Controles de seguridad

Privacidad en navegadores web

La recopilación y el seguimiento de datos se han convertido en una epidemia digital en la última década, ya que la información de la persona usuaria se ha convertido en el producto más grande del mundo. Los principales navegadores son algunos de los peores delincuentes.

En particular, *Google Chrome*, *Microsoft Edge* y *Safari* usan *cookies* (que veremos más adelante), para rastrear los sitios web que visita y mantener registros de su historial de navegación, todo para enviarle anuncios dirigidos.

¿Cómo configurar la privacidad en los navegadores web?

Una de las formas más simples de cubrir sus pistas *en línea* es eliminar manualmente el historial de su navegador. Todos los navegadores web, como *Internet Explorer*, *Firefox*, *Safari* o *Google Chrome*, le permiten eliminar el historial de navegación web.

Google Chrome

Google Chrome tiene mucho cuidado para mantener su información personal privada. Ofrece varias formas de controlar su privacidad, incluida la modificación de su configuración de privacidad, la eliminación de su historial y la navegación en modo *incógnito*.

Chrome le permite controlar parte de la información que comparte *en línea*, que puede modificar en su configuración de privacidad. Recomendamos que no cambie las selecciones predeterminadas de *Chrome*, ya que permiten el mejor equilibrio de privacidad y seguridad mientras navega. Sin embargo, puede modificarlas si lo desea.

Para modificar la configuración de privacidad:

- Haga clic en el menú de *Chrome* en la esquina superior derecha del navegador, luego seleccione *Configuración*.
- Localice y seleccione *Mostrar configuración avanzada*.

- Las opciones de privacidad aparecerán. Para modificar la configuración de privacidad básica, como habilitar la protección contra *malware*, marque o desmarque las casillas junto a cada opción.
- Para modificar configuraciones específicas, como cuando las páginas web pueden guardar *cookies* o acceder a su ubicación, haga clic en el botón *Configuración de contenido*.

Eliminar sitios específicos del historial:

- Haga clic en el menú de *Chrome* en la esquina superior derecha del navegador y luego seleccione *Historial*.
- Haga clic en la casilla de verificación junto a cada enlace que desea eliminar de su historial, luego elija *Eliminar elementos seleccionados*.
- Aparecerá un cuadro de diálogo. Haga clic en *Eliminar* para continuar.
- Los sitios web seleccionados se eliminarán de su historial.

Mozilla Firefox

La última versión de *Firefox* se ha configurado para ***compartir datos técnicos y de interacción*** con *Mozilla*. Es recomendable deshabilitar esta configuración.

Para deshabilitar, vaya a Abrir menú (tres barras en la esquina superior derecha del navegador)> Opciones > Privacidad y seguridad > Recopilación y uso de datos de *Firefox*, y luego desmarque las casillas.

También puede deshabilitar el intercambio de datos con *Firefox* para *Android* yendo a Menú > Opciones > Privacidad > Opciones de datos y luego desmarque las tres categorías para Telemetría, *Crash Reporter* y Servicio de ubicación de *Mozilla*.

Firefox ahora utiliza como motor de búsqueda predeterminado a *Google*, pero existen otros motores de búsqueda privados que puede utilizar en su lugar.

Para hacer esto, vaya a Menú > Opciones > Buscar > Motor de búsqueda predeterminado. *Firefox* no le da demasiadas alternativas directamente en el área de configuración. Sin embargo, puede ver más opciones yendo a *Motores de búsqueda* con un clic y luego dé clic en *Buscar más motores de búsqueda*, para ver las otras alternativas.

Opera

Para administrar su configuración de seguridad en *Opera*, haga lo siguiente:

- Vaya a *Opera*> Configuración. Aparece la ventana de Configuración.
- Haga clic en Privacidad y seguridad en el panel de navegación izquierdo.
- Haga clic en *Administrar certificados* para obtener una descripción general de sus certificados instalados. Aparece la ventana del Administrador de certificados.
- Puede ver, eliminar, importar o exportar cualquiera de estos certificados. Luego, haga clic en Aceptar.
- Para no permitir ninguna *cookie* en su ordenador, seleccione *Bloquear sitios* para que no configuren ningún dato y Bloquear *cookies* de terceros y casillas de verificación de datos del sitio.

Brave

Hay algunas características en *Brave* que le permiten mejorar su experiencia de navegación conectándose a un servicio web. La mayoría de estos están desactivados *por defecto*.

Para administrar su configuración de privacidad y seguridad :

- Inicie *Brave* y abra el menú.
- Vaya a Configuración → Avanzado → Privacidad y seguridad.
- Seleccione de la lista de configuraciones de privacidad y seguridad:
    - Servicio de predicción para ayudar a completar búsquedas y *URL* escritas en la barra de direcciones.
    - Servicio de predicción para cargar páginas más rápidamente
    - Navegación segura
    - Política de manejo de *IP* de *WebRTC*
    - Enviar automáticamente informes de fallos a *Brave*
    - Enviar una solicitud de «No rastrear» con su tráfico de navegación
    - Permitir que los sitios verifiquen si tiene métodos de pago guardados
    - Administrar certificados
    - Configuración de contenido
    - Eliminar datos de navegación

Microsoft Edge

Puede modificar cómo *Microsoft Edge* maneja la configuración de privacidad para mantener segura la información sobre sus hábitos de navegación o identidad.

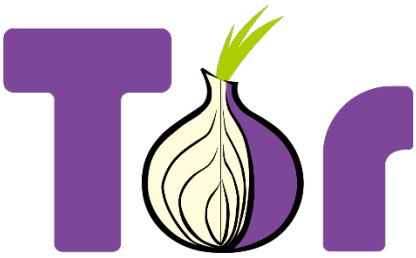
- En *Microsoft Edge*, haga clic en el botón *Más acciones* y luego en *Configuración*.
- Mueva el puntero del ratón hacia el borde derecho del panel *Configuración* para mostrar la barra de desplazamiento, desplácese hacia abajo y haga clic en *Ver configuración avanzada* en *Configuración avanzada*.
- En el panel de *Configuración avanzada*, desplácese hasta la parte inferior del panel, más allá del encabezado *Privacidad y Servicios*. Haga clic en la lista desplegable debajo de *Cookies*, luego en *Bloquear todas las cookies* o *Bloquear solo las cookies de terceros*.
- Presione *Esc* o haga clic fuera del panel para cerrarlo.

También puede usar la configuración *Bloquear ventanas emergentes* cerca de la parte superior del panel *Configuración avanzada*. Cuando se activa esta configuración en *Microsoft Edge*, se evita que se carguen ventanas emergentes cuando visita un sitio. Si bien las ventanas emergentes generalmente muestran anuncios inofensivos o molestos, algunas pueden estar asociadas con esquemas de *phishing* o *malware*, por lo cual su ordenador es más seguro con las ventanas emergentes bloqueadas.

Iridium

Es un navegador basado en el proyecto *Google Chrome*, pero el equipo de *Iridium* cambió el código para respetar la privacidad.

Tor



Usar el navegador *Tor* es un acto de equilibrio entre la privacidad / seguridad y la usabilidad web. De forma predeterminada, la seguridad está configurada en Estándar, aunque todavía es mucho más segura que cualquier otro navegador web.

Si desea aumentar esto, haga clic en el ícono de cebolla a la izquierda de la barra de direcciones y seleccione *Configuración de seguridad*. Use el control deslizante *Nivel de seguridad* para elegir su nivel de protección preferido, teniendo en cuenta las advertencias que aparecen sobre las funciones que pueden dejar de funcionar en los sitios que visita.

Mientras navega por *Internet*, el navegador *Tor* le ayuda a mantenerse seguro al evitar conectarse directamente a sitios web. En cambio, su conexión rebota entre múltiples nodos en la red *Tor*, y cada salto presenta anonimato.

Epic Privacy

Una de las opciones existentes para navegar por *Internet* con mayor seguridad y privacidad es *Epic Privacy*. Dentro de sus funciones, cabe destacar el modo de incógnito. En la casualidad casi todos los navegadores modernos disponen de una opción de este tipo, que no registra lo que visitamos en el historial, ni las búsquedas.

El modo de incógnito de *Epic Privacy* viene aplicado *por defecto* y no existe opción de quitarlo.

Además de esto, impide el rastreo de sitios visitados. También se bloquean las *cookies* de manera automática. También tiene un *proxy* cifrado que es posible activar con un solo clic.

Puede enmascarar la *IP* real de la persona usuaria con este *proxy* integrado y cifrar los datos transmitidos.

Cookies

Una *cookie* es un fichero de datos que una página web le envía a su ordenador cuando la visita. Da igual si está entrando a la web desde el ordenador o desde el móvil, siempre se solicitará el almacenamiento de la *cookie*. Tampoco importa si entra desde un navegador independiente o desde el navegador integrado en alguna herramienta o aplicación, también se solicitará la *cookie*.

La solicitud de almacenamiento del fichero de información en su ordenador la hará directamente el servidor de la web a la cual entra, en el mismo momento en el que accede a ella. Por lo general, notará que se está solicitando la utilización de *cookies* porque las webs están obligadas a avisarle y a preguntar cuáles quiere usted instalar.

Las *cookies* suelen utilizarse principalmente para dos finalidades principales: recordar accesos y conocer hábitos de navegación. Las *cookies* hacen que las páginas web puedan identificar su ordenador, y, por lo tanto, si vuelve a entrar a ellas podrán recordar quién es usted y qué ha hecho antes dentro de ellas.

Las *cookies* no son malas por naturaleza, ya que son útiles al recordar sus configuraciones y estados en las webs que ha visitado en su actual sesión de navegación. También ayudan a recordar otros datos como que prefiere usted usar el tema oscuro en una web, que está buscando vuelos a Los Ángeles o que su divisa preferida es el colón.

Pero también sirven para conocer la información sobre sus hábitos de navegación, algo que pueden utilizar terceros para enviarle información relacionada a sus intereses, pero también para identificarle como usuario(a), según las páginas que visita.

Algunas empresas como *Facebook* y otros servicios publicitarios insertan paquetes de *cookies* en muchísimas de las webs que visita en *Internet*, aunque no estén relacionadas con sus servicios. De hecho, cuando configura las *cookies* puede fijarse en que uno de los apartados que puede deshabilitar es el de los socios comerciales, que son precisamente las empresas de publicidad.

Estas *cookies* son como cámaras de vigilancia colocadas por estas empresas por todo *Internet*, de manera que pueden saber en qué páginas entra y, por lo tanto, crear un perfil de sus gustos personales.

También pueden registrar sus búsquedas en los buscadores como *Google* o *Bing*, o los internos de tiendas *online*, también para conocer sus gustos y necesidades.

De esta manera, se puede crear un perfil sobre usted y sus gustos que luego se puede vender o intercambiar con otras empresas. Así, cuando visita una web que tiene instalado determinado sistema de publicidad, gracias a las *cookies* que ese sistema tiene en todo *Internet* puede mostrar anuncios de temas que sabe que le van a gustar. Esto también vale para cuando *Google*, *Facebook* o *Twitter* venden publicidad, ya que ellos también tienen sus datos.

Esto propicia que los anunciantes puedan pagar por crear campañas publicitarias orientadas a determinado público. Por ejemplo, una marca deportiva posiblemente prefiera centrarse en los(as) usuarios(as) a quienes les gusten los deportes, ya que si compran una campaña de un número concreto de impresiones (cada impresión es una vez que le aparecen a alguien), mostrarle publicidad de zapatillas de *running* a alguien que no ha corrido en su vida posiblemente sea tirar el dinero.

¿Qué tipo de *cookies* se pueden configurar?

Existen diferentes tipos de *cookies* cuando entra en una web. Los primeros dos tipos son las *cookies* temporales y las permanentes. Las *cookies* temporales solo permanecen en su navegador hasta que se va de la página web, por lo cual no se quedan instaladas en su navegador u ordenador. Las *cookies* permanentes o persistentes, en cambio, se quedan en el disco duro de su ordenador para que la página que las instala pueda leerlas e identificarle cada vez que vuelva a visitarla. Suelen tener fecha de expiración.

Las *cookies* también pueden ser propias o de terceros. Las propias son las que utiliza una página web, y que han sido diseñadas por esta misma web. Las *cookies* de terceros son las que otras empresas y servicios le han pedido a la página web que también instalen en su ordenador cuando accede a ella.

También hay *cookies* cuyos tipos varían según la finalidad que tienen. Cuando suele entrar en un navegador y le preguntan si quiere usted configurar las *cookies*, normalmente podrá activar o desactivar grupos de *cookies* dependiendo de sus finalidades.

Las *cookies* técnicas o necesarias son esas que nunca va a poder desactivar en la configuración de *cookies* de una web. Permiten, por ejemplo, que las páginas puedan controlar el tráfico y la comunicación de los datos internos, que se puedan finalizar procesos de compra, utilizar elementos de seguridad, o guardar en su navegador contenidos cuando elige las opciones de compartir, para luego poder compartirlos en redes sociales. En definitiva, sirven para optimizar el funcionamiento de la web.

En segundo lugar, tenemos las *cookies* de preferencias o de personalización. Son esas que almacenan sus preferencias y configuraciones en las webs a las cuales ha accedido anteriormente. Por ejemplo,

permiten recordar su idioma predeterminado, el tipo de navegador que utiliza, o la configuración regional desde la cual ha entrado.

Las *cookies* de rendimiento y análisis sirven para que la página que visita pueda recopilar la información relacionada sobre lo que hace en ella. Analiza todo lo que hace en una web mientras está en ella, y con ello pueden saber, por ejemplo, si no llegó a terminar un proceso de compra o en qué enlaces suele hacer clic más a menudo. Esto les permite tener estadísticas masivas con las cuales saber qué elementos se usan más, o dónde puede haber problemas y errores.

Y, por último, tiene las *cookies* publicitarias o de *marketing*, las cuales sirven para gestionar la publicidad que se incluye en las webs. A través de estas *cookies* se crea un perfil con sus intereses analizando de forma continuada su comportamiento en la web. Por ejemplo, tras instalar estas *cookies*, algunas podrían ir analizando las páginas en las cuales entra o las búsquedas que realiza, y así poder saber sus gustos. Con ello, se crean perfiles que pueden vender o ceder a anunciantes, para mostrar publicidad que pueda ser relevante.

Lo que pasa cuando se desactivan las *cookies*, dependerá de las *cookies* que desactive. Si simplemente borra las *cookies* de su ordenador a través del navegador, borrará también las *cookies* que guardan sus inicios de sesión. Al hacerlo, tendrá que volver a iniciar sesión en todos sitios escribiendo sus nombres de usuario y contraseñas. También se perderán sus preferencias, teniendo que reconfigurar algunos parámetros en webs, y al borrarlas también tendrá que volver a configurar las *cookies* de todas las webs. Si en la configuración de *cookies* de una web desactiva las publicitarias, cuando esté navegando en esa web no se estará recopilando lo que hace en ella con el fin de completar el perfil de sus gustos personales. Pero esto solo se aplica a la web donde lo ha configurado, por lo cual las empresas publicitarias pueden seguir recopilando la información en otras webs.

En términos de privacidad, ha de saber siempre que cuantas menos *cookies* active, más privacidad tendrá a la hora de navegar por *Internet*, pero menos personalización tendrá de su experiencia de navegación. Así pues, la clave está en que encuentre su equilibrio personal entre privacidad y experiencia. Puede incluso hacer que su navegador no guarde *cookies* o buscar uno que las borre automáticamente, para maximizar esa privacidad.

Borra con frecuencia las *cookies* de su ordenador

Para evitar todo esto, le recomendamos que borre con frecuencia las *cookies* de su ordenador. A continuación, le ofrecemos algunos enlaces donde encontrará información práctica para aprender a eliminar las *cookies* de su navegador:

- *Google Chrome*: https://goo.gl/AwLwfD
- *Mozilla Firefox*: https://goo.gl/QRhMEI
- *Internet Explorer*: https://goo.gl/swHnam

Otra opción es bloquear o eliminar las *cookies* instaladas anteriormente en su equipo, configurando las opciones de su navegador. En los siguientes enlaces encontrará información muy útil sobre cómo puede activar las preferencias en los navegadores más utilizados:

- *Google Chrome:* https://goo.gl/2BHhBs
- *Mozilla Firefox:* https://goo.gl/yXYrXt
- *Internet Explorer:* https://goo.gl/NTEoD4

Herramientas *anti-phishing*

Existen varias técnicas diferentes para combatir el *phishing*, incluyendo la legislación y la creación de tecnologías específicas que tienen como objetivo evitarlo.

Respuestas organizativas: entrenar a los(as) colaboradores(as) en el reconocimiento de posibles ataques.

Respuestas técnicas: existen varios programas informáticos *anti-phishing* disponibles. La mayoría de ellos trabajan identificando contenidos *phishing* en sitios web y correos electrónicos, algunos *softwares anti-phishing* pueden integrarse con navegadores web y clientes de correo electrónico como una barra de herramientas, revisando el dominio real del sitio visitado, con filtros de *spam*.

Los diferentes navegadores también poseen opciones que se pueden activar para prevenir y detectar los *phishing*.

Le invitamos a indagar sobre las opciones del mercado y las disponibles con su navegador web y su antivirus.