CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

Uso seguro de iOS

Documento Público

GENERALITAT VALENCIANA

Unión Europea
Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa

Sobre CSIRT-CV

CSIRT-CV es el Centro de Seguridad TIC de la Comunitat Valenciana. Nace en junio del año 2007, como una apuesta de la **Generalitat Valenciana** por la seguridad en la red. Fue una iniciativa pionera al ser el primer centro de estas características que se creó en España para un ámbito autonómico.

Está formado por un equipo multidisciplinar de personal técnico especializado en los distintos ámbitos de la seguridad y dedicado a desarrollar medidas preventivas y reactivas para mitigar los incidentes de seguridad en sistemas de información dentro del ámbito de la Comunidad Valenciana, que abarca tanto la Administración Pública, como PYMES y ciudadanos.

CSIRT-CV ha certificado su Sistema de Gestión de Seguridad de la Información con AENOR según la norma UNE-ISO/IEC 27001:2014 cuyo alcance son los sistemas de información que dan soporte a los servicios prestados a la Generalitat Valenciana, otras Administraciones Públicas, Ciudadanos y Pymes de la Comunidad Valenciana, para la prevención, detección y respuesta ante incidentes de seguridad en las TIC's.

Datos de contacto

CSIRT-CV Centro de Seguridad TIC de la Comunitat Valenciana
http://www.csirtcv.gva.es/
https://www.facebook.com/csirtcv
https://twitter.com/csirtcv

Licencia de uso

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

Índice de contenido

1. Uso seguro de dispositivos iOS

La presente guía explica los principales aspectos a tener en cuenta para utilizar un dispositivo iOS de forma segura: configuración ideal, instalación, seguridad de aplicaciones, protección de la información y de las comunicaciones. El análisis de la guía se va a realizar sobre dispositivos con una versión de iOS original, es decir, sobre los que no se ha realizado "*jailbreak*" que permitiría realizar otro tipo de acciones, ya que suprimiría las limitaciones impuestas por Apple[1].

2. Introducción

iOS es el sistema operativo móvil de Apple. Fue lanzado en 2007 para los dispositivos móviles iPhone, pero después ha evolucionado y se ha utilizado también para otros dispositivos de la marca Apple, como los iPod, reproductores de música, y los iPad, las *tablets* de Apple. iOS tiene su base en Darwin BSD, utilizado también en OS X –sistema operativo que utiliza Apple en sus ordenadores- que integra servicios de UNIX. Aunque iOS es un software privativo, su base hace que muchas de las funcionalidades del sistema sean las propias del sistema UNIX.

Actualmente el sistema operativo iOS va por su versión 8, concretamente en el momento de escribir esta guía en la 8.3, versión soportada para los iPhone 4S y posteriores y para los modelos del iPad 2 en adelante.

El ya conocido aumento de estos dispositivos y la cantidad de información que manejamos con ellos, unido a la falta de formación y concienciación existente en materia de seguridad, nos llevan a elaborar esta guía. Cuando adquirimos un dispositivo de estas características nos preocupamos de conocer y aprender su usabilidad pero solemos olvidarnos de revisar y

[1] Si realiza *jailbreak* sobre el dispositivo, perderá todo tipo de garantía que pudiese tener el dispositivo con Apple ya que es una acción no recomendada por el fabricante.

conocer las opciones de configuración y seguridad del mismo. En muchos casos damos por supuesta la seguridad y conforme vamos utilizando el dispositivo es cuando nos vamos encontrando con los problemas. A través de esta guía queremos transmitir la importancia de ser más conscientes de sobre la seguridad en los dispositivos iOS y de conocer las medidas que debemos aplicar.

3. Seguridad de la información

Generalmente no somos conscientes de la cantidad de información que almacenamos en nuestros teléfonos móviles.

Si nos preguntan acerca de la información que contienen nuestros dispositivos, seguramente diremos que algunas fotos o algún correo, pero la realidad es bien distinta hasta el punto de que si toda la información que contiene cayese en malas manos podría causarnos un daño importante.

Para hacernos una idea, podemos plantearnos el peor de los casos en el que alguien con muy malas intenciones nos robase el móvil:

- Podría leer nuestras últimas conversaciones de chat, como pueden ser WhatsApp o Hangouts, y suplantar nuestra identidad insultando o enviando contenidos inapropiados a familiares, parejas, amigos o incluso jefes.

- Podría acceder a nuestras redes sociales y de nuevo causar estragos entre nuestros amigos, cambiar la configuración de privacidad para que todos los usuarios puedan ver todo, o incluso borrarnos la cuenta.

- Podría copiar toda nuestra lista de contactos y publicarla en Internet con el único fin de dañar también a nuestros amigos. Imaginemos esta situación si además tenemos apuntada la dirección postal de los mismos y direcciones de clientes.

- Podría acceder a nuestro historial de navegación web, historial de búsquedas, de ubicaciones, o de aplicaciones, donde se podría encontrar contenido comprometido.

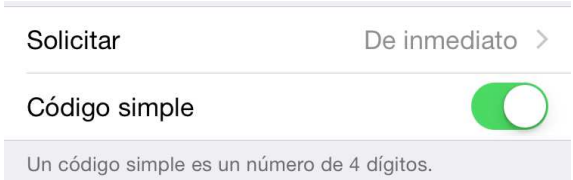
- Podría publicar cualquier tipo de fotografía o vídeo que tengamos en el móvil, compartirlo en redes sociales, o enviárselo a todos nuestros contactos mediante mensajería instantánea.

- Si tenemos configurada alguna aplicación de compras online, como la de Amazon o la propia Apple Store, podría comprar artículos a cargo de nuestra cuenta bancaria.

Por todos estos motivos resulta tremendamente necesario proteger tanto el acceso a nuestro dispositivo móvil, como la información que contiene.

3.1. Pantalla de bloqueo/código

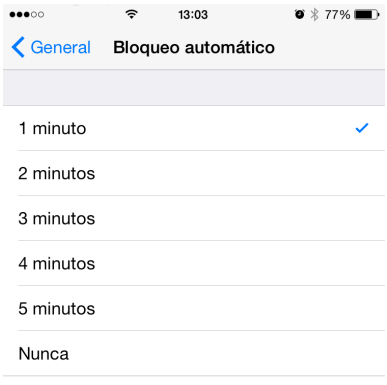
La primera medida de seguridad que resulta **imprescindible** aplicar consiste en activar el bloqueo de pantalla de forma que cada vez que un usuario quiera utilizar el dispositivo se le solicitará un código. Para ello se debe activar en >Ajustes >Touch ID y código >Activar código. iOS dispone de dos tipos de código que se pueden introducir en este caso: *simple*, que consiste en un código de 4 dígitos (según han anunciado con iOS9 será de 6 dígitos); o *complejo*, siendo un código alfanumérico sin límite de caracteres. Ambos casos son válidos aunque evidentemente resulte más seguro el código complejo (especialmente si se utilizan mayúsculas, minúsculas, números y símbolos), pero lo principal es disponer de un código y no anotarlo ni compartirlo con terceros. Asimismo debemos tener en cuenta la opción de >Solicitar



que indica cuánto tiempo va a tardar el dispositivo en solicitarnos el código después de cada desbloqueo. Recomendamos que sea "De inmediato" para no poder realizar ninguna acción sobre el sistema sin haber insertado el código de desbloqueo previamente.

Desde el iPhone 5S los terminales disponen de una tecnología añadida: **Touch ID**. Esto permite al usuario añadir hasta 5 huellas digitales que permiten, entre otras acciones, desbloquear el móvil. Los datos de la huella se cifran y son protegidos con una clave solo disponible en ese dispositivo y protegida del resto del sistema. Touch ID es una opción complementaria al código numérico o alfanumérico, ya que en determinadas situaciones nos va a ser solicitado éste aunque tengamos habilitada la opción Touch ID. Estas situaciones son:

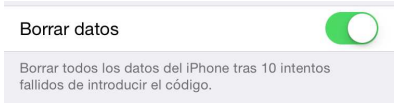
- Después de reiniciar el dispositivo
- Cuando hayan transcurrido más de 48 horas desde la última vez que desbloqueaste el dispositivo
- Para acceder al ajuste de Touch ID y código.



No sirve de nada disponer de un código si tenemos el móvil desbloqueado en todo momento o si no se bloquea tras un tiempo de inactividad. Por tanto en la opción >Ajustes >General >Bloqueo automático debe estar activada, recomendando que se bloquee automáticamente pasado 1 minuto de inactividad.

El sistema operativo nos permite añadir una medida adicional que consiste en borrar todos los datos del dispositivo tras 10 intentos fallidos de introducir el código. De esta forma si consiguiesen sustraernos el móvil e

intentaran desbloquearlo después de 10 intentos se borrarían todos los datos automáticamente. Esta opción la podemos activar en >Ajustes >Touch ID y código >Borrar datos.



Touch ID solo permite realizar cinco intentos fallidos de reconocimiento de la huella antes de tener que introducir el código manualmente, y no podremos continuar hasta que lo hagamos. Por tanto es importante no olvidar el código introducido aunque habitualmente utilicemos la huella para desbloquearlo.

Otra de las opciones que debemos revisar es la que nos permite realizar acciones en el teléfono aún con la pantalla bloqueada. Debemos comprobar estas acciones en Permitir acceso mientras está bloqueado en >Ajustes >Touch ID y código. Todas las acciones que estén activadas podrán llevarse a cabo sin necesidad de introducir el código o la huella dactilar.

3.2. Cifrado de información

Tal como hemos visto en el apartado anterior, lo más normal ante la pérdida o robo de un dispositivo es que, si éste tiene el bloqueo de pantalla, sea restaurado de fábrica por lo que nuestra información no será accesible por nadie.

Si tenemos activado el código de bloqueo, Apple lo utiliza junto a una clave de 256 bits única almacenada en el hardware del dispositivo para cifrar nuestros datos, como el correo electrónico. Ninguna persona sin autorización podrá por tanto extraer información personal del dispositivo.

Si por ejemplo conectamos el teléfono a un ordenador, tendremos que introducir el código de desbloqueo en el dispositivo para poder activar la opción "Confiar" para que éste sea reconocido por el ordenador.

Aunque de las copias de seguridad hablamos más adelante, también debemos tener en cuenta que éstas deben estar cifradas. Para ello al conectar el dispositivo al ordenador, se nos abrirá iTunes donde debemos marcar "Cifrar copia de seguridad" en la pestaña "Resumen". Cuando la

copia esté cifrada deberemos introducir la contraseña al habilitar o deshabilitar el cifrado así como cuando queramos restaurar la copia de seguridad.

3.3. Copias de seguridad

Hablamos ahora de las copias de seguridad. Como ya hemos comentado, la información que manejamos en estos dispositivos es enorme, y en muchas ocasiones es información importante o que al menos, nos gustaría no perder. Pues bien, para ello debemos tener copias de seguridad.
En los dispositivos iOS tenemos dos opciones:

- Realizar la copia directamente en el ordenador en el que tengamos sincronizado el dispositivo. Para ello debemos conectarlo al ordenador por USB y en la Pestaña "Resumen" de iTunes seleccionar "Copia de seguridad en este ordenador".
- Realizar las copias de seguridad a través de iCloud, entorno en la nube de Apple. Esto nos permite hacer las copias sin tener que conectar nuestro dispositivo al ordenador. Esta opción podemos activarla directamente desde el dispositivo en >Ajustes >iCloud >Copia de seguridad >Copia en iCloud.

4. Permisos de aplicaciones

Antes de comenzar con los permisos, debemos conocer que para poder instalar una aplicación en estos terminales, debe haber sido autorizada primero por la propia Apple y estar disponible a través de su tienda, App Store. En ningún otro caso, salvo si se ha realizado *jailbreak*, se puede instalar una aplicación de terceros.

El sistema operativo iOS no permite ver antes de la descarga de una aplicación los permisos a los que ésta tendrá acceso. Una vez instalada la aplicación, la primera vez que la abramos nos solicitará permisos para acceder a información o funcionalidades del sistema como la cámara, fotos, micrófono, calendario o

contactos. Estos permisos posteriormente se pueden comprobar y revocar desde >Ajustes >Privacidad donde podemos ver los accesos que se tienen a:

- Localización
- Contactos
- Calendarios
- Recordatorios
- Fotos
- Compartir Bluetooth
- Micrófono
- Cámara
- Salud
- HomeKit
- Actividad física

Dentro de cada una de estas opciones se ven las aplicaciones que tienen acceso a esa característica y también se pueden eliminar esos permisos. Cabe tener en cuenta que la revocación de alguno de estos permisos pueden provocar que la aplicación en cuestión no funcione correctamente.

Otra manera de revisar los accesos de los que dispone cada una de las aplicaciones es accediendo a las **opciones de privacidad** de cada una de ellas. Para ello en >Ajustes, aparecen todas las aplicaciones instaladas en el dispositivo y accediendo a ellas podemos visualizar y modificar estos permisos.

Como hemos comentado en el anterior apartado, es fundamental conocer el uso que están haciendo las aplicaciones de las utilidades del dispositivo y las configuraciones de privacidad de las que dispone. Apple dispone de sus herramientas de validación de *apps* con sus requisitos pero los usuarios finales somos nosotros y es nuestra privacidad la que está en juego.

4.1. Localización

La localización es una de las características más utilizada por las aplicaciones e iOS permite, además de impedir el acceso a la ubicación de

determinada aplicación, definir si una aplicación puede tener acceso a la ubicación aunque se esté ejecutando en segundo plano, o solo permitir el acceso cuando la aplicación esté visible en pantalla.

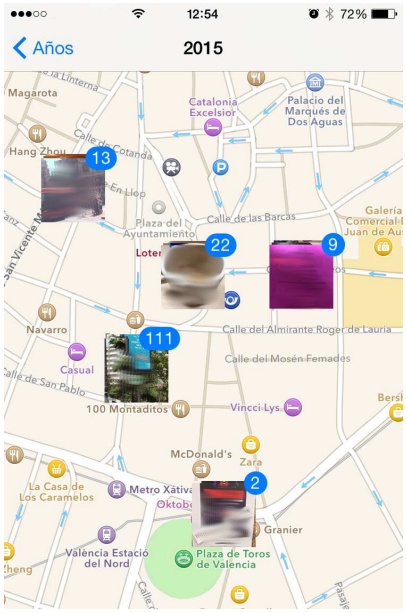
Además de las aplicaciones, el sistema operativo también utiliza la ubicación de nuestro dispositivo. Podemos ver qué servicios utilizan la localización en >Ajustes >Privacidad >Localización >Servicios del sistema. Recomendamos revisar todas estas opciones y desactivar aquellas que se consideren innecesarias para el uso que vamos a realizar del dispositivo. Entre las opciones más destacables están:

- Ubicaciones frecuentes: Apple registra en el dispositivo las ubicaciones en las que solemos estar y el momento en el que estamos. Si tenemos habilitada esta opción, veremos el historial de los sitios más frecuentes en los que hemos estado y el momento concreto. Esta información sirve entre otras cosas, según informa la propia empresa, para tener información de los sitios habituales y ofrecer cálculos de lo que se tardaría en llegar a casa o al trabajo. Desde Apple informan que esta información solo está almacenada en el dispositivo de forma cifrada y que solo podrá ser utilizada por ellos de forma anónima y solo en el caso en que tengamos activada la opción Mejorar Mapas. Debemos valorar la utilidad del servicio prestado frente al almacenamiento de estos datos en el dispositivo.

- iAds según la ubicación: proporciona servicios publicitarios personalizados basándose en la localización. Según Apple es una información que no facilitan a los anunciantes pero en cualquier caso su única funcionalidad es la de ofrecer anuncios dirigidos, algo que a priori tampoco aporta un importante valor al usuario por lo que recomendamos deshabilitarla.

- Diagnóstico y uso: Apple dispone de una opción en >Ajustes >Privacidad >Diagnóstico y uso donde recoge y envía automáticamente información diaria del uso del dispositivo para mejorar sus productos y servicios. Esta información puede incluir datos de localización por lo que recomendamos deshabilitar también

esta opción.



Dentro de las aplicaciones que utilizan la localización, aparecen algunas propias del dispositivo como es el uso que hace la cámara de la localización para geoposicionar las imágenes y los vídeos que se hacen con el dispositivo. Teniendo activada esta opción, incluso, como vemos en la imagen que acompaña este texto, nos permite posicionar en un mapa las fotos realizadas.

En definitiva, debemos conocer qué aplicaciones tienen acceso a nuestra localización y revocar aquellas que no utilicemos o no consideremos necesarias.

4.2. Contactos

Lo mismo que hemos comentado que ocurre con la localización pasa con la agenda de contactos. Son muchas las aplicaciones que intentan hacer uso de esta información almacenada en el dispositivo. Un ejemplo son algunas redes sociales que comprueban los contactos que tiene el usuario en la propia red social con la agenda de contactos del teléfono para mostrar coincidencias o sugerir añadir los perfiles de los contactos a la red de forma fácil. Otro ejemplo que también ocurre es el de los juegos que nos permiten enviar invitaciones a nuestros contactos y para ellos nos solicita acceso a toda nuestra agenda. En estos casos, sino consideramos necesaria esa funcionalidad de la aplicación que hace uso de los contactos podemos eliminar los permisos como hemos indicado anteriormente.

5. Configuración segura de iOS

Una vez explicadas las principales consideraciones a tener en cuenta para proteger la información almacenada en nuestro dispositivo, se va a dar un

repaso por los principales parámetros de configuración que tiene iOS explicando aquellos relevantes para evitar que nuestro terminal se infecte con un virus, que espíen nuestras conversaciones, o incluso para evitar que se hagan pagos con nuestro móvil sin permiso.

5.1. Wifi

Cada vez más usuarios de dispositivos móviles están concienciados de que es altamente peligroso conectarse a redes Wifi desprotegidas (aquellas que no llevan contraseña), ya que por norma general resulta muy sencillo interceptar la información que por ahí se envía, incluyendo conversaciones y contraseñas de acceso.

No obstante, esta no es la única consideración a tener en cuenta en lo que a redes Wifi se refiere: existen una serie de ataques informáticos mediante los cuales, por el simple hecho de tener la conexión Wifi activada, es posible robar la contraseña de algunas de las redes a las que previamente nos hayamos conectado, o incluso falsificar una red Wifi conocida por el móvil e interceptar toda la información que por ahí se envíe.

Es importante pues que mientras no estemos utilizando la conexión Wifi la apaguemos, ya que además de reducir el consumo de batería conseguiremos mejorar nuestra seguridad.

5.2. Bluetooth

De forma similar a lo que sucede con las conexiones Wifi, existen diferentes ataques informáticos mediante los cuales se puede acceder a información de nuestro teléfono móvil a través del Bluetooth. Por norma general, este tipo de ataques intentarán acceder a nuestra agenda de contactos o archivos multimedia (fotos y vídeos), además de intentar utilizar nuestra conexión de datos o incluso realizar llamadas telefónicas.

Este tipo de ataques suele aprovechar agujeros de seguridad en los programas que utilizan los fabricantes de los dispositivos móviles. Por tanto se recomienda que esta opción esté deshabilitada siempre que no se esté utilizando, tal como recomendábamos con la Wifi. En caso de activar el

Bluetooth recomendamos configurar el modo oculto para no aparecer en las búsquedas de otros dispositivos. Mientras estemos en la pantalla de "Ajustes de Bluetooth" el dispositivo será visible al resto de dispositivos cercanos, pasando al estado oculto al salir de la misma.

5.3. NFC

Con el lanzamiento del iPhone 6, los dispositivos incorporan un chip NFC con el que se podrá pagar en distintos comercios a través del sistema Apple Pay y confirmando el pago mediante la huella dactilar utilizando el Touch ID.

Apple garantiza que el sistema es seguro y que los datos bancarios se almacenan de forma cifrada en un chip especial llamado Secure Element por lo que, según aseguran, no son almacenados en servidores Apple. A pesar de esto, la tecnología NFC permite realizar compras con tan sólo acercar la tarjeta, o en este caso el teléfono, al dispositivo de pago. De esta forma, aunque para validar la compra en principio requiere que el usuario inserte un código PIN o la huella dactilar en el caso del iPhone, se podría obtener información valiosa de la tarjeta. Conviene saber que la tecnología NFC en el momento de publicación de esta guía, no es todo lo segura que podría serlo, pero como tampoco lo es el proceso tradicional de pago con tarjetas de banda magnética. Por tanto antes de utilizar esta tecnología debemos conocer los riesgos y tomar las medidas preventivas necesarias.

5.4. Privacidad/Localización

Como hemos comentado en el apartado 4.1., los permisos de localización son concretos para cada aplicación por lo que se pueden modificar en cada caso. Conviene revisar las aplicaciones que tienen acceso a la localización, así como las funcionalidades del sistema.

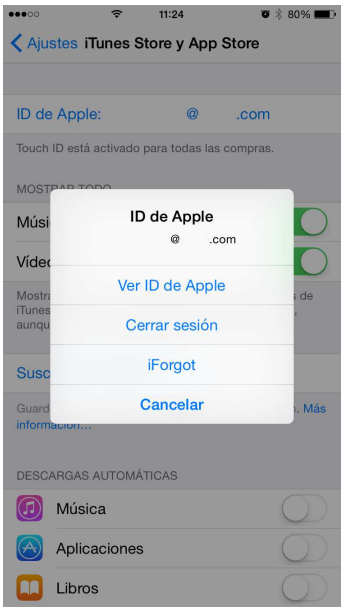
5.5. Compras

Las aplicaciones de iOS se descargan desde la conocida App Store, donde al realizar una compra siempre se nos solicitará la contraseña de ID de Apple. Los dispositivos que disponen de Touch ID pueden utilizar la huella digital en lugar de la contraseña si tienen

activada la opción correspondiente en >Ajustes >Touch Id y código >iTunes Store y App Store. Como medida adicional, en la primera compra después de un reinicio del dispositivo se nos pedirá obligatoriamente la contraseña del ID de Apple.

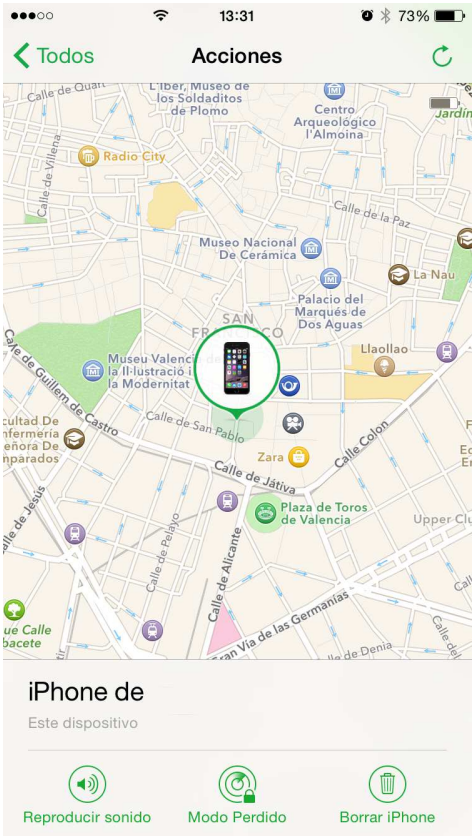
Actualmente iOS permite que se puedan realizar **compras desde dentro las propias *apps***, como puede ser el caso de algún juego que permite comprar "vidas extra" o algunos complementos adicionales. En cualquier caso al descargar la aplicación desde la App Store se nos informa con el texto "Compras dentro de la app" de que en dicha aplicación podemos encontrarnos opciones de compra. Generalmente, también se solicitará la contraseña del ID de Apple al realizar este tipo de compras. En cualquier caso debemos tener cuidado de no comprar cosas de forma involuntaria desde dentro de cualquier App.

Apple almacena **los datos de pago** en sus propios servidores. Para poder consultar la información desde el teléfono debemos acceder a >Ajustes >iTunes Store y App Store >ID de Apple: *dirección@dominio.com* >Ver ID de Apple y nos solicitará la contraseña asociada al ID. En ese apartado aparecerá la información asociada al ID de Apple y seleccionado "Datos de pago" podremos ver el método de pago que tenemos asociado e información de los pagos para iTunes, iCloud y Apple Online Store, entre otros. En el caso de la tarjeta de crédito solo aparecerán los 4 últimos dígitos de la misma. Estos datos bancarios están almacenados en los servidores de Apple Store. En el apartado 5.7. Llavero de iCloud podemos encontrar más información sobre las medidas de seguridad de esta información y la forma de almacenamiento de Apple.



5.6. Buscar mi iPhone

Apple introdujo en todos sus dispositivos la opción "Buscar", una herramienta que te permite localizar todos los dispositivos asociados a la misma cuenta de iCloud. De este modo si perdemos o nos roban uno de estos dispositivos, podemos realizar alguna de estas acciones en remoto desde otros dispositivos o desde la web:



- Localizar el dispositivo en el mapa
- Reproducir un sonido en el dispositivo extraviado.
- Activar el modo perdido. Modo que bloquea el terminal con un código, podemos mostrar un mensaje personalizado en la pantalla mientras hacemos el seguimiento de su ubicación.
- Borrar toda la información del dispositivo.

Además, en el caso en el que haya algún dato bancario en la aplicación Passbook, "Buscar mi iPhone" intentará eliminarlas de forma inmediata.

Para activar "Buscar mi iPhone", debemos activarlo en >Ajustes > iCloud >Buscar mi iPhone. Cabe destacar que para que sea efectiva la búsqueda, el dispositivo debe tener batería. En el caso de que se quedase sin batería no se podría saber la ubicación salvo que tengamos habilitada también la opción Enviar última ubicación que envía la localización a Apple cuando el nivel de batería del dispositivo sea muy bajo.

Hay que tener en cuenta que todas estas opciones nos ayudan a localizar el

iPhone en determinadas situaciones, pero que por otro lado cualquier que dispusiese de nuestra contraseña de iCloud podría localizarnos a través de esta funcionalidad. Por tanto la contraseña de iCloud debe ser única, personal y robusta.

Por último, señalar que con la opción Buscar mi iPhone habilitada, no se podrá restaurar el dispositivo, ni directamente desde el terminal, ni conectándolo al ordenador a través de iTunes.

5.7. Llavero de iCloud

El llavero de iCloud nos permite sincronizar todas las contraseñas y datos de nuestras tarjetas de crédito a través de iCloud de forma que podamos disponer de ellos en todos nuestros dispositivos iOS o equipos con OS X. Por ejemplo, si introducimos nuestras credenciales de acceso en algún sitio web en Safari, nos preguntará si queremos recordarlas. Si seleccionamos esa opción, la contraseña quedará almacenada en el llavero de iCloud y por tanto disponible en todos los dispositivos donde tengamos habilitado el llavero con el mismo ID de Apple. Cuando un nuevo dispositivo se configura para acceder al llavero iCloud el resto de dispositivos reciben una notificación solicitando la aprobación.

Se pueden visualizar y eliminar las contraseñas almacenadas en Safari desde el dispositivo. Para ello debemos acceder a través de >Ajustes >Safari >Contraseñas y autorrelleno >Contraseñas guardadas. Para acceder se nos solicitará el código de seguridad del teléfono.

Según Apple, el llavero iCloud "utiliza un cifrado AES de 256 bits para almacenar y transmitir contraseñas e información sobre tarjetas de crédito". En cualquier caso, aseguran que a través de los servidores de Apple solo pasan los datos del llavero cifrado, y son descifrados en el propio dispositivo asociado.

Si deseamos habilitar "Llavero de iCloud", recomendamos al menos deshabilitar la opción de recuperación del llavero. Esta opción nos permite poder recuperar el llavero en caso de perder los dispositivos pero a cambio el llavero, aunque cifrado, permanecerá en los servidores de Apple.

5.8. Publicidad

En cuanto a la publicidad, además de la opción recomendada en el apartado 4.1. de desactivar la localización para iAd, en >Ajustes >Privacidad >Publicidad disponemos de la opción "Limitar seguimiento de publicidad". Si la opción está activada se evita recibir anuncios de iAd relacionados con los intereses del usuario ya que limita el seguimiento del usuario por parte de anunciantes y agencias de publicidad en base a un identificador temporal del dispositivo. Esta opción no significa que recibamos menos publicidad sino que esta irá menos dirigida porque los anunciantes tendrán el seguimiento limitado. Recomendamos, desde el punto de vista de la privacidad, activar esta opción "Limitar seguimiento" así como restablecer periódicamente el identificador temporal asociado al dispositivo. Con estas medidas, así como la de la localización para las redes de anuncios y publicidad (iAd) limitamos la información que los anunciantes dispondrán sobre nosotros y el uso del dispositivo.

6. Actualizaciones del sistema operativo y de las aplicaciones

Igual que sucede en los ordenadores, cada día se descubren vulnerabilidades y agujeros de seguridad que afectan igualmente a aplicaciones móviles como al propio sistema operativo del dispositivo.

Es por ello que igual que hacemos con nuestro ordenador y sus aplicaciones, debemos de tener el dispositivo móvil y sus aplicaciones correctamente actualizadas.

Ya que no resulta cómodo actualizar las aplicaciones "a mano" cada vez que surge una actualización nueva (pueden surgir varias a la semana dependiendo del número de aplicaciones que tengamos instaladas), lo más recomendable es activar las actualizaciones automáticas de las aplicaciones. Esto se activa desde >Ajustes >iTunes Store y App Store >Actualizaciones,

comprobando que tenemos desactivada la opción "Usar datos móviles" para que solo se descarguen si estamos conectados a una red Wifi y no se consuman *megas* de la tarifa de datos.

En lo referente a las actualizaciones del sistema operativo, Apple nos mostrará una notificación cuando haya alguna disponible. Debemos ir a >Ajustes >Actualización software y seleccionar la nueva versión o bien actualizarla desde iTunes conectando el dispositivo al equipo. Recordemos hacerlo cuando estemos conectados a una red Wifi y habiendo realizado previamente una copia de seguridad de la información.

7. ¿Antivirus en el móvil?

Dejamos para el final uno de los temas que más dudas causa entre los usuarios de dispositivos móviles: ¿hace falta instalar un antivirus?

De la misma forma que existen virus informáticos para ordenadores, existen virus informáticos para teléfonos inteligentes. Los creadores de virus cada día dedican más recursos a intentar infectar y comprometer los dispositivos móviles, ya sea para robar información, contraseñas, información personal, o sencillamente para controlarlos y poder lanzar ataques desde estos, exactamente igual que con los ordenadores. El hecho de que casi todo el mundo tenga un teléfono propio el cual suele estar conectado a Internet todo el día, los convierte en un objetivo muy atractivo para este tipo de delincuentes

Si bien es verdad que la forma de funcionar de los virus para móvil es muy similar a la de los ordenadores, en los móviles existen ciertas limitaciones en cuanto a la forma de propagación. Aunque los sistemas no son 100% fiables, Apple indica que su sistema es invulnerable en el caso de no realizar *jailbreak* y por tanto no instalar nada que no esté en la App Store. El proceso de verificación de A*pps* de Apple para iOS es muy exhaustivo pero a pesar de todo puede aparecer alguna vulnerabilidad o una fuente de infección.

Por tanto, a pesar de las medidas que garantiza el fabricante, no estaría de más disponer de algún antivirus, siempre recordando que lo más importante es no bajar la guardia en el resto de buenas prácticas: no abrir ficheros sospechosos (correos, mensajería instantánea, Internet), no realizar *jailbreak*, y tener en todo momento el sistema operativo y las aplicaciones lo más actualizadas posible.

8. Contacto y consultas

En caso de desear ampliar la información sobre este u otros temas, o acceder a toda la oferta formativa del Centro de Seguridad TIC de la Comunitat Valenciana, es posible hacerlo en las siguientes direcciones:

http://www.csirtcv.gva.es

https://www.facebook.com/csirtcv

https://twitter.com/csirtcv