Sociedad Andaluza para el Desarrollo de las Telecomunicaciones
CONSEJERÍA DE EMPLEO, EMPRESA Y COMERCIO

seguridad+ Y CONFIANZA DIGITAL | AndalucíaCERT CENTRO DE SEGURIDAD TIC

# *Informe de divulgación*
# *Seguridad en dispositivos iOS*

| | |
|---|---|
| Tipo de documento: | *Informe* |
| Autor del documento: | *AndalucíaCERT* |
| Código del Documento: | *CERT-IF-9960-170816* |
| Edición: | *0* |
| Categoría | *Uso Interno* |
| Fecha de elaboración: | *17/08/2016* |
| N° de Páginas | *1 de 12* |

# 1 TABLA DE CONTENIDOS

## 2 OBJETIVO

El objeto de este documento es aproximar a un usuario poco experimentado a la seguridad en dispositivos iOS.

## 3 ALCANCE

Este documento va dirigido tanto al personal de la Junta de Andalucía, como al público en general. Pretende aportar las nociones básicas necesarias para entender el uso y configuración, desde el punto de vista de la seguridad, de los dispositivos iOS. Este documento ayudará a los usuarios a proteger la información gestionada por estos terminales, mantener el terminal actualizado, realizar comunicaciones seguras, etc; en cualquier caso no se debe considerar como una política de uso corporativo.

## 4 SEGURIDAD DE LA INFORMACIÓN

Hoy en día existen muchos más terminales móviles que PCs (Ordenadores Personales) y, sin duda, el sistema operativo más extendido para estos dispositivos es Android, seguido por el sistema iOS. Además, la mayor parte de estos dispositivos cuenta con conexión autónoma a Internet. Sin duda, esto supone que la cantidad de información que se gestiona en estos sistemas, más la que es transmitida hacia o desde ellos, sea enorme. Toda esta información es susceptible, tal como sucede en cualquier otro sistema TI (Tecnologías de la Información), de ser modificada, borrada o accedida de forma fraudulenta, por lo que es necesario aplicar una serie de medidas de protección.

A continuación vamos a exponer una serie de pautas para reforzar la seguridad de nuestro sistema iOS ante accesos indeseados, tanto al sistema como a la información que en él se almacena y gestiona.

### 4.1 Protección frente al acceso físico

El primer nivel de seguridad en cualquier sistema TI es el acceso físico a los sistemas que contienen la información que se necesita proteger. Para este fin tenemos cuatro opciones básicas: el bloqueo por PIN asociado a la tarjeta SIM, el bloqueo de pantalla por inactividad (o bloqueo voluntario del usuario), lector biométrico Touch ID y cifrado.

#### 4.1.1 Bloqueo por PIN asociado a la tarjeta SIM

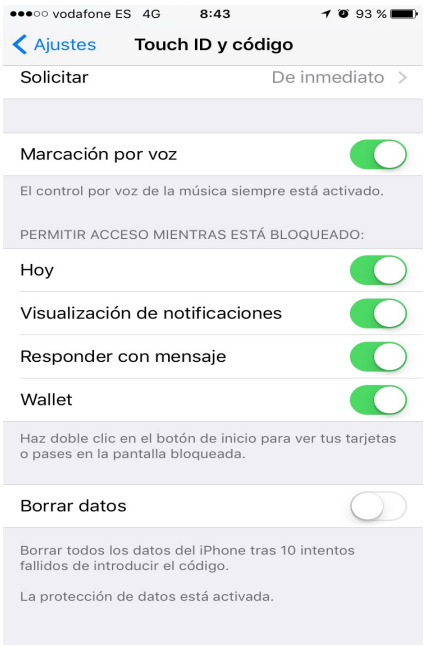
Este sistema de seguridad sólo es aplicable cuando el terminal es iniciado/reiniciado. Cuando el sistema completa el proceso de arranque nos solicita un código de activación SIM que nos ha proporcionado el operador. Sin este código el terminal sólo nos permitiría la realización de llamadas a números de emergencia. Por desgracia, la mayoría de operadores usan PIN muy cortos (lo más común es que sean de 4 dígitos), lo que los hace vulnerables a ataques por adivinación. Una primera configuración de seguridad sería cambiar la clave por defecto de nuestra tarjeta SIM por una más robusta. iOS lo permite

dentro de Ajustes → Teléfono → PIN de la SIM. Esto nos permitirá establecer un PIN de hasta de 8 dígitos.


### 4.1.2 Bloqueo de pantalla

Disponemos de una segunda capa de bloqueo de pantalla por inactividad o por bloqueo voluntario del usuario. Este sistema es el más esencial desde el punto de vista de la seguridad ante accesos indeseados al dispositivo. Mientras que el bloqueo por PIN de tarjeta sólo es aplicable en el inicio del sistema y al uso de la tarjeta telefónica, el bloqueo de pantalla nos permitirá que nuestro terminal esté activo, pero bloqueado, siempre que queramos. Incluso que se bloquee de forma automática. Este tipo de bloqueo impedirá el acceso a las funcionalidades del sistema y a la información almacenada en el mismo. iOS permite dentro de Ajustes → Touch ID Y Código ,configuraciones de complejidades mínimas para las claves. Hay que tener en cuenta que aunque el método PIN es menos seguro en cuanto a la posibilidad de la complejidad de la clave a usar, iOS implementa un sistema de retardo en la introducción de la clave tras intentos fallidos, lo que refuerza el sistema ante intentos de fuerza bruta.

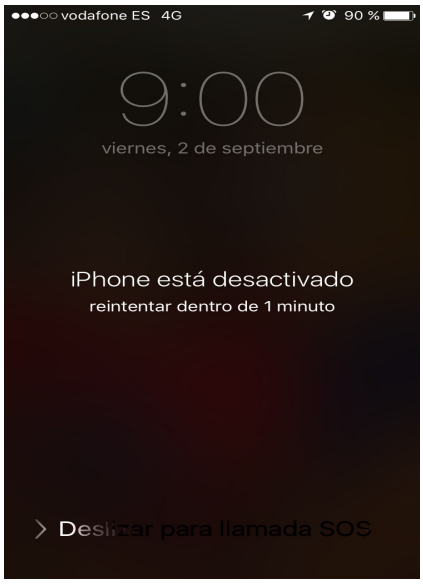
Existe una opción de seguridad en la cual, tras 10 intentos fallidos al introducir el código, el terminal borra todos los datos internos. Esta opción está desactivada por defecto en el terminal.


### 4.1.3 Touch ID

El llamado Touch ID es un lector biométrico usado para la lectura de huellas digitales. Este sistema es usado en sustitución del método de entrada por PIN, aunque en realidad hay que tener en cuenta que no lo sustituye, siempre tendremos la opción de acceso por clave aunque hayamos configurado el acceso por lectura de huella digital.

Es posible añadir varias huellas digitales y desactivar la opción de código. De hecho en el caso de que la lectura de la huella falle repetidamente el sistema nos pedirá la clave de acceso, hasta 28 intentos consecutivos, una vez pasado el numero de intentos el sistema se desactivara durante 1 minuto.


### 4.1.4 Cifrado

Aunque los métodos anteriores nos protegen de forma efectiva ante accesos ocasionales de terceros al dispositivo, como último recurso ante una posible pérdida o substracción del dispositivo, a diferencia de otros sistemas, iOS implementa por defecto una capa adicional de seguridad mediante el cifrado de los datos personales que se encuentren en el sistema. Ya que el sistema de cifrado viene implementado por defecto, en principio no hay mucho más que conocer para su uso y protección de los datos del dispositivo. Lo más importante es saber que la clave de cifrado de los datos del usuario tiene su base en la clave de acceso al dispositivo por lo que es muy recomendable que esta sea una clave robusta. Para ello es recomendable como ya se vio en el punto 4.1.2 realizar los ajustes necesarios para forzar el uso de claves robustas.

Llegados a este punto podemos intuir que en caso de que olvidemos nuestra clave de acceso al terminal, puede ser imposible acceder a nuestros datos y estos se perderían para siempre. Sin embargo Apple puede activar de forma remota el código de acceso mediante unas pautas de verificación de datos del cliente y la contraseña ID del Apple Store.

## 4.2 Protección frente a la pérdida de datos. “Copias de seguridad”

Mediante los tres pasos anteriores aplicados a un dispositivo iOS podemos afirmar, aunque la seguridad nunca es un termino absoluto, que nuestro dispositivo está configurado de forma robusta ante intentos de accesos físicos no deseados. No obstante, la información es importante y “frágil”, por lo que debemos protegerla de ataques lógicos o incluso de posibles errores involuntarios que nosotros mismos

podemos cometer. Es frecuente, sobre todo cuando se trabaja con gran volumen de información, que se borren o modifiquen datos valiosos de forma accidental. Ante estas incidencias y otros riesgos actuales como el ransomware o la pérdida del dispositivo, la medida más efectiva es el mantenimiento de copias de seguridad periódicas de la información sensible.

El sistema iOS permite por defecto dos sistemas de copia de seguridad, uno para almacenamiento en la nube iCloud y iTunes para almacenamiento de datos en local.

Las copias en local se realizan mediante la utilización del cliente iTunes el cual es compatible con los sistemas OS X y las versiones Vista, 7, 8 y 10 de Windows. Para realizar una copia de seguridad de nuestros datos personales, fotos, vídeos, libros, etc y de las configuraciones de las aplicaciones, contactos, calendarios etc, debemos conectar mediante USB o WIFI el dispositivo iOS al ordenador. En la aplicación iTunes nos deberá aparecer el dispositivo móvil en la lista de dispositivos. Realizando clic con el botón derecho del ratón, seleccionaremos la opción "Back Up" del menú contextual. Esto realizará una copia de los datos indicados anteriormente en la ruta "~/Library/Application Support/MobileSync/Backup/" en sistemas OS X y en la ruta "C:\Users\<usuario>\AppData\Roaming\Apple Computer\MobileSync\Backup\" en sistemas Windows. Es importante saber que podemos cifrar los datos de las copias de seguridad como medida adicional de protección mediante la opción "Cifrar copia de seguridad local". En caso de cifrar estos datos deberíamos hacer uso de una clave robusta.

La siguiente opción para la realización de copias de seguridad es usar la nube de Apple o iCloud. iCloud permite un servicio de almacenamiento en la nube así como la sincronización de dichos datos para todos nuestros dispositivos iOS con una limitación de 5GB para datos personales e ilimitado para las aplicaciones del APP Store. Es importante tener en cuenta que los métodos de copia de seguridad local y en iCloud no son compatibles por lo que deberemos elegir el más adecuado para nuestras necesidades. Para habilitar las copias de seguridad vía iCloud deberemos irnos a Ajustes → iCloud → Almacenamiento y copia.

# 5 OTRAS CONFIGURACIONES DE SEGURIDAD

Aparte de la protección frente accesos físicos y el control de las acciones que permitimos que las aplicaciones instaladas realicen en nuestro dispositivo, los sistemas iOS permite otras opciones de seguridad dignas de ser mencionadas a continuación.

## 5.1 Borrado remoto

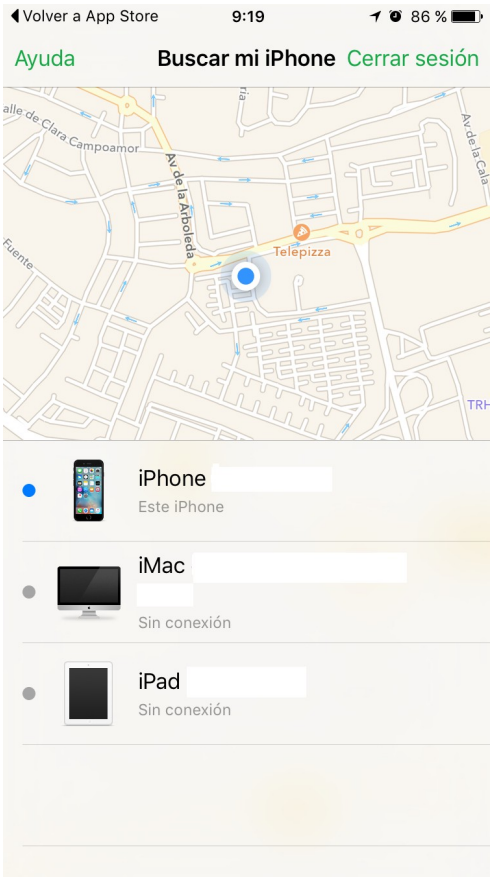
En caso de sustracción del dispositivo iOS dispone de un sistema que nos permitirá impedir el acceso al dispositivo aunque la persona que tenga acceso al terminal pueda llegar a adivinar la clave de acceso al dispositivo. El sistema, mediante una orden lanzada desde nuestra cuenta de iCloud, nos permitirá eliminar del dispositivo la clave de descifrado de los datos, de tal modo que aunque los datos no

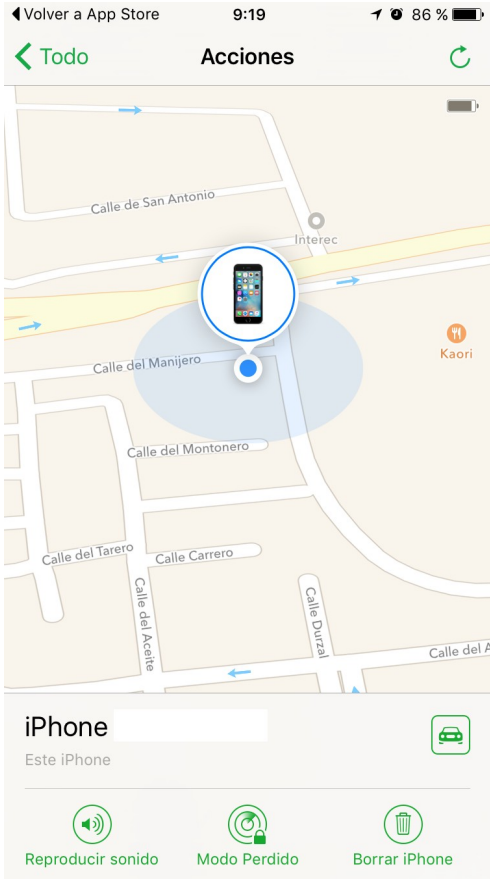
son realmente borrados sería virtualmente imposible que el atacante descifre los datos o que el propio dispositivo consiga arrancar ya que habría perdido la capacidad de leer sus propios datos.

## 5.2 Búsqueda del dispositivo

Una opción útil en caso de pérdida del dispositivo es la geolocalización. Tanto vía GPS como mediante triangulación entre las antenas de servicios 2/3/4G y WIFI se podría localizar físicamente el dispositivo.

También dispone en el menú la opción de reproducir un sonido para ayudar a la localización en caso de perdida del dispositivo incluso cuando el terminal esté en modo silencio.




## 5.3 Privacidad y Geolocalización

Aunque en caso de robo, como hemos visto en el punto anterior es útil permitir la localización del dispositivo mediante geolocalización, es muy recomendable por privacidad, controlar que información de nuestra localización aportamos y a quien se la aportamos. En iOS es posible gestionar de forma individual

en el menú de "Ajustes" en la sección de "Privacidad" gestionar de forma individual que aplicaciones pueden acceder a nuestra localización, incluso se puede afinar el filtro de cada una de ellas mediante estas 3 opciones:

- Nunca.
- Cuando se use la aplicación.
- Siempre.

Es comprensible que una aplicación tipo mapa navegador (Google Maps), necesite acceder a nuestra ubicación. Pero hay que prestar mucha atención a algunas APP's en las cuales se pide activación de micrófono, cámara frontal y localización, lo que conlleva que si no existe revisión en estos casos, nuestras conversaciones, imágenes y nuestra ubicación este expuesta al exterior.



## 5.4 Conectividad

Dentro de las posibilidades de fortificación de conectividad las más importantes son la conexión Wi-Fi y Bluetooth. En cualquier caso, como medida de seguridad se recomienda utilizar el APN corporativo en la conexión de datos móviles.

### 5.4.1 WIFI

El mejor consejo para mantener cierta seguridad en la conectividad de nuestro dispositivo a través de redes WIFI, es que no activemos la interfaz de red WIFI del dispositivo salvo que queramos conectarnos de forma consciente. Además, debemos conectarnos únicamente a redes conocidas y de confianza. Esto quiere decir que mantengamos todo el tiempo la capacidad WIFI del terminal apagada y que sólo nos conectemos a redes conocidas, evitando las típicas redes "libres". Para habilitar o deshabilitar la WIFI podremos hacerlo en Ajustes → Wi-Fi.

Es importante saber que el estado de la interfaz WIFI se mantiene cuando el terminal es reiniciado.

### 5.4.2 Bluetooth

Al igual que en el caso de la WIFI, la mejor recomendación de seguridad es no tener activada esta interfaz a menos que sepamos que vamos a hacer un uso de ella. Evitando de esta forma la interacción malintencionada de terceros con nuestro dispositivo mediante esta vía de comunicación. De nuevo, y al igual que pasaba con la interfaz WIFI, hay que tener en cuenta que ésta mantiene su estado tras un reinicio del dispositivo.

Dentro de Ajustes → Bluetooth, podemos activar o desactivar esta interfaz. También sería recomendable, ya que el nombre del dispositivo bluetooth por defecto indica de que tipo de dispositivo se trata, modificar el nombre del dispositivo por uno que no aporte información a un atacante Ajustes → General → Información.

### 5.4.3 AirDrop

AirDrop es un servicio ad-hoc de Apple que permite a los usuarios transferir archivos entre ordenadores Mac y con dispositivos iOS sin usar el correo electrónico o un dispositivo de almacenamiento masivo. Puede configurar AirDrop siguiendo las instrucciones:

- Desliza el dedo desde la parte inferior de la pantalla para abrir el Centro de control.
- Pulsa AirDrop.
- Escoge una de estas opciones:
  - Desactivado: Desactiva AirDrop.
  - Solo contactos: Solo tus contactos pueden ver el dispositivo.
  - Todos: Todos los dispositivos iOS cercanos que usen AirDrop podrán ver tu dispositivo.

## 5.5 Borrado de contenido


Aunque ya hemos visto que en caso de sustracción, iOS proporciona un sistema de borrado de datos de forma remota, también es posible realizar un borrado voluntario de los datos del sistema en caso de querer restablecer valores del sistema o borrar datos que no queramos que puedan ser accedidos nunca más.

En Ajustes → General → Restablecer, podemos realizar varias tipos de borrados tanto de contenidos y ajustes como un borrado completo hasta su restauración a los valores de fábrica.

## 6 ACTUALIZACIÓN SISTEMA OPERATIVO

En iOS, como en cualquier otro sistema operativo, es importante mantener las aplicaciones y el propio sistema actualizados. Este es un punto esencial para la defensa contra atacantes que aprovechan agujeros de seguridad para vulnerar el sistema y acceder a nuestros datos. Para ello, podemos comprobar si existen nuevas versiones de software en el menú Ajustes → General → Actualización de software.


También es posible la actualización mediante iTunes, es importante tener en cuenta que existen dos posibilidades de actualización Completa donde el sistema se descarga íntegramente llegando a los 1,2 GB para las versiones 9 de iOS o solo los archivos necesarios si la actualización se realiza desde el mismo dispositivo, sin iTunes. Debemos tener en cuenta, que cualquier proceso pesado como una actualización del sistema debe ser tomado en consideración e intentar realizarlo sólo cuando podamos garantizar la conexión y la alimentación del dispositivo.

Además será siempre recomendable realizar una copia de seguridad previa.

## 7 CONCLUSIONES

Nuestros terminales son portales a nuestras casas, familiares, amigos y trabajo. Debemos ser conscientes de que al protegernos, también lo hacemos con las personas que nos rodean. Ninguna de las configuraciones que hemos propuesto en este documento nos ofrecen una protección al 100%, aunque la combinación de las diferentes técnicas expuestas nos garantizará un grado de seguridad razonablemente aceptable. La mejor protección es un usuario consciente de los riesgos y dispuesto a tomas las decisiones necesarias en pro de su seguridad, aunque estas decisiones conlleven, sobre todo al principio, cierto esfuerzo por su parte.

En el entorno corporativo se recomienda el uso de una plataforma de gestión de dispositivos móviles (MDM – Mobile Device Management) para la gestión centralizada de los dispositivos móviles y el acceso de datos mediante el APN corporativo.

## 8 DOCUMENTACION DE REFERENCIA

Manual información iPhone 6, 6s

Manual del usuario iPhone iOS 8

Manual del usuario iPhone iOS 9

Guía de referencia sobre la implantación de iOS

Si has olvidado el código o si el dispositivo está desactivado

Cómo realizar una copia de seguridad

Actualizar el software iOS

Si pierdes o te roban el dispositivo

Gestión de dipositivos móviles de RCJA