

Recurso Pedagógico Taller Formativo

Aprende a utilizar las herramientas básicas de
protección de dispositivos móviles



TU AYUDA EN
CIBERSEGURIDAD



INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. Objeto del documento.....	3
2. Organización y estructura	4
3. Objetivo	5
4. Metodología y recursos	6
5. Contenidos.....	7
5.1. Diapositiva 1. Presentación del taller	7
5.2. Diapositiva 2. Índice	7
5.3. Diapositiva 3. Introducción	7
5.4. Diapositiva 4. Los dispositivos móviles también necesitan protección	7
5.5. Diapositiva 5-6. Antivirus.....	8
5.6. Diapositiva 7. Protección al descargar <i>software</i> y aplicaciones	10
5.7. Diapositiva 8-10. Protección al descargar <i>software</i> y aplicaciones. Google Protect.....	10
5.8. Diapositiva 11-12. Protección al descargar <i>software</i> y aplicaciones. Mecanismo de seguridad iOS	13
5.9. Diapositiva 13-17. Aplicaciones Antirrobo	14
5.10. Diapositiva 18-20. Bloqueo de aplicaciones.....	18
5.11. Diapositiva 21-22. Gestores de contraseñas	19
5.12. Diapositiva 23-24. Aplicaciones de verificación en dos pasos o factor múltiple de autenticación.....	21
5.13. Diapositiva 25. Actividad 1	22
5.14. Diapositiva 26-28. Aplicaciones de privacidad y navegación por Internet de forma segura	22
5.15. Diapositiva 29-31. Cifrado del dispositivo y aplicaciones	27
5.16. Diapositiva 32-33. CONAN mobile, análisis del estado de seguridad del dispositivo	28
5.17. Diapositiva 34. Actividad 2	30
5.18. Diapositiva 35. Cuestionario de evaluación 1	30
5.19. Diapositiva 36. Cuestionario de evaluación 2	30
5.20. Diapositiva 37. Cuestionario de evaluación 3	30
5.21. Diapositiva 38. Cuestionario de evaluación 4	30
5.22. Diapositiva 39. Cuestionario de evaluación 5	31
5.23. Diapositiva 40. Cuestionario de evaluación 6	31
5.24. Diapositiva 41. Cuestionario de evaluación 7	31
5.25. Diapositiva 42. Cuestionario de evaluación 8	31
5.26. Diapositiva 43. Cuestionario de evaluación 9	31
5.27. Diapositiva 44. Cuestionario de evaluación 10.....	31
5.28. Diapositiva 45. Final del taller	31
6. Recursos de evaluación	32
6.1. Cuestionario de evaluación	33
ANEXO	35
Recursos para ampliar	35

1. OBJETO DEL DOCUMENTO

El presente documento constituye una herramienta didáctica que servirá de apoyo al docente para la planificación del **taller formativo ‘Aprende a utilizar las herramientas básicas de protección de dispositivos móviles’**.

Esta herramienta supone un **instrumento específico de planificación, desarrollo y evaluación** de cada una de las áreas de las que se compone la acción formativa, y requiere de la labor docente para concretar los distintos elementos curriculares adaptándolos a las características del alumnado.

A lo largo de la guía docente, se profundizará en los **objetivos generales y específicos de la acción formativa, sus contenidos, criterios de evaluación y aquellos materiales y recursos adicionales** que se requieran para la impartición de las competencias recogidas en el taller.

2. ORGANIZACIÓN Y ESTRUCTURA

La estructura del taller estará compuesta por 10 temas que comprenderán los contenidos teóricos y actividades para el trabajo individual de cada alumno.

La estructura completa del taller es la siguiente:

1. Los dispositivos móviles también necesitan protección.
2. Antivirus.
3. Protección al descargar *software* y aplicaciones (Google Protect + iOS).
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.

3. OBJETIVO

Este taller tiene como objetivo principal **proporcionar a los alumnos las herramientas y conocimientos necesarios para descargar, configurar y utilizar las herramientas de protección básicas de cualquier dispositivo móvil**. Dado el enfoque teórico-práctico, así como el nivel de profundidad de sus contenidos, el taller va dirigido a un colectivo de usuarios con conocimientos muy básicos sobre tecnología y seguridad.

A lo largo del taller, se ofrecerá a los alumnos recursos de ampliación en forma de enlaces de la OSI, con el fin de expandir sus competencias y satisfacer su curiosidad. Del mismo modo, servirán al docente para enriquecer los contenidos del taller.

4. METODOLOGÍA Y RECURSOS

La metodología empleada en el desarrollo de este taller es de **carácter teórico-práctico, visual y buscando la participación activa del alumnado** durante la impartición del taller:

- **Teórico-práctica:** Los contenidos teóricos vendrán acompañados en todo momento de ejemplos reales que aterricen la teoría. A través de casos reales y actividades, el alumnado pondrá en práctica la información transmitida a través del taller.
- **Visual:** Las imágenes técnicas y decorativas abundarán a lo largo de todo el taller. Además, para dinamizar aún más los talleres, se incluirán recursos audiovisuales relacionados con el contenido (al menos 1 vídeo por taller).
- **Participación activa:** El alumnado tendrá un papel fundamental en los talleres, pues no se limitarán a escuchar. Los contenidos están preparados para que se pongan en práctica desde el comienzo del taller en cada uno de los equipos del alumnado.
 - Además, se busca enriquecer la experiencia formativa a través de las dudas y comentarios que se expongan durante su desarrollo.

El taller cuenta con diferentes **actividades y recursos** al servicio del docente para la impartición:

- **Presentación en Power Point.** Se trata de una presentación con comentarios en texto para apoyar al docente, y los contenidos a compartir con el alumnado.
- **Actividades.** Se trata de pequeñas actividades que permiten al alumnado poner en práctica los conocimientos recién adquiridos, y que acompañan a los apartados principales.
- **Vídeos y enlaces para ampliar.** Servirán para afianzar los contenidos desarrollados mediante ejemplos y contenidos para ampliar, con los que enriquecer la acción formativa.
- **Cuestionario de evaluación.** Cuestionario final del taller formado por 15 ítems con opción múltiple con el que realizar la evaluación final de los alumnos.

5. CONTENIDOS

A continuación, se muestra el contenido del taller ordenado en diapositivas para facilitar la tarea al docente.

5.1. Diapositiva 1. Presentación del taller

Presentación del taller “Aprende a contrastar la información”. Debe mencionarse la labor de INCIBE y el teléfono de ayuda 017.

5.2. Diapositiva 2. Índice

Presentación del índice de contenidos del taller:

1. Los dispositivos móviles también necesitan protección.
2. Antivirus.
3. Protección al descargar *software* y aplicaciones (Google Protect + iOS).
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.

5.3. Diapositiva 3. Introducción

Nuestros dispositivos móviles almacenan una enorme cantidad de información sobre nosotros, como nuestros contactos, mensajes, fotografías, etc.

Esta información corre el riesgo de ser sustraída si no está debidamente protegida o si, por ejemplo, perdemos nuestro teléfono, nos lo roban o si se infecta por un *malware*.

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

5.4. Diapositiva 4. 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:

- Corren el riesgo de ser robados y, sin un mecanismo de bloqueo lo suficientemente robusto, un tercero podría tener acceso a su interior, como por ejemplo un segundo factor de autenticación al iniciar sesión.
- También pueden ser infectados con virus o *malware*, por lo que necesitan disponer de un antivirus instalado y debidamente actualizado.

- Navegar por Internet es otra de las actividades que cada vez realizamos más a menudo con nuestros teléfonos móviles, por lo que necesitamos disponer de herramientas que nos ayuden a proteger nuestra navegación.
- Descargar aplicaciones de sitios no oficiales también puede significar poner en riesgo nuestra privacidad al descargar apps con *malware* o que nos soliciten demasiados permisos a la hora de instalarlos, como acceso a nuestra cámara o micrófono, contactos o permisos para enviar y leer mensajes.

En definitiva, a lo largo de este taller vamos a conocer más en profundidad las diversas herramientas de protección que podemos instalar en nuestros dispositivos, sus funciones y cómo podemos instalarlas y comenzar a utilizar para añadir esa capa extra de seguridad que tanto necesitamos.

5.5. Diapositiva 5-6. Antivirus

Estos programas son fundamentales para prevenir la gran mayoría de amenazas que podemos encontrarnos cuando navegamos por Internet. 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.

Su funcionamiento es el siguiente:

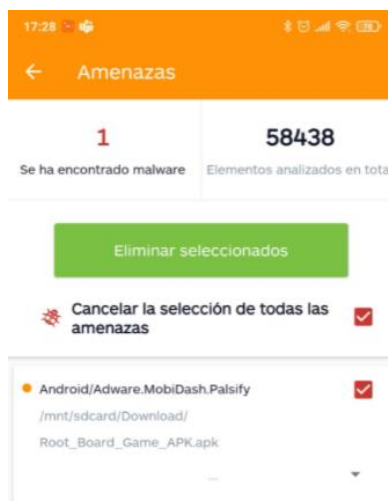
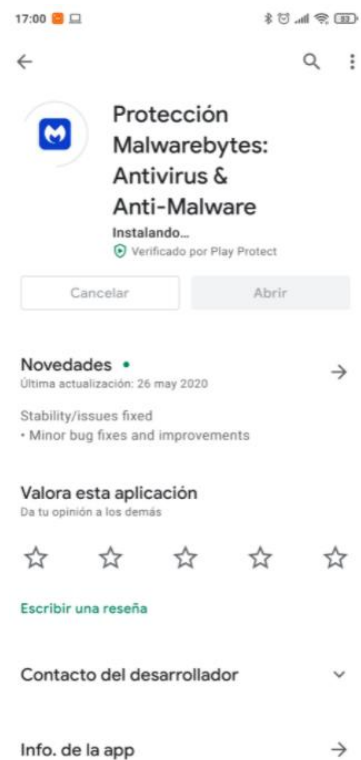
1. Primero, **los antivirus analizan nuestro sistema de archivos, comparándolo con sus bases de datos de virus, *malware* y otros programas maliciosos** para ver si tenemos alguno de ellos instalados en nuestro dispositivo.
2. En caso de detectarla, **aíslan la amenaza para evitar que se propague** por nuestro sistema.
3. Luego, **la eliminarán automáticamente o nos notificarán para que seamos nosotros los que lo eliminemos manualmente**, ya que en ocasiones, los antivirus detectan falsas amenazas.

Lamentablemente, muchos de nuestros dispositivos móviles no cuentan con un antivirus preinstalado. Pero sí podemos acceder a nuestra tienda oficial de aplicaciones ([Play Store](#) o [App Store](#)) e instalar uno recomendado por la OSI.

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**:

Tanto si utilizamos un dispositivo con Android, como uno de Apple (iOS), el proceso será muy similar:

1. Lo primero será acceder a la [Play Store](#) o [App Store](#) para buscar el antivirus entre todas las aplicaciones disponibles.
2. Una vez localizado, es importante que nos aseguremos de que es la aplicación correcta, revisando el fabricante, su descripción, número de descargas y los comentarios y valoraciones de otros usuarios.
3. Tras hacer clic en **Instalar u Obtener**, la aplicación se descargará e instalará en nuestro dispositivo. Al iniciarse, podremos realizar un primer análisis del estado de nuestro teléfono o *tablet* haciendo clic sobre **Analizar ahora**.
4. Una vez haya terminado de analizar todo nuestro sistema de archivos y aplicaciones instaladas, **el antivirus nos informará de las posibles amenazas**, elementos sospechosos o, por el contrario, **si nuestro dispositivo está totalmente seguro**.



5. Es recomendable **realizar estos análisis de forma periódica**. Además, para asegurarnos de recibir la mejor protección, **es fundamental que mantengamos la aplicación actualizada a su última versión**, para que así disponga de una base de datos de virus y *malware* actualizada.

5.6. Diapositiva 7. Protección al descargar *software* y aplicaciones

Una de las principales funciones y acciones que llevamos a cabo con nuestros dispositivos móviles, ya sean Android o iOS, es la descarga de aplicaciones. Estas aplicaciones son programas informáticos que añaden una gran cantidad de funciones a nuestros dispositivos, como las aplicaciones para comunicarlos con nuestros contactos, como es WhatsApp, redes sociales, o juegos online.

En el mercado existen un sinfín de aplicaciones, pero 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.

Por ello, desde la OSI recomendamos siempre utilizar las tiendas oficiales, como [Play Store](#) o [App Store](#), ya que aplican diversos filtros para eliminar este tipo de *software* malicioso.

Sin embargo, ya que estos filtros pueden fallar, nuestros dispositivos móviles cuentan con mecanismos de protección a la hora de descargar e instalar aplicaciones. Además, es recomendable que los usuarios revisemos siempre los comentarios y valoraciones de otros usuarios, el número de descargas y la información del desarrollador.

5.7. Diapositiva 8-10. Protección al descargar *software* y aplicaciones. Google Protect

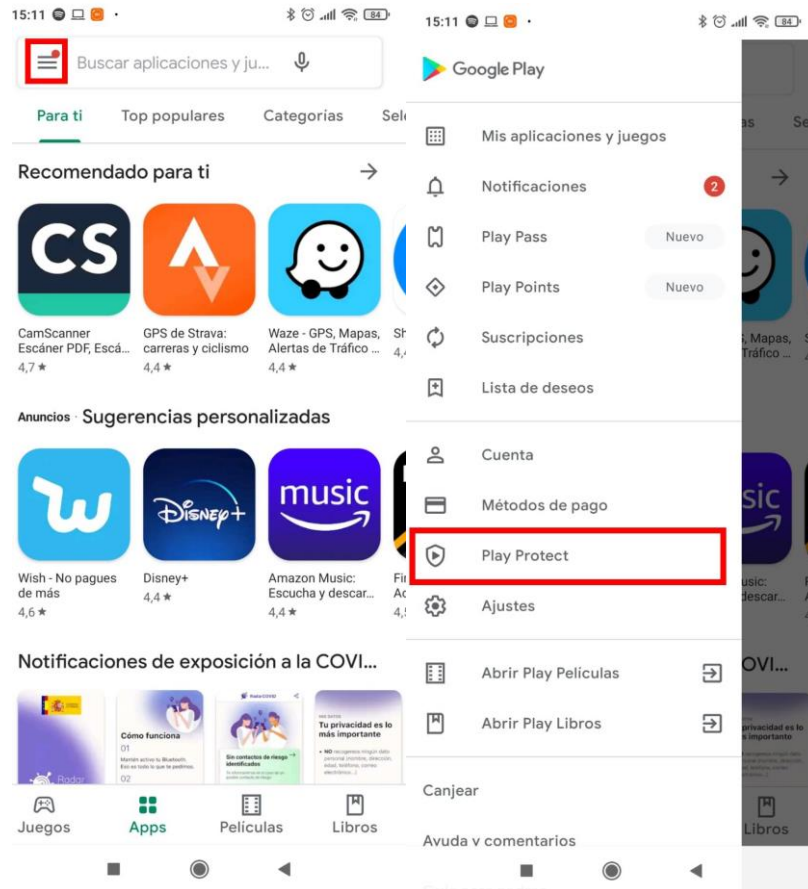
Nuestros dispositivos móviles, como *smartphones* o *tablets*, con el sistema Android, disponen de una herramienta de protección contra las aplicaciones dañinas, conocida como [Google Play Protect](#). Sus funciones son:

- Realización de un escáner de las aplicaciones sospechosas o maliciosas.
- Protección contra robo de nuestro dispositivo.
- Protección cuando navegamos por Internet.

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

1. Acceder a la aplicación [Play Store](#) y pulsar sobre el icono de menú de la esquina superior izquierda: las tres rayas horizontales.





2. Luego, pulsaremos sobre la opción de **'Play Protect'**. Una vez dentro, veremos el estado en el que se encuentra nuestro dispositivo y las aplicaciones instaladas. Aquí podremos comprobar si tenemos alguna aplicación maliciosa instalada o si, por el contrario, todo está correcto. En este caso, veremos el siguiente mensaje: **'No se ha encontrado ningún problema'**.

Además, veremos cuándo se realizó el último análisis y sobre qué aplicaciones.

3. Si queremos, también podemos forzar un nuevo análisis pulsando sobre **'Analizar'**.
4. Finalmente, debemos asegurarnos de que están activadas las opciones de **'Analizar aplicaciones con Play Protect'** y **'Mejorar la detección de aplicaciones dañinas'**, haciendo clic en el **icono de la rueda de la esquina superior derecha**.

De ser así, aparecerá en color verde y podremos tener la tranquilidad de que Google estará monitorizando las aplicaciones que instalemos en busca de posibles amenazas. En caso de que detecte una amenaza, Google nos informará de ello y nos pedirá que la desinstalemos.

15:12 [íconos de notificación] [íconos de conexión] [83%]

← Ajustes de Play Protect

General

Analizar aplicaciones con Play Protect

Play Protect puede analizar este dispositivo y avisarte si encuentra aplicaciones dañinas



Mejorar la detección de aplicaciones dañinas

Envía aplicaciones desconocidas a Google para mejorar la detección



← Play Protect



Tu dispositivo está en peligro

1 aplicación dañina detectada

✖ ¿Desinstalar aplicación dañina?

Es posible que esta aplicación sea dañina

Desinstalar

Aplicaciones analizadas recientemente



Las aplicaciones se analizaron hace 2 minutos

Play Protect comprueba de forma periódica si hay comportamientos dañinos en tus aplicaciones



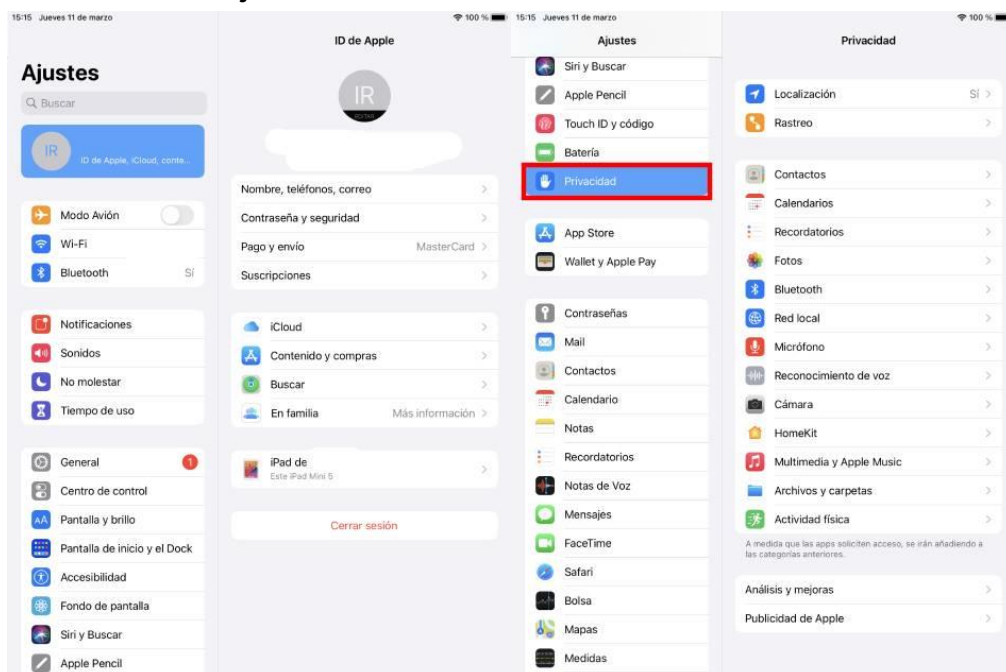
Adicionalmente, los usuarios podemos comprobar los permisos concedidos a las aplicaciones instaladas desde los ajustes de nuestro dispositivo y buscando por permisos, privacidad o aplicaciones. De este modo, podremos comprobar si estamos concediendo algún permiso de más a alguna aplicación que ya no utilizemos, por ejemplo.

Como cualquier otra aplicación, necesitamos que Google Play Protect se mantenga **actualizado** para ofrecernos la mejor protección posible. Esto se hará de forma automática cada vez que actualicemos nuestro dispositivo.

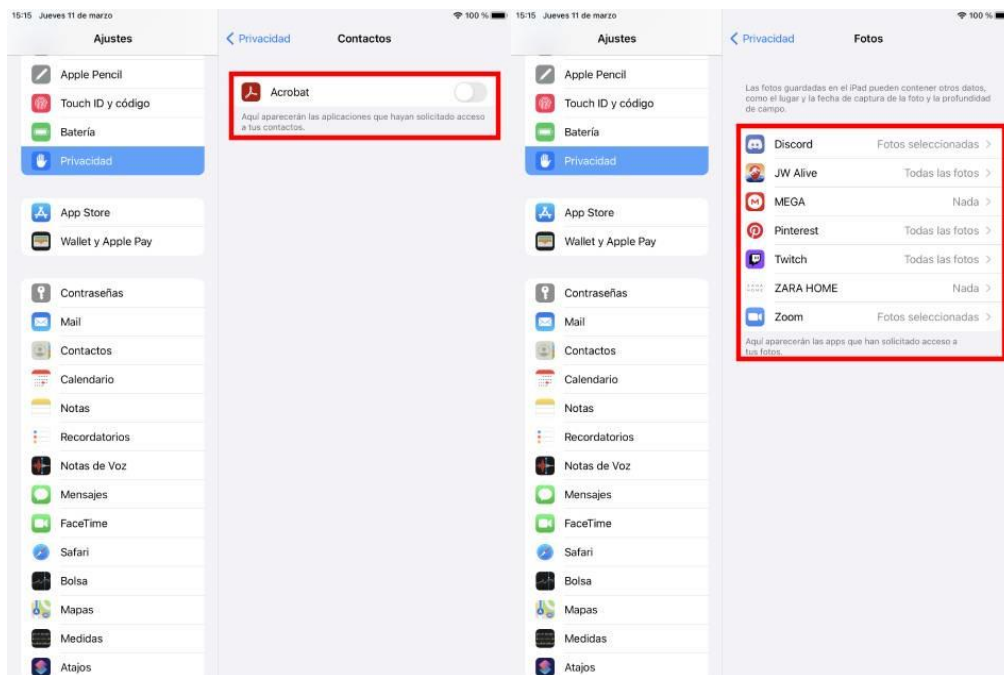
5.8. Diapositiva 11-12. Protección al descargar software y aplicaciones. Mecanismo de seguridad iOS

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. Nuestra principal protección serán los [filtros de seguridad de la App Store](#). Sin embargo, adicionalmente podemos gestionar los permisos que damos cuando instalamos una aplicación en el dispositivo para tener bajo control qué puede hacer. Podemos ir aplicación por aplicación, o gestionar todos los permisos concedidos desde **Ajustes > Privacidad**.



2. A continuación, seleccionaremos una categoría de información, como **'Contactos'** o **'Fotos'**. Así veremos las aplicaciones que han solicitado este permiso y si está habilitado.



3. Para evitar cualquier riesgo, es conveniente que [revisemos los permisos frecuentemente](#) y deshabilitemos aquellos que no coincidan con la función de la aplicación.

Por ejemplo, ¿para qué querría una aplicación de dibujo acceso a mis contactos y al reconocimiento de voz?

4. No debemos olvidarnos tampoco de [mantener las aplicaciones actualizadas](#) para corregir posibles errores de seguridad y asegurarnos de disponer de la mejor protección contra estas aplicaciones maliciosas.

5.9. Diapositiva 13-17. 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.

En estos casos, tanto el sistema operativo de Android, como el de iOS, cuentan con sus propias aplicaciones y funciones con las que tratar de:

- Geolocalizar nuestro teléfono o *tablet*.
- Enviar una notificación o alerta para tratar de localizarlo.
- Bloquear el acceso al dispositivo.
- Y, en el peor de los casos, eliminar toda la información almacenada en su interior, incluidas fotos, vídeos, contactos y la información de nuestra cuenta de Google o Apple.

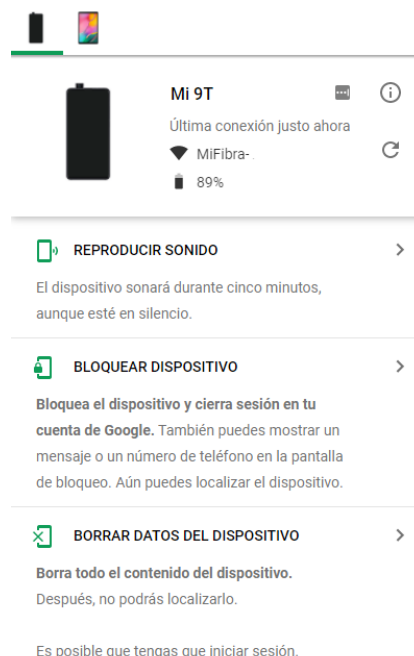
A continuación, vamos a ver cómo configurar estas opciones paso a paso para tener la tranquilidad de que, en caso de pérdida o robo, **seguiremos manteniendo intacta nuestra seguridad y privacidad**.

En el caso de Android:

Gracias a nuestra cuenta de Google, contamos con una función que nos permite gestionar todos los dispositivos vinculados a nuestra cuenta, como nuestro teléfono móvil o *tablet*.

Entre las herramientas que pone a nuestra disposición está la de **geolocalizar nuestros dispositivos**, siempre y cuando tengamos activado el GPS del dispositivo. Para acceder a ella:

1. Lo primero será comprobar que tenemos activada la función **Encontrar mi dispositivo**. Para ello, deberemos entrar en los ajustes de nuestro teléfono
2. Deberemos acceder a [nuestra cuenta de Google](#).
3. Luego, pulsaremos sobre **Seguridad > Tus dispositivos**, donde encontraremos la opción **Buscar un dispositivo perdido**. Para que aparezca deberemos haber iniciado previamente sesión con nuestra cuenta de Google en el dispositivo.
4. Al hacer clic en uno, **obtendremos información** sobre:
 - a. Su ubicación geográfica, siempre y cuando tengamos activado el GPS.
 - b. Si está conectado a Internet y a qué conexión está conectado o la batería que le queda.



También podremos ejecutar algunas opciones adicionales:

- c. **Reproducir sonido:** hará sonar el teléfono móvil a un volumen muy alto para que podamos localizarlo si lo hemos perdido por casa, por ejemplo.
- d. **Bloquear dispositivo:** activando esta opción, el dispositivo se bloqueará. Además, se podrá redactar un mensaje para que la persona que lo haya encontrado sepa qué hacer con él o indicar un número de teléfono al que llamar.

Nueva pantalla de bloqueo

La pantalla de bloqueo actual se sustituirá con una pantalla de contraseña. No utilices la contraseña de tu cuenta de Google.

Contraseña nueva

Confirmar contraseña

Mensaje de recuperación (opcional)

Número de teléfono (opcional)

- e. **Borrar datos del dispositivo:** se devolverá el dispositivo a los ajustes de fábrica y se borrará toda la información almacenada. Una vez ha comenzado el borrado, este proceso no puede interrumpirse por lo que antes de hacerlo, es importante que estemos completamente seguros.

Para evitar la pérdida de información, es recomendable que llevemos a cabo copias de seguridad de los datos almacenados en nuestros dispositivos con frecuencia. Así, si perdemos el teléfono, nos lo roban o eliminamos por error información importante, siempre podremos contar con una alternativa.

Por otro lado, el borrado puede que no afecte al contenido de la tarjeta SD (espacio de almacenamiento externo) por lo que es recomendable que la cifremos.

< BORRAR DATOS DEL DISPOSITIVO

Los datos de este dispositivo se borrarán de forma permanente. Después, no podrás localizarlo.

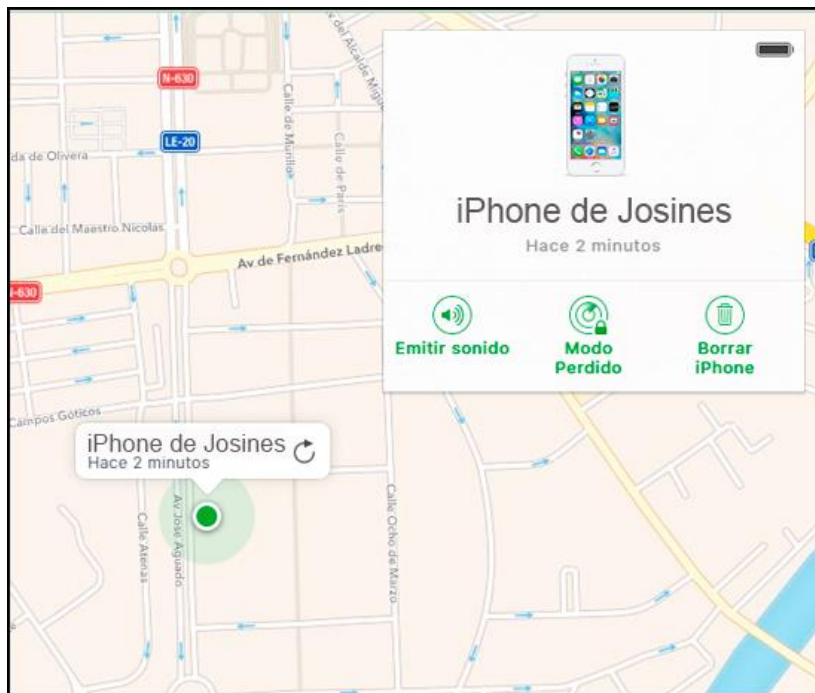
Si tu dispositivo no tiene conexión, los datos se borrarán cuando vuelva a estar conectado.

Para borrar los datos de tu dispositivo, es posible que tengas que iniciar sesión de nuevo con tu cuenta de Google.

BORRAR DATOS DEL DISPOSITIVO

En el caso de iOS:

La herramienta de Apple que permite tener controlados los dispositivos vinculados a una determinada cuenta se conoce como **Buscar mi iPhone**. Para utilizar esta aplicación, es necesario acceder a la **cuenta de iCloud** o utilizar la aplicación [Buscar mi iPhone](#) en otro dispositivo.



Primero, deberemos asegurarnos de tener activada la función **Buscar mi iPhone** en el dispositivo.

1. Para lo cual entraremos en **Ajustes** y **pulsaremos sobre nuestro nombre**.
2. Luego pulsaremos sobre **Buscar > Buscar mi iPhone/iPad** y activaremos todas las opciones. **Enviar última ubicación** nos ayudará a localizar nuestro dispositivo incluso si está desactivado y **Red de Buscar** nos permitirá encontrarlo incluso aunque no esté conectado a Internet.

Cuando queramos localizar nuestro dispositivo robado o perdido, debemos hacer lo siguiente:

1. Entrar en la aplicación **Buscar mi iPhone** en el otro dispositivo e ingresar con nuestro ID de Apple y contraseña.
2. Luego, seleccionaremos el dispositivo que queremos encontrar. Aparecerán varias acciones:
 - a. **Reproducir sonido**: emitirá un sonido que nos ayudará a localizar nuestro dispositivo.
 - b. **Modo Perdido**: bloqueará el iPhone a distancia para que nadie pueda acceder a él. Además, podremos incluir un mensaje y un número de teléfono para que, si alguien lo encuentra, pueda devolvérselo.
 - c. **Borrar iPhone**: esta opción eliminará toda la información del dispositivo restableciendo su configuración a los ajustes de fábrica. El mensaje y el teléfono de contacto seguirá mostrándose por pantalla en caso de que otro usuario lo haya encontrado y pueda devolvérselo.

5.10. Diapositiva 18-20. 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, como por ejemplo, herramientas de mensajería instantánea o redes sociales.

Todas funcionan de forma similar, al tratar de acceder a una aplicación protegida con esta herramienta, se nos solicitará el ingreso de una “contraseña de desbloqueo”, un patrón, un código PIN, o la utilización de un sensor biométrico como los lectores de huellas dactilares.

A diferencia de la verificación en dos pasos, aquí no es necesario el uso de un segundo dispositivo al que nos envíen la clave, por ejemplo. Únicamente añadiremos una clave de protección adicional a las aplicaciones o a nuestro dispositivo.

Desde dispositivos Android, disponemos de varias alternativas para añadir esta capa extra de seguridad a nuestras aplicaciones:

La primera opción es mediante los **Ajustes de nuestro dispositivo**:

1. Deberemos hacer clic en **Ajustes > Seguridad y privacidad > Bloqueo de aplicaciones**. Algunas versiones de Android pueden seguir un camino diferente, aunque podremos llegar a ellas desde el buscador de nuestro menú de Ajustes.
2. Luego, será necesario que **especifiquemos la clave o el patrón** con el que vamos a proteger el acceso a nuestras aplicaciones.
3. Tras seguir los pasos, podremos llevar a una pantalla donde **seleccionar que aplicaciones queremos proteger**. Al **habilitar el bloqueo de aplicaciones**, la próxima vez que quieras acceder a dicha app, tendrás que ingresar la clave o el patrón para desbloquearla.

Algunas aplicaciones incluyen esta función de bloqueo de forma predeterminada y bastará con acceder a sus opciones de configuración para añadirla. Por ejemplo, WhatsApp permite activar el bloqueo por huella dactilar o código desde sus **Ajustes**.

Finalmente, podemos recurrir a **aplicaciones de terceros** para bloquear las aplicaciones que tengamos instaladas en nuestro dispositivo por medio de una contraseña.

En el caso de dispositivos iOS, no existe un bloqueo como tal, pero podemos impedir su acceso a terceros mediante un tiempo de uso, tras el cual, la aplicación se bloqueará y tendremos que volver a ingresar la clave de desbloqueo:

1. Lo primero será acceder a **Ajustes > Tiempo de uso** y pulsar sobre **Usar código para “Tiempo de uso”**. Al hacerlo, deberemos ingresar una **clave** con la que desbloquearemos las apps.
2. Una vez hecho, pulsaremos sobre **ver toda la actividad** para ver un listado de las apps utilizadas. Al pulsar en alguna de ellas, encontraremos una opción llamada **Añadir límite**.
3. Especificaremos el **tiempo máximo de uso**, por ejemplo 1 minuto. Ahora, cuando intentemos acceder a la app, aparecerá bloqueada y si hacemos clic, nos solicitará nuestra **clave de desbloqueo** y que especifiquemos durante cuánto tiempo queremos que permanezca desbloqueada. Por ejemplo, podemos añadirle 15 minutos de uso para que, cuando terminemos de usarla, se vuelva a bloquear.

De forma adicional, podemos utilizar aplicaciones de terceros cuya función sea la de añadir una capa extra de seguridad a nuestras aplicaciones y evitar que terceros con acceso a nuestro dispositivo puedan utilizarlas.

5.11. Diapositiva 21-22. 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”. De este modo, podemos gestionar todas nuestras cuentas de usuario desde una misma herramienta, memorizando únicamente una clave maestra.

Aunque las funciones y características son:

- **Verificación en dos pasos:** muchos gestores online incluyen esta función para proteger nuestras cuentas principales.
- **Multidispositivo:** algunos nos permiten sincronizar nuestras contraseñas con el servidor del fabricante, es decir, en la nube. Allí estarán protegidas y podremos acceder a ellas desde una app y desde cualquier dispositivo.
- **Generación de contraseñas:** nos permitirán crear una contraseña robusta desde cero y en un momento, ya que disponen de un generador automático. Algunos gestores disponen de una opción para crear cuentas temporales, que podemos utilizar para registrarnos en alguna web o servicio online de forma puntual y no recibir publicidad en nuestro correo principal, por ejemplo.
- **Integración con los navegadores a través de extensiones y autocompletado:** esta función nos ayudará a automatizar el proceso a la hora de iniciar sesión a través del navegador ya que estará sincronizado con nuestro gestor de contraseñas.
- **Alertas de vulnerabilidad:** en el caso de que una fuga de información haya vulnerado la privacidad de nuestros datos, los gestores podrán avisarnos para que cambiemos las contraseñas de aquellas cuentas afectadas.

En el mercado existe una gran variedad de aplicaciones con esta función, tanto para dispositivos móviles, ordenadores Windows o macOS y navegadores. A continuación, a modo de ejemplo, vamos a ver los pasos a seguir para configurar nuestras contraseñas desde el gestor LastPass.

1. Lo primero será [descargar la aplicación](#) y crearnos una cuenta. Este paso es idéntico en todos los gestores, y nos requerirá el uso de una dirección de correo electrónico y una contraseña maestra. **Es fundamental que no nos olvidemos de esta contraseña, ya que es la clave que utilizaremos para poder acceder al resto de cuentas.**



The image shows the LastPass login interface. At the top, the LastPass logo is displayed. Below it, there are two links: 'INICIAR SESIÓN' and 'O CREE UNA CUENTA'. The 'INICIAR SESIÓN' link is highlighted. Below the links, there are two input fields: 'Dirección de e-mail' and 'Contraseña maestra'. Both fields have placeholder text: 'introduzca una dirección de e-mail válida' and 'introduzca una contraseña' respectively. Below the input fields, there is a red button labeled 'INICIAR SESIÓN'. Below the button, there is a link '¿HA OLVIDADO LA CONTRASEÑA?' and a link 'Opciones avanzadas' with a dropdown arrow.

Vamos a crear su contraseña maestra

Elija una que no suela utilizar en ningún otro sitio. No podrá restablecerla, así que utilice algo que pueda recordar.

Contraseña maestra 

Confirmar contraseña maestra 

Indicio de contraseña (opcional)

ESTABLECER MI CONTRASEÑA

2. Una vez entremos en la aplicación, deberemos **agregar nuevos elementos** para nuestras cuentas (correo electrónico, redes sociales, cuenta bancaria). Como mínimo nos pedirán la URL o servicio para el que será utilizado, el nombre de usuario, la contraseña y algún comentario o nota que queramos añadir.
3. Ahora, siempre que necesitemos acceder a una de nuestras cuentas, podremos acceder a esta herramienta. Además, muchos de los gestores incluyen **funciones adicionales** para ayudarnos a crear contraseñas robustas, recordatorios para cambiar las contraseñas y medidas para recuperar nuestra clave maestra en caso de que la olvidemos.

5.12. Diapositiva 23-24. 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. Al activarla, además de un usuario y una contraseña, será necesario facilitar otro código para autenticarnos.

Este código suele enviarse a otro dispositivo, como puede ser nuestro móvil. De este modo, para acceder a nuestra cuenta se necesita, además de nuestro usuario y contraseña, tener acceso a nuestro dispositivo personal, lo que minimiza las posibilidades de que un atacante nos robe la cuenta.

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”. Estas aplicaciones se pueden descargar en [Play Store](#) y [App Store](#) para nuestras cuentas de Gmail, Amazon, Facebook, Outlook, PayPal, Dropbox y Twitter...

La instalación y el funcionamiento son muy similares en ambas aplicaciones.

1. Lo primero que deberemos hacer es descargar e instalar la aplicación. Tanto si utilizamos Android como iOS, deberemos acceder a [Play Store](#) o [App Store](#) respectivamente y buscar el nombre de la aplicación en el buscador: Microsoft Authenticator o Google Authenticator.

Una vez descargada e instalada, **abriremos la aplicación y se nos solicitará crear nuestra primera cuenta**. Para ello dispondremos de dos opciones, mediante un **código QR** o mediante una **clave**. Ambos podemos obtenerlos desde el servicio o cuenta que queremos proteger, como nuestra red social, por ejemplo.

2. Luego, deberemos ingresarlo en la aplicación para sincronizar la cuenta con nuestra aplicación de verificación en dos pasos. Ahora, cada vez que queramos ingresar en esta cuenta, además de la contraseña se nos solicitará un código de autenticación que solo podremos obtener a través de la aplicación.

De este modo, aunque un tercero obtuviese nuestro usuario y contraseña, seguiría sin poder acceder a nuestra cuenta a menos que también tuviese acceso a nuestro dispositivo móvil. Además, estas claves son temporales, lo que dificulta aún más el trabajo a los ciberdelincuentes.

5.13. Diapositiva 25. Actividad 1

Diapositiva para introducir a los usuarios la actividad. El tiempo aproximado de duración será de entre 3 y 5 minutos. Los pasos habrán sido descritos en las diapositivas anteriores.

La labor del docente será la de acompañar a los usuarios y ayudar en caso necesario. Se debe valorar la iniciativa, la resolución de la actividad y la proactividad.

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.

5.14. Diapositiva 26-28. Aplicaciones de privacidad y navegación por Internet de forma segura

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. Una página web sospechosa o descargarnos algún archivo potencialmente malicioso puede ser suficiente para dejar nuestro dispositivo totalmente inutilizado o infectado por algún tipo de *malware* que vulnere nuestra privacidad.

A la hora de proteger nuestra navegación disponemos de varias alternativas:

1. **Utilizar un navegador seguro y actualizado.** Los navegadores son las herramientas que nos permiten acceder a Internet y navegar a través de las páginas web. La mayoría de dispositivos móviles ya vienen con algún navegador instalado por defecto, como Google Chrome en Android o Safari en iOS.

Sin embargo, existen otras alternativas, por ejemplo, Opera, que incluye una VPN y extensiones contra anuncios instalados por defecto. En las tiendas de aplicaciones encontraremos otras muchas alternativas, como Kiwi Browser, Tor o DuckDuckGo.

- Para instalarlas, bastará con **abrir nuestra tienda oficial** ([Play Store](#) o [App Store](#)) y **buscar el nombre del navegador**.
- Luego, haremos clic en **Obtener o Instalar**. Debemos recordar que, para evitar descargar una app maliciosa, podemos revisar el número de descargas, la información del fabricante o los comentarios y valoraciones de otros usuarios.

2. **Activar el modo incógnito.** Siguiendo el punto anterior, todos los navegadores incluyen una modalidad de incógnito o anónima que nos permite navegar por Internet sin dejar rastro. Al hacerlo, el navegador que utilicemos no guardará datos sobre nuestro historial de navegación, las cookies, datos de inicio de sesión ni información que hayamos introducido en formularios web.

Activarlo es muy sencillo y se realiza de forma similar en la mayoría de navegadores.

- Primero deberemos acceder a nuestro navegador e ir a los **Ajustes** pulsando sobre el **icono de los tres puntos** de la esquina superior derecha.
- Luego haremos clic sobre **Activar una pestaña en modo incógnito** o **Nueva pestaña incógnito**.

Al hacerlo, ya podremos navegar sin dejar rastro de nuestra actividad online.

3. **Instalar extensiones o plugins.** Las extensiones o *plugins* son un tipo de *software* que permite personalizar los navegadores web. Existen diferentes tipos de extensiones según su funcionalidad y el navegador en el que se instalan. Algunas de ellas pueden ayudarnos a navegar de forma privada, servirnos como gestores de contraseñas o detectar cuando entramos en una web maliciosa. En este caso, vamos a hablar sobre aquellas que nos permiten bloquear los anuncios cuando navegamos por las páginas web.

Para instalar las extensiones, lo primero que debemos tener en cuenta es que, para evitar acabar infectados por una extensión fraudulenta, utilicemos las tiendas o *markets* oficiales:

- Extensiones oficiales de [Microsoft Edge](#).
- Extensiones oficiales de [Google Chrome](#).
- Extensiones oficiales de [Mozilla Firefox](#).
- Extensiones oficiales de [Safari](#).

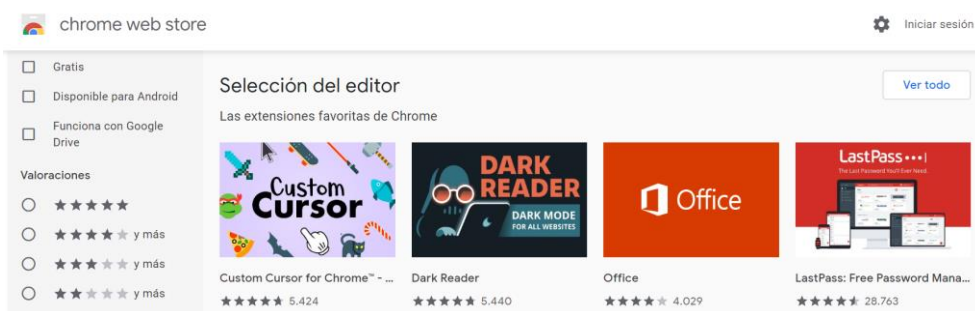
Veamos el proceso de instalación en dos de los navegadores más utilizados, Chrome y Safari:

En el caso de Google Chrome:

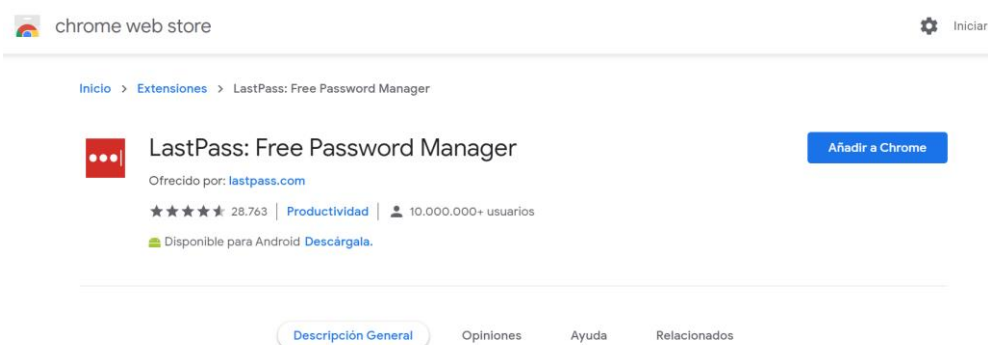
1. Desde Chrome, abriremos la [Chrome Web Store](#) y seleccionaremos la opción **“Extensiones”** en el menú.



2. Una vez dentro, seleccionaremos la extensión que más nos interese. Podemos poner en el nombre de la extensión en el buscador o el tipo de extensión que estamos buscando. Es fundamental que comprobemos el número de descargas y las valoraciones y comentarios de otros usuarios para evitar descargarnos una copia o una app maliciosa.

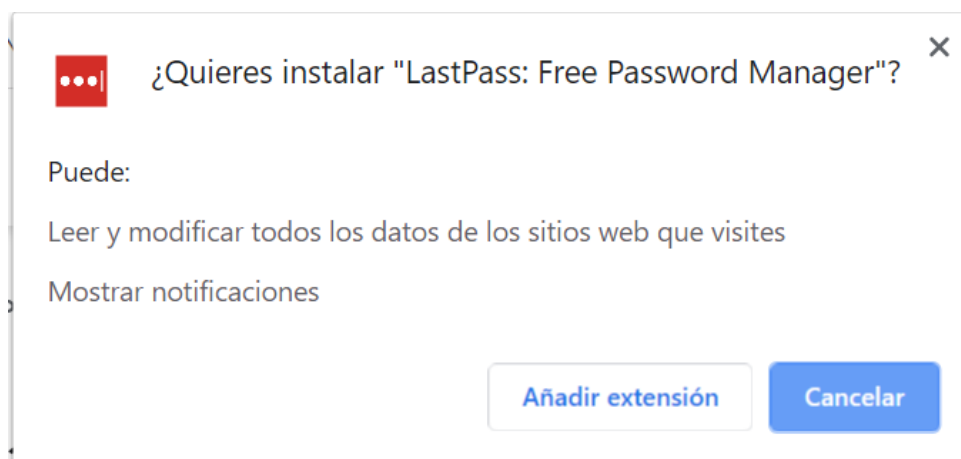


3. Al seleccionarla, nos llevará a la **página de descripción de la extensión**, en donde veremos la puntuación, reseñas, permisos, fecha de las últimas actualizaciones, entre otras características, así como descripción de lo que hace la misma.



4. Una vez estemos seguros, seleccionaremos la opción **“Añadir a Chrome”**.

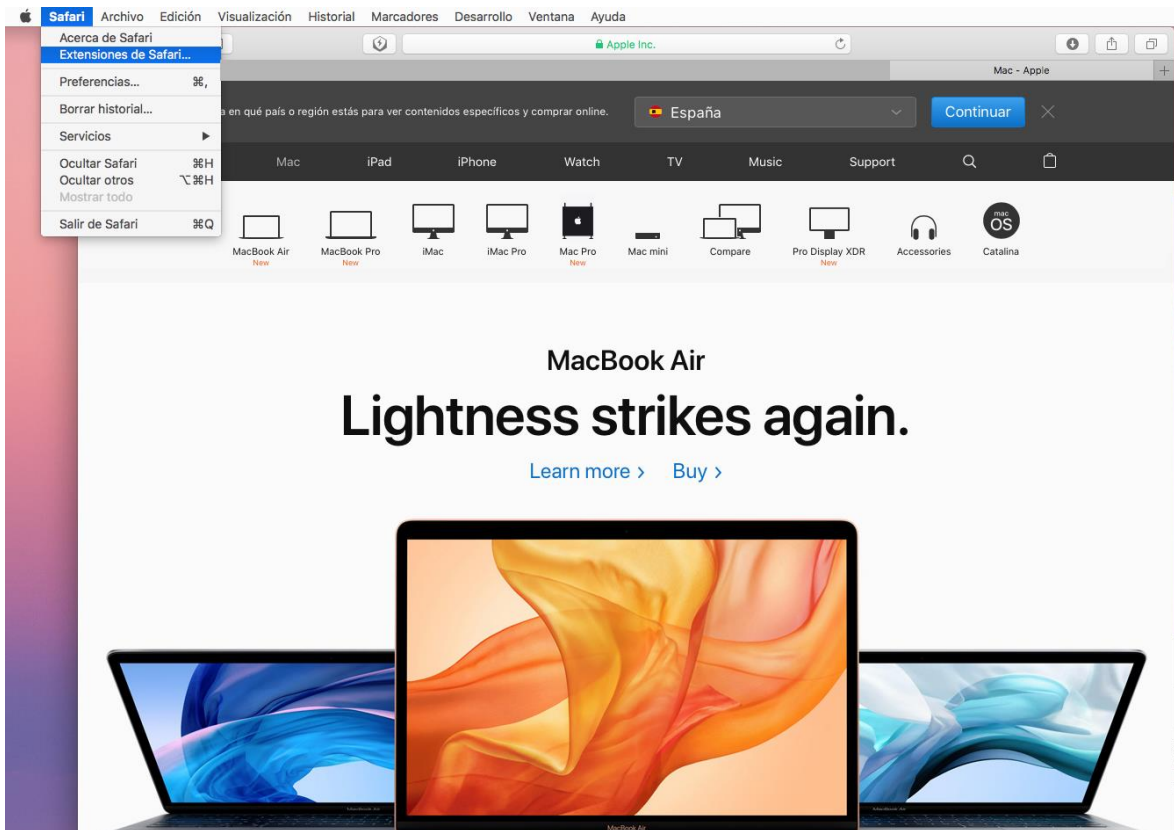
5. Revisaremos los tipos de datos a los que la extensión podrá tener acceso y luego, **si nos parecen coherentes**, pulsaremos sobre el botón **“Agregar extensión”**.



Podemos ver todas las extensiones instaladas en la barra de herramientas de nuestro navegador, en la parte superior derecha.

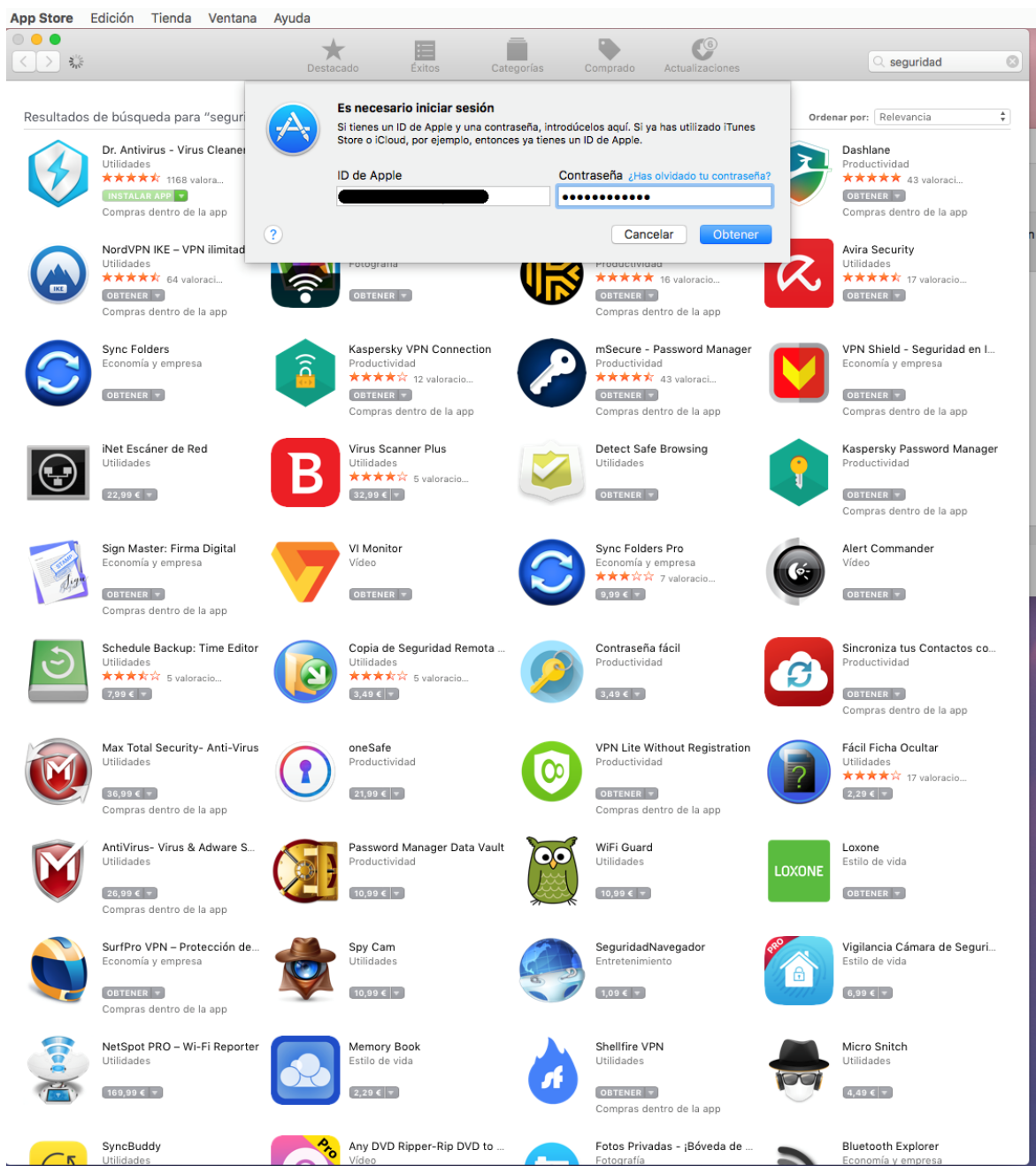
En el caso de Safari:

- a. Abriremos nuestro navegador y haremos clic sobre la pestaña **“Safari > Extensiones de Safari”**. Dentro, se nos abrirá automáticamente la **página de extensiones de Safari**.



En versiones anteriores, nos abrirá la página web de la galería de extensiones del navegador.

- b. **Seleccionaremos la extensión que queramos**, insertaremos nuestras **credenciales** y comenzará el proceso de instalación.



5.15. Diapositiva 29-31. 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. De este modo, si un tercero consiguiese acceso a nuestro teléfono y quisiese entrar a nuestra galería de imágenes, debería introducir una contraseña previamente, de lo contrario, no podrá visualizar las imágenes.

A diferencia de la verificación en dos pasos, con el cifrado lo que hacemos es bloquear el acceso mediante una clave que debemos conocer nosotros previamente, sin embargo no requiere de un segundo elemento donde recibir la clave temporal que caracteriza a la verificación en dos pasos.

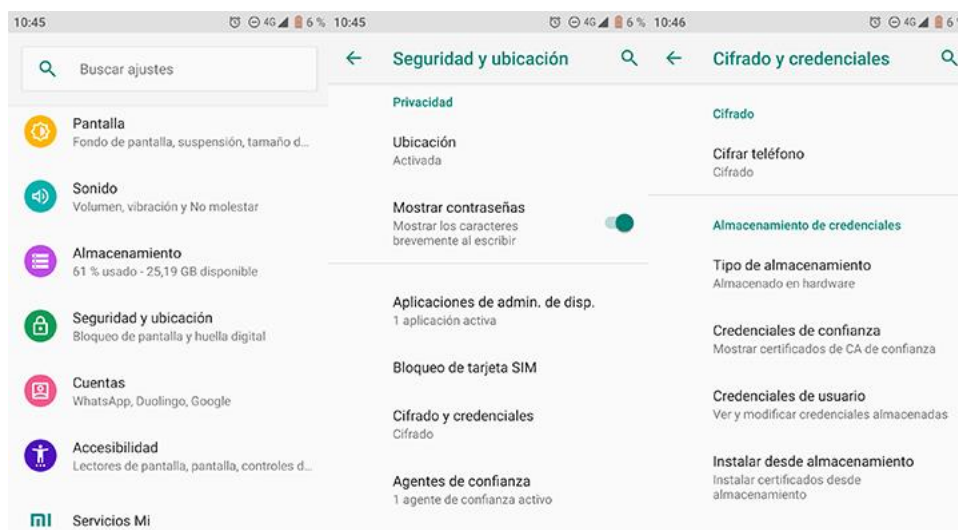
Una vez cifrado, nuestra música, vídeos, fotos y datos de las aplicaciones sólo serán accesibles si introducimos la contraseña o el código PIN que hayas configurado durante el proceso de cifrado.

Esta función está disponible tanto en dispositivos Android como en iOS y viene ya incluida dentro del propio sistema, por lo que no tendremos que descargar ninguna aplicación adicional.

En el caso de Android, el procedimiento puede variar ligeramente dependiendo de la versión de nuestro sistema operativo, pero podremos seguir los pasos sin problema.

Lo único que necesitaremos tener en cuenta es que deberemos utilizar un PIN o contraseña como método para cifrar y descifrar el dispositivo y que deberemos recordar.

1. Lo primero será acceder a los **Ajustes** de nuestro dispositivo y buscar las opciones de **Seguridad y ubicación**.
2. Una vez localizado, pulsaremos sobre la opción **Cifrado y credenciales** y dentro, pulsaremos sobre la opción **Cifrar teléfono**.



3. Una vez dentro, seguiremos los pasos indicados para **crear una contraseña o PIN** que nos servirá para cifrarlo y descifrarlo.

Una vez hecho, toda la información de nuestro dispositivo, incluida la que tengamos almacenadas en dispositivos de almacenamiento externo, como una tarjeta MicroSD, quedará totalmente cifrado.

En este caso, si quisiésemos utilizar la tarjeta en otro dispositivo, tendríamos que descifrarla primero utilizando la contraseña o PIN que hemos creado previamente.

En los dispositivos iOS el proceso es aún más sencillo, ya que todos los dispositivos de la marca Apple (iPhone o iPad) ya están cifrados por defecto y no tendremos que hacer ni activar nada.



5.16. Diapositiva 32-33. 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:** realizará un estudio y evaluará la configuración de nuestro dispositivo en busca de un posible riesgo. También nos compartirá varias recomendaciones para mejorar la seguridad del dispositivo.
- **Análisis de aplicaciones:** clasificará las aplicaciones que tengamos instaladas en función de su estado o peligrosidad.
- **Clasificación aplicaciones por permisos:** nos proveerá de un listado de los permisos que hemos dado a las aplicaciones, ordenadas por los más relevantes y por su nivel de riesgo.
- **Servicio proactivo:** se trata de un seguimiento en tiempo real de eventos de seguridad en el dispositivo y notificaciones en la barra de estado ante determinados eventos:
 - Conexiones a redes WI-Fi inseguras.

- Detección de envío de SMS y llamadas a números de tarificación especial.
 - Modificaciones del fichero *hosts*.
 - Instalación de paquetes maliciosos o sospechosos.
 - Identificación de conexiones potencialmente peligrosas por conectarse a sitios inseguros.
 - Conexiones de red realizadas por las aplicaciones (IP destino, servicio asociado, geolocalización, información ampliada sobre la IP destino)
 - Identificar si desde nuestra conexión a internet se ha detectado algún incidente de seguridad relacionado con Botnets (Servicio AntiBotnet).
- **Consejos OSI:** son recomendaciones ofrecidas por la Oficina de Seguridad del Internauta sobre dispositivos móviles.

Para su instalación, debemos seguir estos pasos:

1. Acceder a la [Play Store](#) y descargar la aplicación CONAN mobile. Es importante que nos aseguremos de que sea la aplicación original revisando la información del desarrollador, el número de descargas y los comentarios y valoraciones de los usuarios.
2. Tras abrirla y **aceptar los términos y condiciones**, accederemos a la aplicación. Lo primero que deberemos hacer es pulsar sobre **Analizar mi dispositivo**. Luego, deberemos **aceptar los permisos correspondientes**.
3. Tras esto, se nos mostrará una pantalla con el **resultado del análisis** y un resumen general. Si hacemos clic en cada uno de los elementos, la aplicación nos dará instrucciones sobre el riesgo y cómo solucionar la vulnerabilidad.



5.17. Diapositiva 34. Actividad 2

Diapositiva para introducir a los usuarios la actividad. La duración aproximada será de entre 3 y 5 minutos. Los pasos habrán sido descritos en las diapositivas anteriores.

La labor del docente será la de acompañar a los usuarios y ayudar en caso necesario. Se debe valorar la iniciativa, la resolución de la actividad y la proactividad.

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](#).

5.18. Diapositiva 35. Cuestionario de evaluación 1

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

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

5.19. Diapositiva 36. Cuestionario de evaluación 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

5.20. Diapositiva 37. Cuestionario de evaluación 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

5.21. Diapositiva 38. Cuestionario de evaluación 4

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

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

5.22. Diapositiva 39. Cuestionario de evaluación 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

5.23. Diapositiva 40. Cuestionario de evaluación 6

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

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

5.24. Diapositiva 41. Cuestionario de evaluación 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

5.25. Diapositiva 42. Cuestionario de evaluación 8

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

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

5.26. Diapositiva 43. Cuestionario de evaluación 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

5.27. Diapositiva 44. Cuestionario de evaluación 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

5.28. Diapositiva 45. Final del taller

¡Gracias por vuestra atención!

6. RECURSOS DE EVALUACIÓN

Las herramientas de evaluación del alumnado permitirán controlar la calidad del aprendizaje recibido, gracias a una serie de **criterios de evaluación**:

1. **Participación durante el taller.** La participación del alumnado mediante dudas u otro tipo de aportaciones resulta de un gran valor evaluativo (10% de la evaluación final).
2. **Actividades.** Estas actividades situadas al final de la mayoría de los apartados son uno de los medios de mayor potencial para la asimilación de las competencias recogidas en el taller. Además, permitirá al docente recibir u *feedback* directo sobre la evolución del alumnado (25% de la evaluación final).

1	<p>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.</p> <p>Sigue los pasos indicados en el taller y en los recursos publicados en la OSI y asegúrate de que tus cuentas estén debidamente protegidas.</p>
2	<p>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 <u>guía de dispositivos móviles de la OSI</u>.</p>

3. **Cuestionario de evaluación.** Este instrumento de evaluación proporcionará gran parte de la puntuación final del alumnado y pondrá a prueba a los alumnos al finalizar un taller (65% de la evaluación final).

EVALUACIÓN FINAL = Participación + Actividades aprendizaje + Cuestionario de evaluación

6.1. Cuestionario de evaluación

El cuestionario de evaluación está compuesto por 10 preguntas de tipo test “opción múltiple” (3 opciones). La respuesta correcta está destacada en color verde.

1	La herramienta que sirve para analizar nuestros archivos para detectar y eliminar amenazas antes de nuestros dispositivos se conoce como:	Antivirus
		Gestor de contraseñas
2	Si descargamos una aplicación desde una tienda no oficial, corremos el riesgo de:	Antispam
		Feedback: Los antivirus utilizan bases de datos para identificar las amenazas, como virus o <i>malware</i> , y eliminarlas de nuestros dispositivos. Por eso, deben estar siempre actualizados.
3	¿Por qué debemos revisar los permisos que concedemos a las aplicaciones al instalarlas?	Ambas opciones
		Descargar una app maliciosa
4	Para poder utilizar aplicaciones antirrobo, es fundamental que tengamos activada la función de:	Descargar aplicaciones falsas
		Feedback: Utilizar tiendas no oficiales es siempre un riesgo, por eso debemos evitarlas. Además, es conveniente revisar los comentarios, valoraciones, número de descargas e información del desarrollador en las tiendas oficiales.
5	El bloqueo de aplicaciones nos puede ayudar a:	Para evitar que tengan acceso a demasiada información
		Para evitar funciones premium de la app
6	¿Cuál de las siguientes funciones está relacionada con los gestores de contraseñas?	Para evitar que haya conflicto con otras apps
		Feedback: Los permisos sirven para que la aplicación pueda funcionar correctamente. Sin embargo, a veces solicitan permisos de más que no debemos conceder para proteger mejor nuestra privacidad.
7	Para poder utilizar aplicaciones antirrobo, es fundamental que tengamos activada la función de:	Geolocalización
		Mapeado
8	El bloqueo de aplicaciones nos puede ayudar a:	Activación remota
		Feedback: Al activar la geolocalización, los servicios de Google e iOS podrán detectar nuestros dispositivos en caso de robo o pérdida. Por ello, es fundamental que lo activemos por seguridad.
9	El bloqueo de aplicaciones nos puede ayudar a:	Proteger su contenido de terceros
		Protegermos de un uso prolongado del dispositivo
10	¿Cuál de las siguientes funciones está relacionada con los gestores de contraseñas?	Evitar que se abran solas las apps
		Feedback: En caso de perder nuestro dispositivo o que un tercero nos lo robe y consiguiese desbloquearlo, seguiría teniendo otro obstáculo al no poder acceder a nuestras aplicaciones y la información almacenada, como las redes sociales, fotos, mensajes, etc.
11	¿Cuál de las siguientes funciones está relacionada con los gestores de contraseñas?	Ambas opciones
		Crear contraseñas robustas
12	¿Cuál de las siguientes funciones está relacionada con los gestores de contraseñas?	Cifrar nuestras credenciales

	<i>Feedback:</i> Los gestores nos ayudan a controlar todas nuestras cuentas, utilizar contraseñas robustas y además se protegen mediante cifrado para que nadie pueda acceder a nuestros usuarios y contraseñas a menos que tenga la clave maestra.	
7	La verificación en dos pasos nos ayuda a proteger nuestra privacidad. ¿Cómo lo hace?	Al requerir una clave temporal que se envía a otro dispositivo
		Al pedirnos dos contraseñas en lugar de una
		Ninguna es correcta
	<i>Feedback:</i> Con la verificación en dos pasos podemos vincular un segundo dispositivo para que el servicio que tenga esta función o una aplicación de verificación en dos pasos, nos envíe una clave temporal con la que iniciar sesión. Cuando introduzcamos nuestro usuario y contraseña, se nos solicitaría esta clave temporal para evitar que terceros consigan acceder a nuestras cuentas, incluso si tuviesen nuestra contraseña.	
8	A la hora de proteger nuestra privacidad en Internet, podemos utilizar:	Extensiones o <i>plugins</i>
		Navegadores de pago
		Ordenadores públicos
	<i>Feedback:</i> Estas extensiones pueden protegernos contra los anuncios maliciosos, detectar webs maliciosas, aplicaciones con virus o <i>malware</i> , así como ayudarnos a navegar sin dejar rastro.	
9	El cifrado de nuestro dispositivo móvil nos ayuda a:	Proteger la información almacenada de terceros.
		Mejorar el rendimiento de nuestro dispositivo.
		Crear copias de la información.
	<i>Feedback:</i> Un dispositivo cifrado protegerá toda la información almacenada, desde contactos, mensajes, fotografías, documentos hasta aplicaciones. De modo que, aunque un tercero se hiciese con nuestro teléfono o <i>tablet</i> , no podría ver su contenido ya que estaría cifrado.	
10	Entre las funciones de CONAN mobile, se encuentran:	Todas son correctas
		Analizar las aplicaciones instaladas
		Evaluar la configuración de nuestro dispositivo
	<i>Feedback:</i> La aplicación CONAN mobile analizará nuestro dispositivo en busca de vulnerabilidades, aplicaciones maliciosas y nos ayudará a mejorar su seguridad y nuestra privacidad con consejos y recomendaciones, además de un seguimiento a tiempo real sobre eventos que estén relacionados con nuestra protección.	

ANEXO

RECURSOS PARA AMPLIAR

Se recomienda la lectura de la siguiente selección de recursos complementarios, por parte del docente:

- [¡Ayuda! Instalé una app no fiable](#)
- [¡Conexión gratis a la vista! ¿Conecto mi móvil?](#)
- [¡No pierdas nada! Protege la información de tu dispositivo](#)
- [¿Cómo actuar si me han robado o he perdido el teléfono móvil?](#)
- [¿Has perdido el móvil? Cierra sesión en tus cuentas por prevención](#)
- [¿Para qué usamos los dispositivos móviles y qué información almacenan?](#)
- [¿Por qué piden tantos permisos las apps?](#)
- [Acepto o no lo acepto: revisando los permisos de las apps](#)
- [Blinda tu smartphone: apps de seguridad para tu dispositivo móvil](#)
- [Campaña ¿Es seguro dónde guardas y cómo envías la información?](#)
- [Cómo bloquear un dispositivo Android e iOS con biometría](#)
- [Cómo bloquear un dispositivo Android e iOS con biometría](#)
- [Cómo nos protegen los antivirus](#)
- [CONAN mobile](#)
- [Desinfecta tus dispositivos](#)
- [Empodérate: mantén seguros tus dispositivos y protégete en Internet](#)
- [Guía para configurar dispositivos móviles](#)
- [Permisos de apps y riesgos para tu privacidad](#)
- [Protege tu móvil iOS y Android con 5 consejos](#)
- [SIM Swapping o el fraude de la SIM duplicada](#)
- [Tecnología Motion Sense: desbloquea tu smartphone con un gesto](#)