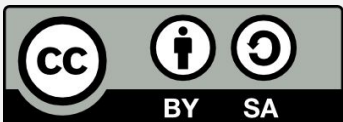


CONFIGURACIÓN: NAVEGACIÓN SEGURA



Esta obra está bajo una [Licencia Creative Commons Atribución-CompartirIgual 4.0 Internacional](https://creativecommons.org/licenses/by-sa/4.0/).

Última actualización: septiembre 2023

ÍNDICE



NAVEGACIÓN SEGURA

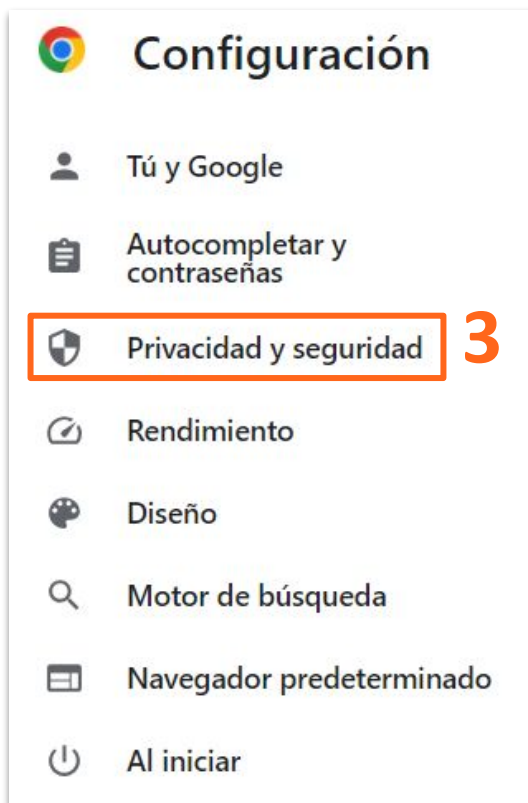
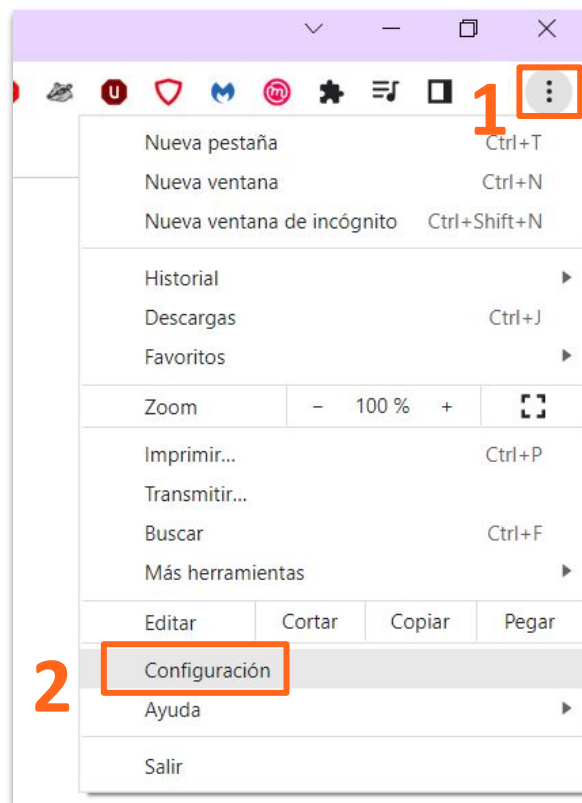
- Configuración Segura: Google Chrome
- Configuración Segura: Mozilla Firefox
- Extensiones de Navegadores:
 - Privacy Badger
 - uBlock Origin
- Seguridad de tu navegador
- Recomendaciones

GOOGLE CHROME



1. Activa la Protección de Seguridad Estándar

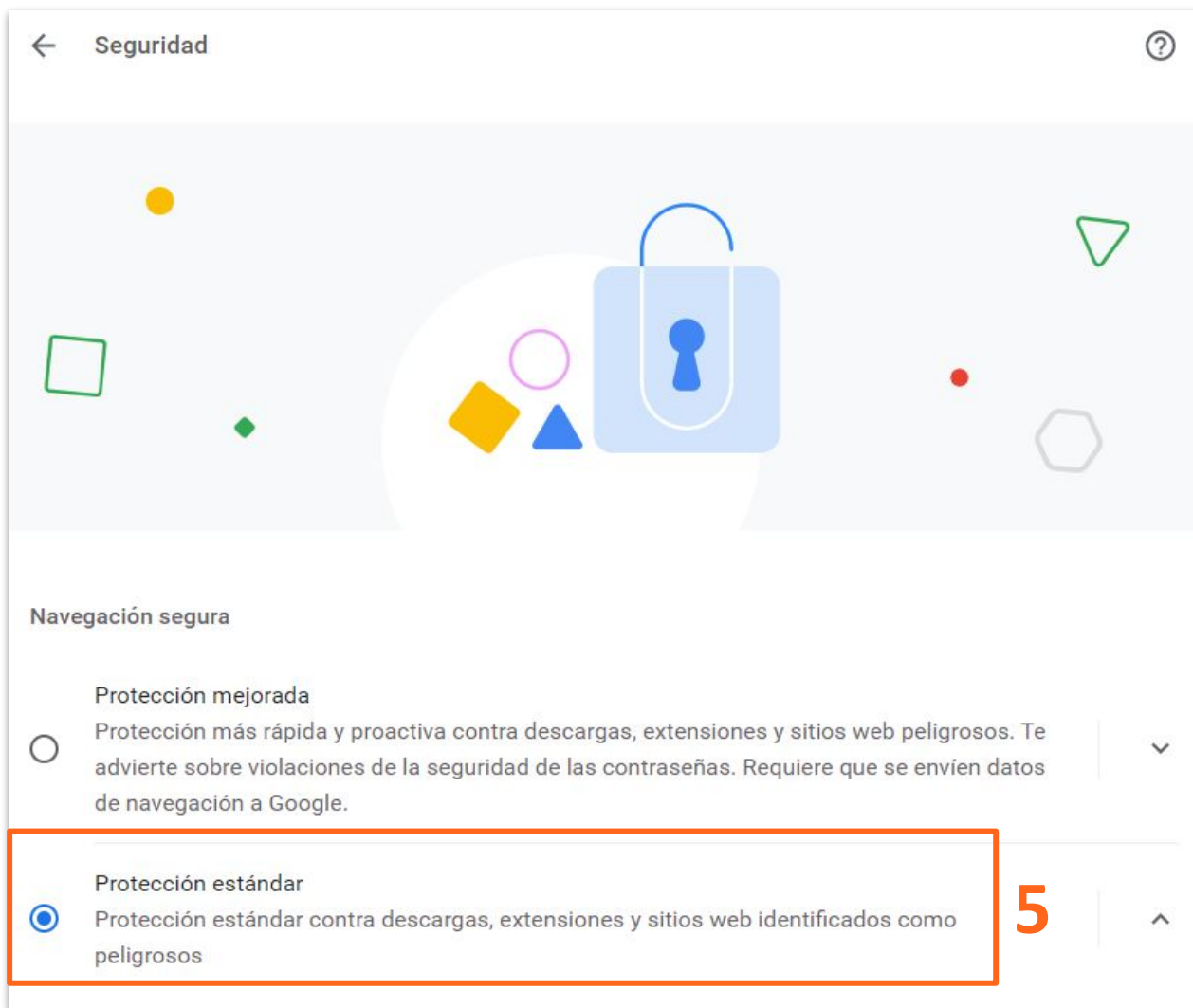
- En la parte superior derecha de tu navegador, haz clic en el menú 
- Selecciona la opción "Configuración". Serás redirigido al panel de configuración de tu navegador
- En el menú lateral izquierdo selecciona "Privacidad y Seguridad"
- Haz clic en "Seguridad"



GOOGLE CHROME



1. Activa la Protección de Seguridad Estándar



→ Revisa que la opción “Protección estándar” esté activada, y evaluar si se quiere usar la protección mejorada.



2. Activa la conexión a sitios seguros con HTTPS

- Ingresa al apartado de "Seguridad" del panel de configuración de tu navegador: (Menú > Configuración > Privacidad y Seguridad > Seguridad)
- En "Configuración avanzada" activa la opción "Usar siempre conexiones seguras"

The screenshot displays the Google Chrome settings interface. On the left, the 'Configuración' (Settings) menu is visible, with 'Privacidad y seguridad' (Privacy and security) highlighted and labeled with a large orange '2'. The main panel shows the 'Configuración avanzada' (Advanced settings) section, which is labeled with a large orange '3'. Within this section, the 'Usar siempre conexiones seguras' (Use secure connections) option is highlighted with an orange box. This option is described as 'Cambia los accesos a páginas al protocolo HTTPS y muestra una advertencia antes de cargar sitios que no sean compatibles con ese protocolo.' and has a toggle switch turned on (blue). Below this, the 'Usar DNS seguro' (Use secure DNS) option is also shown with its toggle switch turned on. The 'Usar DNS seguro' section includes two radio button options: 'Con tu proveedor de servicios actual' (selected) and 'Con Personalizado' (unselected).

Configuración 1

- Tú y Google
- Autocompletar y contraseñas
- Privacidad y seguridad** 2
- Rendimiento
- Diseño
- Motor de búsqueda
- Navegador predeterminado
- Al iniciar

Buscar en configuración

(donde esté disponible) de la Navegación segura en otros servicios de Google, como Gmail y la Búsqueda.

Configuración avanzada 3

Usar siempre conexiones seguras
Cambia los accesos a páginas al protocolo HTTPS y muestra una advertencia antes de cargar sitios que no sean compatibles con ese protocolo. ☒

Usar DNS seguro
Determina cómo conectarse a sitios web mediante una conexión segura ☒

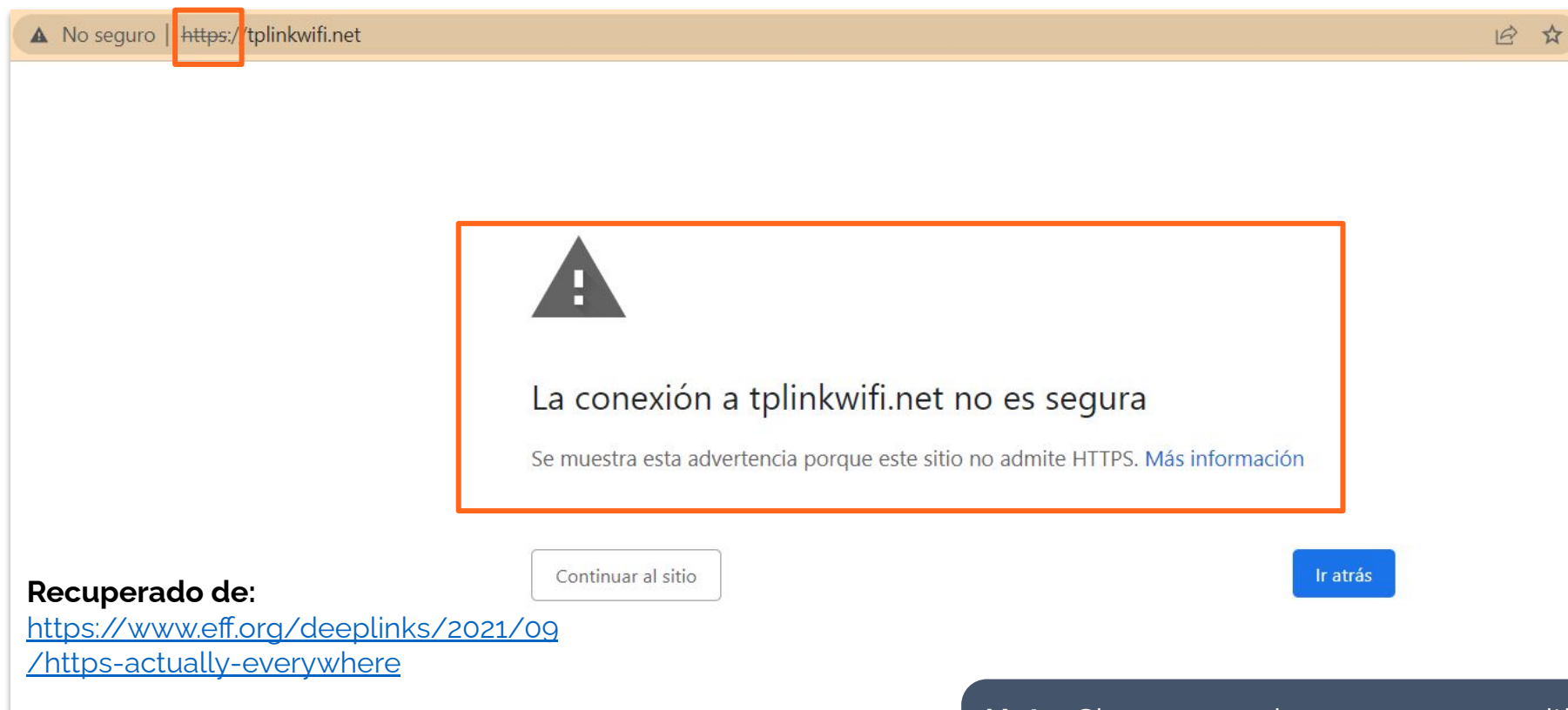
☒ Con tu proveedor de servicios actual
Es posible que el DNS seguro no esté disponible en todo momento

☐ Con Personalizado ▼



2. Activa la conexión a sitios seguros con HTTPS

- Cuando trates de ingresar a una página web que no tenga el protocolo HTTPS, te mostrará una advertencia

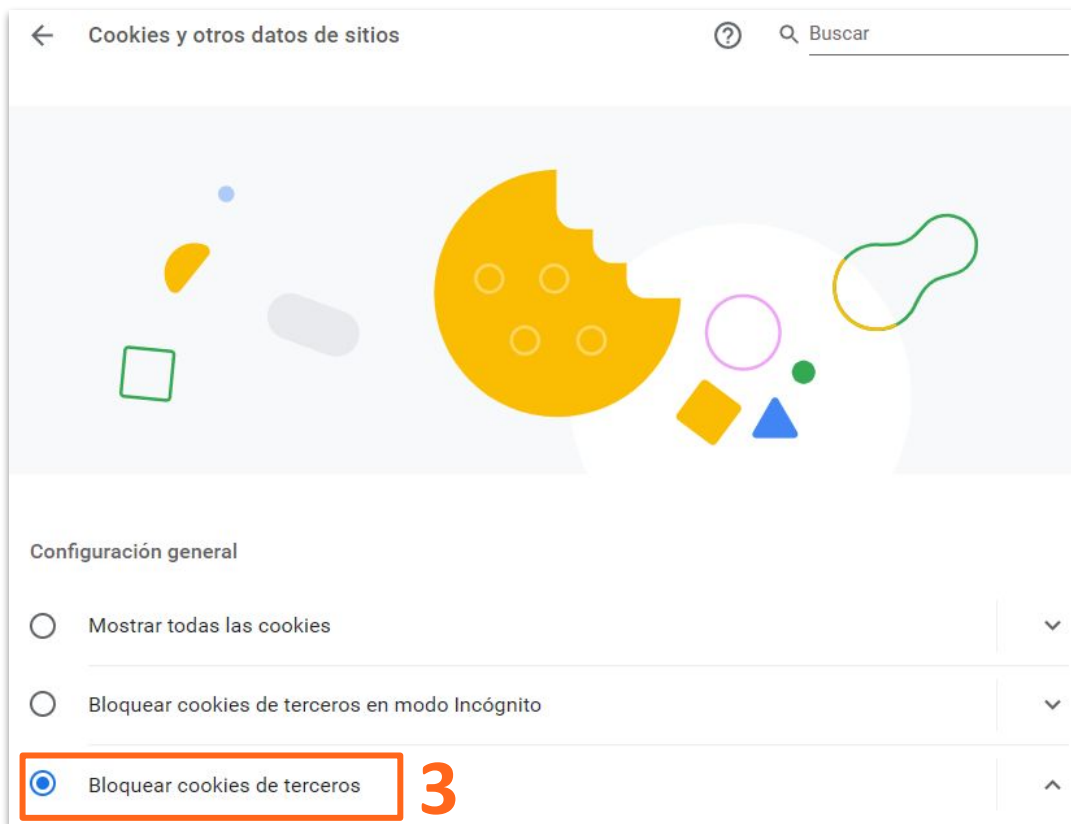
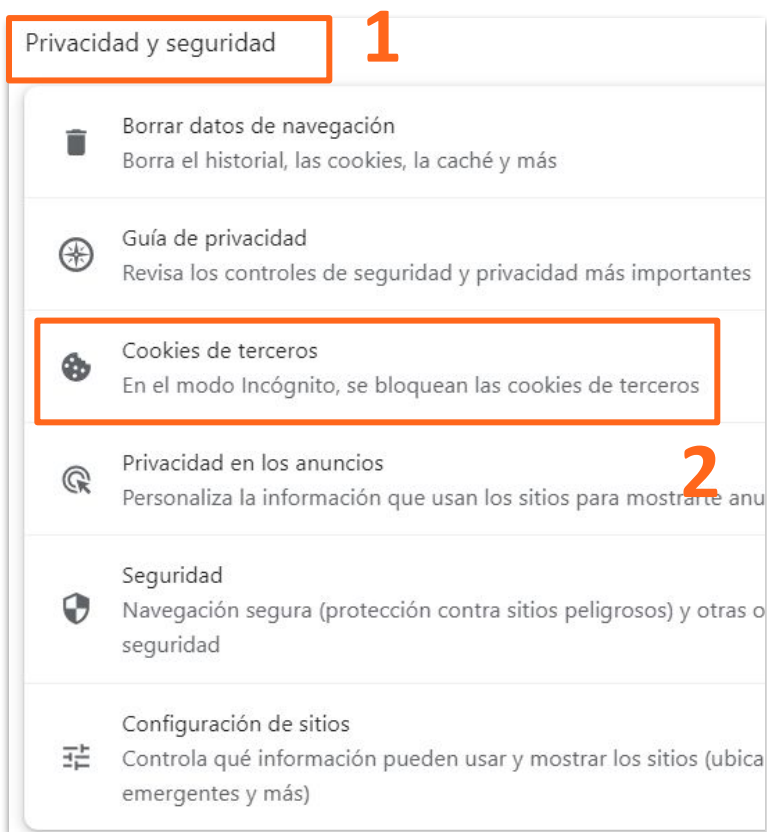


Nota: Si es necesario navegar en un sitio no seguro (sin https), puedes hacer clic en el botón "**Continuar al sitio**", para acceder a él.



3. Bloquea las cookies de terceros

- Ingresa al apartado de "Privacidad y Seguridad" del panel de configuración de tu navegador: (Menú > Configuración > Privacidad y Seguridad)
- Haz clic en "Cookies de terceros"
- Haz clic en la opción "Bloquear cookies de terceros" para activarla





4. Borra los datos de navegación

- Ingresa al apartado de "Privacidad y Seguridad del panel de configuración de tu navegador": (Menú > Configuración > Privacidad y Seguridad)
- Haz clic en "Borrar datos de navegación"
- Selecciona "Todos" en el intervalo de tiempo
- Haz clic en "Borrar datos"

The image displays two screenshots from the Google Chrome settings interface, illustrating the steps to clear browsing data. The first screenshot shows the 'Privacidad y seguridad' (Privacy and security) section, with the 'Borrar datos de navegación' (Clear browsing data) option highlighted by an orange box and the number 1. The second screenshot shows the 'Borrar datos de navegación' (Clear browsing data) dialog box, with the 'Intervalo de tiempo' (Time range) dropdown menu set to 'Todos' (All) highlighted by an orange box and the number 3. The 'Borrar datos' (Clear data) button is highlighted by an orange box and the number 4. The dialog box also shows the 'Básicas' (Basic) tab selected, with options to clear 'Historial de navegación' (Browsing history), 'Cookies y otros datos de sitios' (Cookies and other site data), and 'Imágenes y archivos almacenados en caché' (Cached images and files). A note at the bottom states: 'Es posible que el historial de búsqueda y otras formas de actividad se guarden en tu Cuenta de Google cuando accedes. Podrás borrarlas en cualquier momento.' (It's possible that search history and other forms of activity are saved to your Google Account when you sign in. You can delete them at any time.)

Privacidad y seguridad **1**

2 Borrar datos de navegación
Borra el historial, las cookies, la caché y más

Guía de privacidad
Revisa los controles de seguridad y privacidad más importantes

Cookies de terceros
En el modo Incógnito, se bloquean las cookies de terceros

Privacidad en los anuncios
Personaliza la información que usan los sitios para mostrarte anuncios

Seguridad
Navegación segura (protección contra sitios peligrosos) y otras opciones de seguridad

Configuración de sitios
Controla qué información pueden usar y mostrar los sitios (ubicaciones emergentes y más)

Borrar datos de navegación

Básicas Configuración avanzada

Intervalo de tiempo Todos **3**

☒ Historial de navegación
Borra el historial, incluido el del cuadro de búsqueda.

☒ Cookies y otros datos de sitios
Esta acción te hace salir de la mayoría de los sitios.

☒ Imágenes y archivos almacenados en caché
Esta acción libera hasta 305 MB. Es posible que algunos sitios carguen más lento en tu próxima visita.

Es posible que el [historial de búsqueda](#) y otras formas de actividad se guarden en tu Cuenta de Google cuando accedes. Podrás borrarlas en cualquier momento.

Cancelar **4** Borrar datos

GOOGLE CHROME



5. Borra contraseñas almacenadas

The screenshot shows the 'Clear browsing data' dialog box in Google Chrome. The 'Advanced' tab is selected. The 'Interval of time' is set to 'All time'. The 'Passwords and other sign-in data' and 'Form autofill data' are checked. The 'Clear data' button is highlighted.

1. Borrar datos de navegación

2. Configuración avanzada

3. Intervalo de tiempo

4. Contraseñas y otros datos de acceso
72 contraseñas

5. Borrar datos

- Ingresa al apartado de "Borrar datos de navegación" del panel de configuración de tu navegador:
(Menú > Configuración > Privacidad y Seguridad > Borrar datos de navegación)
- Haz clic "Configuración avanzada"
- Selecciona "Todos" en el intervalo de tiempo
- Selecciona "Contraseñas y otros datos de acceso" y "Datos del formulario de autocompletar"
- Haz clic en Borrar Datos



6. Desactiva la sugerencia de almacenar contraseñas

- Ingresa al apartado de "Autocompletar y contraseñas" del panel de configuración de tu navegador (Menú > Configuración > Autocompletar y contraseñas)
- Haz clic en "Administrador de contraseñas de Google"

The screenshot displays the Google Chrome settings interface. On the left, the 'Configuración' (Settings) menu is open, with 'Privacidad y seguridad' (Privacy and security) highlighted and labeled with a large orange '2'. Above it, the 'Configuración' header is labeled with a large orange '1'. The main panel on the right is titled 'Autocompletar y contraseñas' (Autocomplete and passwords). Within this panel, the 'Administrador de contraseñas de Google' (Google Password Manager) option is highlighted with an orange box. Other visible options include 'Formas de pago' (Payment methods) and 'Direcciones y más' (Addresses and more).



6. Desactiva la sugerencia de almacenar contraseñas

- Haz clic en “Configuración”
- Deshabilita las opciones: “Sugerir que se guarden las contraseñas” y “Acceder automáticamente”

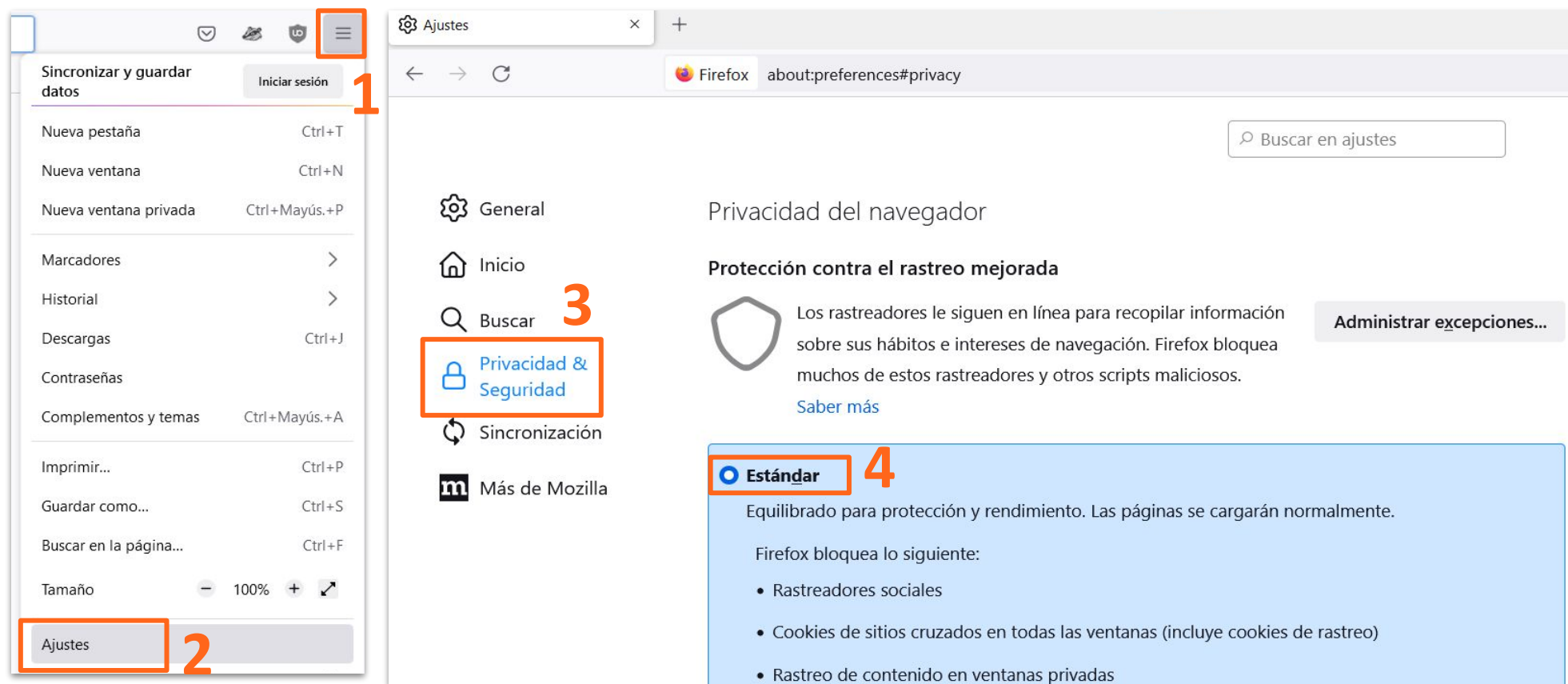


MOZILLA FIREFOX



1. Activa la Protección de Seguridad Estándar

- En la parte superior derecha de tu navegador, haz clic en el Menú ☰
- Haz clic en "Ajustes". Serás redirigido al panel de ajustes de tu navegador.
- Selecciona en el menú lateral izquierdo "Privacidad y Seguridad"
- Verifica que esté activada la Protección del navegador "Estándar"





2. Activa la conexión a sitios seguros con HTTPS

- Ingresa al apartado de "Privacidad y Seguridad" del panel de ajustes de tu navegador: (Menú ☰ > Ajustes > Privacidad y Seguridad)
- En "Modo solo-HTTPS" activa la opción "Activar el modo solo-HTTPS en todas las ventanas"

⚙ General

🏠 Inicio

🔍 Buscar **1**

🔒 Privacidad & Seguridad

🔄 Sincronización

m Más de Mozilla

Modo solo-HTTPS **2**

HTTPS proporciona una conexión segura y cifrada entre Firefox y los sitios web que visita. La mayoría de los sitios web admiten HTTPS, y si el modo solo-HTTPS está habilitado, entonces Firefox actualizará todas las conexiones a HTTPS.

[Más información](#)

☒ Activar el modo solo-HTTPS en todas las ventanas **3**

☐ Activar el modo solo-HTTPS solamente en ventanas privadas

☐ No activar el modo solo-HTTPS

Gestionar excepciones...



MOZILLA FIREFOX

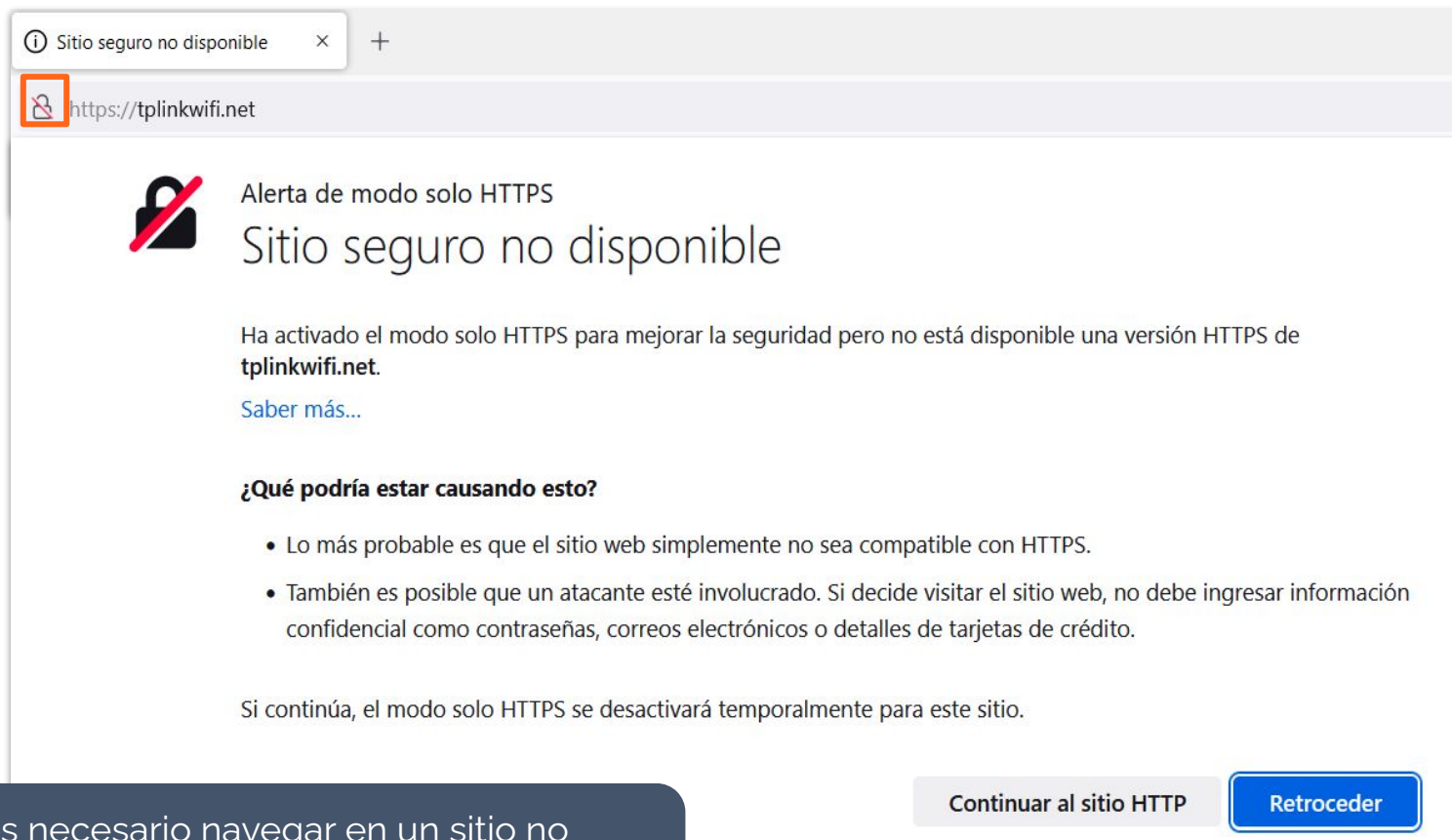
Recuperado de:

<https://www.eff.org/deeplinks/2021/09/https-actually-everywhere>



2. Activa la conexión a sitios seguros con HTTPS

- Cuando trates de ingresar a una página web que no tenga el protocolo HTTPS, te mostrará una advertencia



Nota: Si es necesario navegar en un sitio no seguro (sin https), puedes hacer clic en el botón **"Continuar al sitio HTTP"**, para acceder a él.





3. Borra los datos de navegación y cookies

- Ingresa al apartado de "Privacidad y Seguridad" del panel de ajustes de tu navegador: (Menú ☰ > Ajustes > Privacidad y Seguridad)
- En "Cookies y datos del sitio" habilita la opción "Eliminar cookies y datos del sitio cuando cierre Firefox"
- Haz clic en "Limpiar datos" > "Limpiar" para eliminar las cookies y datos almacenados hasta el momento,

The screenshot shows the Firefox settings interface with five numbered steps indicating the process to clear cookies and site data:

- 1** Click on "Privacidad & Seguridad" (Privacy & Security) in the left sidebar.
- 2** Click on "Cookies y datos del sitio" (Cookies and Site Data).
- 3** Check the box for "Eliminar cookies y datos del sitio cuando cierre Firefox" (Delete cookies and site data when Firefox closes).
- 4** Click on "Limpiar datos..." (Clear Data...).
- 5** In the "Limpiar datos" (Clear Data) dialog, check "Cookies y datos del sitio (48.7 KB)" and "Contenido web en caché (56.3 MB)", then click "Limpiar" (Clear).

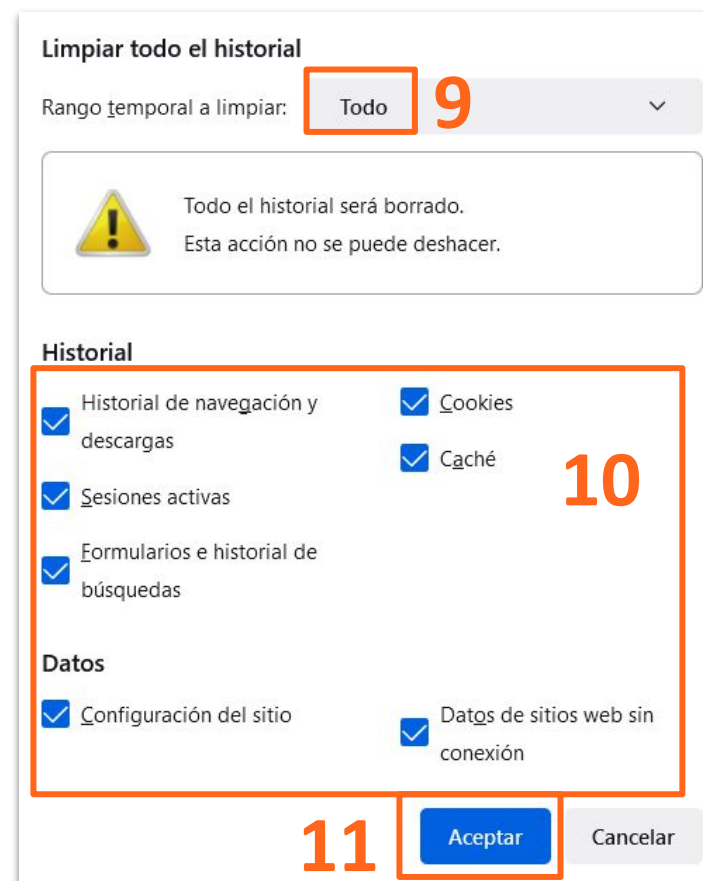
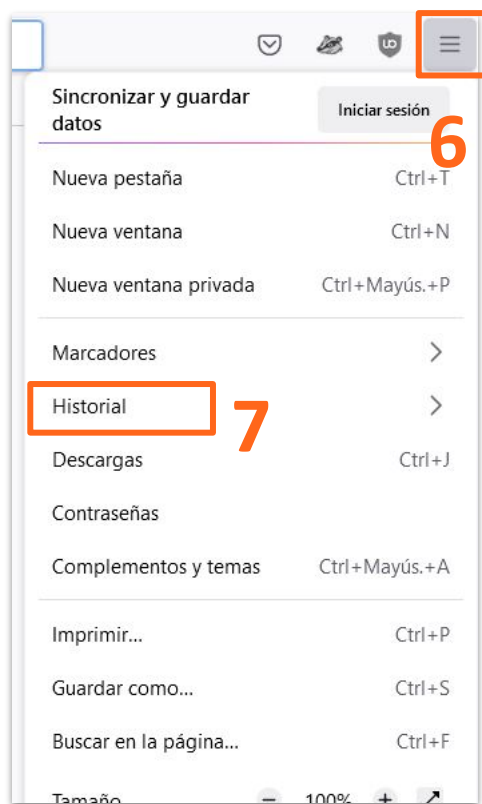
The "Limpiar datos" dialog includes the following text: "Limpiar todas las cookies y datos del sitio guardados por Firefox puede desconectarle de los sitios web y eliminar el contenido web sin conexión. Limpiar los datos del caché no afectará a sus sesiones." (Clearing all cookies and site data saved by Firefox can disconnect you from websites and remove offline web content. Clearing cache data will not affect your sessions.)

Item	Size	Description
☒ Cookies y datos del sitio	48.7 KB	Puede ser desconectado de los sitios web si se borran las cookies
☒ Contenido web en caché	56.3 MB	Requerirá que los sitios web recarguen las imágenes y datos



3. Borra los datos de navegación y cookies

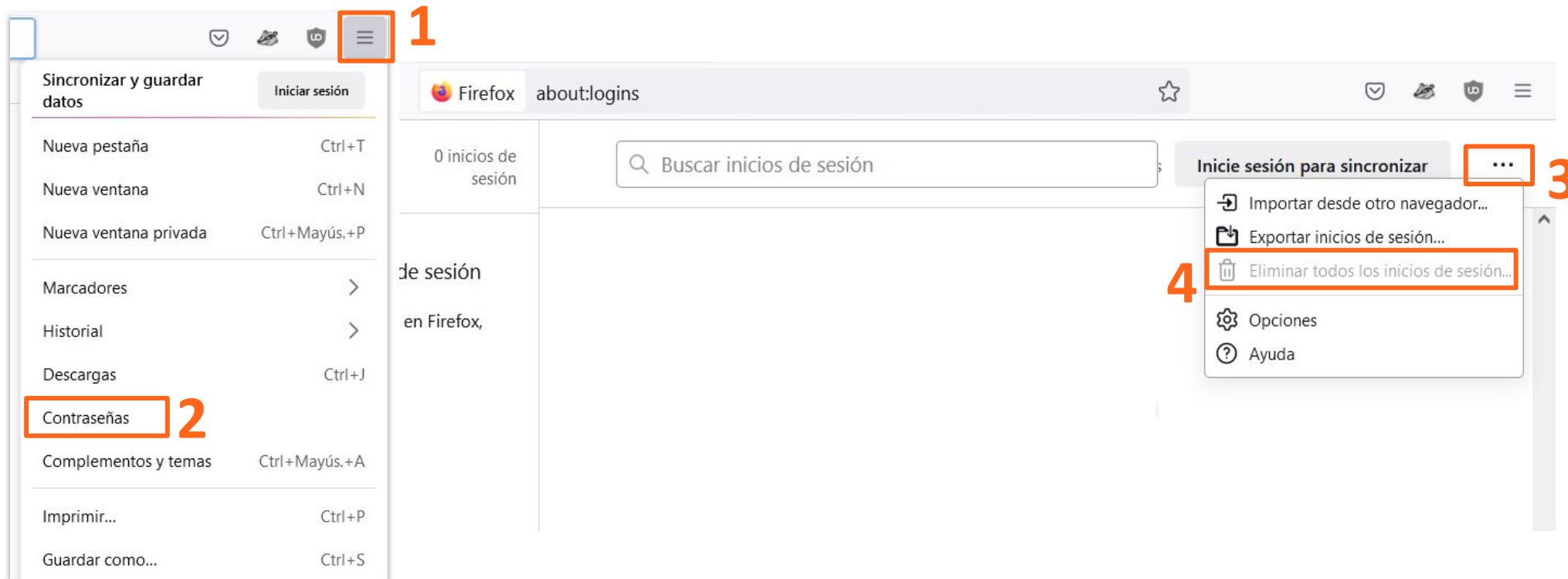
- Ingresa al "Historial" de tu navegador: (Menú ☰ > Historial)
- Haz clic en "Limpiar el historial reciente"
- Selecciona "Todo" en el rango temporal a limpiar
- Selecciona lo que vas a eliminar
- Haz clic en "Aceptar"





4. Borra contraseñas almacenadas

- Ingresa al apartado de "Contraseñas" de tu navegador: (Menú ☰ > Contraseñas)
- Se abrirá el administrador de "Inicio de Sesión y Contraseñas" de Firefox.
- En el menú de ajustes haz clic en "Eliminar todos los inicios de sesión"





5. Desactiva la sugerencia de almacenar contraseñas

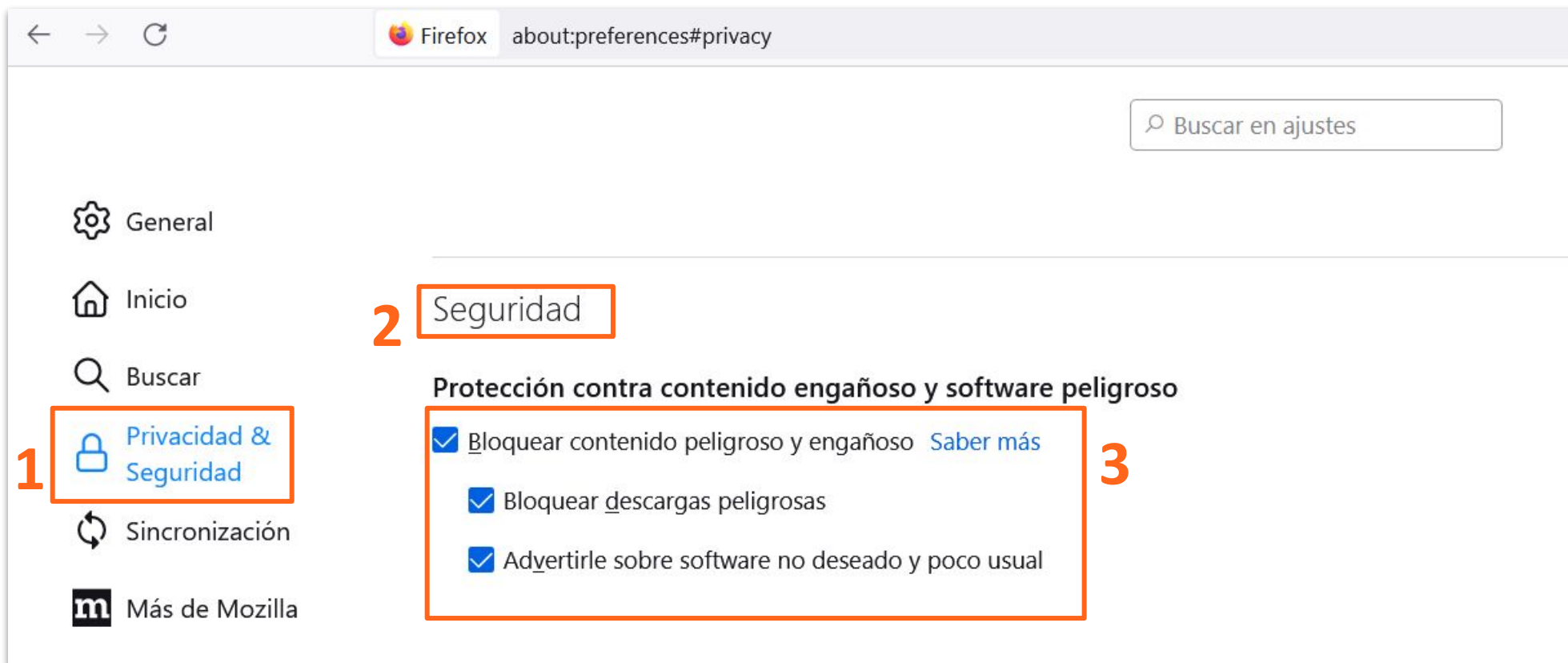
- Ingresa al apartado de "Privacidad y Seguridad" del panel de ajustes de tu navegador: (Menú ☰ > Ajustes > Privacidad y Seguridad)
- En "Usuarios y contraseñas" desactiva la opción "Preguntar para guardar contraseñas e inicios de sesión de sitios web"





6. Activa la Protección contra contenido engañoso y software peligroso

- Ingresa al apartado de "Privacidad y Seguridad" del panel de ajustes de tu navegador: (Menú ☰ > Ajustes > Privacidad y Seguridad)
- En "Seguridad" verifica que estén habilitadas todas las opciones



MOZILLA FIREFOX



Total Cookie Protection

Firefox está implementando **Total Cookie Protection** de forma predeterminada para todos los usuarios de Firefox en todo el mundo, lo que convierte a **Firefox en el navegador más privado y seguro disponible en Windows, Mac y Linux.**

Total Cookie Protection es la protección de privacidad más sólida de Firefox hasta la fecha, ofrece fuertes protecciones contra el seguimiento sin afectar la experiencia de navegación.



Total Cookie Protection funciona mediante la creación de un **"tarro de cookies"** asignado para cada sitio web que visites.

En lugar de permitir que los rastreadores vinculen tu comportamiento en varios sitios, solo pueden ver el comportamiento en sitios individuales.

Recuperado de:

<https://blog.mozilla.org/en/products/firefox/firefox-rolls-out-total-cookie-protection-by-default-to-all-users-worldwide/>



Privacidad de los datos - Google Chrome vs. Mozilla Firefox



Buscar

ABRIR



Datos asociados con tu identidad
Los siguientes datos pueden recopilarse y asociarse con tu identidad:

 Información financiera

 Ubicación

 Información de contacto

 Contactos

 Contenido de usuario

 Historial de búsqueda

 Historial de navegación

 Identificadores

 Datos de uso

 Diagnóstico

 Otros datos



Datos no asociados con tu identidad
Los siguientes datos pueden recopilarse, pero no están asociados con tu identidad:

 Contenido de usuario

 Diagnóstico



Buscar

OBTENER

Privacidad de la app [Ver detalles](#)

El desarrollador (Mozilla) indicó que las prácticas de privacidad de la app pueden incluir el manejo de datos que se describe a continuación. Para obtener más detalles, consulta la [política de privacidad del desarrollador](#).



Datos asociados con tu identidad
Los siguientes datos pueden recopilarse y asociarse con tu identidad:

 Información de contacto

 Identificadores

 Datos de uso



Datos no asociados con tu identidad
Los siguientes datos pueden recopilarse, pero no están asociados con tu identidad:

 Ubicación

 Datos de uso

 Diagnóstico

Esta comparativa demuestra como Google Chrome recopila más datos que pueden asociarse a tu identidad, que Mozilla Firefox.

En temas de privacidad de datos, ésta es una de las razones por las cuales recomendamos el uso de Mozilla Firefox como navegador seguro

EXTENSIÓN: Privacy Badger



Instalación en Google Chrome

- Ingresa a <https://privacybadger.org/>
- Haz clic en "Agregar a Chrome"
- Serás dirigido a la Chrome web store. Haz clic en "Add to Chrome"
- Habilita los permisos haciendo clic en "Agregar extensión"

EFF Sobre Temas Nuestro trabajo Póngase en acción Herramientas

Privacy Badger

Idioma: Español

Privacy Badger es una extensión de navegador que aprende automáticamente a bloquear rastreadores invisibles.

Agregar a Chrome 1

Agregar a Firefox Agregar a Firefox para Android Agregar a Edge Agregar a Opera

Home > Extensions > Privacy Badger

Privacy Badger

www.eff.org Featured

★★★★★ 1,677 | Productivity | 1,000,000+ users

2 Add to Chrome

Overview Privacy practices Reviews Support Related

¿Quieres instalar "Privacy Badger"?

Puede:

- Leer y cambiar todos tus datos en todos los sitios web
- Cambiar la configuración relacionada con la privacidad

3 Agregar extensión Cancelar

EXTENSIÓN: Privacy Badger



Instalación en Google Chrome

- Espera que se descargue. Serás dirigido a una ventana cuando culmine el proceso
- Fija la extensión como acceso directo

EFF UN PROYECTO DE LA ELECTRONIC FRONTIER FOUNDATION

Privacy Badger

¡Gracias por instalar Privacy Badger!

Privacy Badger aprende automáticamente a bloquear rastreadores invisibles. Tómate un minuto para ver cómo lo hace.

HACER EL RECORRIDO

Extensiones

No se necesita acceso
Estas extensiones no necesitan ver ni cambiar información en este sitio.

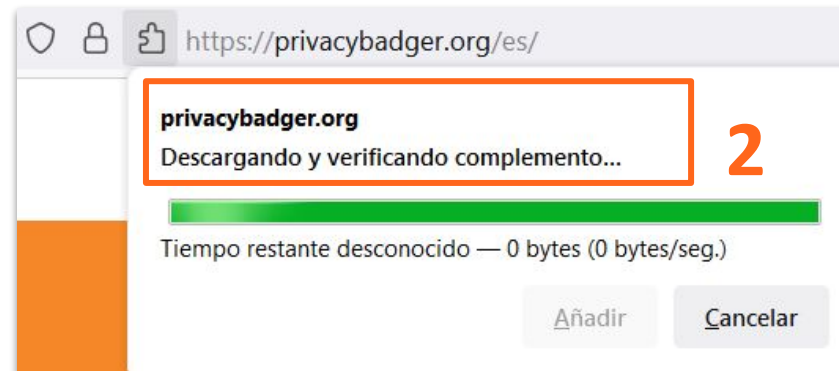
- 1Password – Gestor de contras...
- ClickUp: Tasks, Screenshots, Em...
- Mailvelope
- Privacy Badger
- uBlock Origin
- Administrar extensiones

EXTENSIÓN: Privacy Badger



Instalación en Mozilla Firefox

- Ingresa a <https://privacybadger.org/>
- Haz clic en "Agregar a Firefox"
- Espera a que se descargue
- Haz clic en "Añadir"



EXTENSIÓN: Privacy Badger



Instalación en Mozilla Firefox

→ Habilita los permisos para mantenerla en la barra de tareas y haz clic en aceptar

Extensión (Privacy Badger) moz-extension://b6130535-07dc-464d-98ff-100ff4f10929/skin/firstRun.html

EFF UN PROYECTO DE LA ELECTRONIC FRONTIER FOUNDATION

Privacy Badger

¡Gracias por instalar Privacy Badger!

Privacy Badger aprende automáticamente a bloquear rastreadores invisibles. Tómame un minuto para ver cómo lo hace.

HACER EL RECORRIDO

Se ha añadido Privacy Badger
Administre sus complementos y temas desde el menú de la aplicación.

☐ Permitir que esta extensión se ejecute en ventanas privadas

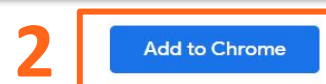
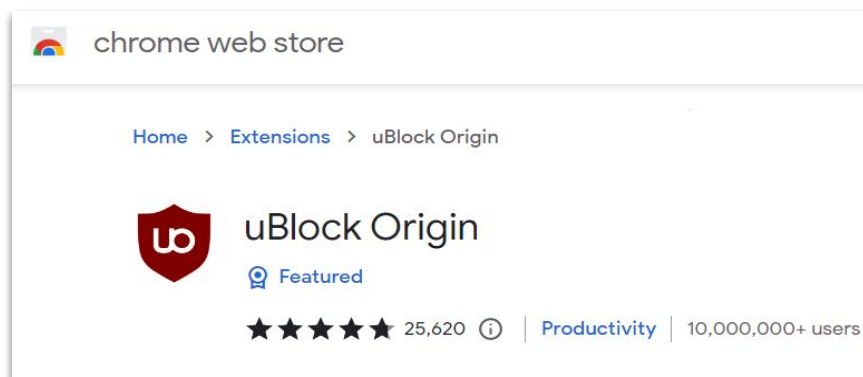
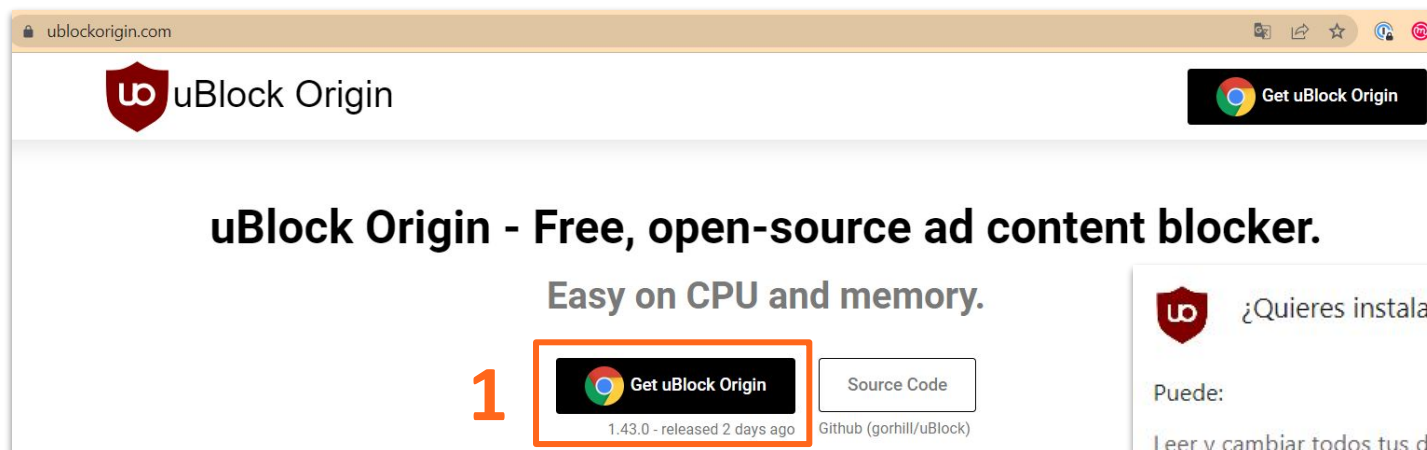
Aceptar

EXTENSIÓN: uBlock Origin



Instalación en Google Chrome

- Ingresa a <https://github.com/gorhill/uBlock#ublock-origin>
- Haz clic en "Get uBlock Origin"
- Serás dirigido a la Chrome web store. Haz clic en "Add to Chrome"
- Habilita los permisos haciendo clic en "Agregar extensión"



EXTENSIÓN: uBlock Origin



Instalación en Google Chrome

- Espera a que se descargue, serás notificado cuando haya culminado la instalación
- Fija la extensión como acceso directo

The screenshot shows a Google Chrome browser window with the address bar displaying 'ublockorigin.com'. The main content area shows the uBlock Origin website with the heading 'uBlock Origin - Free, open-source ad content b' and 'Easy on CPU and memory.' Below this, there are two buttons: 'Get uBlock Origin' and 'Source Code'. The 'Get uBlock Origin' button is highlighted with a red box and the number 4. A notification bubble is visible in the bottom left corner with the text 'Se agregó uBlock Origin a Chrome' and a red box around it with the number 4. On the right side, the Chrome extension menu is open, showing a list of installed extensions. The 'uBlock Origin' extension is highlighted with a red box and the number 6. The menu is titled 'Extensiones' and lists several extensions, including '1Password - Gestor de contras...', 'ClickUp: Tasks, Screenshots, Em...', 'Mailvelope', 'Privacy Badger', and 'uBlock Origin'. The 'uBlock Origin' extension is the last one in the list, and its icon is highlighted with a red box and the number 6. The menu also includes an option 'Administrar extensiones' at the bottom.

EXTENSIÓN: uBlock Origin



Instalación en Mozilla Firefox

- Ingresa a <https://github.com/gorhill/uBlock#ublock-origin>
- Haz clic en "Obtener uBlock Origin"
- Serás dirigido a la Firefox Browser ADD-ONS. Haz clic en "Add to Firefox"
- Espera a que se descargue y Haz clic en "Añadir"

The screenshot shows the uBlock Origin website and the Firefox Add-ons page. The website has a header with the uBlock Origin logo and a button labeled "Obtener uBlock Origin". The main content area says "uBlock Origin - Bloqueador de contenido publicitario gratis, de código abierto" and "Bajo consumo de memoria y CPU." Below this is a button labeled "Obtener uBlock Origin" with the version "1.43.0 - lanzado hace 10 días". The Firefox Add-ons page shows the "uBlock Origin by Raymond Hill" extension. It has a "Recommended" badge and a button labeled "Add to Firefox".

1. **Obtener uBlock Origin** (1.43.0 - lanzado hace 10 días)

2. **Add to Firefox**

3. **Añadir**

¿Añadir uBlock Origin? Esta extensión tendrá permiso para:

- Acceder a sus datos de todos los sitios web
- Leer y modificar configuración de privacidad
- Acceder a las pestañas del navegador
- Acceder a la actividad del navegador durante la navegación

[Saber más](#)

EXTENSIÓN: uBlock Origin



Instalación en Mozilla Firefox

→ Habilita los permisos para mantenerla en la barra de tareas y haz clic en aceptar

Firefox Browser
ADD-ONS Extensions Themes More... v

Firefox Add-ons Blog Extension

Se ha añadido uBlock Origin
Administre sus complementos y temas desde el menú de la aplicación.

☒ Permitir que esta extensión se ejecute en ventanas privadas

4 5 Aceptar

uBlock Origin
by Raymond Hill

Finally, an efficient wide-spectrum content blocker. Easy on CPU and memory.

Remove

Recommended

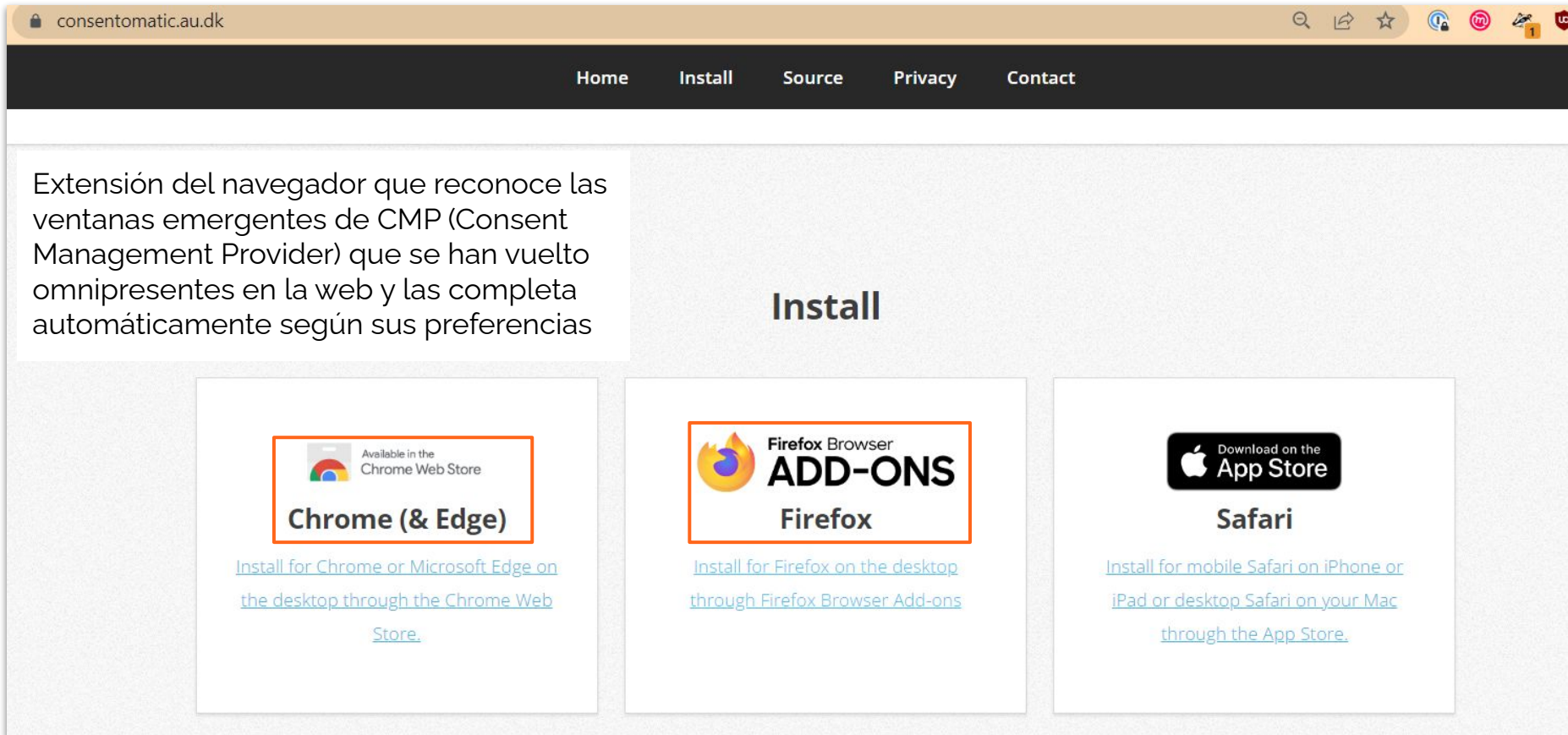
5,465,516 Users 13,744 Reviews 4.8 Stars

Stars	Count
5 ★	12,039
4 ★	1,005
3 ★	278
2 ★	141
1 ★	281

EXTENSIÓN: Conset O-Matic

Instalación

- Ingresa a <https://consentomatic.au.dk/>
- Selecciona la versión de tu navegador
- Habilita los permisos, instala la extensión y fíjala en tu barra de tareas del navegador



The screenshot shows the website consentomatic.au.dk with a navigation bar containing links: Home, Install, Source, Privacy, and Contact. A text box on the left describes the extension: "Extensión del navegador que reconoce las ventanas emergentes de CMP (Consent Management Provider) que se han vuelto omnipresentes en la web y las completa automáticamente según sus preferencias". The main section is titled "Install" and features three installation options:

- Chrome (& Edge)**: Available in the Chrome Web Store. Link: [Install for Chrome or Microsoft Edge on the desktop through the Chrome Web Store.](#)
- Firefox**: Firefox Browser ADD-ONS. Link: [Install for Firefox on the desktop through Firefox Browser Add-ons](#)
- Safari**: Download on the App Store. Link: [Install for mobile Safari on iPhone or iPad or desktop Safari on your Mac through the App Store.](#)

EXTENSIONES



Revisar Administrador de Extensiones (Chrome)

Te recomendamos que accedas al Administrador de extensiones de tu navegador y valides que las instaladas, fueron autorizadas por ti. Recientemente se han realizado investigaciones sobre extensiones que se instalan en tu navegador sin consentimiento y acceden a toda tu información de navegación

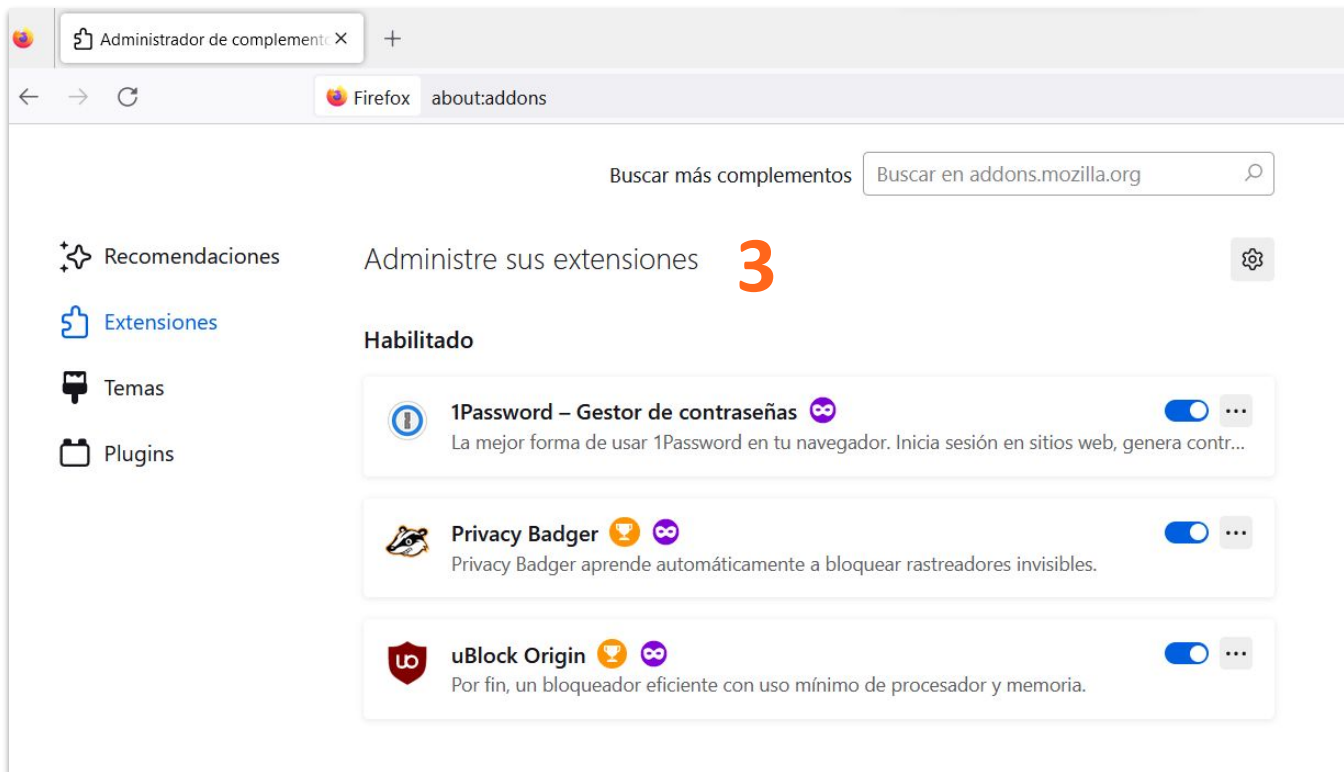
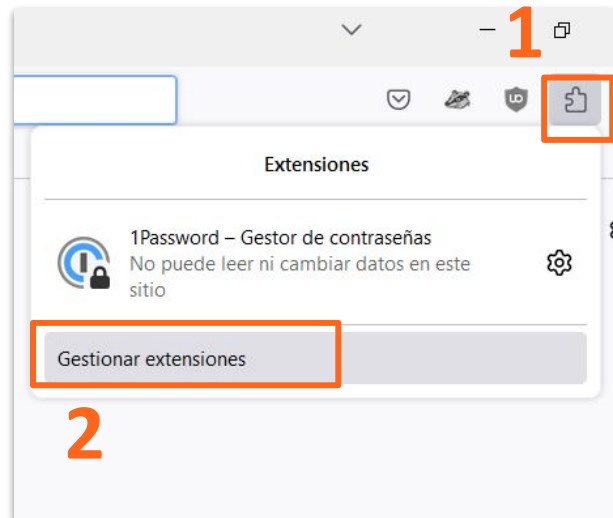
The image shows two screenshots of the Chrome browser interface. The left screenshot shows the Chrome toolbar with the puzzle piece icon highlighted by a red box and the number '1'. Below the toolbar, the 'Extensiones' sidebar is open, showing a list of installed extensions. At the bottom of this sidebar, the 'Administrar extensiones' button is highlighted by a red box and the number '2'. The right screenshot shows the 'chrome://extensions' page. The address bar shows 'chrome://extensions' and the page title is 'Extensiones', which is highlighted by a red box and the number '3'. The page displays a grid of extension cards, each with a toggle switch to enable or disable the extension. The extensions listed include 1Password, Bitwarden, Mailvelope, Office, Privacy Badger, uBlock Origin, Documentos de Google, and Selector de aplicaciones para Drive.

EXTENSIONES



Revisar Administrador de Extensiones (Firefox)

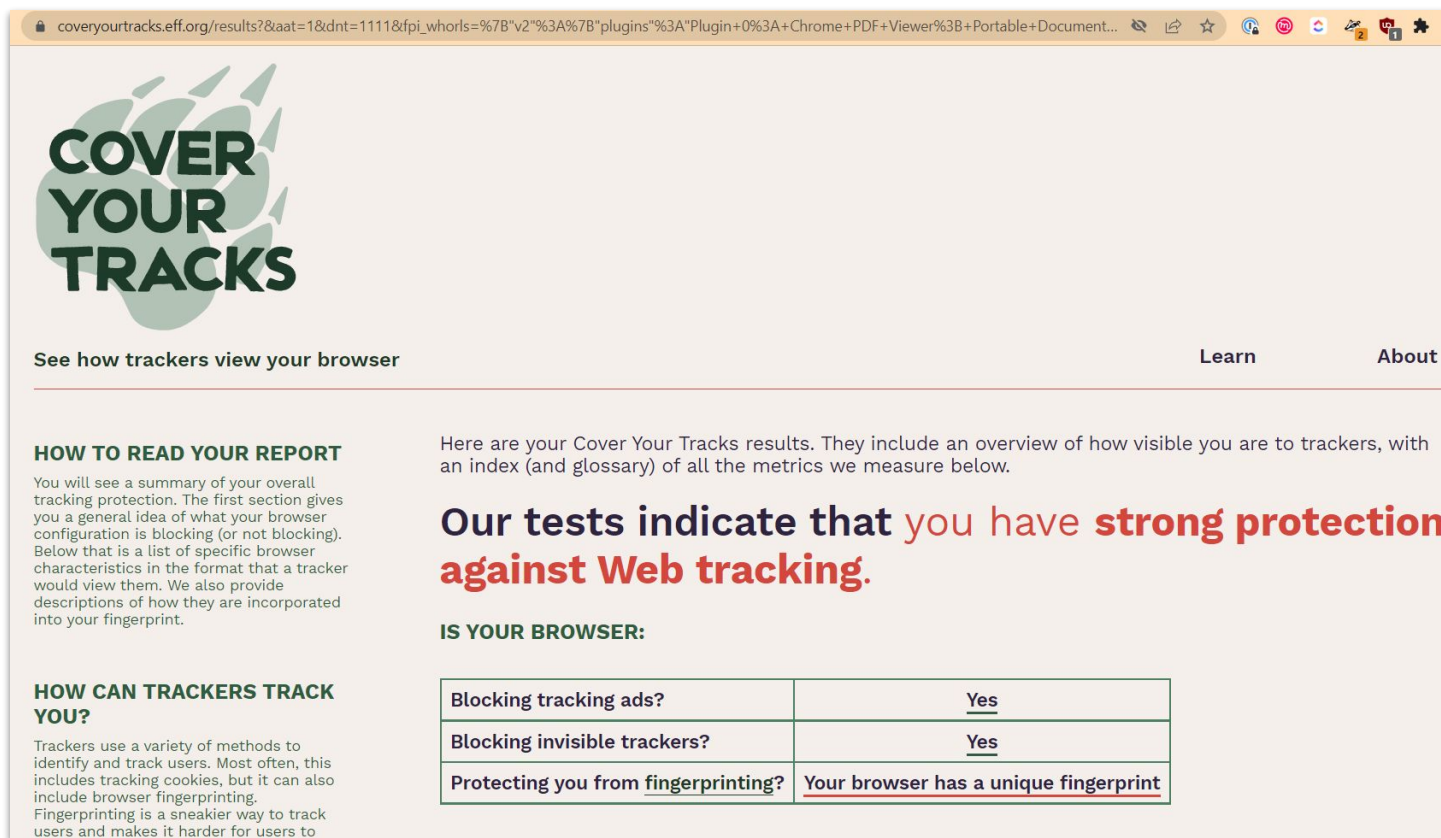
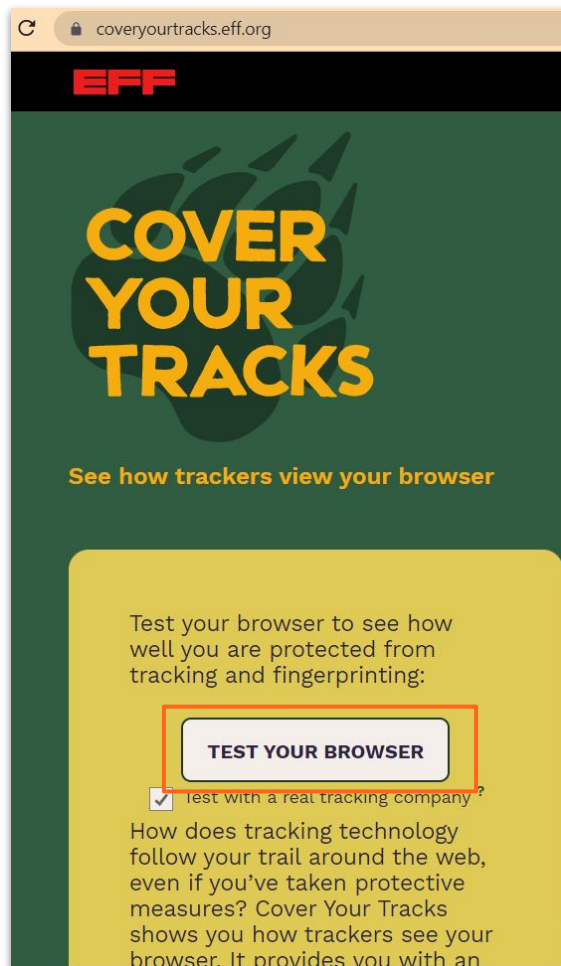
Te recomendamos que accedas al Administrador de extensiones de tu navegador y validez que las instaladas, fueron autorizadas por ti. Recientemente se han realizado investigaciones sobre extensiones que se instalan en tu navegador sin consentimiento y acceden a toda tu información de navegación



SEGURIDAD DE TU NAVEGADOR

Revisión del estado de seguridad de tu navegador

- Ingresa a <https://coveryourtracks.eff.org/>
- Haz clic en "Test your Browser"
- Espera los resultados
- Evalúa las próximas acciones de acuerdo al reporte



Here are your Cover Your Tracks results. They include an overview of how visible you are to trackers, with an index (and glossary) of all the metrics we measure below.

Our tests indicate that you have strong protection against Web tracking.

IS YOUR BROWSER:

Blocking tracking ads?	Yes
Blocking invisible trackers?	Yes
Protecting you from fingerprinting?	Your browser has a unique fingerprint



RECOMENDACIONES



Recomendaciones

Mejores prácticas para una navegación segura:

- Mantén tu navegador actualizado.
- Activa la protección de seguridad estándar.
- Activa la conexión a sitios seguros que tengan el protocolo HTTPS.
- Utiliza bloqueadores de anuncios y de rastreadores como uBlock Origin y Privacy Badger.
- Bloquea las cookies de terceros.
- Borra regularmente tus datos de navegación (historial de navegación, cookies y caché).
- No almacenes contraseñas o inicios de sesión en tu navegador; Utiliza un administrador de contraseñas seguro como 1Password, Bitwarden o LastPass.
- Revisa el estado de privacidad de tu navegador con <https://coveryourtracks.eff.org/>.
- Descarga y activa sólo las extensiones o complementos de navegador que sean necesarias y revisa que estén actualizadas (Cuida tu huella de navegación).
- Utiliza extensiones exclusivamente de desarrolladores verificados.
- Utiliza aplicaciones de VPN para acceder a sitios que se encuentren bloqueados o censurados y para que tu proveedor de servicios de internet no pueda conocer las páginas web que visitas.

