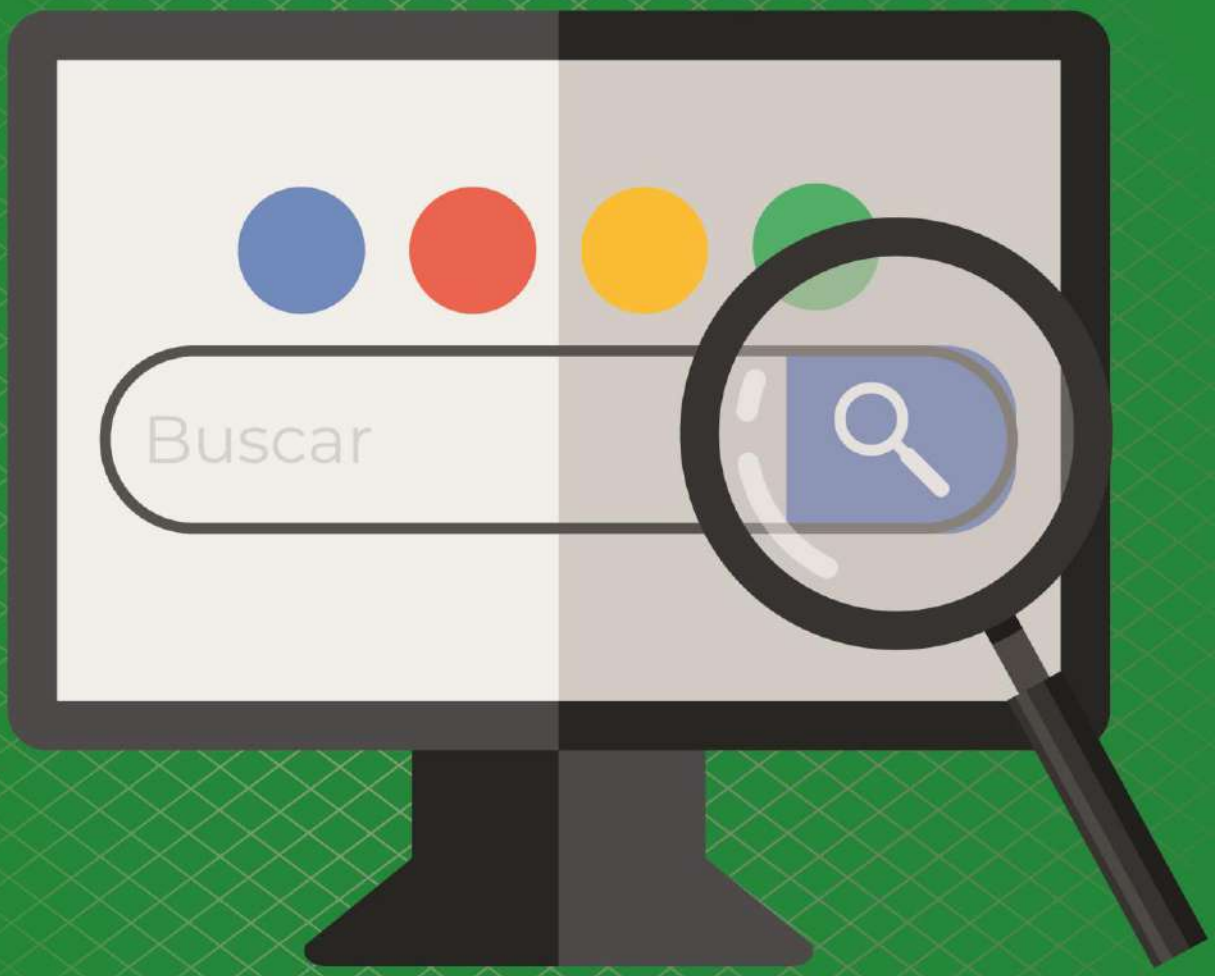
ASOCIACIÓN NACIONAL DE UNIVERSIDADES
E INSTITUCIONES DE EDUCACIÓN SUPERIOR

Dirección General de Administración
Dirección de Tecnologías de la Información y Comunicación



Manual de Navegadores Web

Contenido

¿Qué son los navegadores de internet? 3
Principales navegadores de internet 3
Amenazas al navegar en los navegadores 4
Configurar Chrome para cuidar tu privacidad al navegar en la web 5
Para desactivar la sincronización por completo 6
Las cookies 6
Administrar la información que se recopila durante la navegación 7
Verificar la privacidad desde Mi cuenta de Google 7
Revisión de seguridad 8
Privacidad 9
Los complementos y plugins 10
Actualizaciones 11
Consejos finales 11
Referencias 13

¿Qué son los navegadores de internet?

Los navegadores de internet también conocidos como web browsers, son programas informáticos que brindan el acceso a toda la información que está dispuesta en la web. Es decir, este tipo de softwares están diseñados para interpretar los datos que poseen los diversos sitios, así como sus archivos, permitiendo al usuario una navegación e interacción.

Su función elemental consiste en permitir la visualización tanto de archivos de texto como de recursos multimedia insertos en páginas web, para que de esta manera las personas puedan realizar distintas actividades en ellas, tales como: imprimir, enlazar sitios, recibir y enviar correos, etc.

Poco a poco los navegadores han ido ganando funcionalidades que nos hacen la vida en Internet más fácil: guardan un historial de los lugares que visitamos, autocompletan las palabras o frases que escribimos e, incluso, recuerdan las contraseñas de acceso a los servicios.

Estas prestaciones son muy útiles, pero debemos tener en cuenta que los navegadores son empleados también por individuos malintencionados para acceder a nuestros dispositivos. Por ello, hemos de conocer sus riesgos y adoptar precauciones para poder disfrutar de las ventajas de la tecnología de forma segura.

Principales navegadores de internet

Hoy en día, hay una gran variedad de navegadores de internet entre los que podemos elegir y la elección se puede inclinar hacia uno en particular debido a:

Velocidad y accesibilidad que ofrece al navegar en un sitio.

Opciones de navegación que brinda y adaptación a una versión móvil.

Cada persona escoge su favorito de acuerdo a lo anterior, pero entre los principales navegadores de internet se encuentran Google Chrome, Mozilla Firefox, Safari e Internet Explorer.

Amenazas al navegar en los navegadores

Se entiende como virus Troyano cuando ustedes bajan un programa gratuito de internet de una fuente desconocida, al bajarlo y tener un Troyano, es indetectable por el usuario, después de instalarse el programa o software, propaga el virus Troyano e infecta el equipo desde adentro.

La importancia vital de los navegadores en nuestra vida personal y profesional reside en que se han convertido en la ventana en la que observamos el mundo digital y nos comunicamos con él.

Toda la información que descargamos o transmitimos a los servidores web es susceptible de ser observada o manipulada al igual que la información a al que tiene acceso nuestro navegador, pero que no debería ser transmitida, todo eso convierte a nuestro navegador en una de las principales superficies de ataque aprovechable por muchos tipos de amenazas.

Existe una amenaza creciente de ataques de software que aprovechan los navegadores web vulnerables. Se han observado nuevas vulnerabilidades de software explotadas y dirigidas a los navegadores web mediante el uso de sitios web comprometidos o maliciosos. Este problema se agrava por una serie de factores, incluidos los siguientes:

- Los usuarios tienden a hacer clic en los enlaces.
- Las direcciones de las páginas web se pueden disfrazar o llevar a un sitio inesperado.
- Muchos navegadores web están configurados para proporcionar una mayor funcionalidad a costa de una menor seguridad.
- A menudo se descubren nuevas vulnerabilidades de seguridad después de que el fabricante configura y empaqueta el software.

- Los sistemas informáticos y los paquetes de software pueden incluirse con software adicional, lo que aumenta la cantidad de vulnerabilidades que pueden ser atacadas.
- El software de terceros puede no tener un mecanismo para recibir actualizaciones de seguridad.
- Muchos sitios web requieren que los usuarios habiliten ciertas funciones o instalen más software, poniendo la computadora en un riesgo adicional.
- Muchos usuarios no saben cómo configurar sus navegadores web de forma segura.
- Muchos usuarios no están dispuestos a habilitar o deshabilitar la funcionalidad según sea necesario para asegurar su navegador web.

Como resultado, la explotación de vulnerabilidades en los navegadores web se ha convertido en una forma popular para que los atacantes comprometan los sistemas informáticos.

Configurar Chrome para cuidar tu privacidad al navegar en la web

Chrome tiene una opción que permite sincronizar los datos de navegación de la cuenta de Google para que información como marcadores, contraseña y el historial esté disponible en los diferentes dispositivos que se utilicen. También sirve para iniciar sesión automáticamente en Gmail, YouTube, la búsqueda y otros servicios de Google.

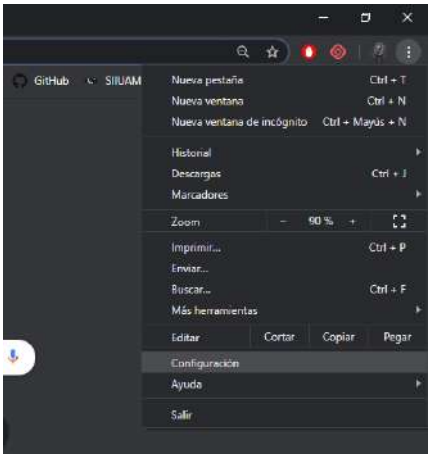
Los datos que se recopilan de este modo ayudan, entre otras cosas, a lograr una experiencia personalizada, como menciona Google en su página de soporte.

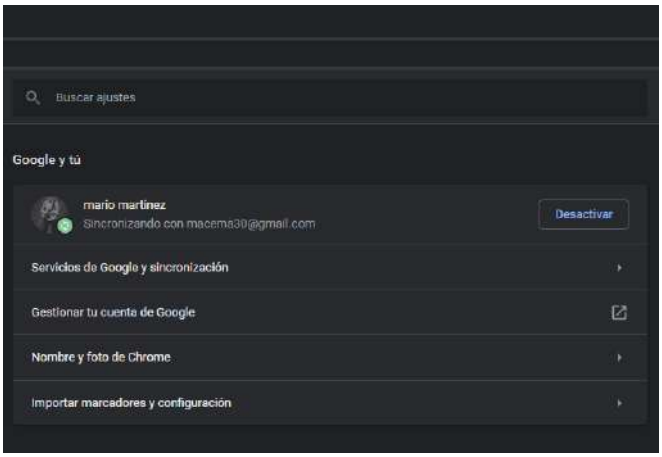
Aunque se desactive la sincronización, los cambios no se guardarán en la cuenta de Google ni se reflejarán en el resto de los dispositivos. Al desactivar la sincronización, también se cierra sesión en los otros servicios de Google, como Gmail.

Para desactivar la sincronización por completo

Hay que presionar en los tres puntos que figuran en el margen superior derecho, e ir hasta **Configuración** y luego allí desactivar la opción de sincronización.

Se puede desactivar la opción de sincronización en Chrome desde el menú de ajustes





Las cookies

Las cookies son pequeños ficheros que los navegadores almacenan en el ordenador con datos del usuario sobre las páginas web visitadas.

Esta información puede contener las opciones de idioma o visualización elegidas, el contenido que ha sido consultado, el identificador de sesión de un usuario o las credenciales de acceso. Su utilidad es facilitar la navegación aunque, una vez guardada, la información puede servir para otros propósitos.

Hoy en día no tenemos, para el usuario medio, muchas alternativas aparte de aceptar el uso de cookies. Si las desactivamos, es posible que algunos servicios no funcionen correctamente. No obstante, puedes borrar periódicamente las cookies instaladas en tu equipo.

Administrar la información que se recopila durante la navegación

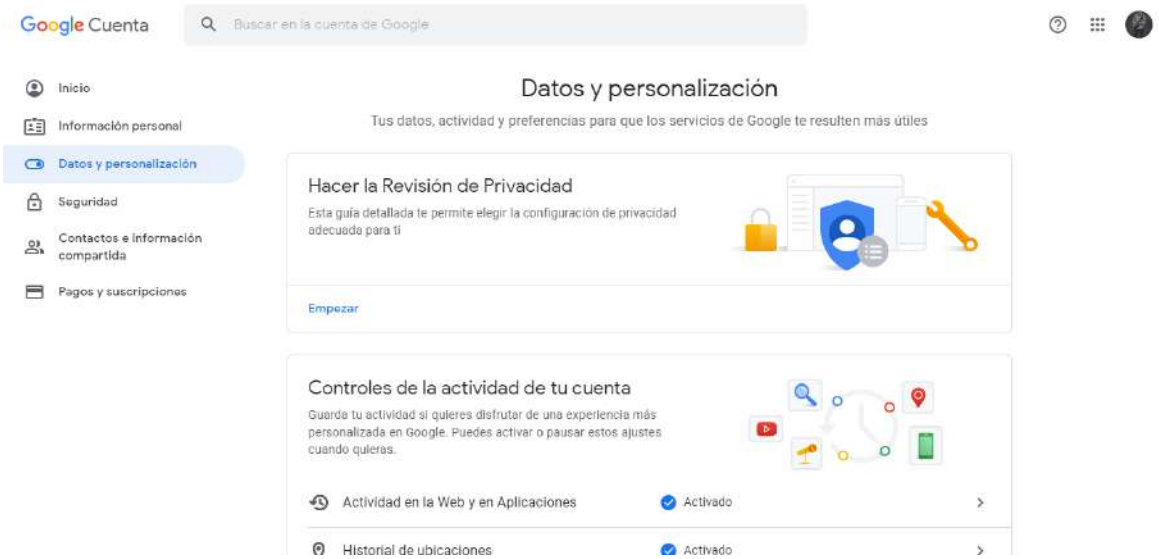
Como se ve, dentro del apartado Privacidad y seguridad hay varias opciones que se pueden gestionar. Una de ellas es la de Configuración del sitio web.

Dentro de **Permisos** se puede ver a qué tipo de información se le va a dar acceso a los sitios web que se visiten. Una de las opciones dice "cookies", que son los archivos que crean los sitios web que se visitan para guardar información de la navegación.

Cabe destacar que hay dos tipos de cookies: las de origen, que son las que crea el sitio que se visita, y las de terceros, que son las que crean otros sitios y que rastrean la actividad del usuario. Se puede desactivar esta opción, pero es posible que algunos sitios requieran que esté activada para poder navegar.

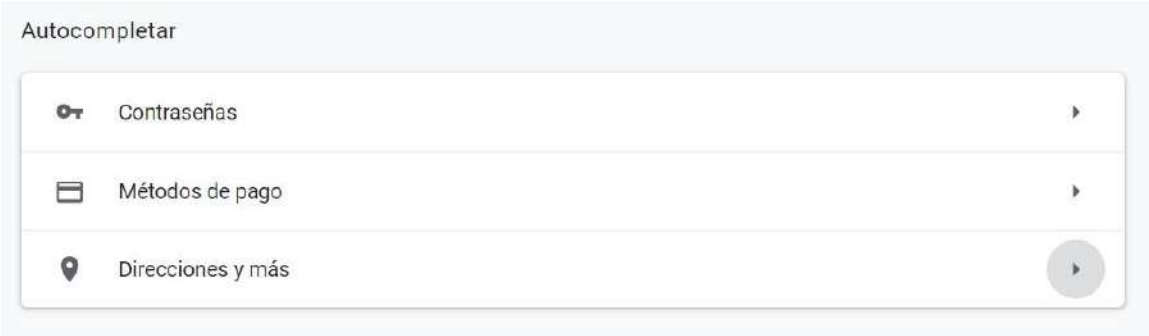
Verificar la privacidad desde Mi cuenta de Google

Se puede hacer un chequeo de la actividad que se está registrando; desde Gmail hay que presionar en el menú punteado en el margen superior derecho, ir hasta Cuenta y allí, en el menú de la izquierda, se verá la opción Datos y personalización. Al seleccionar esta alternativa se verá el apartado Controles de actividad.



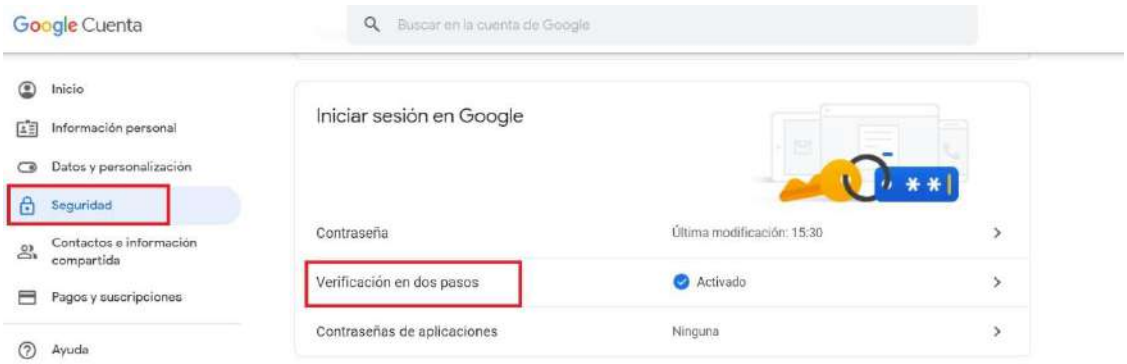
En esta sección es posible administrar y ver qué información se está recopilando: actividad en la web, historial de ubicaciones, actividad de voz y audio (que es lo que se recopila cuando se activa el asistente de voz de Google), etc.

Si se continúa bajando, dentro de esa página también está la opción Autocompletar. Para mayor seguridad, se puede optar por desactivar todas las opciones para que no se ofrezca completar de modo automático los datos de tarjetas, direcciones y contraseñas.



Revisión de seguridad

Otro punto importante para cuidar la privacidad es tomar precauciones para evitar, o al menos disminuir las chances, de que la cuenta sea vulnerada. Dentro del menú de configuración de la cuenta, en el margen izquierdo hay una opción que se llama Seguridad.



Desde el menú de configuración, ingresar en la opción Seguridad

Ingresar allí y activar la verificación de seguridad en dos pasos, si es que ya no se lo hizo. También se puede ver cuáles son todos los dispositivos en los que se inició

sesión con esa cuenta. Si algún equipo no se reconoce o ya no se utiliza, se le puede desactivar la sesión desde ahí.

Privacidad

Los navegadores incorporan muchas funciones para hacernos la vida más fácil. Sin embargo, en ocasiones esto puede suponer un verdadero riesgo para nuestra privacidad:

- El historial de navegación es el registro completo de toda nuestra actividad en Internet. Cualquier persona que tenga acceso a nuestro navegador podrá ver qué hemos estado haciendo y cuándo.
- Normalmente visitamos las mismas páginas web y buscamos cosas parecidas. Por ello cuando tecleamos una búsqueda el navegador nos ofrece una selección de búsquedas basadas en otras anteriores. Esto nos ahorra el trabajo de escribir, por ejemplo, las direcciones completas.

Sin embargo, cualquier persona que emplee nuestro navegador verá esas mismas sugerencias cuando comience a escribir, lo que le dará pistas acerca de nuestro comportamiento y preferencias.

- Es habitual que cada vez más servicios de Internet requieran que utilicemos un nombre de usuario y contraseña para acceder. Que el navegador los recuerde implica que cualquier persona con acceso a nuestro navegador puede suplantar nuestra personalidad en todos esos sitios.
- Si cuando entramos en las redes sociales (Google+, Facebook, Twitter, etc.) seleccionamos la opción de 'mantener la sesión abierta', no bastará con cerrar la página para cerrar la sesión. Cualquiera que entre a estas redes con nuestro navegador tendrá acceso a nuestro perfil.

Normalmente, las funciones que nos hacen la navegación más fácil tienen un lado oscuro: la pérdida de privacidad.

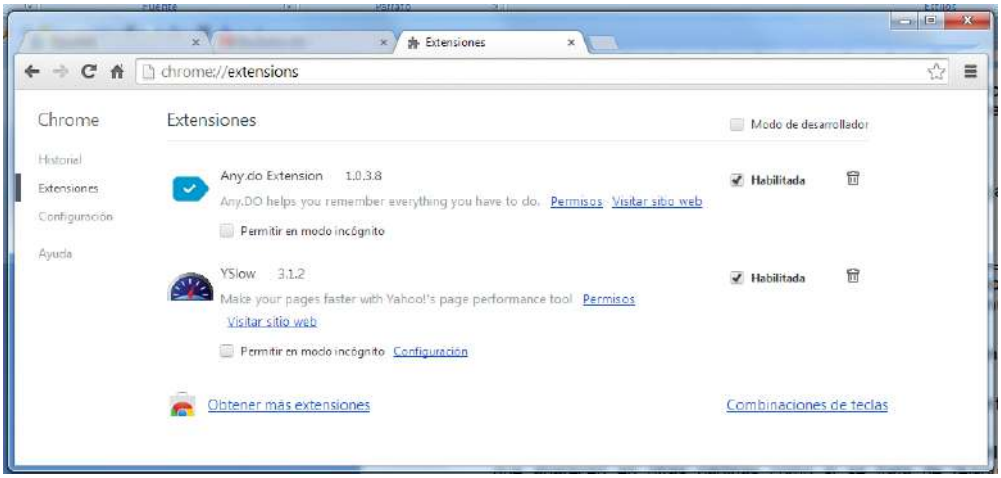
Para limitar los riesgos de privacidad, podemos utilizar las pestañas de navegación privada que existen en los principales navegadores. Éstas reducen la información que el navegador almacena de nosotros, como el historial, cookies, o archivos temporales, lo que resulta muy útil cuando navegamos desde ordenadores públicos.

Los complementos y plugins

Los complementos o extensiones son elementos que se instalan en nuestros navegadores para hacerlos más eficientes, encargándose de funciones específicas: barras de búsqueda, integración con otros servicios, bloqueo de pop-ups, etc.

Sin embargo, algunos de estos complementos pueden estar destinados a fines malintencionados: recopilar información acerca de nuestros hábitos o insertar anuncios. Generalmente, esto se hace de forma encubierta al instalar aplicaciones gratuitas, por lo que es importante revisar las opciones de instalación.

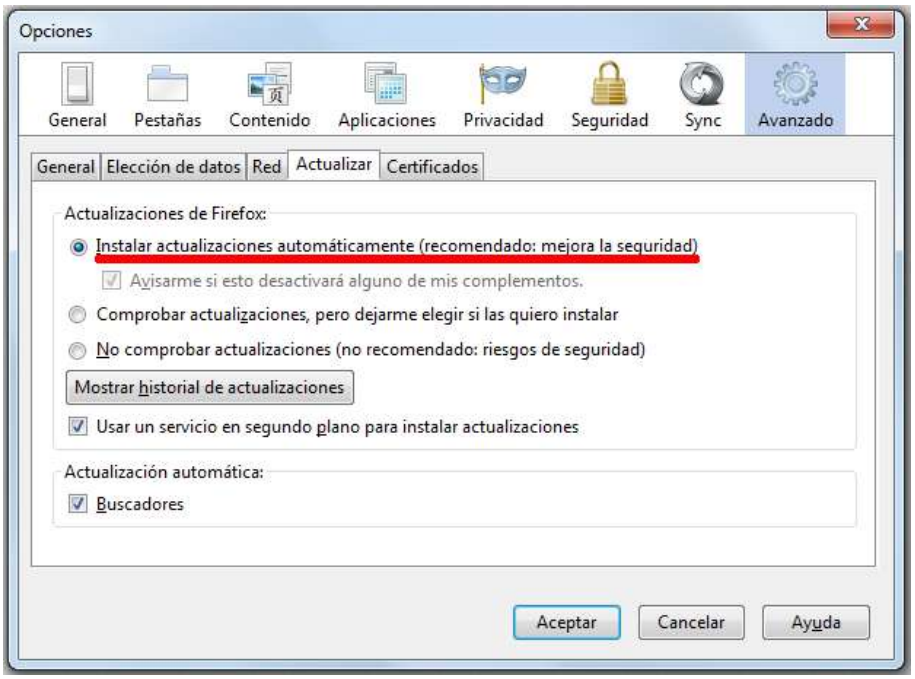
También hay que tener cuidado con algunas aplicaciones asociadas a los navegadores (o plugins) que tenemos instaladas sin ser conscientes de ello: Java, Flash, reproductores de vídeo, etc. Muchas de éstas son utilizadas como vía de acceso para infectar nuestro ordenador debido a sus fallos de seguridad.



Actualizaciones

Los navegadores también están expuestos a fallos de seguridad que pueden suponer una puerta de acceso para que individuos maliciosos accedan a nuestra información o tomen el control de nuestros dispositivos.

Por tanto, hemos de mantenerlos al día, preferiblemente a través de la opción de actualizaciones automáticas. Esta funcionalidad viene incorporada por los principales navegadores.



Las actualizaciones de software son esenciales para mantener la seguridad de nuestros dispositivos y nuestra información.

Consejos finales

Navegar por Internet no es como ver una revista. Si no somos cuidadosos estamos expuestos a toda una serie de riesgos: robo de información, pérdida de privacidad, o perjuicio económico entre otros.

Por tanto, si queremos disfrutar de las ventajas de la tecnología sin incurrir en riesgos debemos tomar ciertas precauciones al navegar:

- Evitar utilizar la opción de recordar contraseñas.
- Cerrar las sesiones a través de la opción 'logout' o 'cerrar sesión', en lugar de simplemente cerrar la ventana.
- Desmarcar la opción de 'mantener la sesión abierta' al iniciar una sesión en redes sociales o servicios de correo electrónico, especialmente si estamos en un equipo compartido.
- Revisar de vez en cuando los complementos y extensiones instaladas. Instalar sólo aquellos con buena reputación y ofrecidos en las páginas oficiales de los navegadores.
- Emplear la opción de navegación 'en privado' en equipos compartidos o públicos.
- Instalar un verificador de páginas web, normalmente proporcionado por los principales antivirus.
- Proteger nuestra privacidad evitando las opciones que permiten al navegador guardar información sensible.
- Familiarizarnos con las opciones de ajuste que ofrece nuestro navegador.
- Mantener el navegador actualizado.
- Estar alerta y no visitar páginas sospechosas.

La mejor herramienta de seguridad es el sentido común. También al navegar por Internet.

Referencias

Y. (2019, 3 diciembre). Navegadores de Internet. Recuperado de https://www.seoenmexico.com.mx/navegadores-de-internet/

M. (2020, 31 enero). Forum.huawei.com. Recuperado de https://forum.huawei.com/enterprise/es/seguridad-inform%C3%A1tica-seguridad-en-los-navegadores-web/thread/599054-100233

A. (2019a, agosto 1). Cómo configurar Google Chrome para cuidar tu privacidad al navegar por la web. Recuperado de https://www.infobae.com/america/tecno/2019/08/01/como-configurar-google-chrome-para-cuidar-tu-privacidad-al-navegar-por-la-web/