



INSTITUTO NACIONAL DE CIBERSEGURIDAD

Taller “Aprende a utilizar las herramientas básicas de protección de disp. móviles”



GOBIERNO
DE ESPAÑA

VICEPRESIDENCIA
PRIMERA DEL GOBIERNO

MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL



TU AYUDA EN
CIBERSEGURIDAD




Oficina
de Seguridad
del Internauta



- ❖ 1. Los dispositivos móviles también necesitan protección
- ❖ 2. Antivirus
- ❖ 3. Protección al descargar software y aplicaciones
- ❖ 4. Aplicaciones antirrobo
- ❖ 5. Bloqueo de aplicaciones.
- ❖ 6. Gestores de contraseñas
- ❖ 7. Aplicaciones de verificación en dos pasos o factor múltiple de autenticación
- ❖ 8. Aplicaciones de privacidad y navegación por Internet de forma segura
- ❖ 9. Cifrado del dispositivo y aplicaciones
- ❖ 10. CONAN mobile, análisis del estado de seguridad del dispositivo

INTRODUCCIÓN

Nuestros dispositivos móviles almacenan una enorme cantidad de información sobre nosotros. Esta información corre el riesgo de ser sustraída si no está debidamente protegida.

Para evitarlo, vamos a ver varias **aplicaciones y herramientas de protección** que nos ayudarán a blindar estos dispositivos y la información almacenada en ellos.



1. LOS DISPOSITIVOS MÓVILES TAMBIÉN NECESITAN PROTECCIÓN

Cuando hablamos de ciberseguridad y protección de dispositivos, la mayoría de usuarios piensa en sus ordenadores. Sin embargo, los dispositivos móviles como *smartphones* o *tablets* también necesitan una **capa extra de protección**, ya que:

Robo de dispositivos

Navegación segura



Infección por *malware*

Descarga de aplicaciones y *software*

2. ANTIVIRUS

Su función principal es la de **detectar y eliminar virus, troyanos y otras clases de *malware*, evitando el robo de información y protegiéndonos de todo tipo de amenazas** que traten de acceder a nuestro sistema:

1. Analizan nuestro sistema

2. Aíslan la amenaza

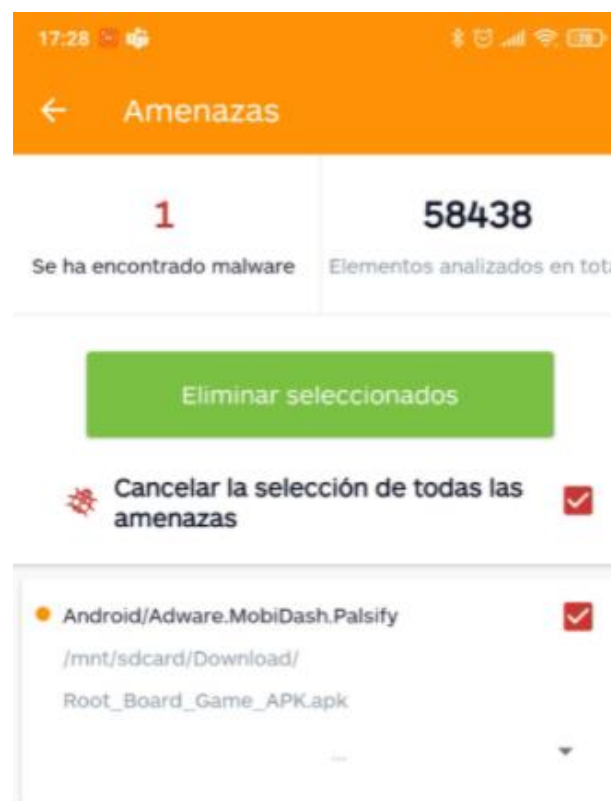
3. Eliminan la amenaza



2. ANTIVIRUS

A continuación, vamos a ver los pasos a seguir para **descargar, instalar y analizar nuestro dispositivo** con uno de estos antivirus, usaremos como ejemplo **Malwarebytes**:

1. Acceder a la **Play Store** o **App Store**.
2. Buscar el **antivirus Malwarebytes**.
3. Instalar y **analizar nuestro dispositivo**.



3. PROTECCIÓN AL DESCARGAR SOFTWARE Y APLICACIONES

Las aplicaciones son programas informáticos que añaden una gran cantidad de funciones a nuestros dispositivos, aunque si no tenemos cuidado, podemos terminar descargando alguna **app maliciosa** que tenga como objetivo infectar nuestros dispositivos o aprovecharse de los permisos que les concedemos al instalar.



3. PROTECCIÓN AL DESCARGAR SOFTWARE Y APLICACIONES. GOOGLE PROTECT

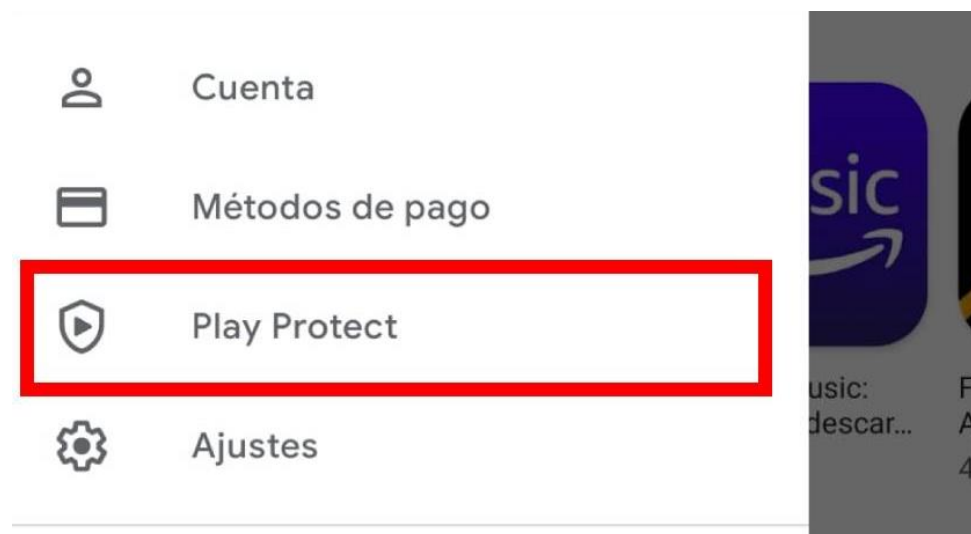
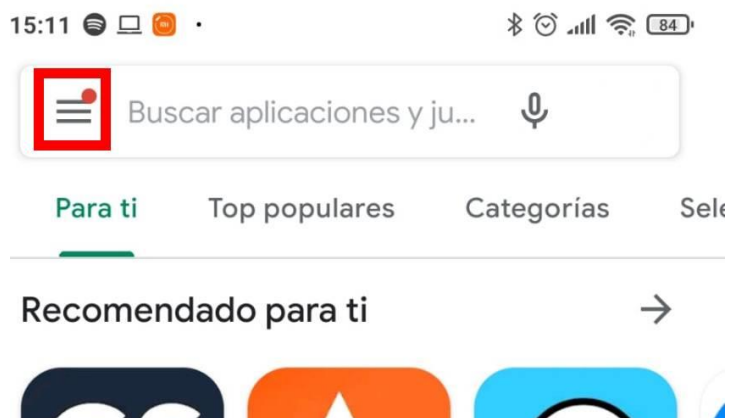
Nuestros dispositivos móviles, como *smartphones* o *tablets*, con el sistema Android, disponen de una herramienta de protección contra las aplicaciones dañinas, conocida como [Google Play Protect](#).



3. PROTECCIÓN AL DESCARGAR SOFTWARE Y APLICACIONES. GOOGLE PROTECT

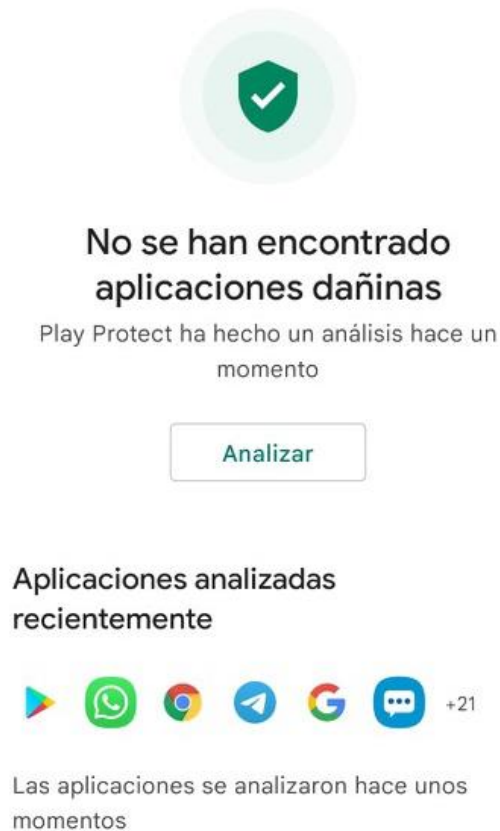
Para acceder a esta herramienta y comprobar que está activa y protegiéndonos de estas amenazas, deberemos:

1. Acceder a la app de **Play Store** y pulsar sobre el **icono del menú**.
2. Luego, abriremos la opción **Play protect**.

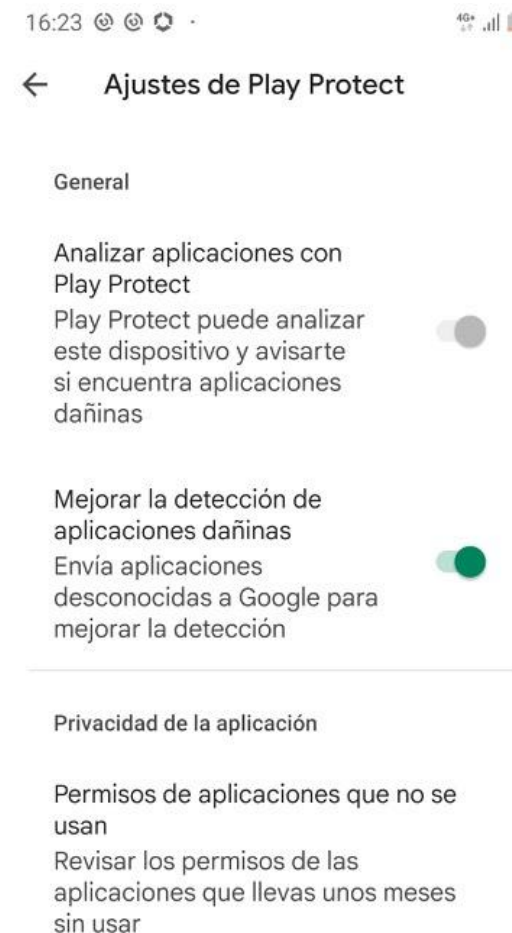


3. PROTECCIÓN AL DESCARGAR SOFTWARE Y APLICACIONES. GOOGLE PLAY PROTECT

3. Podemos forzar un análisis en **Analizar**.



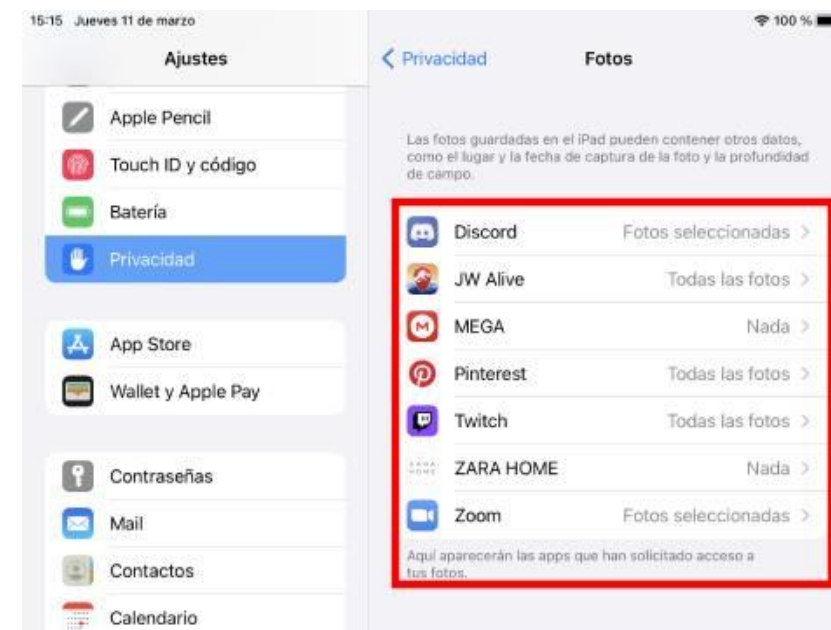
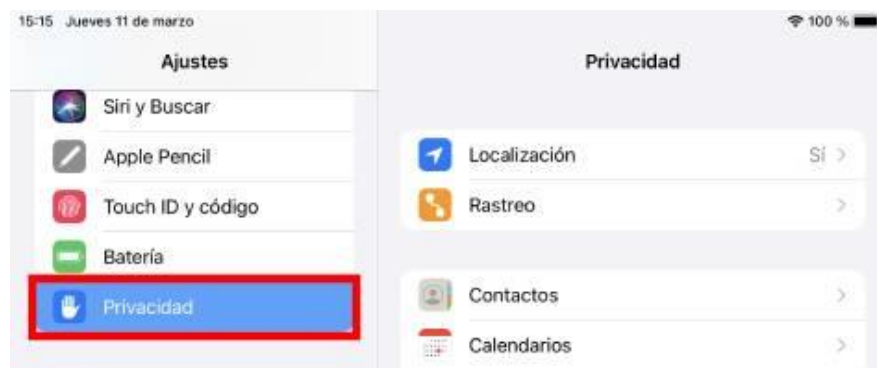
4. Finalmente, debemos activar las opciones de **Analizar aplicaciones con Play Protect** y **Mejorar la detección de aplicaciones dañinas**.



3. PROTECCIÓN AL DESCARGAR SOFTWARE Y APLICACIONES. MECANISMO DE SEGURIDAD IOS

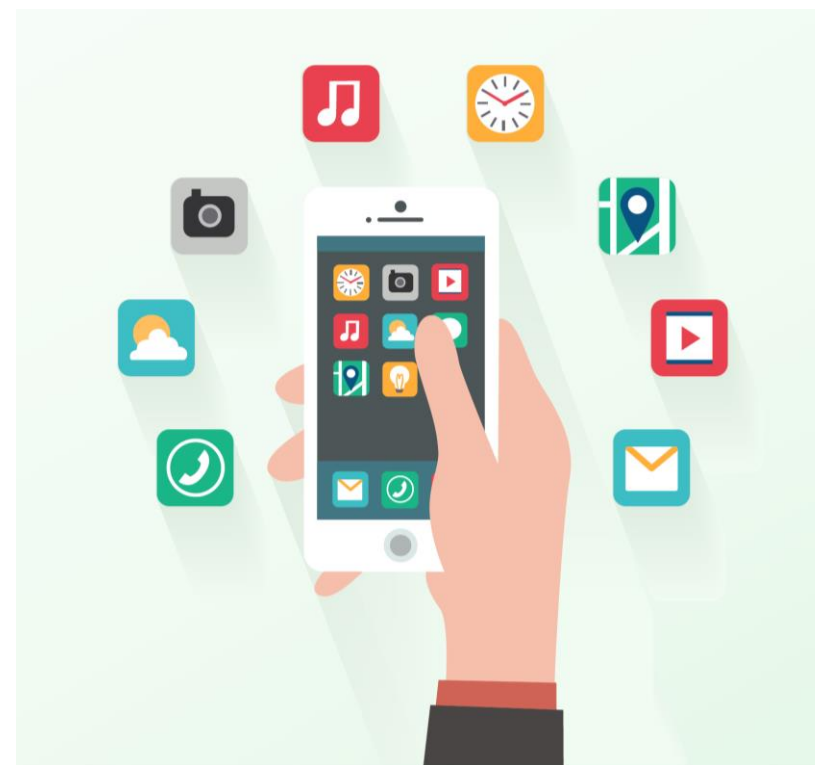
Los dispositivos como el iPhone o el iPad disponen de herramientas de protección preinstaladas que nos ayudan a prevenir la instalación de aplicaciones o programas maliciosos.

1. Para gestionar los permisos iremos a **Ajustes > Privacidad**.
2. Luego, seleccionaremos una categoría, como **Contactos o Fotos**.



3. PROTECCIÓN AL DESCARGAR SOFTWARE Y APLICACIONES

- ❖ Descargar desde las **tiendas oficiales**.
- ❖ Revisar **desarrollador, descripción, número de descargas, valoración y comentarios**.
- ❖ Comprobar **permisos solicitados**.
- ❖ Por protección, es recomendable **revisar los permisos frecuentemente**.
- ❖ Mantener las **apps actualizadas**.
- ❖ Periódicamente, **limpieza de apps**.



4. APLICACIONES ANTIRROBO

Aunque seamos muy cuidadosos y **tomemos todas las precauciones posibles**, puede que llegue el día donde perdamos o nos **roben nuestro dispositivo móvil**.

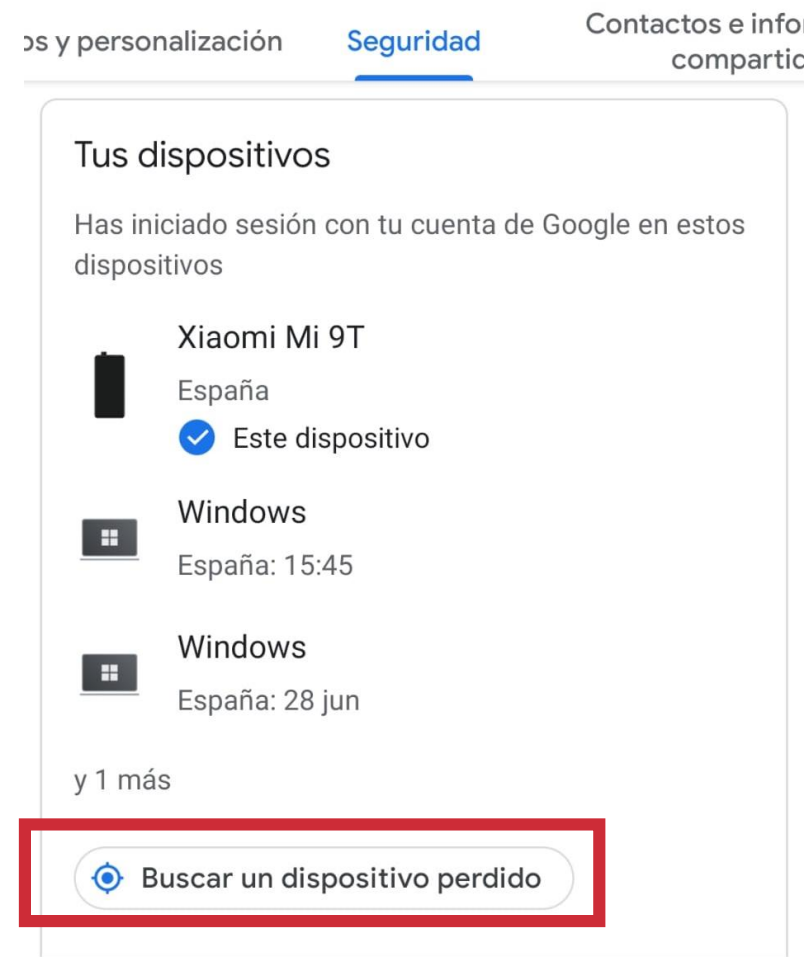


- ❖ Geolocalizar nuestro dispositivo.
- ❖ Enviar una notificación o alerta.
- ❖ Bloquear el acceso.
- ❖ Eliminar toda la información almacenada.

4. APLICACIONES ANTIRROBO

En el caso de **Android** , disponemos de la opción **Administrador de dispositivos**:

- ❖ Iremos a **Ajustes > Estado de seguridad / Seguridad y ubicación o Google > Seguridad**.
- ❖ Nos aseguraremos de que la función [Encontrar dispositivo](#) esté activada y actualizada.
- ❖ Podemos comprobar que la herramienta funciona desde: <https://android.com/find>.



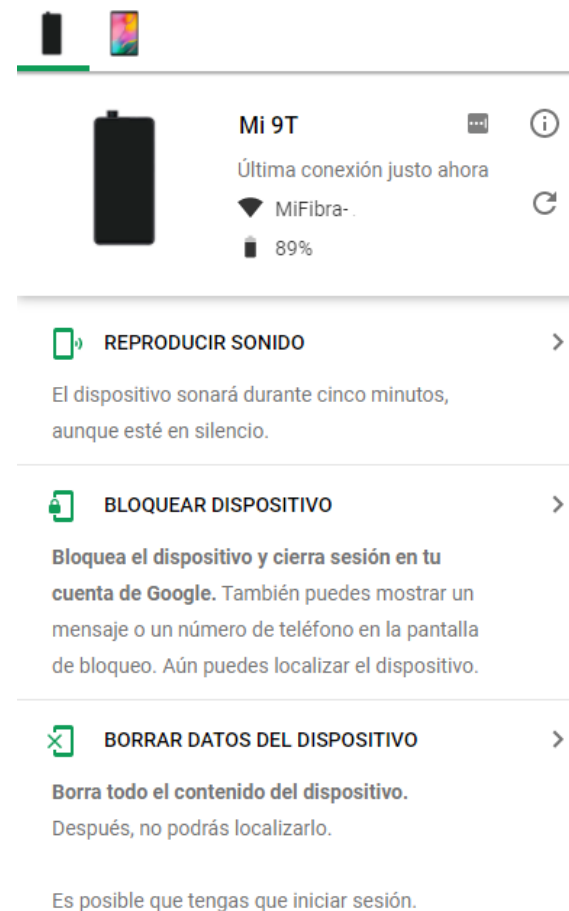
4. APLICACIONES ANTIRROBO

En el caso de **Android**:

1. Obtendremos **información** (ubicación, conexión a Internet...).

2. **Acciones adicionales:**

1. Reproducir sonido.
2. Bloquear dispositivo.
3. Borrar datos del dispositivo.



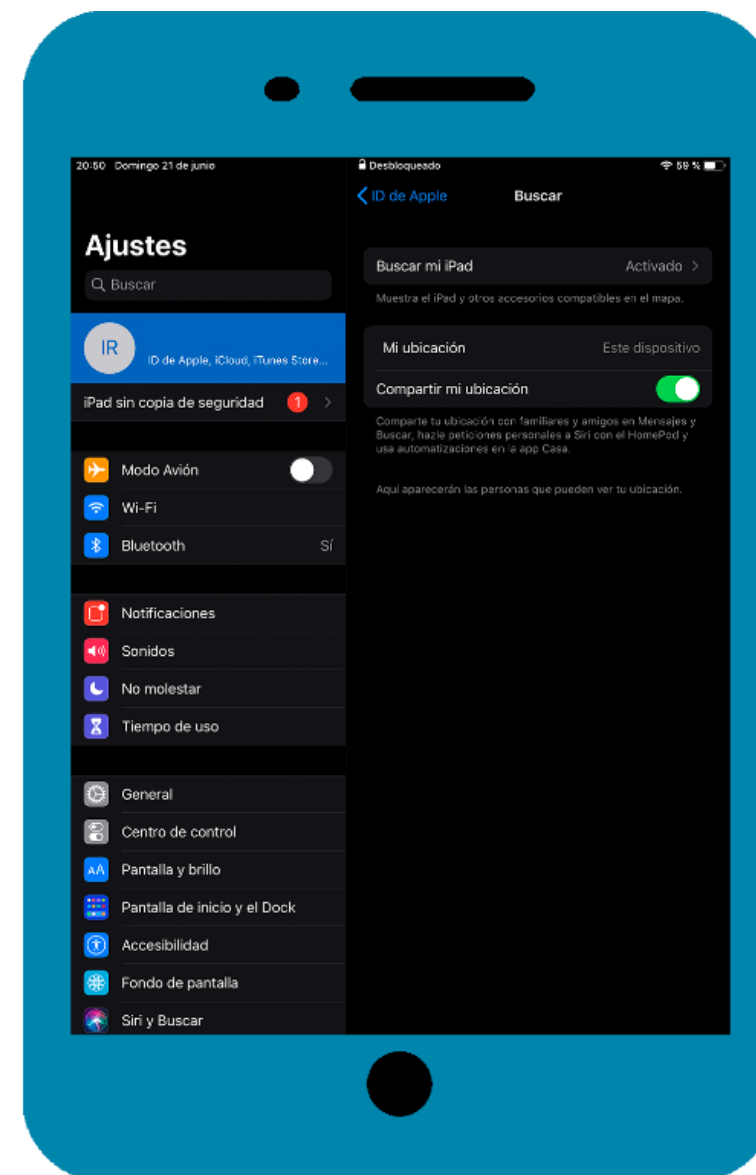
4. APLICACIONES ANTIRROBO

En el caso de **iOS** podemos utilizar la función **Buscar mi iPhone/iPad** :

1. Accederemos a **Ajustes > [nombre] > Buscar > Buscar mi iPhone/iPad** y activaremos todas las opciones.

1. Red de Buscar
2. Enviar mi última ubicación.

Podemos probar esta función ingresando con nuestra cuenta de Apple en: <https://www.icloud.com/find>.



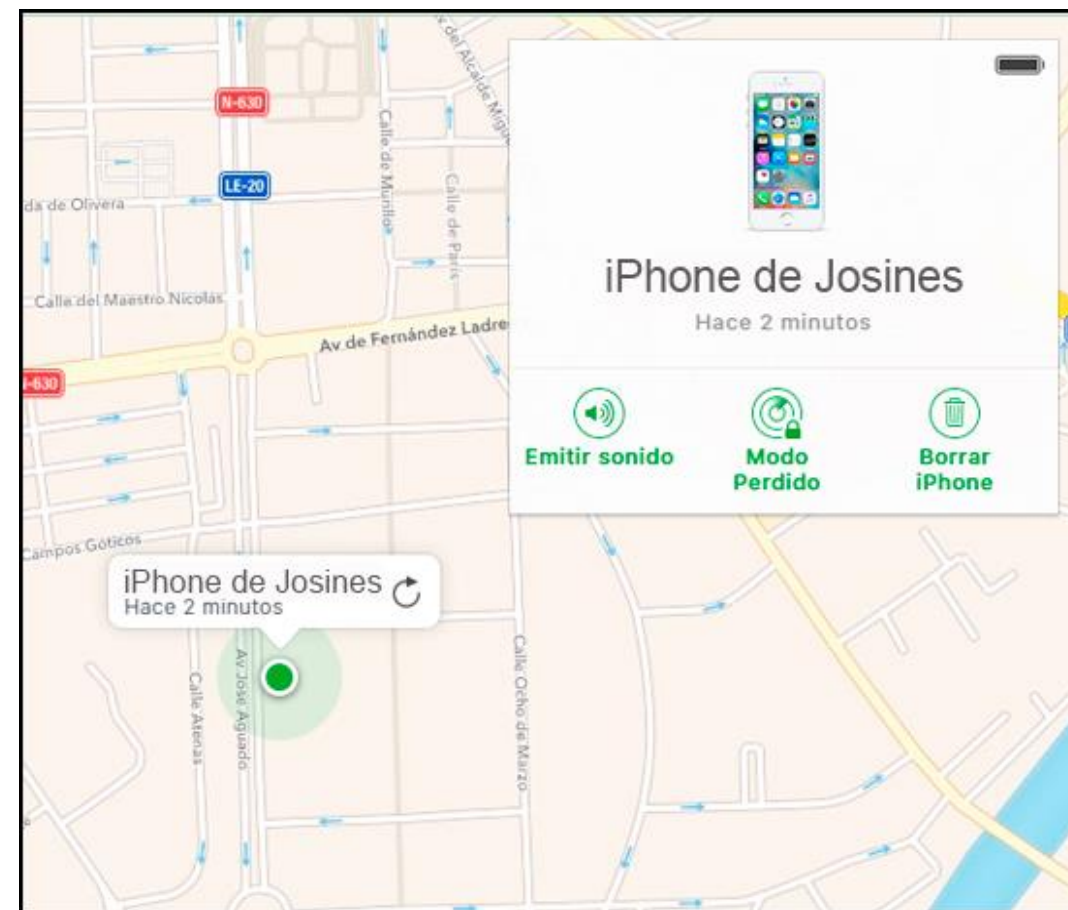
4. APLICACIONES ANTIRROBO

En el caso de **iOS**:



Buscar mi iPhone

1. Entraremos en la app **Buscar mi iPhone**.
2. Seleccionaremos el dispositivo y encontraremos varias **acciones**:
 1. Reproducir sonido.
 2. Modo Perdido.
 3. Borrar iPhone.



5. BLOQUEO DE APLICACIONES

Este tipo de aplicaciones **mejoran la protección de nuestra información más personal**, evitando el acceso no autorizado de terceras personas a nuestro dispositivo móvil y/o a las apps en las que manejamos información sensible:

Contraseña

Código PIN

Patrón

Sensor biométrico



5. BLOQUEO DE APLICACIONES

Desde dispositivos **Android**:

1. Iremos a **Ajustes > Seguridad y privacidad > Bloqueo de aplicaciones**.
2. Luego, especificaremos la **clave o patrón**.
3. Finalmente, **seleccionaremos las aplicaciones a proteger**.

16:20



← Bloqueo de aplicaciones



🔍 Buscar entre 108 aplicaciones

105 aplicaciones no bloqueadas



Grabadora de pantalla

Aplicaciones del sistema



Amazon compras

Aplicaciones instaladas



YouTube

Aplicaciones del sistema



5. BLOQUEO DE APLICACIONES

En dispositivos iOS:

1. Iremos a **Ajustes > Tiempo de uso** y pulsaremos en **Usar código para “Tiempo de uso”**.
2. Pulsaremos en **Ver toda la actividad** y, tras seleccionar una app, en **Añadir límite**.
3. Especificaremos un **tiempo máximo de uso** (1min).



6. GESTORES DE CONTRASEÑAS

Los gestores de contraseñas son aplicaciones que sirven para **almacenar todas nuestras credenciales** (usuarios, contraseñas, sitios web a los que corresponden, etc.) en una **base de datos cifrada** mediante una contraseña “maestra”.

Verificación en dos pasos

Multidispositivo

Generación de contraseñas



Integración con extensiones de navegadores

Alertas de vulnerabilidad

Cuentas temporales

6. GESTORES DE CONTRASEÑAS

En el mercado existe una gran variedad de aplicaciones con esta función:

1 Descargar la aplicación y crear una cuenta

2 Agregar nuevos elementos (cuentas)

3 Disfrutar de funciones adicionales



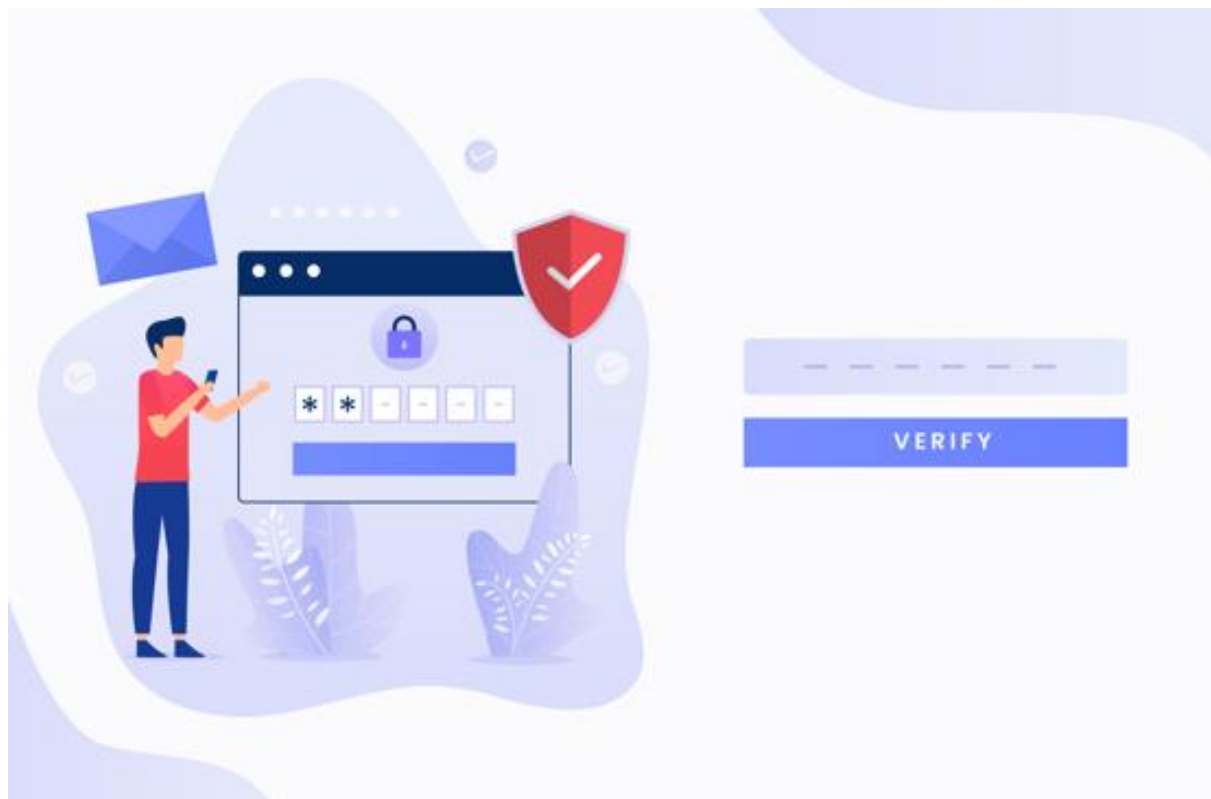
7. APLICACIONES DE VERIFICACIÓN EN DOS PASOS O FACTOR MÚLTIPLE DE AUTENTICACIÓN

La **verificación en dos pasos** es una medida de protección adicional a la contraseña con la que podemos dificultar que alguien sin autorización acceda a nuestra cuenta:

Usuario



Contraseña



Código

7. APLICACIONES DE VERIFICACIÓN EN DOS PASOS O FACTOR MÚLTIPLE DE AUTENTICACIÓN

Muchos son los servicios que ya cuentan con un sistema de verificación en dos pasos propio. Otros no disponen de esta capa extra de seguridad, sin embargo, también podemos utilizar **aplicaciones de grandes empresas como Google y su “Google Authenticator” o Microsoft con “Microsoft Authenticator”**:

<https://youtu.be/oFzKEogQEsI>



ACTIVIDAD 1



La protección de nuestras cuentas depende, en gran medida, de aplicaciones y configuraciones que podemos gestionar desde nuestro dispositivo móvil. Por eso, **vamos a instalar una app de gestión de contraseñas y de verificación en dos pasos** (pueden ser las explicadas durante el taller) y utilizarlas para proteger alguna de nuestras cuentas que permitan la verificación en dos pasos.

Sigue los pasos indicados en el taller y en los recursos publicados en la OSI y asegúrate que tus cuentas estén debidamente protegidas.

8. APLICACIONES DE PRIVACIDAD Y NAVEGACIÓN POR INTERNET DE FORMA SEGURA



GOBIERNO
DE ESPAÑA

VICEPRESIDENCIA
PRIMERA DEL GOBIERNO
MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL



INSTITUTO NACIONAL DE CIBERSEGURIDAD

Navegar por Internet también puede ser una amenaza si no contamos con las **herramientas de protección adecuadas** y **somos conscientes de los peligros y amenazas que hay en la Red.**

Utilizar un navegador
seguro y actualizado



Activar el modo
incógnito



Instalar extensiones o
plugins



TU AYUDA EN
CIBERSEGURIDAD
incibe

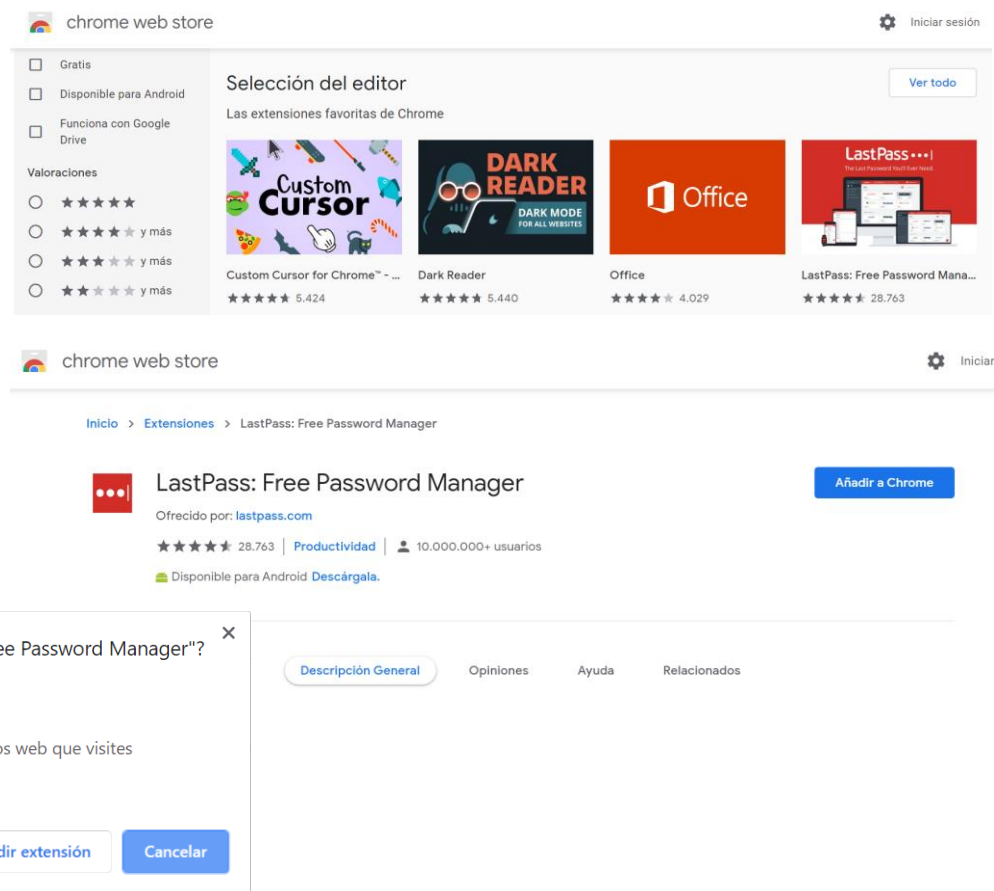


Oficina
de Seguridad
del Internauta

8. APLICACIONES DE PRIVACIDAD Y NAVEGACIÓN POR INTERNET DE FORMA SEGURA

Para instalar extensiones en Google Chrome:

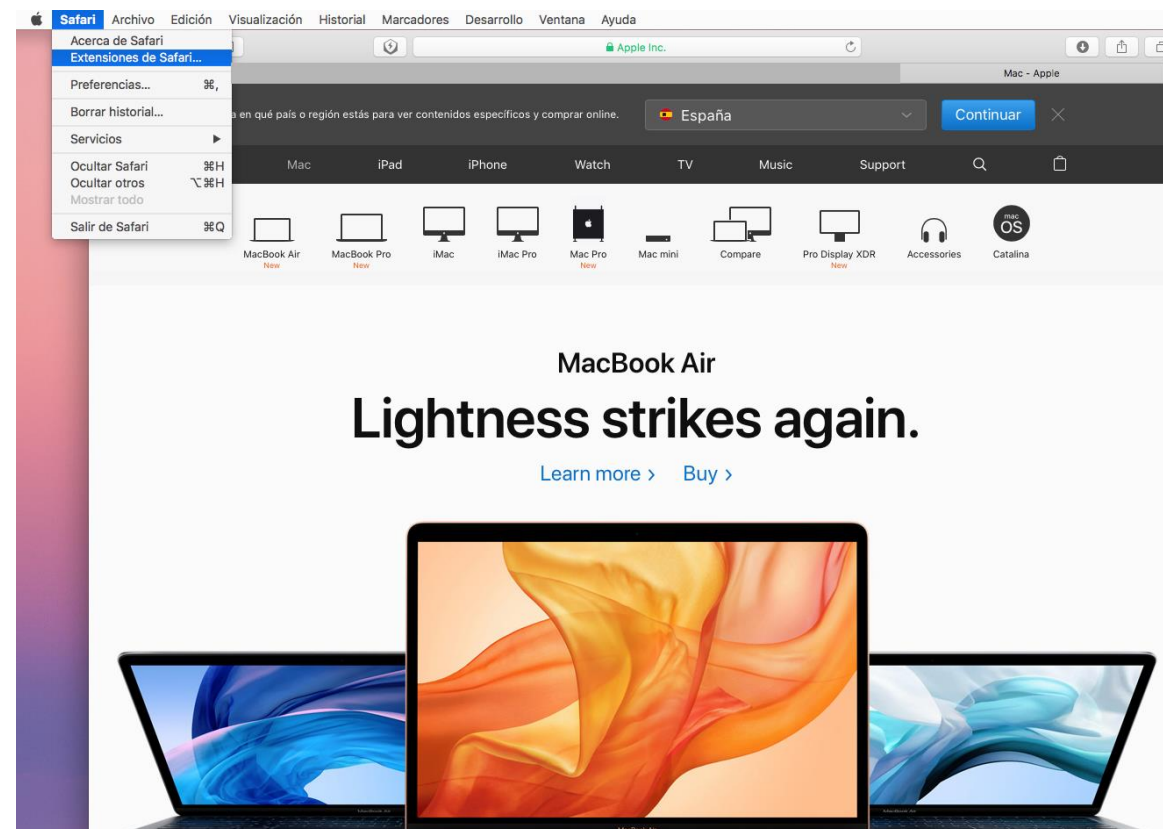
1. Abriremos la **Chrome Web Store** > **Extensiones**.
2. Buscaremos la extensión que queramos.
3. Comprobaremos la información.
4. Pulsaremos en **Añadir a Chrome**.
5. Haremos clic en **Agregar extensión**.



8. APLICACIONES DE PRIVACIDAD Y NAVEGACIÓN POR INTERNET DE FORMA SEGURA

Para instalar extensiones en Safari:

1. Iremos a **Safari > Extensiones de Safari**.
2. Pulsaremos en la extensión que queramos, ingresaremos credenciales y la instalaremos.



9. CIFRADO DEL DISPOSITIVO Y APLICACIONES

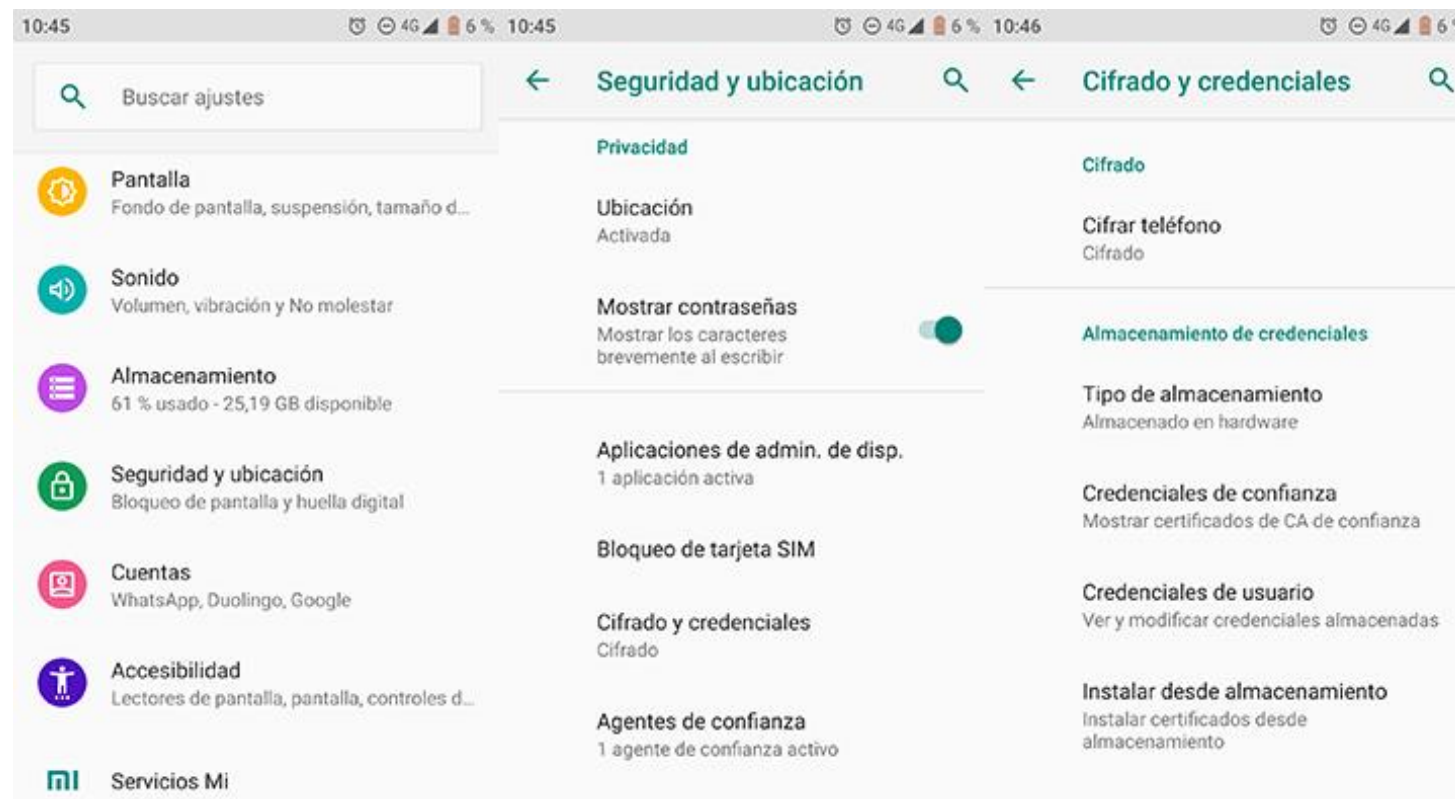
El cifrado de nuestro dispositivo consiste en **hacer que la información que contiene no sea accesible para aquellos que no están autorizados para leerla, modificarla o borrarla.**



9. CIFRADO DEL DISPOSITIVO Y APLICACIONES

En el caso de **Android**:

1. Iremos a **Ajustes > Seguridad y ubicación**.
2. Pulsaremos en **Cifrado y credenciales > Cifrar teléfono**.
3. Luego, seguiremos los pasos para **crear una contraseña o PIN**.



9. CIFRADO DEL DISPOSITIVO Y APLICACIONES

En el caso de **iOS**, el dispositivo ya estará cifrado por defecto y no tendremos que hacer nada.



10. CONAN MOBILE, ANÁLISIS DEL ESTADO DE SEGURIDAD DEL DISPOSITIVO

CONAN mobile es la aplicación para dispositivos Android que permite **conocer el estado de seguridad de nuestros dispositivos, además de las siguientes funcionalidades:**

Análisis de la configuración del dispositivo

Clasificación aplicaciones por permisos



CONAN
m o b i l e

Servicio proactivo

Análisis de aplicaciones

Consejos OSI

10. CONAN MOBILE, ANÁLISIS DEL ESTADO DE SEGURIDAD DEL DISPOSITIVO

Para su instalación, seguiremos estos pasos:

1. Accederemos a la **Play Store** y buscaremos **CONAN mobile**.
2. Tras instalarla, pulsaremos en **Analizar mi dispositivo**.
3. Veremos el resultado y podremos **solucionar las vulnerabilidades**.



ACTIVIDAD 2



No siempre prestamos la atención que se merece a la seguridad de nuestros dispositivos. A continuación, **vamos a buscar e instalar la aplicación CONAN mobile y a realizar los cambios en la configuración recomendados por la misma app.**

Recuerda que, si tienes dudas, puedes consultar los Consejos OSI o la guía de dispositivos móviles de la OSI.

CUESTIONARIO DE EVALUACIÓN



VICEPRESIDENCIA
PRIMERA DEL GOBIERNO
MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL



INSTITUTO NACIONAL DE CIBERSEGURIDAD

Responde a la siguiente pregunta:



1. La herramienta que sirve para analizar nuestros archivos para detectar y eliminar amenazas antes de nuestros dispositivos se conoce como:

- A. Antivirus
- B. Gestor de contraseñas
- C. *Antispam*



TU AYUDA EN
CIBERSEGURIDAD
incibe



Oficina
de Seguridad
del Internauta

CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



2. Si descargamos una aplicación desde una tienda no oficial, corremos el riesgo de:

- A. Descargar una app maliciosa
- B. Descargar aplicaciones falsas
- C. Ambas opciones

CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



3. ¿Por qué debemos revisar los permisos que concedemos a las aplicaciones al instalarlas?:

- A. Para evitar que tengan acceso a demasiada información
- B. Para evitar funciones premium de la app
- C. Para evitar que haya conflicto con otras apps

CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:

4. Para poder utilizar aplicaciones antirrobo, es fundamental que tengamos activada la función de:

- A. Activación remota
- B. Mapeado
- C. Geolocalización



CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



5. El bloqueo de aplicaciones nos puede ayudar a:

- A. Evitar que se abran solas las apps
- B. Proteger su contenido de terceros
- C. Protegernos de un uso prolongado del dispositivo

CUESTIONARIO DE EVALUACIÓN



VICEPRESIDENCIA
PRIMERA DEL GOBIERNO
MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL



INSTITUTO NACIONAL DE CIBERSEGURIDAD

Responde a la siguiente pregunta:

6. ¿Cuál de las siguientes funciones está relacionada con los gestores de contraseñas?:

- A. Crear contraseñas robustas
- B. Cifrar nuestras credenciales
- C. Ambas opciones



TU AYUDA EN
CIBERSEGURIDAD
incibe_



Oficina
de Seguridad
del Internauta

CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



7. La verificación en dos pasos nos ayuda a proteger nuestra privacidad, ¿cómo lo hace?:

- A. Al pedirnos dos contraseñas en lugar de una
- B. Ninguna es correcta
- C. Al requerir una clave temporal que se envía a otro dispositivo

CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



8. A la hora de proteger nuestra privacidad en Internet, podemos utilizar:

- A. Navegadores de pago
- B. Extensiones o *plugins*
- C. Ordenadores públicos

CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



9. El cifrado de nuestro dispositivo móvil nos ayuda a:

- A. Proteger la información almacenada de terceros
- B. Mejorar el rendimiento de nuestro dispositivo
- C. Crear copias de la información

CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



10. Entre las funciones de CONAN mobile, se encuentran:

- A. Evaluar la configuración de nuestro dispositivo
- B. Analizar las aplicaciones instaladas
- C. Todas son correctas



INSTITUTO NACIONAL DE CIBERSEGURIDAD

Gracias por vuestra atención



GOBIERNO
DE ESPAÑA

VICEPRESIDENCIA
PRIMERA DEL GOBIERNO

MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL



TU AYUDA EN
CIBERSEGURIDAD




Oficina
de Seguridad
del Internauta

LICENCIA DE CONTENIDOS

La presente publicación pertenece a Instituto Nacional de Ciberseguridad (INCIBE) y está bajo licencia Reconocimiento-No Comercial-CompartirIgual 4.0 Internacional de Creative Commons. Por esta razón está permitido copiar, distribuir y comunicar públicamente esta obra bajo las condiciones siguientes:

- ❖ Reconocimiento. El contenido de esta publicación se puede reproducir total o parcialmente por terceros, citando su procedencia y haciendo referencia expresa a INCIBE y su sitio web: <https://www.incibe.es>. Dicho reconocimiento no podrá en ningún caso sugerir que INCIBE presta apoyo a dicho tercero o apoya el uso que hace de su obra.
- ❖ Uso No Comercial. El material original y los trabajos derivados pueden ser distribuidos, copiados y exhibidos mientras su uso no tenga fines comerciales.
- ❖ Compartir Igual. Si altera o transforma esta obra, o genera una obra derivada, sólo puede distribuirla bajo esta misma licencia.

Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra.

Alguna de estas condiciones puede no aplicarse si se obtiene el permiso de INCIBE como titular de los derechos de autor.

Texto completo de la licencia: https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es_ES



**Reconocimiento-NoComercial-CompartirIgual 4.0
Internacional (CC BY-NC-SA 4.0)**