INSTITUTO NACIONAL DE CIBERSEGURIDAD

GESTIÓN DE LA PRIVACIDAD, IDENTIDAD DIGITAL Y REPUTACIÓN ONLINE EN INTERNET

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

INSTITUTO NACIONAL DE CIBERSEGURIDAD

017

MÓDULO 4

Navegación segura por Internet

ÍNDICE

1. Navegación segura por Internet

Para navegar seguros por Internet, en primer término, nosotros, como usuarios, debemos seguir una serie de hábitos y buenas prácticas para proteger nuestra privacidad y seguridad de aquellos riesgos a los que nos exponemos al navegar por Internet.

Pero **¿Cuáles son los riesgos a los que podemos enfrentarnos?**

- **Acceder a información falsa.**

Aunque en Internet hay mucha información fiable, no debemos olvidarnos de que también existen "*fake news*" o noticias falsas, que inducen a los usuarios a creer una información no real, para crear controversia o perjudicar la imagen de una persona o entidad.

- **Seguridad y privacidad.**

Existe peligro real como puede ser la usurpación de la identidad, conocidos como malware y phishing, los cuales pueden poner en riesgo nuestros datos personales y financieros.

El *phishing* consiste en suplantar la identidad solicitando información bancaria y personal al usuario mediante enlaces webs.

El malware es un software diseñado exclusivamente para robar y/o extraer información de un sistema informático sin el consentimiento de la persona afectada.

Además, también existe, una amenaza real de robo de datos si se llevan a cabo varias acciones, como, por ejemplo, usar una red ajena a nosotros a través de páginas web fraudulentas de diferente índole.

- **Contenido no apropiado.**

En Internet se pueden encontrad multitud de contenidos inapropiados y de fácil acceso, de tipo violento o de pornografía, y todo ello a través de una simple búsqueda.

- **Uso excesivo de la tecnología.**

Actualmente son muchas las personas que utilizan los dispositivos tecnológicos convirtiéndose está práctica en una conducta bastante asidua y recurrente en el día

a día. Este uso puede repercutir gravemente a la salud, desencadenando trastornos en el comportamiento relacionado con el uso desmedido de las nuevas tecnologías.

- **Ciberacoso.**

El acoso en la red puede tomar varias vertientes que van desde el acoso verbal, pasando por el social o incluso llevarse al plano sexual. Estas situaciones pueden materializarse en diferentes canales de Internet, como son las redes sociales, juegos en línea o foros.

A continuación, se muestra un artículo de la revista Europapress sobre el ciberacoso entre niños y adolescentes.

https://forbes.es/ultima-hora/328434/bullying-los-expertos-de-buencoco-advierten-de-la-importancia-de-la-empatia-como-recurso-de-prevencion/

Para evitar las acciones anteriormente señaladas, existen una serie de recomendaciones que nos ayudaran a navegar de forma más segura por Internet:

1. **Tener actualizado nuestro sistema operativo, *software* o aplicaciones:** Las actualizaciones, aparte de ofrecernos mejoras, solventan posibles vulnerabilidades conocidas que pueden comprometer la seguridad de nuestros dispositivos.
2. **Tener antivirus**: En todos los dispositivos conectados a Internet, debemos tener instalado un antivirus, tenerlo actualizado para una mayor protección ante nuevos virus y ejecutarlo periódicamente.
3. **Utilizar un navegador seguro:** Es importante conocer el navegador que utilizamos y configurar las opciones de seguridad y privacidad según nuestras preferencias. Existen también *plugins* (pequeños programas que se instalan en el navegador) que pueden proporcionar una capa de seguridad adicional. Tenemos a nuestra disposición diversas categorías, por ejemplo, para bloquear anuncios, eliminar *cookies*, notificarnos de riesgos, etc.
4. **Comprobar enlaces dudosos y webs sospechosas:** Es habitual que al navegar por Internet saltemos de una web a otra casi sin darnos cuenta, por ejemplo, utilizando motores de búsqueda, a través de enlaces que nos aparecen, etc. Debemos ser cautelosos a la hora de hacer clic y entrar en enlaces que nos pueden llevar a páginas web fraudulentas.

5. **Usar contraseñas seguras:** Utilizar claves fuertes que combinen letras mayúsculas, minúsculas, caracteres especiales así como números para proteger las distintas cuentas en línea.
6. **Uso razonable de las nuevas tecnologías**. No excederse en el tiempo de conexión, hacer un uso responsable de las nuevas tecnologías.
7. **Realizar copias de seguridad de los datos**. Para evitar perder información importante. Ver enlace

IMPORTANTE

Es aconsejable escribir directamente la URL en el navegador, en lugar de llegar a ella a través de enlaces disponibles desde páginas de terceros, en correos electrónicos o mensajes de texto.

Algunos indicios que nos pueden ayudar a saber si una página es segura son:

- ***HTTP / HTTPS***: Lo primero en lo que deberemos fijarnos es en el tipo de protocolo que aparece al comienzo de la *url*. A diferencia del ***http***, el https utiliza el **protocolo de cifrado SSL/TLS** que garantiza que la comunicación no se podrá leer ni manipular y que la información personal no caerá en las manos equivocadas, como nuestras credenciales, datos personales y/o bancarios.

- **Certificado de seguridad**: Podemos comprobar que una web tiene certificado de seguridad si dispone de un icono de un candado a la izquierda de la *URL*. Se trata de un certificado expedido por una empresa o autoridad de certificación, que acredita que la información intercambiada va a estar cifrada y que la web pertenece a quien dice ser.

  Se puede hacer clic en el candado para comprobar los detalles del certificado. Es importante asegurarse que esté emitido por una autoridad confiable, y, además, que esté en vigor.

Como los ciberdelincuentes se reinventan, muchas páginas fraudulentas ya presentan estas características (https y certificado), por lo que en estas situaciones, debemos seguir haciendo más comprobaciones.

- **Tener precaución con las redes wifi públicas**: Se debe prestar atención a las redes wifi a las que nos conectamos. A pesar de las ventajas y comodidades que ofrecen el poder conectarnos a una red wifi de una cafetería, un hotel o centros comerciales, son poco seguras al no saber quién más está conectado a ellas y cuáles son sus intenciones. Es por ello que en caso de conectarnos a wifis públicas, no debemos realizar acciones en las que se envíe información personal, como realizar compras, interactuar con la app de nuestro banco o acceder a una red social.

- **Comprobar el historial de navegación, *cookies* y ficheros temporales**: Las *cookies* son archivos creados por los propios sitios web que visitamos que ayudan a que, entre otras cosas, las páginas se carguen más rápido y guarden las preferencias de navegación. En general, permiten una navegación más fácil en esos sitios web. Se recomienda borrar periódicamente el historial de navegación, las *cookies* y los ficheros temporales, así como deshabilitar la opción de "recordar contraseña" y cerrar todas las sesiones al salir.

- **Políticas de Privacidad**: Revisar la política de privacidad de la página web, ya que los sitios seguros normalmente tienen políticas claras sobre el manejo de datos de los usuarios. Además, ofrecen información de contacto para posibles dudas o problemas que puedan aparecer.

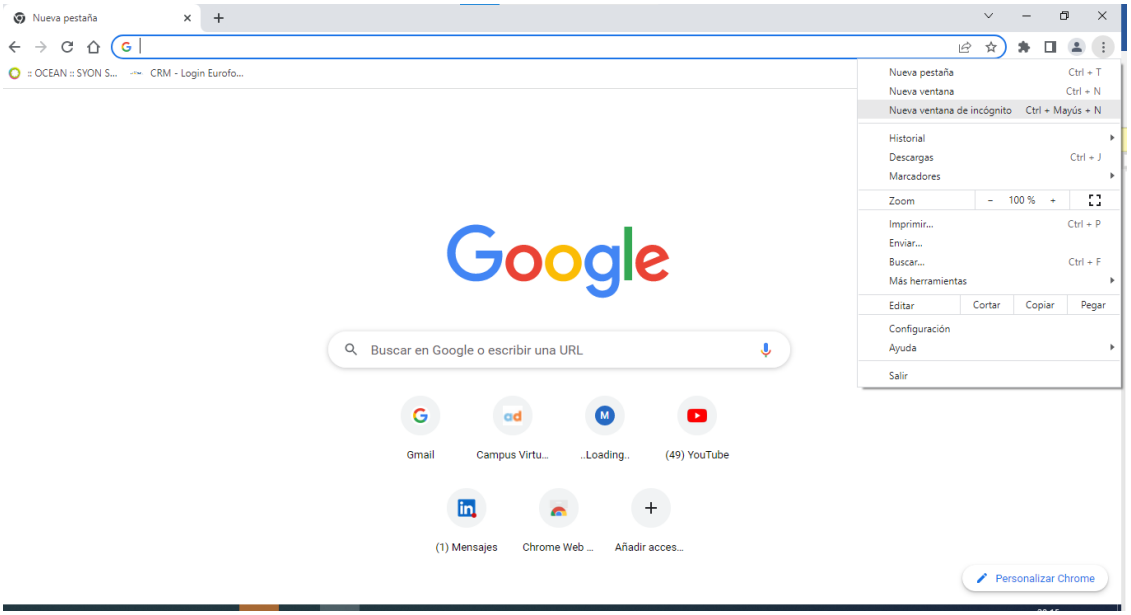
- **Contenido y diseño profesional:** Los sitios webs fiables suelen tener un contenido bien estructurado, organizado y sin ningún tipo de error. Por tanto, una página que presente un diseño "poco profesional" puede ser un indicio de un posible fraude.

- **Usar el modo incógnito:** El modo incógnito es una funcionalidad que ofrecen todos los navegadores con la finalidad de otorgar a los usuarios una navegación más privada. Cuando se navega en modo incógnito, no se guardan las *cookies*, ni los datos del sitio web, ni el historial. Una vez se cierre la ventana de modo incógnito, estos datos son borrados.

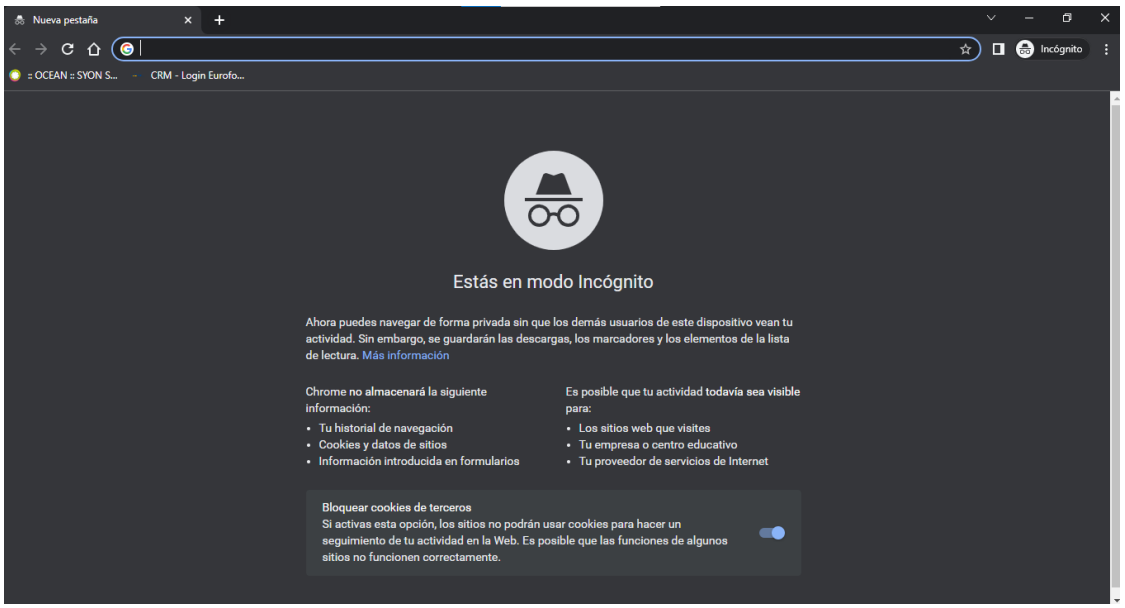
  Para acceder en modo incógnito, por ejemplo, en el navegador Chrome, se deben seguir estos pasos:

- **Desde un ordenador**

1. Abrir Chrome.
2. Pulsar en la parte superior derecha en el icono de los tres puntos" y después en "*Nueva ventana de incognito".*



3. En ese momento se abrirá una nueva ventana. Se puede comprobar que aparezca un icono de incógnito en la esquina superior de la ventana.



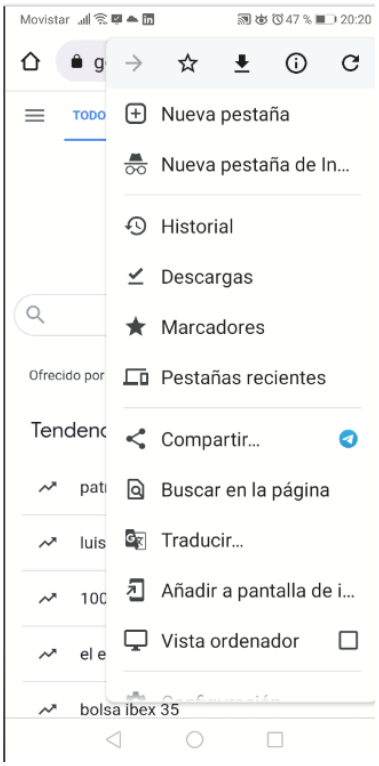
Otra forma más rápida de hacerlo es, teniendo abierto el navegador Chrome, presionar la siguiente combinación de teclas para abrir una ventana de incógnito. "Ctrl + Mayús + N."

- **Desde un dispositivo Android**

1. Abrir la aplicación Chrome.
2. En la parte derecha de la barra de direcciones, pulsar en los tres puntos y a continuación en la opción "Nueva pestaña de incógnito".
3. Una vez pulsado, se abrirá una ventana nueva. En ella aparecerá un mensaje indicando que "Estás en modo incógnito".

IMPORTANTE

Es importante ser conscientes de que navegar en modo incógnito no hace que la navegación sea completamente segura y/o privada. Los datos son simplemente borrados en el dispositivo, pero no en la red. Por este motivo, es importante continuar navegando por páginas web que comiencen por HTTPS para proteger la información transmitida. Además, el modo incógnito tampoco bloquea los anuncios o notificaciones que pueden dirigirnos a webs maliciosas.



2. Cookies

Cuando navegamos por Internet es importante conocer qué son las *cookies* y las implicaciones que tienen.

Una *cookie* es simplemente un pequeño fichero de datos que se almacena en el dispositivo al entrar en una página web. No importa el soporte que se esté utilizando (ordenador móvil o tableta) cuando accedemos a una página web, para poder ver su contenido, el sitio web suele solicitar consentimiento para almacenar este pequeño fichero llamado cookie. Si se acepta, esta solicitud es enviada al servidor de la empresa que gestiona el servicio web de forma automática.

La razón por la que una web avisa de que las *cookies* van a ser utilizadas es para cumplir con la normativa GDPR (Reglamento General de Protección de Datos, Reglamento 2016/679). Fue creado por el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea con la intención de reforzar y unificar la protección de datos para todos los individuos dentro de la Unión Europea.

➢ Utilidad de las *cookies*

Hay varios tipos de cookies y con distintas finalidades. Su principal objetivo es almacenar información sobre la forma de navegar de los usuarios y las acciones que hacen en la web: ver contenido multimedia, empezar una solicitud y abandonarla, acceder a los enlaces, ver anuncios, etc. También se utilizan para registrar datos de acceso al sitio: el nombre de usuario, identificar el ordenador desde el que se accede, última visita, hora, ubicación, etc. con el fin de poder personalizar la página acorde a los intereses de los internautas y mejorar la experiencia de usuario. Incluso, las *cookies* permiten crear perfiles según el gusto de los usuarios para que empresas de marketing *online* ofrezcan los productos de forma segmentada acorde a los intereses de los usuarios.

Adicionalmente, las *cookie*s permiten que los usuarios no tengan que introducir usuario y contraseña cada vez que accedan a un espacio web y permitir que sigan navegando en el punto que lo habían dejado. Por ejemplo, si seleccionas artículos y los dejas en la cesta o carro de una web, pero no finalizas la compra; al volver a

conectarte desde la misma IP te recupera aquellos artículos que ya habías pre-seleccionado en la cesta facilitándote este proceso.

Por tanto, podemos decir que las *cookies* no representan un problema. Simplemente, ayudan a recordar tus configuraciones y estados de la web o preferencias, como idioma, divisa, vuelos que recientemente hayas buscado, etc. Pero cuando son utilizadas para recoger hábitos de navegación (como si fueran cámaras de vigilancia) y, sobre todo, cuando pueden recoger datos personales poniendo en riesgo la privacidad de usuario, genera más preocupación tanto a los propios usuarios de la red cómo a los organismos que trabajan por proteger la privacidad de los ciudadanos, como es la AEPD (Agencia Española de Protección de Datos). Esta entidad se encarga de velar por el cumplimiento de la normativa sobre protección de datos. Su objetivo principal es promover y garantizar el cumplimiento de la normativa de protección de datos, así como informar a cualquier ciudadano sobre sus derechos y obligaciones en relación a la protección y privacidad de sus datos. Entre otras funciones, tiene la de garantizar y tutelar el derecho fundamental a la protección de datos de carácter personal de los ciudadanos.

En el siguiente enlace podrás ver todas las áreas de actuación de la AEPD:

Ver enlace

Las *cookies* no necesariamente se dedican a tratar datos personales. Podemos afirmar que existe tratamiento de datos personales en los siguientes supuestos:

- Cuando el usuario de un servicio en concreto ya esté identificado en su plataforma (bien sea con el nombre o email).
- O en el caso de que se utilicen identificadores únicos.

Veamos los diferentes tipos de cookies que nos podemos encontrar:

1. Según el consentimiento

Se refiere a si el usuario procede a dar su consentimiento. Estas se clasifican en dos tipos, con o sin consentimiento previo. Veamos que son cada una de ellas:

- *Cookies* **sin consentimiento previo**

Son aquellas que no necesitan que el usuario dé el consentimiento previo para que puedan usarse. En general suelen denominarse *cookies* técnicas y *cookies* de personalización. Estas *cookies* se consideran imprescindibles para que el sitio web funcione de manera correcta y por tanto no sería necesario el consentimiento del usuario. Algunas de estas *cookies* técnicas sirven para gestionar el pago, realizar el proceso de compra de un pedido, etc.

- *Cookies* **con consentimiento previo**

Como su nombre indica, necesitan del permiso de los usuarios para establecerse. Es necesario que aparezca un aviso en la web y que el usuario pueda aceptarlas o rechazarlas. Algunas de ellas son las *cookies* de seguimiento o las de tipo publicitarias.

2. Según la entidad que las gestiona

En función de la entidad que gestione las *cookies*, es decir, el dominio o servidor a donde son enviadas las *cookies* y trate los datos que recaban, distinguimos entre:

- *Cookies* **propias o de origen**

Las *cookies* propias o *cookies* de origen, son creadas y gestionadas por el propio propietario de la página web. Son las que utiliza el sitio web para fines estadísticos, como el número de páginas vistas, las sesiones, o el número de usuarios.

- *Cookies* de **terceros**

Se trata de las *cookies* que se establecen sin que la web sea visitada por el usuario. Por ejemplo, ocurre cuando se integran elementos como anuncios, o complementos sociales entre otros.

Estas *cookies* también rastrean a los usuarios y les permiten guardan su información para, por ejemplo, configurar publicidad personalizada.

3. Según el tiempo que permanezcan activas

Otra clasificación es según el tiempo que se encuentran activas en nuestro navegador web. Son las *cookies* de sesión y las *cookies* persistentes.

- *Cookies* de **sesión**

Tienen un periodo de tiempo limitado ya que caducan inmediatamente después de abandonar nuestro navegador web, son cookies temporales. Se utilizan mucho en los sitios web de comercio electrónico, ya que permiten por ejemplo recordar el producto que hemos introducido en el carrito de compra.

No tienen consecuencias en la privacidad del usuario a largo plazo.

- *Cookies* **persistentes**

Estas cookies permanecen en el navegador del usuario durante más tiempo, pueden estar configuradas para expirar después de 30 días, o pueden llegar incluso a persistir varios años. Los sitios web lo utilizan para rastrear a un usuario y su interacción con ese sitio web.

4. Según su finalidad

En esta última clasificación, veremos los siguientes tipos de *cookies*:

- *Cookies* de **personalización**

Sirven para almacenar nuestras preferencias de experiencia del usuario en un sitio web. Un ejemplo lo encontramos al elegir un idioma para ver un sitio web.

- *Cookies* de **análisis**

Se utilizan para realizar un análisis de la interacción de un usuario sobre un sitio web, a efectos estadísticos, no para personalizar o segmentar anuncios.

- *Cookies* **publicitarias**

Estas *cookies* tienen como finalidad reunir información sobre nosotros en nuestro dispositivo, para enviarnos publicidad basada en los temas que nos interesan. Esta información puede compartirse con otras empresas anunciantes como una manera de mejorar el rendimiento de los anuncios. Otra de sus funciones es reunir información para análisis estadísticos sobre el rendimiento de los anuncios.

- *Cookies* de **publicidad comportamental**

Este es una ampliación de la cookie anterior donde, según el comportamiento del usuario en Internet, nos muestran anuncios o contenido que nos pueda resultar relevante.

- *Cookies* de **complementos**

Son aquellas que son generadas cuando un sitio web utiliza estos complementos, como puede ser la localización de una tienda en Google Maps, o los *links* a redes sociales.

- *Cookies* de **reproductor multimedia**

Son aquellas que nos permiten la reproducción de contenido en forma de audio o video.

Una misma *cookie* puede estar incluida en más de una categoría de las mencionadas anteriormente. Y también existen las ***cookies* polivalentes**, que son aquellas que incorporan más de una funcionalidad y persiguen más de una finalidad.

Como ya hemos indicado anteriormente, el uso de las *cookies* está regulado por el Reglamento Europeo de Protección de Datos (RGPD) y, por norma general, es necesario el consentimiento expreso del usuario para poder utilizarlas por una empresa o servicio web. Las *cookies* que están exentas del consentimiento por parte del usuario, aunque sigue siendo recomendable informar, aunque sea de forma genérica, son las siguientes:

- *cookies* de entrada del usuario
- *cookies* de autenticación o identificación del usuario (de sesión)
- *cookies* de reproductor multimedia
- *cookies* de sesión para equilibrado de la carga en el servidor web
- *cookies* de personalización de la interfaz
- *cookies* tipo *plug-in* para intercambio de contenidos sociales
- *cookies* de carga equilibrada
- cookies de carritos de compras

Además, los sitios web están obligados a recabar el consentimiento por parte del usuario a través de algún tipo de declaración en la cual se dé ese consentimiento de una manera afirmativa. Algunas *cookies* se denominan "*cookies* exentas", (ya mencionadas anteriormente cuando hablamos de "cookies sin consentimiento previo"). En estas no se aplica ninguna ley, es decir, en estos casos no es necesario informar ni tampoco obtener el consentimiento. Estas *cookies* suelen ser las necesarias para poder prestar el servicio solicitado en el sitio web al usuario.

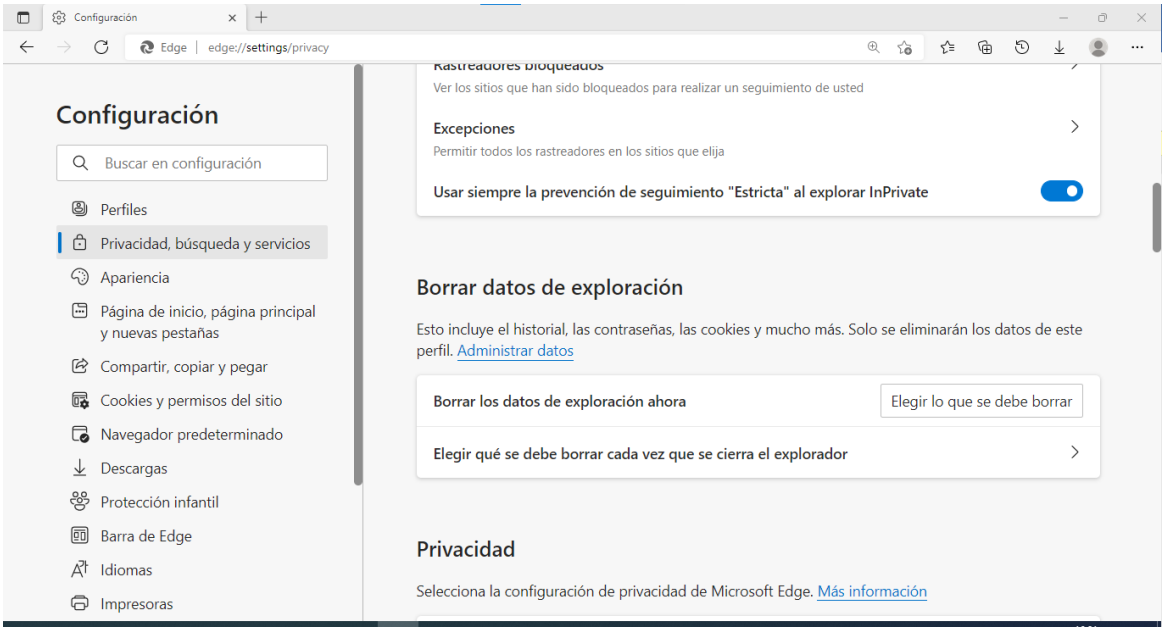
A continuación, se detalla **cómo borrar las *cookies* que han sido almacenadas en el navegador.**

Microsoft Edge

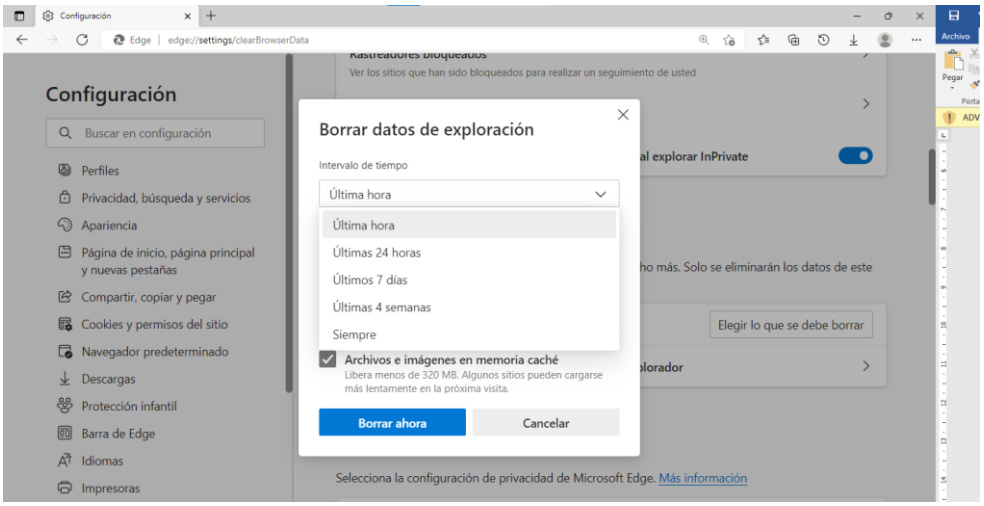
Para borrar nuestros datos de navegación en Microsoft Edge:

1. Pulsamos en el icono de los tres puntos seguidos situado en la esquina superior derecha. Aparecerá un menú y elegiremos la opción de 'Configuración'.

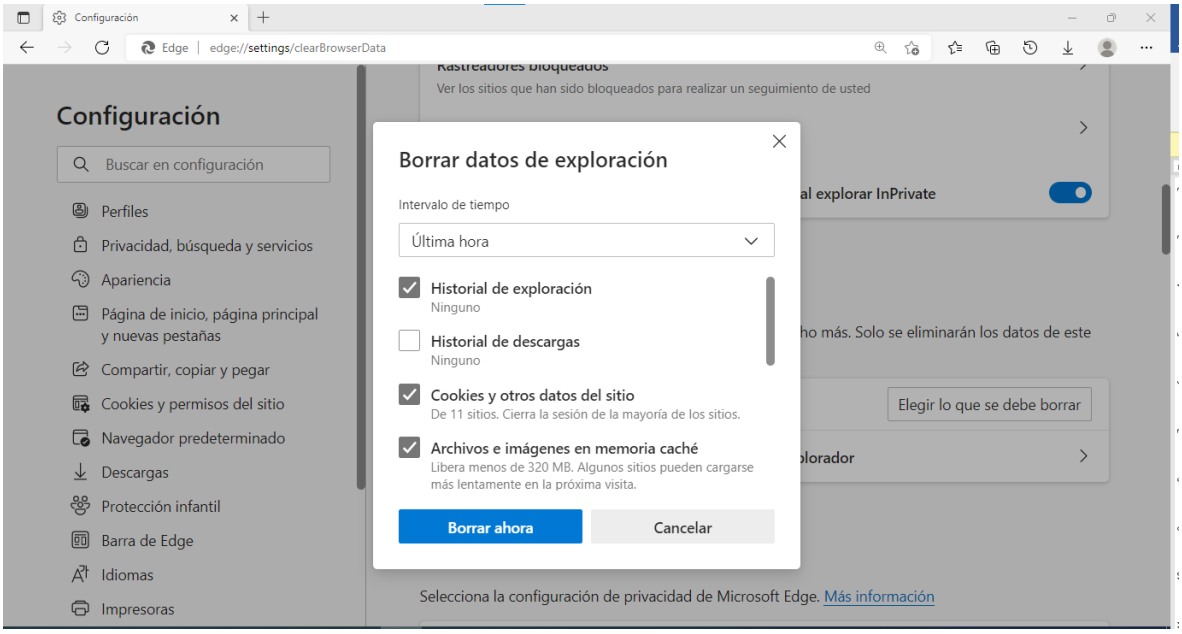
2. A continuación, a la izquierda de la pantalla nos mostrará un menú. Seleccionaremos 'Privacidad, búsqueda y servicios' y en esta nueva pantalla nos desplazaremos hasta encontrar la opción 'Borrar datos de exploración ahora'. Aquí, seleccionaremos la opción de 'Elegir lo que se debe borrar'.



3. Puedes elegir el intervalo de tiempo desde cuándo quieres borrar la información almacenada (última hora, 24 horas, 7 días, siempre) pulsando en el menú desplegable 'Intervalo de tiempo'.



4. También se pueden elegir los tipos de datos de exploración que quieres borrar. Por ejemplo, puedes eliminar las *cookies*, y mantener el historial de descarga. Al finalizar, pulsa en 'Borrar ahora'.

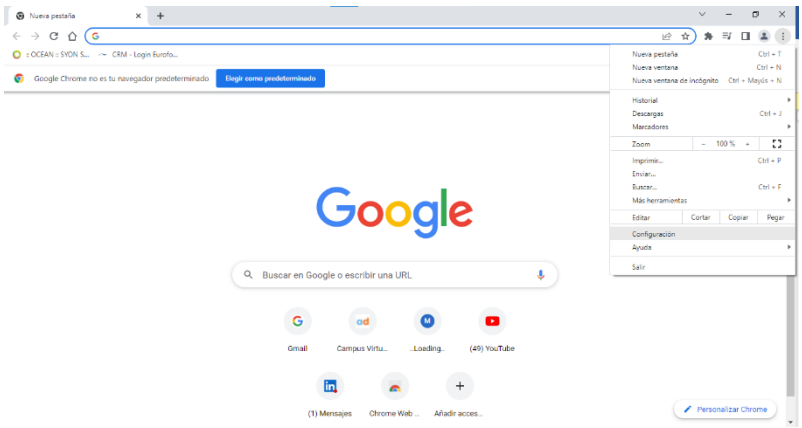


Chrome

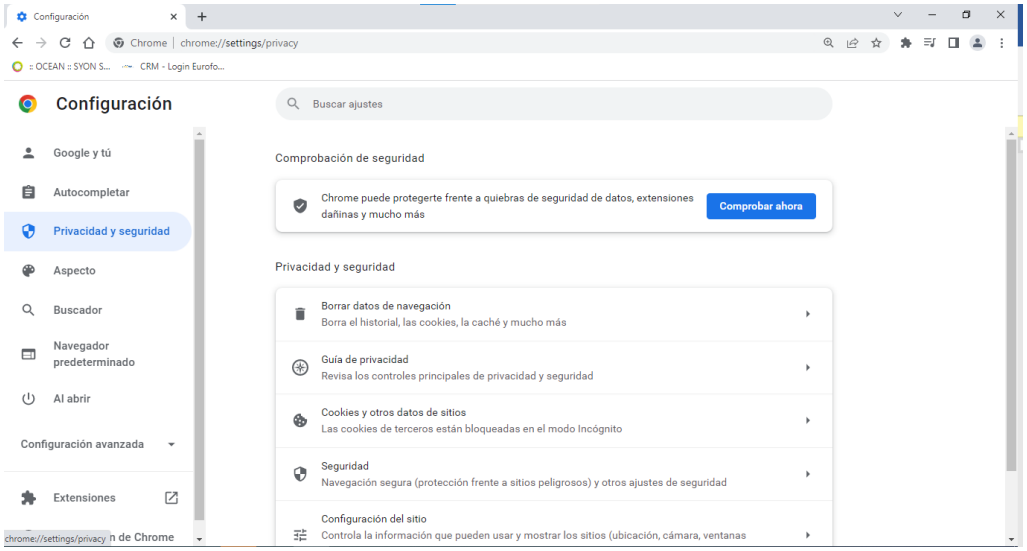
1. Abre el navegador Chrome en tu ordenador o dispositivo móvil.

2. Arriba a la derecha, haz clic en el icono de los tres puntos que despliega las opciones disponibles de configuración.

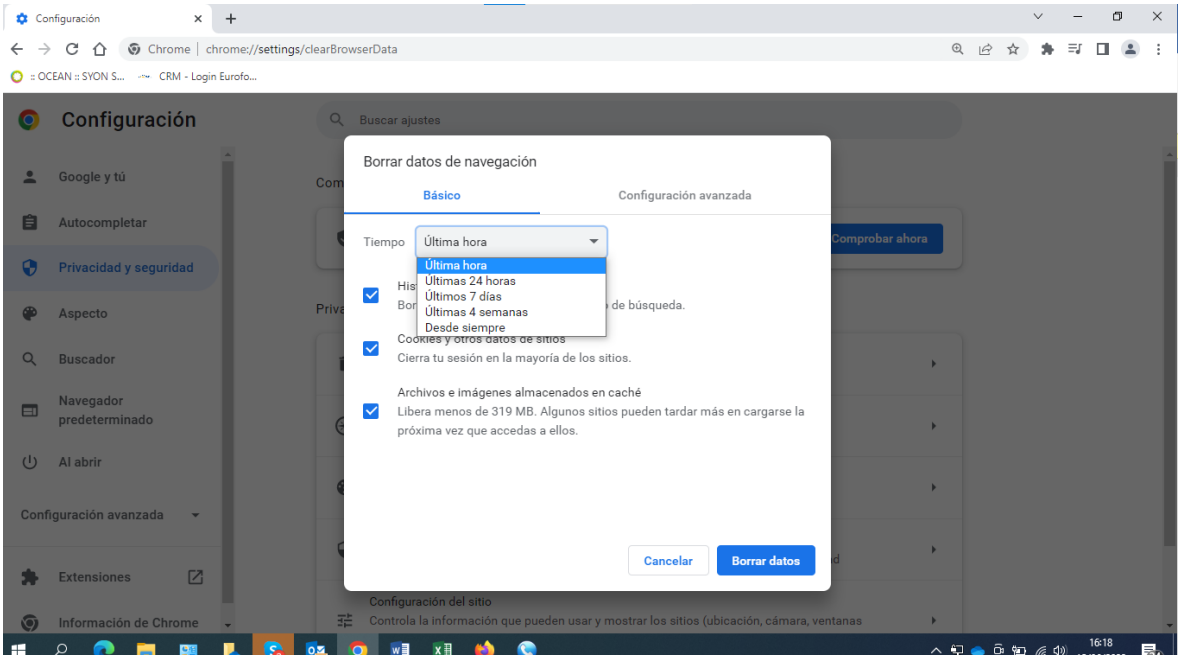
3. Pulsa en la opción 'Configuración'. En la nueva ventana, te aparecerá a la izquierda de la pantalla un menú. Deberás seleccionar la opción 'Privacidad



y seguridad'. A continuación, dirígete al apartado de 'Borrar datos de navegación'.

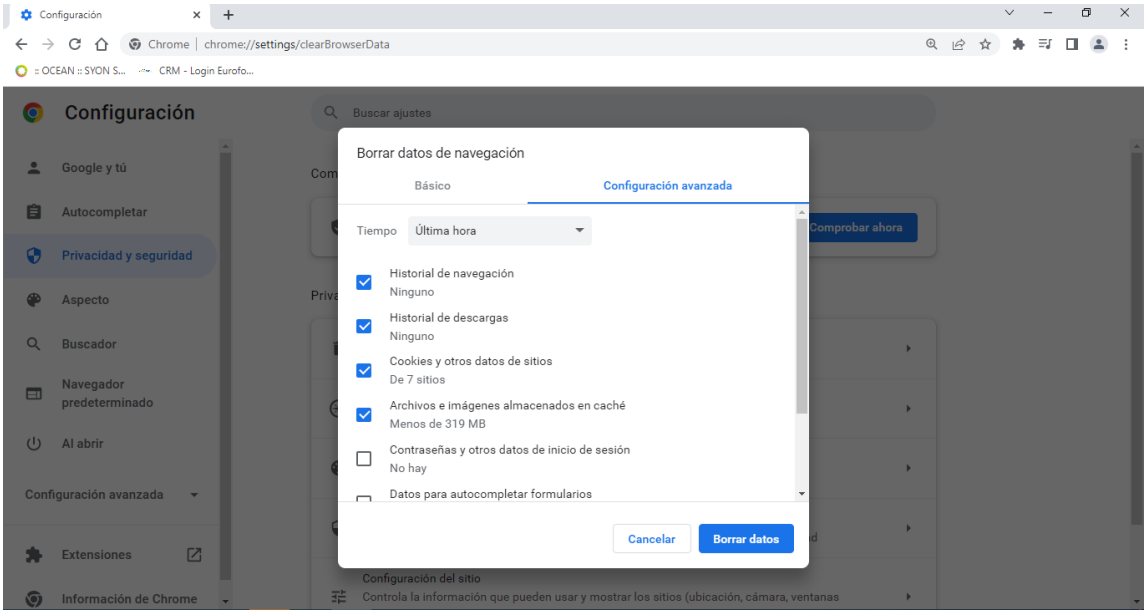


4. Ahora podrás elegir qué quieres borrar: historial de navegación, *cookies*, etc. Marca las casillas de los tipos de datos que quieras que elimine Chrome, incluida la casilla del historial de navegación. Tienes dos opciones:



Básico: permite borrar el historial de navegación, *cookies* y otros datos de sitios, archivos e imágenes almacenadas en caché.

Configuración avanzada: permite eliminar, además de lo especificado en la opción 'Básico', el historial de descargas, contraseñas, datos para autocompletar formularios, configuración del sitio y datos de aplicaciones alojadas.



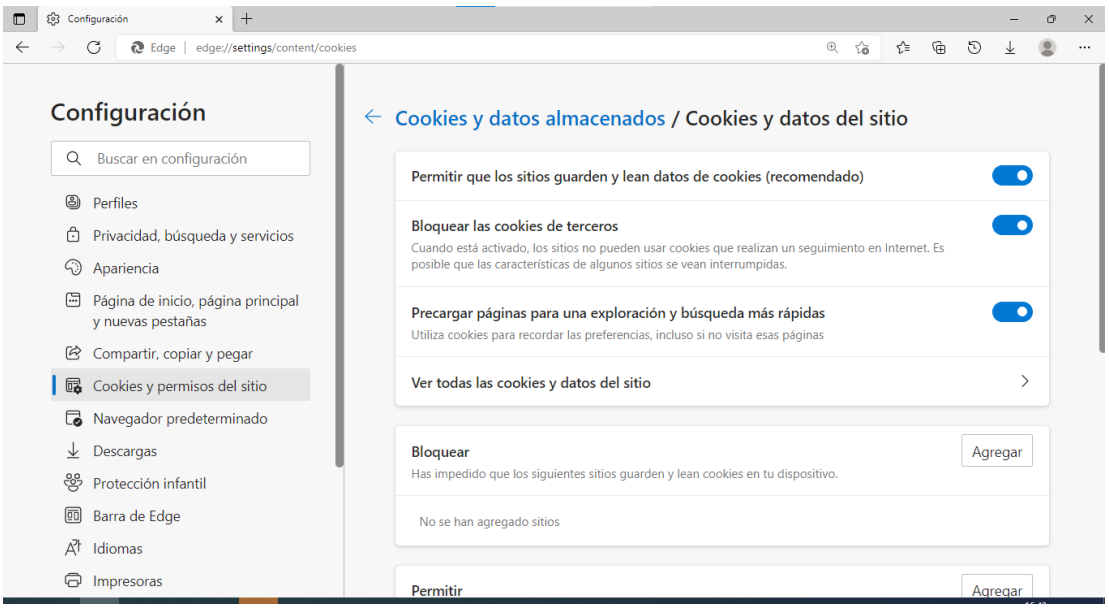
5. Al igual que en el navegador Edge, en Chrome también puedes elegir desde cuándo quieres que se elimine la información (última hora, últimas 24 horas, últimos 7 días, últimas 24 horas, Desde siempre). Para ello, pulsa en el menú desplegable 'Intervalo de tiempo'.

A continuación, se detalla cómo puedes **desactivar la función que permite a las webs almacenar las *cookies*:**

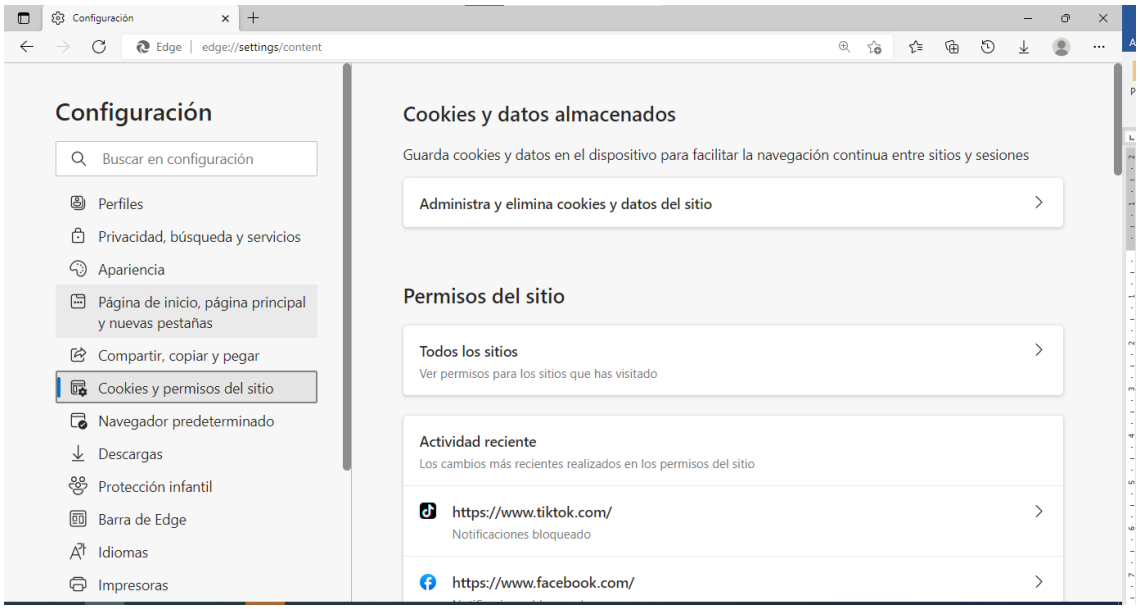
Microsoft Edge

1. Selecciona en la parte superior derecha el icono de los tres puntos. Del menú que se despliega, pulsa en 'Configuración'.

2. A la izquierda de la pantalla, aparecerá un menú. Selecciona la opción '*Cookies* y permisos del sitio' y después en 'Administra y elimina *cookies* y datos del sitio'.

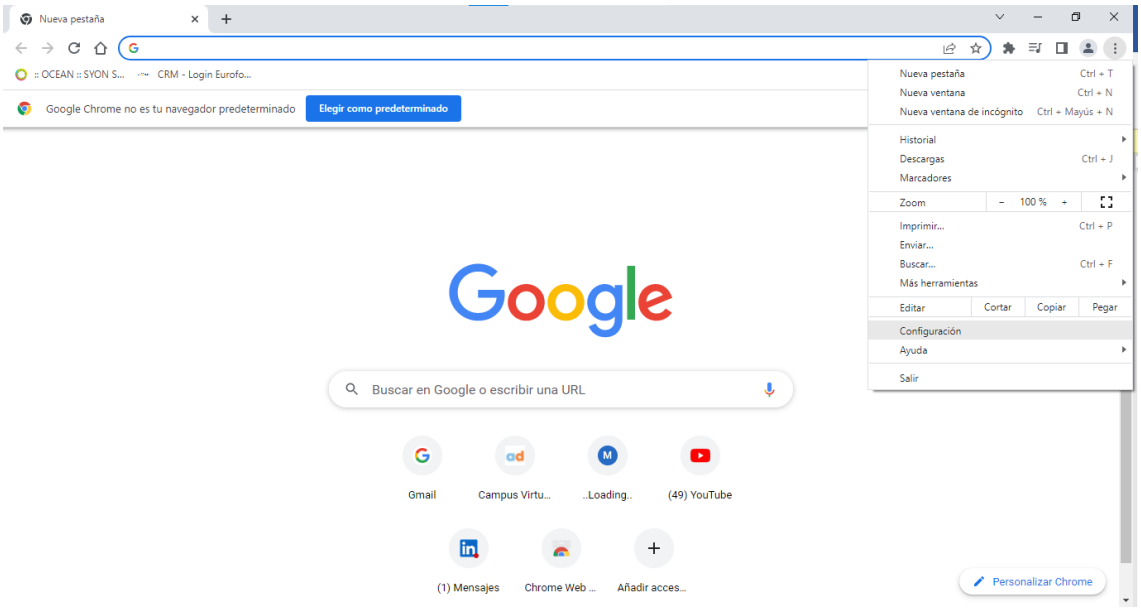


3. Al pulsar en '*Cookies* y datos de sitios' aparecerá la siguiente ventana en la que hay que activar la opción 'Bloquear *cookies* de terceros'.

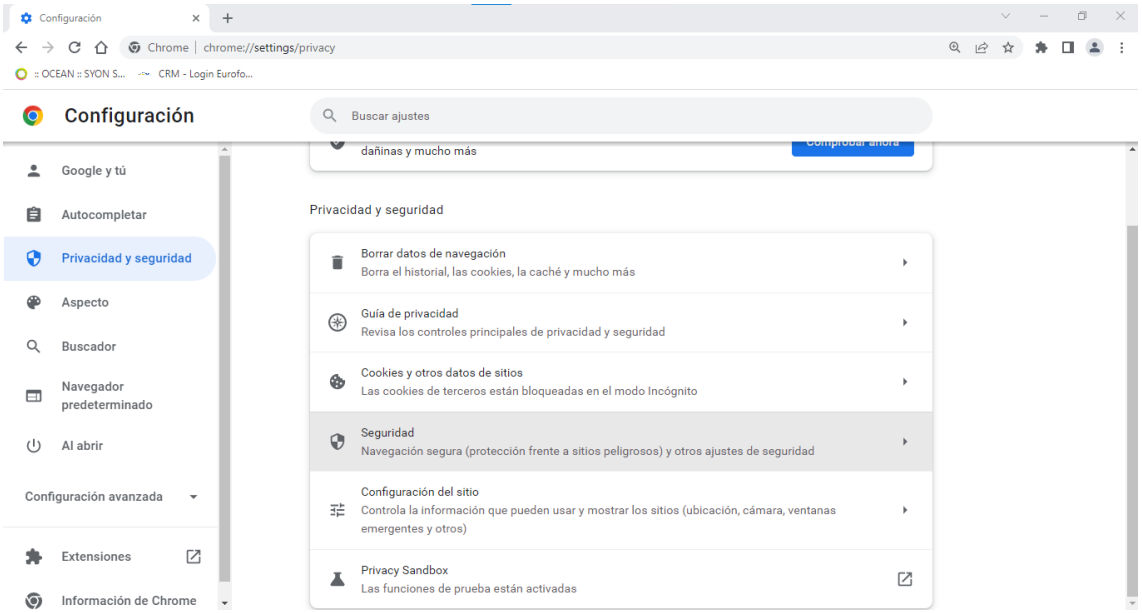


Chrome

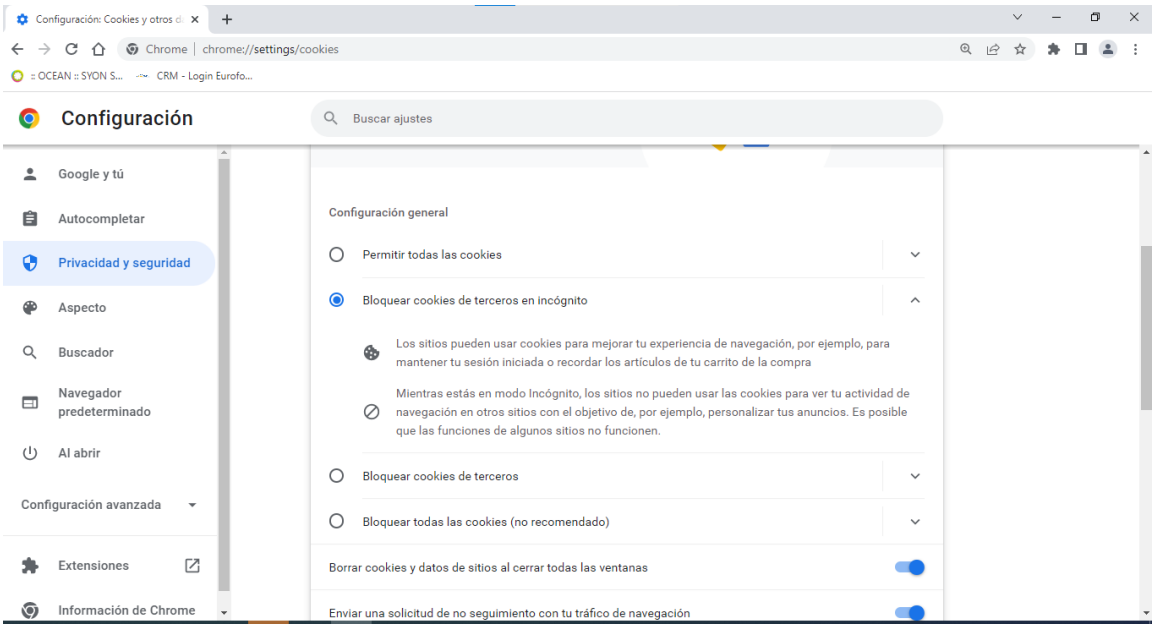
1. Selecciona en la parte superior derecha el icono de los tres puntos. Selecciona del menú la opción 'Configuración'.



2. En el nuevo menú que aparece la parte izquierda, pulsa la opción 'Privacidad y seguridad' y a continuación selecciona '*Cookies* y otros datos de sitios'.



3. Finalmente, activa la opción 'Bloquear cookies de tercero en incognito' o 'Bloquear *cookies* de terceros'.



Para profundizar un poco más en este concepto, en el siguiente vídeo, un experto explicará con detalle qué son las *cookies* y sus implicaciones.

3. Configuración de Chrome

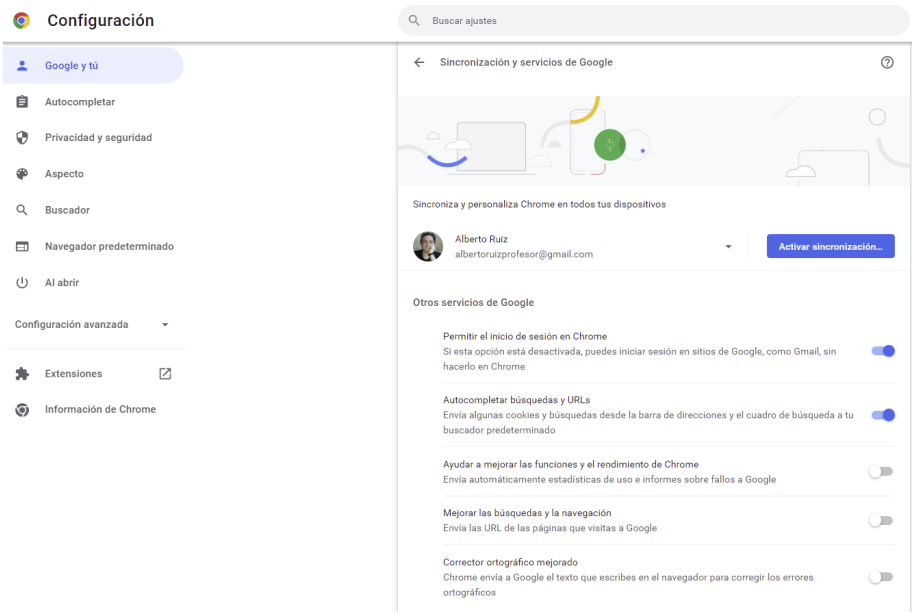
Chrome es un navegador web gratuito desarrollado por Google y una de las plataformas más utilizadas en todo el mundo para la búsqueda de información en la red. Por tanto, debido a que su uso está muy extendido entre los usuarios, explicaremos la manera más adecuada de configurarlo para mejorar la privacidad y seguridad cuando naveguemos con él.

Google Chrome comenzó a funcionar por primera vez el 2 de septiembre de 2008, se convirtió en uno de los navegadores webs más usados a nivel mundial por sus características peculiares y sobre todo su rapidez. Es el navegador más usado en España, registrando un porcentaje del 71,1% de usuarios, y a nivel global, alcanza el porcentaje del 63,3% de usuarios, según datos actualizados del año 2023.

Una premisa importante, además de tener el buscador configurado de la manera más segura posible, es mantenerlo siempre actualizado a la última versión. Por ello, se detalla cómo se puede llegar a conseguir esta última actualización:

Para acceder a esta opción, debemos ir al menú que se encuentra en la parte superior derecha representado por tres puntos y a continuación seleccionar la opción de 'Configuración'. Otra opción es escribir en la barra de direcciones que se sitúa en la parte superior del navegador: *chrome://settings*

Si queremos saber si tenemos nuestro navegador Chrome actualizado, dentro del menú que hemos mencionado en el párrafo anterior, en la opción información de Chrome, podremos ver si nuestro navegador está actualizado, como vemos en la imagen siguiente:



Si existe una actualización disponible, aparecerá un mensaje que indica "Google Chrome se está actualizando automáticamente..." y un botón para reiniciar el navegador y aplicar la actualización.

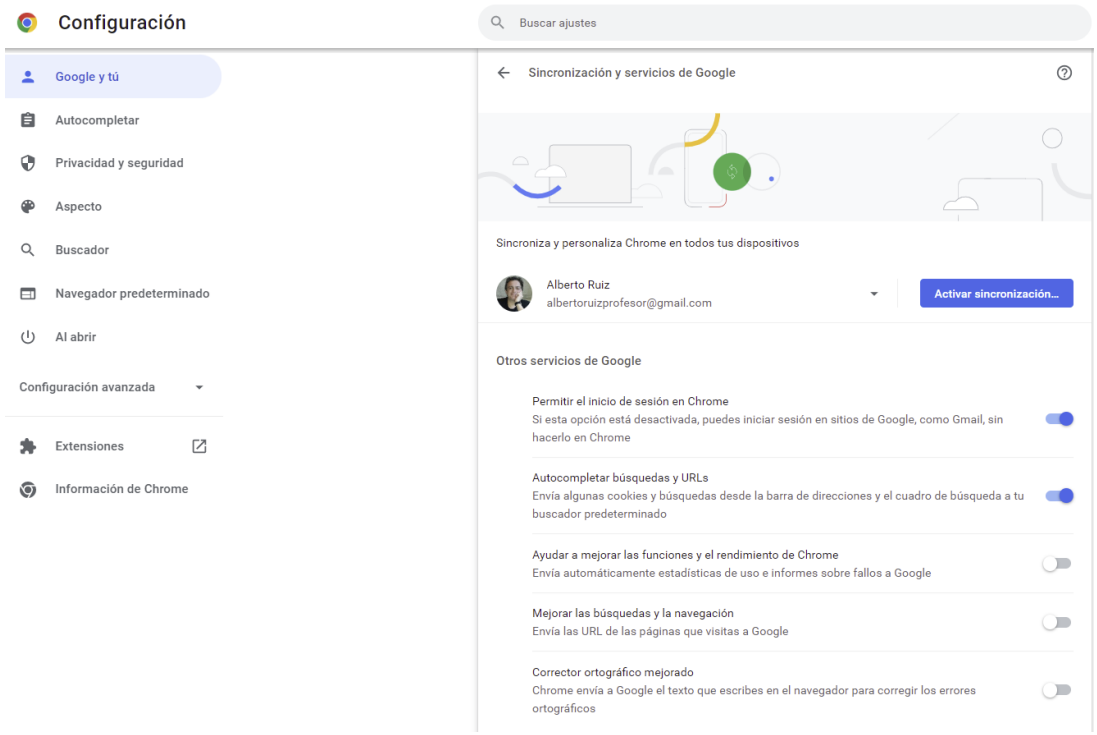
En el caso de que tengamos que actualizarlo, nos aparecería un botón denominado "Actualizar" y solo tendríamos que pulsarlo, en la imagen anterior, nos indica que Chrome está actualizado.

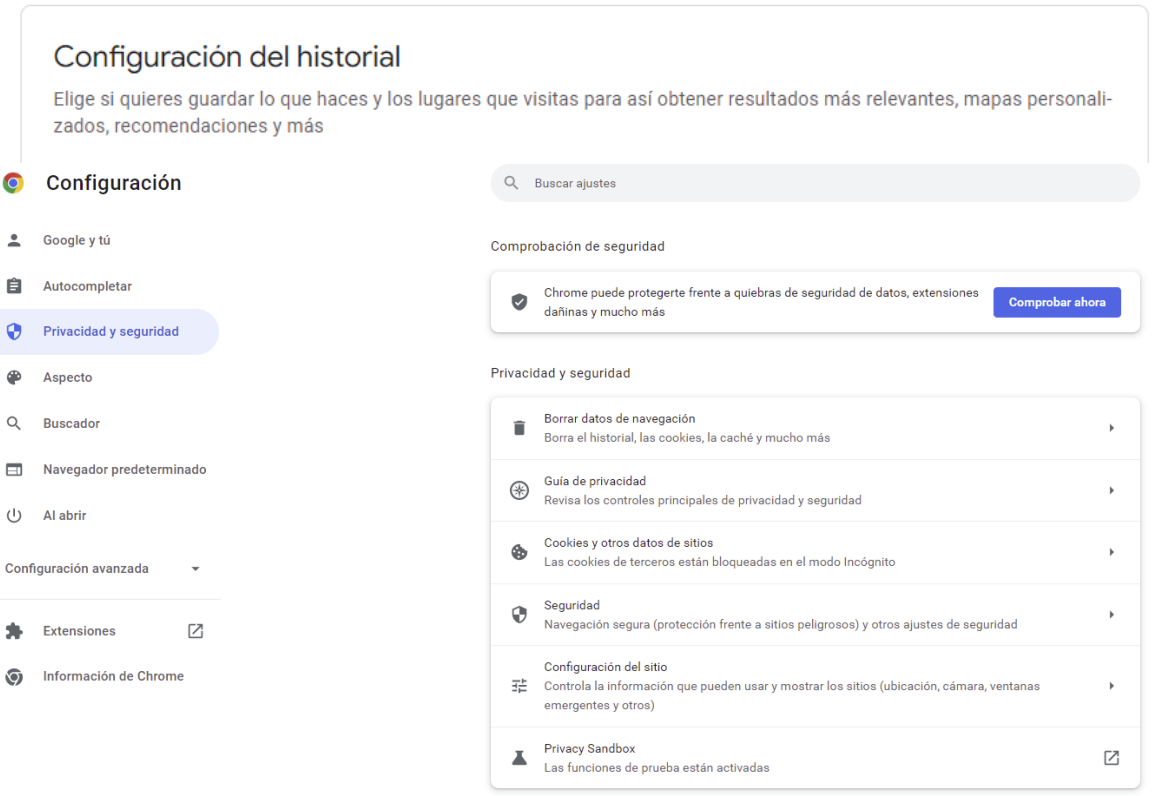
A continuación, la opción en la que vamos a pulsar es 'Sincronización y servicios de Google'. La sincronización de Google almacena de forma automática y para todos los dispositivos electrónicos que usemos con nuestra cuenta de Google, los marcadores, historial y contraseñas.

Por ejemplo, si agregamos el sitio web Ver enlace en marcadores a través de nuestro móvil, podremos ver ese marcador en un ordenador o en una Tablet.

Tal y como podemos apreciar en la imagen, dentro de esta opción tenemos varias configuraciones:

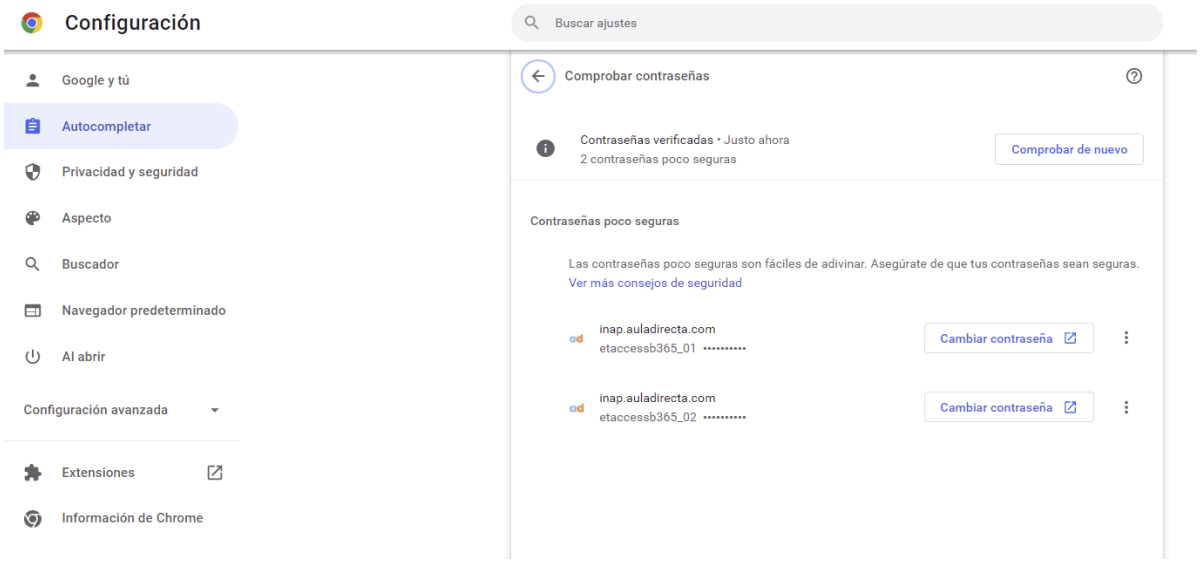
- **Permitir el inicio de sesión en Chrome.** Aunque cierres tu sesión de Google en Chrome, por defecto el navegador volverá a iniciarla cuando accedas a tu cuenta en cualquier servicio de la empresa, como Gmail. Para evitarlo, desactiva esta opción. Para que este cambio se aplique, es necesario reiniciar el ordenador. Además, cuando accedas a un servicio como Gmail, no tendrás que iniciar sesión en Google Chrome.
- **Revisión de la seguridad de tu cuenta de Google**. En este mismo apartado del menú 'Google y tú', si hemos iniciado sesión en Google Chrome, podemos modificar algunas configuraciones de privacidad y seguridad de la cuenta de Google. Para ello, hay que pulsar en 'Gestionar tu cuenta de Google' y a continuación en 'Privacidad y personalización'. Entre las opciones configurables encontramos 'Actividad en la web y en aplicaciones' e 'Historial de ubicaciones'. En ambos casos, y como vemos en la imagen inferior, recomendamos optar por la opción de 'Detenido' si queremos proteger mejor nuestra privacidad, además de ser útil a la hora de interrumpir rápidamente una acción en el navegador.

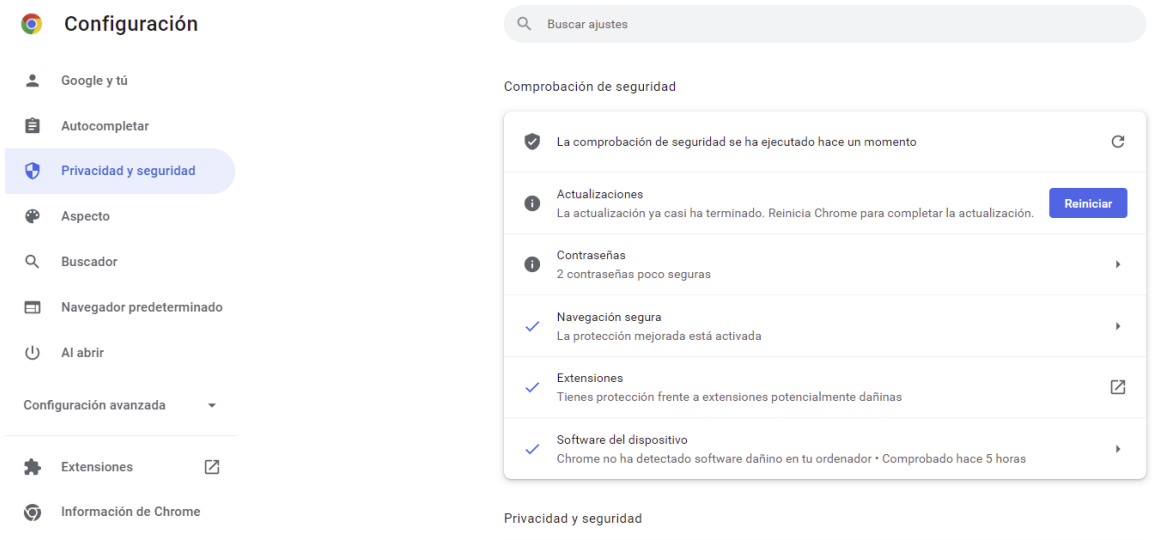

Configuración
Buscar ajustes
Google y tú
Autocompletar
Privacidad y seguridad
Aspecto
Buscador
Navegador predeterminado
Al abrir
Configuración avanzada
Extensiones
Información de Chrome
Sincronización y servicios de Google
Sincroniza y personaliza Chrome en todos tus dispositivos
Alberto Ruiz
albertoruizprofesor@gmail.com
Activar sincronización...
Otros servicios de Google
Permitir el inicio de sesión en Chrome
Si esta opción está desactivada, puedes iniciar sesión en sitios de Google, como Gmail, sin hacerlo en Chrome
Autocompletar búsquedas y URLs
Envía algunas cookies y búsquedas desde la barra de direcciones y el cuadro de búsqueda a tu buscador predeterminado
Ayudar a mejorar las funciones y el rendimiento de Chrome
Envía automáticamente estadísticas de uso e informes sobre fallos a Google
Mejorar las búsquedas y la navegación
Envía las URL de las páginas que visitas a Google
Corrector ortográfico mejorado
Chrome envía a Google el texto que escribes en el navegador para corregir los errores ortográficos


Configuración del historial
Elige si quieres guardar lo que haces y los lugares que visitas para así obtener resultados más relevantes, mapas personalizados, recomendaciones y más
Configuración
Buscar ajustes
Google y tú
Autocompletar
Privacidad y seguridad
Aspecto
Buscador
Navegador predeterminado
Al abrir
Configuración avanzada
Extensiones
Información de Chrome
Comprobación de seguridad
Chrome puede protegerte frente a quiebras de seguridad de datos, extensiones dañinas y mucho más
Comprobar ahora
Privacidad y seguridad
Borrar datos de navegación
Borra el historial, las cookies, la caché y mucho más
Guía de privacidad
Revisa los controles principales de privacidad y seguridad
Cookies y otros datos de sitios
Las cookies de terceros están bloqueadas en el modo Incógnito
Seguridad
Navegación segura (protección frente a sitios peligrosos) y otros ajustes de seguridad
Configuración del sitio
Controla la información que pueden usar y mostrar los sitios (ubicación, cámara, ventanas emergentes y otros)
Privacy Sandbox
Las funciones de prueba están activadas

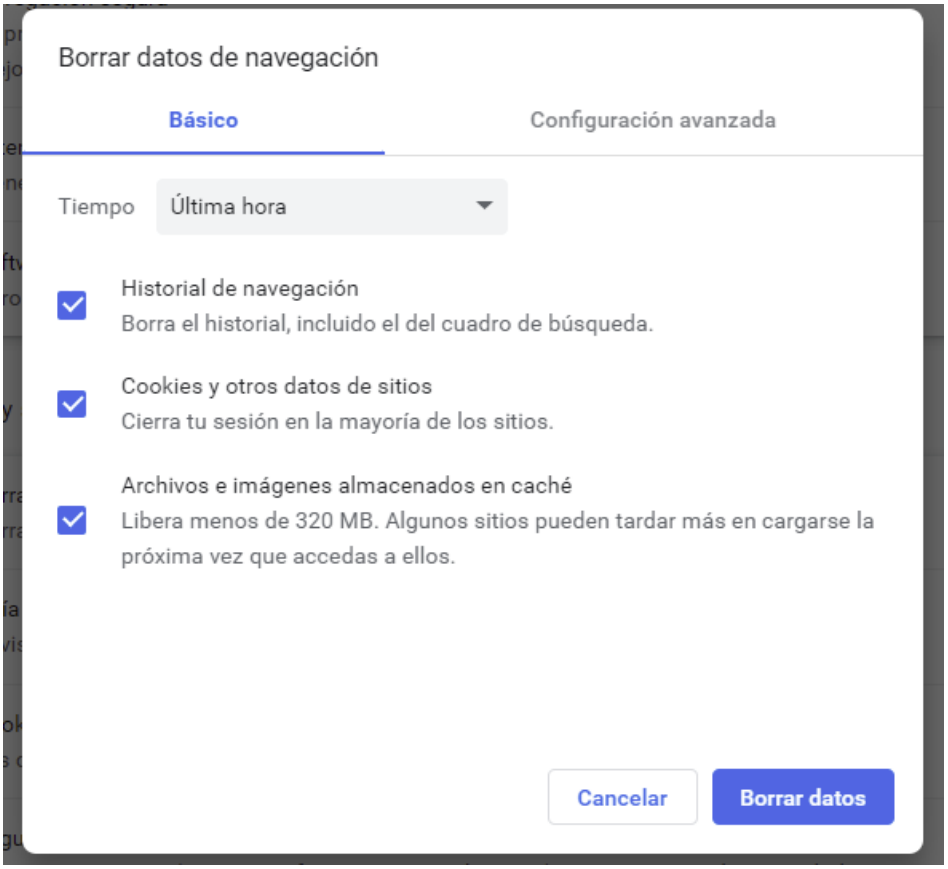
Si volvemos al menú de configuración inicial, en la zona de la izquierda accederemos a la opción de 'Privacidad y seguridad', donde se plantean varias opciones:

- **Comprobaciones de seguridad**. Esta opción nos facilitará un resumen del estado general de seguridad del navegador: si está actualizado o no, si hay contraseñas guardadas, si la protección estándar está activada, etc. Muy interesante para tomar las medidas de seguridad que correspondan. Por ejemplo, si hubiese alguna contraseña almacenada poco segura, podríamos seguir los pasos indicados para eliminarla o incluso cambiar por otra más robusta.

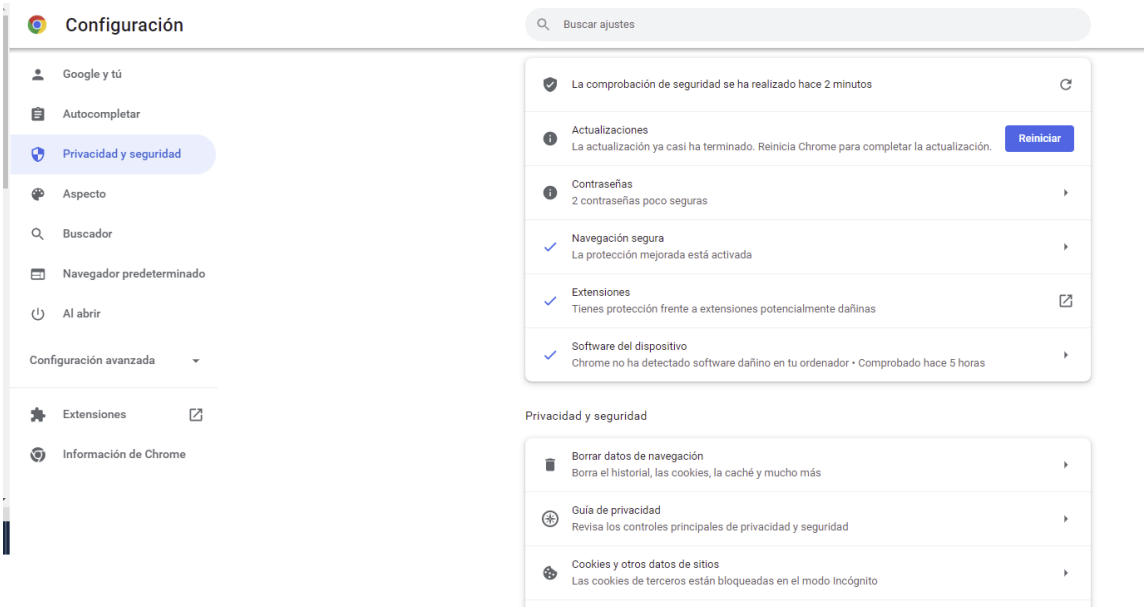


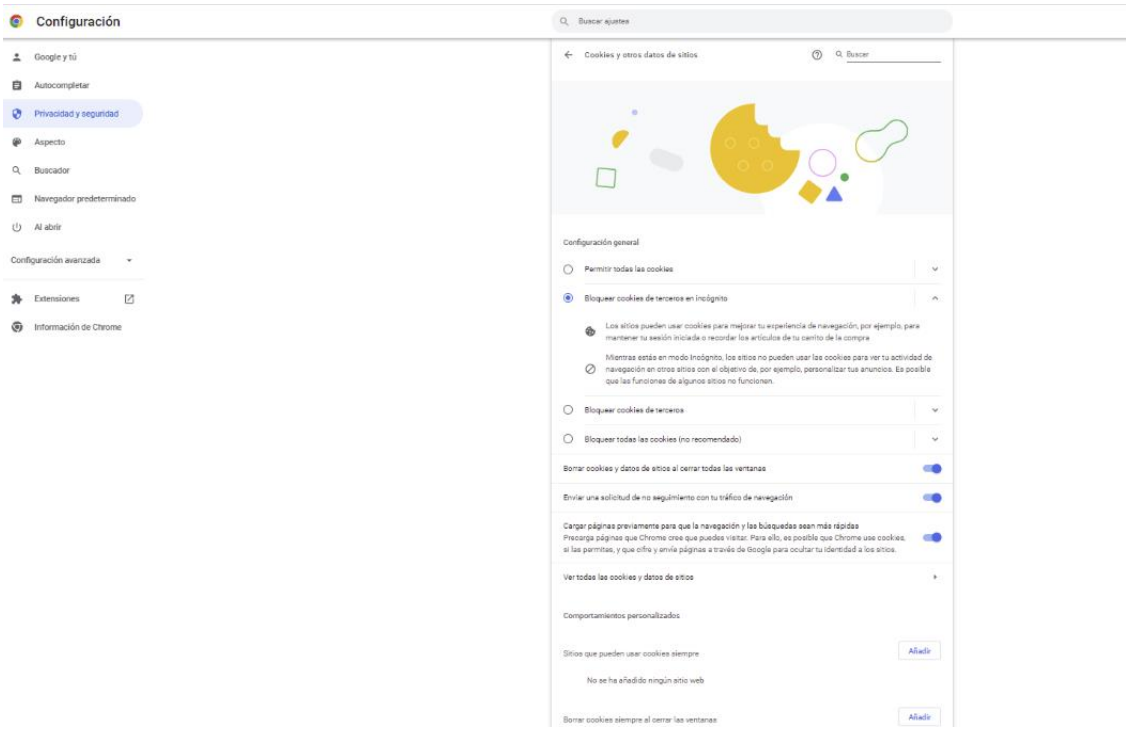


- **Borrar datos de navegación.** Dentro de este mismo menú de 'Privacidad y seguridad', encontramos la opción 'Borrar datos de navegación'. Si accedemos a ella se nos abrirá una ventana donde podremos eliminar historial, *cookies*, caché, etc. También podemos escoger el tiempo desde cuándo queremos que se borre toda la información: última hora, las últimas 24 horas, los últimos 7 días, las últimas 4 semanas o la que recomendamos que es 'desde siempre'. También se pueden seleccionar que tipos de datos se quieren eliminar haciendo clic en las casillas correspondientes. Recuerda que tenemos por un lado el nivel 'Básico', donde podemos eliminar lo que hemos comentado anteriormente, o la 'Configuración avanzada', donde podemos eliminar además de lo indicado para el nivel 'Básico', más información privada: contraseñas guardadas, datos para autocompletar formularios, configuraciones del sitio y datos de aplicaciones alojadas. Una vez seleccionadas las opciones preferentes, se debe de hacer clic en el botón "borrar datos".

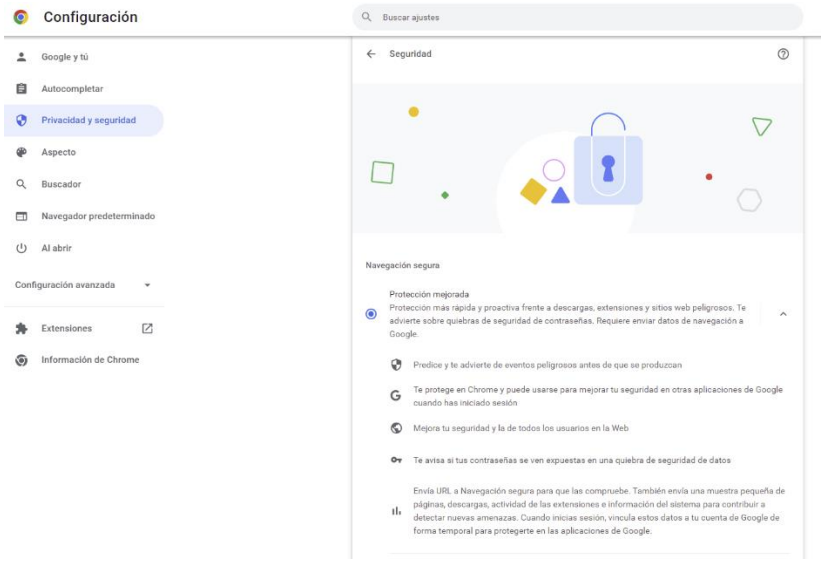


- ***Cookies* y otros datos de sitios.** En esta opción, también muy interesante, podrás escoger la configuración de las *cookies*. Al acceder nos encontraremos una serie de opciones. Recomendamos activar las siguientes:
  - '**Bloquear *cookies* de terceros en incógnito**', esto va a permitir al usuario que por ejemplo vea menor publicidad al navegar en un sitio web.
  - '**Borrar *cookies* y datos de sitios al cerrar todas las ventanas**', de esta manera no se almacenará ninguna *cookie* ni otros datos, ya que al cerrar las ventanas se borrará cualquier rastro o información que se haya almacenado en nuestro dispositivo.
  - '**Enviar una solicitud de no seguimiento con tu tráfico de navegación',** esto nos va a permitir controlar que los sitios web que visitemos no realicen ningún seguimiento de nuestra navegación en ese sitio.

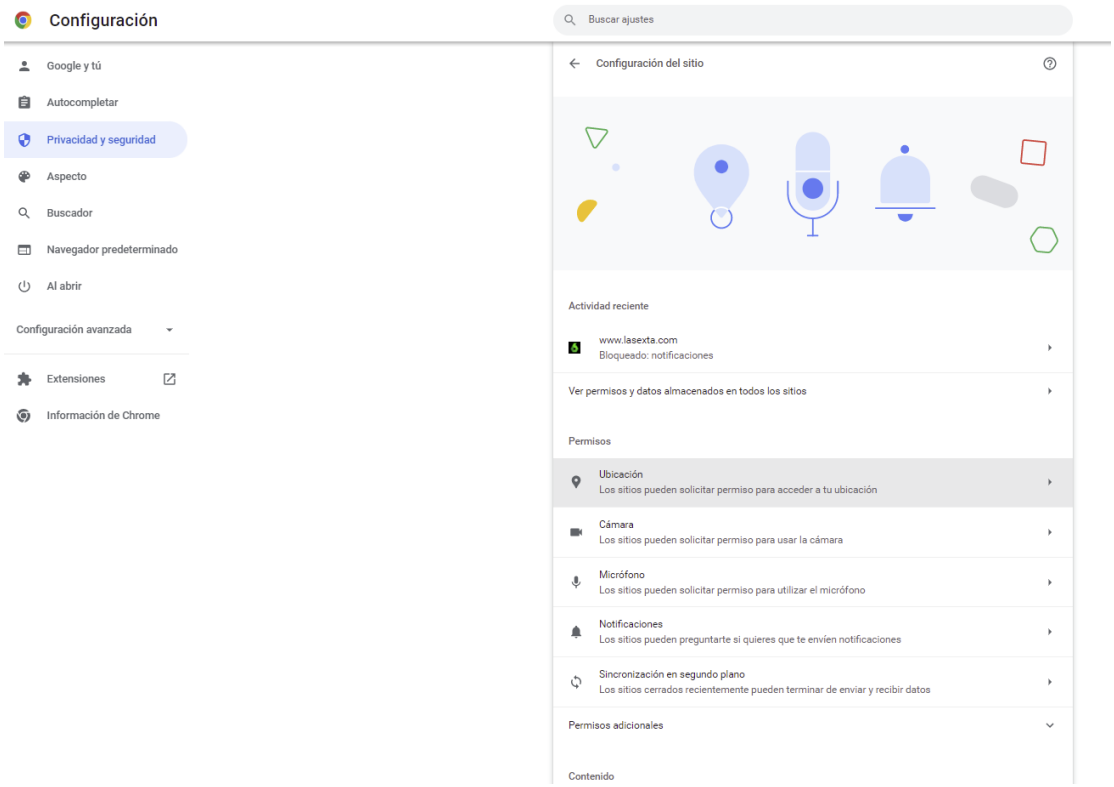




- **Seguridad.** Al entrar en esta opción del navegador, se nos ofrecen distintos tipos de protección. Activando la opción de 'Protección mejorada' el propio navegador nos advertirá si las contraseñas están expuestas, si un archivo a descargar es malicioso o si la web a la que estamos intentando acceder es un sitio peligro. No solo nos advierte, sino que nos protege y mejora nuestra seguridad.



- **Configuración del sitio.** Aquí podremos configurar los diferentes permisos facilitados o concedidos a distintos servicios web como pueden ser el acceso a ubicación, la cámara, micrófono o notificaciones. También los permisos adicionales, como descargas automáticas, portapapeles o controladores de pago entre otros muchos.



En el apartado de 'Contenido' de esta misma opción del menú, se pueden ver las condiciones de cookies, JavaScript, imágenes o ventanas emergentes y redirecciones. Puedes permitir o bloquear cada uno de ellos de manera independiente. Así mismo podemos configurar contenido adicional, desde la reproducción de sonido, hasta el bloqueo de anuncios invasivos o engañosos en los sitios que los vayan a mostrar. También el contenido no seguro, o cómo podemos gestionar los ficheros PDF, visualizarlos en el navegador o directamente descargarlo a nuestro equipo o dispositivo móvil.

4. Configuración de Edge

Microsoft Edge es un navegador web desarrollado por Microsoft, el cual viene de manera predeterminada dentro de los sistemas operativos Windows 10 y Windows 11 en sustitución al navegador Internet Explorer.

La fecha de lanzamiento de Microsoft Edge fue el 29 de julio de 2015. Microsoft lanzó este navegador dada su rapidez y seguridad. Además, gestiona de manera más efectiva la memoria de los dispositivos causando un mayor ahorro en la batería de estos.

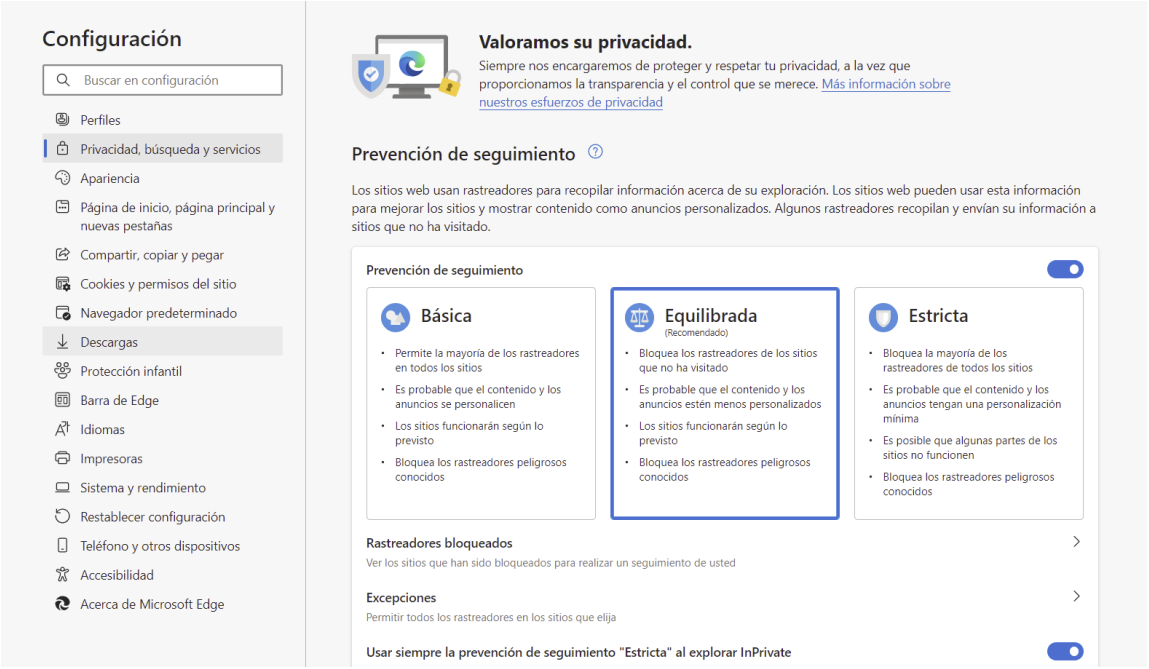
Para configurar las opciones de **seguridad y privacidad de Edge**, hay que seguir estos pasos: Ir a la esquina superior derecha de la pantalla del navegador web Microsoft Edge y pulsar en el icono de los tres puntos seguidos. Aparecerá un menú donde habrá que pulsar en la opción de 'Configuración'. Después en '**Privacidad, búsqueda y servicios**' encontraremos diferentes apartados que detallaremos a continuación:

- **Prevención de seguimiento**: el seguimiento web es realizado por rastreadores que permiten identificar a los usuarios mientras navegan por Internet, recopilando información sobre los sitios que visitan y analizando el comportamiento de estos usuarios. El navegador permite configurar este seguimiento que se realiza del usuario ofreciéndole tres opciones:

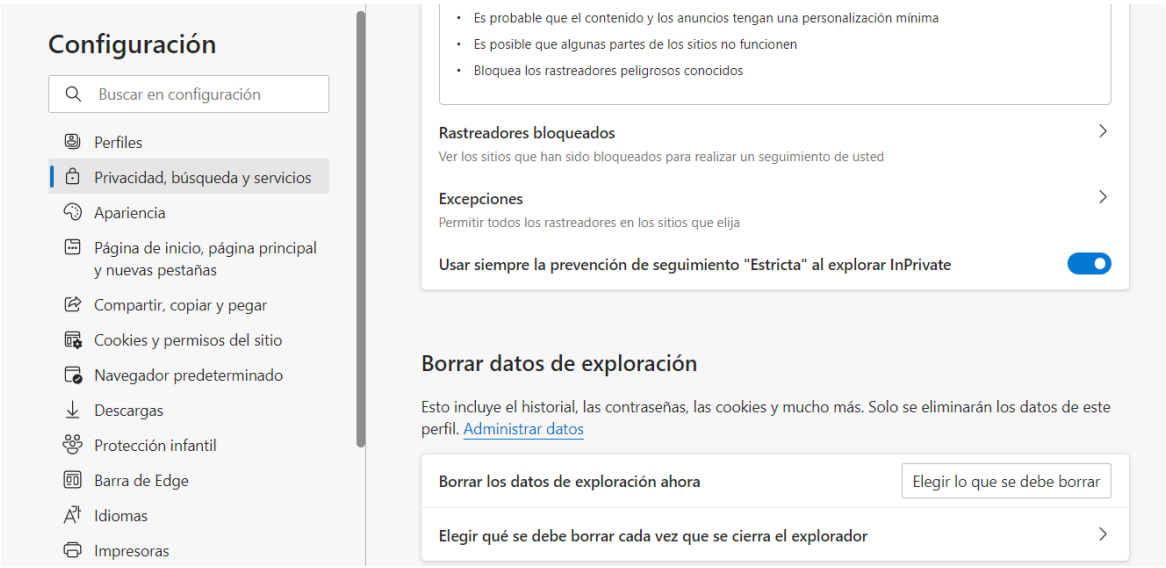
  - **Básica**: Es el nivel menos restrictivo. Está pensado para los usuarios que no les importe los anuncios personalizados o bien las tareas de seguimiento de los sitios web que visitamos. El nivel de protección básico protege frente a rastreadores con malas intenciones.

  - **Equilibrada**: Bloqueará la mayoría de los rastreadores y se reducirá al mínimo la personalización de los anuncios. Esta es la opción que se recomienda tener activada. Tiene las siguientes características: bloquea los rastreadores de los sitios web que no hemos visitado, también permite una total personalización de los anuncios y del contenido que nos muestra estos sitios web, y sobre todo bloquea los rastreadores considerados peligrosos. Esta es la opción recomendada porque equilibra dos conceptos: por un lado, la protección y por otro que los sitios web funcionen, debido a que, para su funcionamiento, muchas webs necesitan hacer uso de estos rastreadores de seguimiento.

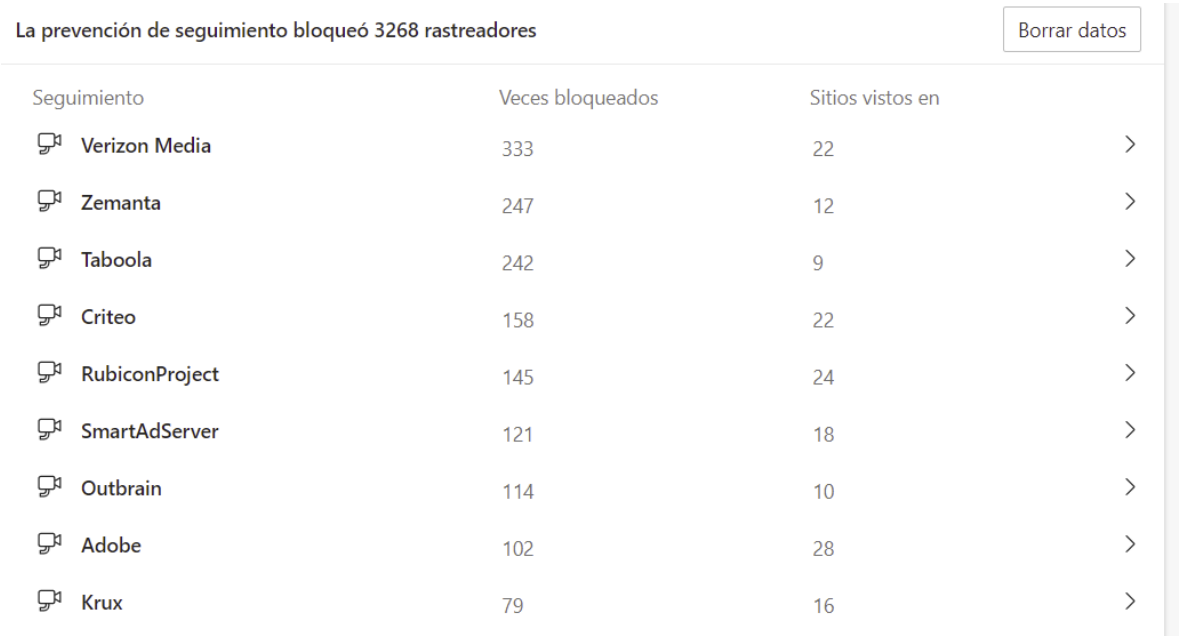
- **Estricta:**
  Esta opción bloqueará la mayoría de los rastreadores en línea. Si bien es cierto que nos proporcionaría la mayor protección, es posible que muchos sitios web dejaran de funcionar, por las razones que hemos definido en el párrafo anterior.



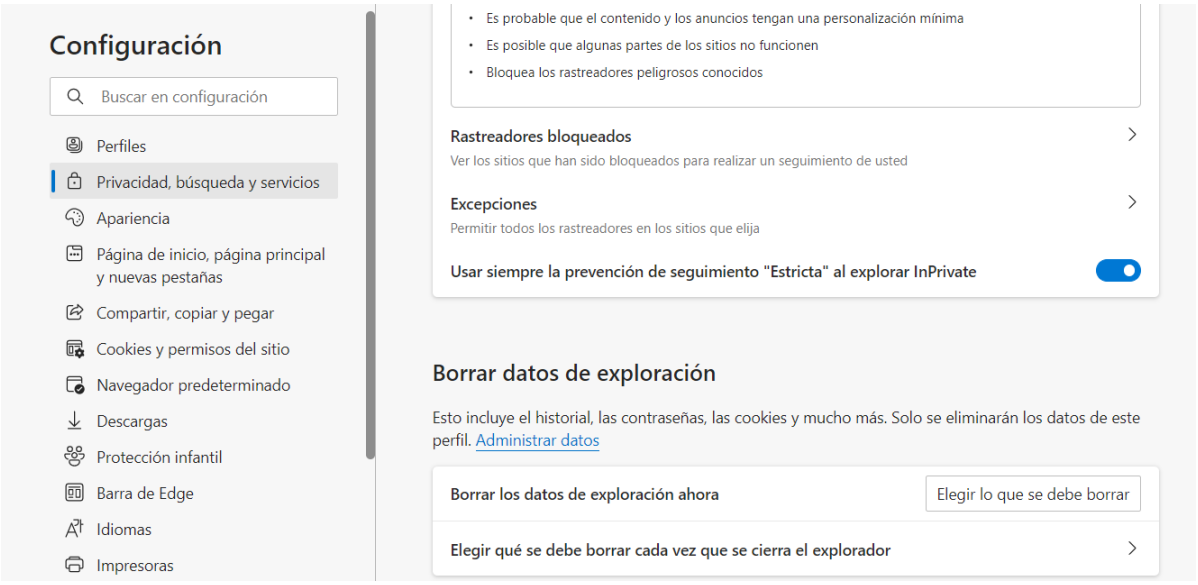
En rastreadores bloqueados, que se encuentra también en la sección de 'Prevención de seguimiento', evitan que los rastreadores no recojan ningún tipo de información de las páginas web visitadas. Haciendo clic en esta opción, se pueden ver los rastreadores que han sido bloqueados y que, por lo tanto, no podrán hacer seguimiento de tu actividad.



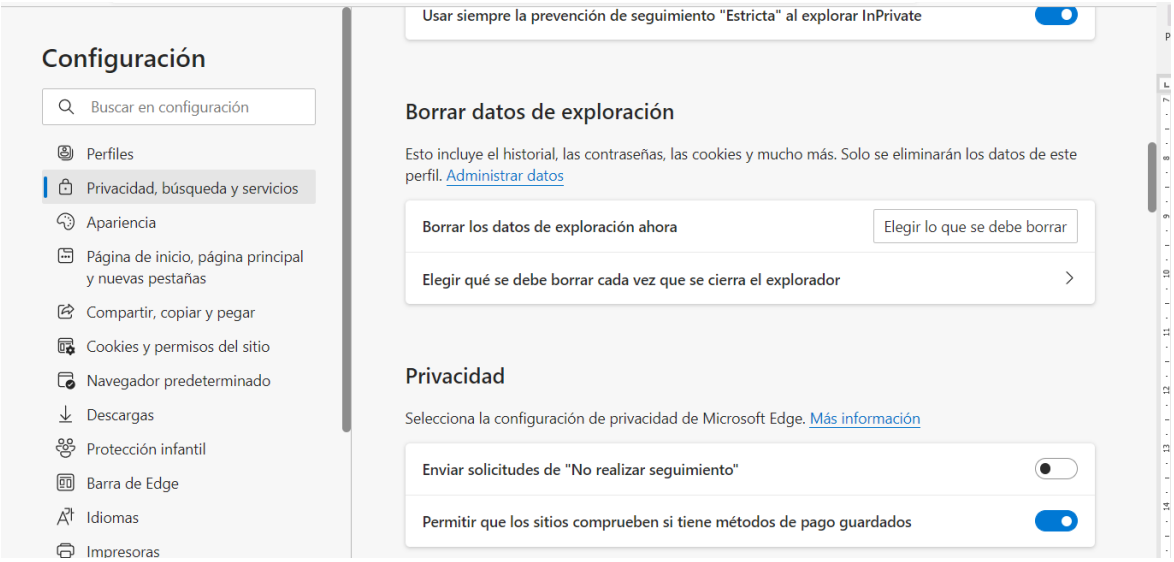
Una vez dentro de esta opción, aparece una lista con el nombre del rastreador, las veces que han sido bloqueados y los sitios vistos (que son los sitios web donde se ha usado este rastreador). Desde aquí, también se podrán borrar todos los datos de los rastreadores haciendo uso del botón 'Borrar datos', situado en la parte superior derecha. Cabe señalar, que está opción garantiza la privacidad, pero puede afectar al funcionamiento de algunos sitios web y funcionalidades en línea que requieren del seguimiento de usuarios ya que promueven contenido personalizados y/o específicos.



Así mismo en el caso de usar siempre ventanas de incógnito, denominadas en **Edge *inPrivate***, deberemos activar la opción 'Usar siempre la prevención de seguimiento "Estricta" al explorar inPrivate', para garantizar la mayor privacidad en la navegación.

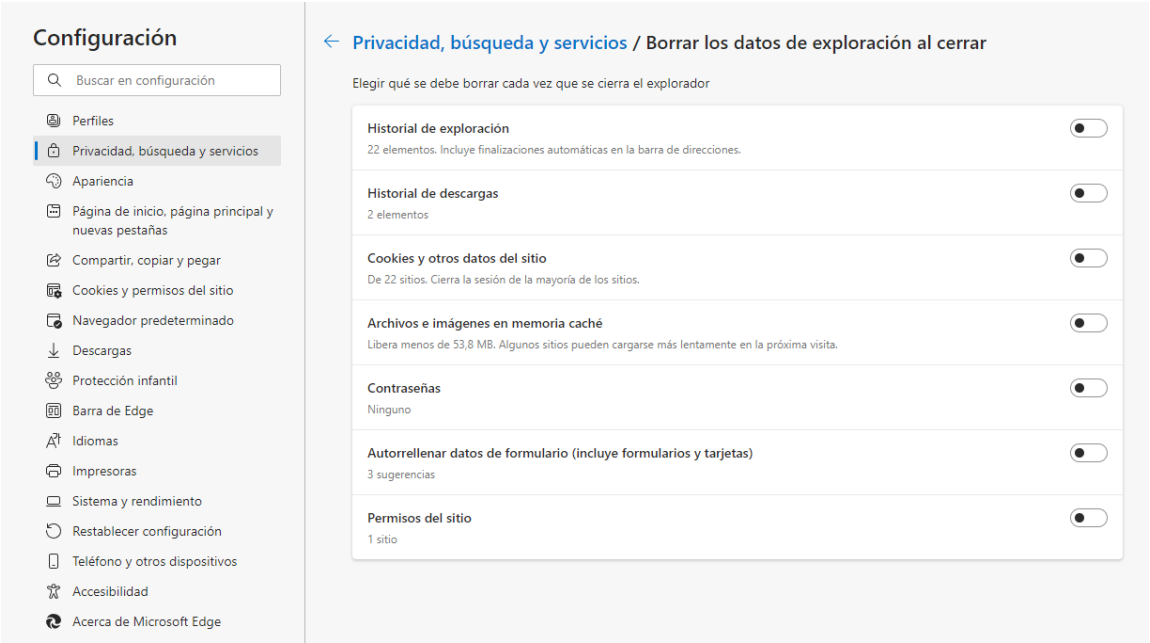


- **Borrar datos de exploración:** en este apartado, pulsaremos en 'Elegir lo que se debe borrar cada vez que se cierra el explorador'. Esta opción se utiliza para borrar aquellos datos que no queremos que se almacenen y también elegir el intervalo de tiempo desde cuándo queremos que se borre.

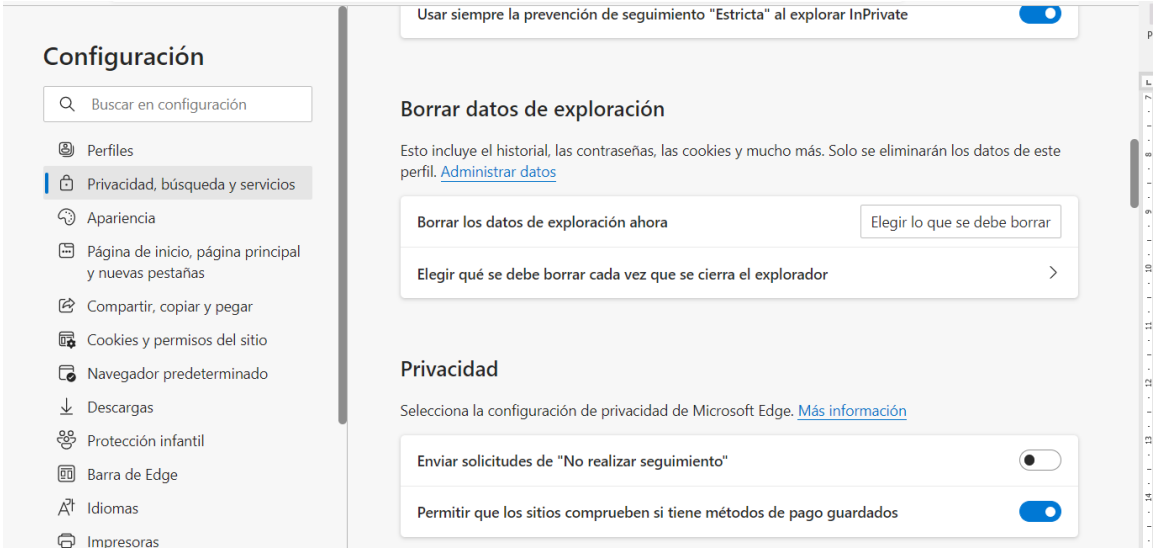


Los datos de exploración que podemos borrar son:

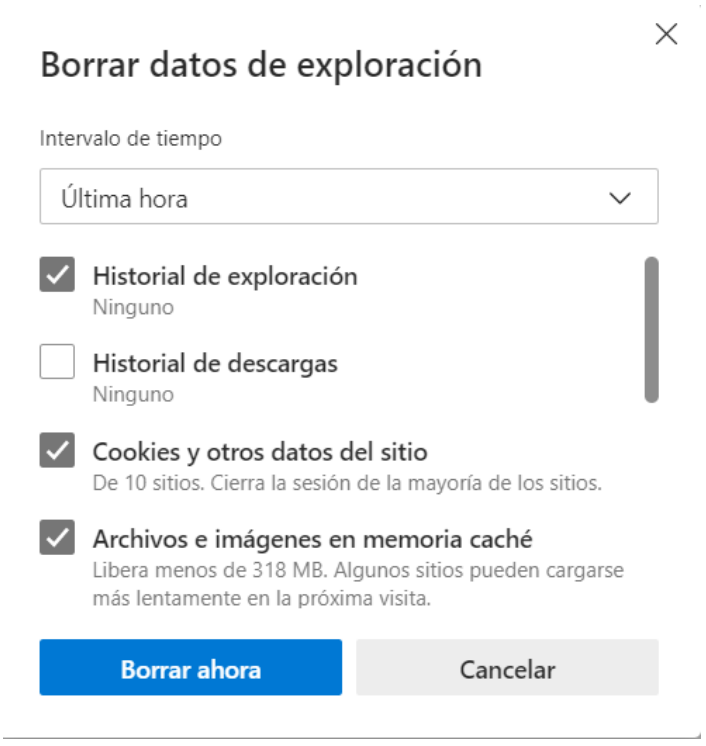
- Historial de exploración
- Historial de descargas
- Cookies y otros datos del sitio
- Archivos de imágenes en memoria caché (una función que permite que, al guardar una serie de datos de manera local, la carga de las páginas web sea más rápida ya que no tiene que volver a cargarla de Internet al regresar a un sitio web ya visitado).
- Contraseñas
- Autorrellenar datos de formularios
- Permisos del sitio



Por tanto, al pinchar en el botón ‘Elegir lo que se debe borrar’ de la opción ‘Borrar datos de exploración ahora’,

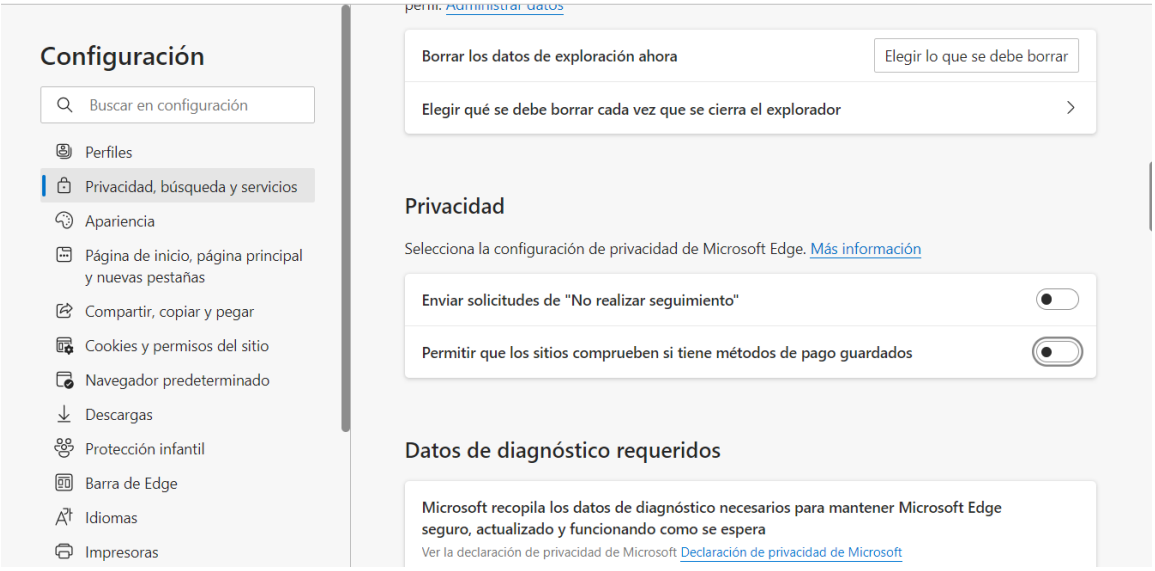


Se pueden marcar las opciones que se quieran eliminar, junto con el intervalo que se encuentra en la parte superior de la ventana. Tras realizar esto, se debe pulsar el botón 'Borrar ahora'.



- **Privacidad**: por defecto, aparece activada la opción 'Permitir que los sitios comprueben si hay métodos de pago guardados'. Es recomendable desactivarla**,** de esta manera evitamos que los sitios web comprueben si tenemos almacenados en el navegador datos sobre nuestra tarjeta de crédito y otros datos relacionados con pagos.

  Adicionalmente, activando la opción 'Enviar solicitudes de no realizar seguimiento', impedimos que se haga algún tipo de seguimiento de nuestra navegación por parte de sitios web. Es posible que no siempre lo cumplan, ya que algunas webs ignoran esta opción que hemos seleccionado y siguen recopilando información sobre nuestra navegación en ese sitio web.



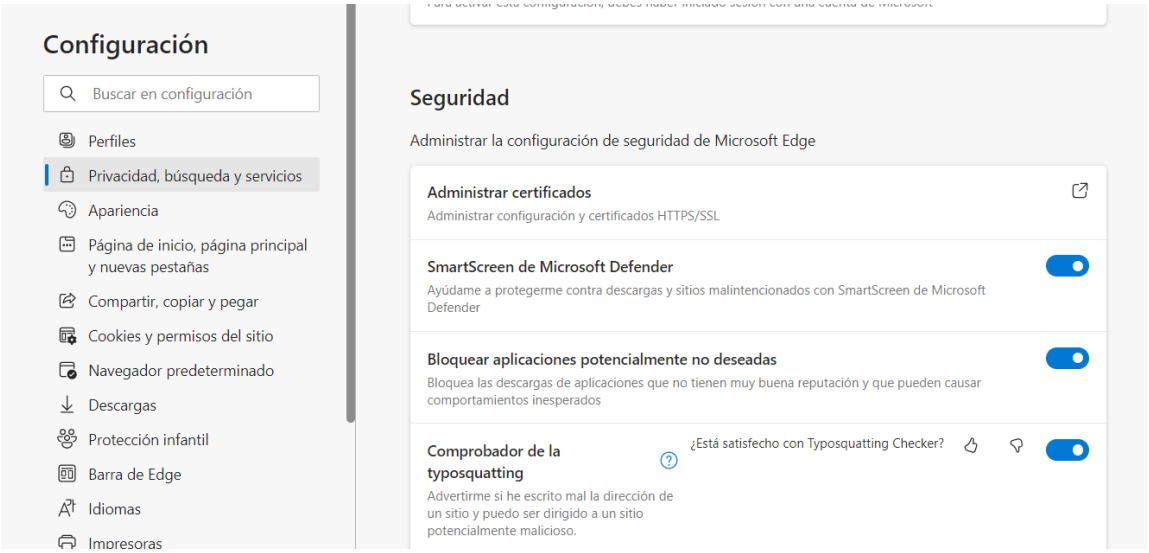
- **Personalizar su experiencia web:** es preferible que esta opción esté desactivada. Cuanta más personalización, menos seguridad y privacidad. Si se activa, se personalizará la publicidad, las búsquedas, las noticias y cualquier otro servicio de Microsoft.

- **Seguridad:** en este apartado nos encontramos las siguientes opciones:
  - '**Administrar certificados'**. Gestiona los certificados digitales que tengamos instalados en nuestro equipo.
  - '***SmartScreen* de Microsoft Defender'**. Es parte de la aplicación de seguridad que viene instalada en Windows y que permite protegernos contra la descarga, o instalación de archivos que puedan ser maliciosos a través de una advertencia. Es recomendable activarlo.
  - '**Bloquear aplicaciones potencialmente no deseadas'**. Te permite bloquear las descargas de aplicaciones que tengan mala reputación y que pueden ocasionar comportamientos inesperados en nuestros dispositivos. Es otra opción que recomendamos activar.

- Enlace de interés:

En el siguiente enlace se pueden ver de manera más detallada las diferentes opciones que ofrece recientemente Microsoft Edge en cuanto a opciones de seguridad:

https://www.microsoft.com/es-es/edge/features/security?form=MA13FJ

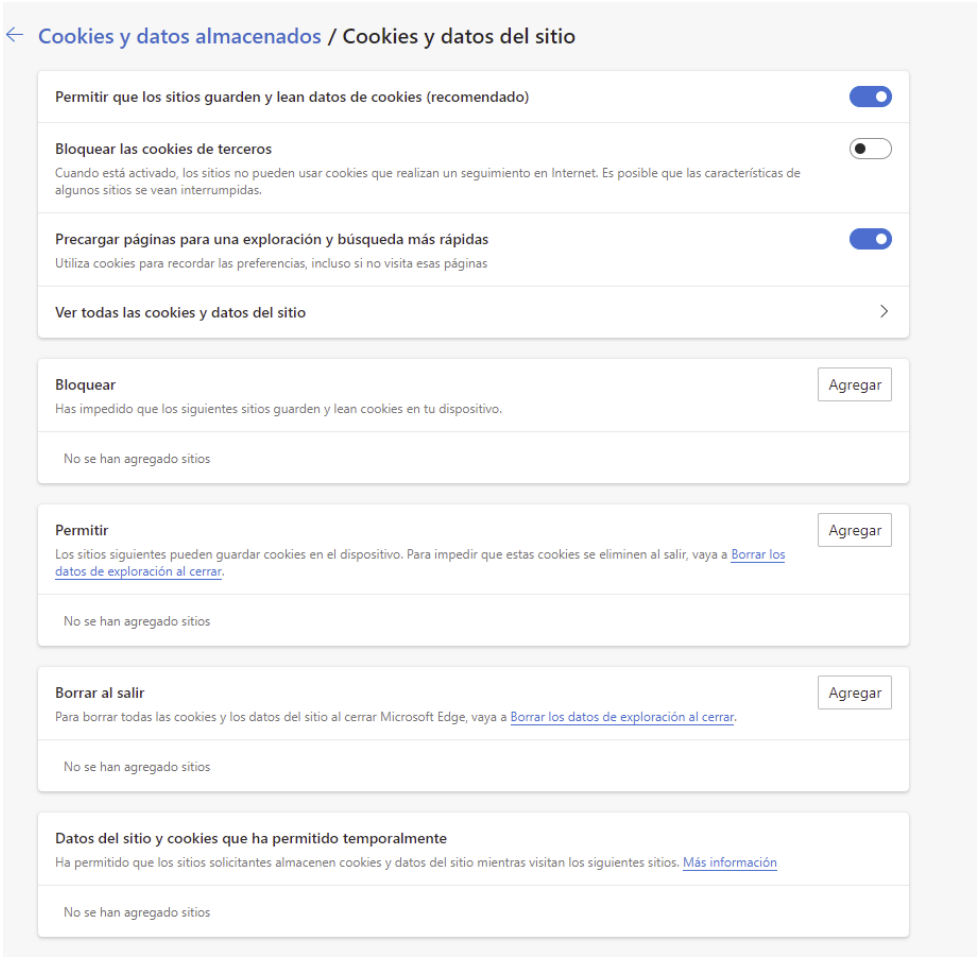


Si volvemos a fijarnos en el menú de configuración ubicado a la izquierda, debemos pinchar ahora en '*Cookies* y permisos del sitio' donde nos aparecerán una serie de opciones de configuración que vamos a repasar.

Lo primero que tenemos que explicar es qué es una *cookie*. La definimos como un archivo de texto que los sitios web visitados envían al navegador web con información sobre tu visita, para que después, al volver a visitar el sitio web, te reconozcan y de esta manera te faciliten la navegación en dicha web.

Nos encontraremos las siguientes opciones:

1. ***Cookies* y datos almacenados**: Con esta opción se puede controlar como el propio navegador usa las cookies y los datos que están almacenados. Permite administrar y eliminar todas las *cookies* (de cualquier tipo), y, datos del sitio. Al entrar veremos varias opciones. Lo primero es que se debe dejar activada la opción 'Permitir que los sitios guarden y lean los datos de *cookies* (recomendado)' porque si se desactiva es posible que algunos sitios web necesiten de estas *cookies* y dejen de funcionar. En cambio, recomendamos activar la opción 'Bloquear las *cookies* de terceros', así se evita el seguimiento de la navegación. Podría ocurrir que algunos sitios web no funcionen correctamente.
   En cuanto a la opción 'Precargar página para una exploración y búsqueda más rápidas', es recomendable desactivarla por las mismas razones que hemos esgrimido anteriormente. Si evitamos estas *cookies,* supone que no se puedan almacenar en el navegador nuestras preferencias de los sitios web que visitamos, por ejemplo, si en una tienda hacemos siempre búsquedas sobre una misma categoría de productos.
   Es importante gestionar bien las particularidades en esta opción según las propias preferencias del usuario.



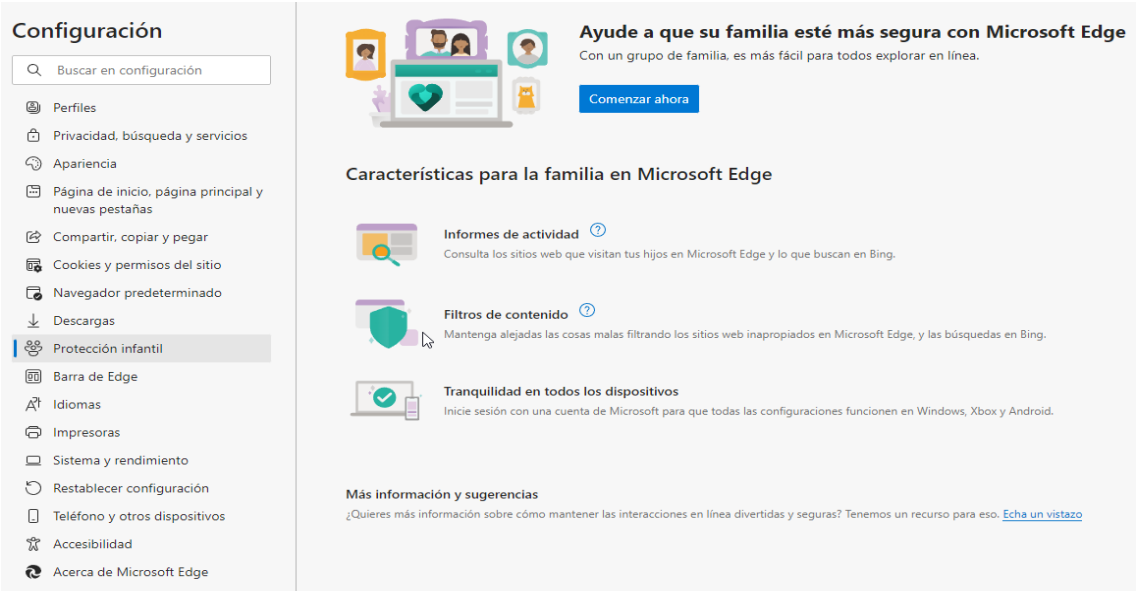
Pasemos de nuevo al menú de configuración de la izquierda. En esta ocasión pincharemos en '**Descargas**'. A través de esta opción es posible configurar diferentes aspectos sobre las descargas de archivos a través del navegador Edge. Nos vamos a centrar en dos de las opciones que están disponibles:

- '**Preguntarme qué hacer en cada descarga**'. Aquí vamos a ver en cada momento (cuando se vaya a descargar un fichero) un aviso a través de un mensaje, preguntando en qué carpeta de nuestro dispositivo queremos guardar el fichero.
- '**Mostrar menús de descargas al iniciar una descarga**'. Esta opción ayudará a ver el fichero que estamos descargando, el tamaño y el tiempo que queda de descarga, información útil para controlar también qué fichero nos estamos descargando.

Una de las opciones que ofrece Microsoft Edge es la de "Descarga segura", que se encuentran dentro del apartado "Privacidad, Búsqueda y servicios". Luego hay que

entrar en “Seguridad”, y, por último, acceder a “Descarga segura”. Si se activa esta opción dentro del navegador, se detectará de manera automática los posibles archivos y amenazas en cuanto a seguridad se refiere. Si se encuentra cualquier archivo perjudicial, el navegador te lo hará saber mediante una advertencia, y se pueden tomar las medidas necesarias de seguridad.

Otra de las opciones a destacar que encontramos en el menú de configuración de izquierda, es el de ‘Protección infantil’, como medida de seguridad en el caso de tener menores en casa. Aquí se podrán establecer filtros de contenido y revisar los informes de actividad. Es posible consultar los sitios web que hayan visitado los menores en Microsoft Edge y también sus búsquedas en el buscador Bing. También te permite que la configuración que hayas realizado se mantenga tanto en Windows, Xbox y Android, en el caso de que tengas las cuentas vinculadas.



5. Configuración de Firefox

Firefox es un navegador web desarrollado por la corporación Mozilla. Es muy popular entre los programadores porque está desarrollado como *software* libre, es decir, el código de programación está abierto al público y permite que los programadores lo modifiquen.

Mozilla Firefox se lanzó por primera vez el 9 de noviembre de 2004. Actualmente es uno de los navegadores más usado, según la web española "Muylinux", relacionada con *software* de código abierto, este navegador es el más popular en el año 2023.

Es importante utilizar siempre la última versión cuando naveguemos a través de este navegador para evitar vulnerabilidades. Normalmente se actualiza de manera automática, se pueden buscar actualizaciones en cualquier momento.

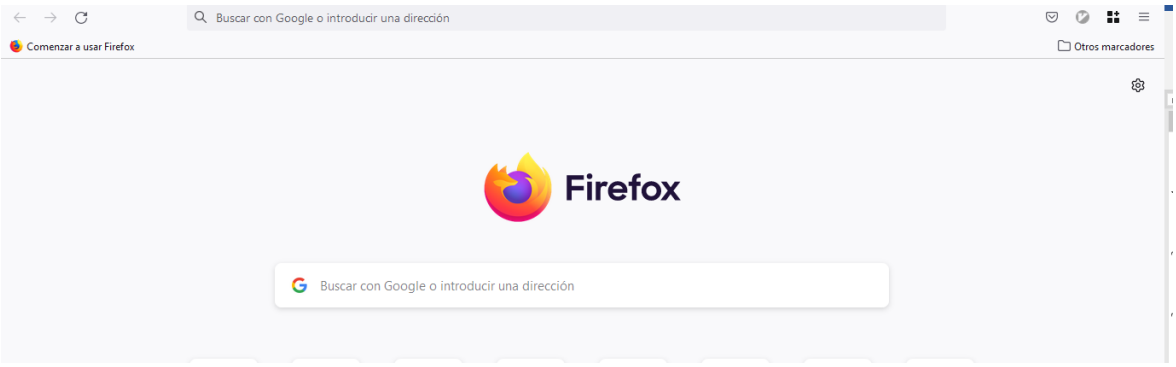
Para actualizar Firefox, se han de seguir los siguientes pasos:

- Hacer clic en el botón de menú (tres líneas situadas en la barra de herramientas), ir a "Ayuda" y seleccionar "Acerca de Firefox", posteriormente, se abrirá una nueva ventana.
- Seguidamente, se buscará actualizaciones de forma automática. Si existen actualizaciones disponibles se descargarán.
- Finalizada la descarga, hay que hacer clic en "Reiniciar para actualizar Firefox"

A continuación, se detallan algunas de las configuraciones de privacidad y seguridad de Firefox. Existen dos formas de acceder a ellas:

- A través del icono de engranaje situado en la parte superior derecha del buscador.

- Mediante el menú ubicado en la esquina superior derecha del navegador, en forma de tres rayas. Al pulsar aparecerá un menú. Abajo encontraremos la opción de 'Ajustes'.

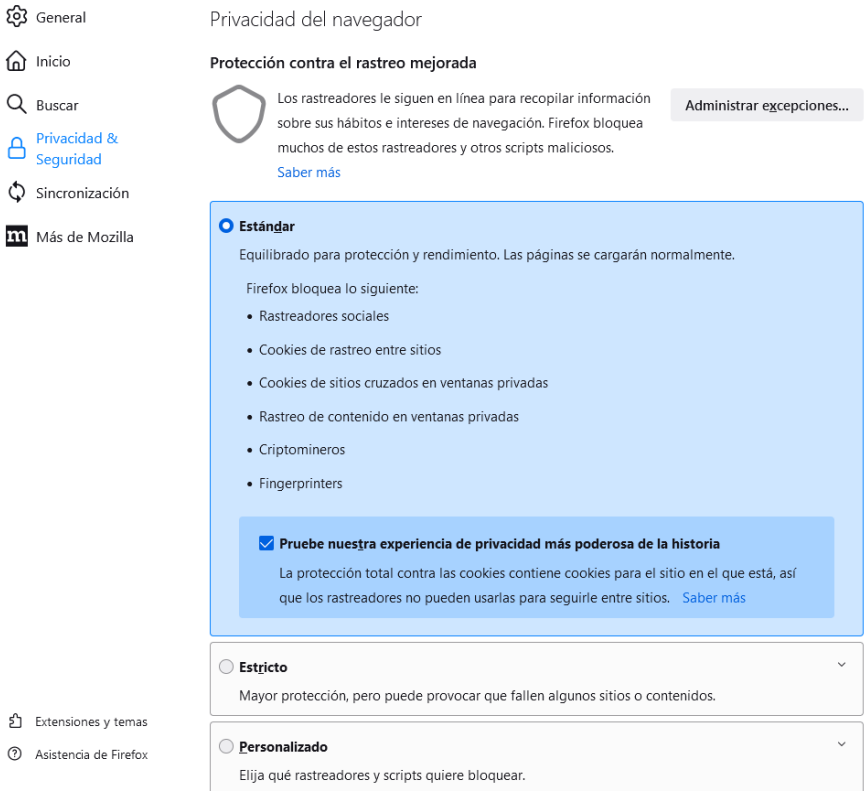


Una vez dentro de 'Ajustes', aparecerá un menú a la izquierda con diferentes opciones.

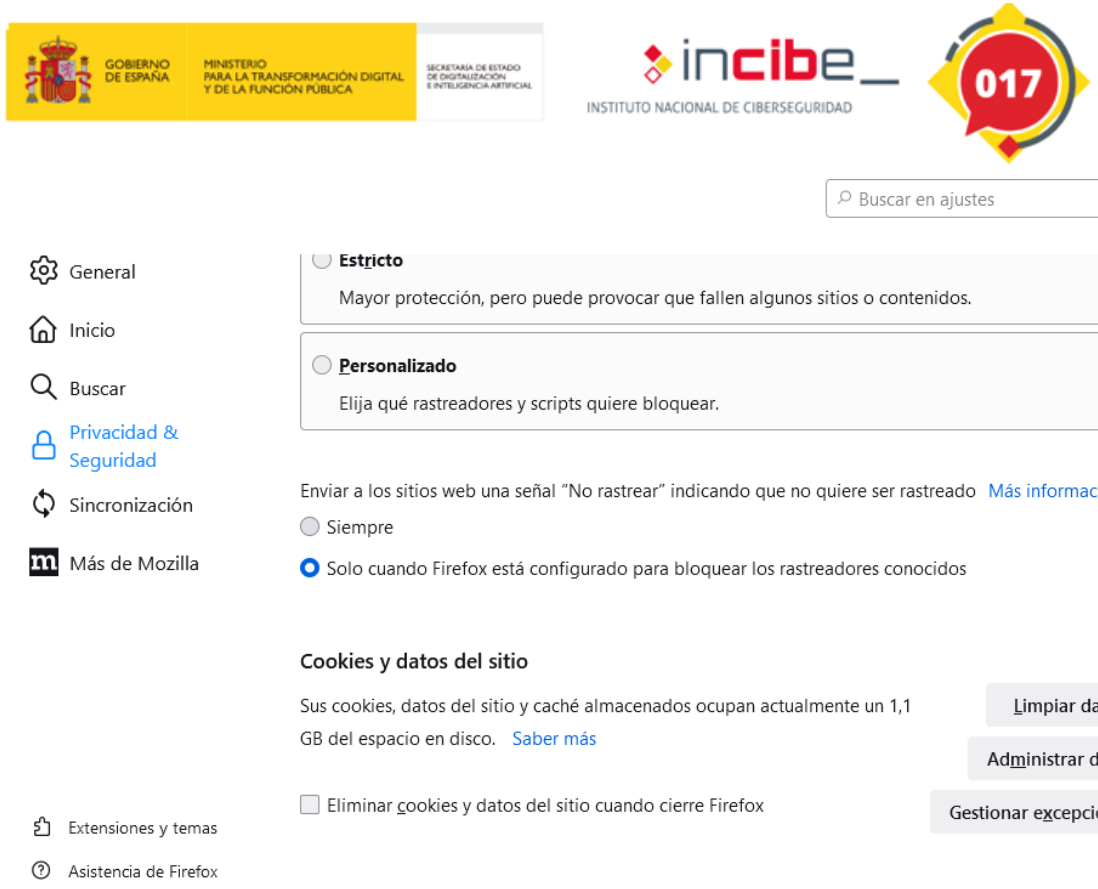
Comenzaremos por la opción de 'Privacidad y seguridad':

- Una de las primeras configuraciones que aparece es **'Protección contra el rastreo mejorada'**, en la que apreciamos tres niveles **(estándar, estricto o personalizado):**
  - Se recomienda usar la opción **'Estándar'**, que bloquea los rastreadores sociales, las *cookies* de rastreos entre sitios y las de sitios cruzados en ventanas privadas, los criptomineros (código malicioso que secuestra un dispositivo para usarlo en la extracción de criptomonedas), y *finger printers* (técnica de seguimiento de usuarios en web, mediante la cual se crea una huella digital de tu paso por Internet).
  - La opción **'Estricto'** es la que ofrece mayor protección y, en caso de activarla, podría suponer que muchos sitios web dejaran de funcionar.
  - En el caso de que nuestros conocimientos sean más avanzados, podríamos usar la opción **'Personalizado'**, donde podremos marcar qué rastreadores y *scripts* bloquear (*cookies*, contenido de rastreo,

criptomonedas y *finger printers*).



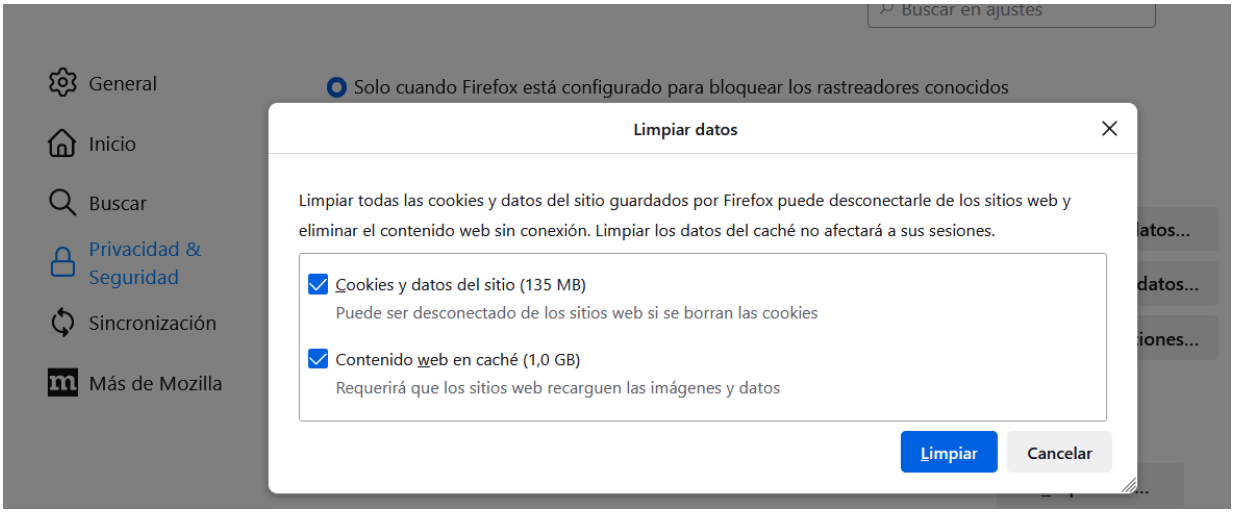
- Justo debajo de estas tres opciones (estándar, estricto y personalizado) encontramos la opción de enviar a las webs una señal de **'no rastreo'**. Esta ofrece la posibilidad de configurarlo para que se envíe siempre o solo cuando el navegador está configurado para bloquear rastreadores conocidos. Para mayor privacidad, lo recomendable es activar la opción 'Siempre'.



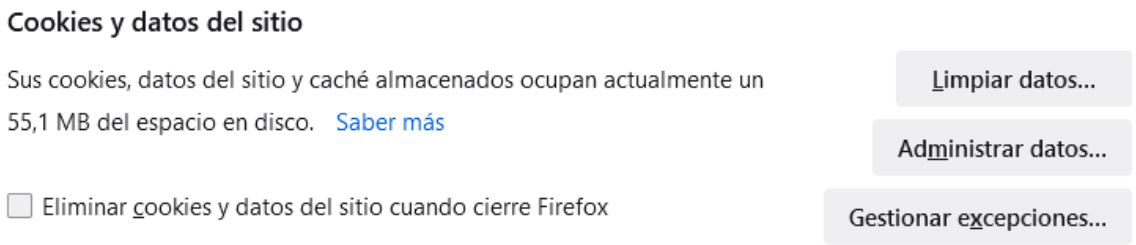
Dependiendo de la versión, esta opción de "no rastreo", puede variar de manera poco significativa, ofreciendo en la mayoría de los casos dos opciones.

- En el apartado de **'*Cookies* y datos del sitio'** es posible borrar las *cookies* y los datos de caché almacenados.

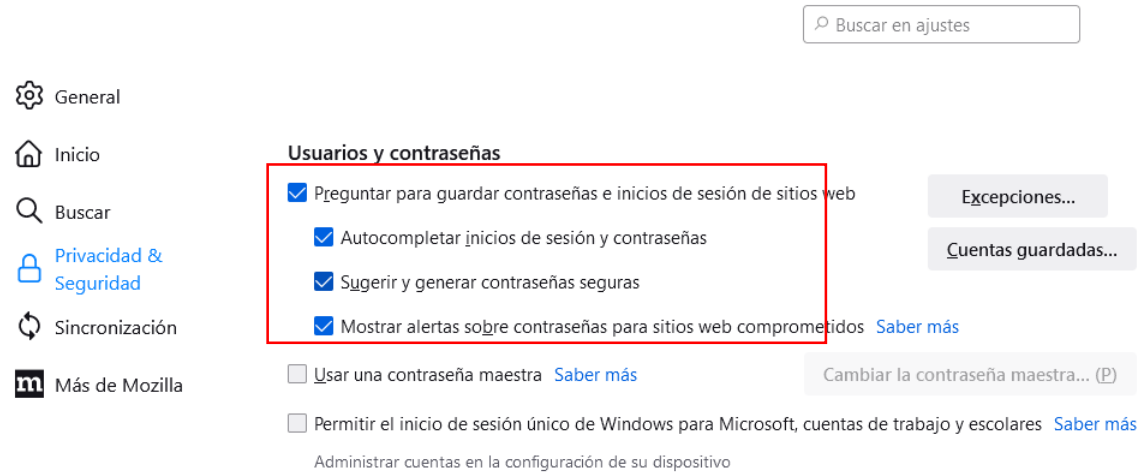
- **'Limpiar datos':** a través de esta opción se eliminan las *cookies* y datos del sitio. También se puede eliminar el contenido web en caché (contenido que se almacena en tu dispositivo para que la carga de los sitios web visitados sea más rápida).



Dentro de esta sección tenemos la posibilidad de marcar la opción 'Eliminar *cookies* y datos del sitio cuando cierre Firefox'. Al marcarla, siempre que cerremos el navegador, se realizará una limpieza automática de los datos almacenados sobre nuestra navegación.

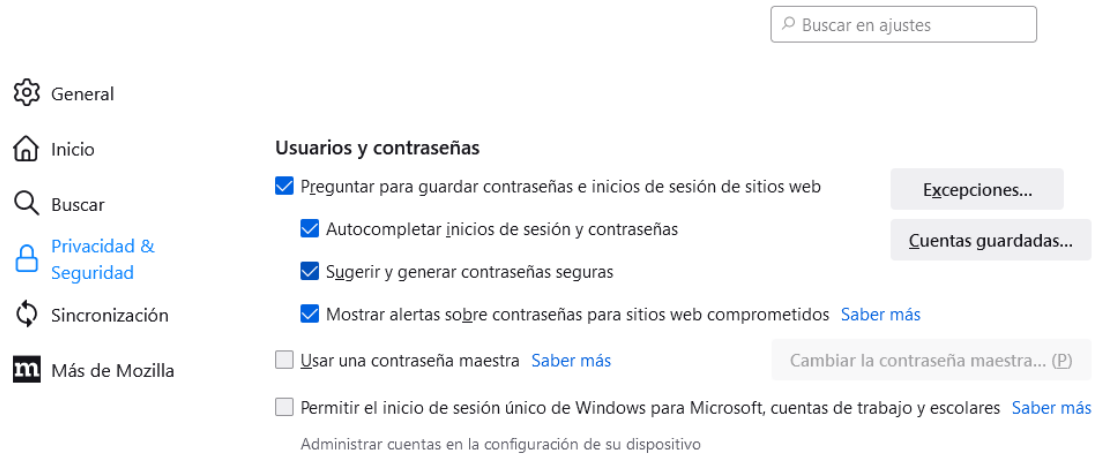


- En el apartado **'Usuarios y contraseñas'** podemos habilitar la opción **'Preguntar para guardar contraseñas y e inicios de sesión de sitios web'**. Con esta opción activada tendremos más control sobre la seguridad de nuestras credenciales. También podremos activar las opciones de 'Autocompletar inicios de sesión y contraseñas', 'Sugerir y generar contraseñas seguras' o 'Mostrar alertas sobre contraseñas para sitios web comprometidos'. Para ello, es conveniente crear una cuenta en Firefox.



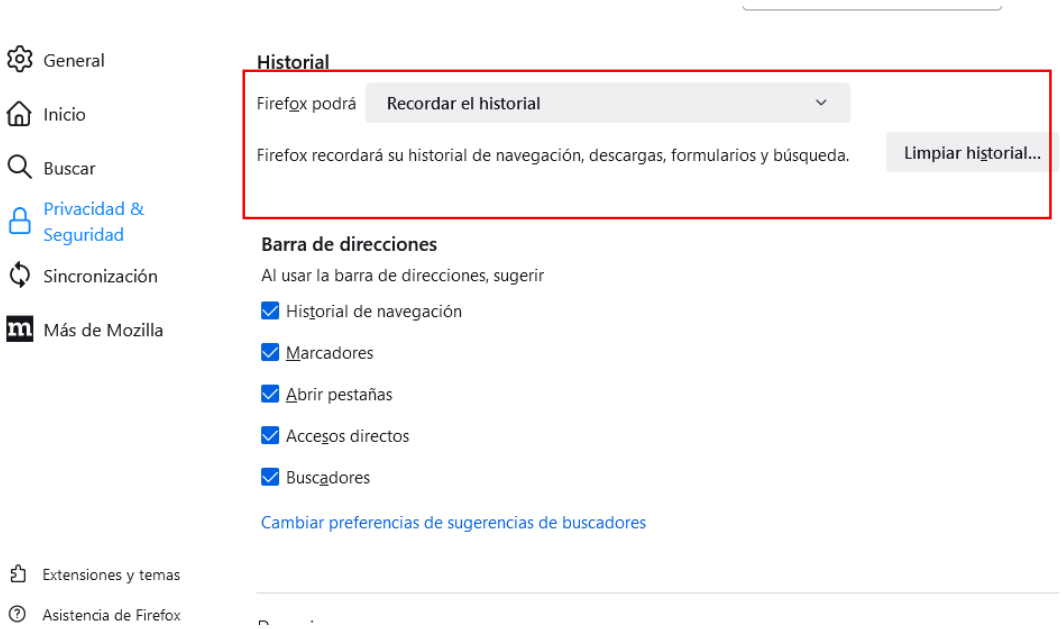
Se recomienda crear una **contraseña maestra** (una contraseña que nos permita proteger el resto de credenciales o cualquier dato confidencial) si el equipo es compartido con otros usuarios. De esta manera, si tenemos cuentas y contraseñas guardadas, nadie podrá acceder a ellas sin la contraseña maestra.

Es importante elegir una contraseña maestra que sea lo más segura posible. Un ejemplo de ella podría ser: "Wpr0P!c4lDOnt@8n$2024!



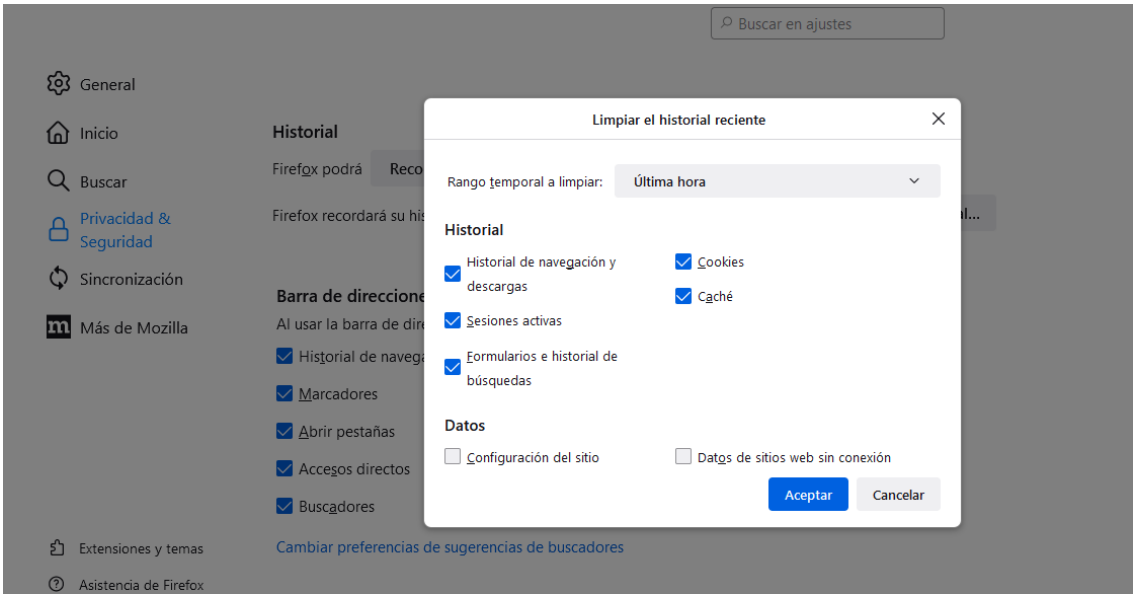
- En el apartado de **'Historial'** se puede seleccionar 'No recordar el historial' (más restrictiva), 'Recordar el historial' o 'Usar una configuración personalizada para el historial'. Por ejemplo, en el caso de que estemos usando un ordenador

compartido, es recomendable usar 'No recordar historial', o en el caso de dejar la opción 'Recordar el historial', podemos optar por 'Limpiar historial" para evitar dejar rastro de nuestras búsquedas y navegación.

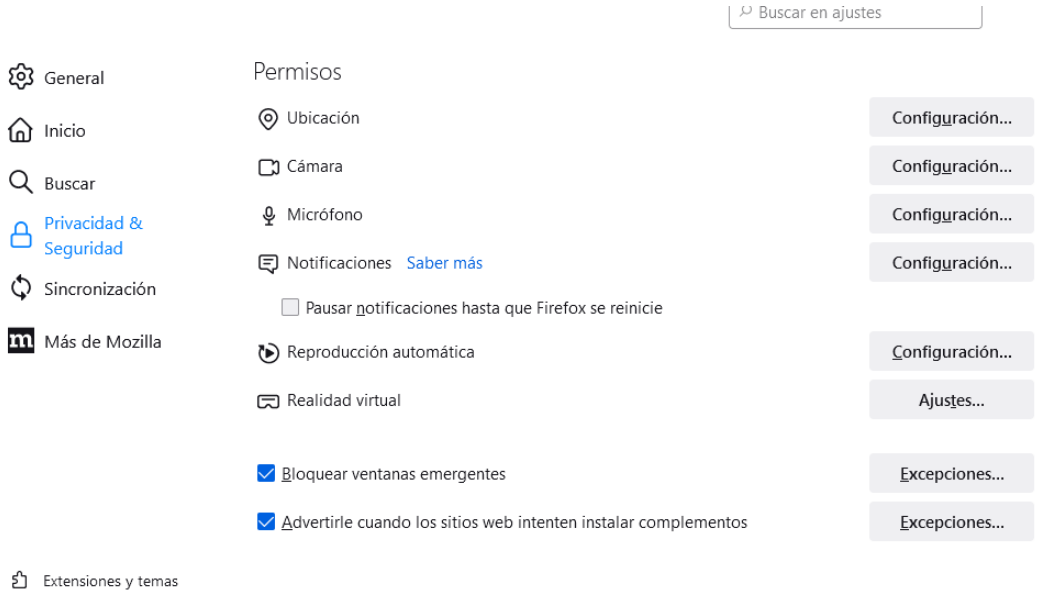


Al pulsar en el botón **'Limpiar historial'** aparecerán las siguientes opciones:

- Por un lado, podemos configurar el rango temporal a limpiar: última hora, últimas dos horas, última cuatro horas, hoy o todo.
- Por otro lado, los datos que queremos limpiar: historial de navegación y descargas, sesiones activas, formulario e historial de búsquedas, *cookies*, caché, datos configuración del sitio y datos de sitios web sin conexión.

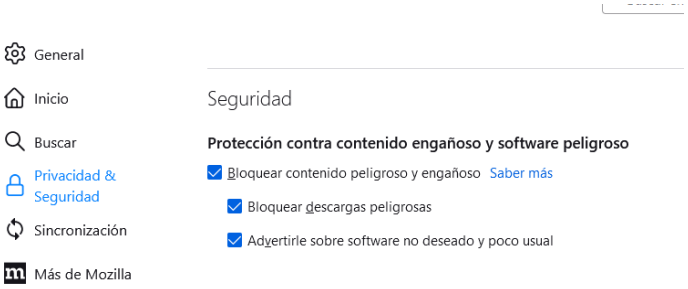


- Desde la sección de **'Permisos'** se pueden crear listas de sitios web que permitan, por ejemplo, el uso de la ubicación, de la cámara, del micrófono, etc. Activando el apartado 'Bloquear nuevas solicitudes de acceso a su categoría', evitaremos que aquellos sitios web que no estén en la lista de permisos puedan utilizarla. Como recomendación, si se quiere mejorar la privacidad, se puede crear una lista con los sitios permitidos en cada una de las opciones y activar la opción de 'Bloquear nuevas solicitudes…'.



- Otra de las opciones es la **'Recopilación y uso de datos de Firefox'**. Tal y como advierte Firefox, esta configuración se usa para recopilar información y mejorar el navegador. Aquí se encuentran varias opciones:
  - 'Permitir a Firefox enviar datos técnicos y de interacción a Mozilla'. Estos datos de interacción son sobre el número de paginas web visitadas, número de pestañas y ventanas abiertas, duración de las sesiones, etc. Los datos técnicos son sobre la versión e idioma de Firefox, fallos, actualizaciones, etc. Es recomendable dejarlo activado porque no supone ninguna información de tipo personal.
  - 'Permitir que Firefox instale y ejecute estudios'. Esta opción permite que el navegador realice cambios para experimentar en sus estudios. Habilitando esta opción los usuarios contribuyen a que el navegador pueda sacar datos de interés y mejorar su funcionamiento.

- En el apartado de **'Seguridad'** es recomendable tener activadas las tres opciones que se presentan: 'Bloquear contenido peligroso y engañoso', 'Bloquear descargas peligrosas', y 'Advertirle sobre *software* no deseado y poco usual'. De esta manera, evitaremos que se puedan descargar contenidos maliciosos.



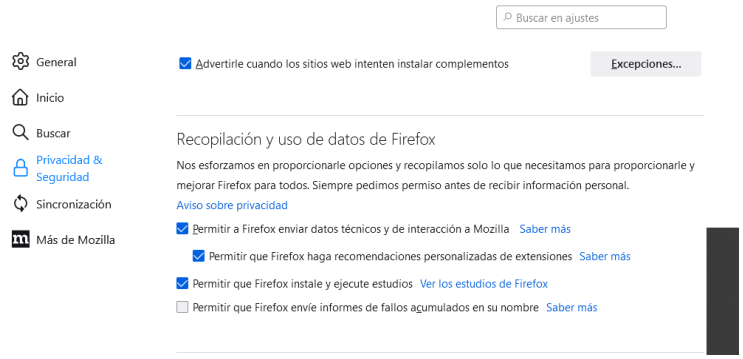
'Bloquear descargas peligrosas' nos protege contra la posibilidad de que podamos ser infectados con *malware* (programas potencialmente dañinos), mientras que 'Advertirme sobre *software* no deseado y poco usual' nos avisará en el caso de que Firefox detecte un *software* que considere peligroso.

Otra configuración importante es la **recopilación y uso de datos de Firefox**, pudiendo establecer diferentes opciones:

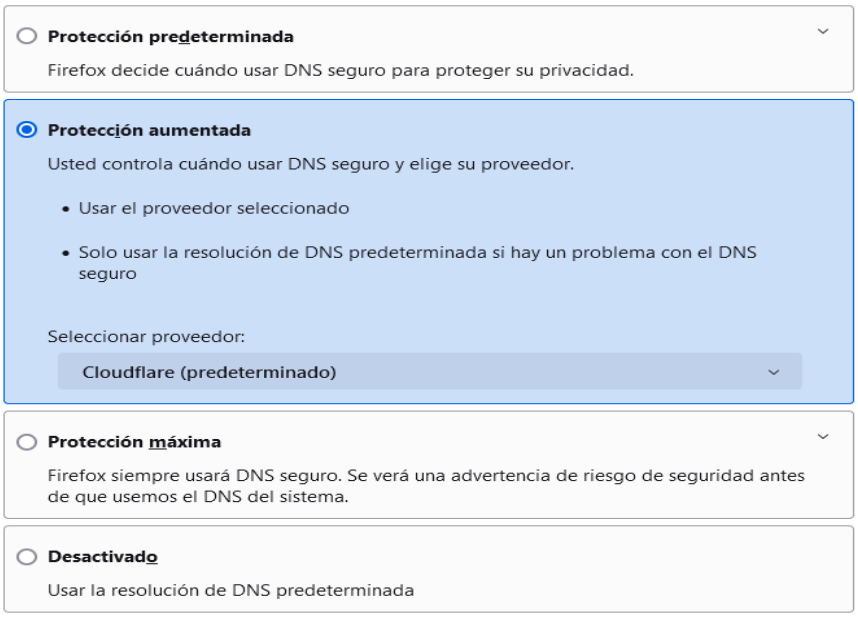
- **'Permitir a Firefox enviar datos técnicos y de interacción a Mozilla':** es útil para mejorar el rendimiento y la estabilidad del navegador web.
- **'Permitir que Firefox haga recomendaciones personalizadas de extensiones':** con esta opción permitimos que Firefox haga recomendaciones

sobre las extensiones, que son complementos que pueden ayudar a mejorar la experiencia en la navegación web.

- **'Permitir que Firefox instale y ejecute estudios':** si marcamos esta opción, permitimos que se puedan instalar y ejecutar estudios estadísticos.
- **'Permitir que Firefox envíe informes de fallos acumulados en su nombre':** esta opción sirve para que se compartan con Firefox los informes de errores que se produzcan en el momento que usemos su navegador.



La opción "*DNS sobre HTTP*", permite a los usuarios enviar consultas mediante HTTP sin usar el protocolo tradicional, por lo que se aumenta la seguridad del navegador al encriptar las consultas DNS. Envía los pedidos de un nombre de dominio mediante una conexión cifrada. Podemos encontrar las siguientes opciones:



6. Cómo borrar tu huella

La huella digital podríamos definirla como el rastro que dejamos al navegar por Internet por las distintas páginas webs y servicios online que utilizamos. Lo primero que debemos tener en cuenta, antes de continuar, es que eliminar por completo el rastro online que puede tener una persona no es una tarea fácil, y en algunos casos, es posible que no se pueda llegar a borrar por completo.

Lo que sí se puede hacer es minimizar dicho rastro para que la información relacionada con un usuario para que no muestre una imagen sobre él que no desee, no caiga en manos de personas no deseadas o se haga un uso indebido de ella. El proceso se puede alargar y se recomienda tener paciencia a la hora de afrontarlo.

Antes de conocer cómo podemos borrar la huella digital, es importante que conozcas todos tus derechos que establece la normativa de protección de datos para que los puedas ejercer ante el responsable si fuera necesario.

Nos referimos a los derechos del RGPD (Reglamento General de Protección de Datos de 2016, del Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea cuya intención es reforzar y unificar la protección de datos para todos los individuos dentro de la Unión Europea) cuyo objetivo es permitir a las personas físicas poder ejercer un control mayor sobre sus datos de carácter personal. A continuación, detallamos cada uno de ellos.

- **Derecho de Acceso**

Consiste en el derecho a solicitar información al responsable de un fichero de datos sobre el tratamiento, finalidad, origen y las comunicaciones que se puedan haber realizado o previsto hacerlo sobre nuestros datos personales. El responsable debe responder antes de un plazo máximo de 30 días, desde la recepción de nuestra solicitud.

- **Derecho de Rectificación**

Este derecho permite solicitar la modificación de datos que se consideren inexactos o incompletos. En este caso se debe justificar documentalmente la rectificación de dichos datos. El responsable del fichero dispondrá entonces de 10 días hábiles para llevar a cabo la resolución de nuestra solicitud.

- **Derecho de Oposición**

Gracias al Derecho de oposición es posible oponerse al tratamiento de nuestros datos personales. Se puede solicitar en los siguientes casos: que no se haya dado el consentimiento, que los ficheros se utilicen con fines publicitarios, que el tratamiento de los datos tenga como finalidad tomar una decisión con la que te puedas sentir afectado. Para realizar la solicitud hay que justificarla con motivos legítimos, tendrán que ser relativos a una situación personal concreta. En ese caso, igual que el anterior, el responsable del fichero dispondrá de 10 días hábiles para llevar a cabo la resolución.

- **Derecho de supresión ("al olvido")**

Ejercer este derecho nos garantiza reducir la huella digital en Internet. Se tienen que dar algunas circunstancias como, por ejemplo, que tus datos personales sean innecesarios con respecto al fin con el que fueron recogidos inicialmente. O si decides retirar el consentimiento de uso de esos datos. También puedes ejercer ese derecho si han sido tratados de forma ilegal tus datos, o si a causa de una obligación legal deben suprimirse.

La RGPD (Reglamento General de Protección de Datos) ha conectado este derecho con el denominado "derecho al olvido". Este derecho no es ilimitado, de tal forma que puede ser factible no proceder a la supresión cuando el tratamiento sea necesario puesto que depende de otros aspectos, como, por ejemplo, el derecho a la libertad de expresión e información entre otros.

- **Derecho a la limitación del tratamiento**

Este derecho consiste en que obtengas la limitación del tratamiento de tus datos que realiza el responsable, pudiendo solicitar la suspensión del tratamiento de tus datos, por ejemplo, en el caso de inexactitud de los datos, o solicitar al responsable la conservación tus datos. Por ejemplo, en el caso de que te hayas opuesto a la supresión de los datos porque el tratamiento de estos ha sido ilegal o bien porque el interesado necesita que se mantengan para ejercer alguna reclamación.

- **Derecho a la portabilidad**

Es un derecho que permite que los datos personales que hayas recibido de un responsable del tratamiento de tus datos, puedas transmitirlo a otros responsables sin que se oponga o impida el anterior responsable.

- **Derecho a no ser objeto de decisiones individuales automatizadas**

Este derecho te garantiza que no serás objeto de decisiones individuales de carácter automatizado. Es decir, que no sea una decisión basada en el tratamiento de tus datos, por ejemplo, elaborando un perfil que pueda provocar efectos de tipo jurídico.

- **Derecho de información**

Este derecho permite a los ciudadanos recibir información transparente y clara sobre como sus datos personales van a ser tratados.

Pasos para minimizar nuestra huella digital

El primer paso para intentar borrar la huella digital es hacer una lista de los sitios webs donde está almacenada la información que se desea eliminar: redes sociales, tiendas online, foros, suscripciones, servicios online, etc. Se trata de hacer *egosurfing*, es decir, realizar una búsqueda en Internet por nuestro nombre completo, DNI, teléfono o cualquier otra información personal (este concepto lo conocimos en el módulo 2) para conocer qué sabe Internet sobre nosotros.

Una vez se haya identificado la información a eliminar y decidido el sitio del que se quiere borrar, se debe acceder a cada una de las plataformas donde está alojada, es decir, almacenada y publicada. Si se quiere eliminar toda la información, lo más efectivo es borrar la cuenta. Para ello, hay que acceder a la red social o el sitio web que corresponda, entrar en la configuración de la cuenta y buscar la opción de desactivar, eliminar o cerrar cuenta de usuario. Dependiendo de la aplicación, la opción puede estar localizada en el apartado de Seguridad, Privacidad o algo similar. A modo de ayuda, os facilitamos cómo eliminar una cuenta en servicios muy conocidos como: Facebook, Instagram, X y TikTok.

En cambio, si se quiere restringir un perfil público, dentro de la configuración de la cuenta, debería estar disponible la opción de ponerlo como privado y solo accesible para aquellos que el usuario permita. Es posible que en algunos servicios sólo quieras borrar cierta información, no el perfil completo. Para estos casos, revisa qué opciones te permite para hacerlo la aplicación o servicio.

En caso de encontrar dificultades en realizar los procesos anteriores, se recomienda utilizar o buscar en las opciones de ayuda y soporte de la propia aplicación o servicio. También se puede buscar en Internet cómo eliminar la cuenta o configurar los niveles de privacidad y seguridad.

En caso de no encontrar una forma de bloquear/eliminar una cuenta o restringirla se recomienda contactar con el responsable o soporte técnico de la aplicación a través de los canales oficiales que ofrezcan de contacto.

Adicionalmente, destacar que las personas también pueden solicitar a los motores de búsqueda que retiren determinados resultados de sus búsquedas a través de los formularios que han puesto a su disposición justificando los motivos por los que desean que se realice esa acción. A continuación, facilitamos algunos de los enlaces de los buscadores más utilizados por los usuarios: Google, Yahoo y Bing.

Además de las redes sociales, buscadores, aplicaciones y servicios web, se recomienda eliminar las cuentas de correo electrónico antiguas y dar de baja las listas de correo o servicios en los que estés suscrito y no utilices o no te interesen para que no te envíen más información.

Por otro lado, borrar las *cookies* almacenadas siguiendo las directrices recogidas en el apartado 2 de este módulo ayudará a reducir tu huella digital. Aunque no sea siempre factible, tienes que tener en cuenta que modificar tanto el número de teléfono como el correo electrónico puede permitir evitar el rastreo de nuestros datos en muchos sitios webs.

Mencionar que cada vez más, existen servicios tanto de pago como gratuitos para ayudar a borrar la huella digital a los usuarios. Por ejemplo, hay aplicaciones que rastrean servicios en los que una dirección electrónica se ha dado de alta y semi-automatizan pasos para eliminar la cuenta.

Alguna de estas aplicaciones, pueden ser *Google Alerts:* recibe notificaciones en función de los parámetros que se haya definido: correo electrónico, teléfono, dni, etc. *Un roll me:* gestiona de manera rápida tus cuentas de correo para que se pongan en orden, teniendo control de lo que llega a la bandeja de entrada. *Have I Been Pwned*: avisa si tu dirección de correo ha sido comprometida por una brecha digital.

También otras webs como '*Just delete me'* ofrecen la dirección exacta de la web en la que un usuario debe dar de baja su cuenta o la suscripción.

Finalmente, indicar que todos los ciudadanos de la Unión Europea están protegidos por la normativa GDPR (Reglamento General de Protección de Datos de la Unión Europea). Esta normativa establece la existencia de derechos básicos de los ciudadanos en la que se encuentra el derecho a supresión (u olvido) que hemos detallado anteriormente. Por tanto, los responsables de la web o aplicación deberán atender la solicitud de borrado de la información y, en caso de no hacerlo, se

recomienda ponerse en contacto con la Agencia de Protección de Datos (https://www.aepd.es/es).

Antes de terminar este apartado, hacer hincapié en que siempre es mejor y menos costoso prevenir que corregir, por tanto, se insiste en el concepto de reflexionar antes de publicar contenido en distintos sitios web, ya que el proceso de eliminación posterior de información, aunque en muchos casos es posible, suele ser complejo para los usuarios.