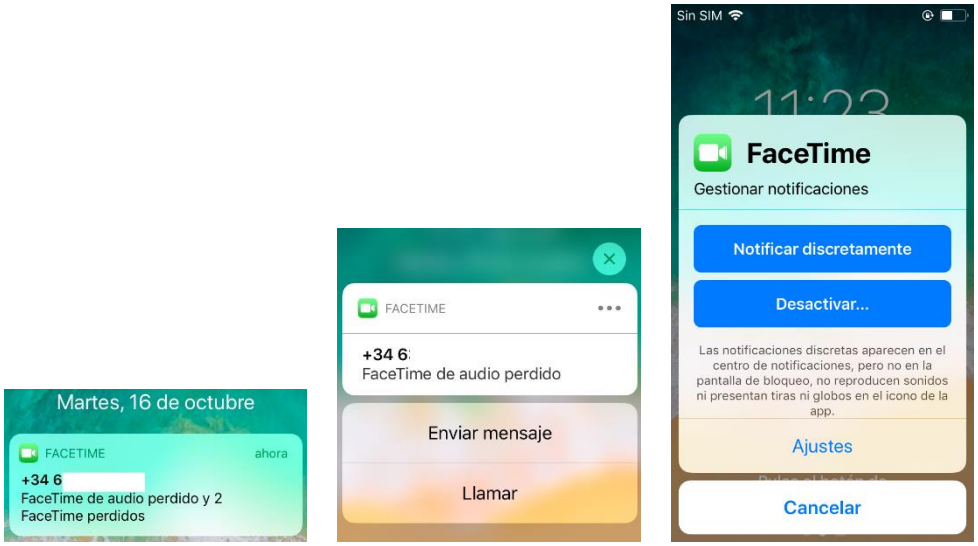


Figura 11 - Gestión de notificaciones en iOS 12.

Como parte de la funcionalidad "Tiempo de uso", se ofrecen estadísticas de notificaciones, que permiten al usuario analizar qué apps son las que más emiten y en qué franjas horarias (ver apartado "17.2. Tiempo de uso").

7.6 MODO "NO MOLESTAR"

El modo "no molestar", configurable desde el menú "Ajustes – No molestar" tiene por objeto silenciar las llamadas y los avisos que se reciban con el dispositivo bloqueado. Las notificaciones irán directamente al Centro de notificaciones, sin presentarse en la pantalla de bloqueo, y no se recibirán en la pantalla de inicio cuando se salga de este modo. iOS 12 introduce el concepto de "alerta crítica", que son notificaciones que sólo pueden generarse por determinadas categorías de apps, por ejemplo, las de salud.

El modo "No molestar" se puede habilitar de forma rápida pulsando el icono de luna disponible en el Centro de control (ver <Figura 3>), y se indica en la barra de estado mediante el símbolo "". Mediante una pulsación larga sobre el símbolo "No molestar" del Centro de control, es posible gestionar la duración de este modo.

Figura 12 - Configuración del modo "No molestar".

Es posible establecer comportamientos excepcionales que alteran el modo "No molestar", como "Permitir llamadas de: Favoritos | Nadie | Contactos | Todos", "Llamadas repetidas", o la entrada en vigor de este modo cuando se está conduciendo, que permite además establecer un mensaje (configurado en la sección "Responder con") que el dispositivo móvil enviará automáticamente a los números seleccionados dentro de la opción "Respuesta automática a".

Desde el punto de vista de seguridad y privacidad, este modo resulta útil en diversas situaciones, por ejemplo, para prevenir accidentes derivados de distracciones al atender llamadas mientras se conduce, o para evitar que un sonido asociado a una notificación se reciba en una situación inoportuna, como una reunión o una visita médica.

8. CONFIGURACIÓN DEL DISPOSITIVO MÓVIL: MENÚ "AJUSTES"

La configuración actual del dispositivo móvil se puede consultar y modificar desde el menú "Ajustes" (*Settings*) representado con un símbolo de engranaje en la pantalla de inicio, que consta de diversas secciones que se pueden recorrer deslizando el dedo hacia la parte superior de la pantalla del terminal. El símbolo ">" a la derecha de cada ajuste proporciona acceso al resto de elementos asociados a la configuración del mismo:

Figura 13– Menú "Ajustes" de iOS 12 (1).

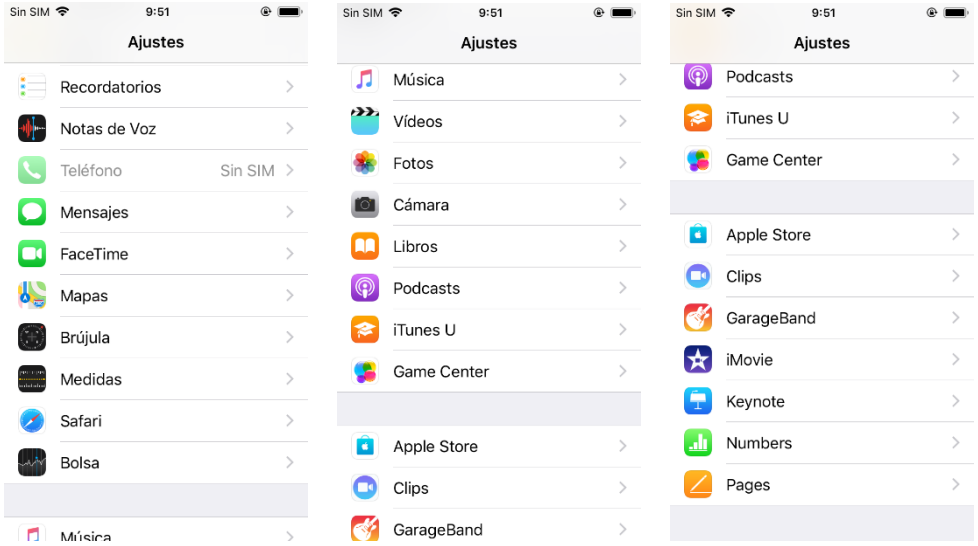


Figura 14 – Menú "Ajustes" de iOS 12 (2).

A lo largo de los sucesivos apartados se describirán los ajustes relacionados con la seguridad y privacidad, correspondientes a las distintas secciones que integran este menú. Adicionalmente, se recomienda definir los siguientes ajustes desde el punto de vista de seguridad (no se incluyen en un apartado propio por ser muy concretos):

Sonidos

- Clics del teclado (activa por defecto): se aconseja desactivar esta opción, que ocasiona la emisión de un sonido cuando se pulsa una tecla, incluso al introducir contraseñas o el propio código de acceso. Un potencial atacante podría conocer la longitud de la contraseña contando el número de clics, disminuyendo así el espectro de prueba en ataques de diccionario o fuerza bruta.
- AirDrop: se aconseja definir un sonido (sirve la "pulsación", definida por defecto), para identificar más fácilmente los intentos de transferencia de archivos.

Batería

- Porcentaje de la batería: se aconseja activar el interruptor para tener mayor control cuándo se debe conectar el dispositivo a la corriente eléctrica, ya que, así, se mostrará en la barra de estado el número que representa el porcentaje de batería disponible. En caso de pérdida del dispositivo móvil, si la batería se agota será imposible utilizar el servicio "Buscar mi iPhone" para localizarlo.
- Modo de bajo consumo: tiene por objeto reducir el consumo de la batería, para lo cual, estando activo, minimiza la actividad de las apps en segundo plano y las actualizaciones automáticas de sus datos. Este modo entra en funcionamiento de forma automática cuando el nivel de batería desciende hasta el 20%, y se desactiva de forma automática cuando llega al 80%. Se recomienda hacer uso de este interruptor para disminuir el tiempo de carga, así como si se prevé que no se podrá recargar la batería antes de que se agote por completo, entre otras razones para no perder el acceso a la funcionalidad "Buscar mi iPhone". Es posible incluir un acceso directo a este modo en el Centro de control.
- Uso de la batería por apps/Mostrar el uso de la batería: permite visualizar el consumo que las apps hacen de la batería. Puede resultar útil para identificar comportamientos no

usuales (por ejemplo, procesos que ejecutan en segundo plano y consumen muchos recursos, que pueden resultar potencialmente maliciosos o, simplemente, tener un fallo de funcionamiento o programación).

Figura 15 – Ajustes de Sonidos y Batería.

9. CUENTAS ASOCIADAS AL DISPOSITIVO MÓVIL

Esta sección encabeza el menú "Ajustes", que, por defecto, muestra el nombre y apellidos definidos por el usuario en la cuenta o ID de Apple asociada al dispositivo móvil. Si se emplea la misma cuenta para iCloud e iTunes/App Store, se mostrará una única dirección (imagen izquierda de la <Figura 16>) o dos (imagen central de la <Figura 16>).

Al seleccionar el símbolo ">" sobre la cuenta, se despliegan sus ajustes:

Figura 16 – Configuración de cuenta de usuario, ID de Apple*, asociada al dispositivo.*

A continuación, se proporcionan las recomendaciones de seguridad (más relevantes) asociadas a los distintos campos de estas subsecciones. La consulta y/o modificación de algunos de ellos

(por ejemplo, el "Nombre") puede requerir la autentificación del usuario a través de la contraseña asociada a la cuenta.

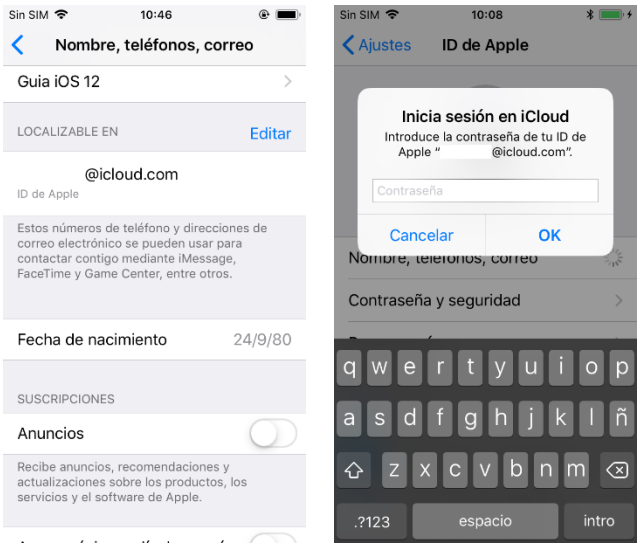


Figura 17 – Solicitud de autentificación en la cuenta del usuario.

Contraseña y seguridad

La contraseña de la cuenta de usuario es el elemento fundamental de protección de la misma y de todos los servicios vinculados a ella, por lo que ***se recomienda seleccionar una contraseña robusta, suficientemente larga, y, preferiblemente, de tipo "passphrase" (frase de paso), en vez de una "password" (palabra de paso).***

- Cambiar contraseña: ***se recomienda cambiar periódicamente la contraseña actual y, en especial, si existe sospecha de que un tercero puede tener conocimiento de la misma***.
- Autenticación de doble factor (2FA): por defecto está ***"Activada" (recomendado)***, con lo cual cada intento de inicio de sesión en la cuenta de iCloud desde otro dispositivo no vinculado actualmente a dicha cuenta (ver apartado "9.4. Dispositivos asociados a la cuenta") requerirá la introducción de un código de verificación, que se enviará al número indicado en el campo "Teléfono de confianza" (ver imagen derecha de la <Figura 16>). A través de "Editar", se permite eliminar el número actual y/o añadir otros adicionales. Es preciso que se disponga de al menos un número de confianza. Esta opción no puede desactivarse desde el dispositivo móvil.
- Teléfono de confianza: es requisito disponer de al menos un teléfono de confianza. Si el usuario dispone de un segundo número de confianza, ***se recomienda añadirlo como respaldo***.
- Obtener un código de verificación: una vez que el dispositivo forma parte de los dispositivos de confianza asociados a la cuenta de iCloud, se puede generar en él un código que autorice el acceso a dicha cuenta desde otros dispositivos no vinculados a ella.

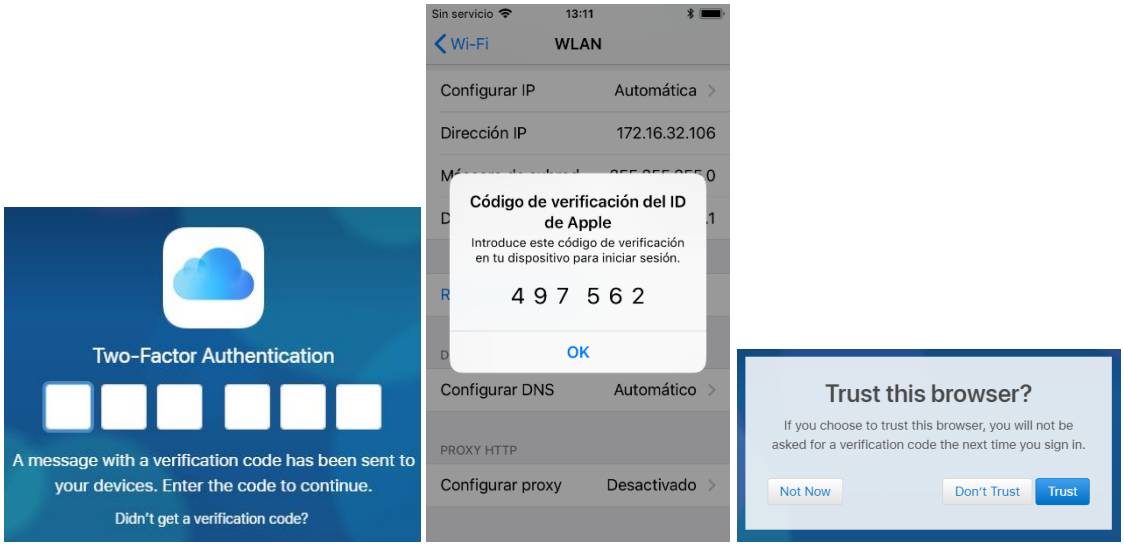


Figura 18 – Segundo factor de autentificación de la cuenta de iCloud.

Pago y envío

La configuración de métodos de pago y envío en el dispositivo móvil no se recomiendan desde el punto de vista de seguridad, por lo que se excluyen del ámbito del presente informe.

9.1 CUENTA DE iCLOUD

iCloud es un servicio de Apple en la nube [Ref.- 6] cuyo objetivo es proporcionar un lugar para el almacenamiento de diversa información, que será compartida por todos los dispositivos móviles vinculados a la misma cuenta de iCloud.

Figura 19 – Ajustes de iCloud.

Se pueden seleccionar las apps cuyos contenidos se sincronizarán con iCloud activando/desactivando los interruptores correspondientes.

Desde el punto de vista de seguridad, los servicios más importantes se describen a continuación. Para que dichos servicios estén disponibles, la sesión en iCloud debe mantenerse abierta en el dispositivo.

Si se desea dejar de hacer uso de los servicios de iCloud, es posible cerrar la sesión a través del menú "Ajustes – [Cuenta de usuario] Cerrar sesión" (ver tercera imagen de la <Figura 16>). ***Se recomienda mantener la sesión de iCloud abierta permanentemente en el dispositivo a fin de poder utilizar estos servicios para disponer del servicio "Buscar mi iPhone".*** Sí se recomienda cerrar la sesión en iCloud si, por cualquier causa, fuese necesario permitir el acceso al dispositivo móvil a un tercero.

Los eventos relevantes relativos al ID de Apple del usuario se notifican a través del correo electrónico de la cuenta asociada a dicho ID de Apple, entre ellos, los relativos a la seguridad de la cuenta, como inicios de sesión desde dispositivos que nunca han sido utilizados previamente para acceder a ella, o cambios en los datos personales asociados a ella. Por tanto, desde el punto de vista de seguridad, ***se recomienda prestar especial atención a los mensajes de correo relativos a la actividad de la cuenta vinculada al* ID de Apple*, a fin de detectar con la máxima rapidez posible situaciones irregulares, pero siendo a su vez conscientes de la existencia de campañas de phishing que hacen uso de mensajes similares a estos para obtener detalles de la cuenta del usuario.***


Tu ID de Apple se ha usado para iniciar sesión en iCloud desde un navegador de Internet

Hace 3 semanas a la(s) 09:53

De Apple Más

Estimado/a Guia iOS 12:

Tu ID de Apple (**l2@icloud.com**) se ha usado para iniciar sesión en iCloud desde un navegador web.

Fecha y hora: 27 de septiembre de 2018, 07:52 UTC
Sistema operativo: Windows

Figura 20 – E-mail relativo a un evento de seguridad en la cuenta de iCloud.

Cuando se configuran apps de terceros para que almacenen su información en la cuenta de iCloud, iOS permite el uso de contraseñas específicas para cada app (por ejemplo, Microsoft Outlook y Mozilla Thunderbird), de forma que no sea necesario que la app acceda a la contraseña asociada al ID de Apple del usuario. El uso de este mecanismo queda fuera del ámbito de la presente guía, pero se pueden consultar los detalles de configuración en la página web oficial de Apple [Ref.- 27].

9.1.1 Buscar mi iPhone

Este servicio permite localizar un dispositivo móvil extraviado, por lo que ***se recomienda tener habilitados los interruptores "Buscar mi iPhone" y "Enviar última ubicación"***.

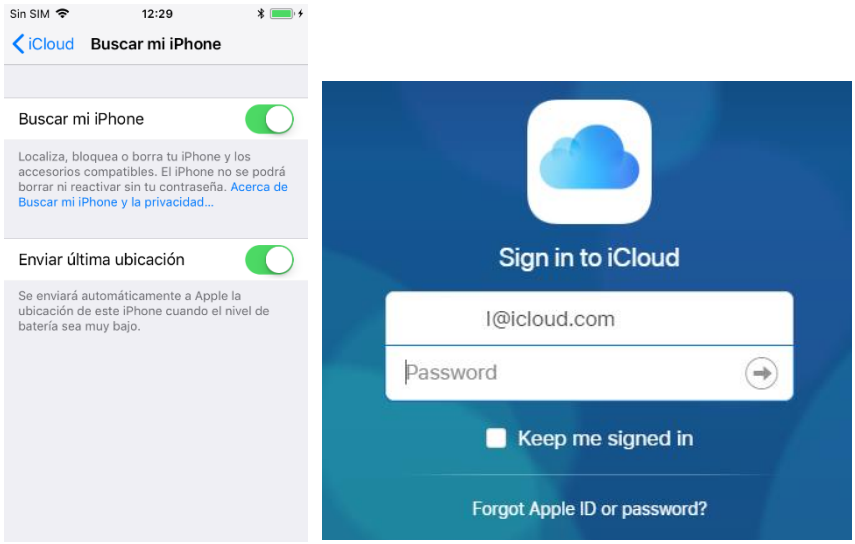


Figura 21 – Menú de ajustes "Buscar mi iPhone" e interfaz web de acceso a iCloud.

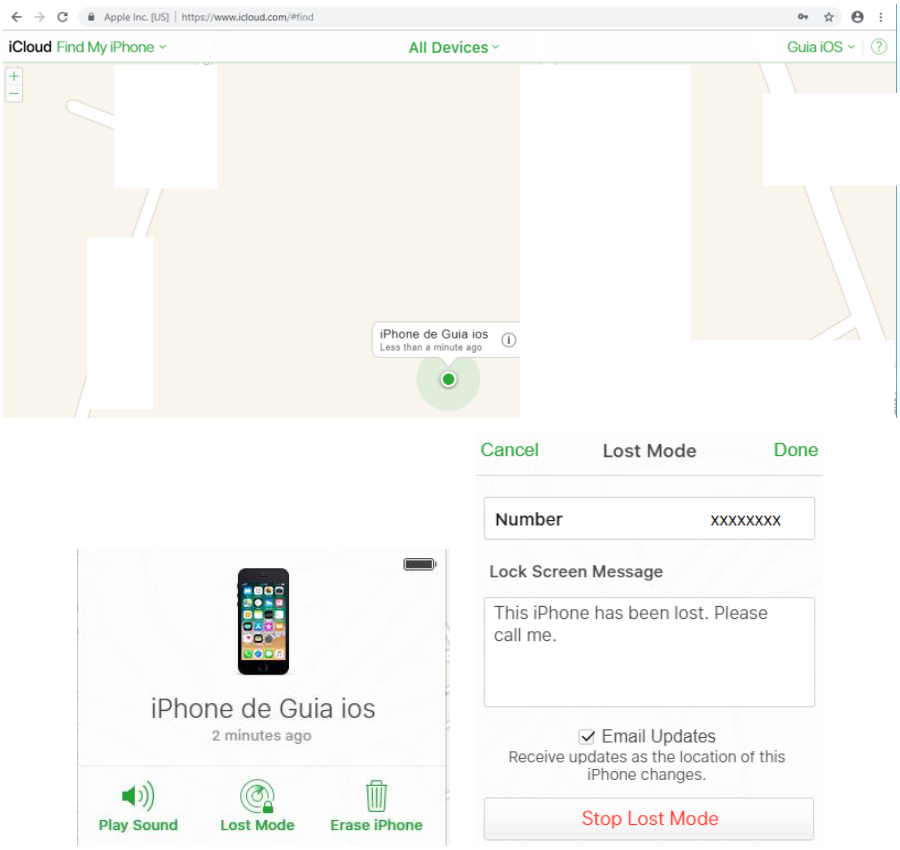


Figura 22 – Interfaz web del servicio "Buscar mi iPhone" en iCloud.

Al activar este ajuste, será posible hacer uso del servicio de localización del dispositivo disponible en la web "https://www.icloud.com/#find". Para que el servicio funcione correctamente, se requiere:

- Tener activa la sesión en iCloud en el dispositivo móvil.

- Iniciar sesión en dicha cuenta de iCloud en el dispositivo desde el que se vaya a invocar el servicio (imagen superior de la <Figura 22>).
- Disponer de conexión vía Wi-Fi y/o de red de datos móviles en el dispositivo.
- Disponer de información de localización (GPS, Wi-Fi, o telefonía) desde el dispositivo.

Una vez autenticado, el usuario obtendrá la vista de un mapa con la última ubicación obtenida para el dispositivo y, pinchando sobre la misma, se desplegará el mapa más detalladamente y un menú que permite enviar al dispositivo la solicitud de emitir un sonido, entrar en "modo perdido" (*lost mode*), o borrar los contenidos remotamente. La selección de la opción "modo perdido" hará que se envíe una solicitud de bloqueo de forma remota al dispositivo, pudiéndose introducir un número de teléfono del usuario y un mensaje, mostrándose ambos en la pantalla del dispositivo (ver <Figura 23>). Sólo es posible salir de este modo introduciendo el código de acceso correcto en el dispositivo o desactivándolo a través del interfaz de administración de la cuenta de iCloud (imágenes de la <Figura 23>).

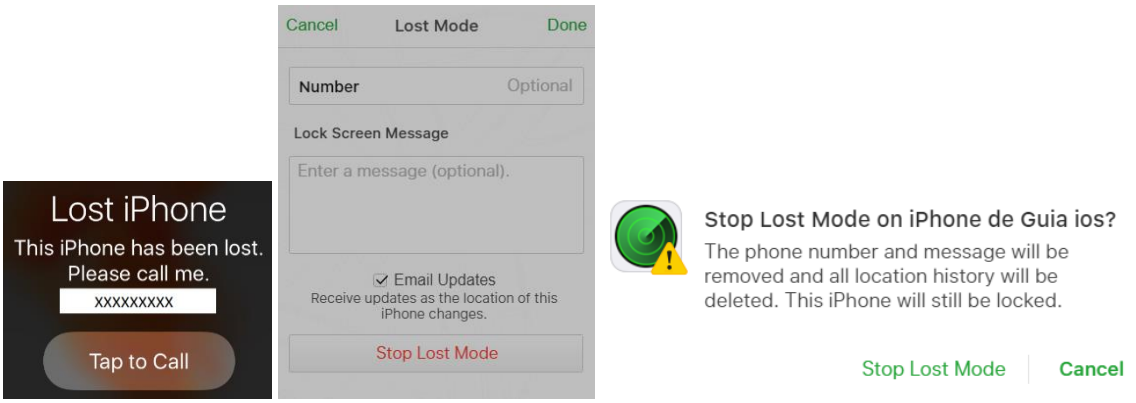


Figura 23 – Pantalla bloqueada mediante "Encontrar mi iPhone": Modo perdido.

Si el dispositivo móvil no puede ser localizado, se mostrará en el interfaz web un mensaje indicándolo y, a través del menú superior de "All devices – <nombre del dispositivo", se podrá habilitar la opción para recibir una notificación cuando se restablezca algún tipo de conexión de datos con él:

Figura 24 – Menú de "Buscar mi iPhone" con un dispositivo inaccesible.

9.2 CUENTA DE iTUNES/APP STORE

La cuenta utilizada para el almacén de contenidos en iTunes (Store) y para la tienda oficial de Apple (App Store) puede estar vinculada en iOS con un ID de Apple diferente del empleado para la cuenta de iCloud. Esta cuenta es la que se empleará para la descarga de contenidos (multimedia, música, libros, apps y actualizaciones de iOS).

Dentro de los ajustes de configuración, se encuentra "Ajustes de contraseña". Desde el punto de vista de seguridad, ***se recomienda activar las opciones "Solicitar siempre" y "[Descargas gratuitas] Solicitar contraseña"*** para poder tener control de qué contenidos se instalan en el dispositivo. La modificación de cualquier campo de esta sección requerirá que la sesión en la cuenta de iTunes/App Store se encuentre activa.

Figura 25 – Ajustes de seguridad de iTunes (Store) y App Store.

9.2.1 Gestión de las apps

Una vez instalada una app, además de controlar qué permisos se le conceden (ver apartado "17. Ajustes de privacidad: Permisos de las apps") es posible:

- Borrarla a través de "Ajustes – General – Almacenamiento del iPhone – [Nombre de la App]" (<Figura 26>): la opción "Desinstalar app" elimina los ficheros binarios de la app, manteniendo los datos y configuración de la misma, que estarán disponibles si se reinstala; la opción "Eliminar app" elimina también todos los ficheros y datos asociados a la app.
- Actualizarla automáticamente a través de "Ajustes – General – Actualizar en segundo plano: Sí | No" (imagen izquierda de la <Figura 26>). Si se selecciona "No", la app podrá actualizarse manualmente accediendo a la sección "App Store – Actualizaciones".

Desde el punto de vista de seguridad, ***se recomienda mantener las apps actualizadas para evitar vulnerabilidades ya resueltas en versiones recientes, pero realizar actualizaciones manuales (***"Ajustes – General – Actualización en segundo plano - No"***) para controlar qué funcionalidades añade o suprime la nueva versión, incluyendo las modificaciones a los términos y condiciones de uso.***

iOS ofrece también la opción de "Quitar apps no usadas" (imagen derecha de la <Figura 26>, que, estando activa, elimina del dispositivo móvil las apps que no se han usado recientemente, pero manteniendo los datos asociados a ellas. Las apps desinstaladas a causa de esta opción aparecerán en la pantalla Home con el símbolo "☁", y, para reinstalarlas, no será necesario abrir la App Store, sino únicamente pulsar sobre ese icono. Esta opción se configura a través de la opción "Ajustes – General – Almacenamiento del iPhone – Quitar apps no usadas", y, una vez activa, se puede desactivar a través del interruptor "Ajustes – iTunes Store y App Store – Desinstalar apps no utilizadas".

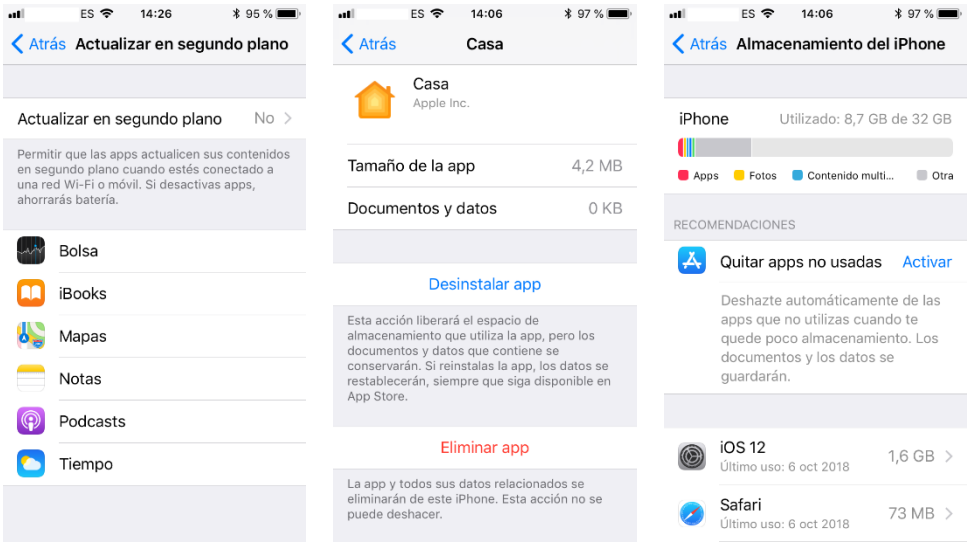


Figura 26 – Gestión de apps en el dispositivo móvil.

9.3 SECCIÓN "CONTRASEÑAS Y CUENTAS"

A través de la sección "Ajustes –Contraseñas y cuentas" se gestiona la configuración asociada a las cuentas existentes en el dispositivo móvil, y se permite añadir nuevas cuentas y cerrar la sesión activa en el dispositivo para dicha cuenta.

Es posible bloquear la adición de nuevas cuentas en el dispositivo móvil estableciendo una restricción (ver apartado "17.1. Restricciones"), concretamente a través del ajuste "Ajustes – Tiempo de uso – Contenido y privacidad – [Permitir cambios] Cambios en la cuenta".

Se recomienda establecer este parámetro a "No permitir" para fijar esta restricción como medida de seguridad.

Bajo la sección "Contraseñas de webs y apps" es posible añadir las credenciales de apps y sitios webs determinados, de forma que, cuando se acceda a ellos, iOS rellenará automáticamente los datos sin que el usuario deba introducirlos. Para poder definir un nuevo login mediante la opción el botón "+", se deberá introducir la huella (si Touch ID está configurado en el dispositivo móvil) o el código de acceso (si Touch ID, o Face ID, no está activo; ver apartado "10.2. Touch ID"). Se aconseja consultar el apartado "15. Navegador web Mobile Safari" para más información sobre el uso de este servicio en el acceso a sitios web.

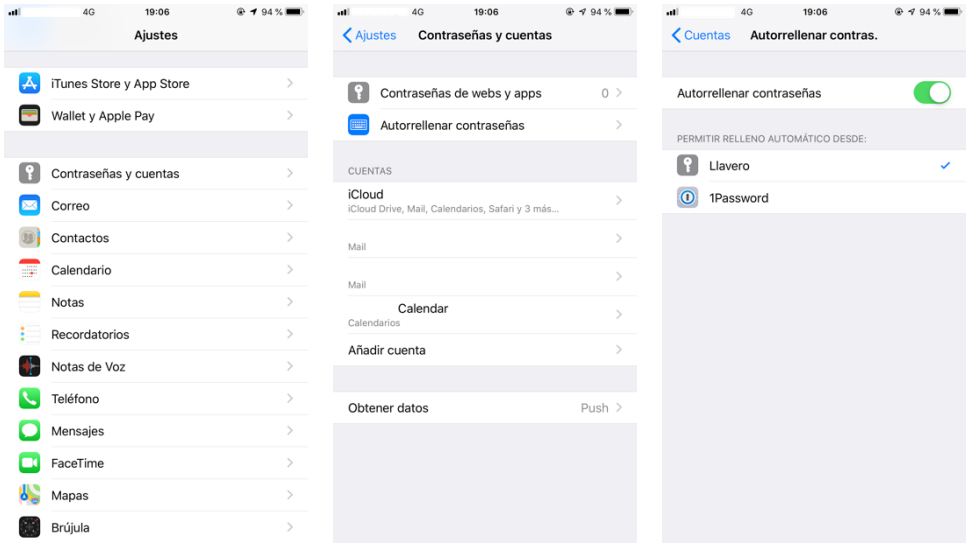


Figura 27 – Sección "Contraseñas y cuentas".

Desde el punto de vista de seguridad, el uso de un gestor de contraseñas simplifica la tarea de recordar múltiples credenciales, y favorece que el usuario seleccione contraseñas más complejas y que no las reutilice en distintos servicios o sitios web. No obstante, no hay que perder de vista el riesgo de que el dispositivo móvil sea sustraído, pudiendo ocurrir que el atacante se pueda validar en todos aquellos sitios configurados dentro del gestor. En iOS 12 se ha introducido un nuevo servicio que notifica al usuario reutiliza una misma contraseña en diferentes servicios.

9.3.1 Autorrellenar contraseñas y códigos de seguridad en iOS 12

Bajo la sección "Contraseñas de webs y apps" es posible añadir las credenciales de sitios webs determinados, de forma que, cuando se acceda a ellos, iOS rellenará automáticamente el usuario y la contraseña sin que el usuario deba introducirlos.

Adicionalmente, iOS 12 introduce la funcionalidad "Autorrellenar contraseñas" (*password autofill*), que, estando activa, utilizará las credenciales almacenadas para apps y sitios web en los gestores de contraseñas que soporten la integración con este servicio (y que se hayan habilitado mediante el "tick" correspondiente del menú de la imagen derecha de la <Figura 27>), y se rellenarán de forma automática. Los gestores de contraseñas disponibles se mostrarán en la lista "Permitir autorrelleno automático desde" (en la imagen derecha de la <Figura 27>, se dispone del gestor "Llavero" (ver apartado "9.5. Llavero de iCloud") y "1Password"[12]). Es posible habilitar más de un gestor, e iOS seleccionará de forma automática las credenciales asociadas al login que se presente. Para hacer uso del autorrelleno, el usuario debe introducir el método acceso solicitado en el menú de diálogo.

Complementariamente, iOS 12 introduce el denominado "relleno automático de códigos de seguridad" (*security code autofill*), que se activa mediante la misma opción y captura los mensajes SMS asociados a contraseñas o códigos de un solo uso y muestra la opción de autorrellenar automáticamente el código recibido en la app destinataria a través de la barra "QuickType" (disponible en la parte superior del teclado), requiriendo simplemente realizar

[12] Algunos gestores de contraseñas soportados son Last Pass (https://www.lastpass.com/es), Dashlane (https://www.dashlane.com/es/) y 1Password (https://1password.com/es/).

una pulsación sobre él para que el código se inserte automáticamente en el campo correspondiente. Esta función pretende simplificar de cara al usuario la introducción de credenciales asociadas a un segundo factor de autentificación (2FA). Para detectar cuándo un SMS puede corresponder a un código, se utilizan elementos heurísticos como inclusión en el texto de las palabras "código" o "contraseña".

Desde el punto de vista de seguridad, el uso de un gestor de contraseñas simplifica la tarea de recordar múltiples credenciales, y favorece que el usuario seleccione contraseñas más complejas y que no las reutilice en distintos servicios o sitios web. No obstante, no hay que perder de vista el riesgo de que el dispositivo móvil sea sustraído, pudiendo ocurrir que el atacante se pueda validar en todos aquellos sitios configurados dentro del gestor. Si se opta por hacer uso de las capacidades del gestor de contraseñas, ***se recomienda realizar la validación en el mismo a través del código de acceso al dispositivo, que deberá ser lo más robusto posible, frente al uso de Touch ID o Face ID.***

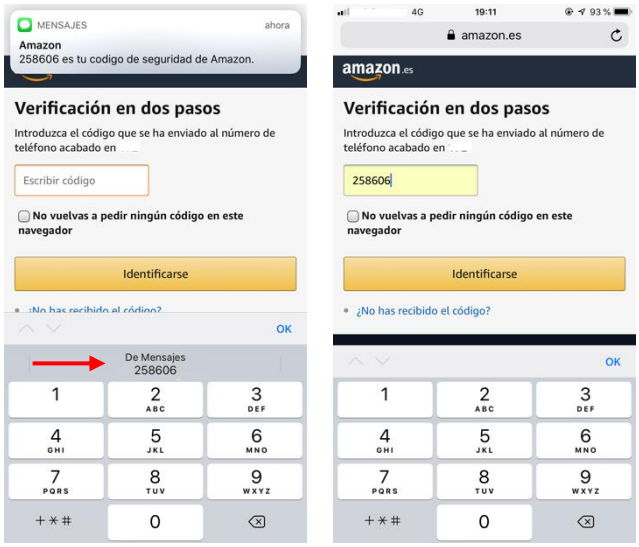


Figura 28 - Función de autorrellenar códigos de un solo uso recibidas por SMS.

9.4 DISPOSITIVOS ASOCIADOS A LA CUENTA

Tras la activación del dispositivo móvil y la configuración de la cuenta de usuario que se utilizará como ID de Apple, el dispositivo móvil se añadirá al apartado correspondiente de la sección "Ajustes – ID de Apple", como se observa en la parte inferior de la <Figura 16>. Los detalles asociados a él se acceden pulsando sobre ">". Los ajustes correspondientes a "Buscar mi iPhone", así como las recomendaciones de seguridad, se describen en el apartado "9.1.1. Buscar mi iPhone". Los detalles del ajuste "Copia en iCloud" se describen en el apartado "19.1. Copia y restauración en iCloud".

Cualquier intento de inicio de sesión utilizando el mismo ID de Apple de iCloud en otro dispositivo diferente, provocará que se muestre en la pantalla el mensaje de la segunda imagen de la <Figura 29> solicitando confirmación. Si se selecciona "Permitir", el dispositivo móvil mostrará el código a introducir en el nuevo dispositivo; si el código es correcto, el nuevo dispositivo se añadirá a la lista de dispositivos vinculados y pasará a poder recibir a su vez códigos de verificación del ID de Apple en lo sucesivo y también podrán consultarse sus detalles:

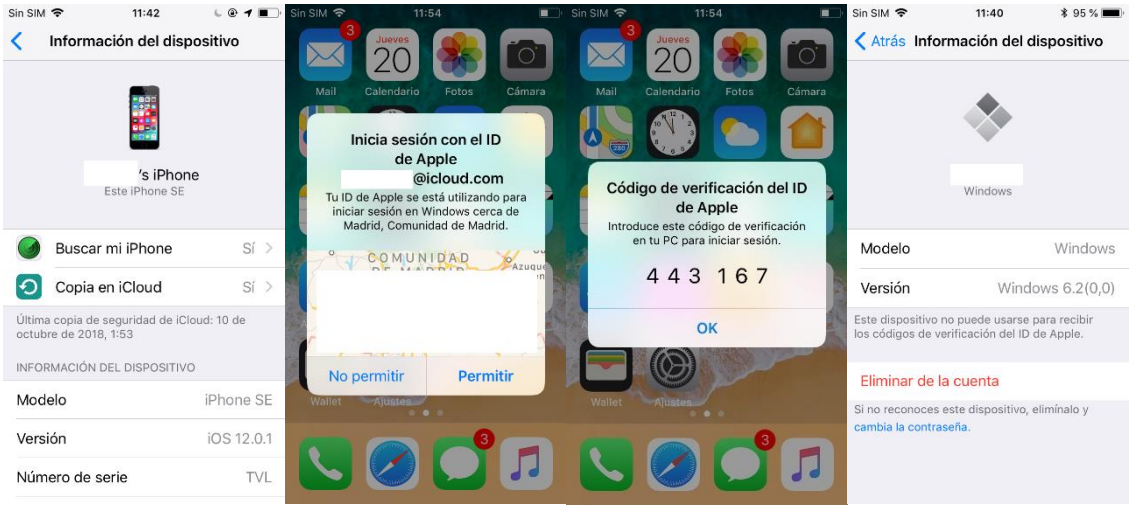


Figura 29 – Dispositivos vinculados al ID de Apple *asociado al dispositivo móvil.*

Desde el punto de vista de seguridad, ***se recomienda prestar atención a los mensajes de inicio de sesión para detectar cualquier acceso no permitido a la cuenta de usuario vinculada al ID de Apple. Asimismo, si un dispositivo considerado de confianza deja de serlo (en especial, si ha sido sustraído), o si se requiere acceder temporalmente a la cuenta de usuario desde un dispositivo ajeno, se recomienda proceder a "Eliminar de la cuenta" dicho dispositivo tan pronto sea posible*** (imagen derecha de la <Figura 29>).

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 del servicio y la licencia de iOS. Sin embargo, no permite seleccionar o modificar el nombre del dispositivo móvil, que quedará establecido a "<tipo de dispositivo> <Nombre del usuario en la cuenta iCloud>". El nombre del dispositivo se puede modificar posteriormente a través de "Ajustes – General – Información", lo cual se recomienda desde el punto de vista de seguridad para no revelar ni el modelo hardware ni el usuario, por ejemplo, en búsquedas Bluetooth.

9.5 LLAVERO DE iCLOUD

Desde iOS 7.0.3, Apple proporcionó nuevas capacidades centralizadas de almacenamiento de credenciales, similares a las de otros gestores de contraseñas, en el repositorio denominado *keychain* a través de iCloud (de lo cual surge el apelativo de "llavero de iCloud" o *iCloud Keychain*). En este repositorio se pueden almacenar credenciales (usuario + contraseña) de sitios web, apps, contraseñas de redes Wi-Fi, e información de tarjetas de crédito.

El llavero de iCloud permite almacenar el *keychain* local existente en iOS y macOS en iCloud, de manera supuestamente segura, mediante la utilización de cifrado AES de 256 bits (AES 256), haciendo posible su utilización y compartición entre los diferentes dispositivos Apple asociados a una misma cuenta de iCloud, tanto móviles como tradicionales.

El llavero de iCloud sólo sincroniza aquellos elementos del *keychain* del usuario que han sido identificados con el atributo que permite su sincronización entre dispositivos, es decir, que son exportables o 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. Por defecto, los elementos añadidos al llavero por las apps de terceros están identificados por defecto como no sincronizables, debiendo el desarrollador de la app modificar el atributo si desea que sea compartido entre diferentes dispositivos.

Tanto la versión de Mobile Safari disponible en iOS como la de macOS se integran directamente con el llavero de iCloud, permitiendo el almacenamiento de credenciales y tarjetas de crédito, su reutilización, e incluso la generación y almacenamiento de nuevas contraseñas (a través de un generador de contraseñas). Esta funcionalidad de Safari se complementa con capacidades para autocompletar formularios web.

La funcionalidad del llavero de iCloud se habilita/deshabilita a través de "Ajustes – [Cuenta de usuario] – iCloud – Llavero" (ver segunda imagen de la <Figura 19>). Si se desea desactivar el uso del llavero de iCloud, se podrá optar por mantener las credenciales almacenadas en el *keychain* local o eliminarlas del dispositivo móvil (ver imagen derecha de la <Figura 19>).

Desde el punto de vista de seguridad, ***se debe valorar si se confía plenamente en Apple para la custodia en la nube de las contraseñas, así como tener en cuenta que, al estar disponibles en todos los dispositivos de un usuario (se empleen o no todas las credenciales en todos los dispositivos), basta con que uno de ellos sea comprometido para que todas las contraseñas puedan quedar expuestas***.

10. ACCESO FÍSICO AL DISPOSITIVO MÓVIL

La posibilidad de disponer de acceso físico al dispositivo móvil permitiría a un potencial atacante acceder a los contenidos del mismo, así como hacer uso de los servicios de telefonía móvil y en la nube disponibles, por lo que se recomienda fervientemente proteger este acceso a través de un código de acceso. Se distinguen dos tipos de código: el de la tarjeta SIM (PIN de la tarjeta SIM) y el de desbloqueo (o acceso) del dispositivo.

El PIN de la tarjeta SIM se solicita, si está configurado, cuando se reinicia el dispositivo móvil, o si la tarjeta SIM es extraída temporalmente y vuelta a introducir (ver imagen izquierda de la figura <Figura 30>). Se dispone de un máximo de tres intentos para el desbloqueo de la tarjeta SIM, mostrándose el número de intentos restantes en la pantalla de solicitud del PIN. Si se agotan, para poder desbloquear la tarjeta SIM, se requerirá introducir la contraseña de desbloqueo denominada PUK (*PIN Unlock Key*).

El acceso físico al dispositivo móvil es posible, aunque no se defina un PIN para la SIM.

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":

Figura 30 – Configuración del PIN de la tarjeta SIM.

En el caso de dispositivos móviles que traen un PIN asociado a la tarjeta SIM fijado por el operador de telefonía móvil, se recomienda modificar el valor por defecto del PIN y emplear una secuencia numérica preferiblemente de 8 dígitos, que no sea fácilmente adivinable y que excluya valores típicos como 0000, 1111 ó 1234. La no existencia de un PIN para la tarjeta SIM permitiría a un potencial atacante, con acceso físico al terminal, extraer la tarjeta SIM y hacer uso de la misma en otro dispositivo, incluidos sus servicios y capacidades de telefonía móvil asociados.

iOS almacena en memoria el PIN de la tarjeta SIM, por lo que no lo solicitará al usuario cuando el dispositivo móvil salga del "Modo avión" (ver apartado "11. Conexiones inalámbricas y redes") para reactivar los servicios de telefonía móvil.

10.1 CÓDIGO DE ACCESO DEL DISPOSITIVO MÓVIL

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. 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 ("Emergency"):

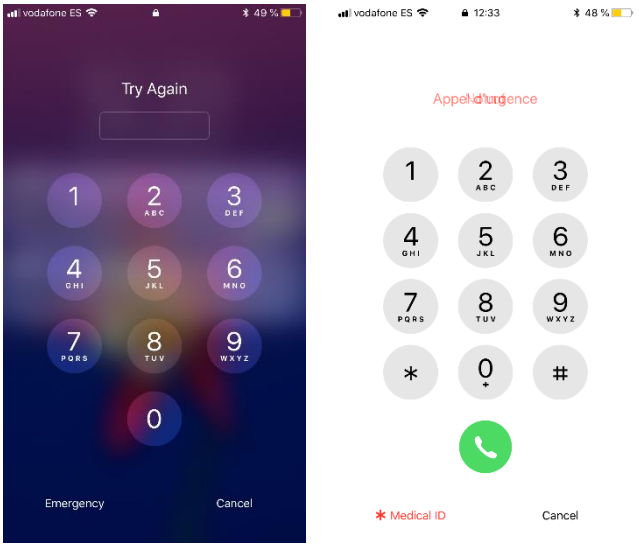


Figura 31 – Pantalla de solicitud del código de acceso.

Desde el punto de vista de seguridad, ***la principal recomendación es disponer en todo momento de un código de acceso al dispositivo lo más robusto posible, al igual que proteger el acceso a los servicios de telefonía y datos móviles definiendo un PIN para la tarjeta SIM (de al menos 4 dígitos, pero preferiblemente de 8 dígitos)***.

Por defecto, los dispositivos móviles basados en iOS no obligan a disponer de un código de acceso para bloquear accesos no autorizados al terminal, pero se incita a su configuración durante la activación (ver apartado "6. Proceso de Activación del dispositivo móvil"). Si no se definió un código de acceso durante la activación, se recomienda establecerlo lo antes posible a través del menú "Ajustes – Touch ID y Código – Cambiar código". Si ya existe un código establecido, para acceder a este menú se solicitará el código vigente:

Figura 32 – Menú de configuración del código de acceso.

iOS 12 ofrece por defecto establecer una contraseña de 6 dígitos, pero se puede elegir entre otros tres tipos de contraseña de acceso mediante el botón "Opciones de código". Desde el punto de vista de seguridad, ***la recomendación es configurar un código numérico o***

alfanumérico de al menos 8[13] caracteres, que no sea sencillo de adivinar ni contenga nombres de personas/animales o fechas fácilmente asociables al usuario del dispositivo[14]. Se desaconseja la utilización de un código numérico de 4 dígitos (o de 6 dígitos, ya que ambos revelan su longitud), que resulta muy sencillo de romper con los medios disponibles actualmente, y también se desaconseja hacer coincidir el código del PIN de la tarjeta SIM con el código de acceso. La longitud mínima permitida por iOS para un código alfanumérico son 4 caracteres.

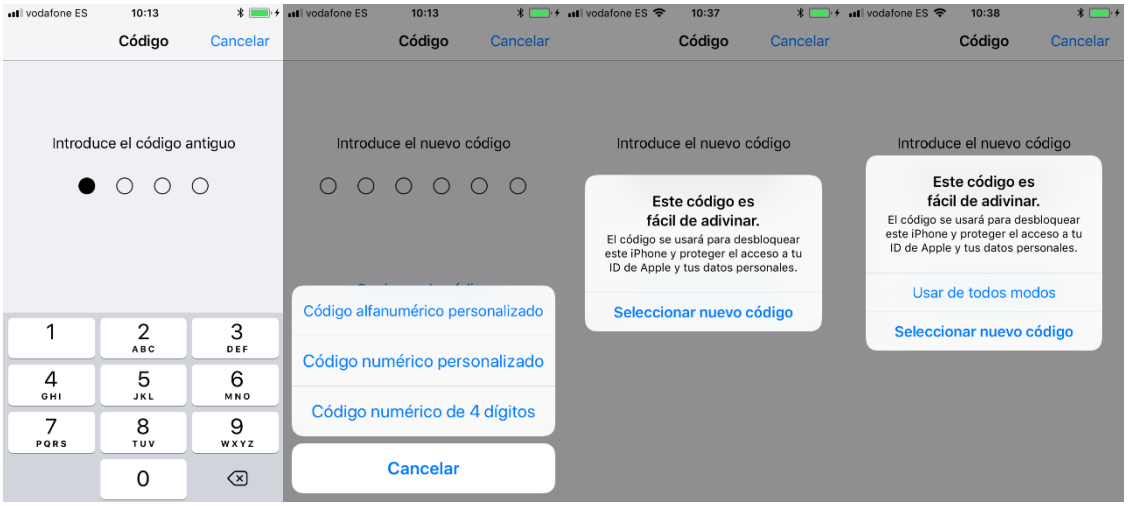


Figura 33 – Configuración de un nuevo código de acceso.

Si iOS 12 detecta que el nuevo código introducido es idéntico al usado previamente, mostrará el mensaje de la tercera imagen de la <Figura 33> y no permitirá repetirlo. Si detecta que el código es demasiado sencillo, mostrará el mensaje de la cuarta imagen de la <Figura 33>, pero permitirá al usuario utilizarlo si presiona "Usar de todos modos".

iOS incrementa la dificultad de adivinar el código por ensayo/error, forzando a que transcurra un tiempo entre intentos fallidos al introducir el código vigente, tanto al introducirlo en la pantalla de bloqueo, como durante la configuración de un código nuevo: tras 5 intentos fallidos, deberá esperarse 1 minuto antes de poder volver a introducir el código (imagen derecha de la <Figura 34>); al sexto, se deberá esperar 5 minutos; al séptimo y octavo, 15 minutos, para cada intento. Tras el noveno intento y sucesivos, deberá esperarse una hora (60 minutos) por cada intento.

[13] Guide to iOS estimated passcode cracking times (assumes random decimal passcode + an exploit that breaks SEP throttling): https://twitter.com/matthew_d_green/status/985885001542782978

[14] La información publicada por el propietario de un dispositivo móvil en las redes sociales puede servir a un potencial atacante como punto de partida para adivinar el código de acceso al dispositivo.

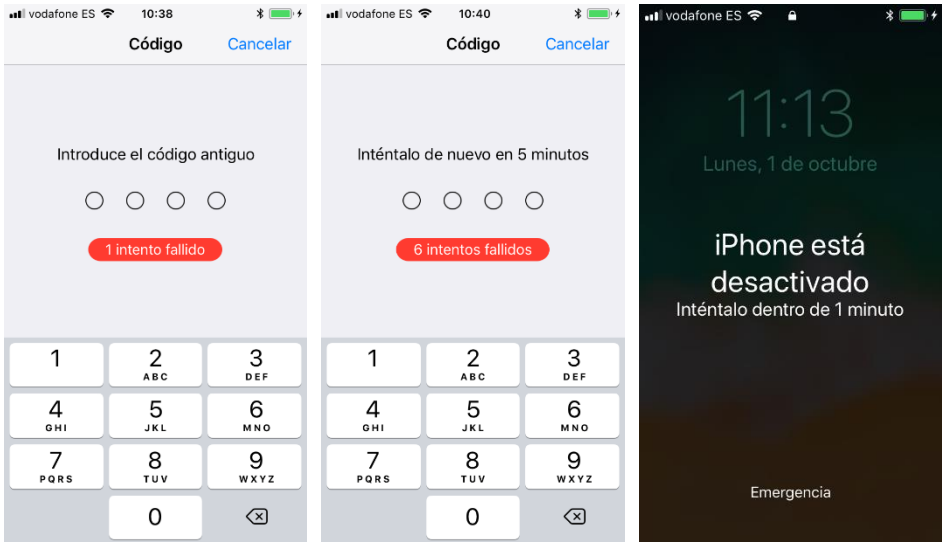


Figura 34 – Mensaje de intento fallido en el cambio de código de acceso.

Si se introduce el código erróneamente múltiples veces, con retardos de tiempo elevados que hacen que el dispositivo esté bloqueado [Ref.- 7], y se desconoce el valor del código, solo será posible desbloquearlo eliminando los datos (que podrán restaurarse desde una copia de seguridad realizada mediante iTunes; se recomienda consultar el apartado "17.1. Restricciones" para más información).

Además, se añade un nivel extra de seguridad mediante la opción "Borrar datos" (imagen derecha de la <Figura 32>), consistente en la eliminación de los datos del dispositivo móvil al décimo intento erróneo. Estos datos no se borrarán de la cuenta asociada al ID de Apple del dispositivo, por lo que podrían ser recuperados por el usuario si dispone de una copia de seguridad en iCloud (o a través de iTunes).

Al cambiar el código (o al introducir el vigente desde cualquier pantalla que lo solicite), se destacarán brevemente en pantalla los caracteres introducidos, por lo que ***se recomienda introducir el código de acceso de forma que un tercero no pueda disponer de acceso visual a la pantalla***.

Existen también ajustes para determinar cuándo es necesario introducir de nuevo el código de acceso al utilizar el dispositivo móvil:

- "Ajustes – Pantalla y Brillo – Bloqueo automático": determina cuándo se bloqueará (o suspenderá) la pantalla del dispositivo móvil tras un tiempo de inactividad (modo reposo). ***Se recomienda fijarlo a un valor de entre 1 y 2 minutos*** (imágenes 1 y 2 de la <Figura 35>)***.***
- "Ajustes – Touch ID y código – Solicitar": determina cuándo se solicitará el código de acceso tras haber sido el dispositivo móvil bloqueado (o suspendido) por inactividad, en base al ajuste previo, o de forma manual por el usuario. ***Se recomienda fijarlo a "De inmediato"*** (imágenes 3 y 4 de la <Figura 35>)***.***

Figura 35 – Configuración del bloqueo automático de pantalla.

La introducción de un código de acceso erróneo producirá la emisión de un sonido acompañado de una vibración del dispositivo móvil.

No es posible modificar de forma remota el código de acceso, aunque sí se puede activar el mismo a través del servicio "Buscar mi iPhone" (ver apartado "9.1.1. Buscar mi iPhone"), que también permite fijar un código de acceso en el dispositivo si, pese a las recomendaciones, no se dispusiese de uno actualmente.

10.2 TOUCH ID

"Touch ID" es un sistema biométrico de reconocimiento de huella dactilar mediante hardware para dispositivos móviles iOS, que se encuentra integrado en el botón de "Home", para facilitar su utilización. Touch ID puede ser empleado para desbloquear el dispositivo móvil, y permite tanto realizar compras en la App Store como validar al usuario en apps de terceros, en lugar de emplear las credenciales asociadas al login del servicio proporcionado por la app.

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 inapropiados. Tras tres intentos fallidos, se solicitará repetir la huella o el código de acceso. Al quinto, solo será posible introducir el código. Adicionalmente, el código de acceso es obligatorio:

- Tras reiniciar el dispositivo móvil.
- Transcurridas 48 horas sin que haya sido desbloqueado.
- Para registrar nuevas huellas en Touch ID (se permiten hasta cinco huellas).
- Tras bloquearse el dispositivo móvil desde el interfaz "Buscar mi iPhone".
- Tras hacer uso de una llamada de emergencia o acceder al ID médico.

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 (del apartado previo; equivalente a la opción "De inmediato") para determinar cuándo es necesario introducir de nuevo el código de acceso.

Para configurar Touch ID, se dispone del menú "Ajustes – Touch ID y código" (ver imagen 2 de la <Figura 32>). Una vez dada de alta una huella (los detalles sobre cómo realizar este proceso se pueden consultar en la [Ref.- 8]), se puede optar por utilizarla para:

- Desbloqueo del dispositivo móvil.
- Apple Pay.
- iTunes Store y App Store.
- Consultar las contraseñas almacenadas en el dispositivo (ver apartado "9.3. Sección "Contraseñas y cuentas"").

Desde la aparición de Touch ID, la comunidad de seguridad continúa encontrando mecanismos para saltarse esta protección biométrica (como ejemplo, se proporcionan enlaces descriptivos en la [Ref.- 10]). Por ello, ***desde el punto de vista de seguridad, se considera que los mecanismos basados en biometría son menos robustos que los basados en un código de acceso suficientemente complejo, aunque potencialmente más recomendables desde el punto de vista de la usabilidad***. En caso se optarse por hacer uso de Touch ID para autentificación en apps o servicios de terceros, se aconseja comprobar que la app no permite reconocer una nueva huella añadida con posterioridad sin necesidad de revalidar las credenciales propias.

10.3 FACE ID

Face ID es un sistema de biometría basado en reconocimiento facial adaptativo vía hardware, que se introdujo por primera vez en iPhone X, junto a iOS 11, reemplazando el acceso mediante huella (Touch ID).

Nota: Debido a que el dispositivo empleado para la elaboración de la presente guía dispone únicamente de Touch ID, otros modelos de iPhone y iPad con soporte para Face ID dispondrán del menú "Face ID y código" en lugar del menú "Touch ID y código" mencionado.

Los dispositivos móviles iPhone XS, XS Max y iPhone XR, liberados en paralelo con iOS 12, han reemplazado también el acceso mediante huella (Touch ID) por el reconocimiento facial de Face ID. Utilizan un procesador denominado "*Secure Enclave Processor (SEP)*", en el que se almacenan (supuestamente de forma segura) los patrones que permiten el reconocimiento del rostro del usuario, y que reside en el chip A12 Bionic de estos dispositivos.

Además de permitir el desbloqueo del terminal, Face ID (al igual que Touch ID) proporciona funcionalidades para el inicio de sesión y autentificación dentro de las apps, y la realización de pagos. La configuración de Face ID queda fuera del alcance de la presente guía, pero se puede consultar más información en [Ref.- 9].

Desde el punto de vista de seguridad, aunque Apple afirma que la tecnología de reconocimiento facial es más segura que la de reconocimiento de huella dactilar (1:1.000.000 frente a 1:50.000 [Ref.- 24]), hay evidencias de que no es infalible ante, por ejemplo, gemelos o la creación de máscaras en tres dimensiones con los rasgos faciales del usuario [Ref.- 13].

Para deshabilitar el uso del reconocimiento facial permanentemente, se dispone del menú "Face ID y código". Para inhabilitarlo de forma temporal, por ejemplo, ante una situación de emergencia en la que se sospeche que un tercero puede tratar de sustraer y desbloquear el dispositivo móvil enfrentando la cara del usuario ante la cámara, se puede recurrir al procedimiento descrito para Touch ID en el apartado "10.4. Medical ID (Emergencia SOS)".

10.4 MEDICAL ID (EMERGENCIA SOS)

El denominado "*Medical ID*" (o identificador o ID médico) es una característica de la app "Salud" (*Health*) cuyo objeto es proporcionar datos médicos importantes al personal sanitario a cargo de asistir al usuario del dispositivo móvil en caso de emergencia. Entre la información que se puede introducir se encuentran las alergias a medicamentos, la medicación que se toma regularmente, o el grupo sanguíneo. Es posible activar el interruptor "Ver cuando está bloqueado" durante la configuración de esta funcionalidad (o, posteriormente, a través de la app "Salud"), lo cual permitirá que, cuando se pulse la opción "Datos médicos" desde la pantalla de bloqueo (imagen central de la <Figura 36>), o pulsando 5 veces seguidas el botón de encendido (imagen derecha de la <Figura 36>), alguien con acceso físico al terminal pueda consultar esta información.

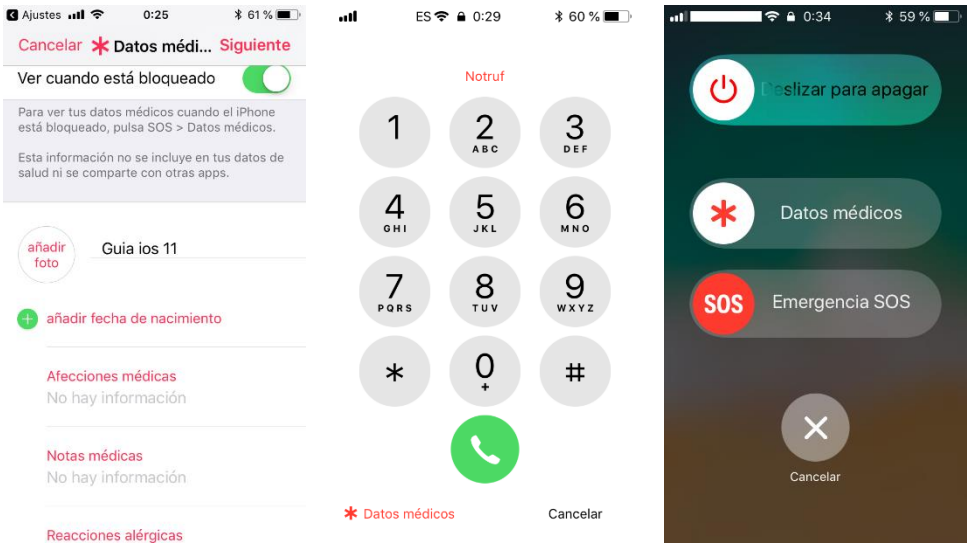


Figura 36 – Emergencia SOS (Medical ID).

Aunque la configuración detallada del "Medical ID" está fuera del alcance de la presente guía (se puede consultar la [Ref.- 20] para más información), es importante conocer que su invocación desactiva el acceso al dispositivo móvil a través de los mecanismos de biometría (Touch ID o Face ID). Por ello, este mecanismo puede ser útil ante una situación de riesgo en la que el usuario tema verse obligado a desbloquear el terminal mediante estos medios (por ejemplo, en un control de aeropuerto), limitando el desbloqueo del dispositivo móvil mediante la introducción del código de acceso.

10.5 AJUSTES ADICIONALES DE "TOUCH ID Y CÓDIGO"

Desde el punto de vista de seguridad, ***se aconseja desactivar todas las opciones de la sección "Ajustes – Touch ID y código – Permitir acceso al estar bloqueado", incluyendo*** "Visualización hoy", "Marcación por voz", "Notificaciones recientes", "Centro de control", "Siri", "Responder con mensaje", "Control de casa", "Wallet" y "Devolver las llamadas perdidas", ***para evitar que un tercero pueda realizar acciones indeseadas desde la pantalla de bloqueo***.

La opción "Accesorios USB", cuya desactivación también se aconseja, evita que se pueda acceder mediante una conexión de datos vía USB al dispositivo móvil si éste ha permanecido bloqueado durante más de una hora.

En el caso de iOS 12, adicionalmente, la conexión de datos vía USB se deshabilitará si han pasado más de 3 días (72 horas) desde que el dispositivo hizo uso de una conexión de datos vía USB por última vez, o si se han deshabilitado los mecanismos de autentificación biométrica y se requiere el código de acceso.

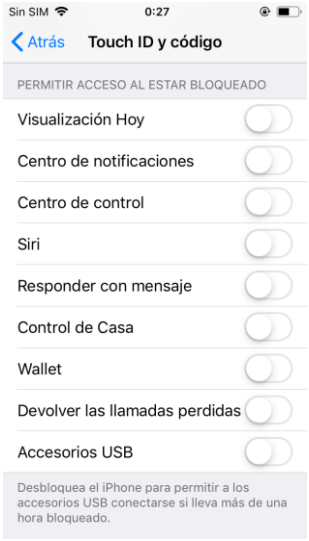


Figura 37 – Ajustes recomendados con la pantalla bloqueada.

11. CONEXIONES INALÁMBRICAS Y REDES

Las conexiones inalámbricas (Bluetooth, datos móviles y Wi-Fi) dotan al dispositivo móvil de las capacidades de comunicación. Su gestión se puede realizar desde el menú "Ajustes", y también a través del Centro de control (ver apartado "7.2. Centro de control"), y el estado de cada una de ellas se puede consultar en la barra superior de estado (ver apartado "7.1. Barra superior de estado"), incluso con la pantalla bloqueada.

La opción "Restablecer ajustes de red" del menú "Ajustes – General – Restablecer" (ver <Figura 72>), permite restaurar los ajustes asociados a las redes de comunicaciones a los parámetros de fábrica, sin interferir con el resto de los datos del usuario.

11.1 MODO AVIÓN

El denominado "modo avión" de iOS es un ajuste que, al activarse, deshabilita los interfaces Wi-Fi, Bluetooth, datos y AirDrop. Se localiza en el menú principal de "Ajustes" (ver <Figura 13>) y se representa con un icono de avión en el Centro de control (en color naranja cuando el modo está activo).

En modo avión, el dispositivo móvil carece por completo de conectividad. La conectividad a redes Wi-Fi o Bluetooth puede ser habilitada posteriormente y de forma independiente, pero no así la conectividad ni de telefonía móvil (voz y SMS/MMS) ni de datos móviles 2/3/4G, directamente ligadas al modo avión.

Para salir del modo avión, se puede pulsar de nuevo el icono del Centro de control o activar el interruptor "Modo avión". iOS restaurará el estado de los interfaces de telefonía, de datos móviles, Wi-Fi y Bluetooth a su estado anterior tras salir del modo avión, sin requerirse volver a introducir el PIN de la tarjeta SIM.

Desde el punto de vista de seguridad, el modo avión implica que el dispositivo perderá toda capacidad de comunicación, por lo que la funcionalidad "Buscar mi iPhone" (ver apartado "9.1.1. Buscar mi iPhone") no estará disponible, motivo por el que se desaconseja que esté accesible a través del Centro de control en la pantalla de bloqueo.

11.2 BLUETOOTH

Por defecto, el interfaz Bluetooth se activa tras el proceso activación inicial del dispositivo y también tras aplicar la actualización de una nueva versión de iOS, independientemente de cuál era su estado antes de la actualización. Su estado se controla desde el interruptor "Ajustes – Bluetooth – Bluetooth". Al entrar en este menú, iOS pasará el interfaz Bluetooth al estado visible e iniciará de forma automática y periódica búsquedas de otros dispositivos Bluetooth visibles, proceso indicado por un icono circular en movimiento a la derecha del texto "Dispositivos", y mostrará los mismos bajo la sección "Dispositivos" de la pantalla de configuración de Bluetooth:

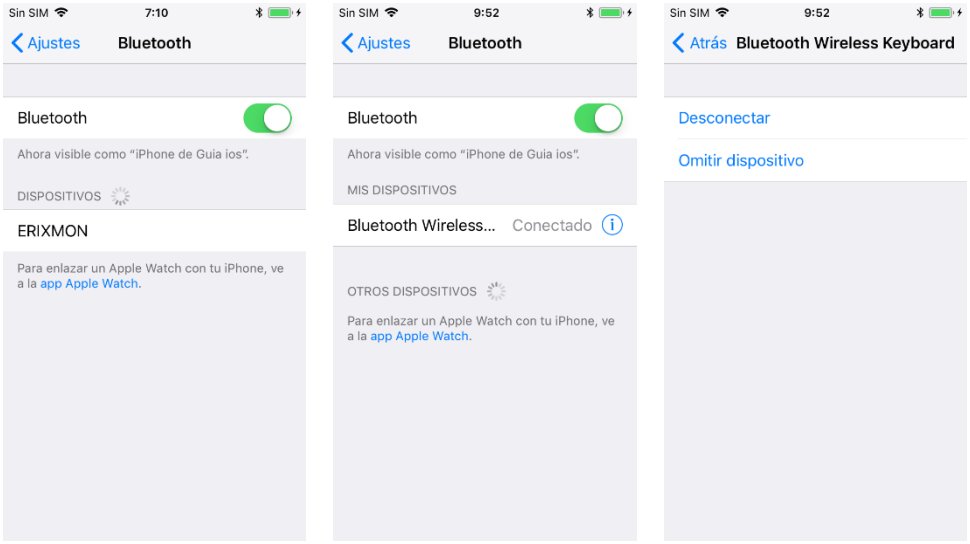


Figura 38 – Menú de configuración de Bluetooth.

iOS siempre muestra los dispositivos Bluetooth que han sido emparejados previamente con el dispositivo y su estado: "No conectado" o "Conectado" (ver <Figura 38>). Si en la zona de cobertura se descubren nuevos dispositivos Bluetooth visibles, estos serán añadidos a la lista de dispositivos, pero sin ningún indicador adicional. 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, lo cual sería muy útil a la hora de reconocer otros dispositivos vinculados al terminal y evitar ataques de suplantación, ni tampoco para modificar el nombre empleado para identificarlos en el dispositivo móvil y determinar si las conexiones deben ser autorizadas.

A diferencia de lo que ocurre en iOS 11, en iOS 12 el icono de estado de Bluetooth " " solo se mostrará en la barra de estado cuando exista una conexión activa [Ref.- 4]. Este comportamiento supone un inconveniente, ya que se pierde la posibilidad de comprobar el estado del interfaz de forma rápida. La razón que alega Apple para este cambio es que recomienda mantener el interfaz Bluetooth siempre activo para que el usuario pueda

beneficiarse en todo momento de servicios como los proporcionados a través de los denominados iBeacons[15].

Tras proceder a la activación del modo avión, iOS permite la activación independiente del interfaz Bluetooth. El interfaz Bluetooth también permanece activo cuando el dispositivo móvil está en espera (encendido, pero con la pantalla apagada) y/o bloqueado (suspendido). 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, y también al salir del modo avión.

Las principales recomendaciones de seguridad asociadas a las comunicaciones Bluetooth en dispositivos móviles iOS son:

- ***Desactivar 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.
- ***Desvincular los dispositivos Bluetooth de los que solo se haga un uso esporádico a través de la opción "Omitir dispositivo"*** que se obtiene al pinchar sobre la entrada correspondiente al mismo.
- ***Salir del menú de configuración de Bluetooth tan pronto se haya terminado de utilizar,*** ya que, mientras se permanezca en dicho menú (o en las pantallas de detalles de los dispositivos ya emparejados), el dispositivo móvil permanecerá en el estado visible (opción desaconsejada), no existiendo ninguna opción en iOS que permita que el dispositivo quede en estado oculto[16]. En caso de que el dispositivo iOS esté suspendido, pasará a modo oculto hasta que se desbloquee la pantalla y se acceda de nuevo a la configuración de Bluetooth.

La dirección del interfaz Bluetooth del dispositivo está disponible a través del menú "Ajustes – General – Información" (ver <Figura 1>). El nombre del dispositivo Bluetooth (mostrado bajo el interruptor de activación mediante el texto "Ahora visible como <*nombre*>" corresponde al nombre del dispositivo móvil iOS, y solo puede ser modificado cambiando el nombre del propio dispositivo. Este nombre es el que se verá desde otros equipos, como en el ejemplo de la <Figura 39>.

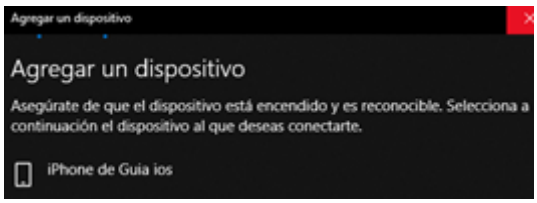


Figura 39 – Descubrimiento de un dispositivo iOS en un ordenador Windows.

iOS dispone del perfil de red de área personal (PAN, Personal Area Network) para establecer conexiones TCP/IP entre el dispositivo móvil y otros dispositivos a través de Bluetooth, y en concreto, para compartir su conexión de Internet móvil (2/3/4G) mediante lo que se denomina un "Personal Hotspot" (ver apartado "11.6. Personal Hotspot"). Este tipo de compartición está

[15] https://en.wikipedia.org/wiki/IBeacon

[16] 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 propio dispositivo móvil, siendo necesario que el otro dispositivo Bluetooth se encuentre en modo visible, o que conozca de antemano la dirección Bluetooth del dispositivo móvil iOS.

desaconsejada desde el punto de vista de seguridad frente a la utilización de un cable USB (si ésta es posible). Para conocer los perfiles Bluetooth soportados por iOS, consultar la [Ref.- 11].

11.3 WI-FI

Durante el proceso de configuración inicial del dispositivo móvil (que se inicia 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 (usando el proceso de configuración de una red Wi-Fi estándar de iOS), para completar el proceso de activación. Tras completar el proceso inicial de configuración, se recomienda deshabilitar el interfaz Wi-Fi del dispositivo móvil con el objetivo de aplicar las recomendaciones de seguridad descritas a lo largo de la presente guía antes de establecer conexiones de datos adicionales.

El interfaz inalámbrico Wi-Fi se controla en iOS a través del menú "Ajustes – Wi-Fi", mediante el interruptor "Wi-Fi":

Figura 40 – Menú de configuración de las conexiones Wi-Fi.

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 icono (el número de barras refleja la intensidad de la señal Wi-Fi), pero la no aparición de este icono en la barra no significa que el interfaz esté desactivado. Desde el Centro de control, sí es posible saber si el interfaz está activo, aunque no esté conectado a una red Wi-Fi (representado por el icono de Wi-Fi con un círculo azul).

Por otro lado, si se desactiva el interfaz Wi-Fi desde el Centro de control (representado por el icono de Wi-Fi con un círculo blanco; ver <Figura 41>), el dispositivo se desconectará de la red Wi-Fi actual y desactivará la funcionalidad "Nearby Wi-Fi", pero mantendrá el interfaz activo para algunas funcionalidades y con objeto de intentar una conexión a otra red en caso de detectar un cambio de ubicación, ser reiniciado o hasta el día siguiente a las 5:00 am (hora local)[17]. En la pantalla del Centro de control, se mostrará un mensaje informativo de desconexión de la red Wi-Fi cercana hasta mañana (como ventana de diálogo en el centro de la pantalla la primera vez que se usa este acceso y como mensaje en la parte superior en veces sucesivas, como ilustran las imágenes 3 y 4 de la <Figura 41>).

[17] https://support.apple.com/en-us/HT208086

Figura 41 – Interfaz Wi-Fi activo pero desconectado de la red Wi-Fi cercana.

iOS mantiene el estado del interfaz Wi-Fi tras reiniciar el dispositivo móvil y tras salir del modo avión, aun cuando el terminal esté bloqueado. Adicionalmente, aun con el modo avión activo, iOS permite la activación independiente del interfaz Wi-Fi.

La dirección MAC del interfaz Wi-Fi del dispositivo está disponible a través del menú "Ajustes – General – Información" (ver <Figura 1>).

La lista de redes en rango se muestra ordenada alfabéticamente, y se actualiza de forma automática. El símbolo de candado a la derecha del nombre de la red indica que se trata de una red protegida con contraseña (no se informa de los mecanismos de seguridad concretos empleados por cada una de las redes). Si no aparece el candado, la red es una red no protegida o abierta. La conexión a redes ocultas se puede realizar a través del menú "Otra…". 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), el mecanismo de seguridad a emplear (ninguna o redes abiertas, WEP, WPA/WPA2 Personal, WPA/WPA2 Empresa) y la contraseña (si la red la requiere). Para poder añadir una nueva red de forma manual, es preciso que ésta se encuentre en la zona de cobertura y poder establecer la conexión a través del botón "Acceder". Sin embargo, ***se desaconseja añadir redes Wi-Fi manualmente en iOS ya que estas serán consideradas como redes ocultas (aunque no lo sean) y desveladas por el dispositivo***.

Desde el punto de vista de seguridad, ***se recomienda conectarse únicamente a redes que emplean WPA2 (Personal o PSK, o Empresarial o Enterprise) como mecanismo de autentificación, y AES (CCMP) como mecanismo de cifrado. Se desaconseja el uso de redes WPA y de TKIP como mecanismo de cifrado.***

En caso de emplear WPA2 en su versión empresarial, la pantalla de ajustes de iOS no permite especificar los parámetros de configuración asociados al modo o tipo de mecanismo EAP a emplear, gestionándolo automáticamente:

Figura 42 – Configuración manual de una red Wi-Fi basada en WPA2 Empresa.

El modo automático de iOS referencia potencialmente diferentes tipos EAP (como por ejemplo PEAP, *Protected EAP*), y hace uso por defecto de usuario y contraseña para las credenciales del usuario (ver <Figura 42>). Por tanto, deben proporcionarse las credenciales del usuario (nombre de usuario y contraseña, y, opcionalmente, el dominio Windows "DOMINIO\usuario", en los campos "Nombre de usuario" y "Contraseña". Para poder fijar otros tipos EAP, así como opciones de configuración más avanzadas, es necesario hacer uso de los perfiles de configuración de iOS (fuera del alcance de la presente guía).

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, se debe transferir el fichero del certificado (.pfx ó .p12) al dispositivo móvil (ver apartado "16.2. Certificados cliente").

Se recomienda que la configuración de redes Wi-Fi WPA2 Empresa se lleve a cabo a través de un perfil de configuración, empleando por ejemplo la utilidad "Apple Configurator" (cuya descripción queda fuera del ámbito del presente informe pero que se puede consultar en la [Ref.- 22]), el cual 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. 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. 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. 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.

Desde el punto de vista de seguridad, ***se desaconseja la conexión a redes abiertas (no protegidas) y a redes ocultas*.** En caso de requerirse conexión puntual a este tipo de redes, se ***aconseja seleccionar "Omitir esta red" tan pronto se finalice su uso desde el menú* "Ajustes – Wi-Fi – [Nombre de la red]"** (ver <Figura 40>). El símbolo de dos elementos entrelazados representa una conexión de tipo "Hotspot" por Wi-Fi (ver apartado "11.6. Personal Hotspot").

Por defecto, iOS se conecta de forma automática a las redes conocidas. Para deshabilitar este comportamiento, se dispone de la opción "Ajustes – Wi-Fi – [Nombre de la red] Conexión

automática" (ver <Figura 40>), ***recomendándose su desactivación para disponer de control sobre cuándo se lleva a cabo la conexión***. La opción "Ajustes – Wi-Fi – Preguntar para acceder" implica que, en caso de que se requiera una conexión Wi-Fi y no se disponga de ella (por ejemplo, si una aplicación genera tráfico), se ofrecerá al usuario la posibilidad de conectarse a alguna de las redes Wi-Fi disponibles en la ubicación, incluidas las redes Wi-Fi abiertas. ***Se recomienda no habilitar esta opción***.

iOS dispone de la posibilidad de compartir la conexión de Internet móvil (2/3/4G) mediante Wi-Fi (ver apartado "11.6. Personal Hotspot"). En caso de hacer uso de esta funcionalidad, el dispositivo móvil utilizará la conexión Wi-Fi en exclusiva para el Hotspot, no pudiendo mantener además su propia conexión a una red Wi-Fi.

En resumen, desde el punto de vista de seguridad de iOS como cliente Wi-Fi, ***se recomienda hacer uso de redes inalámbricas no ocultas, basadas en WPA2 con cifrado AES (CCMP), y autentificación de tipo Personal, con una contraseña de acceso (PSK, Pre-Shared Key) suficientemente robusta (más de 20 caracteres), o de tipo Empresa, basada en mecanismos de autentificación 802.1X/EAP, y preferiblemente basada en EAP–TLS, con todos los ajustes de certificados y del servidor RADIUS minuciosamente configurados a través de un perfil de configuración***.

11.3.1 Compartición de contraseñas de redes Wi-Fi

El servicio de compartición de contraseñas de redes Wi-Fi (*Wi-Fi password sharing*) permite a un dispositivo iOS [1] enviar (de forma inalámbrica) la contraseña de acceso de la red Wi-Fi primaria a la que esté conectado a otro dispositivo iOS [2] sin revelar realmente las credenciales de la red[18].

El procedimiento requiere:

- Que el interfaz Bluetooth esté activo en ambos dispositivos.
- Que el dispositivo [1] esté desbloqueado.
- Que el número de teléfono asociado a [2] forme parte de sus contactos.

Cuando [2] entra en el menú de configuración de la red Wi-Fi y selecciona la red utilizada por [1], se mostrará en la pantalla de [1] una ventana de diálogo solicitando permiso para compartir la contraseña con [2]. Si se selecciona "Compartir contraseña", la contraseña de la red se enviará cifrada mediante AES 256[19] desde [1] a [2], y se almacenará en el *keychain* de [2] empleando un hash, por lo que la contraseña en claro no podrá conocerse por el usuario de [2].

La principal ventaja de este mecanismo es que evita tener que proporcionar a un tercero (aunque sea de confianza) las credenciales de acceso a una red Wi-Fi propia. Como principal inconveniente, sucede que, mientras [2] no olvide voluntariamente la red, tendrá la contraseña almacenada, y podrá a su vez aceptar peticiones de compartición de otros dispositivos que cumplan los requisitos expuestos.

Desde el punto de vista de seguridad, si se va a hacer uso de este mecanismo, ***la recomendación es renovar las contraseñas de la red Wi-Fi regularmente, de forma que los dispositivos con los que se hayan compartido no dispongan de ella permanentemente.***

[18] Este procedimiento no es de aplicación en redes Wi-Fi que emplean filtros por dirección MAC.
[19] El cifrado mediante AES 256 se introdujo en iOS 11. Hasta entonces, este procedimiento era inseguro.

Figura 43 - Compartición de contraseñas de redes Wi-Fi.

11.4 VOZ Y DATOS MÓVILES

El interfaz de telefonía móvil se habilita por defecto en iOS tan pronto se introduce una tarjeta SIM que proporciona dicho servicio, activándose adicionalmente el interfaz de datos móviles (si se incluyen en los servicios de la tarjeta SIM). En la barra superior de estado aparecerá el símbolo " " (el número de barras representa la intensidad de la señal), junto al nombre del operador de telefonía móvil y, opcionalmente, el tipo de conexión (GPRS, E, 3G, 4G, LTE). iOS determina cuál es la mejor conexión de datos disponible, sin interrogar al usuario, y proporciona la conectividad necesaria a las aplicaciones que ejecutan en el dispositivo móvil. En el Centro de control, se dispone del icono situado a la derecha del correspondiente al modo avión (ver <Figura 3>), que informa del estado del interfaz de datos móviles y permite su activación y desactivación.

iOS permite seleccionar el operador de telecomunicaciones de la lista ofrecida a través del menú "Ajustes – Operador" si se desmarca el modo "Automático":

Figura 44 – Ajustes de telefonía móvil.

La vinculación con un operador fijará en el dispositivo móvil una serie de ajustes, tanto para los servicios de telefonía de voz como de datos móviles.

11.4.1 Ajustes de privacidad del módulo de telefonía

Para proteger la privacidad del usuario, se dispone de ciertos ajustes en el menú "Ajustes – Teléfono", de aplicación principalmente a llamadas entrantes:

Desde el punto de vista de seguridad y privacidad, se recomienda la configuración:

- "Anunciar llamadas": ***Nunca***. Este ajuste controla si el aviso de llamada tradicional se sustituirá por la voz de Siri informando de quién realiza la llamada, lo que podría ser inadecuado en presencia de terceros.
- "Bloqueo e ID de llamadas": ***incluir los contactos no deseados***.
- "Llamadas en otros dispositivos": ***deshabilitar la opción "Permitir en otros dispositivos".*** Cuando se dispone de otros dispositivos Apple cercanos y conectados por Wi-Fi vinculados a la misma cuenta de iCloud que la asociada al dispositivo móvil (ver imagen derecha de la <Figura 44>), se ofrece la opción de utilizar la conexión de telefonía del iPhone para realizar y recibir llamadas, lo cual se puede además autorizar o denegar para cada dispositivo de forma individual. Desde el punto de vista de seguridad, ***se recomienda deshabilitar esta opción, para proteger la conexión de telefonía del dispositivo móvil en caso de compromiso de algún otro equipo que comparta la cuenta de iCloud o de la propia cuenta de iCloud***.
- "Responder con mensaje": permite configurar una serie de mensajes que se mostrarán en la pantalla de llamada, de forma que el usuario pueda elegir cuál enviar si no puede atender la llamada. Se considera útil disponer de esta opción.
- "Desvío de llamadas": permite redirigir la llamada a un número distinto cuando la opción está activa.
- "Mostrar ID de llamada": permite al usuario definir si se enviará la información de identificación de la llamada, disponiendo de la opción de ocultar siempre el número o mostrar el número para todas las llamadas.
- "PIN de la SIM": permite fijar el PIN de la tarjeta SIM. Se recomienda consultar el apartado "10. .Acceso físico al dispositivo móvil" para más información.

11.4.2 Ajustes de datos móviles

La configuración del interfaz de datos se controla en iOS a través del menú "Ajustes – Datos móviles". El interruptor "Datos móviles" activa y desactiva las capacidades de transmisión de datos a través de las redes de telefonía móvil, pero aún deshabilitado, sigue siendo posible emplear las capacidades de voz y SMS/MMS:

Figura 45 – Configuración de las conexiones de datos móviles.

Es importante saber que, si el dispositivo tiene conexión de datos a través de una red Wi-Fi, todo el tráfico se cursará a través de dicho interfaz. Así, los datos móviles solo se emplean si no se dispone de acceso a Internet vía Wi-Fi. El único caso en que ambas conexiones estarán activas simultáneamente es cuando el dispositivo móvil se configura para actuar como punto de acceso Wi-Fi y compartir su conexión de datos (ver apartado "11.6. Personal Hotspot"), y cuando está activa la opción "Asistencia para Wi-Fi" y la señal de la red Wi-Fi es débil (ver la <Figura 45>).

Desde el punto de vista de seguridad, se considera 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 abiertas, siempre que la conexión de datos de telefonía móvil emplee tecnologías 3G/4G frente a 2G. Para ello sería necesario deshabilitar el interfaz Wi-Fi y habilitar las comunicaciones de datos móviles. Para hacer uso de la tecnología 4G, se recomienda seleccionar "Activar 4G" del menú "Ajustes – Datos móviles – Opciones" y fijarlo al valor "Voz y datos". Se recomienda deshabilitar la opción "Itinerancia de datos" (o *roaming*), para bloquear el uso automático de las capacidades de datos de telefonía móvil cuando se viaja al extranjero y el terminal se encuentra en una red de otro operador al asociado por defecto a su tarjeta SIM[20], y habilitarlo expresamente solo en caso deseado.

[20] Muchas aplicaciones iOS generan tráfico de red sin necesidad de interacción directa con el usuario. Al viajar al extranjero, tener la opción de itinerancia de datos activa puede suponer un elevado gasto (en función del contrato de telefonía móvil de que se disponga).

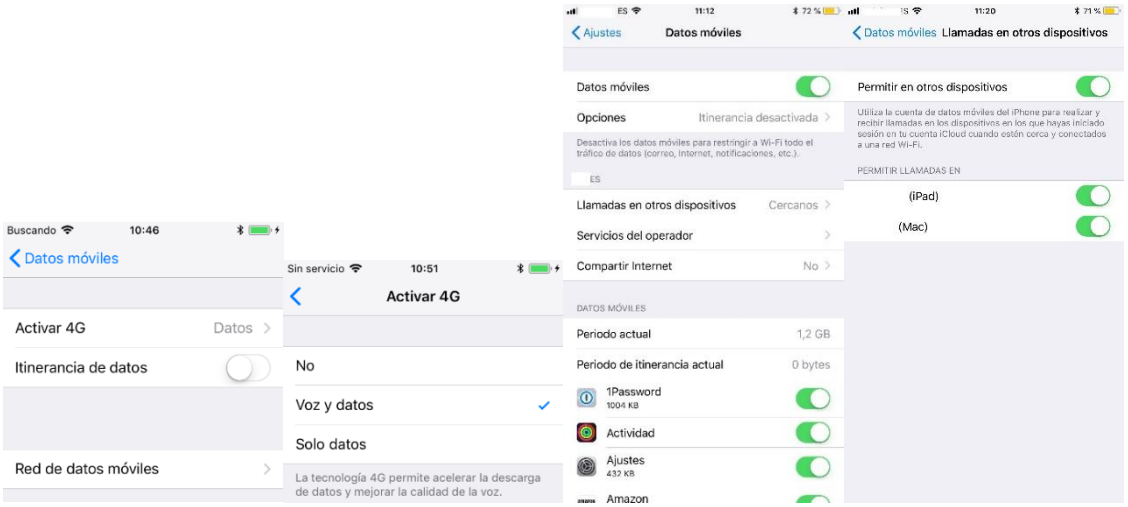


Figura 46 – Itinerancia de datos y 4G y compartición de telefonía con otros dispositivos.

iOS mantiene el estado del interfaz de telefonía de datos tras reiniciar el dispositivo móvil e introducir el PIN de la tarjeta SIM. El único modo de desactivar las capacidades de telefonía de voz y SMS/MMS es activar el modo avión.

La sección "Datos móviles" (ver <Figura 45>) permite establecer limitaciones para el uso de datos de las aplicaciones. ***Se recomienda deshabilitar el uso de datos móviles de todas aquellas apps para las que no se requiera*** (mediante el interruptor asociado a la app). Adicionalmente, desde el punto de vista de seguridad, ***se recomienda vigilar la cantidad de datos móviles empleada por las apps, a fin de detectar consumos inusuales que podrían desvelar que la app está cursando tráfico no deseado.*** La información sobre el consumo de datos asociado a los procesos del sistema operativo se muestra al final de la lista de apps, bajo "Servicios del sistema", no siendo posible deshabilitar los mismos, pero sí recomendándose vigilar este valor.

Adicionalmente, cuando se dispone de otros dispositivos Apple vinculados a la misma cuenta de iCloud que el dispositivo móvil, se mostrará la opción "Llamadas en otros dispositivos" (<Figura 46>), idéntico al ajuste descrito en el apartado "11.4.1. Ajustes de privacidad del módulo de telefonía", que se recomienda consultar para más detalles.

El botón "Restablecer estadísticas" permite restaurar las estadísticas de consumo de datos móviles recopiladas actualmente.

11.5 COMUNICACIONES PROPIETARIAS DE APPLE

11.5.1 iMessages

iMessages es el servicio propietario de Apple para el envío de mensajes instantáneos (a través de redes Wi-Fi o de datos de telefonía móvil), junto a imágenes, vídeos, contactos, localizaciones, etc. Para disponer del servicio iMessages, es necesario asociar una cuenta de iCloud al dispositivo móvil. Las capacidades de sincronización de iCloud hacen que los mensajes intercambiados a través de iMessages aparezcan de manera sincronizada en todos los dispositivos móviles iOS asociados al mismo ID de Apple o cuenta en iCloud. La configuración de iMessages se realiza desde el menú "Ajustes – General – Mensajes", y la

aplicación de acceso al servicio disponible por defecto en iOS se denomina "Mensajes", que también se emplea para el envío y recepción de mensajes de texto (SMS o MMS).

Figura 47 – Configuración de iMessages.

Desde el punto de vista de seguridad y/o privacidad, se recomienda la configuración:

- "Notificar lectura": ***desactivado***. De este modo no se enviará acuse de recibo de la lectura de los mensajes al emisor.
- "Enviar como SMS": ***activado***. Para asegurar las posibilidades de recepción del SMS por parte del destinatario, sin limitarlo al propio servicio de iMessage[21].
- "Enviar y recibir": determina las direcciones empleadas para enviar y recibir mensajes por parte del usuario del dispositivo móvil (ver imagen derecha de la <Figura 47>). La activación del servicio iMessages se asocia tanto a la dirección de e-mail vinculada al ID de Apple como al número de teléfono móvil del dispositivo móvil[22]. Este último es un identificador obligatorio que no puede ser desvinculado del servicio para la recepción de mensajes en el caso de los dispositivos iPhone (por lo que aparece sombreado en color gris). Se recomienda ***eliminar*** aquellas direcciones que no se desea publicar para este servicio.
- "Contactos bloqueados": corresponden a la misma lista que la descrita en la sección "11.4.1. Ajustes de privacidad del módulo de telefonía".
- "[Mensajes de audio] Levantar para escuchar": ***desactivado***. Para impedir que un mensaje pueda ser escuchado indebidamente por un tercero.
- "Filtrar desconocidos": al activar este ajuste, los mensajes de números que no aparezcan en la lista de contactos se agruparán en la categoría "Remitentes desconocidos", y no se emitirá ninguna notificación cuando se reciban. Esta característica puede resultar útil para evitar "spam".

[21] Esta recomendación se hace bajo el punto de vista de seguridad, pero el usuario debe evaluar previamente su tarifa de telefonía móvil.

[22] En el caso de dispositivos móviles iPad, que carecen de capacidades de telefonía móvil de voz y SMS/MMS, es necesario asociar el servicio de iMessage a la dirección de e-mail asociada al ID de Apple.

El servicio iMessage emplea cifrado extremo a extremo entre los dispositivos Apple involucrados en una comunicación, y utiliza dos pares de claves privadas y públicas, una para cifrado y otra para firma. Las claves privadas se almacenan en el dispositivo móvil, mientras que las públicas se envían al iDS de Apple (*iMessage Directory Service*). Los dispositivos iOS, en caso de ser extraviados o robados, son vulnerables a que el nuevo usuario 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 (ID de Apple) y el dispositivo móvil. Dado que 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, un nuevo usuario podría suplantar al usuario previo enviando y recibiendo mensajes en su nombre.

Los mensajes se clasifican en base al otro interlocutor en lo que se denominan "conversaciones", de modo que todos los mensajes intercambiados con un mismo número de teléfono de un mismo contacto (o de un número que no pertenezca a la lista de contactos) se muestran agrupados. Durante el uso de la app Mensajes, si se borra una conversación determinada deslizando el dedo de izquierda a derecha mientras se pulsa la conversación, se presentará una ventana de diálogo interrogando al usuario si desea que Apple marque dicha conversación como "No deseada", pero esto no implicará que se bloquee el contacto.

Adicionalmente, el servicio iMessage soporta el "Reenvío de SMS", que permite que los mensajes de texto (SMS) recibidos en el número de teléfono asociado al dispositivo móvil se reciban también en aquellos dispositivos vinculados al mismo ID de Apple. Si se habilita esta funcionalidad de reenvío de SMS con un ordenador macOS Mojave, la función de autorrellenar códigos de un solo uso se activará en el navegador Safari de dicho ordenador tan pronto se reciba el mensaje en él (ver apartado "9.3.1. Autorrellenar contraseñas y códigos de seguridad en iOS 12").

11.5.2 FaceTime

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.

iOS 12 extiende los controles de privacidad y mecanismos de cifrado existentes a las llamadas de grupo de FaceTime.

11.5.3 Siri

Nota: El alcance de la presente guía no contempla la realización de un análisis de seguridad detallado de Siri y sus protocolos de comunicaciones.

Siri es el sistema de reconocimiento de voz y lenguaje natural introducido por Apple en iOS 5.x, que permite al usuario realizar multitud de tareas mediante comandos de voz, por ejemplo, enviar mensajes SMS, realizar llamadas de voz, crear citas en el calendario, buscar información, etc., convirtiéndose en un asistente personal digital.

Siri se invoca tras mantener pulsado el botón "Home" del iPhone, o el botón de llamada en dispositivos manos libres Bluetooth. Sus ajustes se encuentran bajo "Ajustes – Siri y Buscar", y

se puede consultar más información sobre las recomendaciones de seguridad y privacidad relacionadas en el apartado "7.3. Búsqueda mediante texto y voz".

Siri hace 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 en base a la localización actual del usuario, enviando los datos a Apple para procesar la solicitud.

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 por lo que, teóricamente, sería posible eliminar toda la información que Siri hubiera almacenado previamente sobre el usuario desactivando el servicio.

La activación de Siri tiene relación con las capacidades de dictado de iOS en las aplicaciones que permiten hacer uso del teclado, a través del icono del micrófono existente en el mismo.

Por ejemplo, si el servicio de localización está activo durante una búsqueda y no se ha desactivado la búsqueda de Siri, el dispositivo enviará a Apple la ubicación. Este comportamiento puede desactivarse tanto para Siri como para la función de dictado a través de "Ajustes – Privacidad – Localización – Siri y Dictado: Nunca" (ver apartado "14. Servicios de localización").

Es posible bloquear las búsquedas web a través de Siri estableciendo una restricción en el menú "Ajustes – Tiempo de uso – [Restricciones de contenido] – [Siri] Contenido de búsquedas web" (consultar el apartado "17.1. Restricciones" para más información sobre el establecimiento de restricciones en el dispositivo móvil).

Además de las precauciones relativas a la privacidad que pueden alegarse al enviar a Apple toda la información del usuario vinculada a Siri, Siri no está exento de vulnerabilidades, como las encontradas por el investigador español José Rodríguez en iOS 12.0 [Ref.- 25]. Por ello, ***desde el punto de vista de seguridad y privacidad, se desaconseja el uso de Siri, o, cuando menos, deshabilitar su uso en la pantalla de bloqueo***. Es posible desactivar Siri en la pantalla de bloqueo mediante el menú "Ajustes – Touch ID y código – Permitir acceso al estar bloqueado: Siri".

11.5.4 AirDrop

AirDrop es un servicio para compartir contenido entre dispositivos Apple, que utiliza Bluetooth Low Energy (BLE) para descubrir dispositivos que soporten el servicio y una conexión Wi-Fi extremo a extremo para la transmisión de datos entre los dispositivos implicados en la comunicación[23].

Las capacidades de comunicación de AirDrop se pueden activar y desactivar desde el Centro de control realizando una pulsación larga sobre cualquiera de los iconos asociados a comunicaciones y seleccionando el icono "AirDrop" (ver imagen derecha de la <Figura 3>). Por defecto, se encuentra habilitado solo para los contactos.

Para iniciar una comunicación mediante AirDrop, tanto el dispositivo emisor como el receptor requieren tener activos los interfaces de Bluetooth y Wi-Fi, y tener la pantalla desbloqueada. Desde el contenido a compartir, el emisor debe pulsar el icono y seleccionar el dispositivo

[23] https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf - AirDrop security.

receptor bajo la opción "Pulsa para compartir con AirDrop"[24] (ver imagen central de la <Figura 48>). Esta acción hará que el dispositivo receptor solicite confirmación en la pantalla (ver imagen derecha de la <Figura 48>), a la vez que emite una vibración y una señal sonora.

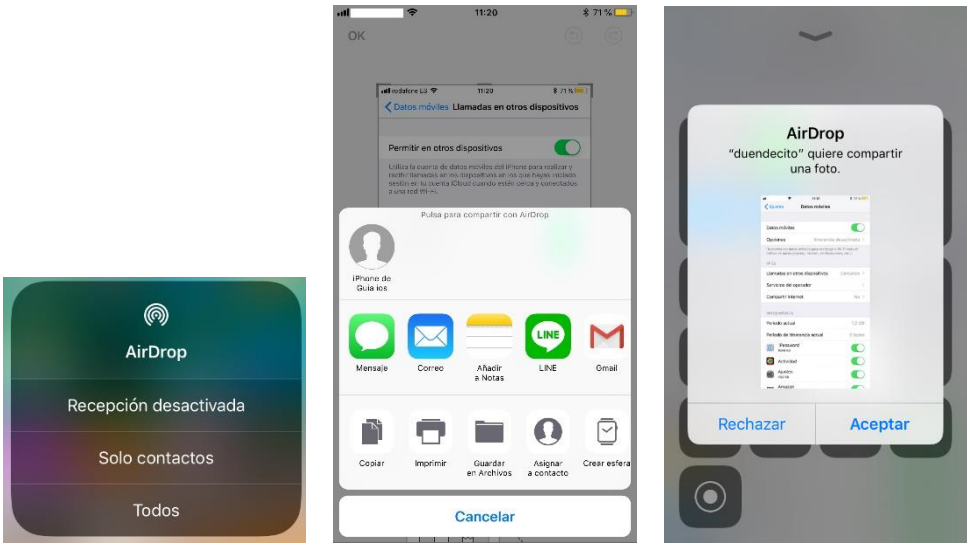


Figura 48 – Compartición de contenidos vía AirDrop.

Desde el punto de vista de seguridad, ***se recomienda mantener deshabilitado el servicio AirDrop, para lo cual se debe fijar el parámetro "recepción desactivada" en el Centro de control, y, en caso de requerirse utilizar las capacidades de transmisión de datos de AirDrop, habilitarlo solo para los contactos y solo mientras se lleve a cabo el intercambio de datos***.

El servicio AirDrop emplea un identificador que se almacena en el dispositivo, y cifra los contenidos en base a un certificado ligado a la identidad de las cuentas de iCloud involucradas, por lo que se puede considerar más seguro de cara a la transferencia de información que otros mecanismos, como el correo electrónico. Pese a ello, adolece de los riesgos de seguridad asociados a la necesidad de mantener los interfaces Bluetooth y Wi-Fi activos para su operativa.

11.6 PERSONAL HOTSPOT

iOS permite compartir su conexión de Internet de datos móviles con otros dispositivos (*tethering*) mediante lo que Apple denomina "Personal Hotspot". La compartición de datos puede llevarse a cabo a través del interfaz Bluetooth, Wi-Fi, y mediante un cable USB. Para ello, desde la pantalla principal de "Ajustes", se debe activar la opción "Compartir Internet":

[24] El dispositivo emisor realizará la búsqueda de dispositivos cercanos y presentará los que estén en rango y tengan la recepción habilitada.

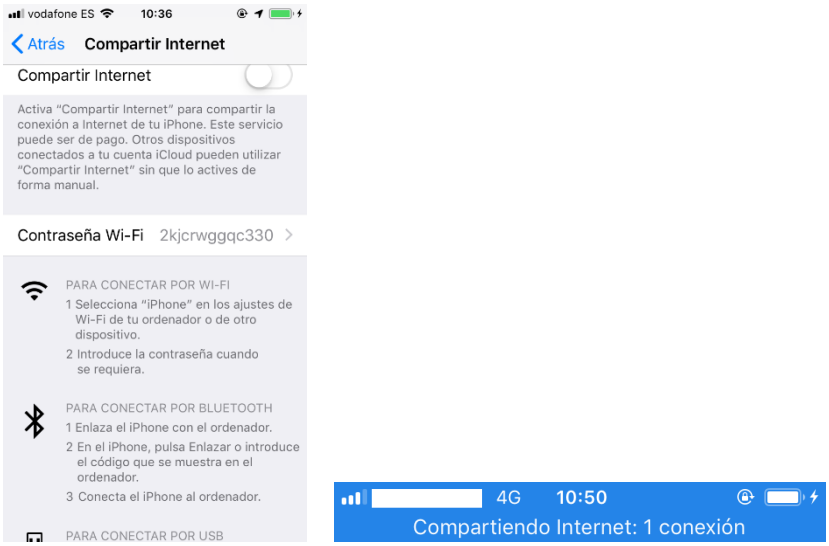


Figura 49 – Opción "Compartir Internet" (Personal Hotspot).

La barra superior de estado mostrará el número de conexiones activas en el *hotspot*, por lo que, desde el punto de vista de seguridad, es importante prestar atención a dicho número para detectar el establecimiento de conexiones no deseadas.

El icono representa que existe una conexión compartida.

Para el establecimiento del *hotspot* a través de Wi-Fi (el dispositivo móvil actúa como punto de acceso Wi-Fi para otros equipos), iOS requiere una contraseña, que debe introducirse en el equipo cliente que va a hacer uso de la compartición de datos del dispositivo móvil. Por defecto, se proporciona una contraseña de 13 caracteres alfanuméricos. Desde el punto de vista de seguridad, ***se recomienda seleccionar una contraseña propia y personalizada de más de 20 caracteres y no confiar en la generada automáticamente por el dispositivo móvil***.

Desde el punto de vista de seguridad, ***se recomienda deshabilitar el Personal Hotspot tan pronto finalice la necesidad de compartir la conexión de Internet con otros dispositivos, y habilitarla solo cuando sea preciso. No obstante, se considera más segura la compartición de la conexión con otro dispositivo propio que el uso de redes Wi-Fi de uso público.***

11.7 VPN

iOS proporciona soporte para las tecnologías VPN: *Cisco IP Security* (IPSec), IKEv2, 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. Adicionalmente, iOS permite la conexión a redes VPN SSL empresariales a través de aplicaciones cliente propietarias.

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.

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 pre-configuradas. 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. Esta funcionalidad puede ser empleada no sólo por aplicaciones de sistema existentes por defecto en iOS (como Mail o Mobile Safari), sino también por aplicaciones de terceros.

El proceso para añadir certificados digitales raíz específicos para su utilización en conexiones Wi-Fi o VPN se detalla en el apartado "16. Certificados digitales".

La configuración de redes VPN en iOS puede realizarse a través de perfiles de configuración (cuya descripción excede el ámbito de la presente guía) o de forma manual. Para ello, se accederá a "Ajustes – General – VPN – Añadir configuración VPN":

Figura 50 – Menú de configuración de VPN.

En el caso de redes L2TP/IPSec (reflejadas como "L2TP"), iOS obliga a configurar el secreto L2TP (o clave pre-compartida para el acceso a la red), opción que permite autentificar el propio túnel L2TP mediante un secreto compartido entre el cliente y el servidor (ver imagen derecha de la <Figura 50>). Como se puede ver en dicha imagen, la configuración para L2TP/IPSec permite especificar si se hará uso de autentificación mediante contraseña o a través de dos factores, (opción 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), y recomendada desde el punto de vista de seguridad.

Una vez establecida la conexión con la red VPN, el usuario (junto al servidor de VPN) es quien puede restringir las comunicaciones, de forma 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).

En el caso de redes Cisco IPsec, iOS permite establecer el secreto o clave pre-compartida para el acceso a la red, el nombre de grupo IPSec, y si se hará uso de un certificado digital para la autentificación del dispositivo móvil. En caso de emplear un certificado digital (ver imagen superior), 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 "16. Certificados digitales"), tanto los importados previamente por el usuario a través de los perfiles de configuración como los que iOS proporciona por defecto. El certificado digital necesario para Cisco IPSec es de tipo personal, y permitirá autentificar al dispositivo móvil y a su usuario. Adicionalmente es necesario instalar un certificado raíz

(perteneciente a la CA), asociado a la generación del certificado digital empleado por el servidor o concentrador de VPN.

Una vez configurada, el uso de una red VPN puede activarse desde "Ajustes – VPN". iOS reflejará la duración de la conexión actual e informará sobre el direccionamiento IP, y mostrará el icono "VPN" en la barra superior de estado.

Las contraseñas de las redes VPN pueden quedar almacenadas por defecto en los ajustes de configuración de red, no siendo necesario por parte del usuario introducir las credenciales de acceso a la VPN (nombre de usuario y contraseña) para establecer la conexión con la red VPN seleccionada. Desde el punto de vista de seguridad, no se recomienda permitir este comportamiento. Para ello, la única opción que proporciona iOS a través del interfaz de usuario pasa por dejar en blanco el campo "Contraseña" en la configuración de la red VPN, con lo que el campo quedará marcado como "Preguntar cada vez" (en color gris), frente a otros campos que son obligatorios (indicado por el texto "Obligatorio").

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 solo uso asociado.

Los dispositivos móviles iOS no disponen de un mecanismo por defecto (sí a nivel empresarial) para limitar la conectividad únicamente a través de redes VPN, 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.

12. COMUNICACIONES TCP/IP

iOS dispone de soporte de TCP multiruta, que permite realizar conexiones a través de varias interfaces como LTE (4G), Wi-Fi y Bluetooth simultáneamente. En la práctica, esta funcionalidad implica que las transmisiones de datos no se interrumpen si, habiéndose iniciado sobre una conexión Wi-Fi y se sale de su alcance, se obtiene conexión a través de la red 2/3/4G.

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: por ejemplo, "Ajustes – Wi-Fi" (apartado "11.3. Wi-Fi") o "Ajustes – Datos móviles" (apartado "11.4. Voz y Datos móviles").

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, pulsando en el icono ⓘ situado a la derecha de la entrada correspondiente a la red Wi-Fi en cuestión del menú "Ajustes – Wi-Fi".

La configuración de direccionamiento IP del interfaz Wi-Fi es independiente para cada una de las redes Wi-Fi configuradas.

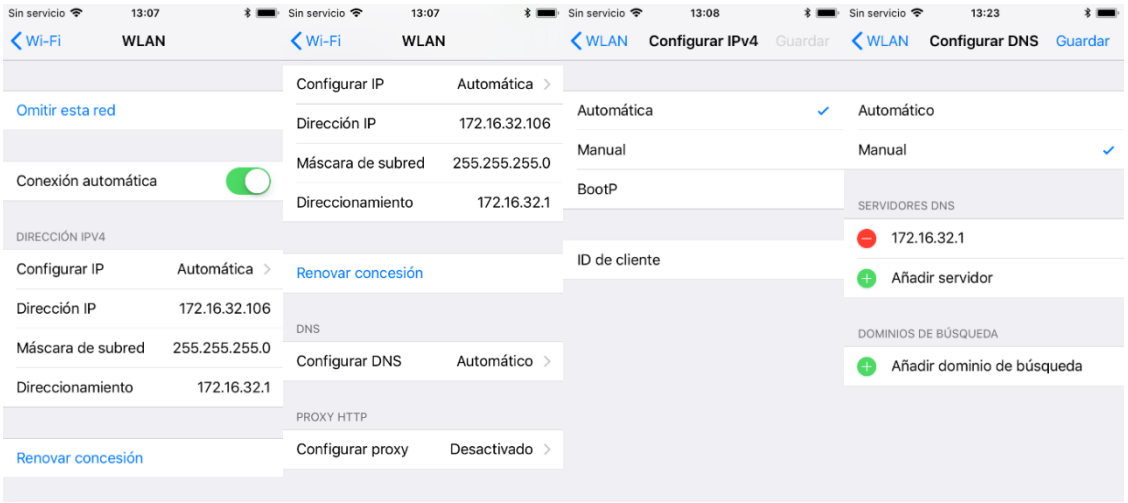


Figura 51 – Configuración de los parámetros TCP/IP del interfaz Wi-Fi.

En el caso del interfaz móvil 2/3/4G, iOS no dispone de opciones de configuración avanzadas, y tampoco 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. Desde iOS 11 esta información no es mostrada tampoco a través del denominado "modo de prueba" (*Field Test*), disponible en iOS al marcar el código *3001#12345#*, y pulsar la tecla de llamada:

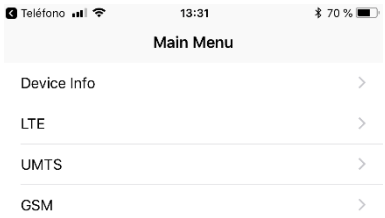


Figura 52 – Información del interfaz de telefonía y datos móviles a través del "Field Test".

El "Field Test" proporciona numerosos detalles relacionados con las redes de telefonía móvil y el interfaz de radio del dispositivo móvil, como la intensidad de diferentes parámetros de la señal y frecuencias empleadas, y la celda de servicio actual y las celdas vecinas, para LTE, UMTS y GSM.

13. COMUNICACIONES USB

La conexión USB del dispositivo a un ordenador proporciona cuatro funcionalidades:

- Suministro de corriente para cargar el dispositivo móvil: recientemente se ha extendido el uso de cargadores USB en lugares públicos, como cafeterías o aeropuertos. Desde el punto de vista de seguridad, en caso de requerirse conectar el dispositivo móvil a uno de estos cargadores, ***se recomienda hacer uso de un adaptador USB especial que bloquee la transferencia de datos.***
- Acceso limitado al almacenamiento interno, que permite la descarga de imágenes y vídeos, así como un servicio de compartición de ficheros disponible a través de iTunes que permite escribir contenido que consumirán las apps que ofrecen "*File sharing*" (por ejemplo, un certificado digital o una configuración concreta), y descargar al ordenador los contenidos

que la app permita. Para que esta conexión se produzca, es necesario establecer una relación de confianza entre el ordenador y el dispositivo móvil, que se establece al aceptar el mensaje "¿Confiar en este ordenador?" que se mostrará en la pantalla del dispositivo móvil.

- Conexión a la aplicación iTunes instalada en un ordenador, a través de la cual se pueden realizar múltiples operaciones de gestión del dispositivo móvil, como actualizaciones de iOS, sincronización automática y transferencia puntual de contenidos, y operaciones de backup y restauración. Para que esta conexión se produzca, es también necesario establecer la relación de confianza entre el ordenador y el dispositivo móvil.
- Compartición de la conexión de datos de telefonía móvil (2/3/4G), *tethering* (no así la de Wi-Fi), del dispositivo móvil con el ordenador.

La relación de confianza se establecerá solo mientras dure la conexión USB puntual, no siendo posible definir autorizaciones permanentes (a diferencia de lo que sucede en otras plataformas como Android).

Respecto a la compartición de la conexión de datos a través de USB, se recomienda hacer uso de la misma frente a la que emplea Bluetooth o Wi-Fi (ver apartado "11.6. Personal Hotspot").

Con la versión 11.4.1 de iOS, Apple introdujo el denominado "modo restringido USB" (*USB Restricted Mode*), una medida de seguridad que impide que los accesorios USB que se conectan al puerto USB (*Lighting*) del dispositivo móvil establezcan conexiones de datos con él si lleva bloqueado más de una hora. Esta medida surge de la disponibilidad en el mercado de ciertos productos que pueden obtener el código de acceso por este medio (consultar el apartado "18. Cifrado del dispositivo móvil" para más información).

14. SERVICIOS DE LOCALIZACIÓN

El servicio de localización de iOS permite a las apps y otros servicios conocer la ubicación del dispositivo móvil, no solo a través del módulo GPS sino también a través de las redes Wi-Fi y las torres de telefonía móvil cercanas.

Para deshabilitar por completo el servicio de localización, se puede desactivar el interruptor "Ajustes – Privacidad – Localización". El inconveniente de este ajuste es que el servicio "Buscar mi iPhone" (ver apartado "9.1.1. Buscar mi iPhone") dejaría de estar disponible para el dispositivo móvil.

Para que una app pueda hacer uso de la ubicación, debe disponer del permiso "Localización", el cual debe ser concedido explícitamente por el usuario. Se recomienda habilitar el ajuste "Ajustes – Privacidad – Localización – Servicios del sistema – Icono de barra de estado" para que, cuando una app esté haciendo uso del servicio de localización, la barra superior de estado del dispositivo informe de ello poniéndose en color azul y mostrando un mensaje:

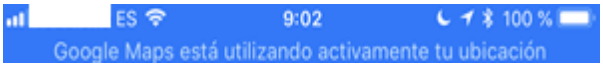


Figura 53 – Barra de estado mostrando uso del servicio de ubicación de una app.

Además de las apps de navegación (como "Mapas"), muchas otras aplicaciones y servicios hacen uso de la localización, entre ellas App Store, Cámara, Safari, Twitter, Brújula, Tiempo o "Buscar mi iPhone". Adicionalmente, durante su uso, Siri enviará la localización del dispositivo a Apple. Para ver qué apps tienen concedido el permiso de localización, se debe acceder a

"Ajustes – Privacidad – Localización". Los valores que puede tomar este ajuste para una app se muestran en la segunda imagen de la <Figura 54>:

Figura 54 – Ajustes de localización.

La sección "Servicios del sistema" (tercera y cuarta imagen de la <Figura 54>) proporciona información sobre qué servicios de iOS pueden acceder a la ubicación y qué uso efectivo han hecho de ella.

iOS proporciona el servicio "Compartir mi ubicación" (primera imagen de la <Figura 54>), a través del cual se permite compartir la ubicación del dispositivo a través de la app "Mensajes" y del servicio "Buscar a mis amigos" (el cual queda fuera del ámbito de la presente guía, pero del cual se puede obtener información en la [Ref.- 12]). Este servicio puede resultar interesante como medida de control parental sobre dispositivos de menores, especialmente para los miembros de una familia en iCloud. Desde el punto de vista del usuario adulto, la activación del ajuste debería ser solo puntual, y eliminarse tan pronto finalice la necesidad de usarlo. Ambas acciones requieren que el dispositivo móvil disponga de conexión a Internet.

iOS permite añadir información de la localización geográfica a las fotografías realizadas con la cámara del dispositivo móvil si la app "Cámara" tiene concedido el permiso de localización, información conocida como geoetiquetas (o *geotags*). En caso afirmativo, al realizar la fotografía, se añaden a la cabecera EXIF de la imagen las coordenadas GPS.

Desde el punto de vista de privacidad, ***se recomienda deshabilitar:***

- ***Aspectos relativos a los anuncios de la sección*** "Servicios del sistema" ***y a la subsección*** "Mejora del producto".
- ***El envío de información de ubicación a Apple durante el uso de Siri.***
- ***El permiso de localización para las apps que proporcionan servicios de redes sociales.***
- ***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.***

De forma general, ***se recomienda conceder el permiso de localización solo a las apps que proporcionan servicios de ubicación, mediante la opción "***Cuando se use la app***".***

Si se desea que el usuario vuelva a ser preguntado acerca de los permisos de localización de todas las apps, en lugar de tener que revisarlo individualmente, se puede proceder a restablecer los valores que iOS ofrece por defecto a través de la opción "Ajustes – General – Restablecer – Restablecer localización y privacidad" (ver <Figura 72>).

15. NAVEGADOR WEB MOBILE SAFARI

Mobile Safari (en adelante, Safari) es el navegador web incluido por defecto en iOS, cuyos ajustes se acceden a través de "Ajustes – Safari":

Figura 55 – Ajustes del navegador web Mobile Safari.

Desde el punto de vista de seguridad, se recomienda:

- ***Activar "Bloquear ventanas"***: para evitar las ventanas emergentes (*pop–ups*) que los sitios web pueden tratar de abrir sin que el usuario lo solicite expresamente.
- ***Activar "Impedir a los sitios rastrearme" y "Sin seguimiento entre los sitios"***: para evitar que los sitios web realicen seguimiento de las actividades de navegación y búsquedas con objetivos de publicidad.
- ***Activar "Aviso de sitio web fraudulento".***
- ***Desactivar "Acceso a cámara y micrófono".***
- ***Desactivar "Comprobar Apple Pay".***
- ***Autorrelleno:*** esta sección permite 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. Por ejemplo, cuando se accede a una página web y la función de autorrelleno de contraseñas se encuentra habilitada, Safari mostrará en la barra "QuickType" situada sobre el teclado el menú "Contraseñas" que, al pulsarse, solicitará la introducción del método de bloqueo activo en el dispositivo y presentará la lista de credenciales guardadas para que el usuario seleccione la que corresponda al sitio web (ver <Figura 56>). S*e* ***recomienda deshabilitar todas las opciones de autorrelleno de Safari,*** aun sacrificando la usabilidad.

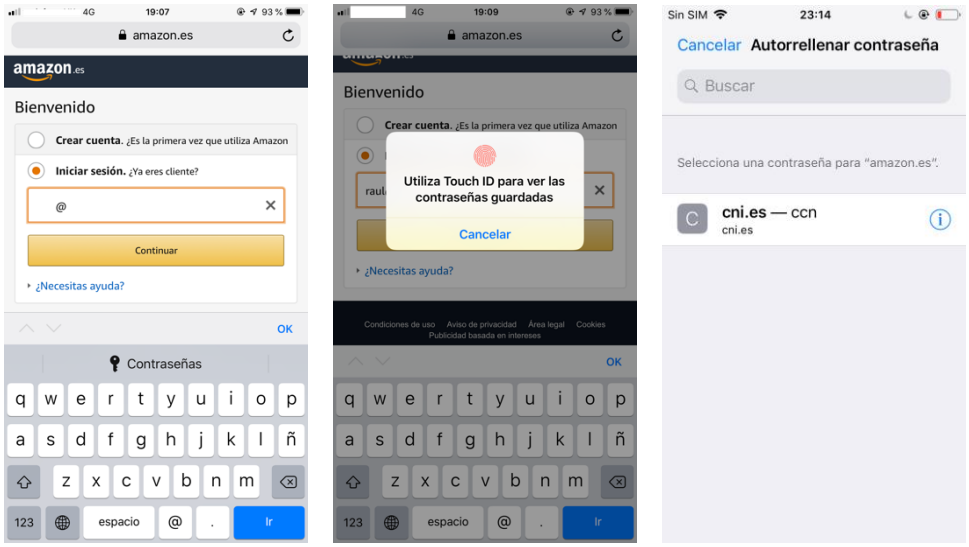


Figura 56 - Autorrelleno de contraseñas en Safari.

Cuando Safari hace uso del llavero (o *keychain*), mostrará en la barra un símbolo de llave y, al acceder a un sitio web cuyas credenciales no ha almacenado previamente, solicitará confirmación al usuario para proceder a añadirlas al llavero:

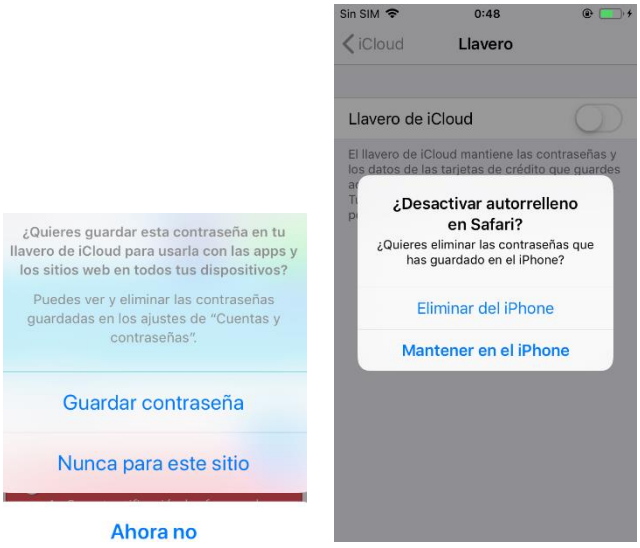


Figura 57 – Uso del llavero (o keychain) de iCloud.

- ***Avanzado – JavaScript***: dependerá de las preferencias del usuario.

Los ajustes permiten además "Borrar historial y datos de sitios web", tanto global (aplicará a los datos de navegación y cookies de todos los sitios web) como individualmente, a través de "Avanzado – Datos de sitios web – Editar". ***Se recomienda limpiar el historial periódicamente para proteger la privacidad del usuario***.

Se recomienda hacer uso de las capacidades de navegación privada (*Private Browsing*) de Mobile Safari, que evitan que se almacene en el dispositivo el histórico de navegación o las cookies, o que se sincronicen otros datos de navegación con otros dispositivos, para salvaguardar la privacidad del usuario. Para ello se dispone de la opción "Nav. privada" existente en la esquina inferior izquierda al abrir una nueva pestaña vacía.

16. CERTIFICADOS DIGITALES

iOS dispone de un 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, donde se almacenan los certificados digitales, contraseñas y otras credenciales, por ejemplo, las asociadas a redes VPN y redes Wi-Fi. Éste constituye un complemento a la solución de cifrado del dispositivo, que iOS proporciona a través de otros mecanismos específicos (ver apartado "18. Cifrado del dispositivo móvil").

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". 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 podrá ser copiado y protegido con contraseña. Desde iOS 4.0, el *keychain* puede ser restaurado desde una copia de seguridad en el mismo dispositivo móvil desde el que se copió o en otro dispositivo (salvo que la app establezca restricciones explícitas para no permitirlo).

El *keychain* y su gestión no está directamente accesible para el usuario a través del interfaz gráfico de iOS, pero se permite importar certificados digitales X.509 en formato PKCS#12 que contengan sólo una identidad, tanto ficheros con extensión .p12 y .pfx, como .cer, .crt y .der.

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

16.1 CERTIFICADOS RAÍZ

Los certificados de autoridades certificadoras, conocidas como CAs (*Certificate Authorities*), necesarios para establecer cadenas de confianza, pueden ser instalados automáticamente, opción recomendada desde el punto de vista de seguridad, mediante el uso de perfiles MDM (*Mobile Device Management*) o a través de Apple Configurator, o manualmente (transfiriéndolos al dispositivo móvil a través de un ordenador e iTunes, a través de un fichero adjunto a un correo electrónico, o descargándolos directamente desde una página web mediante Safari). En caso de emplear un servidor web interno a la organización, éste debe hacer uso de mecanismos de autentificación 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 la descarga a través del navegador web Safari.

Al seleccionar el certificado digital, iOS mostrará al usuario una ventana de diálogo informando de la intención del sitio web de instalar un perfil de configuración; si el usuario acepta mediante el botón "Permitir" se mostrará información sobre el certificado, que se puede ampliar mediante "Más detalles". Si se pulsa en "Instalar", iOS solicitará confirmación del código de acceso del dispositivo móvil, y, tras pulsar de nuevo en "Instalar", se mostrará la confirmación del perfil instalado. Este proceso se ilustra en la <Figura 58>.

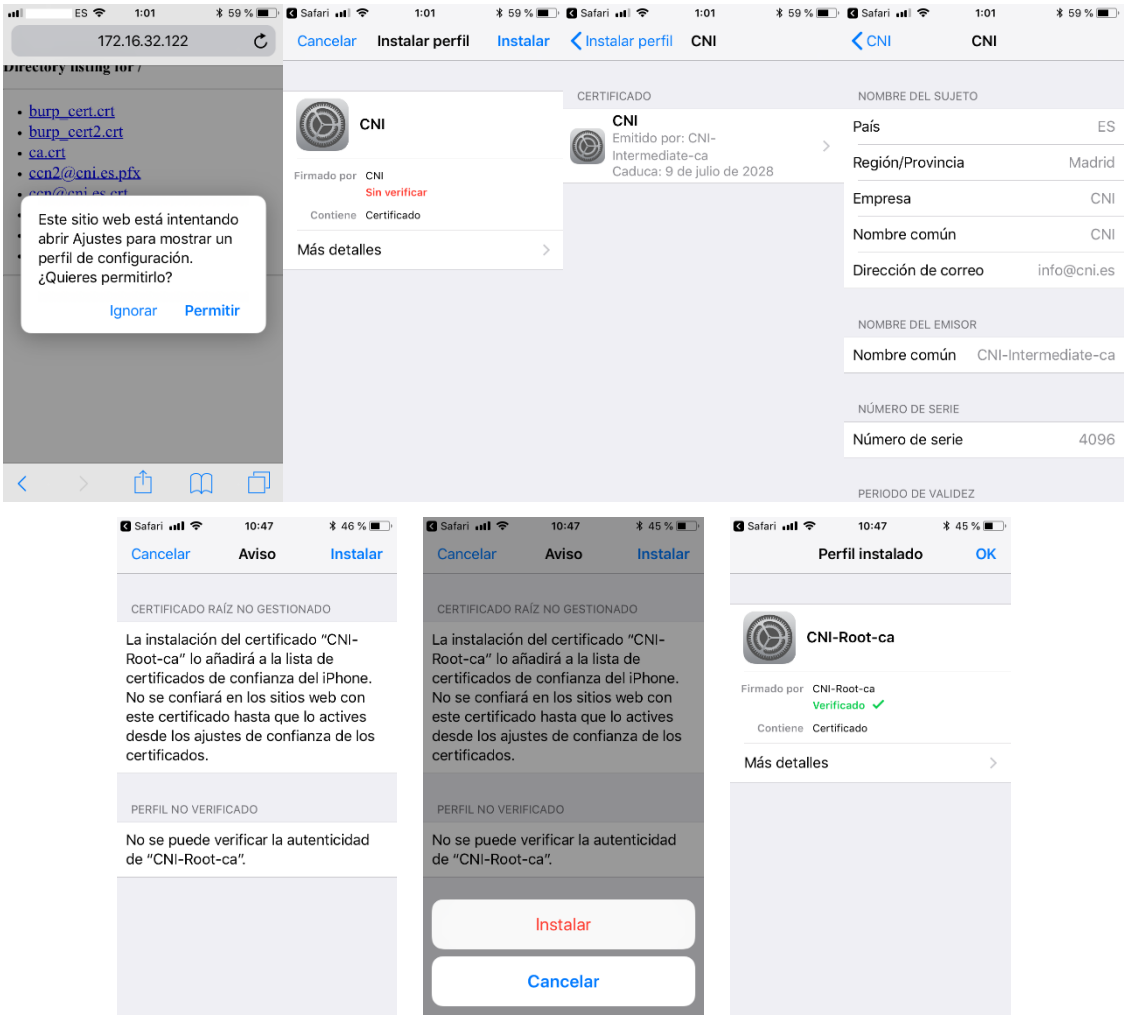


Figura 58 – Proceso de instalación de un certificado (perfil de configuración) a través de Safari.

A partir de iOS 10.3 en adelante, la instalación manual de un certificado (como parte de un perfil) no implica que se confíe en él para las comunicaciones que usan TLS, sino que se requiere que el usuario del dispositivo móvil active la confianza en él a través del interruptor "Ajustes – Información – Ajustes de confianza de los certificados – [Confiar en los certificados raíz] [entrada del certificado]":

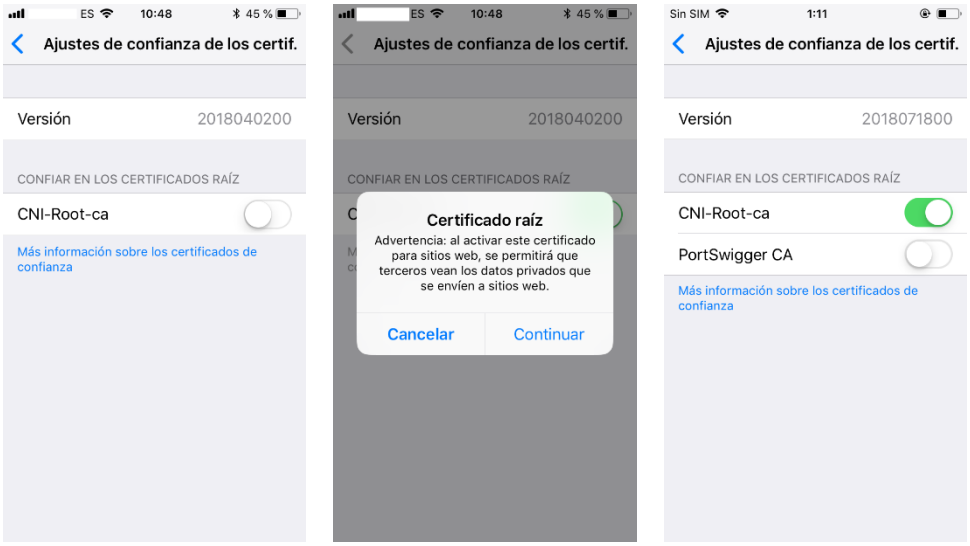


Figura 59 – Activación de la confianza en un certificado.

Las implicaciones del uso de certificados digitales en funciones de seguridad críticas requieren que el usuario 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.

Respecto al conjunto de certificados digitales raíz preinstalados por defecto en el dispositivo móvil, conocido como "almacén de confianza" (*Trust Store*), iOS no proporciona ningún menú o interfaz gráfico del dispositivo móvil que permita consultarlos, ni tampoco se dispone de ninguna opción en el interfaz de usuario que permita modificar la lista de autoridades certificadoras raíz proporcionada por defecto. Sí es posible acceder a los certificados digitales raíz instalados por el usuario a través del menú "Ajustes – General – Perfiles", desde donde pueden eliminarse de forma individual.

Los certificados de confianza se clasifican según tres políticas de confianza:

- De confianza (*trusted*): corresponden a los certificados de confianza de autoridades certificadoras (CAs) raíz o intermedias.
- Preguntar siempre (*always ask*): corresponden a certificados que no son de confianza, por lo cual, al ser utilizados, se interrogará al usuario para que decida si confía en él y lo acepta o no.
- Bloqueados (*blocked*): corresponden a certificados que han sido comprometidos y nunca serán aceptados como de confianza.

En la [Ref.- 21] se puede consultar la última versión de la *Trust Store*, dependiente de la versión de iOS empleada. La versión de la *Trust Store* instalada en un dispositivo iOS se puede consultar en "Ajustes – General – Información – A Ajustes de confianza de los certif. " (ver imagen izquierda de la <Figura 59>).

16.2 CERTIFICADOS CLIENTE

Al instalar un certificado digital cliente, denominado certificado de identidad (*Identity Certificate*) y también conocido como certificado "hoja", protegido por una contraseña, iOS solicitará al usuario tanto el código de acceso al dispositivo móvil como la contraseña del

certificado antes de proceder a su instalación (al introducir esta última, los caracteres se mostrarán brevemente tras cada pulsación, por lo que debe realizarse esta operación fuera del alcance visual de terceros), confirmándose finalmente si el perfil ha sido o no instalado:

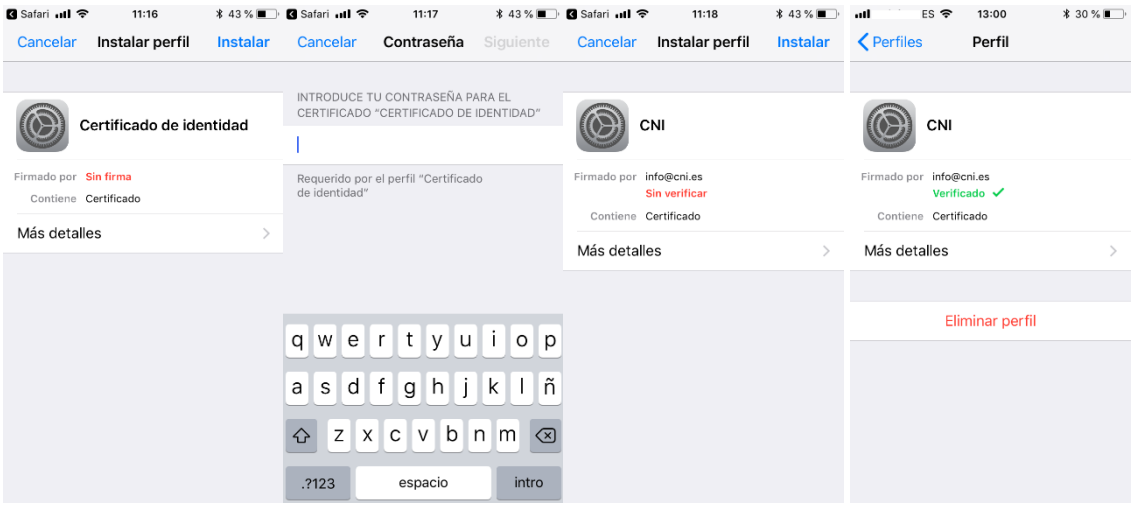


Figura 60 – Instalación de un certificado cliente o de usuario.

La confianza reflejada en el certificado ("Sin verificar", tercera imagen de la <Figura 60>) depende de si iOS dispone de la cadena de confianza completa para dicho certificado, es decir, si también confía en la CA que lo ha emitido. En iOS, si un certificado hoja ha sido emitido por una CA que aún no se ha dado de alta en el almacén de certificados del dispositivo móvil, el certificado hoja aparecerá como "Sin verificar" hasta que se importe el certificado de la CA emisora (ver apartado "16.1. Certificados raíz"). En este punto, el certificado digital cliente será identificado como "Verificado" (ver <Figura 60>).

Es posible acceder a los certificados que han sido instalados previamente a través del menú "Ajustes – General – Perfiles", y eliminarlos de forma individual.

Figura 61 – Información sobre los perfiles.

16.3 GESTIÓN DE CERTIFICADOS EN MOBILE SAFARI

iOS dispone de una implementación propia de los protocolos TLS (*Transport Layer Security*), utilizando TLS 1.2 por defecto para conexiones HTTPS y la negociación Wi-Fi EAP-TLS (este comportamiento se puede cambiar mediante un perfil de configuración).

iOS 11 eliminó el soporte para conexiones TLS basadas en certificados SHA–1, así como la confianza en certificados cuyas claves RSA sean de tamaño inferior a 2.048 bits.

Aplicaciones cliente como Safari, Calendario o Mail hacen uso de estos protocolos si el acceso al servidor correspondiente solicita su utilización. Al acceder a un sitio web mediante HTTPS (y,

por tanto, HTTP sobre TLS) utilizando Safari, el dispositivo móvil verificará el certificado digital asociado y su cadena de confianza, hasta la autoridad certificadora (*CA, Certificate Authority*) reconocida correspondiente.

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 "Mostrar detalles"). Si, pese a ello, se opta por aceptar el certificado, se volverá a pedir al usuario confirmación sobre la intención de visitar el sitio web:

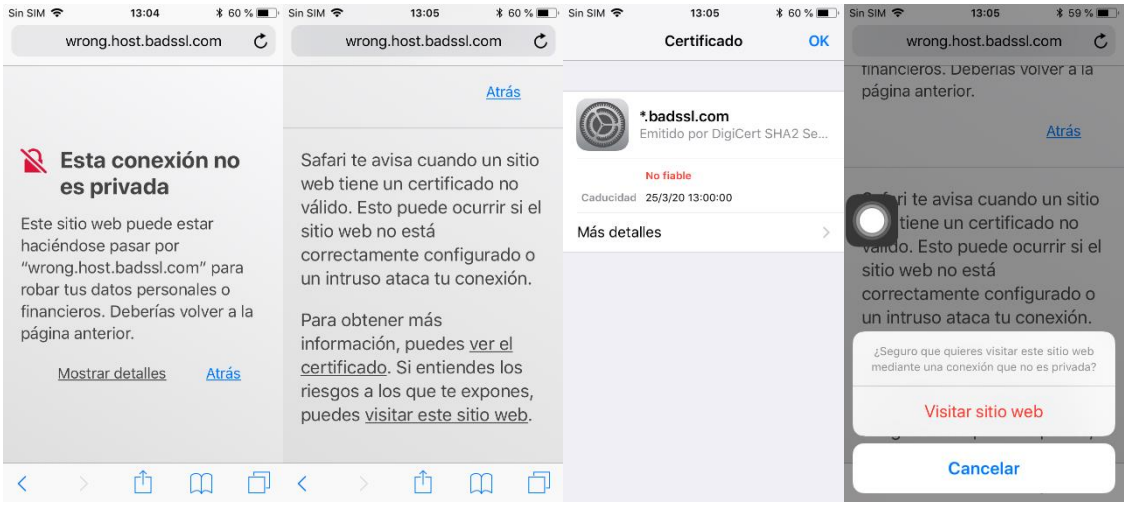


Figura 62 – Manejo de certificados inválidos en Safari.

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.

Mediante la eliminación de los datos del sitio web accedido (a través del menú "Ajustes – Safari – Avanzado – Datos de sitios web" y el botón "Editar"), 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"), tampoco se puede eliminar la validez del certificado aceptado por el usuario.

La acción de aceptar un certificado no verificado tiene el riesgo de que el certificado digital aceptado (y desconocido) pertenezca a un potencial atacante realizando un ataque de interceptación, MitM (*Man–in–the–Middle*), sobre el protocolo TLS y las comunicaciones (supuestamente) cifradas del usuario.

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 TLS e imposibilita que el usuario realice ninguna verificación.

Por las razones anteriormente mencionadas, ***es extremadamente importante evitar la aceptación de un certificado que no sea de confianza y no haya podido ser validado***.

Los perfiles de configuración de iOS (cuyo detalle excede el ámbito de la presente guía) 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"). 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.

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.

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 web, que será de color verde si se trata de un certificado con validación extendida y negro o gris si no lo es:

Figura 63 – Visualización del uso de un certificado en la barra de Safari.

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).

17. AJUSTES DE PRIVACIDAD: PERMISOS DE LAS APPS

iOS ofrece un modelo de control de acceso a las apps basado en permisos o privilegios, que impone restricciones a los recursos y componentes del sistema a los que un proceso puede acceder. La primera vez que una app solicite acceso a un recurso, iOS presentará un menú de diálogo, gestionándose por tanto los permisos en tiempo de ejecución.

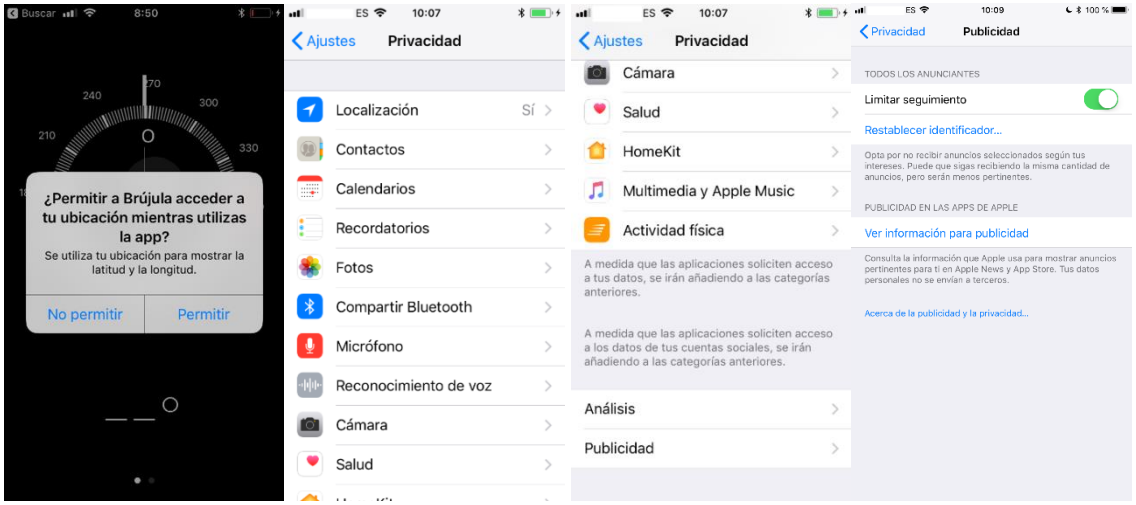


Figura 64 – Menú de diálogo solicitando el permiso de ubicación.

Los permisos se controlan a través del menú "Ajustes – Privacidad", identificando cada entrada un grupo de permisos. Bajo cada tipo o grupo de permisos se puede ver qué apps tienen concedido el permiso y, si el permiso admite distintas opciones, qué valor se ha autorizado (por ejemplo, lectura/escritura, nunca/siempre/al usarse, etc.):

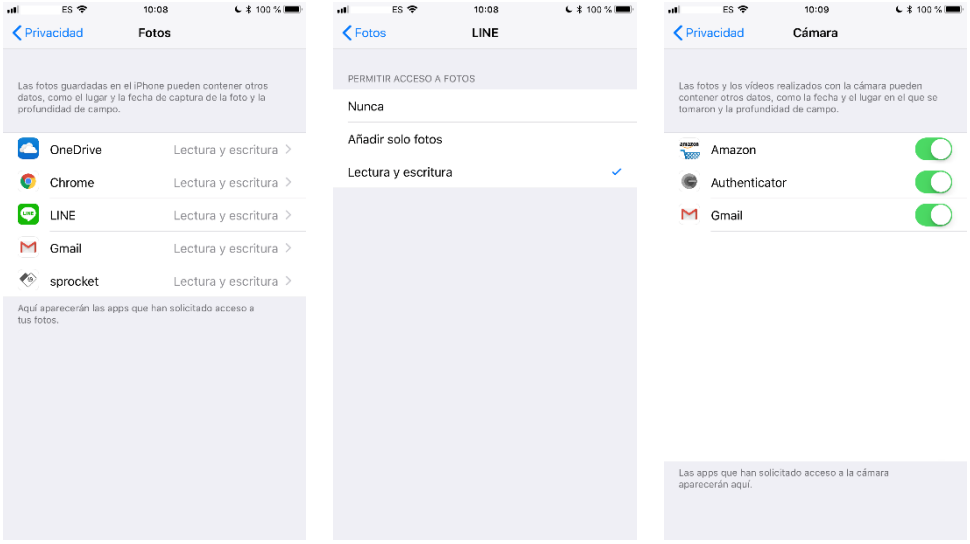


Figura 65 – Permisos a algunos recursos específicos.

Los permisos considerados más delicados desde el punto de vista de seguridad/privacidad son:

- Cámara: ya que permite a una app tomar fotografías y vídeos.
- Micrófono: permite a la app grabar conversaciones.
- Salud: por lo sensible de esta información.
- Contactos (personales y/o profesionales).
- Localización: permite a la app conocer la ubicación del dispositivo (ver apartado "14. Servicios de localización").

Adicionalmente, se incluyen las secciones "Análisis" (que remite a Apple datos sobre el uso del dispositivo) y "Publicidad" (para la recepción de anuncios personalizados, que también es enviada a Apple). Se recomienda ***limitar el acceso a estos servicios, marcando la opción "***Ajustes – Privacidad – Publicidad – Limitar seguimiento" ***y desmarcar todas las opciones bajo "***Ajustes – Privacidad – Análisis***".***

Para el resto de permisos, especialmente los más sensibles, ***se recomienda analizar cuidadosamente el acceso a los permisos de que dispone cada app y suprimir aquellos que no sean estrictamente necesarios; en caso de requerirse conceder un permiso a una app de forma ocasional, se recomienda suprimirlo tan pronto cese la necesidad.***

Se puede proceder a restablecer los valores que iOS ofrece por defecto para los permisos concedidos a las apps a través de la opción "Ajustes – General – Restablecer – Restablecer localización y privacidad" (ver <Figura 72>).

17.1 RESTRICCIONES

Importante: antes de proceder a la configuración de restricciones, se recomienda realizar una copia de seguridad del dispositivo móvil, ya que, si se olvidase la contraseña, no sería posible realizar ninguna modificación adicional (ni tan siquiera desactivarlas), siendo preciso restablecer a fábrica los ajustes del dispositivo móvil.

La funcionalidad "restricciones" permite limitar el uso de apps, funcionalidad dentro de dichas apps, y funcionalidades específicas del dispositivo móvil, protegiendo parcialmente la utilización del dispositivo móvil. Aunque el objetivo de ese servicio es establecer un control parental sobre el dispositivo, también cumple una función de protección del mismo incluso aunque un tercero disponga de acceso temporal a él con la pantalla desbloqueada.

Para habilitarlas, se accede a "Ajustes – Tiempo de uso – Contenido y privacidad" (en lugar de "Ajustes – General – Restricciones" como en iOS 11). En iOS 12, la protección de los ajustes de restricciones a través de un código de acceso de 4 dígitos es posible a través de la opción "Usar código para tiempo de uso" (fila 1, imagen izquierda de la <Figura 66>).

El código para desbloquear la configuración de las restricciones presenta el mismo comportamiento que el código de acceso al dispositivo móvil (descrito en el apartado "10.1. Código de acceso del dispositivo móvil"), incrementando progresivamente el tiempo necesario para un nuevo reintento tras 5 intentos fallidos.

Figura 66 - Restricciones del menú "Tiempo de uso – Contenido y privacidad"

Los ajustes de seguridad recomendados en esta sección son:

- "Compras en iTunes y App Store": ***establecer "Solicitar contraseña – Requerir siempre"*** (fila 2, imagen izquierda de la <Figura 66>).
- "Compras y descargas repetidas en tiendas": ***fijar todos los parámetros a "No permitir"***, salvo cuando puntualmente se vaya a hacer uso de estos servicios.
- "Restricciones de contenido – [Game Center]": ***establecer "No permitir" para la "Grabación de pantalla"***.
- "Restricciones de contenido – [Siri] Contenido de búsquedas web": permite/bloquea las búsquedas web cuando se invoca a Siri.
- "Privacidad": en esta sección es posible definir restricciones de acceso para las apps que se instalen en el dispositivo con posterioridad al establecimiento del ajuste correspondiente, y no se aplicará a las apps que lo obtuvieron previamente. ***Se recomienda valorar cada uno de estos recursos, y fijar a "No permitir" aquellos sobre los que se desea tomar más control***. De forma particular, se aconseja desactivar el permiso a "Localización", "Contactos", "Compartir Bluetooth", "Micrófono" y "Compartir mi ubicación".
- "Permitir cambios": todos los ajustes que se fijen a "No permitir" provocarán que el menú correspondiente de la sección principal de "Ajustes" no se muestren, impidiendo así que se puedan modificar. Por ejemplo, si se establece "Cambios del código - No permitir", el menú "Touch ID y código" desaparecerá de la pantalla de "Ajustes", no permitiendo la modificación del código de acceso al dispositivo mientras esté vigente la restricción. ***Se recomienda fijar a "No permitir" "Cambios en la cuenta" y "Cambios del código", teniendo presente que habrá que retornar el valor "Permitir" cuando voluntariamente se desee llevar a cabo alguna de estas acciones*** (fila 1, imagen derecha de la <Figura 66>).
- "Apps permitidas": (fila 2, imagen derecha de la <Figura 66>) este ajuste resulta muy interesante desde el punto de vista de seguridad, ya que permite suprimir de la pantalla "Home" los accesos correspondientes a las apps cuyo interruptor esté desactivado. Esto permite ocultar (y, por tanto, impedir) el uso de apps de forma selectiva.

Para más información sobre la configuración de restricciones en iOS 12, se aconseja la lectura de la [Ref.- 28].

17.2 TIEMPO DE USO

iOS 12 introduce la funcionalidad "Tiempo de uso", formada por un conjunto de herramientas y ajustes destinados a proporcionar al usuario información sobre el tiempo que dedica a interactuar con el dispositivo móvil, con las distintas apps en él instaladas, las visitas a sitios web, y el número de notificaciones recibidas.

La configuración del tiempo de uso permite establecer un período de inactividad ("Tiempo de inactividad"), durante el cual únicamente podrá accederse a las llamadas telefónicas y a las apps que se definan como excepción en la sección "Siempre permitido". Las apps se clasifican en una serie de categorías en la sección "Límite de uso de las apps", para cada una de las cuales se puede fijar un plazo máximo de utilización.

Al pulsar sobre la sección [Tiempo de uso], se obtendrán las estadísticas de interacción con las diferentes apps, tanto por nombre como por categoría, y, hacia el final de la pantalla, se presentarán también estadísticas sobre el uso de las notificaciones, desde dónde se puede abrir el interfaz de gestión de notificaciones para cambiar los ajustes de cada una de las apps que han emitido notificaciones en el intervalo de tiempo consultado.

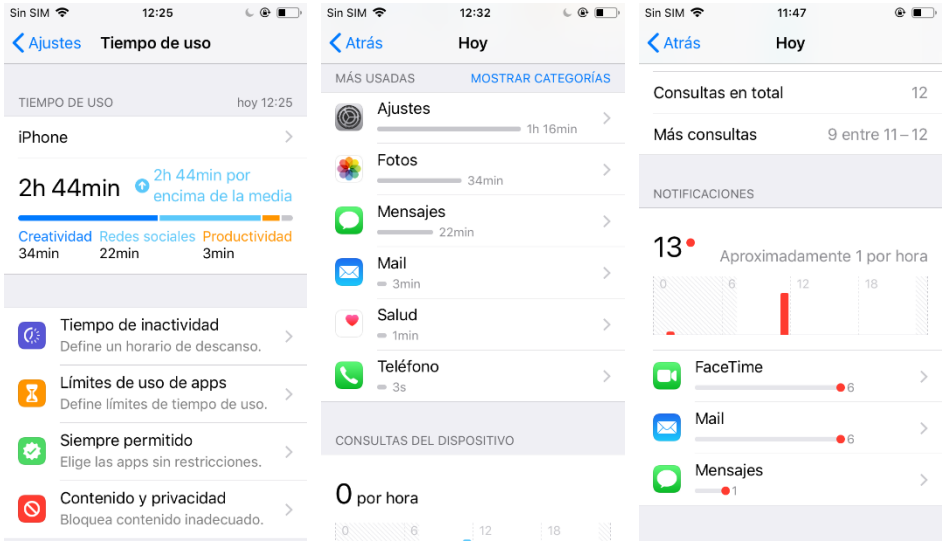


Figura 67 - Estadísticas de tiempo de uso, apps y notificaciones.

Desde el punto de vista de seguridad y privacidad, los ajustes relevantes se encuentran bajo la sección "Contenido y privacidad", el cual se describe en detalle en el apartado "17.1. Restricciones".

18. CIFRADO DEL DISPOSITIVO MÓVIL

A través del mecanismo denominado "cadena de arranque seguro" (*Secure Boot Chain*), iOS comprueba que todos los elementos implicados en el proceso de arranque (gestor de arranque, kernel y firmware de la banda base) están firmados por Apple, impidiendo el arranque del dispositivo móvil si el proceso de verificación falla y no es posible garantizar la autenticidad e integridad del sistema. Adicionalmente, desde la versión 3GS del iPhone, Apple

proporciona capacidades de cifrado hardware de la memoria flash del dispositivo móvil (en la que residen los datos de usuario) mediante un chip criptográfico, con objeto de proteger los datos incluso aunque otros elementos hayan sido comprometidos. Esta tecnología se conoce como "*Data protection*", y se basa en una jerarquía de claves criptográficas AES 256 ligadas a cada fichero (según su clase), y al sistema de ficheros en su conjunto, que se crea en la partición de datos de usuario.

iOS hace uso de clases para ofrecer las diferentes categorías de protección disponibles a nivel del sistema de ficheros (que se clasifican en cuatro: cuando el dispositivo está desbloqueado, cuando el dispositivo está bloqueado, tras el primer desbloqueo, o siempre), interviniendo en el proceso la clave única del dispositivo móvil (disponible en el módulo hardware criptográfico de los dispositivos móviles iOS), la clave del sistema de ficheros, las claves individuales de cada fichero, y las claves para las diferentes categorías de protección disponibles en el sistema, junto al código de acceso del usuario.

Adicionalmente, iOS implementa cuatro repositorios de claves o *keybags* diferentes para almacenar las claves de las diferentes clases: **usuario** (*user*), utilizado internamente para proporcionar acceso a los datos del sistema de ficheros y a los secretos del *keychain*, **dispositivo** (*device*), empleado para operaciones asociadas a datos específicos del dispositivo, **copias de seguridad** (*backup*), que ofrece la funcionalidad de copias de seguridad cifradas, y **custodia** (*escrow*), 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. Se dispone de información más detallada sobre el propósito e implementación de cada clase de protección de los ficheros y las entradas en la *keychain*¸ así como del uso de las *keybags*, y los mecanismos de cifrado en el documento oficial de seguridad de iOS [Ref.- 14] (y documentos similares [Ref.- 15]).

A pesar de todos los mecanismos de cifrado y verificación, a lo largo de la historia de iOS se han descubierto diversas vulnerabilidades y procedimientos para saltarse la protección que han permitido acceder a los datos del dispositivo móvil [Ref.- 16] [Ref.- 17]. Adicionalmente, en el pasado, se rumoreó que Apple disponía de capacidades para eliminar el código de acceso de un dispositivo móvil iOS sin conocer su valor disponiendo de acceso físico al mismo, y permitiendo acceso completo al dispositivo móvil y sus datos [Ref.- 18]. Apple ha negado este aspecto públicamente. A fecha de elaboración de la presente guía, existen empresas que ofrecen servicios y productos cuyo objetivo es obtener el código de acceso de un dispositivo móvil mediante técnicas de fuerza bruta y utilizando *exploits* no resueltos por Apple (algunos de los cuales se detallan en el informe publicado por CCN-CERT referenciado en [Ref.- 19]).

Por tanto, la mejor protección de los datos del dispositivo móvil se basa en incrementar la seguridad física, tanto del propio dispositivo como del ordenador al que se conecta (evitando accesos no autorizados), disponer de la última versión de iOS en el dispositivo móvil que resuelva la mayor parte de vulnerabilidades, elegir un código de acceso al dispositivo móvil robusto 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).

19. COPIAS DE SEGURIDAD Y RESTAURACIÓN

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.

Se recomienda realizar copias de seguridad de forma regular, y siempre que se vaya a realizar una configuración en el dispositivo que pueda ser preciso revertir (o que, por lo delicado de su proceso, pueda ocasionar pérdidas de datos o de ajustes en el dispositivo móvil).

Desde el punto de vista de seguridad, ***se recomienda realizar el backup del dispositivo móvil vía iTunes a través de un equipo de total confianza, evitando que los datos del usuario sean almacenados por Apple en iCloud.***

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

19.1 COPIA Y RESTAURACIÓN EN iCLOUD

La copia de seguridad en iCloud se almacena en los servidores de Apple y está siempre protegida por contraseña, aunque el espacio de almacenamiento gratuito se limita a los primeros 5 GB. Estas copias no incluyen los datos que el usuario ya tenga almacenados en iCloud (entre otros, Contactos, Calendarios, Notas, Fotos de iCloud, iMessages, y mensajes SMS y MMS) ni los de otros servicios de la nube (como Microsoft One Drive).

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 que se establezca ninguna vinculación con el usuario.

Para hacer uso de este servicio, hay que activar el interruptor "Ajustes – [Cuenta de usuario] – iCloud – Copia en iCloud". La opción "Realizar copia de seguridad ahora" inicia un backup si el dispositivo móvil se encuentra conectado a Internet por Wi-Fi. Con el ajuste activo, se realizará una copia diaria siempre que el dispositivo obtenga conexión a Internet mediante Wi-Fi.

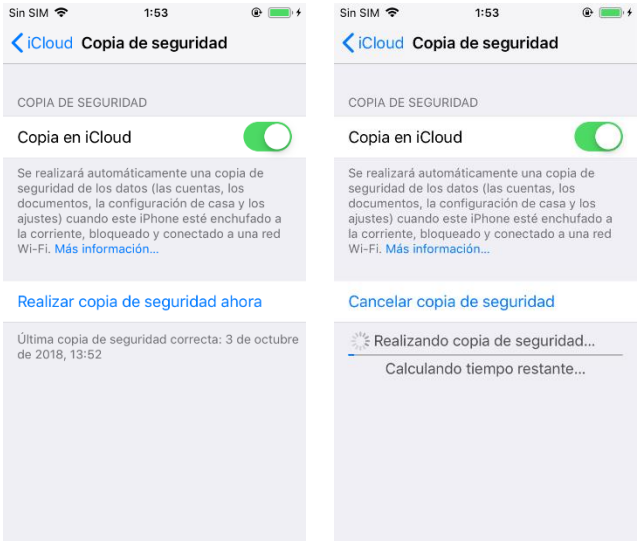


Figura 68 – Realización de copias de seguridad en iCloud.

Este mismo menú mostrará la información sobre la fecha de la última copia de seguridad realizada con éxito.

Para poder volcar en el dispositivo móvil una copia de seguridad desde iCloud, es preciso restablecerlo a fábrica (ver apartado "21. Eliminación de datos del dispositivo móvil") y, tras el

reinicio, conectarlo a una red Wi-Fi y seleccionar la opción "Restaurar con copia de iCloud", lo cual solicitará iniciar sesión utilizando el ID de Apple asociado a la cuenta de iCloud. Si la sesión se inicia correctamente, se mostrarán las copias disponibles, de entre las cuales se seleccionará la deseada. El menú de restauración guiará al usuario durante el proceso, aconsejándose posponer los pasos de configuración del ID de Apple y Touch ID para más adelante.

19.2 COPIA Y RESTAURACIÓN MEDIANTE iTUNES

La copia de seguridad se almacenará en un ordenador (macOS o Windows), pudiendo cifrarse o no (opción por defecto). Esta copia no incluye el código de acceso ni los ajustes relacionados con el acceso al dispositivo por biometría. Por su parte, para salvaguardar los datos de salud y los asociados al llavero de iCloud, se requiere que la copia sea cifrada en iTunes (opción que, en cualquier caso, es la recomendada desde el punto de vista de seguridad).

Para proceder a realizar las copias de seguridad a través de iTunes, se recomienda actualizar iTunes a la versión más reciente, que resuelve las vulnerabilidades conocidas. Tras conectar por primera vez el dispositivo móvil al ordenador, se mostrará una ventana de diálogo con el mensaje "¿Confiar en este ordenador?", que deberá ser aceptada. Una vez establecida la conexión, se seleccionará en la pantalla de iTunes el dispositivo móvil. Aunque la sincronización y backups con la aplicación iTunes del ordenador vía Wi-Fi es posible, desde el punto de vista de seguridad ***se recomienda hacer uso de la conexión mediante USB***.

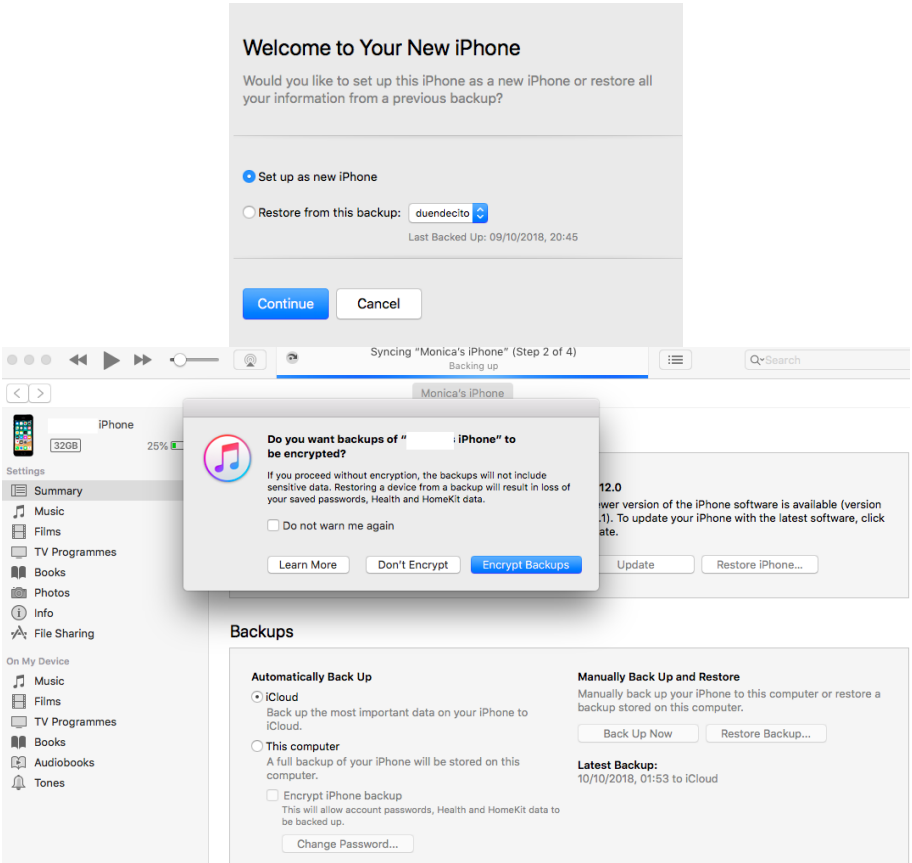


Figura 69 - Conexión al dispositivo móvil a través de un ordenador con iTunes.

Para cifrar la copia de seguridad, se debe marcar la casilla "Cifrar copia de seguridad [Dispositivo]", seleccionando una contraseña robusta. Es importante recordar esta contraseña, porque, en caso contrario, no será posible restaurar la copia de seguridad en el dispositivo móvil.

A diferencia de en versiones previas, desde iOS 11 es posible eliminar los requisitos de contraseña de los backups de iTunes, mediante "Ajustes - General - Restablecer - Restablecer ajustes", pudiendo realizar nuevos backups no cifrados o con una nueva contraseña en iTunes.

La restauración de una copia de seguridad requiere que el dispositivo móvil se conecte (preferiblemente a través de USB) al ordenador en el que ejecuta iTunes. Una vez realizada esta conexión, el proceso de restauración dependerá de la versión de iOS actualmente instalada en el dispositivo móvil y la que residía en él en el momento de la copia de seguridad:

- Si ambas coinciden, bastará con pulsar "Restaurar copia de seguridad en iTunes" y elegir la copia óptima.
- Si la versión de iOS actualmente instalada en el dispositivo es más antigua, se deberán seguir los pasos descritos en la [Ref.- 23].
- Si la versión de iOS actualmente instalada en el dispositivo móvil es más reciente, bastará con pulsar "Restaurar copia de seguridad en iTunes" y elegir la copia óptima, restaurándose la versión antigua de la copia de seguridad al dispositivo móvil.

20. ACTUALIZACIÓN DEL SISTEMA OPERATIVO iOS

Desde el punto de vista de seguridad, ***se recomienda mantener actualizada la versión de iOS, pues en cada revisión se incluyen los parches que resuelven problemas de seguridad***. No obstante, antes de proceder a instalar una nueva versión, se recomienda esperar un periodo prudencial de varios días para evitar las consecuencias de los fallos no detectados en las fases beta, a menos que la migración a la nueva versión solucione problemas de seguridad que afecten significativamente al dispositivo móvil.

Importante: Antes de proceder a la instalación de una nueva actualización, se recomienda realizar una copia de seguridad del dispositivo móvil que posibilite la vuelta atrás (*rollover*) en caso de fallo o si surge algún problema con la versión de iOS más moderna.

Antes de proceder a la instalación de una nueva actualización, se solicitará al usuario confirmación del código de acceso del dispositivo móvil, no siendo válida la confirmación mediante biometría (aunque esté configurado Touch ID o Face ID).

Los dos métodos disponibles para proceder a la actualización de la versión de iOS son la descarga a través de la red Wi-Fi desde el propio dispositivo móvil o la actualización a través de iTunes; ambos se describen a continuación.

20.1 ACTUALIZACIÓN VÍA WI-FI

A partir de iOS 12, durante el proceso de activación (ya sea en un terminal nuevo o en uno que se actualice desde la versión 11) se solicitará al usuario decidir si desea que el dispositivo móvil se actualice automática o manualmente (imagen izquierda de la <Figura 70>). La opción seleccionada dará valor al ajuste "General – Actualización de software – Actualizaciones automáticas". En caso de haber elegido la opción "Continuar", se activará este ajuste y el dispositivo móvil procederá a descargar y actualizar la versión de iOS tan pronto detecte que

existe una nueva versión. ***Se recomienda deshabilitar esta opción para disponer de mayor control sobre las actualizaciones de sistema operativo***.

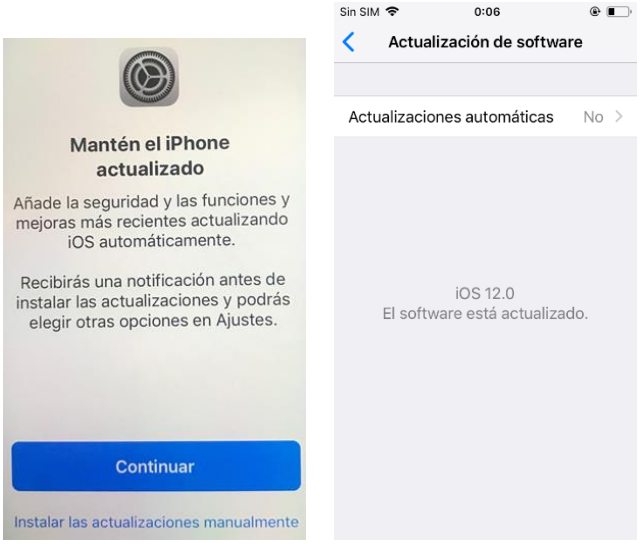


Figura 70 – Menú de activación de actualizaciones automáticas.

20.2 ACTUALIZACIÓN MEDIANTE ITUNES

La actualización de iOS a través de iTunes requiere de la conexión a través de USB[25] del dispositivo móvil a un ordenador que disponga de una versión lo más reciente posible de iTunes y en el cual se haya dado de alta el dispositivo móvil, con la correspondiente confirmación de la relación de confianza entre ambos.

La búsqueda de actualizaciones se realiza de forma semanal por parte de iTunes, pero también se puede iniciar la búsqueda manualmente desde su interfaz.

Cuando se detecta una nueva versión disponible para el dispositivo, la ventana principal del interfaz de iTunes mostrará información sobre dicha versión, y ofrecerá la posibilidad de actualizar a ella, solicitándose en el dispositivo móvil la introducción del código de acceso. Una vez validado el código, comenzará la descarga de la nueva versión y su posterior instalación. El interfaz de iTunes irá informando de las diferentes etapas asociadas a la actualización.

[25] No es posible emplear las capacidades de comunicación con iTunes a través de la red Wi-Fi para las actualizaciones de iOS.

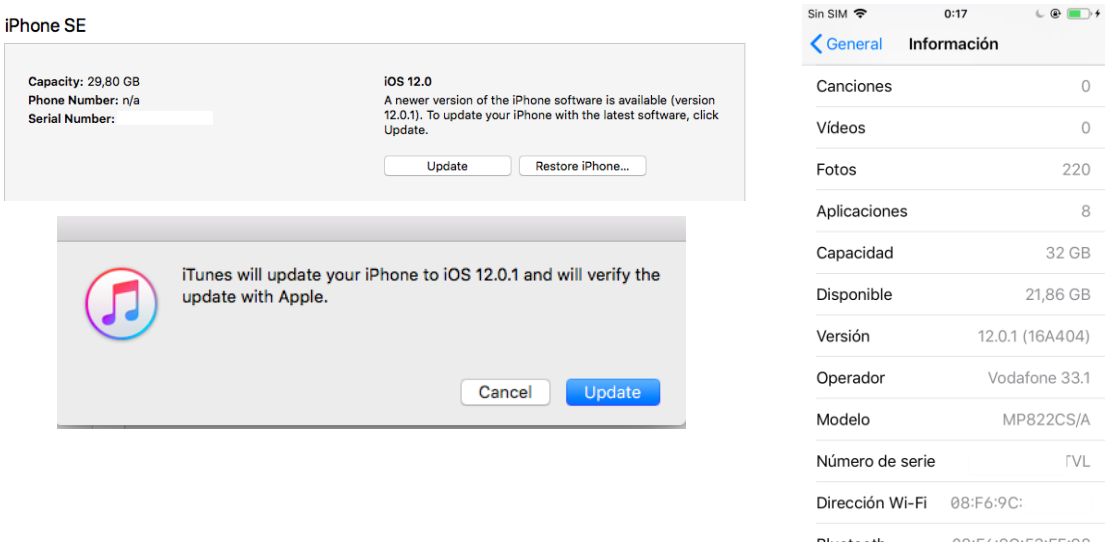


Figura 71 - Actualización de iOS a través de iTunes.

Nota: Durante la elaboración del presente informe, se liberó la versión de iOS 12.0.1, que resuelve dos vulnerabilidades descubiertas en la pantalla de bloqueo de su predecesora, iOS 12.0, por lo que se recomienda actualizar a iOS 12.0.1 tan pronto resulte posible [Ref.- 25].

21. ELIMINACIÓN DE DATOS DEL DISPOSITIVO MÓVIL

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.

Este proceso eliminará todos los datos del dispositivo, incluyendo cuentas de iCloud, iTunes y App Store, las configuraciones realizadas por el usuario, los datos de aplicaciones y del sistema, y las aplicaciones previamente instaladas. No se eliminará el software del sistema operativo ni las actualizaciones de sistema ya aplicadas, es decir, la versión existente del propio iOS. Este mecanismo es el recomendado en caso de que el dispositivo móvil vaya a pasar a manos de un nuevo usuario.

Figura 72 – Borrado de datos del dispositivo móvil.

La opción "Restablecer ajustes" permite restaurar los ajustes del dispositivo móvil a la configuración de fábrica, y también eliminará la información del usuario, junto a la clave de cifrado de los datos. El tiempo requerido para este proceso puede variar según el tipo de dispositivo móvil y la versión de iOS.

La operación de borrado de datos local también puede ser activada tras un número determinado de intentos de desbloqueo de pantalla 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 (la cual queda fuera del alcance de la presente guía). El número máximo de intentos fallidos de acceso por defecto en iOS es de 10. Este valor también puede ser definido mediante las políticas de seguridad a través de los perfiles de configuración o las soluciones de gestión empresariales (MDM). Puede verificarse si esta funcionalidad ha sido activada a través del menú "Ajustes – Touch ID y Código – Borrar datos" (ver apartado "10. Acceso físico al dispositivo móvil").

Adicionalmente, en caso de pérdida del dispositivo móvil, también es posible invocar la operación de borrado a través del servicio "Buscar mi iPhone" (ver apartado "9.1.1. Buscar mi iPhone").

22. RESUMEN DE LAS RECOMENDACIONES DE SEGURIDAD DE iOS 12

	Decálogo Básico de Seguridad
1	El acceso al dispositivo móvil debe estar protegido mediante un código de acceso, preferiblemente una contraseña alfanumérica, de al menos 8 caracteres que no esté directamente relacionado con información del usuario. El código de acceso debe solicitarse inmediatamente tras apagarse la pantalla, automáticamente a la mayor brevedad posible si el usuario deja de interactuar con el dispositivo. El dispositivo móvil no debe dejarse desatendido, menos aún estando con la pantalla desbloqueada, y debe evitarse su préstamo a terceros, incluso temporalmente.
2	Mantener el dispositivo actualizado, de forma manual (evaluando cuidadosamente la posibilidad de realizar actualizaciones automáticas en iOS 12), y realizando previamente una copia de seguridad previa a la actualización. La copia de seguridad debe estar cifrada, y, preferiblemente, realizarse a través de iTunes (frente al uso de iCloud) en un ordenador de confianza.
3	Activar el segundo factor de autentificación (2FA) en la cuenta asociada al ID de Apple asociada al dispositivo, y proteger la cuenta asociada al ID de Apple (iCloud, iTunes y App Store) con una contraseña robusta, prestando atención a las alertas de seguridad que se recibirán en los dispositivos vinculados a la cuenta y en la dirección de correo electrónico correspondiente.
4	El acceso al Centro de control debe estar deshabilitado en la pantalla de bloqueo, y la disponibilidad de contenido en las notificaciones (individuales o agrupadas en iOS 12) en la pantalla de bloqueo debe evaluarse en detalle, sobre todo para las apps más sensibles. En iOS 12 el tiempo de uso facilita la identificación de las apps que generan más notificaciones.
5	Evitar la conexión a redes Wi-Fi abiertas y ocultas, prefiriendo establecer conexiones de datos a través de un *hotspot* de uso personal. Desconectar los interfaces Wi-Fi y Bluetooth (especialmente en iOS 12 al no visualizarse fácilmente su estado) cuando no se estén utilizando, pero mantener activa la conexión de datos móviles para permitir la localización del dispositivo a través del servicio "Buscar mi iPhone". Igualmente, mantener desactivado el servicio AirDrop, y, en caso de tener que utilizarlo, configurarlo solo para los contactos.
6	Evitar conexiones USB con dispositivos ajenos, y prestar atención a los mensajes de solicitud de relaciones de confianza si, eventualmente, se requiere conectar el dispositivo a una toma USB de datos ajena.
7	Evaluar la utilización del llavero de iCloud como gestor de contraseñas, tratando de no incluir en él las contraseñas más sensibles y críticas, junto a las nuevas capacidades de autorrellenar contraseñas y códigos de seguridad en iOS 12, y al servicio de comprobación de reutilización de contraseñas.
8	Deshabilitar el uso de los servicios de localización para todas las apps que no proporcionen funcionalidad expresa de ubicación, incluidas las fotografías. Asimismo, deshabilitar el envío de información de ubicación a Apple a través de Siri, en caso de utilizarse este asistente.
9	El uso del asistente personal digital Siri se desaconseja frente a la búsqueda tradicional basada en texto. Se debe revisar el ajuste de "Sugerencias de Siri y Buscar" para cada app individualmente, desactivándolo para las aplicaciones más delicadas.
10	Configurar restricciones para limitar el uso de apps sensibles, funcionalidad dentro de dichas apps, ajustes críticos y funcionalidades específicas del dispositivo móvil, protegiendo parcialmente la utilización del dispositivo móvil sin el código concreto asociado.

23. REFERENCIAS

La siguiente tabla muestra las fuentes de información a las que se hace referencia a lo largo de la presente guía:

Referencia	Título, autor y ubicación
[Ref.- 1]	iPhone. Apple. URL: http://www.apple.com/iphone/
[Ref.- 2]	iPad. Apple. URL: https://www.apple.com/ipad-pro/ URL: https://www.apple.com/ipad/ URL: https://www.apple.com/ipad–mini/
[Ref.- 3]	Iconos y símbolos de estado en el iPhone. Apple. URL: https://support.apple.com/es–es/HT207354
[Ref.- 4]	"Bluetooth Icon Missing in iOS 12: What to Do?". Teknologya. URL: https://teknologya.com/bluetooth–icon–missing–in–ios–12/
[Ref.- 5]	"Utilizar y personalizar el Centro de control del iPhone, el iPad y el iPod touch". Apple. URL: https://support.apple.com/es–es/HT202769
[Ref.- 6]	"iCloud". Apple. URL: https://www.apple.com/es/icloud/
[Ref.- 7]	"Si has olvidado el código del iPhone, iPad o iPod touch o si el dispositivo está desactivado". Apple. URL: https://support.apple.com/es–es/HT204306
[Ref.- 8]	"Utilizar Touch ID en el iPhone y el iPad". Apple. URL: https://support.apple.com/es–es/HT201371
[Ref.- 9]	"Usar Face ID en el iPhone X o posterior". Apple. URL: https://support.apple.com/es–es/HT208109
[Ref.- 10]	"Chaos Computer Club breaks Apple Touch ID". CCC. September 2013. URL: http://ccc.de/en/updates/2013/ccc–breaks–apple–touchid URL: http://vimeo.com/75324765
[Ref.- 11]	"iOS: Supported Bluetooth profiles". Apple. URL: https://support.apple.com/en–us/HT204387
[Ref.- 12]	"Configurar y usar Buscar a mis amigos". Apple. URL: https://support.apple.com/es–es/HT201493
[Ref.- 13]	"Bkav's new mask beats Face ID in "twin way": Severity level raised, do not use Face ID in business transactions". Bkav. November 2017. URL: http://www.bkav.com/d/top-news/-/view_content/content/103968/face-id-beaten-by-mask-not-an-effective-security-measure
[Ref.- 14]	"iOS Security" (iOS 12). Apple. September 2018. URL: https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf
[Ref.- 15]	"iOS Hardening Configuration Guide for iPod Touch, iPhone and iPad devices running iOS 9.3 or higher". Australian Cyber Security Center. August 2016. URL: https://acsc.gov.au/publications/protect/ios–hardening–guide.htm
[Ref.- 16]	"iPhone security model & vulnerabilities". Cédric Halbronn, Jean Sigwald. Sogeti / ESEC. HITB SecConf 2010. 2010. URL: http://esec–lab.sogeti.com/static/publications/10–hitbkl–iphone.pdf
[Ref.- 17]	"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.- 18]	"iOS Forensic Analysis for iPhone, iPad, and iPod touch". Sean Morrissey. APress. URL: http://www.apress.com/9781430233428
[Ref.- 19]	"CCN–CERT IA–10/18 Informe de Ciberamenazas 2017 y Tendencias 2018 – Dispositivos y Comunicaciones Móviles". CCN–CERT. Mayo 2018. URL: https://www.ccn–cert.cni.es/informes/informes–de–amenazas–ia/2892–ccn–cert–ia–10–18–informe–de–ciberamenazas–2017–y–tendencias–2018–dispositivos–y–comunicaciones–moviles/file.html

Referencia	Título, autor y ubicación
[Ref.- 20]	"Configurar tus datos médicos en la app Salud de tu iPhone". Apple. URL: https://support.apple.com/es–es/HT207021
[Ref.- 21]	"List of available trusted root certificates in iOS 12, macOS 10.14, watchOS 5, and tvOS 12". Apple. URL: https://support.apple.com/es–es/HT209144
[Ref.- 22]	"Apple Configurator". Apple. URL: https://support.apple.com/apple–configurator
[Ref.- 23]	"Restaurar a partir de una copia de seguridad de iTunes o iCloud cuando se requiere una versión posterior de iOS". Apple. URL: https://support.apple.com/es–es/HT203434
[Ref.- 24]	"Acerca de la tecnología avanzada Face ID". Apple. URL: https://support.apple.com/es-es/HT208108 URL: https://images.apple.com/business/docs/FaceID_Security_Guide.pdf
[Ref.- 25]	"Bypassing iOS Lock Screens: A Comprehensive Arsenal of Vulns". DinoSec. URL: http://blog.dinosec.com/2014/09/bypassing-ios-lock-screens.html "Acerca del contenido de seguridad de iOS 12.0.1". Apple. URL: https://support.apple.com/es-es/HT209162 "Canal de YouTube "videosdebarraquito". José Rodríguez. URL: https://www.youtube.com/watch?v=CjiLN2L_v5k URL: https://www.youtube.com/watch?v=X2yQS1VzmZ0
[Ref.- 26]	"Here's how Apple's new Files app works in iOS 11". Digital Trends. October 2017. URL: https://www.digitaltrends.com/mobile/files-ios-11-app-attack/
[Ref.- 27]	"Usar contraseñas específicas para apps". Apple. URL: https://support.apple.com/es-es/HT204397
[Ref.- 28]	"Utilizar los controles parentales del iPhone, iPad y iPod touch de tu hijo/a". Apple. URL: https://support.apple.com/es–es/HT201304#set–restrictions

La siguiente tabla muestra las referencias documentales asociadas directamente a las publicaciones del CCN–CERT:

Referencia	Título, autor y ubicación
[Ref.- 400]	"Guía CCN–STIC–450: Seguridad de dispositivos móviles". CCN–CERT. Marzo 2013. URL: https://www.ccn–cert.cni.es/series–ccn–stic/guias–de–acceso–publico–ccn–stic/6–ccn–stic–450–seguridad–en–dispositivos–moviles/file.html
[Ref.- 401]	"Guía CCN–STIC–453(A) – Seguridad de dispositivos móviles: Android 2.x". CCN–CERT. Mayo 2013. URL: https://www.ccn–cert.cni.es/series–ccn–stic/guias–de–acceso–publico–ccn–stic/11–ccn–stic–453–seguridad–en–android/file.html
[Ref.- 402]	"Guía CCN–STIC–453B – Seguridad de dispositivos móviles: Android 4.x". CCN–CERT. Abril 2015. URL: https://www.ccn–cert.cni.es/series–ccn–stic/guias–de–acceso–publico–ccn–stic/827–ccn–stic–453b–seguridad–en–android–4–x/file.html
[Ref.- 403]	"CCN–STIC–457: Gestión de dispositivos móviles: MDM (Mobile Device Management)". CCN–CERT. Noviembre 2013. URL: https://www.ccn–cert.cni.es/series–ccn–stic/guias–de–acceso–publico–ccn–stic/14–ccn–stic–457–herramienta–de–gestion–de–dispositivos–moviles–mdm/file.html
[Ref.- 404]	"Buenas Prácticas. CCN–CERT BP–03/16. Dispositivos móviles". CCN–CERT. Octubre 2016. URL: https://www.ccn–cert.cni.es/informes/informes–de–buenas–practicas–bp/1757–ccn–cert–bp–03–16–dispositivos–moviles/file.html
[Ref.- 405]	"Guía CCN–STIC–453C – Seguridad de dispositivos móviles: Android 5.x". CCN–CERT. Marzo 2018. URL: https://www.ccn–cert.cni.es/series–ccn–stic/guias–de–acceso–publico–ccn–stic/2733–ccn–stic–453c–seguridad–en–android–5–x/file.html
[Ref.- 406]	"Guía CCN–STIC–453D – Seguridad de dispositivos móviles: Android 6.x". CCN–CERT. Junio 2018. URL: https://www.ccn–cert.cni.es/pdf/guias/series–ccn–stic/guias–de–acceso–publico–ccn–stic/2901–ccn–stic–453d–seguridad–de–dispositivos–moviles–android–6–x/file.html
[Ref.- 407]	"Guía CCN–STIC–453E– Seguridad de dispositivos móviles: Android 7.x". CCN–CERT. Septiembre 2018. URL: https://www.ccn–cert.cni.es/series–ccn–stic/guias–de–acceso–publico–ccn–stic/3040–ccn–stic–453e–seguridad–de–dispositivos–moviles–android–7–x.html
[Ref.- 408]	"Guía CCN–STIC–456 Cuenta de Usuario Servicios Aplicaciones Google para Dispositivos Móviles Android". CCN–CERT. Septiembre 2018. URL: https://www.ccn–cert.cni.es/pdf/guias/series–ccn–stic/guias–de–acceso–publico–ccn–stic/3043–ccn–stic–456–cuenta–de–usuario–servicios–aplicaciones–google–para–dispositivos–moviles–android/file.html
[Ref.- 409]	"Guía CCN–STIC–454 Seguridad en iPad". CCN–CERT. Agosto 2014. URL: https://www.ccn–cert.cni.es/series–ccn–stic/guias–de–acceso–publico–ccn–stic/12–ccn–stic–454–seguridad–en–ipad.html
[Ref.- 410]	"Guía CCN–STIC–455 Seguridad en iPhone". CCN–CERT. Agosto 2014. URL: https://www.ccn–cert.cni.es/series–ccn–stic/guias–de–acceso–publico–ccn–stic/13–ccn–stic–455–seguridad–en–iphone.html