CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

USO SEGURO DE iOS

Documento Público

Marzo de 2020

GENERALITAT VALENCIANA
Conselleria d'Hisenda i Model Econòmic

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa
UNIÓN EUROPEA

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.

Este documento es de dominio público bajo licencia Creative Commons Reconocimiento – NoComercial – CompartirIgual (by-nc-sa): No se permite un uso comercial de la obra original ni de las posibles obras derivadas, la distribución de las cuales se debe hacer con una licencia igual a la que regula la obra original.

Índice de contenidos

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 segura 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.

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.

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 desarrollar esta guía. Cuando adquirimos un dispositivo de estas características nos preocupamos de conocer y aprender su usabilidad pero solemos olvidarnos de revisar y 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 este contenido queremos transmitir la importancia de ser más conscientes 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 y 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 o 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 el propio 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.

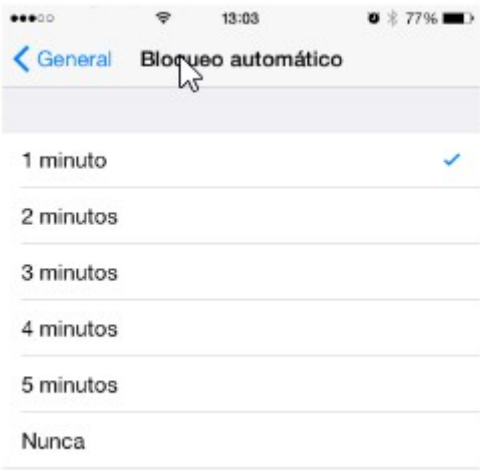
iOS dispone de dos tipos de código que se pueden introducir en este caso: *simple*, que consiste en un código de 4 dígitos (desde iOS9 podrá ser de 6 dígitos); o *complejo*, siendo un código alfanumérico sin límite de caracteres.

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. Personalizar mensaje en la pantalla de bloqueo

Como hemos comentado anteriormente, debemos establecer un bloqueo de pantalla que garantice que nadie pueda tener acceso a utilizar nuestro dispositivo.

Pero en caso de pérdida del teléfono o en caso de emergencia, nadie podrá acceder a nuestros contactos para avisar de la situación. Por tanto, sería muy útil que aparezca un texto informativo en la pantalla de bloqueo, indicando un número de teléfono al que podrían llamar.

De momento en iOS no hay posibilidad de configurarlo desde ninguna opción de ajustes, pero podemos hacerlo de la siguiente manera:
La imagen que queremos tener como fondo en la pantalla de bloqueo, la editamos y le añadimos un texto con el teléfono y el mensaje que queremos que se muestre. Guardamos la imagen editada y la elegimos como fondo de la pantalla de bloqueo.

Por ejemplo, podemos escribir el siguiente texto:
"(escribir un teléfono al que deberán llamar) para emergencias"

3.3. Información médica y contactos de emergencia

Aunque tengamos el teléfono bloqueado, siempre es posible llamar al 112, pero en caso de accidente, resulta muy útil tener configurado en el móvil algún teléfono al que avisar y aquella información médica nuestra que cualquiera podría ver sin necesidad de desbloquearlo. Pese a que los datos de salud son considerados como datos personales de categoría sensible, sería importante informar del grupo sanguíneo que somos, nuestro peso, la medicación actual, alergias, la fecha de nacimiento para que sepan nuestra edad… aunque el móvil esté bloqueado.

Para configurarlo, desde la versión iOS 8 y posteriores, debemos seguir estos pasos:
Acceder a la aplicación Salud > Datos médicos > Crear datos médicos

Para visualizar esta información debemos pulsar en "SOS" que siempre estará accesible, aunque tengamos el teléfono bloqueado.

3.4. Cifrado de la 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 (es decir, se borre por completo tanto las configuraciones como los datos) 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.

3.5. 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 con el programa correspondiente, normalmente iTunes para equipos con Windows y aquellos Mac que tengan macOS Mojave o versiones anteriores. Para un Mac con macOS Catalina 10.15 se utiliza el programa Finder para hacer la copia de seguridad.
  Para comenzar la copia, debemos conectar el móvil 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. **Requiere que el dispositivo esté conectado a una red Wi-Fi y que dispongamos en iCloud del espacio libre suficiente para almacenar la copia**. Esto nos permite hacer las copias sin tener que conectar nuestro dispositivo al ordenador. Esta opción podemos activarla directamente desde el dispositivo en >Ajustes >[tu nombre]>iCloud >Copia en iCloud y presionaremos

en "Realizar copia de seguridad ahora". Podemos comprobar que la copia se ha realizado si accedemos de nuevo a esta misma opción y nos fijamos en la fecha y hora de la última copia de seguridad.

Puedes consultar más información sobre las copias de seguridad, desde la *página de soporte de Apple*.

4. ¿Qué son los permisos y cómo funcionan?

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 de cada apartado, las aplicaciones que tienen permitido el acceso:

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. Podemos ver las **aplicaciones que tienen acceso** a la ubicación y el tipo de permiso que tienen otorgado, accediendo a **Ajustes>Privacidad>Localización**

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, si no 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. Desactivar "Oye Siri"

Recomendamos desactivar el asistente por voz Siri, para lo cual debemos seguir los siguientes pasos:

Ajustes > Siri y Buscar > desactivar la opción ***Activar al oír "Oye Siri"***

Si en cualquier momento deseamos hacer uso del asistente por voz, bastará con activar esta opción nuevamente.

5.2. Desactivar acceso al centro de control.

Cuando tenemos la pantalla bloqueada, se permite el acceso al centro de control de nuestro iPhone. Debemos desactivar esta opción para aumentar la seguridad, ya que por ejemplo, si nos roban el móvil no podrán activar el modo avión si no disponen de la contraseña.

Para desactivarlo, debemos seguir estos sencillos pasos:

Ajustes > Touch ID y código > en la sección "Permitir acceso al estar bloqueado" desactivar "Centro de control".

Desde aquí también podemos desactivar Siri para cuando el dispositivo está bloqueado, en caso de no hayamos desactivado por completo el asistente por voz, siguiendo los pasos indicados en el apartado anterior.

5.3. Personalizar las notificaciones

Debemos personalizar las notificaciones que se nos mostrarán cuando el dispositivo está bloqueado, ya que es posible que no deseemos que se lean los mensajes recibidos o las notas del calendario, cuando tenemos la pantalla bloqueada.

Para personalizar esta opción, debemos hacerlo desde Ajustes > Notificaciones

Se puede personalizar por aplicaciones concretas o de manera generalizada.

Desde "Mostrar previsualizaciones" podemos elegir: Siempre, Si está bloqueado, Nunca.

Si pulsamos Atrás, en "Estilo de notificación" podemos elegir para cada app el "Permitir notificaciones" y en su caso, decidir también cómo y dónde queremos que aparezcan para esa app concreta.

5.4. 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.

5.5. 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.

5.6. NFC / Apple Pay

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.

5.7. 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.

5.8. 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 > [tu nombre] > 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 cualquiera 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.

Al configurar Buscar mi iPhone, los Apple Watch y los AirPods enlazados a ese iPhone también se configuran automáticamente.

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.

5.9. Buscar a mis Amigos

Para las versiones iOS 9 a 12 del iPhone, iPad o iPod touch, la app "Buscar a mis amigos" se instala automáticamente. En dispositivos con iOS 8 se debe instalar la app desde el App Store. Debemos asegurarnos de que nuestros amigos también tienen la aplicación instalada, para poder compartir la ubicación con ellos, previo proceso de "Añadir" su ID de Apple en la aplicación.

La ubicación solo se envía cuando uno de nuestros amigos nos la solicita, y aceptamos compartirla. Existe un límite de máximo 100 amigos a los que podemos seguir o pueden seguirnos. Podemos visualizar las ubicaciones aceptadas en forma de lista o en un mapa de la propia aplicación, o en iCloud.com.

En cualquier momento podemos dejar de compartir nuestra ubicación, con tan solo desactivar la opción desde la app o desde iCloud.com.

5.10. Llavero de iCloud

Gracias al llavero de iCloud, podrás mantener a salvo todas tus contraseñas y demás información de seguridad, para que esté siempre actualizada y accesible en todos tus dispositivos. Permite guardar las contraseñas creadas por tí o incluso generar contraseñas seguras que almacenará para posteriores usos.

Además puedes guardar las tarjetas de crédito que sueles utilizar para hacer compras en Internet.

Para activar el llavero, debes seguir los siguientes pasos:
1. Acceder a Ajustes > [tu nombre] > iCloud.
2. Pulsa en Llavero.
3. Activa "Llavero de iCloud"

Una vez activado, cuando accedamos a un sitio web con usuario y contraseña, se nos pedirá si queremos guardar esas credenciales en el llavero. Además, se autocompletarán cuando volvamos a esa misma web en otro momento.

En caso de que el navegador Safari no solicite guardarnos las credenciales introducidas, debemos comprobar desde Ajustes de Safari, que tenemos **activado el Autorrelleno para Nombres y contraseñas**. Además, debemos asegurarnos de que **no estamos utilizando la Navegación privada,** si queremos que nos aplique el autorrelleno y guardado de credenciales.

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**.

Para actualizar el sistema operativo a la versión más reciente que se nos ofrece para nuestro modelo de dispositivo, debemos seguir los siguientes pasos:

1. Conectarnos a una red Wifi de confianza (por ejemplo, nuestra red Wifi de casa)
2. Hacer una copia de seguridad del dispositivo, usando iCloud o el ordenador.
3. Acceder al menú Ajustes > General > Actualización de software.
4. Pulsar "Descargar e instalar", y en caso de disponer de poco espacio en el dispositivo, se nos pedirá desinstalar algunas aplicaciones, lo cual debemos aceptar para poder actualizar el sistema. A continuación, y de manera automática, se volverán a instalar las aplicaciones que se eliminaron antes.

Desde iOS 12 se puede activar las actualizaciones automáticas desde Ajustes > General > Actualización de software > pulsar Actualizaciones automáticas.

Todas las aplicaciones requieren de ciertos permisos para funcionar, pero algunos no son realmente necesarios para cumplir con su finalidad. Por tanto, hay que **limitar los permisos que tienen las aplicaciones**, para lo cual tenemos que denegar aquellos que no consideremos apropiados (acceso al micrófono, contactos, localización,…). Esto lo podemos realizar desde Ajustes > Privacidad > elegir una categoría (Contactos, Cámara, Micrófono,…) y revisar la lista de aplicaciones que tienen acceso, denegando

el permiso a aquellas que no consideremos apropiadas (basta con pulsar en una aplicación de la lista y elegir un nivel de acceso distinto o incluso denegárselo).

Debemos desinstalar todas aquellas aplicaciones que no estemos utilizando, ya que además de ganar espacio, evitamos sus actualizaciones y que tengan permisos de acceso a nuestro dispositivo.

7. Instalación de aplicaciones

Para los dispositivos iOS, las aplicaciones se instalan desde la App Store, donde disponemos de más de un millón de aplicaciones, siendo la mayoría de ellas gratuítas.

Apple desarrolla sus propias aplicaciones, lo que garantiza que las app disponibles en su tienda funcionarán correctamente en el dispositivo, sin afectar al funcionamiento del terminal, ya que solo se publican si han pasado con éxito las pruebas a las que se someten.

Es posible encontrar en Internet aplicaciones para iOS que no han sido desarrolladas por Apple, lo cual supone un peligro para nuestro dispositivo, y que en caso de llegar a instalarlas, deberemos indicar que "Confiamos" en ese desarrollador y asumir las posibles consecuencias que se deriven del uso de esa aplicación.

8. Evitar compras en aplicaciones

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 de 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 seleccionando "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.

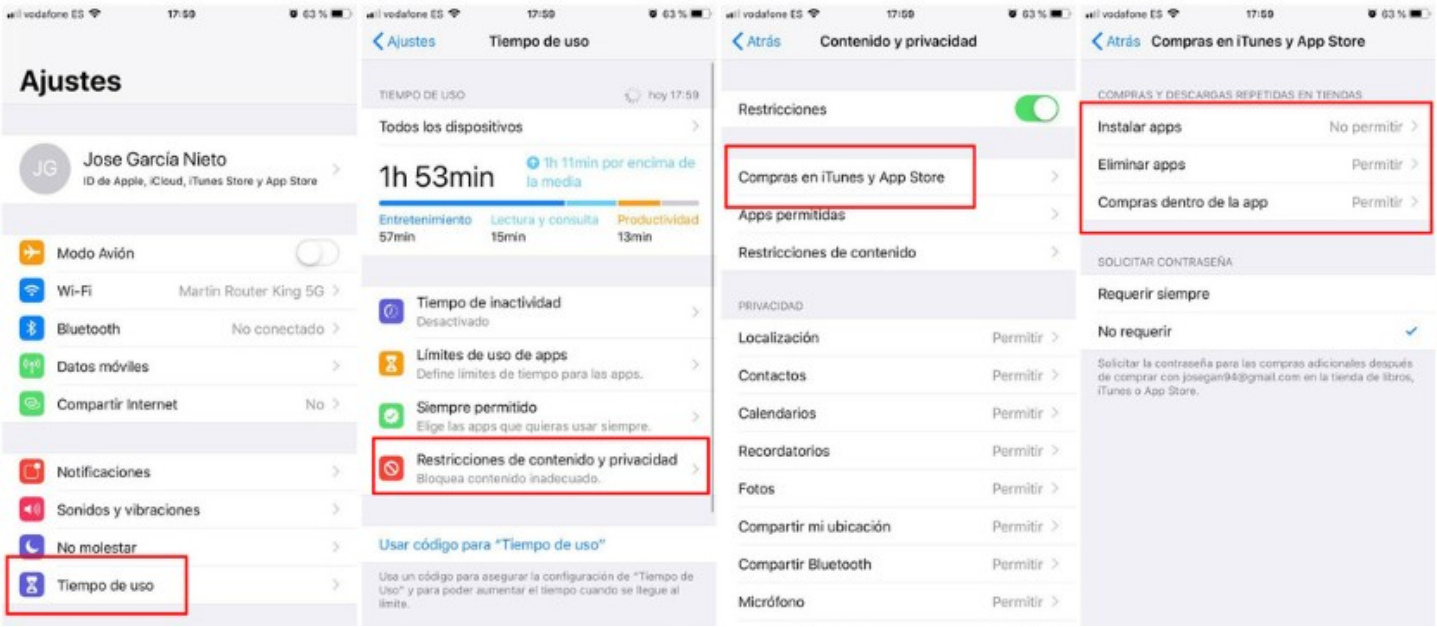
En el caso de la tarjeta de crédito solo aparecerán los 4 últimos dígitos de la misma. Estos datos bancarios están almacenados en los servidores de Apple Store. En el apartado "5.7. Llavero de iCloud" podemos encontrar más información sobre las medidas de seguridad de esta información y la forma de almacenamiento de Apple.

Para **evitar posibles compras automáticas desde alguna aplicación**, debemos configurar correctamente nuestro dispositivo, para evitar que las aplicaciones puedan hacer compras de manera automática, lo cual puede llevarnos a gastos innecesarios.

Se recomienda establecer una contraseña, que deberemos introducir cada vez que nos interese permitir una determinada compra.

Los pasos a realizar son los siguientes:

1. Ajustes
2. Tiempo de uso
3. Restricciones de contenido y privacidad
4. Activar “Restricciones”
5. Compras en iTunes y App Store
6. Compras dentro de la app.
7. Pulsar en “No permitir”
8. En el apartado "Solicitar contraseña", marca la opción "Requerir siempre"



9. Instalar teclados alternativos

iOS permite la instalación de aplicaciones de teclado, que podremos usar cuando estemos en una aplicación que requiera escritura, y que están disponibles en la App Store para su descarga.

Una vez hemos descargado la app de teclado que nos interesa, debemos añadir ese nuevo teclado. Para ello, sigue los siguientes pasos:

Ajustes > General > Teclado >Teclados > Añadir nuevo teclado
Selecciona la app que has instalado.

Cuando estamos usando el teclado, podemos elegir el que nos interesa utilizar, tan solo con mantener pulsado el icono o y seleccionar el teclado que queremos usar.

No obstante, habrá ocasiones en que no podamos utilizar los teclados añadidos desde apps, como es el caso de cuando vamos a escribir contraseñas, dado que por seguridad, no se confía en los teclados de terceros.

En caso de querer eliminar un teclado, basta con desinstalar la app asociada que instalaste, o bien, puedes hacerlo siguiendo estos pasos:

Ajustes > General > Teclado >Teclados > Editar

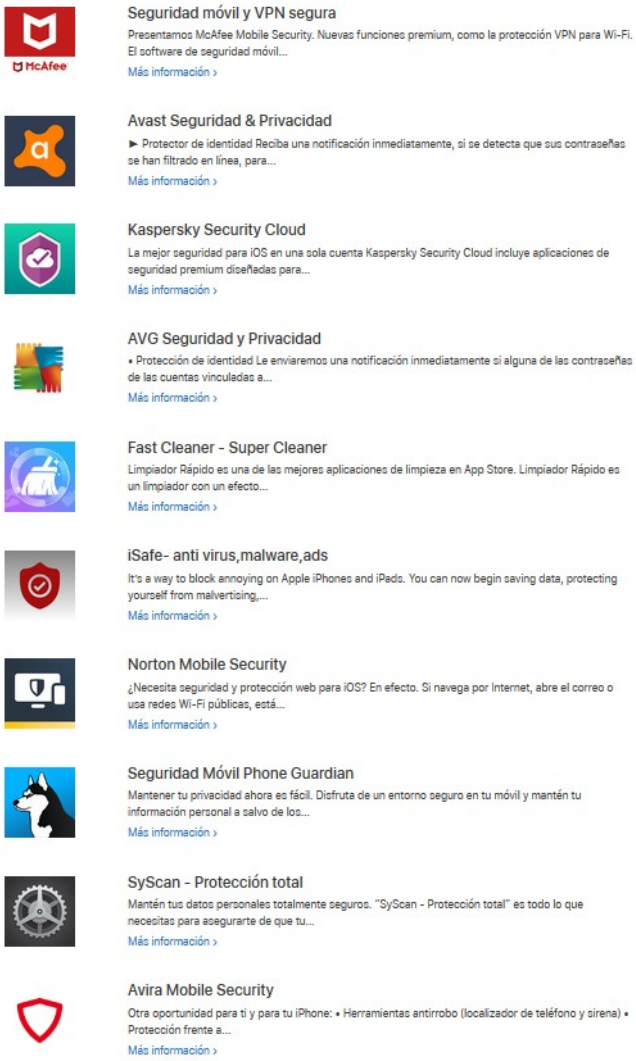
Pulsamos . del teclado que queremos quitar.

10. ¿Antivirus en el móvil?

Dejamos para el final uno de los temas que más dudas causa entre los usuarios de dispositivos móviles: ¿Es iOS lo suficientemente seguro como para no necesitar un antivirus?

El hecho de que las aplicaciones del iPhone no pueden ser accedidas por otras apps (salvo alguna excepción), confirma que las aplicaciones antivirus no podrán escanear las demás aplicaciones que tengamos instaladas, en busca de malware. Pero debemos tener en cuenta, que hay otras formas de infección y medidas de seguridad que podemos encontrar en los antivirus para iOS. Entre estas amenazas que un antivirus podría protegernos están, por ejemplo, el Phishing, o avisarnos de conexiones a redes WiFi no seguras, o incluso ayudarnos a encontrar nuestro dispositivo en caso de pérdida o robo.

Antivirus para iPhone en la App Store:



No obstante, recordemos que no por ello podemos bajar la guardia en el resto de buenas prácticas: no instalar aplicaciones de fuentes poco fiables (generalmente copias ilegales), no abrir ficheros sospechosos (correo, mensajería instantánea, Internet), y tener siempre tanto el sistema operativo como las aplicaciones lo más actualizadas posible.

11. 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