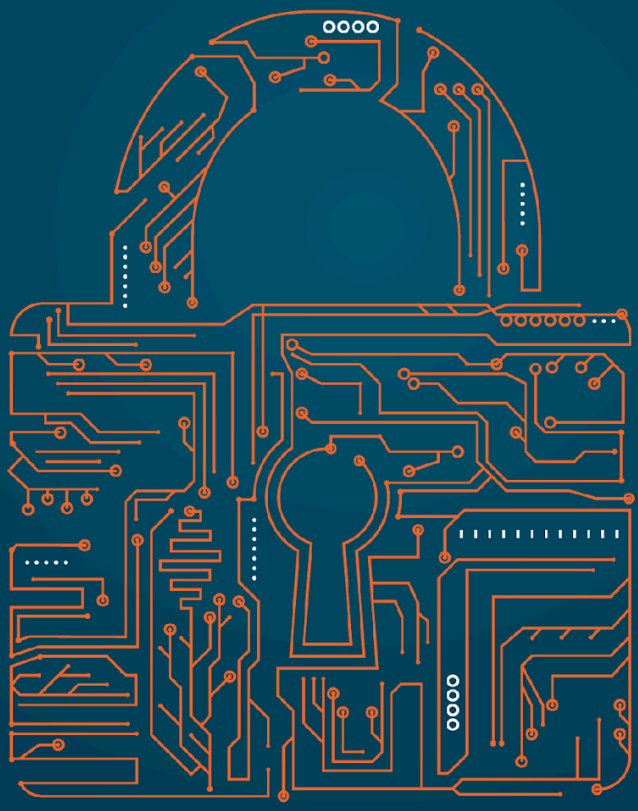
CONEXO



USO Y CONFIGURACIÓN SEGURA DE NAVEGADORES

Edición: Noviembre 2024

Esta obra está bajo una Licencia Creative Commons Atribución-CompartirIgual 4.0 Internacional.

ÍNDICE

1 LA HUELLA DE NAVEGACIÓN 5

2 NAVEGADORES DE INTERNET 6

GOOGLE CHROME 6
Características de seguridad y privacidad: 6

MOZILLA FIREFOX 8
Características de seguridad y privacidad: 8

BRAVE 9
Características de seguridad y privacidad 9

SAFARI 11
Características de seguridad y privacidad: 11

3 COMPARACIÓN DE LAS CARACTERÍSTICAS DE SEGURIDAD Y PRIVACIDAD DE LOS NAVEGADORES 13
PRIVACIDAD EN NAVEGACIÓN DE TELÉFONOS MÓVILES 14
EXTENSIONES 14

4 CONFIGURACIÓN SEGURA DE LOS NAVEGADORES 16

5 RECOMENDACIONES SEGÚN PERFIL DE RIESGO 19

6 REFERENCIAS 20

Los navegadores son elementos fundamentales para nuestra experiencia diaria en internet. Sin ellos sería muy difícil navegar por la web y encontrar la información que necesitamos pero, a pesar de ser muy útiles, estos tienden a almacenar información, fundamentalmente lo que hacemos durante nuestra estadía en la red, lo que puede generar ciertas amenazas dependiendo de nuestro trabajo y perfil de riesgo.

En un mundo donde la tecnología avanza a pasos agigantados, y cada día más aumenta el tránsito de información a través de la internet, es necesario aprender a resguardar nuestra seguridad digital y, sobre todo, mantener la privacidad de nuestros datos.

Este material tiene como objetivo enseñarnos un poco acerca de: qué es la huella digital o huella de navegación, cómo nos puede afectar, qué podemos hacer a la hora de utilizar nuestros navegadores para preservar la seguridad y la privacidad de nuestros datos y mostrarnos las diferentes opciones de navegadores que podemos utilizar. Si bien es cierto que es casi imposible estar protegidos en un 100%, con buenas prácticas y hábitos podemos minimizar este riesgo.

LA HUELLA DE NAVEGACIÓN

La huella de navegación también llamada huella digital, es una técnica de rastreo, diferente a las cookies, que utilizan las empresas con el fin de crear perfiles sobre los usuarios. La Electronic Frontier Foundation (EFF), en la página web de su proyecto “Cover Your Tracks” (2020) especificó:

Una huella digital es, en esencia, una lista de características que son exclusivas de un usuario, su navegador y su configuración de hardware particular. Esto incluye información que el navegador necesita enviar para acceder a los sitios web, como la ubicación del sitio web que solicita el usuario, pero también incluye una serie de datos aparentemente insignificantes (como la resolución de la pantalla y las fuentes instaladas) recopilados por scripts de seguimiento. Los sitios de seguimiento pueden unir todas las pequeñas piezas para formar una imagen única, o "huella digital", de su dispositivo.

A pesar de que esta huella de navegación no se puede relacionar con un rostro y un nombre, la misma proporciona un perfil de quienes somos:rango de edad, ubicación, idioma, intereses, etc. y esta información es vendida a empresas y anunciantes quienes luego nos mandan anuncios personalizados y recomendaciones de sitios web para visitar.

Originalmente esta tecnología se desarrolló para ofrecer seguridad: para prevenir la pirateria de software, el robo de identidad y fraude con tarjetas de crédito, entre otros. Hoy en día, donde la rentabilidad es lo más importante, esta tecnología también permite a las empresas recolectar información y datos que serán la materia prima de los sistemas del futuro. A pesar de que estos elementos recopilados parecieran inofensivos, es una intrusión a nuestra privacidad.

En este sentido, lo primero que podemos hacer para resguardarnos, es adiestrarnos y entrenarnos en cómo podemos hacer para evitar dejar rastros durante nuestra estadía en la internet, y así tratar de resguardar nuestra información de todos estos rastreadores. Para esto es fundamental que sepamos cómo los diferentes navegadores tratan nuestros datos, cómo protegen nuestra información, si es que lo hacen, y qué podemos hacer nosotros al momento de configurarlos para incluir medidas adicionales que eviten, de la mejor manera posible, la filtración de los mismos.

NAVEGADORES DE INTERNET

Los navegadores son programas que nos permiten acceder a las diferentes páginas web. Estos programas interpretan el código de las páginas web y lo muestran de forma que el usuario lo pueda entender.

Existen múltiples navegadores en el mercado, por lo que para esta guía hemos seleccionado la revisión de 4 de ellos considerados como los más populares, o que han sido muy bien evaluados en términos de privacidad por la comunidad, estos son: Google Chrome, Mozilla Firefox, Brave y Safari.

Es importante no confundir los navegadores con los buscadores que son herramientas que nos permiten conseguir información específica en internet con mayor facilidad. Los buscadores rastrean la web en busca de sitios web, imágenes, videos etc. y los presentan de acuerdo a un índice de relevancia. Entre los más populares están: Google, Bing y Yahoo.

A continuación mostraremos las características más importantes de los navegadores antes mencionados, de forma que los diferentes usuarios puedan decidir cuál es la mejor opción para ellos tomando en cuenta sus características y su perfil de riesgo, así cómo se deben configurar para resguardar su seguridad y privacidad.

GOOGLE CHROME



Google Chrome es un navegador gratuito de código abierto, creado por la empresa de Google y lanzado en el año 2008. Es uno de los navegadores más utilizados a nivel mundial debido a su alto rendimiento, simplicidad, compatibilidad con diferentes sistemas operativos y dispositivos, integración con otros productos de Google entre muchas otras características básicas que lo hacen el preferido de muchos usuarios.

Características de seguridad y privacidad:

Buscando ser el navegador preferido por los usuarios, Google Chrome ha ido evolucionando desde su lanzamiento para ofrecer cada vez más seguridad y privacidad. Actualmente entre estas características están:

- **Actualizaciones automáticas:** mantenernos al día con las versiones más recientes del software, incluidos los parches de seguridad, nos proporciona mayor seguridad en la navegación. En las versiones de Chrome para dispositivos móviles, las actualizaciones se administran a

través de Google Play Store en Android o del App Store en iOS. Las extensiones y aplicaciones de Chrome también se mantienen actualizadas con un sistema similar al que se usa para actualizar Chrome.

- **Navegación segura de Chrome**: cuando usamos esta característica, recibimos advertencias que nos protegen contra software malicioso, extensiones y sitios abusivos, phishing, anuncios intrusivos y maliciosos, y ataques de ingeniería social. Podemos elegir entre 3 opciones:
    - **Protección mejorada**: cuando activamos la *Protección mejorada*, recibimos advertencias sobre sitios, descargas y extensiones potencialmente peligrosos, incluso sobre aquellos que Google no conocía.
    - **Protección estándar:** está activada de forma predeterminada. Con ella recibimos advertencias sobre sitios, descargas y extensiones que se identificaron como peligrosos.
    - **Sin protección:** No recomendada.

- **Modo Incógnito**: cuando abrimos una ventana en este modo no se guardará **en el dispositivo** nuestro historial de navegación, las cookies, los datos del sitio ni la información que hayamos ingresado en los formularios. Debemos cerrar las ventanas en modo incógnito para que Chrome descarte la información anterior.
- **Bloqueo de cookies de terceros:** podemos decidir si se permiten las cookies de terceros o no mientras navegamos.
- **Privacidad en los anuncios:** es una opción alternativa, si no se quiere activar el bloqueo de cookies de terceros, para evitar los problemas que puedan surgir en algunas de las funciones de los sitios web. . Esta función ofrece la misma experiencia de navegación sin rastreo que cuando se activa el bloqueo de cookies de terceros.
- **Configuración de sitios**: controla los permisos e información de los diferentes sitios que visitamos.
- **Configuración de sitios seguros:** podemos configurar el navegador para que advierta sobre los sitios que no poseen certificado SSL para navegación cifrada en tránsito (HTTPS).
- **Protección Avanzada:** es un programa de Google diseñado para periodistas, activistas, ejecutivos de grandes empresas y, en general, personas de alto riesgo que manejan información particularmente sensible. Para activarla se necesita una llave de seguridad con los estándares FIDO o una llave de acceso.
- **Encontrar dispositivos y cerrar sesiones en dispositivos perdidos o robados:** podemos usar la opción de encontrar dispositivos en caso de extravío. Si no es posible recuperarlos se podrá cerrar sesión en ellos desde otro dispositivo.
- **Bloqueo de paginas emergentes:** de forma predeterminada, Google bloquea las páginas emergentes para evitar que sitios maliciosos se abran de forma automática.
- **Posibilidad de utilizar complementos o extensiones**: Google Chrome nos permite agregar diferentes extensiones de seguridad y privacidad a

través de su página oficial para personalizar nuestro navegador de acuerdo a nuestras preferencias.

- **Revisión de seguridad**: Chrome ejecuta la verificación de seguridad automáticamente en los dispositivos para ayudarnos a encontrar y solucionar problemas de privacidad y seguridad.

MOZILLA FIREFOX



Mozilla Firefox es un navegador gratuito similar a Chrome, está disponible en más de 90 idiomas y presenta una gran cantidad de funciones para facilitar la navegación. Entre sus características generales destaca: gran capacidad de carga, compatibilidad con el buscador de Google, multiplataformas y dispositivos, actualizaciones automáticas, entre otras.

Características de seguridad y privacidad:

Este navegador es reconocido por las características que posee para resguardar la privacidad y seguridad de los usuarios. Entre estas están:

- **Bloquea los creadores de huellas de navegación conocidos**: la versión más reciente del navegador Firefox protege contra la creación de huellas de navegación (fingerprinting) al bloquear las solicitudes de terceros a empresas que se sabe que participan en su creación. Esta es una configuración predeterminada del navegador.
- **Firefox contiene protección contra *phishing* y *malware*** para garantizar la seguridad mientras navegamos. Al tener activadas estas herramientas, advertirá cuando visitemos una página web que ha sido denunciada como potencialmente peligrosa, como una fuente de software no deseado o un sitio web donde un atacante puede obtener control de los dispositivos. Esta característica también advierte cuando descargamos archivos que puedan estar infectados y sean de tipo malicioso.
- **Posibilidad de usar complementos o extensiones:** Firefox permite agregar diferentes extensiones de seguridad y privacidad a través de su página oficial para personalizar el navegador de acuerdo a nuestras preferencias.
- **Posee la opción de navegación privada:** al utilizar este tipo de navegación, en una ventana nueva, se borrarán todos los datos de navegación y cookies, cuando cerramos la misma.
- **Posee una opción de protección de rastreo mejorada:** para bloquear los rastreadores que nos siguen de un sitio a otro y recopilan información sobre tus hábitos de navegación. A través de una lista de rastreadores conocidos, proporcionada por *DIsconnect,* Firefox bloquea diferentes tipos de rastreadores y script, como por ejemplo: rastreadores de redes sociales, criptomineros, cookies de sitios cruzados, entre otros Esta configuración se puede hacer en 3 niveles diferentes: estándar, estricto y

personalizado. La opción de *Cookie Total Protection,* está habilitada de forma predeterminada en el modo estándar.

- **Permite configurar el modo *Solo-HTTPS:*** al hacer esto el navegador avisará cuando una página no posea cifrado en la capa de transporte antes de acceder a la misma.

BRAVE

Es un navegador web de código abierto basado en Chromium, creado por la compañía Brave Software en el año 2016, fundada por el cofundador del Proyecto Mozilla y creador de JavaScript, Brendan Eich. En 2019 se lanzó para Windows, MacOS, Linux, Android y iOS.

Este navegador es compatible con 6 buscadores, entre los cuales se puede elegir cuál será el predeterminado para las ventanas regulares y las de incógnito: Brave, Google, DuckDuckGo, Qwant, Bing y Startpage.

Una característica importante de nombrar es que a pesar de bloquear los anuncios, Brave propone una solución para apoyar a los creadores de contenido a través de un sistema de recompensas. Los usuarios pueden obtener tokens (BAT) al visualizar anuncios opcionales, que luego pueden ser canjeados o donados.

Características de seguridad y privacidad

Este navegador se caracteriza por dar prioridad a la privacidad de los datos de los usuarios, por lo que cuenta con varias funciones específicas en este sentido:

- **Privacidad por defecto**: de entre todos los navegadores web populares, Brave es el que dispone de las protecciones más potentes en materia de privacidad, y lo hace de forma predeterminada. Estas protecciones se presentan en tres capas diferentes:
    - **Escudos Brave:** permiten bloquear rastreadores, cookies de terceros, la huella de navegación entre otros. Adicionalmente permite ver lo que se ha bloqueado. Esto viene en la configuración estándar, pero se puede personalizar en el modo estricto. Una característica muy importante es que Brave realiza una selección aleatoria de la huella de navegación, para evitar el rastreo que se genera a partir de ella, es decir, Brave hace que nuestra apariencia sea distinta en cada sitio que visitamos y cada vez que reiniciamos el navegador, de modo que los sitios no podrán utilizar la huella de navegación para rastrearnos de un sitio a otro ni de una sesión a otra.

- **Protecciones Avanzadas:** esta segunda capa integra muchas funciones y personalizaciones de Chromium en el navegador. Como se explicó antes Brave se basa en el código abierto de Chromium, pero conforme se publican nuevas actualizaciones Brave, modifica, e inclusive elimina, funciones que no son aptas para la privacidad del usuario. Entre estas están:
  - La modificación de la sincronización para que la información de los usuarios esté cifrada y no llegue a los servidores de Google.
  - Eliminación de funciones como la de generación de informes de Google, los temas y las API de estado de la red, entre otros.
  - Limitación de las llamadas de servidores de red. Brave trata de limitar la frecuencia con la que el navegador se comunica con su servidor de actualizaciones en busca de nuevas versiones e información nueva.
  - Eliminación de forma predeterminada de los parámetros de seguimientos de las URL, como los identificadores de clics de Facebook y Google, evitando así que nos rastreen cuando visitamos un sitio web
  - Mejoras en la política de referencia, que es el sistema que los navegadores y sitios web utilizan para informar a un sitio de destino sobre el sitio web de origen. Brave reduce la cantidad de información presente en el encabezado de referencia, para proteger la privacidad del usuario.
  - Bloqueo de RRSS, esta opción tratará de evitar que los sitios que visitamos permitan hacer inicio de sesión con las cuentas de Google o Facebook.
  - Protección frente al rastreo de redirecciones: tratando de evitar la protección contra rastreadores, la industria publicitaria ha diseñado el rastreo de redirecciones, que consiste en ocultar el rastreador en el enlace de la página que quieres visitar. Cuando Brave detecta que vas a visitar un dominio conocido por tener rastreadores, omite la visita a ese dominio y te redirecciona a la página de destino sin pasar por el dominio intermedio.
  - Limitación de la vida de las cookies JavaScript a 7 días, además de ofrecer otras opciones para borrar las cookies en cualquier momento.
- **Politicas y practicas:** el compromiso de la empresa es cumplir e ir más allá de las protecciones reglamentarias de los datos, como el *Reglamento General de Protección de Datos* (RGPD) y la *Ley de Privacidad del Consumidor de California* (CCPA), así como asistir y contribuir con la comunidad que lucha por la privacidad en línea.

Adicionalmente, hay otras características de seguridad y privacidad en su configuración importantes de mencionar tales como:

- **Enviar solicitud de "*No Rastreo*":** al activar esta característica se envía la solicitud a la página para evitar el rastreo a la hora de visitarla. Las páginas que respetan esta solicitud dejarán de rastrear de forma automática.
- **Ventanas privadas o modo incógnito:** evita que otras personas que usen nuestros dispositivos puedan conocer nuestra actividad en línea.
- **Ventanas privadas de Tor:** Brave dispone de una integración con Tor para ofrecer mayor privacidad. Utilizando esta característica se ocultará tu dirección IP, para garantizar tu anonimato.
- **Extensiones o complementos:** aunque Brave posee su repositorio de extensiones, también es compatible con las extensiones de Google Chrome, lo que lo hace ideal si queremos añadir alguna otra extensión.
- **Verificación de seguridad:** Brave verifica con regularidad que el navegador tenga la configuración más segura. En caso de que haya algo que revisar te avisará.

SAFARI



Safari es un navegador web de código cerrado, desarrollado por Apple Inc. Está disponible para macOS, iPadOS e iOS, desde el año 2003. Si posees un dispositivo Apple esta es tu mejor opción, ya que es un navegador que fue diseñado específicamente para estos sistemas operativos. Se puede personalizar de múltiples formas e incluye diferentes características que protegen tu privacidad como: evita el seguimiento entre sitios web y minimiza los datos que se comparten con terceros, entre otras.

Características de seguridad y privacidad:

- **Prevención de Rastreo Inteligente:** esta función viene configurada de forma predeterminada y oculta tu dirección IP de los rastreadores para que los anunciantes no sepan que buscas en le web
- **Navegación Privada:** al activar esta función, no se agregaran al historial de navegación los sitios visitados, el navegador no recordará los temas buscados ni la información de los formularios que se completen. Incluye funciones de protección contra el rastreo y seguimiento por huella digital, para evitar que puedan identificar tu dispositivo.
- **Llaves de acceso**: estas te permitirán iniciar sesión de forma más sencilla y segura, son privadas y no se almacenan en ningún servidor. No salen de tu dispositivos y solo pueden usarse en el sitio web donde la creaste. Están encriptadas de extremo a extremo y se sincronizan con tus dispositivos Apple con el Llavero de iCloud
- **Reporte de Privacidad:** este reporte te permitirá conocer los rastreadores bloqueados con la funcionalidad Prevención de Rastreo Inteligente de Safari.

- **Prevención de rastreo de widgets en redes sociales:** los widgets de redes sociales que se usan en los sitios web, pueden monitorear tu actividad aunque no los uses. Safari bloquea este seguimiento automáticamente e impide a los widgets conocer tu identidad, a menos que sea autorizado por ti.
- **Protección contra seguimiento:** Safari impide que los anunciantes y sitios web usen las características únicas de tu dispositivo para crear una "huella digital" que permita rastrear tu actividad. Para lograr esto el navegador presenta una versión simplificada de la configuración del sistema. Así, muchos dispositivos parecen ser idénticos y es más difícil identificar el tuyo.
- **Búsqueda:** Safari minimiza la cantidad de datos que se envía a los motores externos de búsqueda, por lo que no comparte cookies ni tu ubicación exacta, como lo hacen otros buscadores.
- **Controles de extensiones:** las extensiones a pesar de ser muy útiles pueden usarse para rastrearte o registrar los sitios web que visitas. Con estos controles tu podrás decidir cómo se accede a tu información.

COMPARACIÓN DE LAS CARACTERÍSTICAS DE SEGURIDAD Y PRIVACIDAD DE LOS NAVEGADORES

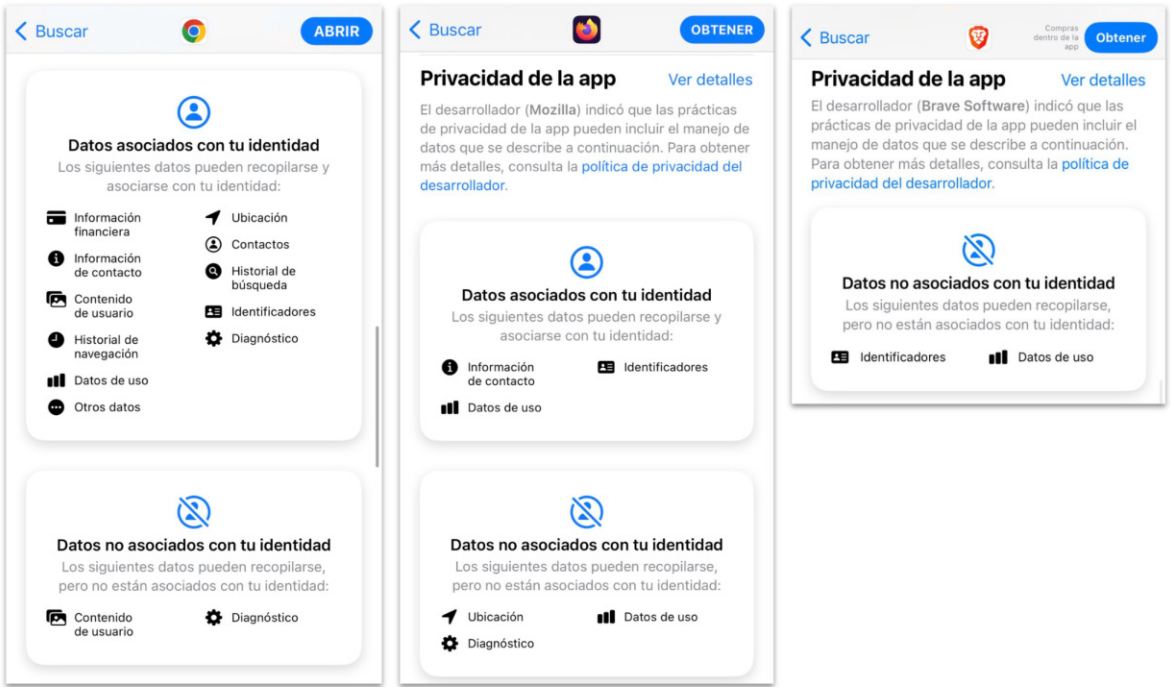
A continuación te presentamos un cuadro comparativo con las principales características de privacidad y seguridad de cada navegador:

	Google chrome	Mozilla Firefox	Brave	Safari
BLOQUEO DE ANUNCIOS DE TERCEROS	! (E)	! (E)	✓	!
BLOQUEO DE VENTANAS EMERGENTES	✓	✓	✓	!
BLOQUEO DE COOKIES DE TERCEROS	!	✓	✓	✓
PROTECCIÓN CONTRA HUELLAS DE NAVEGACIÓN	✗	!	✓	✓
NAVEGACIÓN SEGURA ESTÁNDAR	✓	✓	✓	✓
USAR CONEXIONES SEGURAS HTTPS	✓	✓	✓	✓
VENTANA DE INCÓGNITO O PRIVADA	✓	✓	✓	✓
VENTANA DE INCÓGNITO CON TOR	✗	✗	✓	✗
OPCIÓN DE "NO RASTREO"	!	!	!	!
OPCIÓN DE CONFIGURAR EL BORRADO DE INFORMACIÓN AL CERRAR LA VENTANA	✗	!	!	✗
VERIFICACIÓN DE SEGURIDAD	!	✗	!	✗
REPORTE DE PRIVACIDAD	✗	✗	✗	✓
PROTECCIÓN CONTRA PHISHING Y MALWARE	✓	✓	✓	✓
PERSONALIZAR INFORMACIÓN A COMPARTIR	✓	✓	✓	✓

Habilitado por defecto ✓ Se puede habilitar o usar extensión (E) ! No posee la opción ✗

PRIVACIDAD EN NAVEGACIÓN DE TELÉFONOS MÓVILES

Por otro lado, si comparamos la información compartida por los desarrolladores en sistemas Android o iOS, podemos observar cómo de estos 3 navegadores Brave es el que menos datos recopila:



EXTENSIONES

Adicionalmente, si bien es cierto que Brave tiene muchas funcionalidades de privacidad predeterminadas, también es cierto que podemos agregarle más privacidad a muchos de los otros navegadores instalando algunas extensiones. Entre estas podemos recomendar:

- **uBlock Origin:** es un bloqueador de anuncios que evita las páginas emergentes intrusivas, los rastreadores invasivos y los anuncios maliciosos.

uBlock Origin

- **Privacy Badger:** esta extensión permite bloquear las herramientas de rastreo, los scripts que tienden a registrar tus visitas y crear perfiles basados en los sitios web que visitas.

Ambas extensiones están disponibles en Firefox, Chrome y Brave.

Google Chrome está migrando a **Manifest V3** que es la versión más reciente de la plataforma de extensiones.

Esta nueva plataforma buscaría mejorar la privacidad, seguridad y rendimiento de las extensiones, sin embargo, por lo pronto y al menos hasta la migración total en 2025, está siendo afectado el uso de extensiones que usan Manifest V2, como en el caso específico de la extensión **uBlock Origin.** Por ello **es necesario descargar la nueva versión uBlock Origin Lite**. Esta nueva versión es menos efectiva en el bloqueo de anuncios que la anterior debido a las restricciones que impone la nueva plataforma a la API Declarative Net Request. A diferencia de Google Chrome, Mozilla Firefox no tiene planes de desuso de MV2 y continuará admitiendo extensiones con esta plataforma a corto plazo y, han dicho que de cambiarla, darían un aviso de al menos 12 meses para que los desarrolladores se adapten. En este sentido, te recomendamos **evaluar** el uso de Firefox como tu navegador predeterminado si estas características se adaptan más a tus necesidades.

Cover Your Tracks

Esta herramienta desarrollada por la EFF te permitirá saber cuál es tu huella de navegación según la configuración que tienes en tu navegador y el dispositivo que utilizas para navegar. Te recomendamos realizar el test antes y después de que realices las configuraciones de seguridad que te recomendamos en esta guía para que observes los cambios.

CONFIGURACIÓN SEGURA DE LOS NAVEGADORES

A continuación presentamos una lista de verificación a tomar en cuenta para configurar de manera más segura y privada nuestros navegadores.



RECOMENDACIONES GENERALES

- Verifica que tengas la **última actualización** del navegador.
- Verifica que tengas activada la **seguridad estándar.** Evalúa la posibilidad de activar la protección mejorada (rígida o personalizada en Firefox).
- Verifica que tengas activa la opción de **usar siempre conexiones seguras** (conexiones con **HTTPS**).
- Verifica que tengas activa la opción de **bloqueo de cookies de terceros**.
- Evalúa activar la opción de "**do not track**".
- Borra con frecuencia tu información de navegación: historial de páginas, historial de descargas, cookies, memoria caché, autocompletado de formularios. Es importante que hagas de esto un **hábito.**
- Verifica si tienes guardadas tus contraseñas en el navegador, de ser así, evalúa la opción de migrar a un **administrador de contraseñas** como 1Password, Bitwarden o Proton Pass. Por diseño los navegadores no son los sitios más seguros para almacenar nuestras contraseñas.
- Evalúa la opción de **desactivar** la función de **sugerir guardar la contraseña y el acceso automático en los navegadores.**
- Verifica que tengas activa la opción de **advertencias para violaciones de información de contraseñas.**
- Verifica los **permisos** que tienes activos en el navegador.
- Verifica qué **extensiones** tienes **descargadas y activas** y verifica que estén **actualizadas**.
- Utiliza **bloqueadores de anuncios y de rastreadores** como **uBlock Origin y Privacy Badger.**
- Utiliza una **VPN** para ocultar tu información IP, al menos cuando naveges en sitios que pueden ser sensibles en tu país.

Ten en cuenta que estas configuraciones podrían variar de un navegador a otro, ya que en algunos casos estos ajustes podrían estar de forma predeterminada.

RECOMENDACIONES PARA *GOOGLE CHROME*

- Evalúa qué opciones **quieres deshabilitar** en la parte de **privacidad en los anuncios.**
- Evalúa la opción de **habilitar el Programa Avanzado de Protección de Google.**
- Realiza la **verificación de seguridad de Chrome** cada cierto periodo de tiempo.

RECOMENDACIONES PARA *MOZILLA FIREFOX*

- Verifica que tengas activada la opción de **Eliminar cookies y datos del sitio** cuando **cierre Firefox.**
- Verifica que tengas activa la opción de **protección contra contenido engañoso y software peligroso.**
- Evalúa si quieres enviar la solicitud de **no vender mis datos.**
- Verifica los permisos activos en el navegador.
- Verifica que tengas **deshabilitadas** las opciones de **autocompletado: direcciones y métodos de pago.**
- Evalúa la opción de habilitar el **Modo permanente de navegación privada** para evitar que se guarde información de tu historial de navegación. Si no deseas habilitarlo puedes personalizar esta función decidiendo qué datos se van a borrar cuando se cierren las ventanas de Firefox.
- Verifica que tengas habilitada la **función de bloqueo de paginas emergentes.**
- Verifica que tengas activa la opción **de advertencia cuando los sitios web intentan instalar complementos.**
- Verifica que **información quieres compartir con Firefox** y **desactiva** aquellas que consideres necesarias.
- Verifica que tengas **deshabilitada la opción de preferencias de publicidad.**

RECOMENDACIONES PARA *BRAVE*

- Verifica que tengas **activa el bloqueo anuncios** por lo menos en el **modo estándar**. Evalúa si quieres usar el **modo agresivo.**
- Verifica que tengas **activa las conexiones HTTPS** por lo menos en el **modo estándar.** Evalúa si quieres usar el **modo agresivo.**
- Verifica que tengas **activo** el **bloqueo de huellas de navegación.**
- Verifica que tengas **activo** el **bloqueo de cookies de terceros.**
- **Activa** la opción de **borrado de cookies y otros datos al cerrar la ventana.**
- Evalúa si quieres configurar el **borrado automático de la información al cerrar las ventanas.**
- Verifica que tengas **habilitada la ventana privada de Tor.**
- Verifica qué **información deseas compartir con Brave.**
- Evalúa qué opción deseas como **buscador predeterminado**. Si quieres **más privacidad** utiliza **Brave** o **DuckDuckgo.**
- Evalúa **deshabilitar** las opciones **de guardado y autocompletado en formas de pago.**
- Realiza la **verificación de seguridad de Brave** cada cierto periodo de tiempo.

RECOMENDACIONES PARA *SAFARI*

- Verifica que tengas **activa** la opción **de prevenir el rastreo de sitios.**
- Verifica que tengas **activa** la opción **de Ocultar la dirección IP de los rastreadores.**
- Verifica que tengas **activa activa** la opción **de advertir al visitar un sitio de internet fraudulento.**
- Verifica los sitios web que **tienen permisos** para abrir ventanas emergentes.
- Revisa periódicamente el **reporte de privacidad.**

RECOMENDACIONES SEGÚN PERFIL DE RIESGO

Al momento de seleccionar un navegador debemos tener en cuenta varios factores de forma que podamos decidir cuál se adapta mejor a nuestras necesidades. Entre estos factores están:

- Para qué quiero utilizar el navegador
- Qué integraciones necesito que posea con otros servicios
- Cual es mi sistema operativo
- Cual es mi trabajo y cual es mi perfil de riesgo asociado a él
- Que nivel de privacidad necesito

Tomando en cuenta esta información podemos escoger cual es el navegador que se adapta mejor a nuestras necesidades, por ejemplo:

- Si buscamos **compatibilidad y simplicidad** una buena opción es **Google Chrome**, el cual nos permite trabajar con múltiples usuarios, se puede sincronizar con otros servicios de Google como Gmail, Drive, entre otros, permitiéndonos tener todo en un solo lugar. Pero no todo es perfecto. Su lado débil es la privacidad, por lo que si queremos utilizar este navegador y adicionalmente proteger nuestra información, tendríamos que configurarlo de la mejor manera posible añadiendo incluso extensiones, tomando en cuenta las limitaciones que puede traer consigo la nueva plataforma de Google Chrome Manifest V3.

- Si lo que buscamos es un **alto nivel de privacidad** la opción más clara es **Brave**, que por defecto trae activas múltiples configuraciones con el fin de resguardar nuestros datos, de las cuales una de las más importante es la protección contra la huella de navegación. Brave obtuvo los mejores resultados en la prueba de privacidad de Cover Your Tracks de la EFF. Adicionalmente, si quisiéramos más privacidad y anonimato, podemos abrir una ventana de navegación privada con **Tor**, pero tenemos que tener en cuenta que su nivel de compatibilidad es menor, tiene una menor selección de extensiones en comparación con Chrome y Firefox, es menos popular, ofrece menos opciones de personalización y puede no ser tan eficiente o estar vetado en tu ubicación geográfica.

- El navegador de **Mozilla Firefox** se encuentra en un **punto medio** entre estos dos últimos. Posee más características de privacidad predeterminadas que Google Chrome, lo cual lo hace más llamativo para algunos usuarios y, al mismo tiempo, su rendimiento, velocidad, compatibilidad y sincronización entre equipos es mayor a la de Brave. Pero su compatibilidad con los servicios de Google, consumo de recursos y extensiones disponibles es menor que la de Chrome.

REFERENCIAS

Activar o desactivar la opción “Do Not Track.” (n.d.). Google.com. Consultado el 20 de Septiembre 2024, de https://support.google.com/chrome/answer/2790761?hl=es&co=GENIE.Platform%3DAndroid

Ayuda de Google Chrome. (n.d.). Google.com. Consultado el 20 de Septiembre 2024, de https://support.google.com/chrome?hl=es-419

Cómo bloquear o permitir ventanas emergentes en Chrome. (n.d.). Google.com. Consultado el 20 de Septiembre 2024, de https://support.google.com/chrome/answer/95472?hl=es-419&ref_topic=7439640

Compare Firefox with other browsers. (n.d.). Mozilla. Consultado el 22 de Septiembre 2024 , de https://www.mozilla.org/en-US/firefox/browsers/compare/

Complementos y extensiones del navegador Firefox. (n.d.). Mozilla. Consultado el 18 de Septiembre 2024, de https://www.mozilla.org/es-ES/firefox/features/add-ons/

Comprende la privacidad en Chrome. (n.d.). Google.com. Consultado el 20 de Septiembre 2024, de https://support.google.com/chrome/answer/14225066?hl=es-419&ref_topic=9845306&sjid=12191752588463274l9-NA

Cover your tracks. (n.d.). Eff.org. Consultado el 21 de Septiembre 2024, de https://coveryourtracks.eff.org/learn

El bloqueador de anuncios – un arma secreta contra la publicidad molesta. (n.d.). Mozilla. Consultado el 18 de Septiembre 2024, de https://www.mozilla.org/es-ES/firefox/features/adblocker/

¿Es Firefox un navegador privado? (n.d.). Mozilla. Consultado el 18 de Septiembre 2024, de https://www.mozilla.org/es-ES/firefox/features/private/

El navegador que te da prioridad. (n.d.). Brave. Consultado el 19 de Septiembre 2024, de https://brave.com/es/

Firefox bloquea el rastreo de huellas digitales (fingerprinting). (n.d.). Mozilla. Retrieved Consultado el 18 de Septiembre 2024, de https://www.mozilla.org/es-ES/firefox/features/block-fingerprinting/

Firefox sigue volviéndose cada vez más rápido. (n.d.). Mozilla. Consultado el 18 de Septiembre 2024, de https://www.mozilla.org/es-ES/firefox/features/fast/

Funciones de seguridad y protección de la privacidad. (n.d.). Brave. Consultado el 19 de Septiembre 2024, de https://brave.com/es/privacy-features/

Google cybersecurity innovations - Google safety center. (n.d.). Safety.Google.Consultado el 21 de Septiembre 2024, de https://safety.google/cybersecurity-advancements/

Información de. (n.d.). Brave. Consultado el 19 de Septiembre 2024, de https://brave.com/es/about/

Kessler, D. (2018, 26 de Julio). This is Your Digital Fingerprint. Mozilla.org. https://blog.mozilla.org/en/privacy-security/this-is-your-digital-fingerprint/

Klosowski, T. (13 de julio, 2020). Our favorite ad blockers and browser extensions to protect privacy. The New York Times. https://www.nytimes.com/wirecutter/reviews/our-favorite-ad-blockers-and-browser-extensions-to-protect-privacy/

Modo de navegación privada de Firefox. (n.d.). Mozilla. Consultado el 18 de Septiembre 2024, de https://www.mozilla.org/es-ES/firefox/features/private-browsing/

Privacidad -Prestaciones. (n.d.). Apple (España). Consultado Septiembre 21, 2024, de https://www.apple.com/es/privacy/features/

Safe, secure, protected browsing. (n.d.). Google.com. Consultado el 20 de Septiembre 2024, de https://www.google.com/chrome/safety/

See how Brave stacks up against other browsers. (n.d.). Brave. Consultado el 20 de Septiembre 2024, de https://brave.com/compare/

Szymielewicz, K., & Budington, B. (2018, 19 de Junio). The GDPR and browser fingerprinting: How it changes the game for the sneakiest web trackers. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2018/06/gdpr-and-browser-fingerprinting-how-it-changes-game-sneakiest-web-trackers

Walther. (2023, 10 de Agosto). Brave Browser: Ventajas y Desventajas que deberías conocer. Tutoriales Dongee. https://www.dongee.com/tutoriales/brave-browser-ventajas-y-desventajas-que-deberias-conocer/

Roth, E. (2024, October 15). Google Chrome's uBlock Origin phaseout has begun. The Verge. https://www.theverge.com/2024/10/15/24270981/google-chrome-ublock-origin-phaseout-manifest-v3-ad-blocker

Sullivan, E. (2024, March 13). Manifest V3 & Manifest V2 (March 2024 update). Mozilla Add-Ons Community Blog. https://blog.mozilla.org/addons/2024/03/13/manifest-v3-manifest-v2-march-2024-update/