Guía iOS

EL CICLO DE VIDA SEGURO

DE LOS DISPOSITIVOS MÓVILES

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
017
OSI Oficina de Seguridad del Internauta

ÍNDICE

Contenido **Página**

1. Móvil nuevo en la mano, ¿y ahora qué? 3

2. ¡Qué nadie lo use sin tu permiso! 4

3. Conexiones siempre seguras 5

4. Protección contra virus y fraudes 6

5. ¡No pierdas tu información y protégela! 7

6. Personalización - ¡Hazlo tuyo! 8

7. ¡Localiza tu dispositivo! 9

8. Ya pasará a otra vida - Deshacernos del móvil 10

9. Consejos generales 11

10. Enlaces de interés. 12

Licencia de Contenidos

0 INTRODUCCIÓN

El inmenso abanico de posibilidades que ofrecen los smartphones y tablets hace que cada vez estén más extendidos estos dispositivos entre los usuarios. Sin embargo, no están exentos de riesgos, ya que, por ejemplo, se pueden estropear, ser robados o incluso perderse, derivando en la pérdida y control de la información que se tiene almacenada en ellos.

Además, si te detienes unos segundos a pensar, podrás darte cuenta de todo lo que tus dispositivos conocen sobre ti: quiénes son tus contactos, aplicaciones que utilizas, lugares favoritos que frecuentas, páginas web que visitas, credenciales que utilizas para acceder a tus cuentas, fotografías y vídeos que grabas, etc.

Impresiona, ¿verdad?

Ahora bien,

¿Qué pasa si alguien accede a esa información sin tu consentimiento?

¿O si pierdes o te roban el dispositivo?

¿O si se estropea?

No te preocupes, gracias a esta guía aprenderás a usar y configurar tus dispositivos de forma segura, teniendo en cuenta una serie de consideraciones básicas y protegiendo siempre tu información para que, pase lo que pase, no la pierdas ni esté disponible para terceros que intenten consultarla.

Nota: Las distintas configuraciones que encontrarás en esta guía están basadas en la versión 13.4 de iOS.

PRIMEROS PASOS PARA MEJORAR LA SEGURIDAD

1 MÓVIL NUEVO EN LA MANO ¿Y AHORA QUÉ?

Elige un idioma | Conéctate a una red wifi | Configura la contraseña y el sistema de seguridad biométrico | Crea tu cuenta de Apple ID

Elige un idioma:
El primer paso que debes seguir es seleccionar tu idioma y también tu país o región. Seleccionando el país, la configuración de fecha y hora se realizará automáticamente.

Configura la contraseña y el sistema de seguridad biométrico:
Este paso mantendrá tu dispositivo más seguro en caso de que acabe en malas manos. Introduce un código de 6 dígitos y configura los pasos biométricos, huella dactilar o reconocimiento facial, con las instrucciones que te mostrará el dispositivo.

RECONOCIMIENTO BIOMÉTRICO

Conéctate a una red wifi:
Necesitas conexión a Internet para continuar con la configuración. Deberás seleccionar una de las siguientes opciones:

- Elegir una **red wifi**: asegúrate de conectarte a una red wifi segura y con la que estés familiarizado.
- Introducir una **SIM con datos móviles.**

Conéctate y/o crea tu cuenta de Apple ID:
Para que tu iPhone funcione correctamente, debes vincular tu cuenta de Apple ID de la siguiente forma:

- Introduciendo los datos de tus credenciales de una cuenta ya existente.
- Seleccionando la opción **¿No tienes ID de Apple o lo olvidaste?** y creando una cuenta nueva.

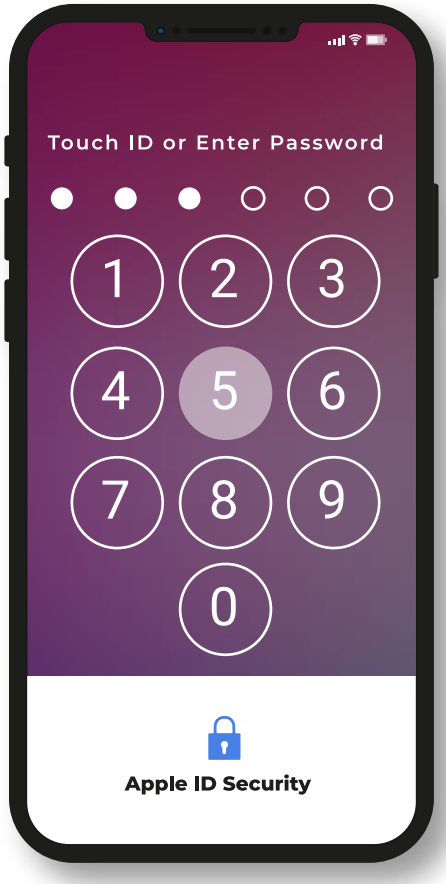
NOTA: Desde iOS11 se puede configurar un dispositivo nuevo iOS usando la información del dispositivo actual gracias a la opción Inicio rápido.

2 ¡QUÉ NADIE LO USE... SIN TU PERMISO!

Establece contraseñas seguras | Doble factor de autenticación

Establece contraseñas seguras:
Dispones de varias medidas de seguridad para bloquear tu dispositivo e impedir que terceras personas puedan hacer uso de él. ¡Gestiona tus contraseñas y resto de medidas de manera segura!

- **Código PIN:** dirígete a **Ajustes > Touch ID/Face ID y código > Activar código.**
- **Huella dactilar:** si tu iPhone dispone de esta funcionalidad, ve a **Ajustes > Touch ID y código**. Si ya estaba establecido un PIN, introdúcelo para poder seleccionar la opción **Añadir una huella** y continuar con las instrucciones del dispositivo.
- **Reconocimiento facial:** si tu iPhone dispone de esta funcionalidad, ve a **Ajustes > Face ID y código** e introduce el código PIN para verificar tu identidad. A continuación, selecciona **Configurar Facial ID** y continúa los pasos indicados.



Doble factor de autenticación:
Además del uso de una contraseña, añade una capa adicional de seguridad a tu cuenta para que si alguien captura o adivina tu clave de acceso, no pueda acceder a ella.
¿Cómo activar la autenticación de doble factor?

Versión iOS 10.3 o superior: dirígete a **Ajustes > [nombre] > Contraseña y seguridad > Activar autenticación de doble factor > Continuar.**

Versión iOS 10.2 o superior: Nos dirigimos a **Ajustes > iCloud > [Apple ID] > Contraseña y seguridad > Activar autenticación de doble factor > Continuar** y seguir los pasos indicados.

3 CONEXIONES SIEMPRE SEGURAS

Configuraciones de redes inalámbricas

Configuraciones de redes inalámbricas

- **Wifi:**
  Mediante esta opción podrás conectarte a redes wifi que se encuentren dentro del rango del dispositivo. Para ello: **En Ajustes > Wi-Fi** verás las redes disponibles.
  Haz clic en una de las redes de la lista. Si se necesita una contraseña, verás el icono del candado.
  La red se guardará y siempre que tu teléfono esté cerca y la **conexión Wi-Fi activada**, se conectará automáticamente.

  Recuerda: evita el uso de redes wifi públicas y, si por alguna razón tienes que hacerlo, no accedas a tus cuentas o servicios para que no se hagan con tus credenciales de acceso.

- **Crear un punto de acceso wifi:**
  Un punto wifi te permitirá compartir tus datos de Internet con quien quieras. Para ello:

  Dirígete a **Ajustes > Punto de acceso personal.**
  Habilita la opción **Permitir a otros conectarse.**
  Entonces, selecciona **Solo Wi-Fi y USB** y crea una contraseña, es aconsejable que modifiques la que viene establecida por defecto.

  Cuando termines de compartir tus datos, apaga esta función para que no sea utilizada por alguien más sin tu autorización.

- **Bluetooth:**
  Para configurar el Bluetooth de tu dispositivo dirígete a:
  Ajustes > Bluetooth enciéndelo y verás una lista de dispositivos disponibles para conectar.
  Te pedirá permiso para emparejar los dispositivos. Puedes darle a aceptar o permitir.

  Una vez hayas terminado de utilizarlo, desactívalo. Así evitarás que terceros puedan llegar a conectarse y robar información personal como fotos o vídeos o transferirnos algún archivo malicioso a nuestro dispositivo.

- **NFC:**
  En los dispositivos de Apple esta función se encuentra siempre activa para ser utilizada por Apple Pay. Es decir, no podrás activarlo y desactivarlo cuando quieras.

  Utilizarás esta tecnología principalmente para realizar pagos sin necesidad de usar tarjetas físicas. Infórmate sobre cómo hacerlos con NFC de manera segura.

  Una vez que hayas terminado, recuerda cerrar la aplicación. Un tercero podría realizar algún cargo a tu tarjeta si no tenemos cuidado.

4 PROTECCIÓN CONTRA VIRUS Y FRAUDES

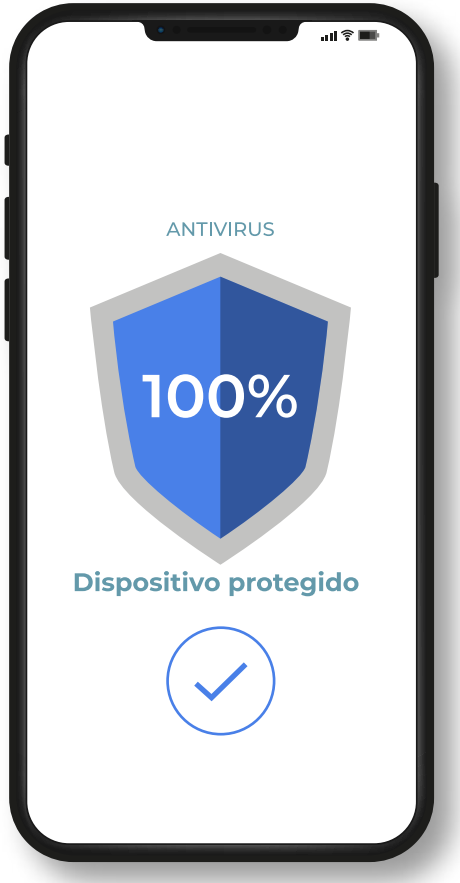
Antivirus | Actualización de software

Antivirus:

Tu dispositivo no está exento de riesgos de infectarse por algún virus a través de una app o al descargarte un archivo infectado. Para protegerlo:

- Selecciona un antivirus directamente desde la tienda oficial App Store, asegurándote que previamente lees las reseñas de este.
- Haz clic en **Instalar** y lee la ventana con los permisos de aplicación que aparecerá. A continuación, pulsa en **Aceptar**.
- Abre la app y configúrala para mantener tu dispositivo iOS libre de virus

Descarga Disponible
App Store



Actualización de *software*:

Durante la vida útil del sistema operativo, los desarrolladores van descubriendo errores y fallos de seguridad que necesitan ser solucionados. Sin actualizaciones, tu dispositivo estaría más expuesto y vulnerable frente a los ataques de los ciberdelincuentes.

- Si no has recibido la notificación de que existe una actualización nueva o quieres revisar si estás actualizado o no, dirígete a **Ajustes > General > Actualización de software > Descargar e instalar**, te solicitará tu **código de desbloqueo** y se descargará la nueva actualización.

Otras herramientas de protección:

Además de con antivirus, blinda el acceso a tu información con aplicaciones de bloqueo de apps, gestores de contraseñas, función de verificación en dos pasos o que protegen tu privacidad, entre otras.

5 ¡NO PIERDAS TU INFORMACIÓN Y PROTÉGELA!

Copias de seguridad | Cifrado

Nuestro dispositivo móvil no es solo una extensión de nosotros, también se convierte en una unidad de almacenamiento de toda nuestra vida. Imagina que un día lo perdieses...

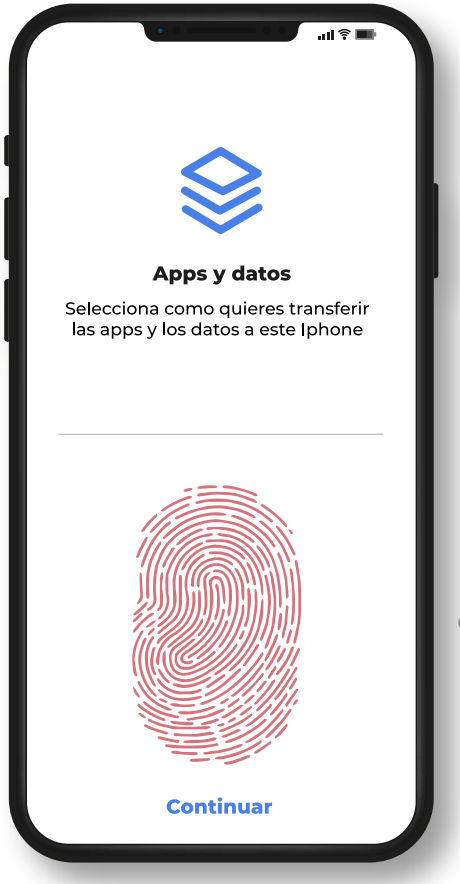
¿Podrías recuperar toda la información almacenada en él?

Para minimizar riesgos, lo mejor es hacer copias de seguridad:

Copias de seguridad en la nube de Apple:
iOS tiene su propio sistema de copias de seguridad en la nube (iCloud). Para realizar las copias de seguridad:

- Dirígete a **Ajustes > [nombre] > [seleccionar el dispositivo]** (en caso de tener varios dispositivos asociados a la cuenta)**> Copia en iCloud > Realizar copia de seguridad ahora**. Además, si habilitas la opción Copia en iCloud, se realizará una copia automática cuando el dispositivo esté enchufado a la corriente, bloqueado y conectado a una red wifi.

iCloud



Cifrado:
No te olvides del cifrado del teléfono y su información. Los dispositivos de Apple (iPhone o iPad) **ya cifran su contenido por defecto una vez implementado el código de desbloqueo.** Cualquier mecanismo de desbloqueo implementado (contraseña, huella dactilar o reconocimiento facial) activará el cifrado del dispositivo automáticamente.

6 PERSONALIZACIÓN ¡HAZLO TUYO!

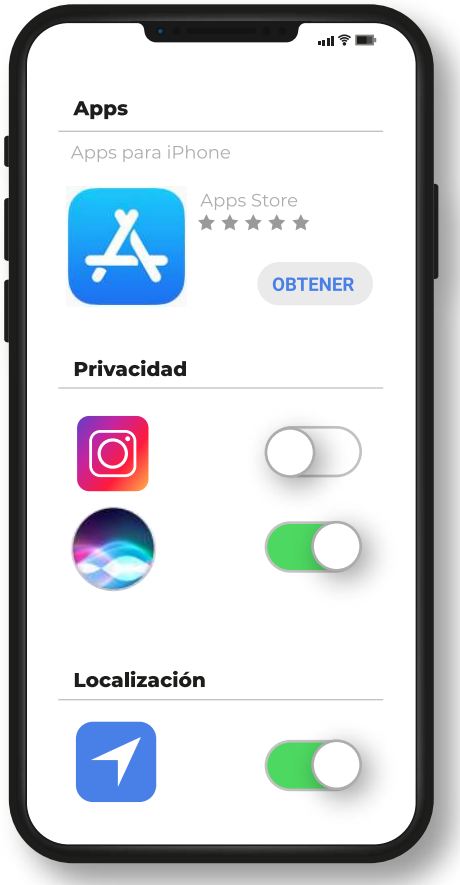
Instalación de apps desde App Store | Permisos de apps | Geolocalización

Juegos, música, vídeos y muchísimos más tipos de apps están a tu disposición para instalar en tu dispositivo móvil. En cuestión de segundos tendrás instaladas todas las apps que quieras, pero ¡ojo!, las apps se instalan en tu dispositivo y acceden a determinadas funcionalidades a través de permisos. Si la app no es del todo fiable puede hacer un mal uso de estos permisos y poner en riesgo tu seguridad y privacidad.

Instalación de apps desde App Store:
Para instalar apps en tu dispositivo Apple, debes dirigirte a la tienda oficial de App Store que ya viene instalada por defecto.

- Busca la app que quieras instalar y haz clic en **Obtener**. No te olvides de revisar los comentarios y valoración de otros usuarios. Aunque esté en la tienda oficial, es importante informarse bien sobre la app.

App Store



Permisos de apps:
Cuando una app pide permisos, está solicitando acceso a alguna funcionalidad de tu dispositivo. Revisa con mucha atención si tiene sentido que pida un permiso determinado y, si quieres revisar o administrar los permisos de las apps ya instaladas:

- Ve a **Ajustes**. Al final de la pantalla encontrarás la lista de apps instaladas.
- A continuación, selecciona la app cuyos permisos quieras administrar y podrás activar y desactivar los permisos que consideres.

Geolocalización:
La función de geolocalización permite obtener información basada en la ubicación del dispositivo y ofrece predicciones sobre tus desplazamientos, restaurantes cercanos, etc. Aunque puede resultar muy útil, puedes sentir que tu privacidad está siendo invadida ya que estos datos se comparten con Apple.

- Para desactivarla ve a **Ajustes > Privacidad > Localización** y selecciona la app que quieres gestionar.

7 ¡LOCALIZA TU DISPOSITIVO!

Buscar mi dispositivo

Supón que has perdido tu dispositivo. No te preocupes, existe una función para localizarlo esté donde esté.

- Configura la opción que te permite encontrar el dispositivo.

  En Ajustes > [nombre] > Buscar, activa la función **Buscar mi iPhone y Enviar última ubicación.** También se puede activar la opción **Encontrar sin conexión** para encontrar el dispositivo cuando no esté conectado a una red wifi o no tenga acceso a datos móviles.
  Otras formas que también te pueden ayudar a encontrar tu móvil será tener habilitadas las siguientes opciones:

- **Compartir mi ubicación**, que se puede habilitar desde la opción Buscar, para compartir tu ubicación con familiares y amigos.

- **En Familia,** que se puede habilitar en los ajustes del iPhone, permitirá que cualquier persona que esté dentro de este grupo pueda ayudarte a localizar el móvil.

- En el caso de querer encontrar tu iPhone y tener habilitada la función Buscar mi iPhone, será tan fácil como acceder a http://icloud.com/find e identificarte con las credenciales de tu cuenta. Podrás ver la localización de todos los dispositivos donde hayas activado esta opción.

  Esta función es muy útil, pero no olvides proteger tu cuenta adecuadamente, con una contraseña robusta y activando la verificación en dos pasos, para evitar que otra persona acceda a ella y localice la ubicación de tu dispositivo, y la tuya.

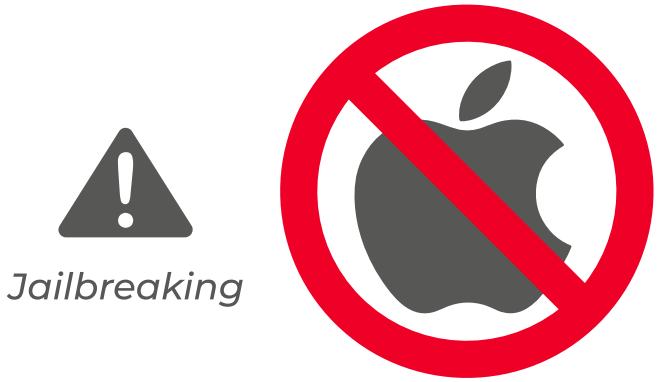
8 YA PASARÁ A OTRA VIDA DESHACERNOS DEL MÓVIL

Borrado seguro

Borrado seguro:
Si tu dispositivo se ha quedado anticuado y quieres deshacerte de él por uno nuevo, ¡no lo tires sin más! Aunque creas haber eliminado todo rastro de tu información, es posible que aún pueda recuperarse si cae en malas manos. Para hacer un borrado seguro de toda tu información personal, deberás hacer lo siguiente:

- Ve a **Ajustes > General > Restablecer** y pulsar sobre **Borrar contenidos y ajustes (recuerda realizar una copia de seguridad antes)** y volverás a disponer de tu dispositivo como si fuera nuevo.

Si al dispositivo se le había hecho un jailbreaking, la opción de restablecer podría no funcionar correctamente. En ese caso tendrás que acudir a un técnico especializado.
Se conoce como ***jailbreaking*** al proceso de eliminar las limitaciones impuestas por Apple en un dispositivo con iOS. Esta práctica no es recomendable para usuarios no técnicos.



PRIMEROS PASOS PARA MEJORAR LA SEGURIDAD

9 CONSEJOS GENERALES

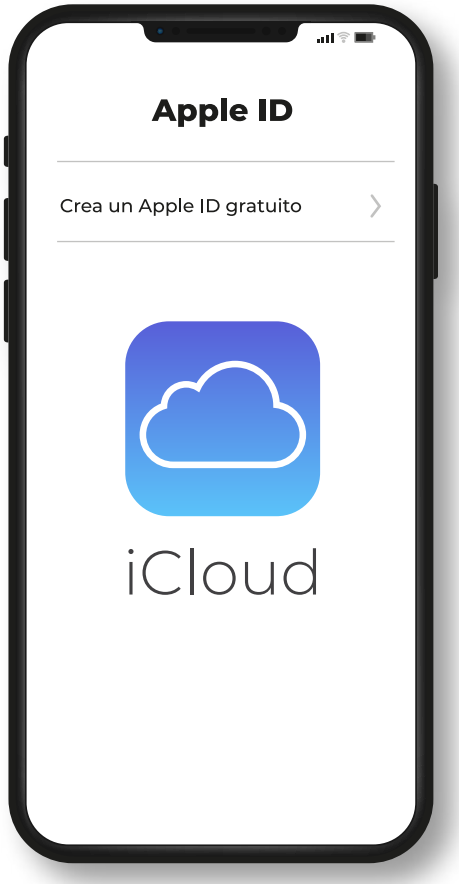
1. Vincula tu dispositivo móvil a una cuenta de iCloud

2. Utiliza una clave de bloqueo para tu dispositivo. Si no es biométrica, recuerda usar una contraseña robusta.

3. Activa el sistema de actualizaciones automáticas de tu dispositivo y aplicaciones, pues con esto se corrigen los defectos en seguridad que puedan tener.

4. Usa aplicaciones de seguridad que añadan una capa extra de seguridad a tu dispositivo, como por ejemplo un antivirus.

5. Protege tu información mediante copias de seguridad. De este modo tendrás una copia de respaldo en caso de pérdida o borrado de tu dispositivo.



6. Desactiva las conexiones inalámbricas una vez hayas terminado de usarlas (wifi, Bluetooth, NFC).

7. Cuando instales aplicaciones, revisa siempre quién es el desarrollador así como las opiniones y valoraciones del resto de usuarios. ¡Y acuérdate de eliminar las que ya no uses!

App Store

8. Otorga los permisos a las apps que sean imprescindibles para su correcto funcionamiento y revisa siempre que sean coherentes con la funcionalidad de la app.

9. Evita prácticas de riesgo con el *jailbraiking* en iOS.

10. Si vas a deshacerte de tu móvil, asegúrate de borrar toda la información que contiene para no dejar rastro.

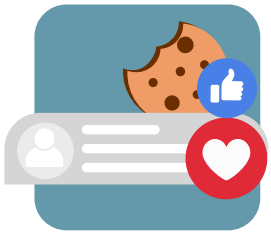
11. Apóyate en herramientas de control parental si el dispositivo lo va a utilizar un menor.

18+

10 ENLACES DE INTERÉS

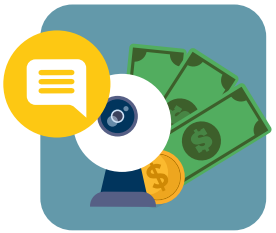
Dispositivos móviles

La 2ª vida de nuestros dispositivos



¿Cuánto valen mis datos en la Red?

¡Contraseñas seguras!



Ingeniería social: que no te engañen

Puesta a punto para el nuevo curso

No te pierdas ningún detalle de la guía, accediendo a la versión digital con este QR.

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017
OSI Oficina de Seguridad del Internauta