Guía de ciberseguridad

La ciberseguridad al alcance de todos

Experiencia SENIOR

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA 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
GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR
DIRECCIÓN GENERAL DE LA POLICÍA
POLICÍA NACIONAL

Índice

Índice

La ciberseguridad al alcance de todos

La ciberseguridad es un tema cada vez más popular, ya que se centra en los **mecanismos y prácticas que sirven para proteger nuestros dispositivos y nuestra seguridad y privacidad cuando navegamos por la Red.**

A diferencia de lo que podamos pensar, la ciberseguridad **no requiere de grandes conocimientos informáticos o sobre redes, ni tampoco requiere equipos tecnológicos muy avanzados**, tan solo necesitamos nuestros dispositivos, sentido común y seguir paso a paso los consejos de esta guía.

¿Te atreves? Pues descubramos juntos cómo podemos convertirnos en usuarios ciberseguros. Ni la edad, ni los conocimientos que tengamos son un problema, **¡la ciberseguridad es para todos!**

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
017
OSI Oficina de Seguridad del Internauta
POLICÍA NACIONAL

1. Tus dispositivos y su seguridad

Hoy en día es raro que no dispongamos de, al menos, un teléfono móvil con conexión a Internet. La mayoría disponemos además de un ordenador o una tablet con la que navegar por la Red, jugar a juegos, comunicarnos con nuestros familiares y amigos, etc.

Lo más probable es que, además, los utilices para almacenar fotografías y vídeos o comprar en tiendas online y tengas algunos datos almacenados en tus dispositivos, ¿verdad? La cantidad de información que almacenan sobre nosotros es enorme debido al uso diario que hacemos de ellos, por eso es tan importante que aprendamos a salvaguardarla y proteger nuestros dispositivos de terceras personas con malas intenciones o para evitar que otras personas puedan acceder a su contenido sin nuestra autorización.

Para ello, existen una gran variedad de **mecanismos de protección** con los que limitar el acceso o ayudarnos en caso de pérdida o robo, así como para **proteger nuestros dispositivos de cualquier riesgo o amenaza** y ataques de los ciberdelincuentes.

Sin estas medidas de protección, nuestros dispositivos son vulnerables y **corremos el riesgo de que nuestra información más sensible acabe en malas manos,** como nuestros datos bancarios, fotos y vídeos personales con nuestra familia o amigos, conversaciones privadas… Además, **los ciberdelincuentes también intentan infectar nuestros dispositivos y tomar control para llevar acabo todo tipo de actividades ilícitas.**

1.1. Cómo actualizar tus dispositivos

En Windows | En Android | En MacOS | En iOS

Las actualizaciones **sirven para resolver fallos o vulnerabilidades que puedan ser aprovechados por los ciberdelincuentes.**

A continuación, vamos a ver los pasos para comprobar que nuestros dispositivos están debidamente actualizados.

En Windows (Versión 10)

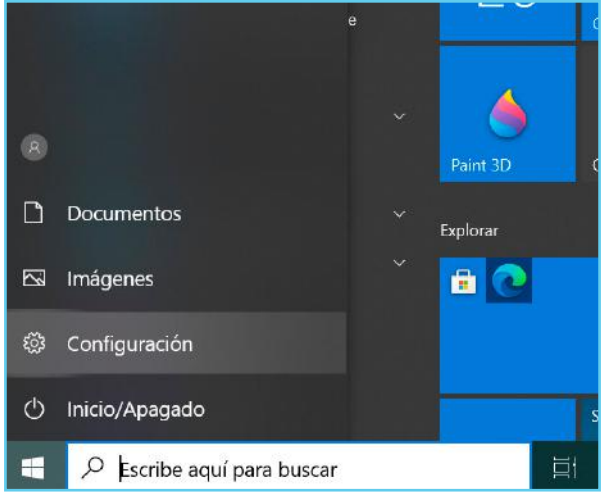
1. Haremos clic sobre el icono de Windows en la esquina inferior izquierda y pulsaremos sobre el icono de la rueda dentada o Configuración.

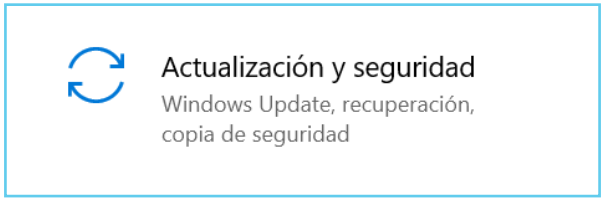
2. En la nueva ventana, seleccionaremos **'Actualización y seguridad'** para acceder a sus opciones.

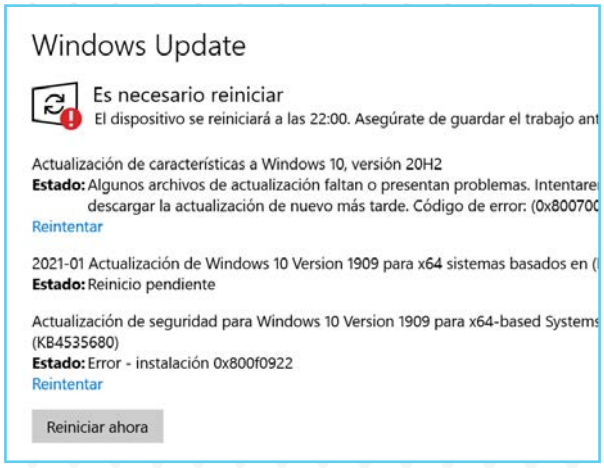
3. Luego, dentro del apartado **'Windows Update'**, podremos ver si disponemos o no de la última versión. En caso de que nos aparezca el texto **"No está todo actualizado"** podremos hacer clic sobre **'Buscar actualizaciones'** para descargar e instalar la última versión.

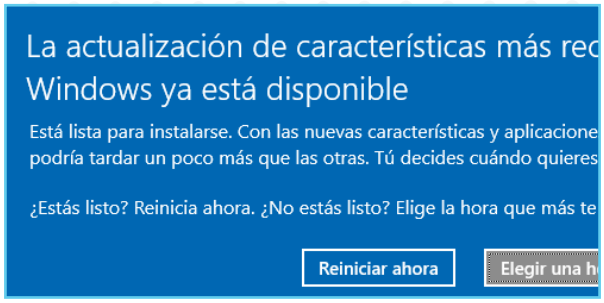
4. Podemos seleccionar la opción de **'Instalar actualizaciones tan pronto como sea posible'** para activar esta función e instalar cada actualización en el momento en que el fabricante la lance. Al finalizar la descarga e instalación, posiblemente nos solicite reiniciar el equipo. En ese caso, nos aseguraremos de cerrar cualquier programa que tengamos abierto y reiniciaremos.

Cuando haya una nueva actualización disponible, veremos iluminado el icono correspondiente en la esquina inferior derecha de nuestra pantalla y la notificación correspondiente (en la imagen nos informa de que ya se ha preparado la instalación y es necesario reiniciar el ordenador). El sistema nos avisa siempre que hay una actualización nueva.









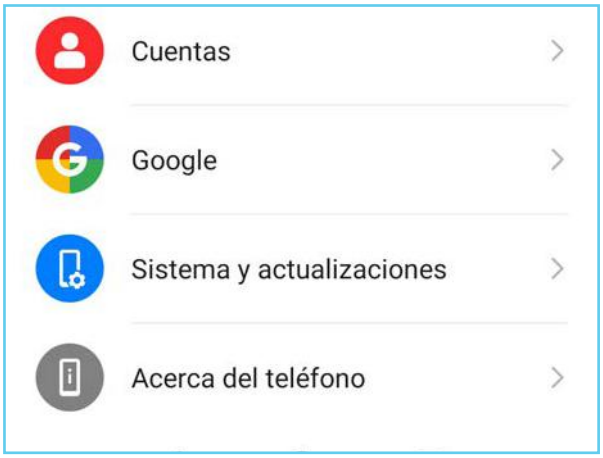
En Android

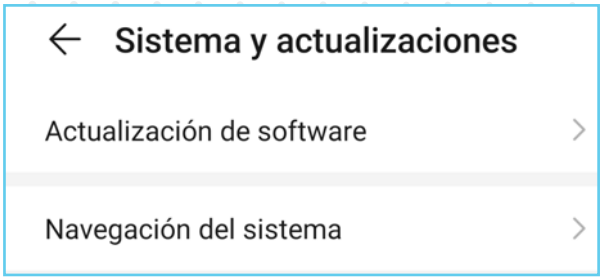
Los pasos a seguir pueden variar de una versión a otra, pero en esencia serán muy similares a los descritos a continuación:

1. Lo primero que haremos será pulsar sobre el icono de **'Ajustes'** de nuestro dispositivo.

2. Luego, buscaremos **'Sistema > Ajustes avanzados > Actualizaciones del sistema'.** Aquí podremos comprobar la versión de Android que tenemos instalada.

3. Si pulsamos en **'Comprobar actualizaciones',** se iniciará la comprobación y, en caso de que haya una nueva versión disponible, podremos descargarla e instalarla.



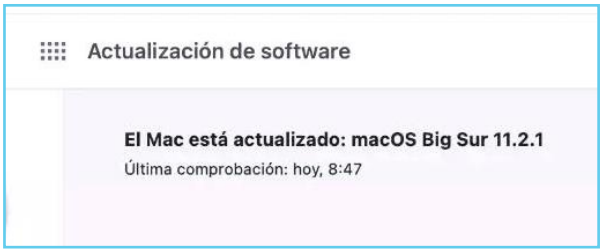


En MacOS

Dependiendo de la versión de Mac los pasos pueden variar ligeramente. Para estos pasos nos basaremos en la versión Big Sur.

1. Acceder al **'menú de Apple > Preferencias del Sistema > Actualización de software'.** Dentro, podremos comprobar las actualizaciones disponibles.

- **Si el mensaje que vemos nos indica que 'Mac ya está actualizado'**, eso implicará que tanto el sistema operativo, como todas las aplicaciones de Apple lo estarán.
- Si, por el contrario, al hacer clic en **'Actualizar ahora'**, el mensaje nos indica que hay una actualización pendiente, podremos descargarla e instalarla en el momento.



2. Finalmente, para asegurarnos siempre de disponer la última versión actualizada, es recomendable marcar la casilla **'Mantener mi Mac actualizado'**. De este modo, recibiremos una notificación cada vez que haya una nueva versión pendiente de instalar.

En iOS

1. Iremos a **'Ajustes > General y buscaremos la opción Actualización de software'.**

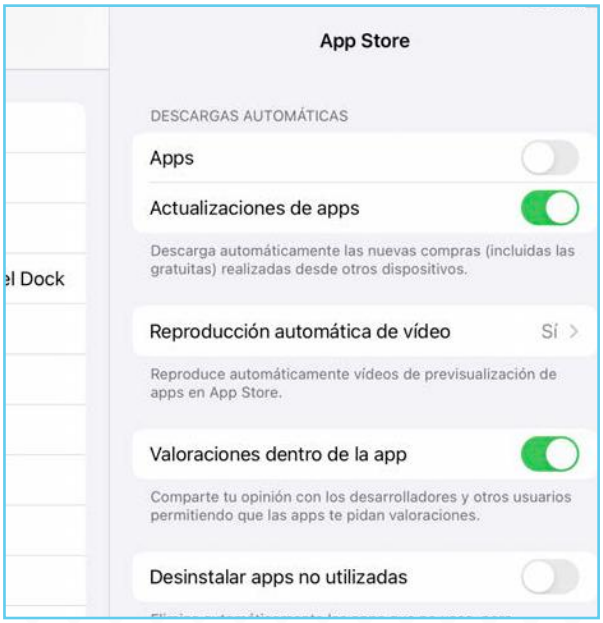
2. Aquí veremos nuestra versión actual de iOS. Si pulsamos sobre **'Descargar e instalar'**, comenzará la descarga de la nueva actualización. En caso contrario, nos informará de que disponemos de la última versión.

3. Es recomendable activar la **'Actualización automática'** del software del dispositivo. De este modo, siempre tendremos la tranquilidad de que nuestro dispositivo dispone de la última versión. Para ello, debemos seleccionar la casilla de **'Personalizar las actualizaciones automáticas / Actualizaciones automáticas'.**

Cada vez que haya una nueva versión, nuestro dispositivo nos informará y podremos descargarla e instalarla en ese momento o más tarde.

4. Para actualizar todas aquellas apps que hemos instalado a través de la App Store, como redes sociales, juegos u otras aplicaciones.

Para ello, deberemos volver al menú de **'Ajustes > App Store'** y activar la función **'Actualizaciones de apps'.**



1.2. Cómo comprobar que tus dispositivos están protegidos (antivirus)

En Windows | En Android | En MacOS | En iOS

La mayoría de dispositivos ya **cuentan con herramientas de protección contra diferentes amenazas.** El antivirus es nuestra principal protección contra ellas y es el mejor filtro que podemos tener para detectar y eliminar cualquier tipo de virus o malware.

1.2. Cómo comprobar que tus dispositivos están protegidos (antivirus)

En Windows (Versión 10)

Nuestro sistema trae varias herramientas de protección ya preinstaladas.

1. Haremos clic en el **icono de Windows**, abajo a la izquierda, y seleccionaremos el icono de la rueda dentada **'Configuración'**.

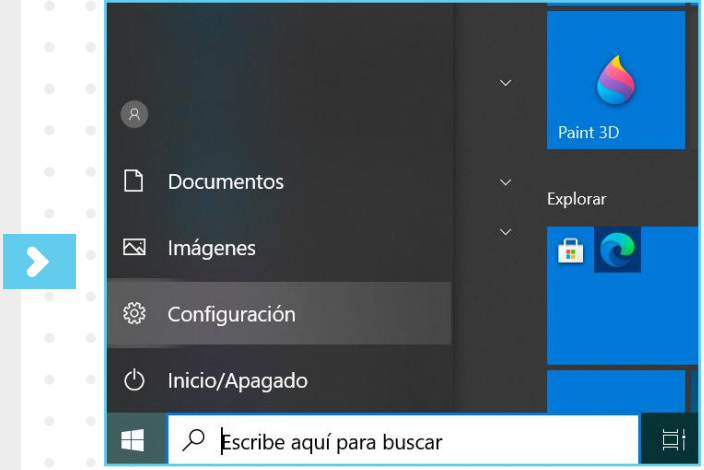
2. A continuación, seleccionaremos el apartado de **'Actualización y seguridad'**.

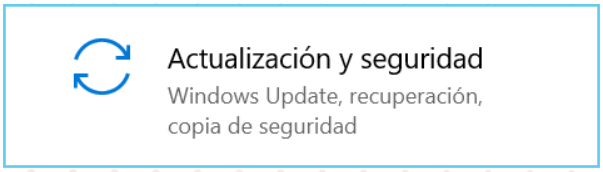
3. Nos aparecerá una nueva ventana donde seleccionaremos la opción **'Seguridad de Windows'** en el menú que aparece a la izquierda.

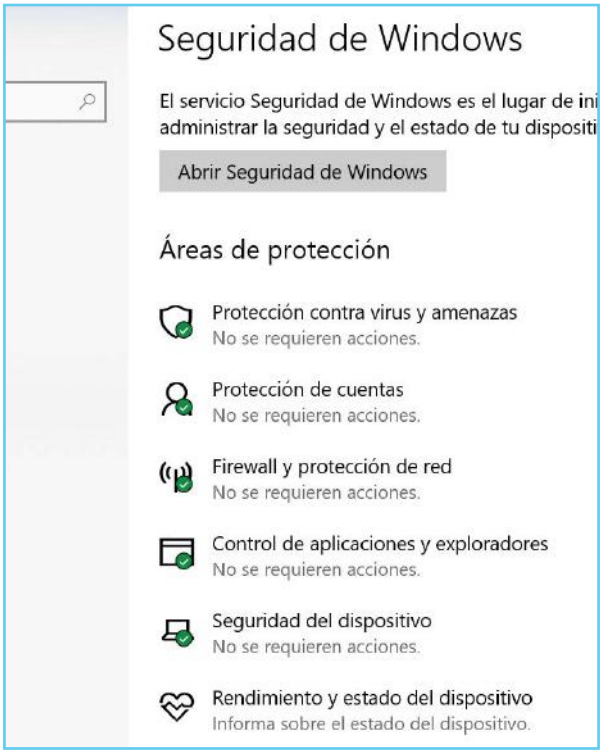
Aquí encontraremos las distintas áreas de protección disponibles, como la **'Protección contra virus y amenazas'**. Sabremos si esta y otras funciones de seguridad están activas, porque aparecen con un círculo verde con un check (marca de confirmación) dentro.

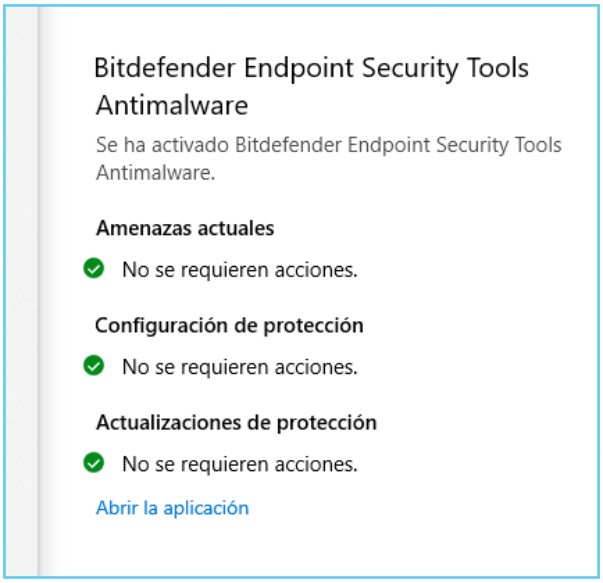
4. Dentro de la opción **'Protección contra virus y amenazas'** veremos las diferentes protecciones que nos ofrece el antivirus que viene instalado por defecto, Windows Defender, y si están activadas o configuradas.

También podremos, por ejemplo, realizar un examen rápido del ordenador para confirmar que está limpio (libre de virus).









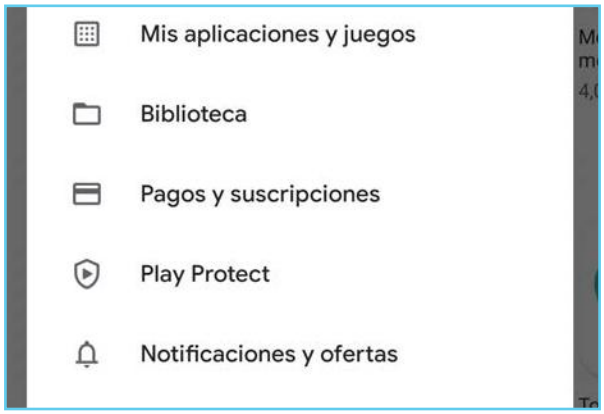
1.2. Cómo comprobar que tus dispositivos están protegidos (antivirus)

En Android

La herramienta Google Play Protect sirve para protegernos de las amenazas a las que nos exponemos. Para comprobar que está activada.

1. Lo primero será acceder a la aplicación **'Play Store'** y pulsar sobre el icono de menú de la esquina superior derecha: icono con nuestra inicial.

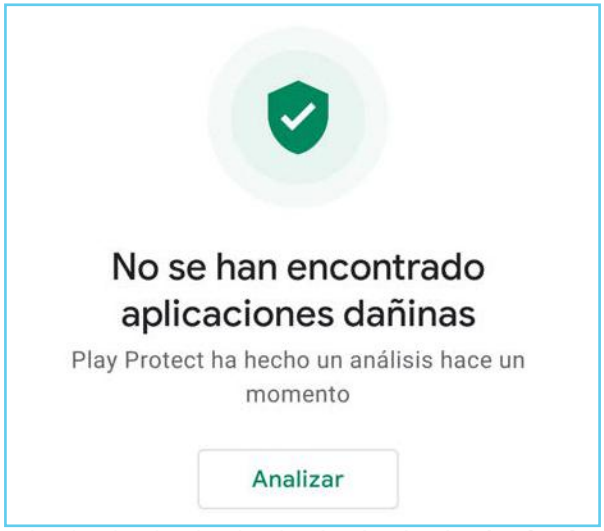
2. Luego, pulsaremos sobre la opción de **'Play Protect'.** Una vez dentro, veremos el estado en el que se encuentra nuestro dispositivo y las aplicaciones instaladas. Si todo está bien, deberíamos ver **'No se ha encontrado ningún problema'.**



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 dentada de la esquina superior derecha.**

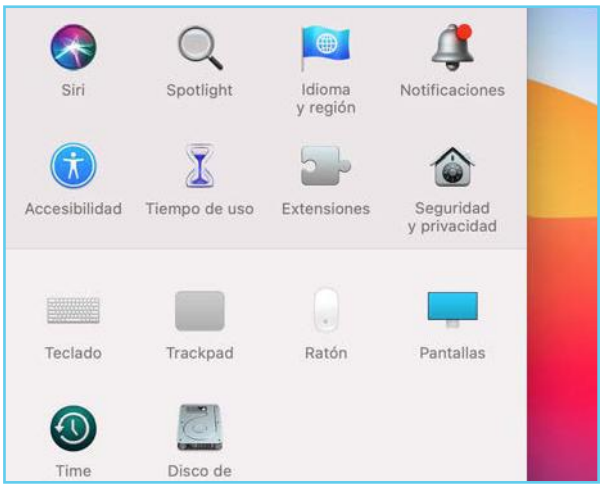


Al activarlas, aparecerá en color verde, y esto significará que Google estará monitorizando las aplicaciones que instalamos en busca de posibles amenazas.

En MacOS

Los ordenadores de Apple también disponen de herramientas de protección preinstaladas.

1. Iremos al **'menú de Apple > Preferencias del Sistema'** y haremos clic en **'Seguridad y privacidad > General'.**

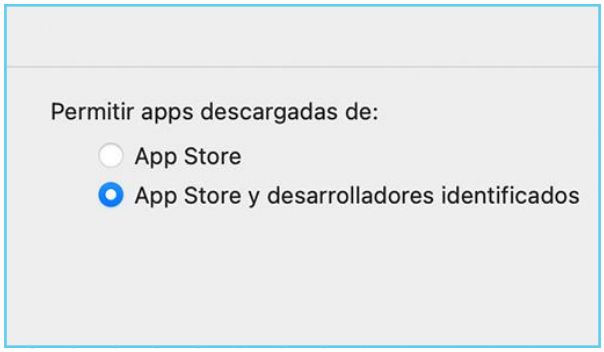


1.2. Cómo comprobar que tus dispositivos están protegidos (antivirus)

2. Si vemos un candado bloqueado en la esquina inferior izquierda, haremos clic en él para **desbloquear el panel de 'Preferencias'.**

3. Tras identificarnos (introducir nombre de usuario y contraseña), podremos seleccionar las fuentes desde las que permitiremos que se instalen las aplicaciones. En este caso seleccionaremos **'App Store'** para permitir únicamente aplicaciones que descarguemos desde la App Store.

Es la opción más segura, ya que estas aplicaciones pasan por filtros de seguridad muy estrictos, con el objetivo de prevenir que aplicaciones maliciosas se publiquen en la tienda oficial de descargas.



En iOS

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.

1. Para ello, deberemos ir a **'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.
Tampoco debemos olvidarnos de mantener las aplicaciones actualizadas para corregir posibles errores de seguridad.

1.3. Cómo comprobar que dispone de un bloqueo de acceso

En Windows | En Android | En MacOS | En iOS

Una de las primeras configuraciones de seguridad que realizamos cuando encendemos por primera vez nuestro equipo es el bloqueo de acceso, ya sea mediante un PIN, un patrón o una clave de seguridad. **El bloqueo de nuestros dispositivos es fundamental para nuestra seguridad.**

A continuación, vamos a hacer un repaso sobre los métodos de bloqueo presentes en los diferentes sistemas.

1.3. Cómo comprobar que que dispone de un bloque de acceso

En Windows (Versión 10)

En los dispositivos con Windows 10 (y versiones anteriores) podemos crear varias cuentas de usuario para que todos los miembros de la casa puedan utilizar un mismo equipo:

1. En Windows existen principalmente dos tipos de cuentas: **las cuentas de administrador**, que son capaces de realizar modificaciones dentro del sistema y **las cuentas de usuario**, que no disponen de tantos privilegios y se crean para el disfrute del equipo.

2. La posibilidad de crear múltiples cuentas implica que cada usuario tenga la suya. Si estas cuentas no están debidamente protegidas, **cualquier usuario podría acceder a la información personal del resto, incluso un tercero con malas intenciones.**

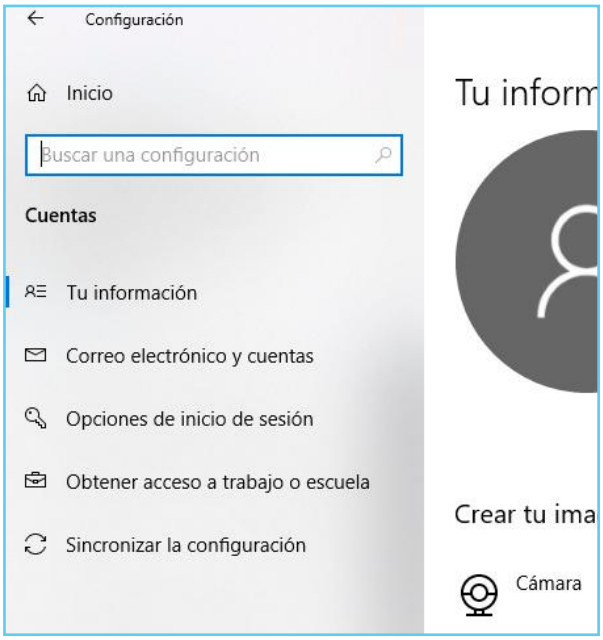
Para evitarlo, debemos **configurar las opciones de bloqueo** de nuestra sesión:

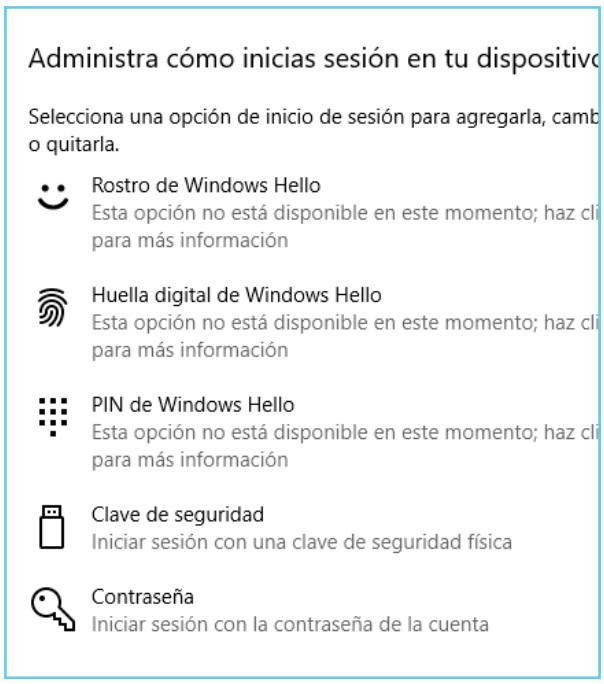
1. Deberemos hacer clic sobre el icono de **'Windows > Configuración'.**

2. Luego, pulsaremos sobre **'Cuentas > Opciones de inicio de sesión'.**

3. Aquí veremos varias opciones, aunque su disponibilidad dependerá del tipo de ordenador y de si tenemos permisos de administrador:

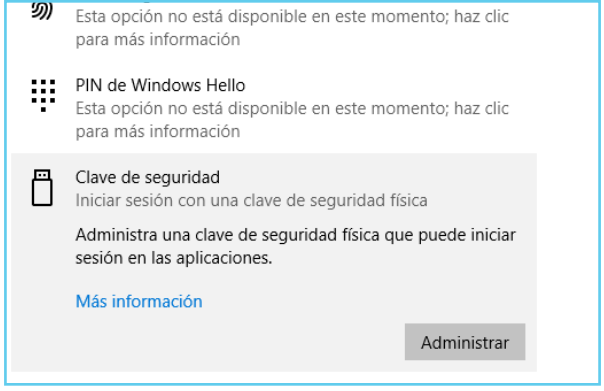
- **Rostro de Windows Hello:** podremos utilizar nuestro rostro para bloquear/ desbloquear nuestro equipo.
- **Huella digital de Windows Hello:** en este caso, utilizaremos nuestra huella dactilar.
- **PIN de Windows Hello:** podremos escoger un código PIN (clave numérica de al menos 4 caracteres), aunque es la opción menos segura.
- **Clave de seguridad:** se trata de una clave física, que se instala dentro de un dispositivo, como una memoria USB, y que necesitamos conectar al equipo para iniciar sesión.





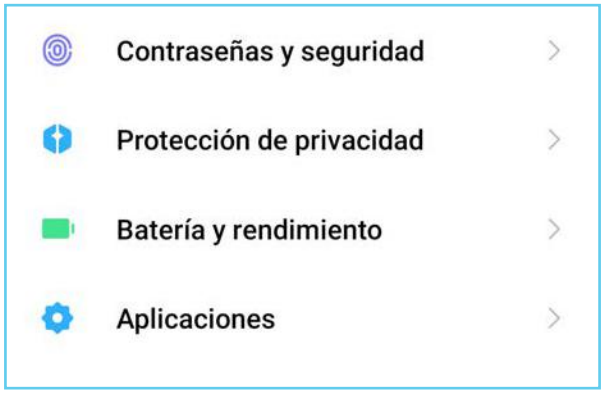
1.3. Cómo comprobar que que dispone de un bloque de acceso

- **Contraseña:** podremos cambiar la contraseña que creamos junto con la cuenta de usuario, es decir, la que utilizamos para desbloquear el ordenador.



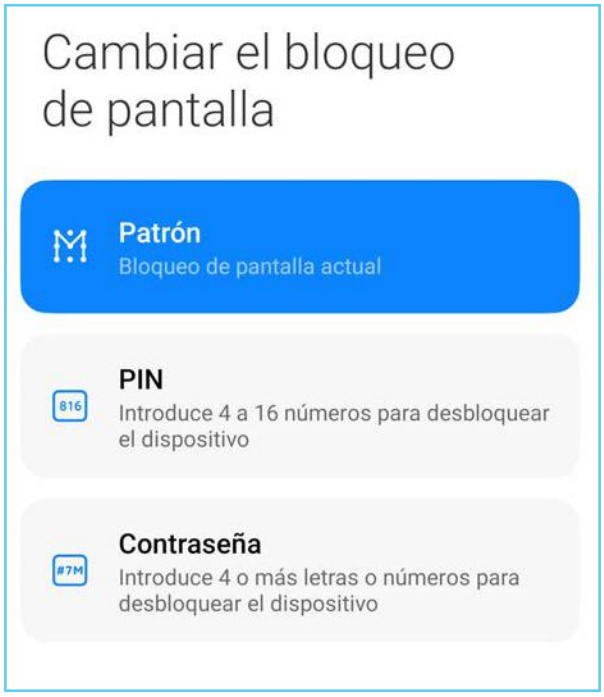
En Android

1. Abriremos la aplicación **'Ajustes'** (icono de una rueda dentada), que podemos encontrar en el escritorio o en la pantalla de menú, y seleccionaremos la opción **'Contraseña y seguridad'**. Buscaremos la sección de 'Seguridad' y, a continuación, **'Bloqueo de pantalla'.**



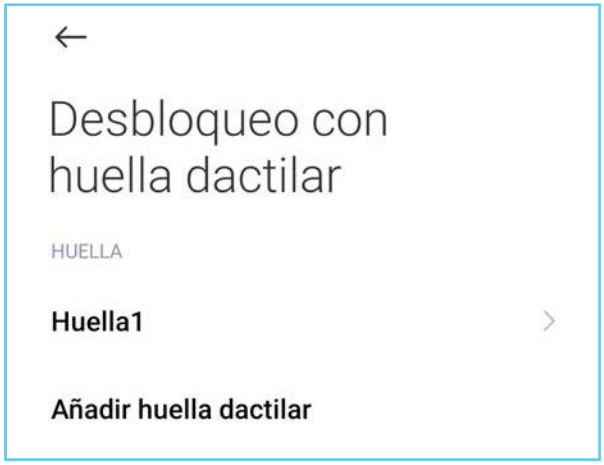
Si pulsamos sobre **'Contraseñas',** accederemos a los diferentes tipos de bloqueo de pantalla:

- **Patrón:** consiste en un dibujo trazado uniendo una serie de nueve puntos en forma de un cuadrado de 3x3. Es la opción menos segura, ya que cualquiera puede ver el trazo en la pantalla.
- **PIN:** se trata de una clave de al menos 4 dígitos. Te recomendamos no utilizar el mismo PIN de la tarjeta SIM o la del banco.
- **Contraseña:** se trata de una clave de al menos 4 dígitos y letras. Debemos utilizar una contraseña difícil de averiguar y única para el dispositivo.



Las otras opciones son:

- **Desbloqueo con huella dactilar:** nuestro dispositivo dispone de un lector de huella dactilar. Puede utilizarse para que una o varias huellas dactilares desbloqueen nuestro móvil o tablet simplemente poniendo el dedo sobre el lector de la huella.
- **Desbloqueo facial:** nuestro dispositivo es capaz de reconocer rostros mediante la cámara frontal. Podemos añadir nuestro rostro o el de otros usuarios como mecanismo de desbloqueo.
- **Desbloquear con dispositivo Bluetooth:** podremos utilizar otro dispositivo inteligente para desbloquear nuestro móvil o tablet,



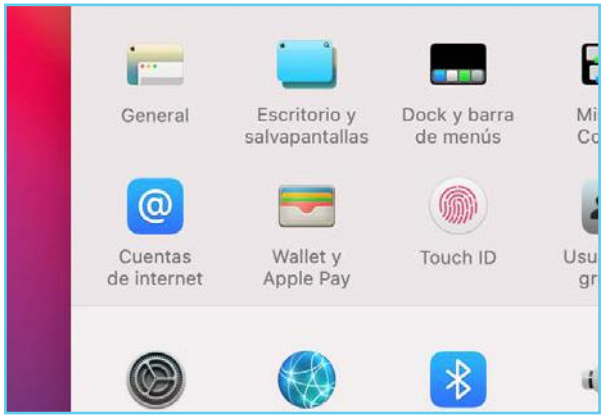
como una pulsera de actividad o reloj inteligente.

2. Cuando hayamos escogido la opción deseada, preferiblemente las últimas opciones, deberemos **seguir los pasos** para configurarla e implementarla como mecanismo de desbloqueo. Nuestro dispositivo nos solicitará que configuremos más de un método de desbloqueo para poder utilizarlo en el caso de que el primero falle y como medida de seguridad extra.

En MacOS

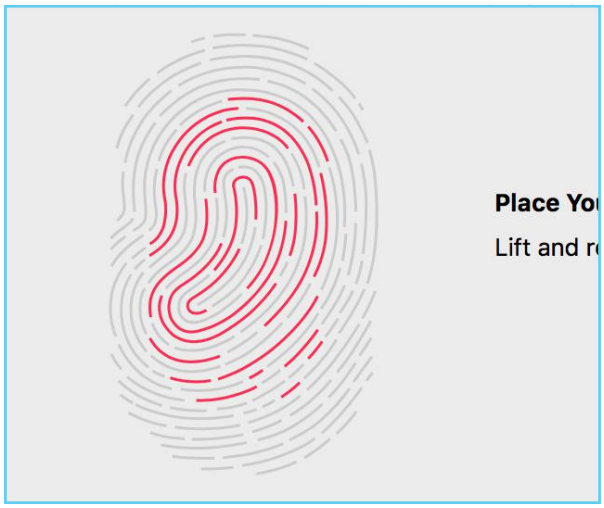
En las versiones más modernas de **macOS (Big Sur 11.0)** es posible utilizar otros mecanismos de bloqueo y desbloqueo de nuestra sesión:

- **Touch ID:** Nuestro dispositivo deberá estar dotado de un lector de huella.
Esta configuración nos permitirá utilizar nuestra huella dactilar para desbloquear el dispositivo. Para ello:



1. Iremos al **'menú Apple > Preferencias del Sistema'** y seleccionaremos **'Touch ID'.**

2. Haremos clic en **'Añadir huella'** y, tras introducir nuestra contraseña, seguiremos las instrucciones.



1.3. Cómo comprobar que que dispone de un bloque de acceso

En iOS

1. Accederemos a **'Ajustes'** (icono de una rueda dentada), que podemos encontrar en el escritorio, y seleccionamos **'ID de Apple > Contraseña y seguridad > Cambiar contraseña'.**

Desde aquí podremos cambiar la clave a una más robusta, estableciéndola como mínimo de 8 caracteres, incluyendo al menos una mayúscula, una minúscula y un número; por ejemplo: Milph0ne11.

2. Dentro de **'Ajustes'** buscaremos las opciones **'Touch ID o Face ID'** (en los modelos más nuevos). Dentro podremos:

- Activar el desbloqueo del iPad/iPhone.
- Añadir una nueva huella o nuestro rosto con alguna modificación.
- Solicitar el código (contraseña) como medida de seguridad adicional.

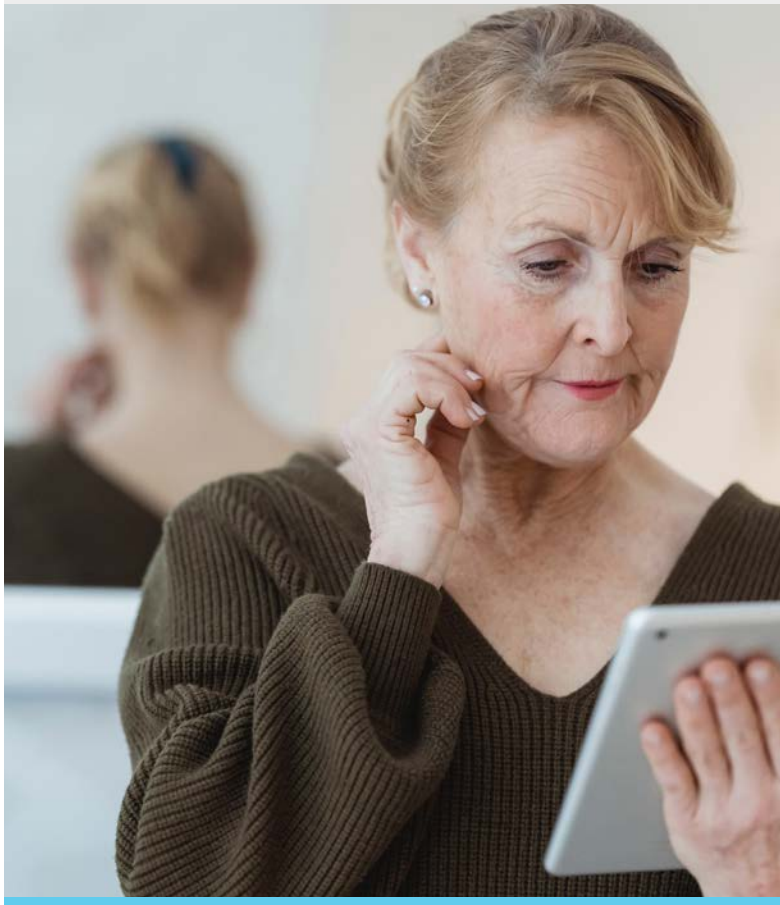
3. También podremos configurar el tiempo que el dispositivo estará inactivo antes de activarse el bloqueo automático. Para ello, iremos a **'Ajustes > Pantalla y brillo',** donde encontraremos la opción de **'Bloqueo automático'.**

1.4. Cómo comprobar que tus dispositivos están cifrados

En Windows | En Android | En MacOS | En iOS

El cifrado de dispositivos **es un mecanismo de protección que protege todo el contenido del mismo,** cifrándolo y volviéndolo inaccesible ante terceros.

Es muy útil para evitar que el contenido de nuestros dispositivos caiga en malas manos, especialmente si son dispositivos móviles, ya que pueden perderse.



1.4. Cómo comprobar que tus dispositivos están cifrados

En Windows (Versión 10)

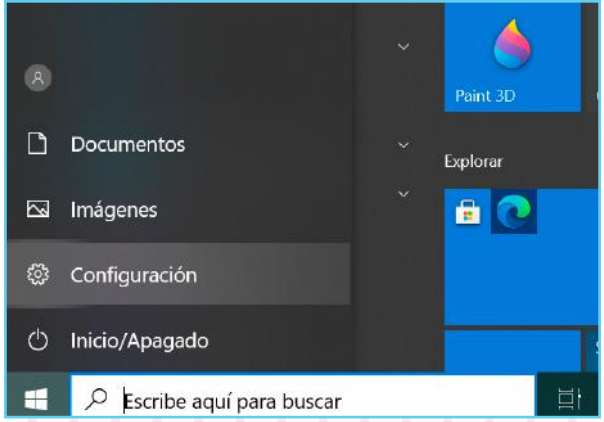
Para activar el cifrado de nuestro dispositivo en Windows 10 necesitaremos acceder con una cuenta administrador y seguir estos pasos:

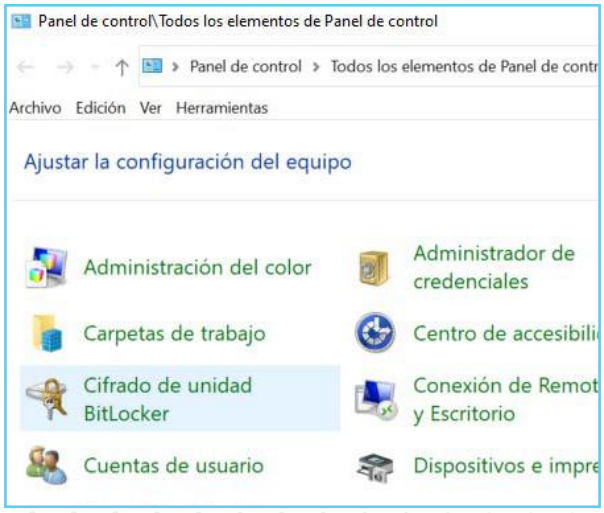
1. Pulsaremos sobre el **'icono de Windows'** y, a continuación buscaremos entre los resultados la carpeta **'Sistema Windows > Panel de control'.**

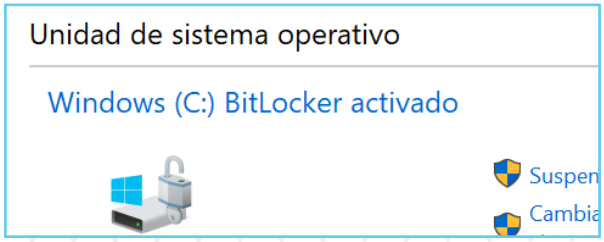
2. Dentro, seleccionaremos **'Cifrado de unidad BitLocker > Administrar BitLocker'.**

3. Luego, deberemos activarlo y seguir las instrucciones. En el caso de que nos aparezca activado, también podremos desactivarlo.

4. Al activarlo, nos solicitará una clave maestra con la que descifrar nuestro dispositivo que deberemos introducir al encender nuestro equipo.







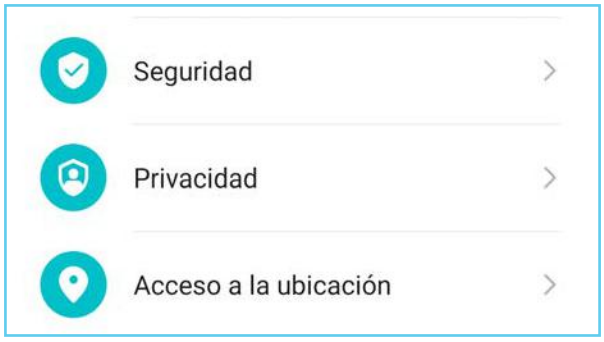
En Android

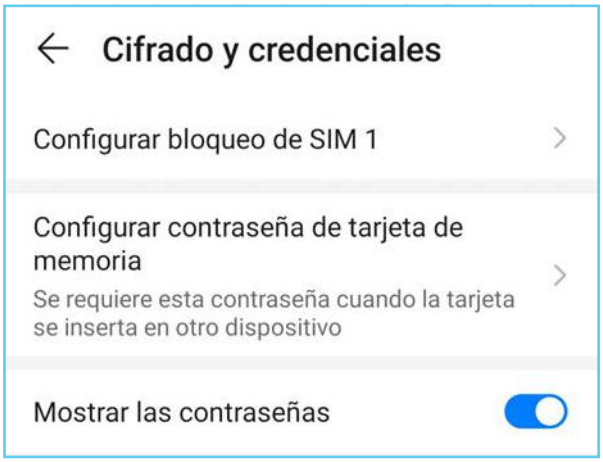
El procedimiento puede variar ligeramente dependiendo de la versión de nuestro sistema, pero podremos seguir los pasos sin problema:

1. Iremos a **'Ajustes'** de nuestro dispositivo y buscar las opciones de **'Seguridad'.**

2. Una vez localizado, pulsaremos sobre la opción **'Cifrado y credenciales > 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 almacenada en dispositivos de almacenamiento externo, como una tarjeta MicroSD, quedará totalmente cifrada. En este caso, si quisiésemos utilizar la tarjeta en otro dispositivo, tendríamos que descifrarla primero utilizando la contraseña o PIN que hemos creado previamente.





1.4. Cómo comprobar que tus dispositivos están cifrados

En MacOS

Los dispositivos de Apple cuentan con una herramienta conocida como FileVault que cifra todo el contenido de archivos del equipo. Para utilizarlo, deberemos:

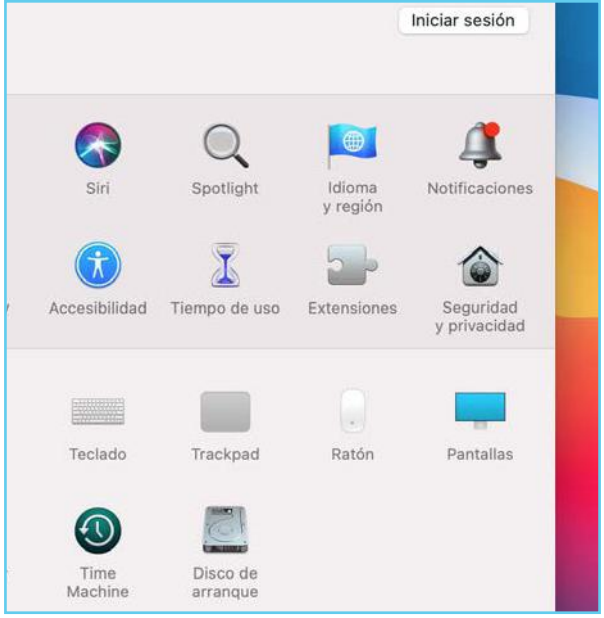
1. Acceder a Preferencias del **'Sistema > Seguridad > FileVault'.** Al hacerlo, tendremos que configurar una **contraseña robusta de encriptación** que nos permitirá acceder y descifrar el sistema, y activar el **'sistema FileVault'.**

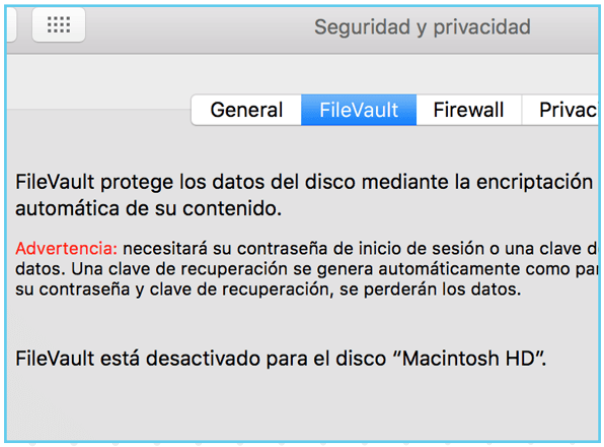
2. Al activarlo, deberemos seleccionar cómo desbloquear el disco y restablecer la contraseña de inicio de sesión en caso de que la olvidemos, por seguridad:

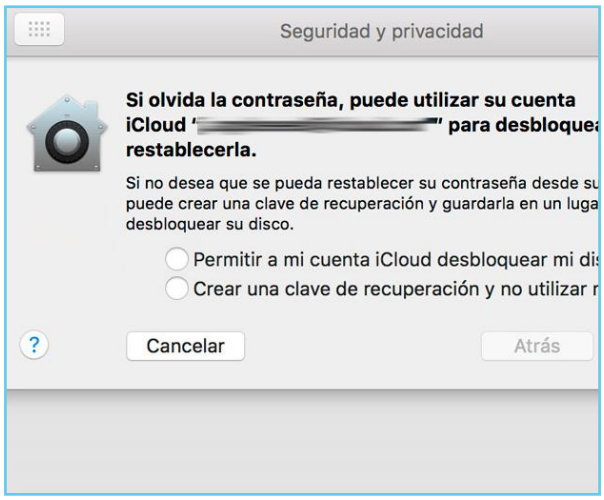
- **Cuenta de iCloud:** al pulsar en 'Permitir desbloquear mi disco desde mi cuenta de iCloud', podremos emplearla en lugar de una contraseña.
- **Clave de recuperación:** al seleccionar 'Crear una clave de recuperación y no utilizar mi cuenta iCloud', deberemos recordar y guardar en un lugar seguro esta clave, pues nos servirá para recuperar el acceso a nuestros archivos.

3. Luego, el sistema **empezará a cifrar todo nuestro dispositivo**, lo que le llevará un tiempo dependiendo de la cantidad de archivos almacenados.

4. Finalmente, el contenido estará protegido, y deberemos **ingresar la contraseña** que creamos anteriormente siempre que queramos acceder a su contenido.







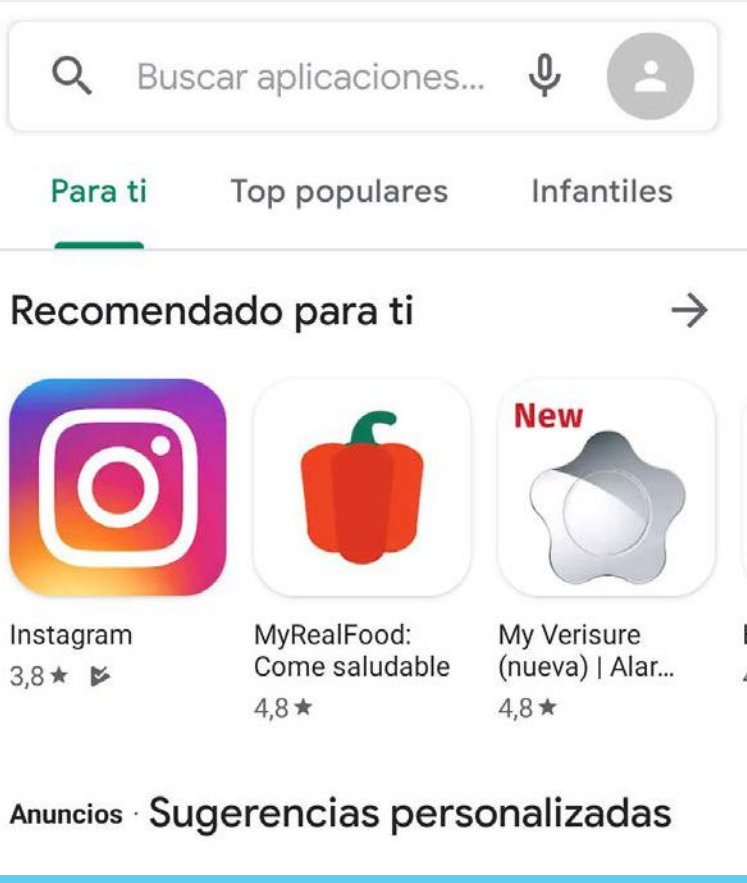
En iOS

Todos los dispositivos móviles de la marca Apple están cifrados por defecto sin que tengamos que hacer nada.

1.5. Cómo descargar aplicaciones y programas sin riesgo

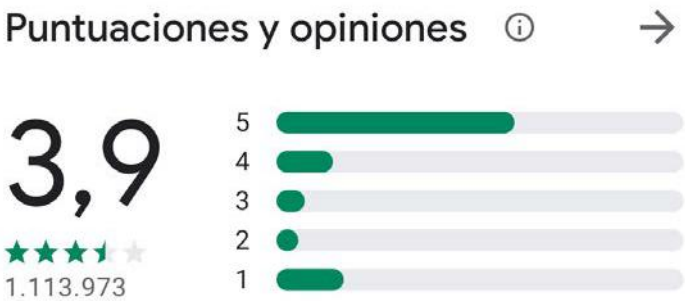
A la hora de descargar aplicaciones, **lo más importante es que lo hagamos siempre desde las tiendas oficiales**. Por defecto, todos los dispositivos móviles Android, iOS (iPhone/iPad) u otros sistemas como Windows o Apple, cuentan con aplicaciones preinstaladas para descargar otras aplicaciones: Play Store, App Store o Microsoft Store.

Aunque estas **tiendas oficiales cuentan con filtros de protección, no son 100% infalibles,** por lo que debemos seguir una serie de pautas a la hora de descargar alguna app:



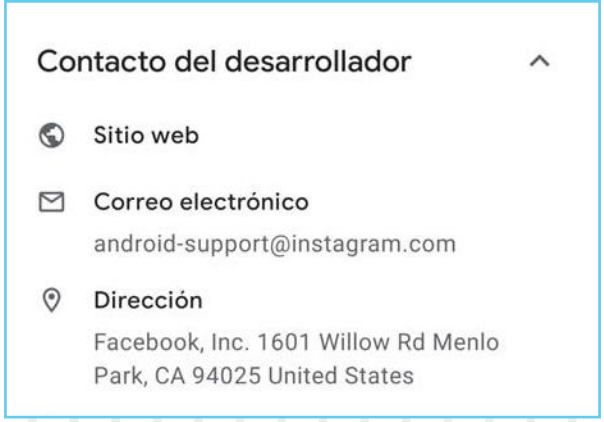
1. Mirar el número de descargas que tiene la aplicación. De este modo, podremos guiarnos por las aplicaciones que ha descargado la mayoría de usuarios.

2. Analizar los comentarios y valoraciones de la aplicación antes de descargarla. Echar un vistazo a los comentarios de otros usuarios nos puede dar pistas sobre qué tipo de aplicación es, si funciona bien, si es fiable, etc.

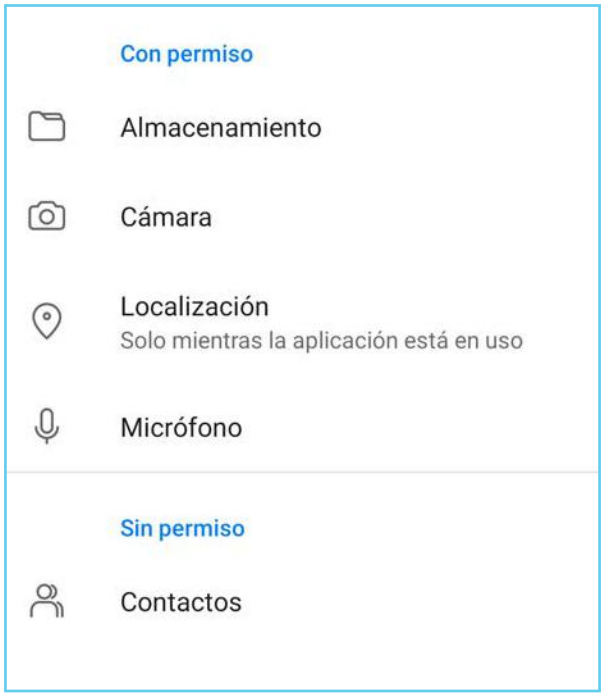


1.5. Cómo descargar aplicaciones y programas sin riesgo

3. Comprobar quién ha creado la aplicación. Es recomendable revisar la página web de la empresa que ha creado la aplicación o buscarla en Google para consultar información sobre la misma y ayudarnos a tomar una decisión a la hora de descargarla.



4. Revisar los permisos que solicita la aplicación al instalarse. Una aplicación para editar fotos o vídeos no debería pedirnos permisos para acceder a nuestros contactos para funcionar, ¿verdad?



También es probable que **descarguemos programas desde Internet**, sin depender de tiendas oficiales, por ejemplo desde nuestro ordenador o portátil. En estos casos, deberemos:

1. Actualizar nuestro equipo y herramientas de protección. Así nos aseguraremos de disponer de la última versión de nuestro sistema y antivirus.

2. Descargar solo de las webs del fabricante. En Internet abundan las webs falsas o dedicadas a publicar software ilegal o "pirata". Debemos huir de ellas y recurrir solo a webs legítimas del fabricante o distribuidores oficiales. **Más adelante en la guía veremos cómo identificar este tipo de webs fraudulentas.**

3. Analizar el programa descargado con el antivirus antes de instalarlo. Cualquier antivirus nos permitirá analizar un archivo simplemente haciendo clic derecho sobre él y pulsando sobre **'Analizar/Examinar con...'.**

Si aún tenemos dudas, en este enlace* encontraremos un recurso para practicar y no dejarnos engañar por las apps fraudulentas.

*https://www.osi.es/es/campanas/dispositivos-moviles/acepto-no-acepto

2. Protege tus cuentas y tu información (buenas prácticas)

1.1. Cómo crear contraseñas robustas
2.2. Cómo funciona la verificación en dos pasos

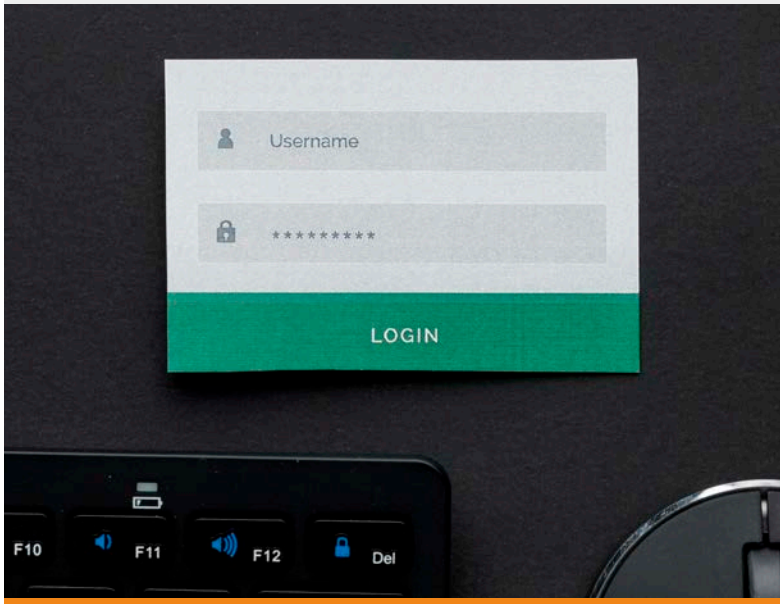
Uno de los primeros pasos que los usuarios damos cuando adquirimos un nuevo dispositivo o accedemos a Internet por primera vez es la creación de nuestras cuentas de usuario. Para ello, necesitamos un correo electrónico y una contraseña con la que registrarnos y, posteriormente, identificarnos, ya que estas cuentas suelen contener una gran cantidad de datos personales: nuestro correo, nombre y apellidos, dirección, datos de nuestra tarjeta bancaria, etc.

Para protegerlas, **podemos recurrir a buenas prácticas** y así evitar cometer despistes o vulnerar la seguridad de nuestra cuenta, o **mecanismos de seguridad que añadirán una capa extra de protección** a nuestra cuenta.

Esto nos ayudará a evitar los principales riesgos y amenazas a los que se enfrentan nuestras cuentas de usuario, como la **suplantación de nuestra identidad**, por ejemplo, si un ciberdelincuente consiguiese acceso a nuestro correo electrónico para engañar a los usuarios, o el **robo de información personal** almacenada en dichas cuentas.

2.1. Cómo crear contraseñas robustas

Las contraseñas **son nuestra primera línea de defensa para proteger nuestros dispositivos y nuestras cuentas**. Por eso es tan importante saber cómo crear contraseñas robustas que impidan a los ciberdelincuentes adivinarlas.



Vamos a ver cómo construir una contraseña robusta desde cero:

1. Pensar una frase de 10 caracteres mínimo. Puede tener significado para nosotros o simplemente unir 2 o 3 palabras al azar, pero que nadie más conozca:
Mi cuenta segura

2. Alternar mayúsculas y minúsculas. Unimos las palabras y resaltamos las iniciales con mayúsculas:
MiCuentaSegura

3. Sustituir letras por números. Un truco es intercambiar algunas letras por cifras, como "o" por 0, "i" por 1, "e" por 3 o "a" por 4:
M1Cu3nt4S3gur4

1.1. Cómo crear contraseñas robustas
2.2. Cómo funciona la verificación en dos pasos

2.1. Cómo crear contraseñas robustas

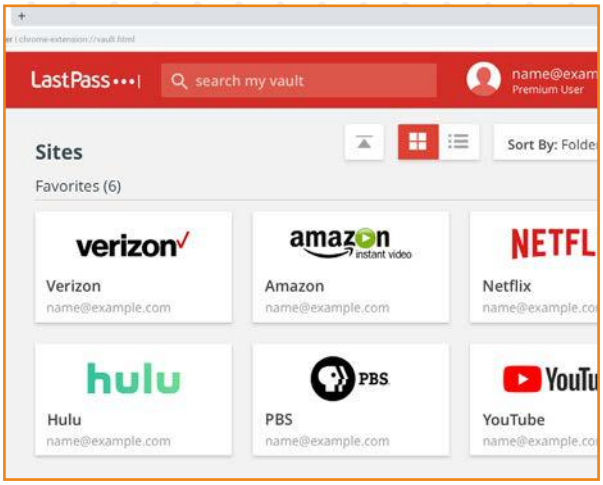
4. Añadir caracteres especiales. Solo queda incluir algún símbolo (~! @ # $% ^& * -+ = ' | \ \ ( ) { }\ [ ]:; "' < >,.? /).:
M1Cu3nt4S3gur4!

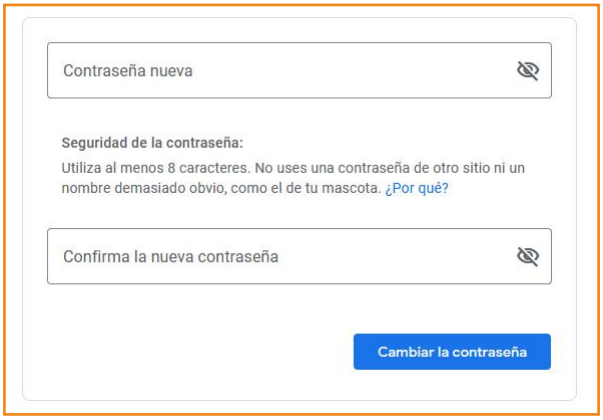
5. Personalizar la clave para cada servicio. Podemos utilizar las dos primeras letras del servicio y una la ponemos al principio y otra al final de la clave, ambas en mayúsculas. Ejemplo: si el servicio se llama "Mailbook", usaremos la M y la A:
MM1Cu3nt4S3gur4!A

Además, debemos recordar seguir estas pautas para minimizar riesgos:

- Utilizar gestores de contraseñas.
- No repetir la misma contraseña en distintas cuentas.
- Actualizarlas cada cierto tiempo. Lo recomendable es cada 3 meses.
- No compartirlas con nadie, ni amigos ni familiares.

Podremos aprender a crear contraseñas seguras si seguimos los consejos y el paso a paso de este recurso*.





*https://www.osi.es/campanas/crea-tu-contrasena-segura

2.2. Cómo funciona la verificación en dos pasos

La verificación en dos pasos es un **mecanismo de protección adicional a la hora de iniciar sesión en nuestras cuentas online**, evitando que alguien sin autorización acceda a nuestra cuenta. Al activarla, será necesario facilitar un código para autenticarnos, además de nuestras credenciales.

Existen muchos servicios y plataformas que ya cuentan con un sistema de verificación en dos pasos propio. **Dentro de la Configuración / Ajustes de nuestra cuenta podremos habilitarlo** y añadir un dispositivo, teléfono o canal adicional para el envío del código de autenticación.

Otra opción es utilizar aplicaciones de terceros, como Google y su 'Google Authenticator' o Microsoft con 'Microsoft Authenticator'. Para utilizarlas, deberemos seguir estos pasos:

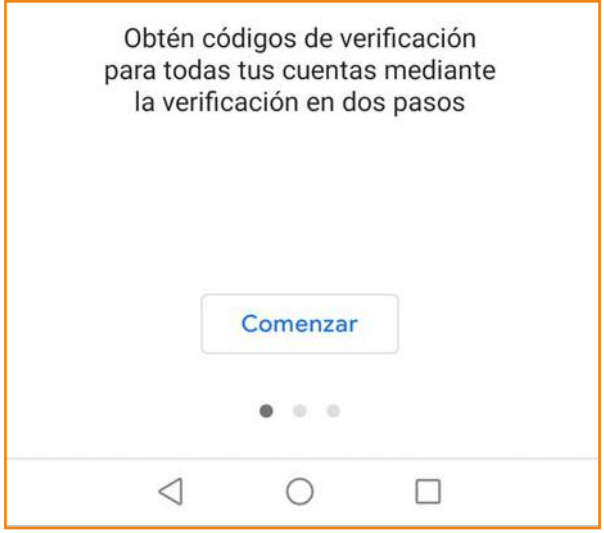
Descarga Disponible
Google play

Descarga Disponible
App Store

1. Descarga la aplicación. Estas aplicaciones se pueden descargar en Google Play y App Store para nuestras cuentas de Gmail, Amazon, Facebook, Outlook, PayPal, Dropbox o Twitter.

2.2. Cómo funciona la verificación en dos pasos

2. Instalar y crear una cuenta. Una vez instalada la aplicación, lo primero que nos solicitará es crear nuestra primera cuenta, para lo cual dispondremos de dos opciones posibles: mediante un código QR o una clave. Ambas alternativas las podemos obtener desde el propio servicio o cuenta que queramos proteger, siempre y cuando el servicio lo permita.



Por ejemplo, en el caso de Facebook, deberemos hacer clic en **'Configuración > Seguridad e inicio de sesión > Usar la autenticación en dos pasos > Usar aplicación de autenticación'.**

3. Ingresa el código. Una vez vinculada la cuenta del servicio con nuestra app de verificación en dos pasos, cada vez que queramos iniciar sesión, además de la contraseña, deberemos ingresar el código que obtendremos en nuestra app.

Estas claves son temporales y cambian transcurridos unos segundos, lo que dificultará mucho más el trabajo de los ciberdelincuentes.

Si queremos más información, la podremos encontrar en este enlace* sobre cómo instalar y utilizar estas apps de verificación en dos pasos.

*https://youtu.be/oFzKEogQEsI

3. Acceder a Internet y navegar de forma segura

Internet se ha convertido en una necesidad para llevar a cabo numerosas actividades en nuestro día a día, desde pedir una cita online o realizar nuestras compra, hasta comunicarnos con nuestros seres queridos.

Hoy en día, prácticamente cualquiera de nuestros dispositivos es capaz de conectarse a Internet, como nuestro teléfono móvil o nuestro ordenador. Solo necesitamos un dispositivo inteligente y un programa que nos permita acceder a Internet, conocido como navegador.

Sin embargo, Internet también es el hogar de los ciberdelincuentes, cuyo único objetivo es engañarnos mediante todo tipo de fraudes y sacar provecho a nuestra costa. Para evitarlos y asegurarnos de poder realizar una navegación segura, es necesario que contemos con unas **nociones básicas para evitar los sitios webs peligrosos o fraudulentos, conectarnos a una red segura y utilizar algunas herramientas que nos ayudarán en esta misión.**

Los riesgos asociados a una navegación no segura son muchos y muy peligrosos, como el **conectarnos a una red wifi que esté siendo monitorizada por un ciberdelincuente, o una web maliciosa que rastree nuestra actividad y robe nuestros datos personales**, así como la **descarga involuntaria de todo tipo de virus y malware** a nuestro dispositivo.

3.1. Cómo conectarnos a Internet de forma segura (conexiones wifi)

Hoy en día existen una gran variedad de puntos wifi donde conectarnos cuando estamos fuera de nuestra casa.

Lamentablemente, **la mayoría de redes wifi públicas y gratuitas son inseguras y nos exponemos** a que los ciberdelincuentes puedan interceptar cualquier información o archivo que intercambiemos, ya sea un correo, una contraseña al iniciar sesión o un mensaje que mandemos a un familiar.

En caso de necesitar una conexión a Internet estando fuera de casa, deberemos **priorizar el uso de nuestra conexión móvil.** Es decir, los datos que tengamos contratados con nuestro proveedor de servicio.
Sin embargo, sabemos que no siempre disponemos de una red segura, por lo que queremos compartir algunas **recomendaciones para minimizar el riesgo y tratar de navegar de la forma más segura posible**, cuando salimos de casa:

1. Comprobar que es la red oficial. Muchos ciberdelincuentes crean redes falsas con un nombre similar a la oficial. Por ejemplo, la red wifi de un restaurante puede ser "RestauranteWifi", y la del ciberdelincuente "1_RestauranteWifi".

3.1. Cómo conectarnos a Internet de forma segura (conexiones wifi)

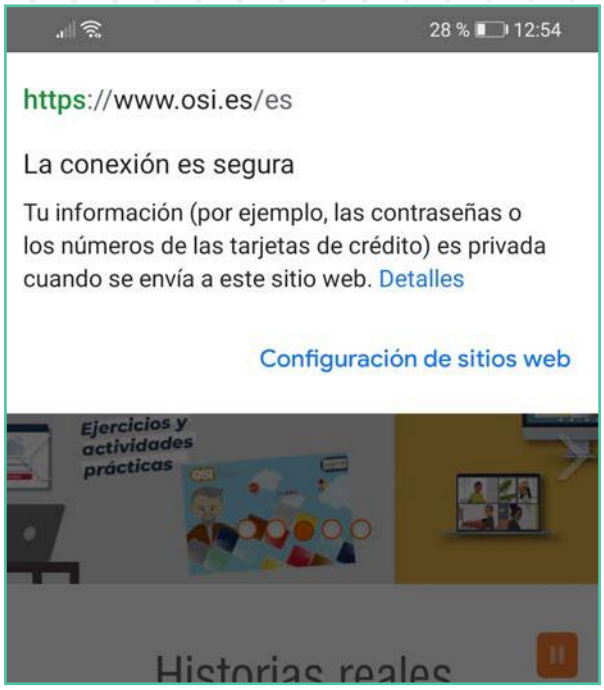
2. No compartir información. Para evitar que caiga en malas manos, debemos evitar ingresar con nuestro usuario y contraseña en alguna web o, incluso, enviar correos. Así nos protegeremos en caso de estar siendo monitorizados por un ciberdelincuente.

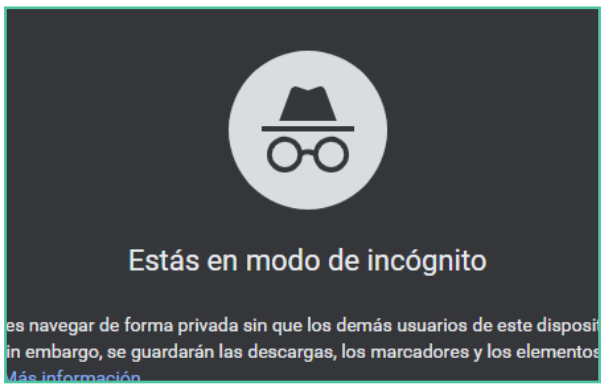
3. Mantener actualizado el dispositivo y las aplicaciones. De este modo, evitaremos que los ciberdelincuentes se aprovechan de vulnerabilidades o fallos en nuestro sistema.

4. Tener un antivirus actualizado instalado en el dispositivo. Analizará el dispositivo en busca de amenazas basadas en software malicioso, las cotejará con su base de datos y las eliminará.

5. Navegar por webs seguras. Las webs con HTTPS y certificado de seguridad siempre serán más seguras, ya que nuestros datos viajan cifrados y minimizaremos riesgos.

6. Utilizar la navegación privada. Este modo nos permite visitar páginas sin que el navegador almacene toda la información sobre las webs visitadas. Más adelante profundizaremos en esta opción.





3.2. Cómo blindar nuestra conexión a Internet (router)

El router **es el dispositivo que necesitamos para conectarnos a Internet.** Es el objetivo de numerosos ataques y su seguridad puede ser vulnerada si nos aseguramos de configurarlo adecuadamente, exponiéndonos a:

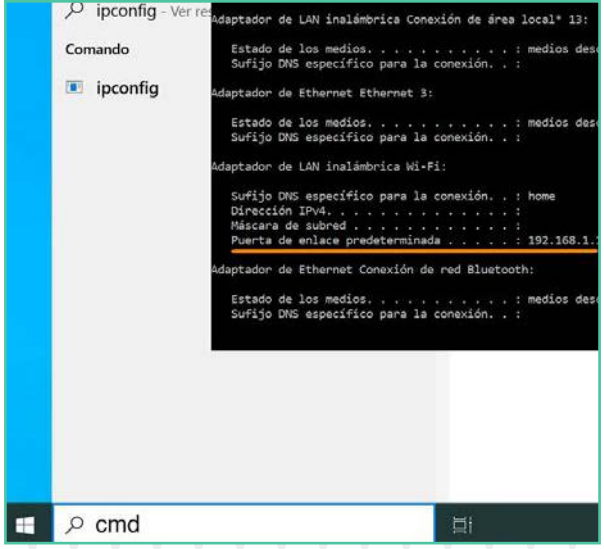
- Espionaje y monitorización de toda nuestra actividad cuando nos conectamos a Internet.
- Uso de nuestra Red para actividades ilícitas, como envío de spam.
- Infección de nuestros dispositivos conectados a Internet.
- Minimizar el ancho de banda (velocidad de Internet).

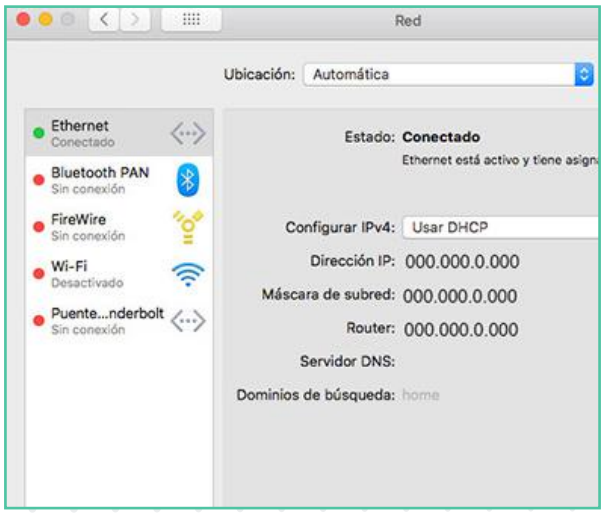
Cada router es un mundo y acceder a su configuración puede variar de un modelo a otro. Por suerte, las recomendaciones que veremos a continuación se encuentran en cualquier modelo y, si tenemos problemas, podemos contactar con nuestro proveedor de servicios de Internet:

3.2. Cómo blindar nuestra conexión a Internet (router)

1. Cómo acceder a su configuración. Para acceder al menú de configuración, lo primero que necesitaremos es conocer nuestra dirección IP:

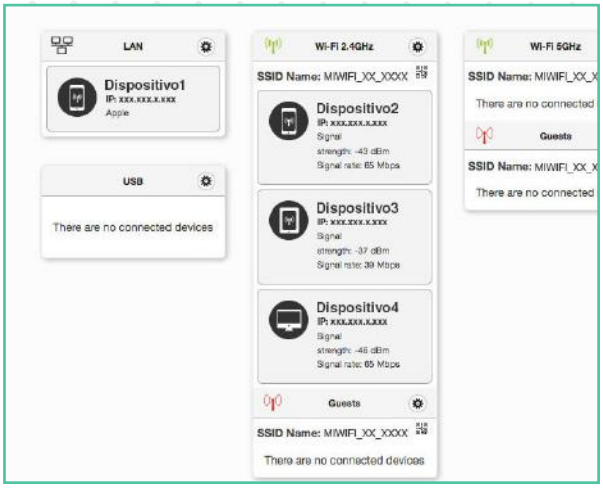
- **'Desde Windows'**, tendremos que escribir "**cmd**" en el **buscador de Windows** y escribir "**ipconfig**". Luego, buscaremos el código que aparece junto a **'Puerta de enlace predeterminada'**, que suele ser: **192.168.1.1**
- **Desde Mac**, haremos clic en el icono de **'Apple > Preferencias del sistema > Red'** y seleccionaremos nuestra conexión (**'AirPort o Ethernet'**). Dentro encontraremos nuestra dirección IP.





Luego, iremos a nuestro navegador favorito y pondremos nuestra dirección IP en la barra de las URL. Al hacerlo nos aparecerá una pantalla donde deberemos introducir nuestras credenciales de acceso. Suelen venir escritas en el propio router, en una pegatina en su parte posterior junto con el nombre de red (SSID) y la contraseña del wifi.

2. Cómo ver que dispositivos están conectados a nuestra conexión a Internet. Todos los router nos permiten visualizar los dispositivos conectados a nuestra Red cuando accedemos a su configuración. En la mayoría de ellos es justo lo primero que veremos al entrar.



Al pulsar sobre ellos podremos acceder a información sobre el tipo de dispositivo, la fecha de conexión y su dirección MAC, por ejemplo, que es una especie de identificador (como un DNI).

También podremos **cortar la conexión con aquellos dispositivos que no queramos en nuestra Red**, porque sean sospechosos o desconocidos.

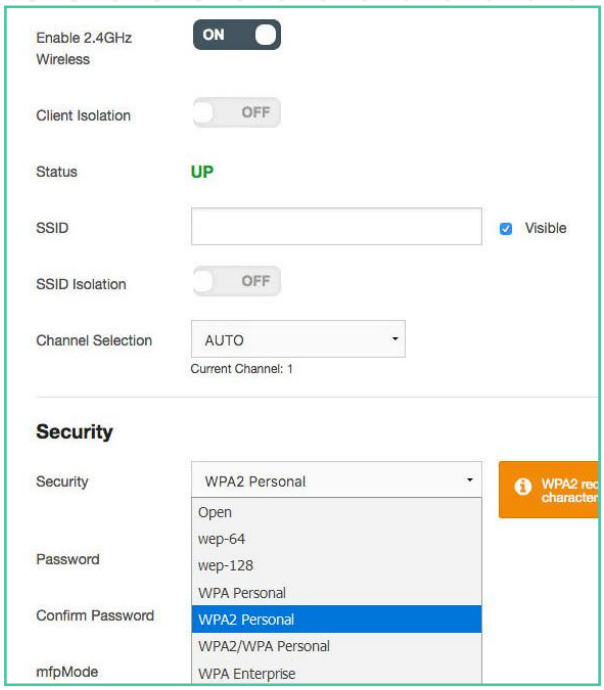
3.2. Cómo blindar nuestra conexión a Internet (router)

Si tenemos problemas para acceder a nuestro router, siempre podemos recurrir a herramientas de terceros con los que analizar los dispositivos que tenemos conectados a nuestra red wifi. Un ejemplo de este tipo de herramientas es Fing.

3. Cómo cambiar las contraseñas por defecto. Los router vienen con unas contraseñas por defecto que no son seguras, al igual que ocurre con la clave de nuestro wifi. Dentro de la Configuración, deberemos buscar el apartado de Usuario o Administración para cambiar las credenciales de acceso.

Luego, en el apartado de red Wi-Fi, modificaremos tanto el nombre de la red (SSID) como la contraseña.

En caso de que queramos conocer más configuraciones y profundizar en nuestro router, podemos hacer clic en este enlace*.



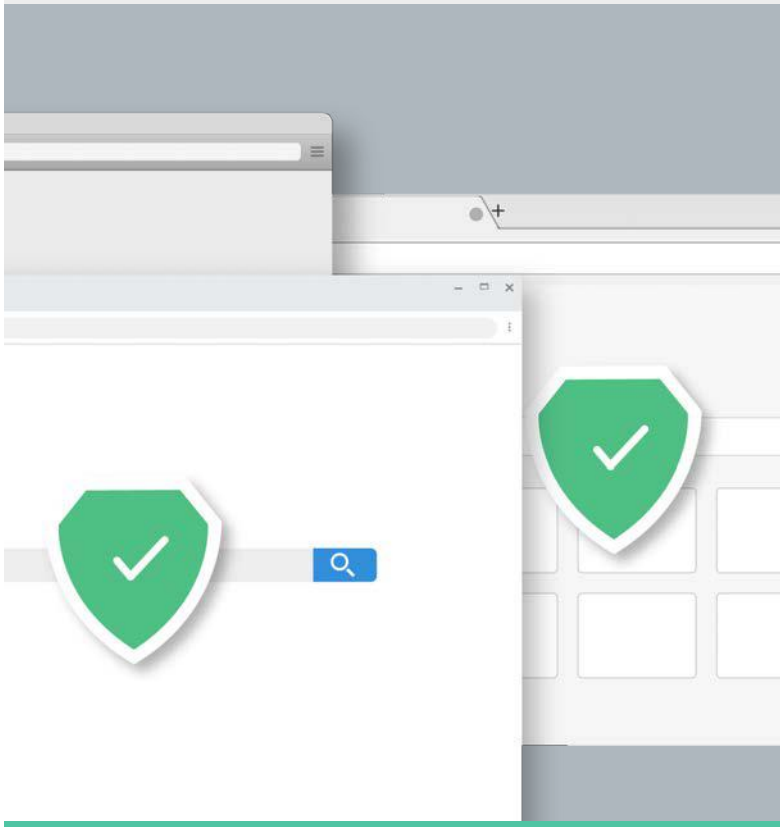
*https://www.osi.es/es/guia-configuracion-router

3.3. Cómo comprobar que nuestro navegador está actualizado

En Chrome | En Firefox | En Safari | En Edge

Los navegadores son los programas que utilizamos para buscar información a través de Internet. **Un navegador desactualizado tendrá fallos y brechas de vulnerabilidad** que los ciberdelincuentes pueden aprovechar para colarse y monitorizar nuestra navegación, robar información o incluso infectarnos con algún virus.

Para comprobar que nuestro navegador dispone de la última versión, debemos seguir estos pasos.



3.3. Cómo comprobar que nuestro navegador está actualizado

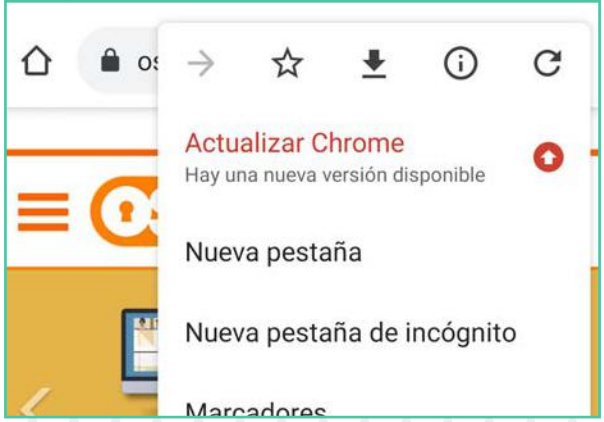
En Google Chrome

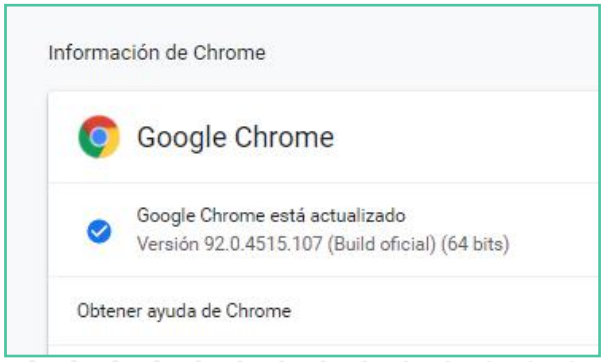
El navegador de Google se actualiza automáticamente de forma predeterminada cada vez que accedemos a Internet. Sin embargo, en caso de fallar podemos comprobarlo manualmente:

1. Pulsaremos sobre el **icono de los tres puntos de la esquina superior derecha.**

2. Si hay alguna actualización pendiente, nos aparecerá un icono de color verde, naranja o rojo, dependiendo de lo antigua que sea la actualización.

3. Luego, pulsaremos en **'Actualizar Google Chrome'.** Si no aparece este botón es porque nuestro navegador está actualizado y disponemos de la última versión. También podemos hacer clic en **'Ayuda > Información de Google Chrome'** dentro del menú para comprobar si está actualizado o iniciar la descarga de la última versión.





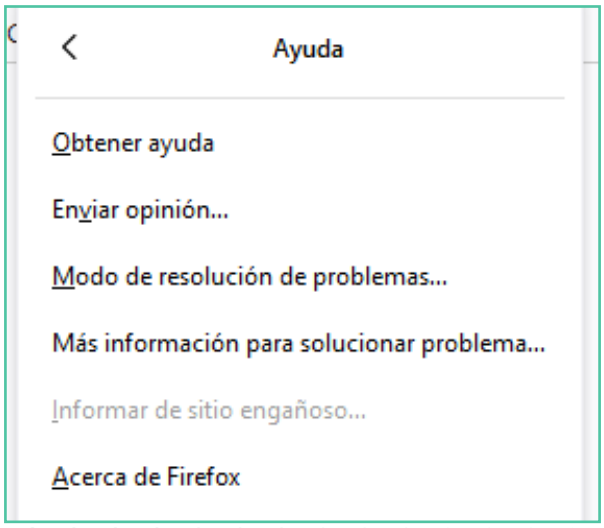
En Mozilla Firefox

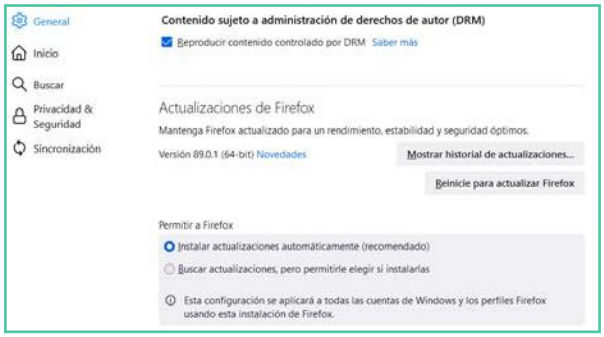
1. Haremos clic sobre el **'botón de menú** (icono con tres líneas) **> Ayuda > Acerca de Firefox'.**

2. Se abrirá una nueva ventana en la que podremos ver si hay alguna actualización pendiente. En caso de que exista, esta empezará a descargarse automáticamente.

3. Para finalizar, solo tendremos que **reiniciar Firefox.**

4. Para las actualizaciones automáticas, deberemos volver a hacer clic en el **'botón de menú > Ajustes > General'** y dentro del apartado **'Actualizaciones de Firefox'**, pulsar en **'Instalar actualizaciones automáticamente' (recomendado).**





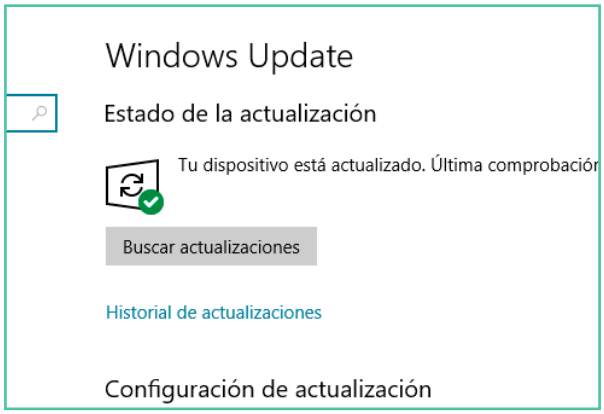
3.3. Cómo comprobar que nuestro navegador está actualizado

En Safari

En Mac, **solo deberemos mantener actualizado nuestro equipo** para que, a su vez, se actualicen todas las herramientas de Apple, como es el caso de su navegador Safari.

En Microsoft Edge

Al igual que en Mac, **este navegador se actualizará siempre y cuando actualicemos nuestro sistema operativo** Windows en nuestro dispositivo.



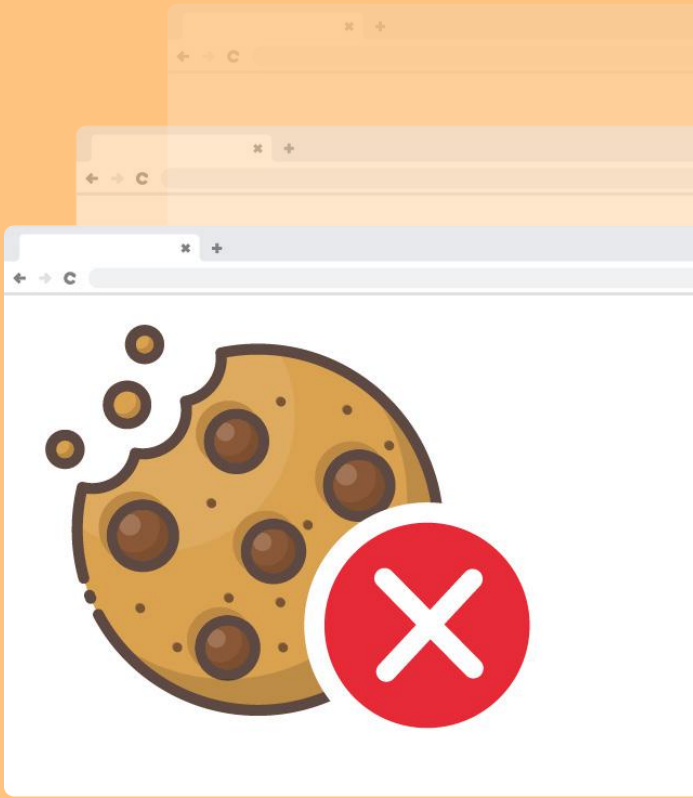
3.4. Cómo eliminar cookies y el historial de navegación

En Chrome | En Firefox | En Safari | En Edge

Cuando navegamos por Internet, **cada clic y página que visitamos deja una traza de información sobre nosotros:**

- Las **cookies** son parte de la información que se intercambia entre nuestro navegador y la página web. Contienen datos sobre nuestro idioma, tipo de dispositivo, versión del sistema operativo, tamaño de nuestra pantalla, el navegador que utilizamos, las contraseñas que ingresamos, etc.
- Por otro lado, **el historial de navegación** almacena todas las webs que hemos visitado.

Por seguridad, para evitar compartir demasiada información y correr el riesgo de que termine en malas manos, es recomendable que eliminemos estos datos de nuestro navegador cada cierto tiempo.



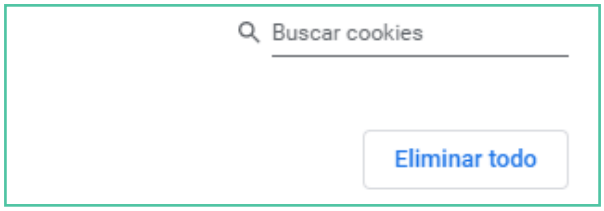
3.4. Cómo eliminar cookies y el historial de navegación

En Google Chrome

1. En la esquina superior derecha encontraremos un **icono con tres puntos.**

Al pulsarlo, debemos hacer clic en **'Configuración'.**

2. Dentro de Privacidad y seguridad, haremos clic en **'Cookies y otros datos de sitio'.** Al pulsar en **'Ver todas las cookies y datos de sitios webs'** podremos seleccionar **'Eliminar todo'.**

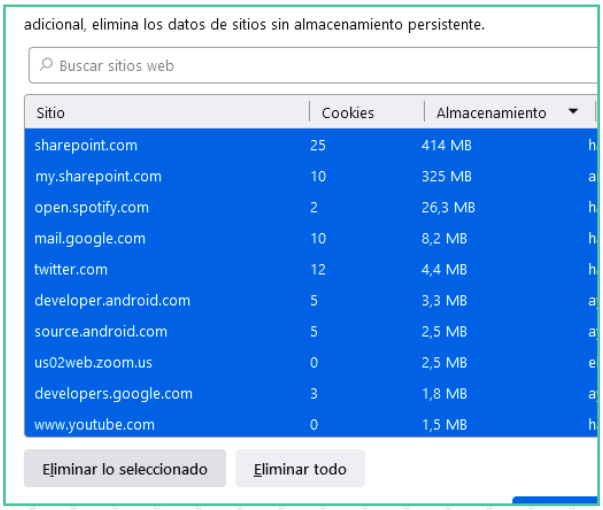


En Mozilla Firefox

1. Haremos clic sobre el **icono de menú** (tres líneas) y luego en **'Ajustes'.**

2. A continuación, pulsamos sobre el panel de **'Privacidad y seguridad'** y accedemos a la sección **'Cookies y datos del sitio'.**

3. Al pulsar sobre **'Administrar datos'** veremos una ventana con todos los datos almacenados, y al pulsar sobre **'Eliminar todo',** se borrará toda la información recogida.

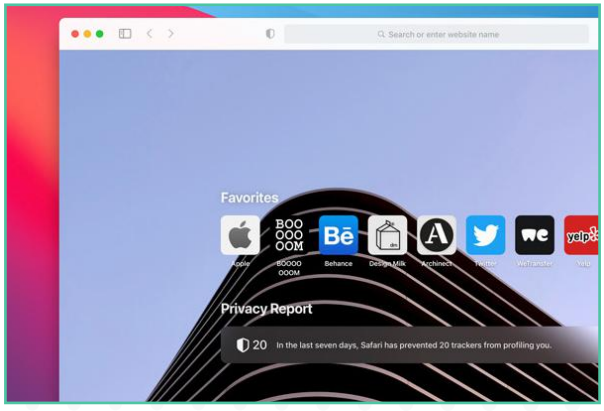


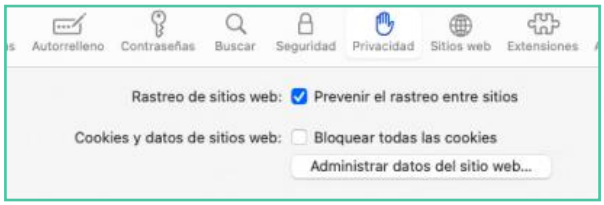
En Safari

1. Pulsaremos sobre **'Safari > Preferencias > Privacidad'.**

2. Dentro, veremos el apartado **'Cookies y otros datos de sitios web'**. Junto a él, veremos el botón para **'Eliminar todos los datos de los sitios web'...**

3. Pulsaremos sobre el botón para borrar todos los datos de navegación o en **'Detalles'...** para eliminar solo los que queramos.





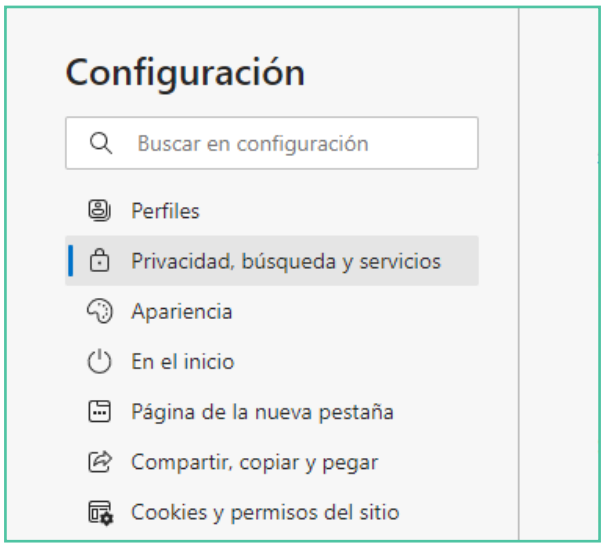
3.4. Cómo eliminar cookies y el historial de navegación

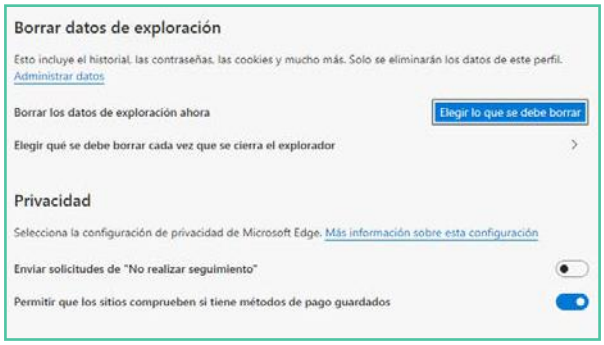
En Microsoft Edge

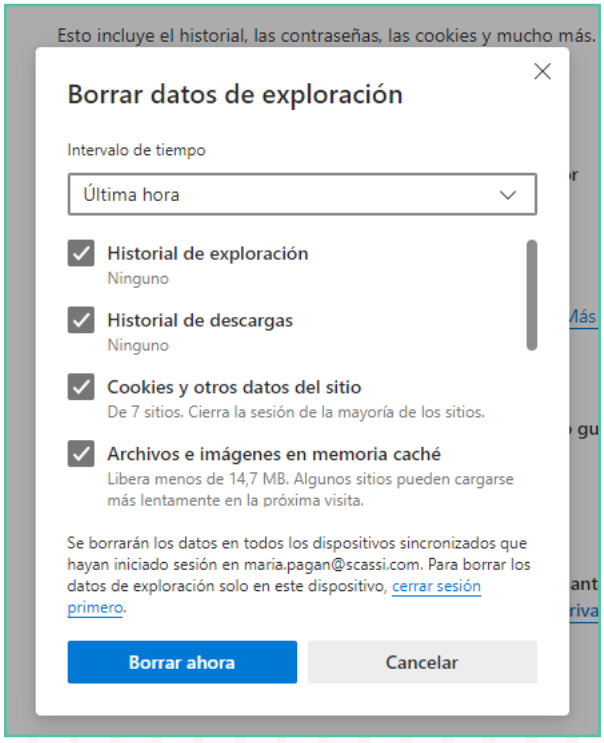
1. Iremos a las opciones de configuración (icono con tres puntos) y pulsaremos sobre **'Configuración > Privacidad, búsqueda y servicios > Borrar datos de exploración'.**

2. Luego, seleccionaremos **'Elegir lo que se debe borrar'**, así como el **intervalo de tiempo.**

3. Finalmente, pulsaremos **'Borrar ahora'** para eliminar los datos.







3.5. Cómo activar el modo incógnito

El modo incógnito es una herramienta disponible en cualquier navegador que **nos permite activarla y navegar por Internet sin que nuestro navegador almacene ningún tipo de información**, como contraseñas o sitios web visitados.

Es muy útil si, por ejemplo, tenemos que utilizar el dispositivo de algún amigo y no queremos dejar rastro:

En Google Chrome: pulsaremos sobre el **icono con tres puntos > Nueva ventana de incógnito.**

En Mozilla Firefox: haremos clic sobre el **icono de menú** (tres líneas) **> Nueva ventana privada.**

En Safari: pulsaremos sobre las **opciones de configuración de Safari y Navegación privada.**

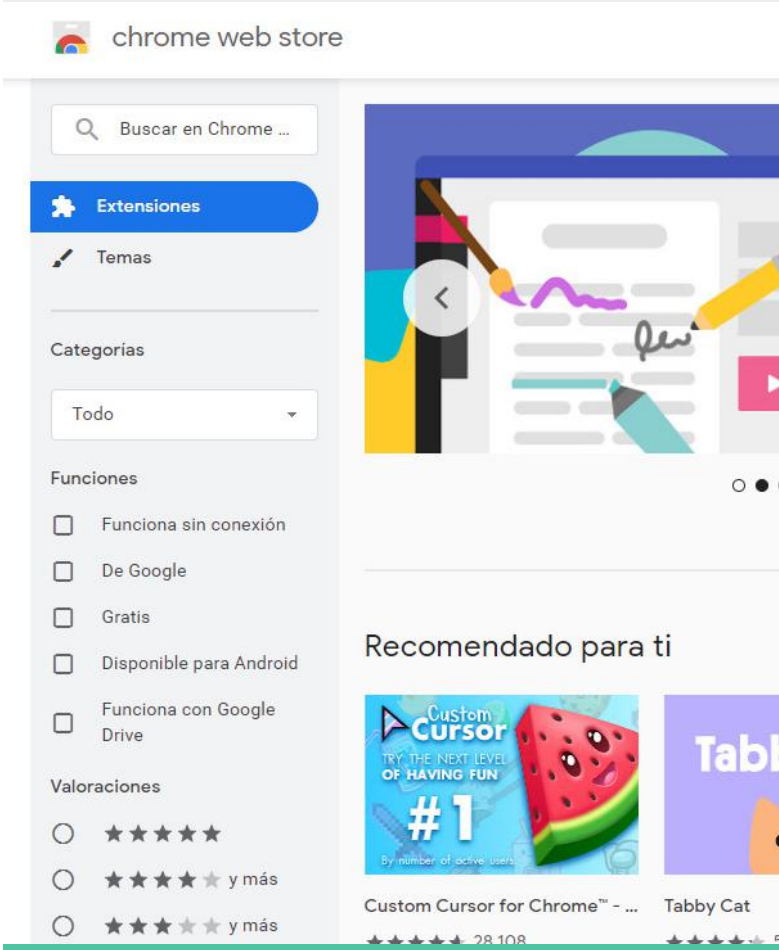
En Microsoft Edge: pulsaremos sobre el **icono con tres puntos > Nueva ventana InPrivate.**

3.6. Cómo instalar extensiones

En Chrome | En Firefox | En Safari | En Edge

Las extensiones **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.
Al igual que las aplicaciones, **también necesitan permisos a la hora de instalarse, por lo que debemos:**

- Revisar siempre los permisos que concedemos para evitar dar más de la cuenta y se haga un uso fraudulento.
- Utilizar siempre tiendas oficiales a la hora de descargarlas para asegurarnos que son extensiones legítimas:
  - *Extensiones oficiales de* Microsoft Edge.
  - *Extensiones oficiales de* Google Chrome.
  - *Extensiones oficiales de* Mozilla Firefox.
  - *Extensiones oficiales de* Safari.



Muchas de ellas nos ayudan a proteger aún más nuestra navegación por Internet al ayudarnos a detectar sitios web fraudulentos, eliminar cookies automáticamente o detectar archivos maliciosos. Para instalarlas en nuestro navegador deberemos:

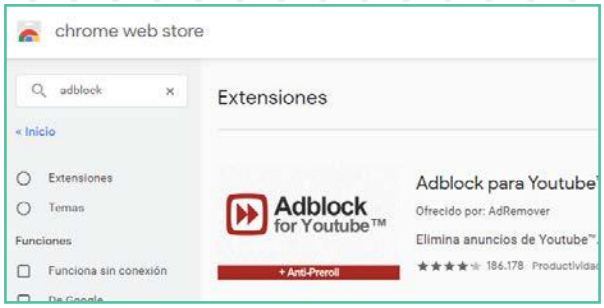
3.6. Cómo instalar extensiones

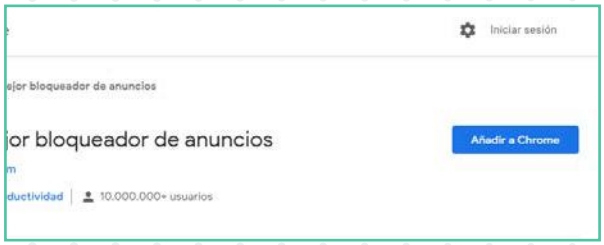
En Google Chrome

1. Desde Chrome, abriremos Chrome Web Store y seleccionaremos la opción **'Extensiones'** en el menú.

2. Al seleccionar una, nos llevará a la **página de descripción de la extensión**, donde veremos la puntuación, reseñas, permisos, fecha de las últimas actualizaciones, entre otras características. Luego, pulsaremos en **'Añadir a Chrome'.**

3. A continuación, veremos los datos a los que tendrá acceso y, tras revisarlos, pulsaremos en **'Agregar extensión'**. (Icono +)





En Mozilla Firefox

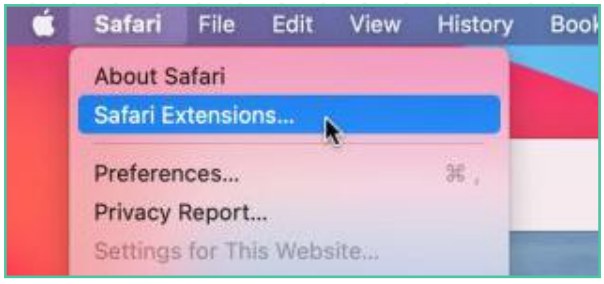
1. Pulsaremos las **'tres líneas horizontales situadas junto al icono del perfil > Complementos > Extensiones'** y pulsaremos sobre la que queramos instalar. Luego, haremos clic en **'Agregar a Firefox'.**

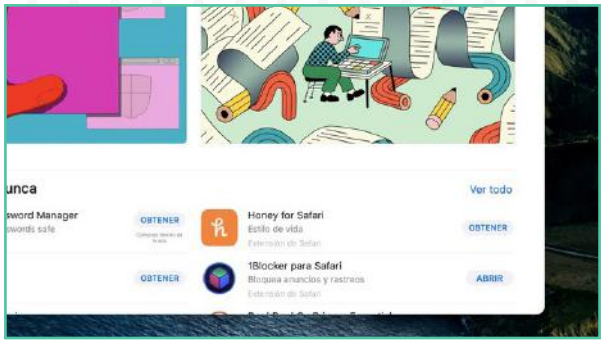
2. A continuación, comprobaremos los **permisos que requiere la aplicación** y luego, si nos parecen coherentes, seleccionaremos **'Añadir'.**

En Safari

1. Haremos clic sobre la pestaña **'Safari > Extensiones de Safari'.**

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





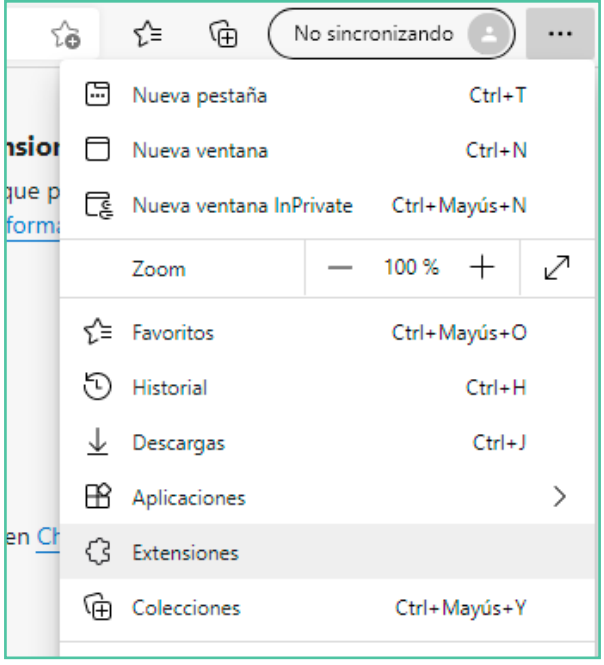
En Microsoft Edge

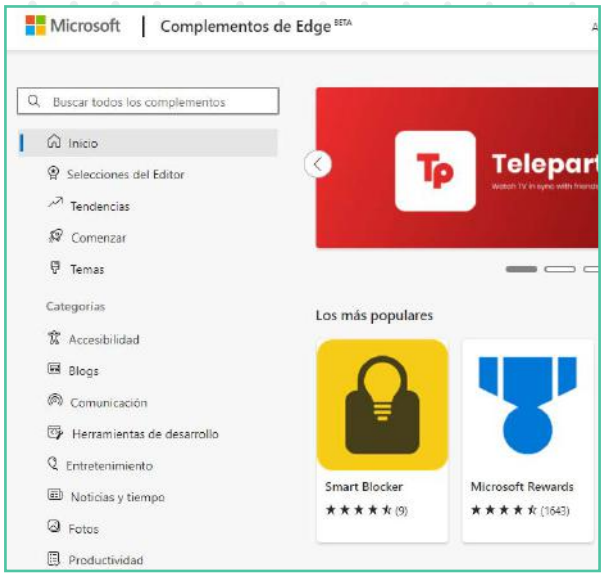
1. Pulsaremos en **'Configuración > Extensiones'** donde encontraremos una lista de extensiones sugeridas. Al final de la pestaña seleccionaremos **'Explorar más extensiones'** para ver más.

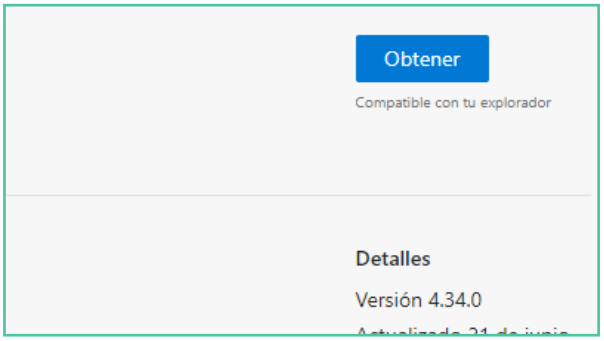
2. Una vez que encontremos la que queramos, seleccionaremos **'Obtener'** para instalarla y **'Lanzar'** para activarla.

3. Podremos leer la notificación sobre los permisos que necesitará la extensión en el lado derecho de nuestro navegador. A continuación, si nos parecen adecuados los permisos solicitados, seleccionaremos el botón **'Activar'.**

En este enlace* encontraremos más información acerca de las extensiones, así como algunas recomendadas.







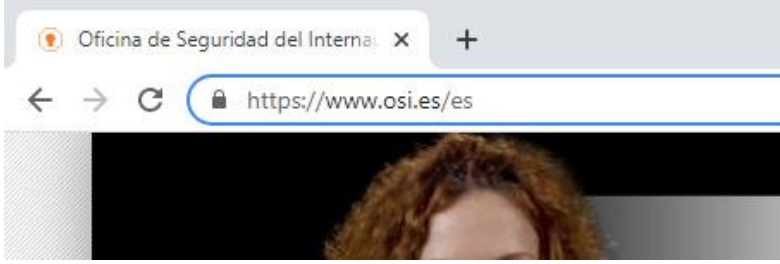
*https://www.osi.es/es/actualidad/blog/2019/11/20/extensiones-superpoderes-para-los-navegadores

3.7. Cómo identificar webs fiables y no fiables

A veces, **los ciberdelincuentes** crean webs falsas, duplicando la estética de otras más conocidas, o directamente **crean sitios web fraudulentos para atraer a los usuarios y conseguir robar nuestros datos o aprovecharse de nosotros.**

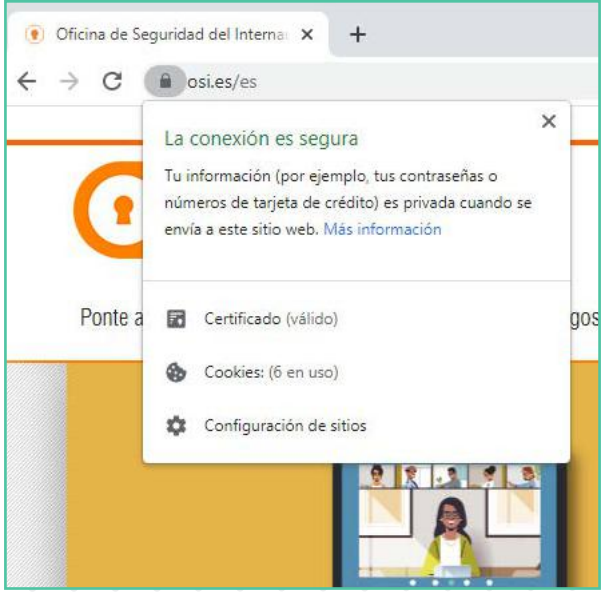
Por eso, es fundamental que aprendamos a identificar este tipo de sitios fraudulentos para evitarlos:

1. Revisar la URL: si la dirección web no coincide con la web, programa o empresa que estamos buscando, debemos desconfiar. Además, podremos comprobar si utiliza una conexión segura, empleando "HTTPS" en la dirección.
Por ejemplo:
http://www.ossi.com,
en lugar de:
https://www.osi.es.



3.7. Cómo identificar webs fiables y no fiables

2. Examinar el certificado de seguridad: si la web es fiable, lo más probable es que a la izquierda de la dirección web veamos un candado cerrado. Esto nos indicará que la web ha sido revisada por una entidad acreditadora. Sin embargo, no es un requisito 100% fiable, ya que pueden utilizar certificados falsos o comprarlos.



3. Analizar el aspecto de la web: estas webs no siempre están cuidadas y utilizan textos traducidos automáticamente, imágenes de poca calidad o tienen aspecto de ser una web hecha muy deprisa, sin cuidar los detalles.

4. Comprobar los anuncios: las webs fraudulentas suelen incluir numerosos anuncios, muchos de ellos peligrosos, que impiden disfrutar de la navegación o que buscan que hagamos clic por todos los medios posibles.

5. Buscar información sobre el propietario de la web: una web fiable siempre tendrá bien identificada la información legal sobre la empresa propietaria de la web o el desarrollador.

Si tras revisar estos puntos, la web en la que nos encontramos nos hace sospechar, lo más seguro es que la cerremos y busquemos en otro sitio.

4. Descubre y evita los principales tipos de fraude

4.1. Cómo identificar ataques de ingeniería social (*phishing*, *vishing*, *smishing*)
4.2. Cómo evitar fraudes en compras online (Chollos falsos, Tiendas online falsas, Métodos de pago)
4.3. Cómo detectar noticias falsas o *Fake News* (Noticias falsas, Cadenas de mensajes)
4.4. Cómo identificar otros fraudes (Anuncios, Alquileres, Préstamos, Webs falsas)

Como ya sabemos, Internet puede ser un lugar lleno de ventajas y posibilidades si sabemos cómo navegar de forma segura. Sin embargo, para ello es necesario que conozcamos cómo funcionan los fraudes y estafas más comunes de la Red para luego poder estar prevenidos y evitarlos.

Solo necesitaremos **utilizar el sentido común y estar atentos**, pues muchos de estos fraudes se aprovechan de la información que recaban sobre nosotros para lanzar ataques dirigidos basados en nuestros intereses, nuestra situación actual o se hacen pasar por personas o servicios de confianza. Por suerte, **su modus operandi suele ser el mismo y, una vez sepamos cómo funcionan, podremos identificarlos y prevenirlos rápidamente.**

Los riesgos derivados de ser víctima de estos fraudes también son muy variados, como el **robo de nuestros datos personales al compartir esta información con un formulario online** para participar en un supuesto sorteo.

También son comunes los fraudes vinculados a la **suplantación de identidad**, donde los ciberdelincuentes se harán pasar por personas de confianza para conseguir que nos instalemos algún malware, compartamos datos con ellos o realicemos algún tipo de pago.

Finalmente, también son comunes los casos de ***Fake News* o noticias falsas en la Red**, cuyo objetivo es desinformar a los usuarios, así como engañarnos para acceder a sitios web fraudulentos.

4.1. Cómo identificar ataques de ingeniería social *(phishing, vishing, smishing)*

Los ataques mediante ingeniería social perpetrados por los ciberdelincuentes **están basados en técnicas de engaño, donde los atacantes se hacen pasar por personas o empresas de confianza para aprovecharse de nosotros.** Algunas de las más conocidas son:

- *Phishing*
- *Vishing*
- *Smishing*

***Phishing*: consiste en el envío de un correo electrónico donde los ciberdelincuentes suplantan la identidad de entidades de confianza, como nuestro banco, una red social o una entidad pública para obtener toda la información personal y bancaria que puedan. También es común que adjunten archivos infectados o enlaces a páginas fraudulentas.**

***Vishing*: consiste en la realización de llamadas telefónicas haciéndose pasar por entidades de confianza, como nuestro banco o un servicio técnico para engañar a los usuarios, obteniendo sus datos personales o tomando control de sus dispositivos.**

***Smishing*: consiste en el envío de mensajes de texto (SMS) o por aplicaciones de mensajería instantánea, haciéndose pasar por entidades de confianza o contactos de la víctima para obtener información personal y bancaria.**

4.1. Cómo identificar ataques de ingeniería social (*phishing, vishing, smishing*)

Para identificarlos, lo primero es no dejarnos llevar por la presión, utilizar el sentido común y seguir estos pasos:

1. Comprobar el remitente (*phishing, smishing* y *vishing*): si coincide con la persona o entidad remitente, podemos estar tranquilos. Sin embargo, si no coincide, nos aparece un número desconocido o un correo extraño, se trata de un fraude.

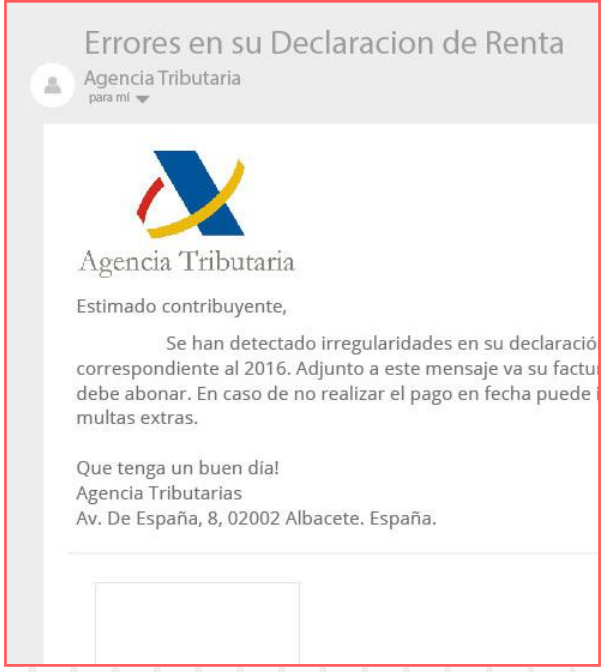
2. Analizar el asunto (*phishing*): la mayoría de fraudes utilizarán un asunto llamativo que capte nuestra atención para que ignoremos el resto de alertas.

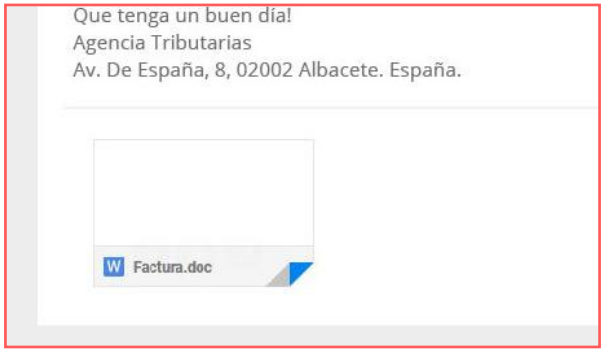
3. Analizar el objetivo del mensaje (*phishing, smishing* y *vishing*): debemos preguntarnos qué quieren de nosotros. Si es una entidad como nuestro banco, lo más probable es que ya tenga nuestros datos y no necesite volver a pedírnoslos. Estos mensajes suelen solicitar llevar a cabo una acción de manera urgente, para evitar que nos paremos a analizar el mensaje, por ello es probable que se trate de un fraude.

4. Examinar la redacción (*phishing* y *smishing*): los errores ortográficos y gramaticales son típicos de mensajes escritos con prisas o mediante una traducción automática, lo que debe hacernos sospechar.

5. Comprobar los enlaces (*phishing* y smishing): si el mensaje incluye un enlace, debemos comprobar si es fiable o no pasando el cursor por encima o manteniendo el dedo sobre el mismo y comprobar cuál es la URL real.

6. Analizar el adjunto (*phishing* y *smishing*): antes de descargar ningún adjunto, deberemos analizarlo con nuestro antivirus para asegurarnos de que no se trata de un malware. Finalmente, debemos recordar que si sospechamos de un fraude, nunca debemos seguir sus indicaciones, ni facilitar ningún tipo de información personal.

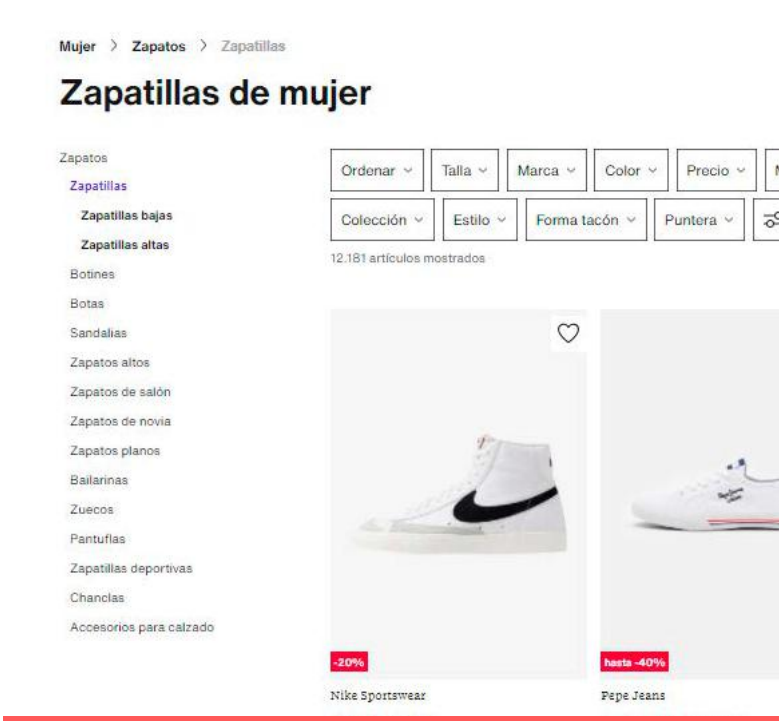




4.2. Cómo evitar fraudes en compras online (chollos falsos, tiendas online falsas, métodos de pago)

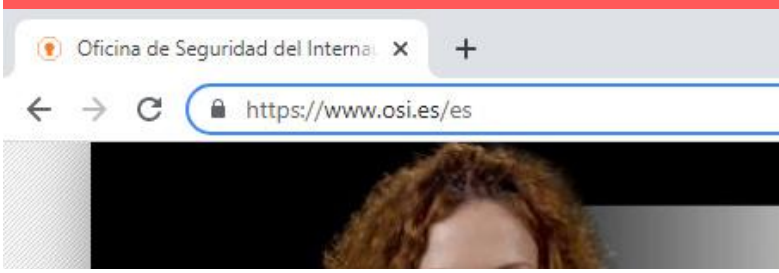
A la hora de comprar online y sacar el máximo provecho a las ofertas y promociones, **debemos estar siempre alerta, no vaya a ser que terminemos en una tienda fraudulenta o realizando un trato con un vendedor con malas intenciones.**

Para evitar este tipo de fraudes, es necesario que sigamos todas estas buenas prácticas:



1. Comprobar la URL: al igual que ocurre con las webs falsas, este método no es 100% fiable, pero nos ayudará a descartar tiendas online que no utilicen una conexión segura (es segura si la URL comienza con 'https://') y sean un riesgo a nuestra seguridad.

2. Al revisar la **dirección web** también veremos **si coincide con el nombre de la empresa o tienda.** Así evitaremos entrar en webs falsas o que suplantan a una marca conocida.



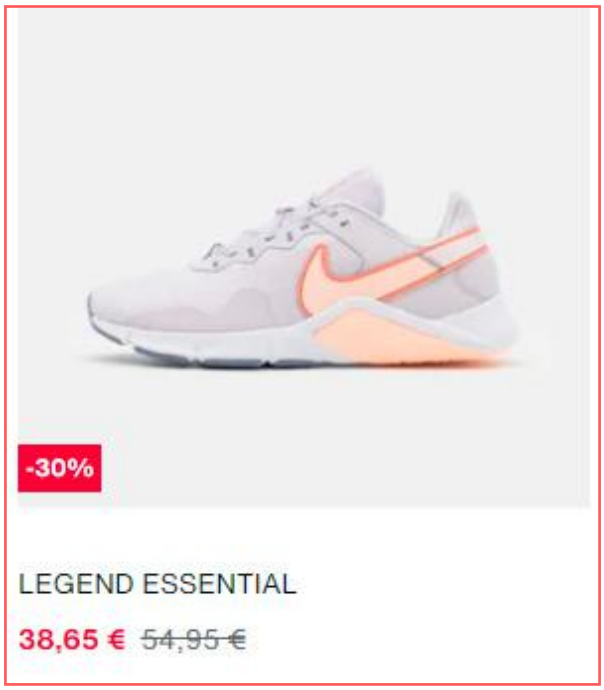
4.2. Cómo evitar fraudes en compras online (chollos falsos, tiendas online falsas, métodos de pago)

3. Buscar información de la empresa: una tienda online legítima dispondrá de un apartado con información sobre la empresa, NIF y otros datos. Es común que se encuentre dentro de un apartado llamado Aviso legal, Contacto o Información.

4. Buscar un sello de confianza: son acreditaciones que tienen como objetivo demostrar al usuario que se trata de un negocio legítimo, preocupados por la seguridad y el bienestar de los consumidores. Por norma general, se encuentran en la parte inferior de la tienda online, en forma de logotipo.

5. Buscar información sobre la devolución de productos: una web legítima debe incluir un apartado destinado a toda la información relativa a la devolución de sus productos. En el caso de las webs fraudulentas, esta información está omitida o es escasa.

6. Comprobar el precio de los productos: lo normal de una tienda online es que tenga promociones y descuentos de vez en cuando, sin embargo si sus precios son muy bajos, tiene grandes descuentos o siempre están rebajados, es probable que se trate de un fraude.

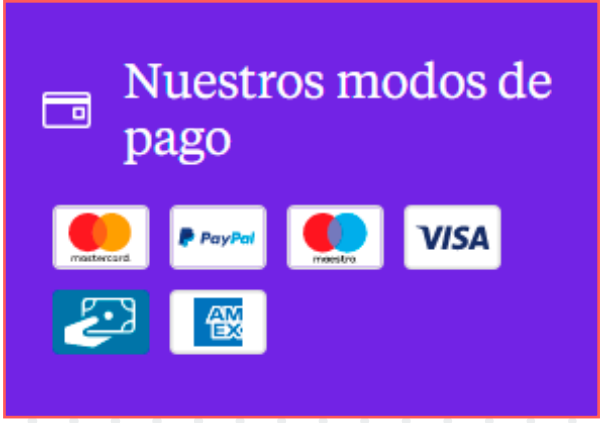


7. También es común que las webs fraudulentas ofrezcan el mismo precio o utilicen **descripciones muy cortas y poco útiles** para sus productos.

8. Examinar la valoración de otros usuarios: es recomendable realizar búsquedas sobre la opinión y comentarios de otros usuarios. En el caso de que no encontremos las valoraciones o que todas sean muy buenas y parezcan hechas por un robot, deberemos desconfiar. Lo normal en una tienda online es que haya comentarios tanto positivos como negativos y muy variados.

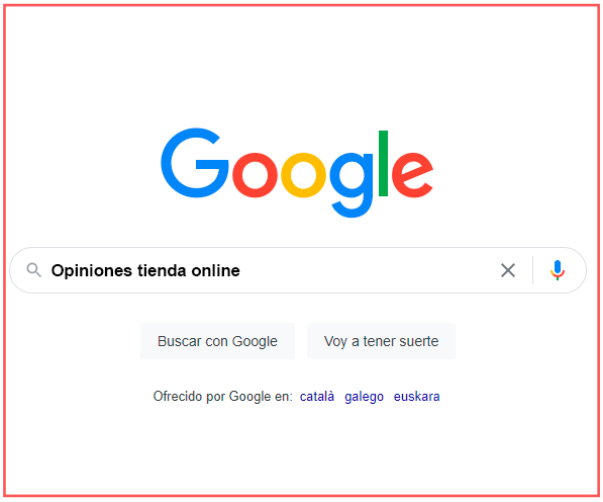
4.2. Cómo evitar fraudes en compras online (chollos falsos, tiendas online falsas, métodos de pago)

9. Analizar los métodos de pago: existen métodos de pago más seguros que otros, si tenemos claro cuáles son los menos seguros, podremos identificar aquellas webs fraudulentas que tratan de hacerse con nuestro dinero. Las transferencias bancarias a bancos extranjeros son uno de los métodos favoritos de los ciberdelincuentes, mientras que las plataformas de pago seguro, el contrarrembolso o el pago mediante tarjetas de crédito suelen ser típicos de negocios legítimos.



10. Utilizar los canales habilitados: tanto si es una tienda online como si vamos a realizar una compra-venta, es fundamental que utilicemos la herramienta de comunicación oficial y las plataformas de pago habilitadas, ya que nos servirán de pruebas en caso de fraude.

11. Comprobar la reputación: si es una tienda o un vendedor online, revisar su reputación u opiniones de otros usuarios en Internet puede ayudarnos a evitar una estafa, incluso si la web esté llena de comentarios positivos.



4.3. Cómo detectar noticias falsas o *fake news* (noticias falsas, cadenas de mensajes)

Las *fake news* **son noticias falsas y bulos que se propagan por la Red con el único objetivo de desinformar, engañar y manipular a los usuarios.** Gracias a su capacidad de difusión a través de las redes sociales y las aplicaciones de mensajería instantánea, como WhatsApp, se han convertido en un verdadero problema, ya que llegan a nosotros antes que las noticias reales.

Los principales riesgos de este tipo de fraude son:

Desinformación: debida a la ausencia de información veraz, lo que nos hace más manipulables.

Infección por malware y robo de credenciales: muchas se alojan en sitios web fraudulentos que nos solicitan un registro, instalar algún *software* malicioso que infecta nuestros dispositivos.

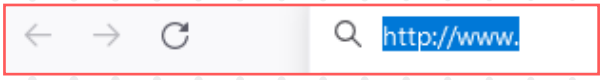
Daños en la reputación online: puede afectar a nuestra credibilidad y que otros usuarios desconfíen de nosotros.

4.3. Cómo detectar noticias falsas o *fake news* (noticias falsas, cadenas de mensajes)

Veamos cómo podemos identificar estas noticias falsas:

1. Buscar la fuente y contrastar la noticia: las noticias reales siempre mencionarán las fuentes utilizadas, que podremos utilizar para contrastar la noticia.

2. Revisar la URL: es frecuente que las noticias falsas se alojen en webs falsas o poco fiables que no dispongan de certificado de seguridad ni HTTPS en la URL.



3. Mirar más allá del titular: suelen recurrir a titulares muy llamativos, agresivos o sensacionalistas. Su objetivo es apelar a nuestras emociones, aunque un rápido vistazo a la noticia nos ayudará a desenmascarar el fraude.

4. Comprobar el formato: las noticias falsas no suelen cuidar el formato, utilizan imágenes de poca calidad, manipuladas y presentan faltas de ortografía.

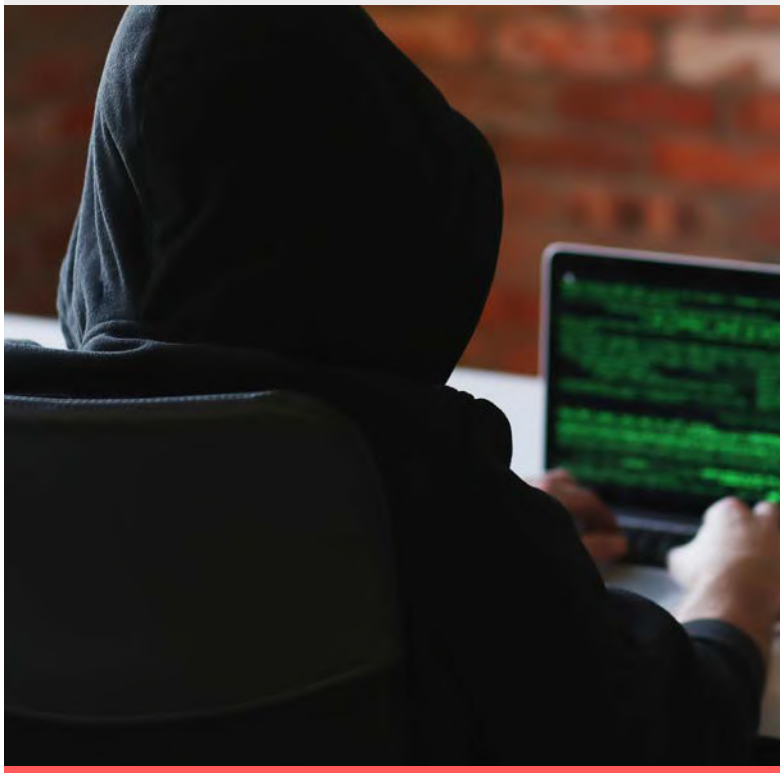
5. Aplicar el sentido común: no debemos dejarnos llevar por las emociones, si la noticia parece que busca atacar, manipularnos o dividir, debemos desconfiar.
Encontraremos información muy útil sobre este tipo de fraudes en el siguiente enlace*.

*https://www.osi.es/es/campanas/redes-sociales/cuadriptico-detectar-fake-news

4.4. Cómo identificar otros fraudes (anuncios, alquileres, préstamos, webs falsas)

Los ciberdelincuentes siempre están al acecho, y **no escatiman en esfuerzos para engañarnos y aprovecharse de nosotros.**

Veamos algunos ejemplos de los fraudes más comunes que podemos encontrarnos:

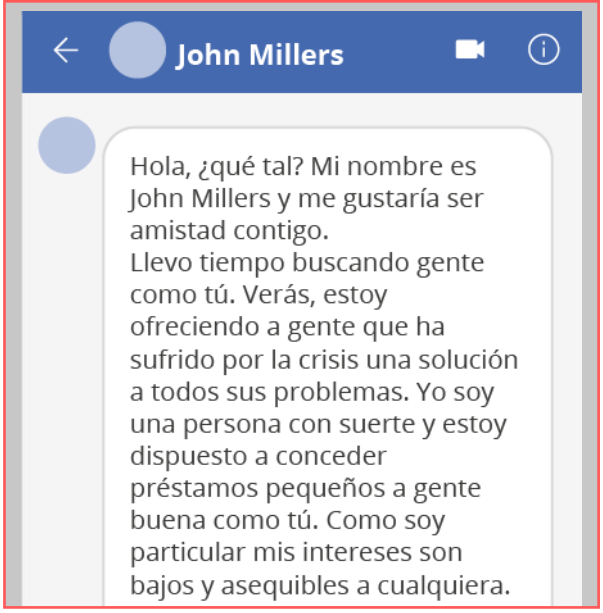


Anuncios maliciosos: son muy invasivos, apareciendo en medio de la pantalla con letras y colores muy atractivos. Suelen aparecer en sitios webs poco fiables y, si hacemos clic en ellos, lo más probable es que terminemos en una web fraudulenta.

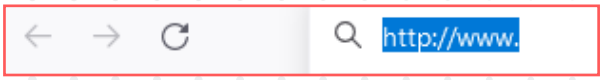
Alquileres fraudulentos: dentro de las plataformas de compra y alquiler de viviendas es común ver anuncios muy atractivos y a muy buen precio. Se sirven de fotografías robadas o copiadas de otros anuncios, utilizan descripciones pobres o mal traducidas y siempre pondrán problemas para visitar u obtener más información sobre la vivienda.

4.4. Cómo identificar otros fraudes (anuncios, alquileres, préstamos, webs falsas)

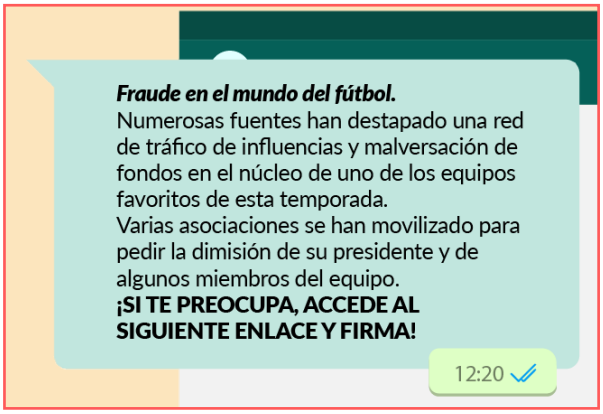
Préstamos engañosos: también es habitual encontrar anuncios o publicaciones en redes sociales de personas que se ofrecen a conceder préstamos a un muy bajo interés porque quieren ayudar a las personas. Este tipo de anuncios requiere que realicemos algún pago inicial a modo de gastos administrativos o bajo cualquier premisa, para que luego esta persona desaparezca.



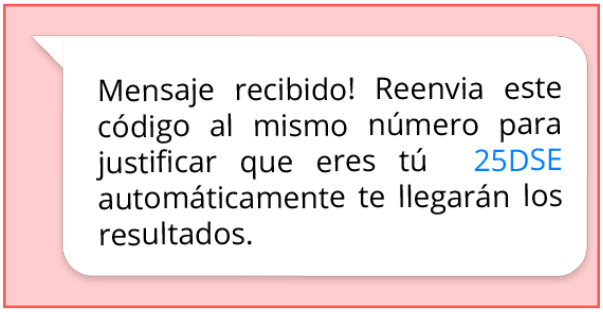
Webs falsas: las webs falsas copian el estilo de otras webs más famosas o de marcas conocidas, utilizando sus colores, logos y estructura. Sin embargo pueden encontrarse diferencias si nos fijamos bien, como imágenes de menos calidad, falta de información sobre la empresa o una URL sin HTTPS y sin certificado de seguridad.



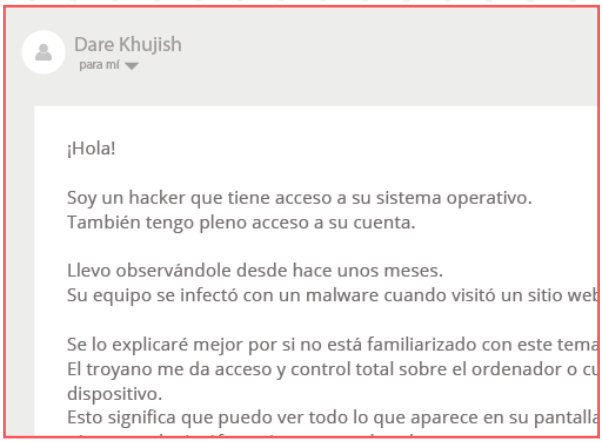
Concursos falsos: si hemos ganado un sorteo sin haber ni siquiera participado, lo más probable es que sea un fraude. Otros concursos utilizan formularios de registro donde nos piden demasiados datos personales (número de tarjeta, email, DNI…) o compartirlos con todos nuestros contactos para llegar a más víctimas.



Suscripciones Premium de SMS: algunos servicios utilizan los SMS como método para financiarse, al cobrar por cada SMS que enviamos. Sin embargo, algunos fraudes utilizan este medio sin nuestro consentimiento, al descargarnos alguna app fraudulenta o al responder a un SMS sospechoso, por eso debemos tener mucho cuidado y estar alerta en este tipo de comunicaciones.



Sextorsión: en el caso de que hayamos conocido a alguien por Internet y esta persona nos solicite pasar al segundo nivel al compartir fotografías o vídeos íntimos debemos desconfiar, después podrá utilizar ese material para chantajearnos.



No nos dejaremos engañar si seguimos las pautas de este enlace* para reconocer estafas en las redes.

*https://www.osi.es/es/aprende-reconocer-fraudes-en-redes-sociales-y-whatsapp

5. Disfrutando sin riesgos de las redes sociales y las comunicaciones por Internet

5.1. Cómo configurar de forma segura nuestro perfil
5.2. Cómo detectar una cuenta falsa y cómo denunciar
5.3. Cómo configurar nuestro WhatsApp de forma segura

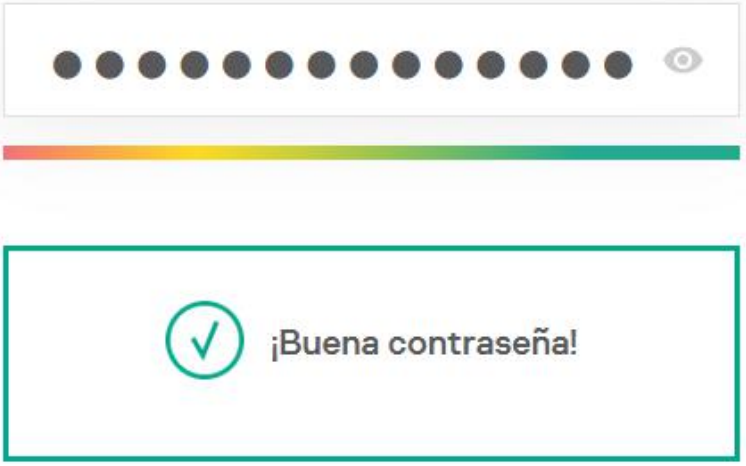
Las comunicaciones son una de las áreas que más han evolucionado desde su aparición en Internet. **Hoy en día, podemos hablar con cualquier persona del mundo**, y solo necesitaremos un dispositivo con acceso a Internet. **Las redes sociales, así como las aplicaciones de comunicación instantánea** o las videollamadas, **son algunos de los servicios más populares.**

Lamentablemente, este dato también es conocido por los ciberdelincuentes, que ven en ellas un canal perfecto para sus artimañas. Pero no debemos preocuparnos, todos estos servicios cuentan con las herramientas y configuraciones de seguridad y privacidad necesarias para proteger nuestra información personal, así como para prevenir los ciberataques y denunciar todos los fraudes perpetrados por los ciberdelincuentes.

No hacerlo podría suponer una serie de riesgos para nuestra privacidad, como el **robo de datos personales** que podrían ser usados para llevar a cabo **ataques de ingeniería social o crear cuentas falsas** con nuestros datos. También podemos ser **víctimas de fraudes y estafas por medio de estos servicios**, por lo que no debemos dejar de ser precavidos.

5.1. Cómo configurar de forma segura nuestro perfil

Cada red social pone a nuestra disposición las herramientas para **configurar nuestro perfil y tomar control de la información que compartimos.** Algunas de estas configuraciones incluyen:



1. Utilizar contraseñas robustas: una clave robusta es fundamental para proteger nuestras cuentas y perfiles. Así evitaremos que un tercero consiga acceder a nuestro perfil, hacerse con nuestros datos, fotografías y engañar a nuestros contactos suplantando nuestra identidad.

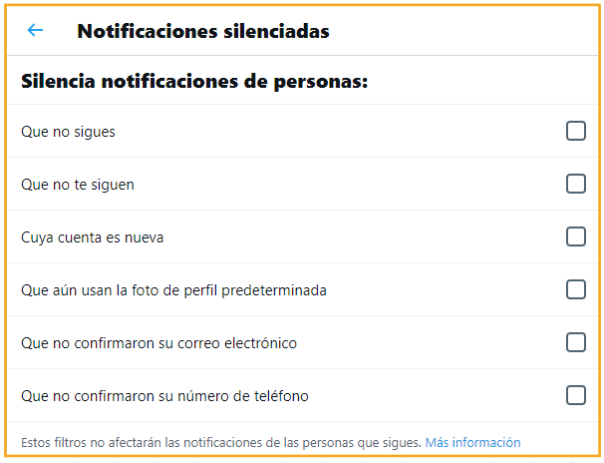
2. Activar la verificación en dos pasos: este mecanismo de protección añadirá una capa extra de seguridad al iniciar sesión. La mayoría de redes sociales disponen ya de esta funcionalidad dentro del servicio, solo deberemos acceder a la configuración de las opciones de seguridad, activarla y seleccionar el método para recibir el código temporal que deberemos introducir cada vez que queramos entrar en nuestra cuenta.

5.1. Cómo configurar de forma segura nuestro perfil

3. Configurar la privacidad de nuestro perfil: configurar nuestra cuenta o perfil para que sea privado nos protegerá ante intentos de robo de información de terceros. Si no somos una empresa o un famoso en la Red, ¿por qué queremos que los desconocidos sepan datos sobre nosotros? La mayoría de redes sociales permite poner nuestro perfil en privado para que solo nuestros contactos puedan ver nuestra información y publicaciones.

4. Limitar las comunicaciones con desconocidos: muchos de los ataques por redes sociales llegan desde perfiles falsos. Es importante que sepamos identificarlos, pero también lo es configurar nuestro perfil para evitar que estos perfiles puedan enviarnos mensajes, invitaciones o mencionarnos en sus publicaciones.

5. Limitar la cantidad de datos que publicamos: cuando publicamos sobre nuestras vacaciones, amigos o hobbies, podemos estar regalando más información de la que debemos, sobre todo si no conocemos a todos nuestros contactos. Es recomendable evitar dar demasiada información personal y tener mucho cuidado de no publicar datos sensibles, como imágenes de menores, datos bancarios, nuestra dirección, etc.
Cada red social es un mundo, y sus opciones de configuración pueden variar mucho entre sí. Dependiendo de la red social que utilicemos, deberemos hacer caso a sus recomendaciones de seguridad y privacidad:



- Configuración de Facebook.
- Configuración de Instagram.
- Configuración de Twitter.

Dentro del siguiente enlace* encontraremos algunas consideraciones adicionales que debemos tener en cuenta al publicar en redes sociales.

*https://www.osi.es/es/actualidad/blog/2019/03/20/consideraciones-tener-en-cuenta-al-publicar-en-redes-sociales

5.2. Cómo detectar una cuenta falsa y cómo denunciar

Una cuenta falsa no es más que **una cuenta que ha suplantado la identidad de otra persona o entidad para aprovecharse de sus contactos**, por ejemplo recabando información personal de los fans de una persona famosa, o solicitando dinero a sus seguidores.

Aunque no siempre son personas o empresas famosas, también los usuarios corremos el riesgo de suplanten nuestra identidad.

5.2. Cómo detectar una cuenta falsa y cómo denunciar

Podemos **identificar una cuenta falsa** si:

- Utilizan fotografías que parecen ser robadas de otras cuentas o imágenes de poca calidad.
- Apenas incluyen información en sus perfiles, ni descripciones en sus publicaciones.
- Publican enlaces a webs maliciosas o sospechosas, concursos falsos con el único objetivo de hacerse con los datos personales de sus contactos.
- Tiene pocos contactos en su perfil. Además, es probable que sus contactos también puedan ser cuentas falsas o bots.
- Trata siempre un mismo tema en sus redes, parece un robot compartiendo y publicando las mismas noticias falsas, los mismos intereses o anuncios sospechosos y, también, es posible que intente desprestigiar a otro usuario o marca.

Una cuenta falsa también puede ser un perfil de un usuario ficticio, inventado por el ciberdelincuente utilizando imágenes robadas, mezcladas y creando un perfil atractivo para el resto de usuarios, ya sea por sus fotos, su descripción, el tipo de contenido que publica, etc. El objetivo siempre será el mismo, ganarse la confianza de los usuarios para luego aprovecharse de ellos mediante algún tipo de fraude, como la sextorsión, venta de productos falsos, concursos o préstamos fraudulentos.

Las redes sociales disponen de un servicio para denunciar este tipo de cuentas falsas:

- Denunciar una cuenta falsa en Facebook.
- Denunciar una cuenta falsa en Twitter.
- Denunciar una cuenta falsa en Instagram.

5.3. Cómo configurar nuestro WhatsApp de forma segura

WhatsApp es una de las aplicaciones de mensajería instantánea más utilizada en el mundo. **Los usuarios la utilizamos para hablar con nuestros amigos y familiares e intercambiar todo tipo de archivos e información**, por eso **es tan importante que aprendamos a configurarla de forma segura.**

Siguiendo estos pasos nos aseguraremos de proteger todas nuestras comunicaciones (pueden variar ligeramente entre dispositivos Android y Apple (iOS):

5.3. Cómo configurar nuestro WhatsApp de forma segura

1. Configurar las opciones de privacidad. Pulsaremos sobre el 'icono de los tres puntos situado en la esquina superior derecha > **Ajustes > Cuenta > Privacidad**'. Dentro, podremos modificar la visibilidad de la siguiente información:

- **Hora de últ. vez:** para seleccionar quién verá la hora de nuestra última conexión:
  - **Todos:** cualquiera con nuestro número de teléfono.
  - **Mis contactos:** solo los que hayamos registrado.
  - **Nadie:** ningún usuario, y tampoco veremos esta información en nuestros contactos.

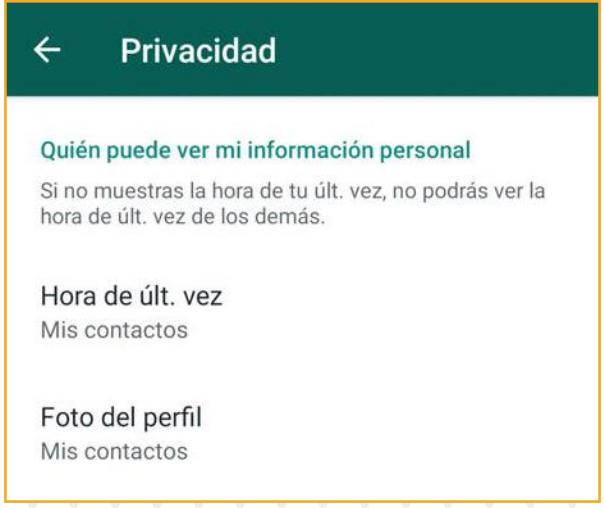
- **Foto de perfil:** podremos seleccionar quiénes pueden verla ('Todos', 'Mis contactos' o 'Nadie').

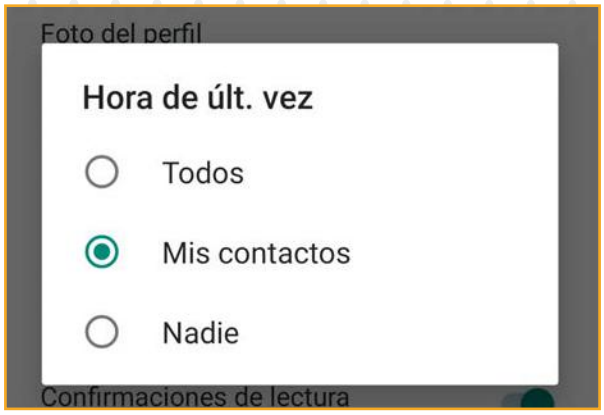
- **Info:** para seleccionar quién puede ver nuestra descripción ('Todos', 'Mis contactos' o 'Nadie').

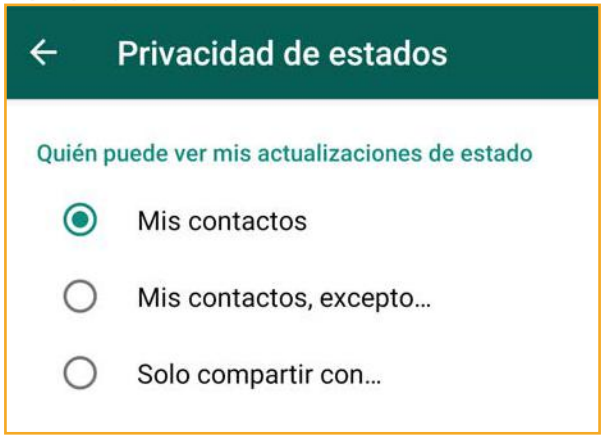
- **Estado:** podemos filtrar para que lo vean todos 'Mis contactos'. Si queremos que ciertos contactos no visualicen nuestros estados, seleccionaremos **'Mis contactos, excepto...'** o **'Solo compartir con...'.**

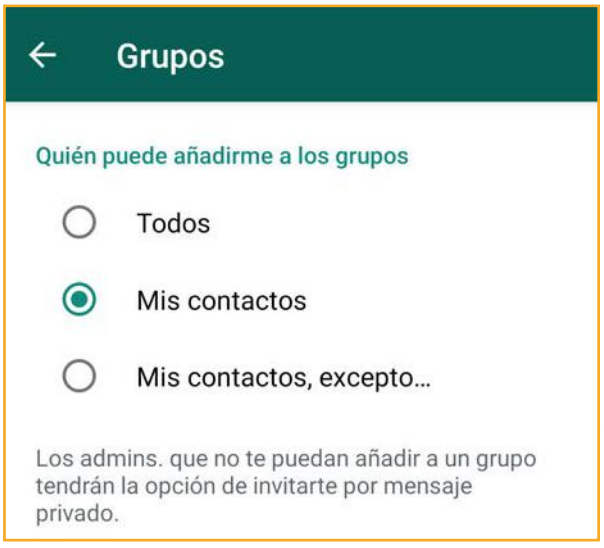
- **Confirmaciones de lectura:** la confirmación de lectura o el famoso "tic azul" nos permite saber si nuestro contacto ha leído nuestro mensaje. **Con esta opción podremos activarlo o desactivarlo**, aunque tampoco veremos las confirmaciones de nuestros contactos.

- **Grupos:** tener muchos grupos puede llegar a ser molesto e incluso peligroso, ya que puede haber contactos desconocidos con malas intenciones. Para evitarlo, haremos clic sobre **'Grupos'** y seleccionaremos quiénes pueden agregarnos a grupos **('Mis contactos' o 'Mis contactos, excepto...').**









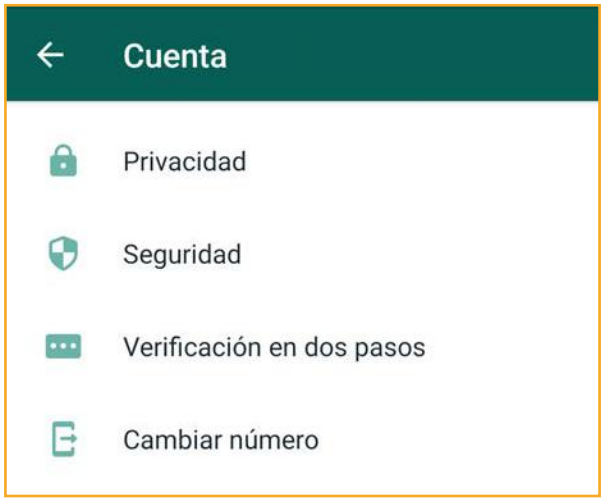
5.3. Cómo configurar nuestro WhatsApp de forma segura

- **Ubicación en tiempo real:** al final de la lista veremos esta opción, que nos informará de si estamos compartiendo nuestra ubicación con algún contacto. Debemos desactivarlo siempre que no lo estemos utilizando (Android e iOS).

- **Contactos bloqueados:** es posible bloquear o reportar contactos desde la aplicación. Hacerlo es muy sencillo, y solo deberemos:
  - Pulsar sobre el icono de **'Añadir contactos'**, situado en la parte superior derecha.
  - Luego, deberemos **seleccionar el contacto** que queramos bloquear.
  - De forma adicional, podemos realizar esta acción desde la conversación con el contacto, pulsando sobre su nombre y haciendo clic sobre **'Bloquear'.**

- **Bloqueo con huella dactilar/bloqueo de pantalla:** algunos dispositivos disponen de una opción para reconocer nuestra huella dactilar o incluso nuestro rostro:
  - En el caso de Android, encontraremos la opción **'Bloqueo con huella dactilar'.** Luego, deberemos seguir los pasos para configurar nuestra huella.
  - En el caso de iOS, encontraremos la opción **'Bloqueo de pantalla'**. Al hacer clic sobre ella, podremos habilitar la función **'Face ID'** o **'Touch ID'**, en función de nuestro dispositivo, para configurar nuestro rostro o huella dactilar.

2. 2. Configurar la verificación en dos pasos. Para habilitar esta función, solo deberemos:



- Volver a **'Ajustes > Cuenta'** y hacer clic sobre **'Verificación en dos pasos' y 'Activar'.**

- Una vez creado, **podremos cambiarlo cuando queramos desde dentro de la aplicación. En caso de olvidar el código, WhatsApp nos enviará un correo electrónico a nuestra cuenta de Gmail con un enlace que nos redirigirá a una**

5.3. Cómo configurar nuestro WhatsApp de forma segura

web desde donde podremos resetear el código. Si no lo hacemos, nuestra cuenta de WhatsApp podría bloquearse durante siete días como medida de seguridad.

3. 3. Configurar Almacenamiento y datos. La aplicación nos permite descargar archivos de todo tipo, así como compartir enlaces:

- Volveremos a **'Ajustes'** y haremos clic sobre **'Almacenamiento y datos'.**

- En **'Descarga automática'** podremos seleccionar qué tipo de archivos descargar en función del tipo de conexión que tengamos:
  - **Datos móviles:** Cuando nos conectemos con los datos contratados con nuestro proveedor de telefonía móvil.
  - **Wi-Fi:** siempre que estemos conectados a una red wifi.
  - **En Itinerancia de datos:** cuando nos conectamos a una red diferente de la que tenemos contratada, como cuando vamos de viaje fuera de nuestro país.

4. Configurar los mensajes temporales. Algunas opciones de configuración se encuentran dentro de las propias conversaciones con nuestros contactos, como es el caso de los **mensajes temporales.**

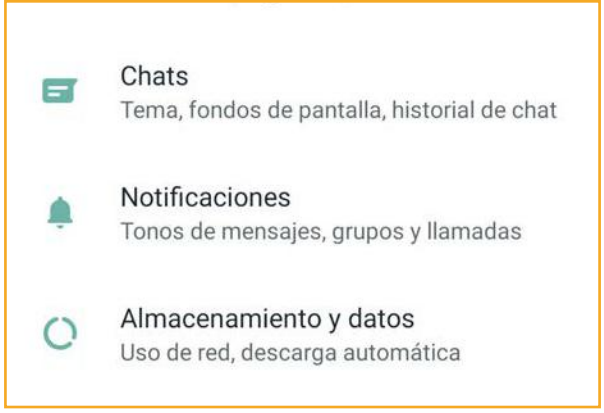
Una vez que activemos esta función en un chat, todos los mensajes que se envíen desaparecerán tras pasar siete días. **Eso sí, los archivos que hayamos descargado seguirán permaneciendo en nuestro dispositivo.**

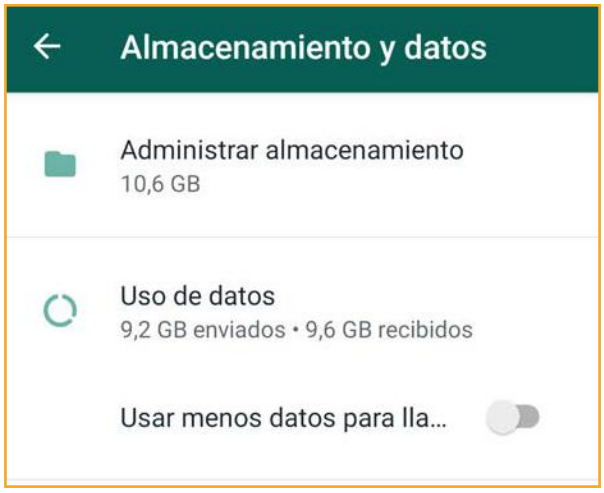
Para activarlo deberemos:

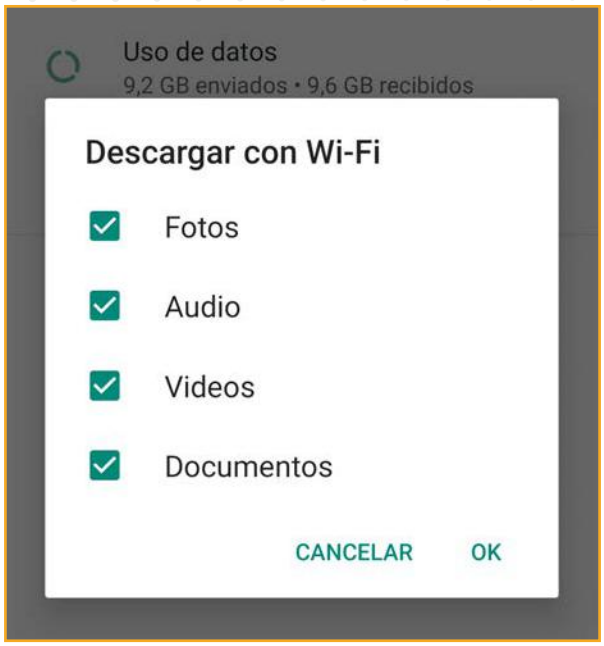
- Pulsar sobre el nombre de nuestro contacto y seleccionar **'Mensajes temporales' > 'Continuar' y 'Activados'** para habilitar la función.

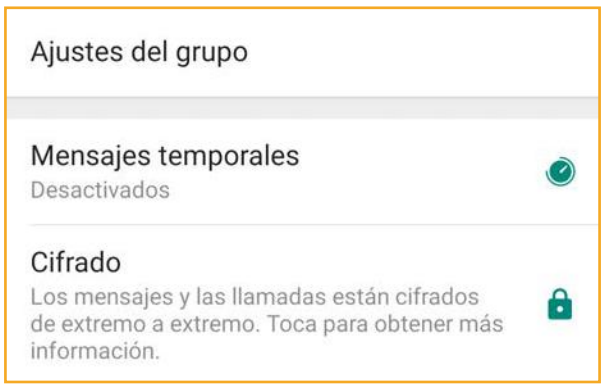
Si queremos conocer más detalles sobre cómo configurar y proteger nuestras comunicaciones por WhatsApp, podemos revisar este enlace*.

*https://www.osi.es/es/actualidad/blog/2021/02/24/mejora-la-privacidad-de-tus-conversaciones-en-whatsapp









6. Checklist de seguridad

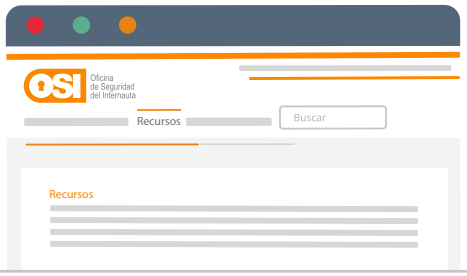
Repasa nuestra lista de acciones ciberseguras y comprueba que todos tus dispositivos están correctamente protegidos.

Dispositivo *(smartphone, tablet, ordenador)*						
Fecha de inspección						
Acciones:	✓	✗	✓	✗	✓	✗
Mi dispositivo está actualizado a la última versión disponible.						
Tengo automatizada la descarga e instalación de actualizaciones de mi dispositivo.						
Tengo instalado y activado un antivirus en mi dispositivo.						
El antivirus está actualizado a la última versión disponible.						
He analizado el dispositivo con el antivirus en busca de virus y malware.						
Tengo activado un sistema de bloqueo para acceder a mi dispositivo (contraseña, PIN, patrón, huella dactilar, etc.).						
Solo yo conozco el sistema de bloqueo/desbloqueo de mi dispositivo.						
En los dispositivos compartidos, solo una de las cuentas corresponde al administrador y es gestionada por un único usuario.						
Mi dispositivo está debidamente cifrado (BitLocker, Android, MacOS o iOS)						

Dispositivo *(smartphone, tablet, ordenador)*						
Fecha de inspección						
Acciones:	✓	✗	✓	✗	✓	✗
Tengo instalados solo programas y aplicaciones legítimas, descargados de repositorios de aplicaciones oficiales o de la web del fabricante.						
Antes de instalar una aplicación, compruebo los comentarios y valoraciones que han compartido otros usuarios sobre ella.						
He eliminado todas las aplicaciones y programas innecesarios que ya no utilizo.						
He revisado los permisos de mis aplicaciones y programas para evitar que tengan acceso a información personal. Además, antes de instalar una nueva aplicación también me fijo en los permisos que solicita.						
He comprobado que todas mis contraseñas son seguras y robustas.						
Tengo activada la verificación en dos pasos en los servicios que lo permiten para proteger mi cuenta.						
Dispongo de una aplicación de verificación en dos pasos para aquellos servicios que no disponen de esta función (Google Authenticator o Microsoft Authenticator).						
Conecto mis dispositivos únicamente a redes wifi seguras.						
He comprobado la configuración de mi router para proteger mi conexión a Internet y a mis dispositivos.						
Mi navegador está actualizado a la última versión disponible.						
Al terminar de navegar elimino los datos de navegación (cookies e historial) para borrar mi rastro.						

Dispositivo *(smartphone, tablet, ordenador)*						
Fecha de inspección						
Acciones:	✓	✗	✓	✗	✓	✗
En caso de utilizar un dispositivo distinto al mío, hago uso de la navegación en modo privado.						
He instalado alguna extensión de seguridad o privacidad en mi navegador y la mantengo actualizada.						
Me conecto solo a páginas web seguras y fiables, y me aseguro de comprobarlo cuando navego.						
He identificado y evitado algún tipo de fraude basado en ingeniería social (correos fraudulentos, anuncios maliciosos, chollos y estafas) mientras navegaba por Internet.						
He recibido, detectado e ignorado alguna cadena de mensajes o noticia falsa que haya llegado a mí.						
Mis cuentas en redes sociales están correctamente configuradas para proteger mi privacidad.						
Mis publicaciones solo son visibles para mis contactos más cercanos.						
Las publicaciones de mi red social no contienen información sensible o personal (direcciones, correos, ubicación, datos bancarios, fotografías íntimas o de menores…).						
He buscado en mis redes sociales perfiles falsos que puedan haber utilizado mi información personal.						
He accedido a la configuración de WhatsApp y he llevado a cabo todos los ajustes y configuraciones de privacidad y seguridad necesarios.						

7. Recursos para ampliar



- ¡Ayuda! Instalé una app no fiable
- ¡Conexión gratis a la vista! ¿Conecto mi móvil?
- ¡No pierdas nada! Protege la información de tu dispositivo
- ¡Sorpresa! El historial te ha delatado
- ¿Hacemos buen uso de las redes sociales?
- ¿Qué es la ingeniería social?
- ¿Sabías que el 90% de las contraseñas son vulnerables?
- ¿Sabrías identificar posibles engaños por la Red? Ponte a prueba
- 7 Datos que nunca debes compartir en Internet
- Blinda tu smartphone
- Cómo comprar online y no caer en el intento
- Cómo disminuir tu rastro en Internet
- Cómo identificar un correo electrónico malicioso
- Cómo saber que navegador me conviene más
- Compra online con cabeza
- Compra segura en Internet
- Conceptos básicos
- Egosurfing: ¿Qué información hay sobre mí en Internet?
- El factor de autenticación doble y múltiple
- El método de pago más seguro
- Gestores de contraseñas: ¿cómo funcionan?
- Guía de Ciberataques
- Guía de privacidad y seguridad en Internet
- Guía para aprender a identificar fraudes online
- Guía para configurar dispositivos móviles
- Identidad digital. ¿Quiénes somos en la red?
- Manual para detectar y denunciar bulos y fake news
- Me robaron la cuenta, ¿qué hago?
- Mejora tus contraseñas
- Muévete seguro por las redes sociales
- No hagas clic en todo lo que lees
- Permisos de apps y riesgos para tu privacidad
- Piénsalo 2 veces antes de publicar
- Principales tipos de virus y cómo protegernos frente a ellos
- Protege tu red en 5 sencillos pasos
- Qué significa el candado que aparece al lado de la URL del navegador
- Qué significa que una web empiece por HTTPS
- Sellos de confianza: acreditando seguridad y privacidad a una web
- Smishing: el fraude de los SMS
- Técnicas de ingeniería social: ¿Cómo consiguen engañarnos?
- Terminología de navegadores web
- Típicos errores que cometemos al usar nuestras contraseñas, y cómo corregirlos
- Un doble en la Red
- Verificación en dos pasos, ¿qué es y cómo me puede ayudar?

8. Denuncia

- Si has sido víctima de un delito o si tienes conocimiento de algún hecho delictivo y quieres ponerlo en conocimiento de la Policía Nacional puedes denunciarlo a través de los siguientes canales:
  - **Presencial**: en cualquier Comisaría de Policía Nacional las 24 horas del día 7 días a la semana.
  - **En línea**: accediendo al sistema de denuncia online a través del portal web de la Policía Nacional.
  - **Telefónicamente**: a través del servicio de denuncias telefónicas para ciudadanos extranjeros mediante el número 902.102.112.

- Para más información puedes consultar la página **www.policia.es**

Experiencia

SENIOR

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA 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
GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR
DIRECCIÓN GENERAL DE LA POLICÍA
POLICÍA NACIONAL