CONFIGURACIÓN: NAVEGACIÓN SEGURA

CONEXO

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

Última actualización: Septiembre 2023

ÍNDICE

NAVEGACIÓN SEGURA

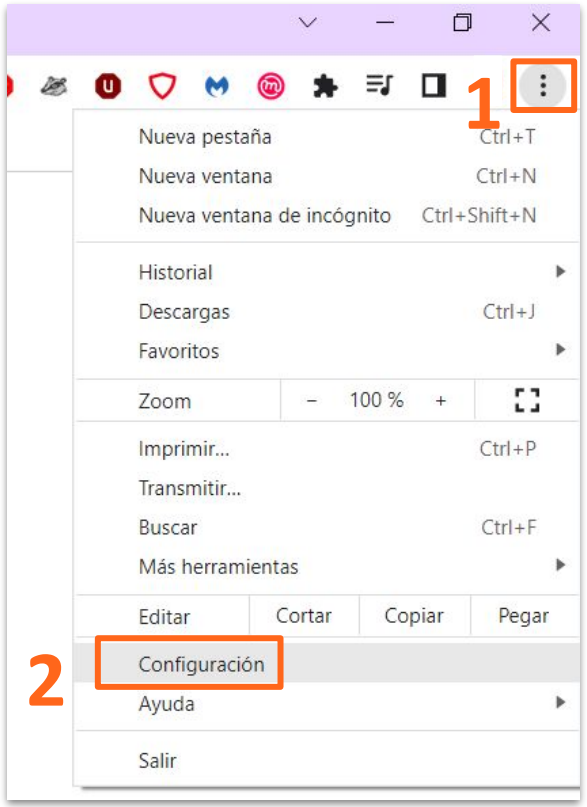
- Configuración Segura: Google Chrome
- Configuración Segura: Mozilla Firefox
- Extensiones de Navegadores:
  - Privacy Badger
  - uBlock Origin
- Seguridad de tu navegador
- Recomendaciones

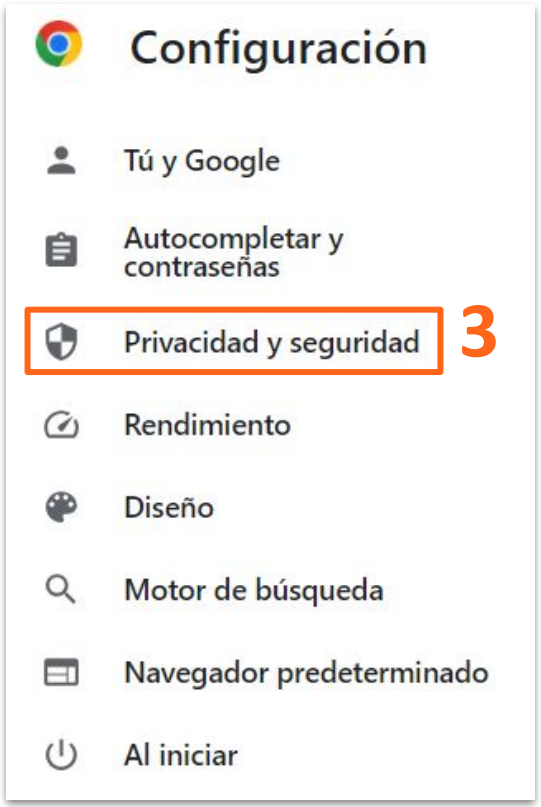
CONEXO

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”

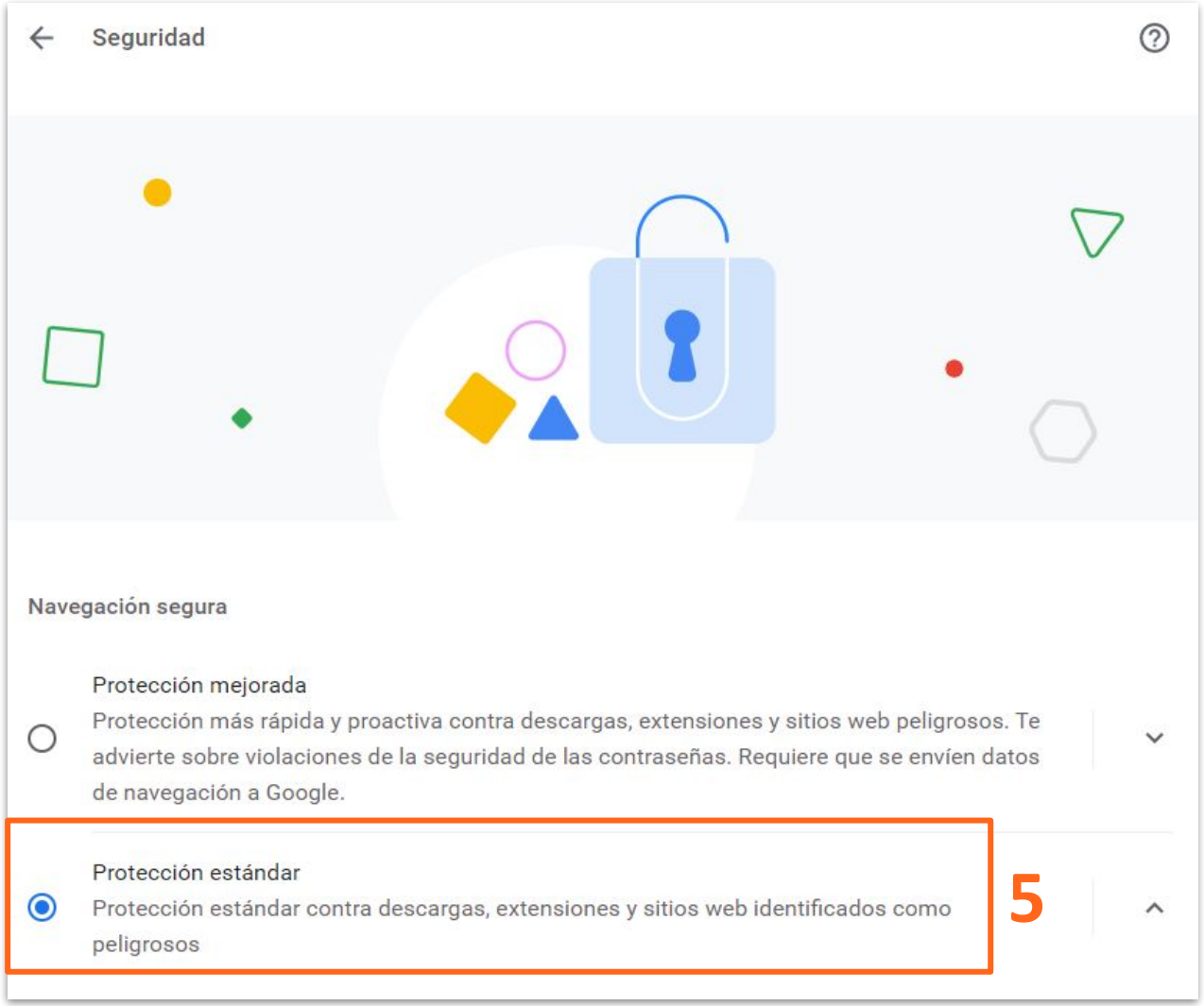






GOOGLE CHROME

1. Activa la Protección de Seguridad Estándar

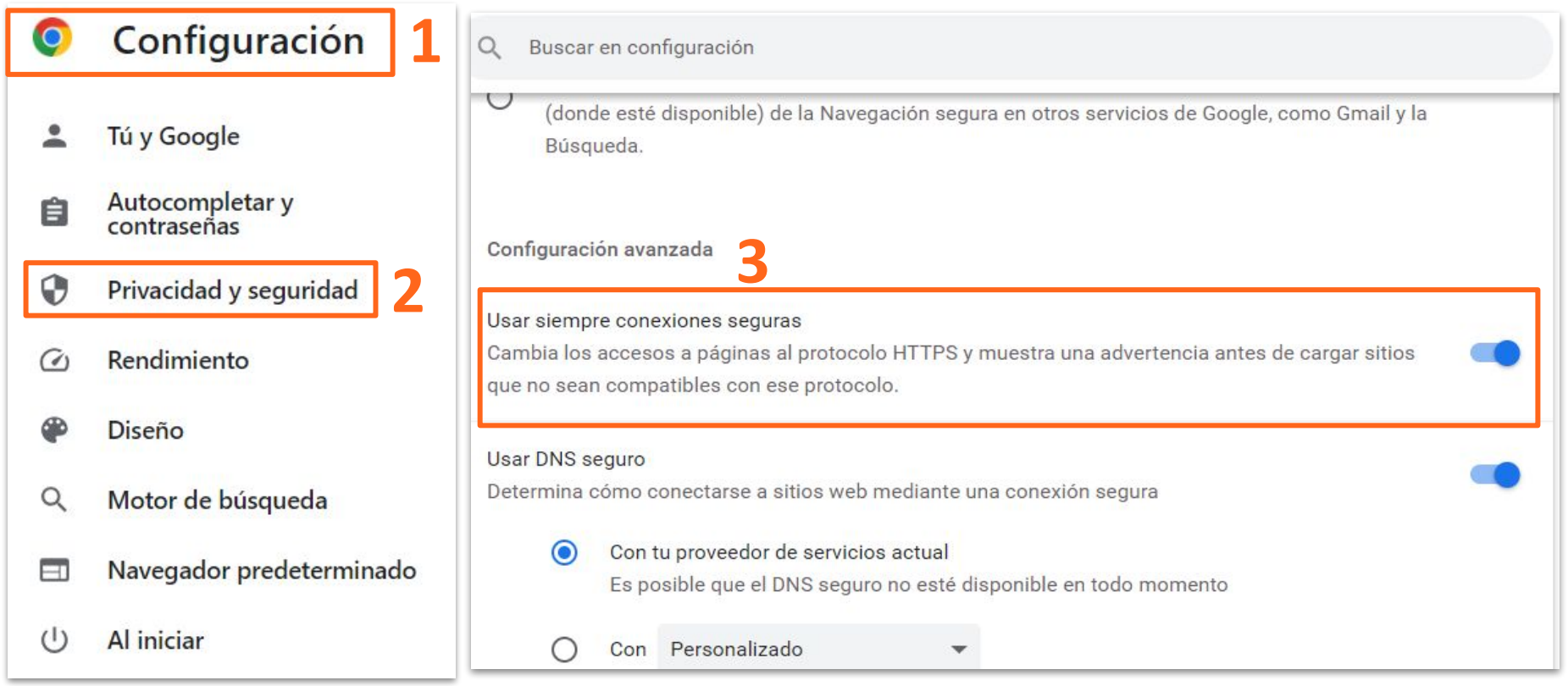


➔ Revisa que la opción “Protección estándar” esté activada, y evaluar si se quiere usar la protección mejorada.

GOOGLE CHROME

2. Activa la conexión a sitios seguros con HTTPS

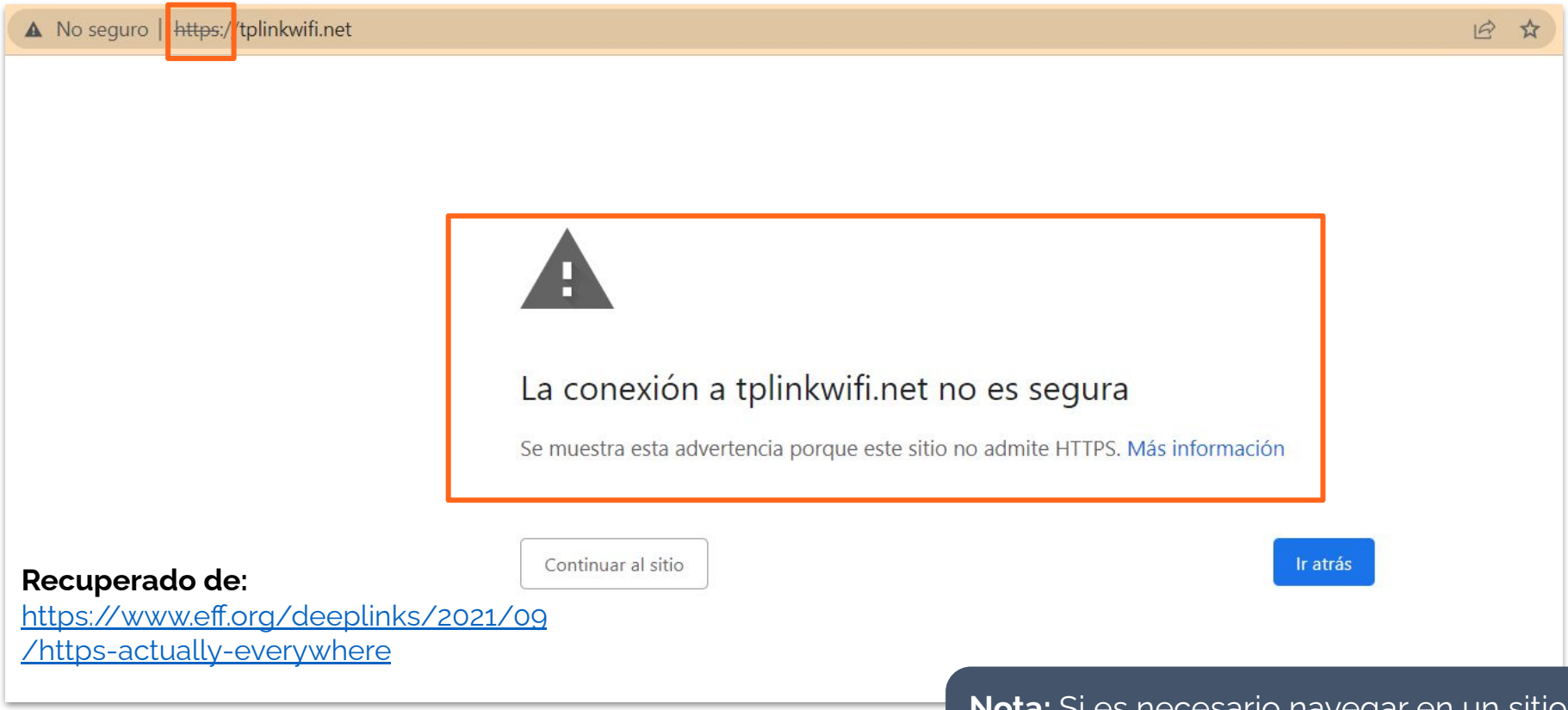
- ➔ Ingresa al apartado de “Seguridad” del panel de configuración de tu navegador: (Menú > Configuración > Privacidad y Seguridad > Seguridad)
- ➔ En “Configuración avanzada” activa la opción “Usar siempre conexiones seguras”



GOOGLE CHROME

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



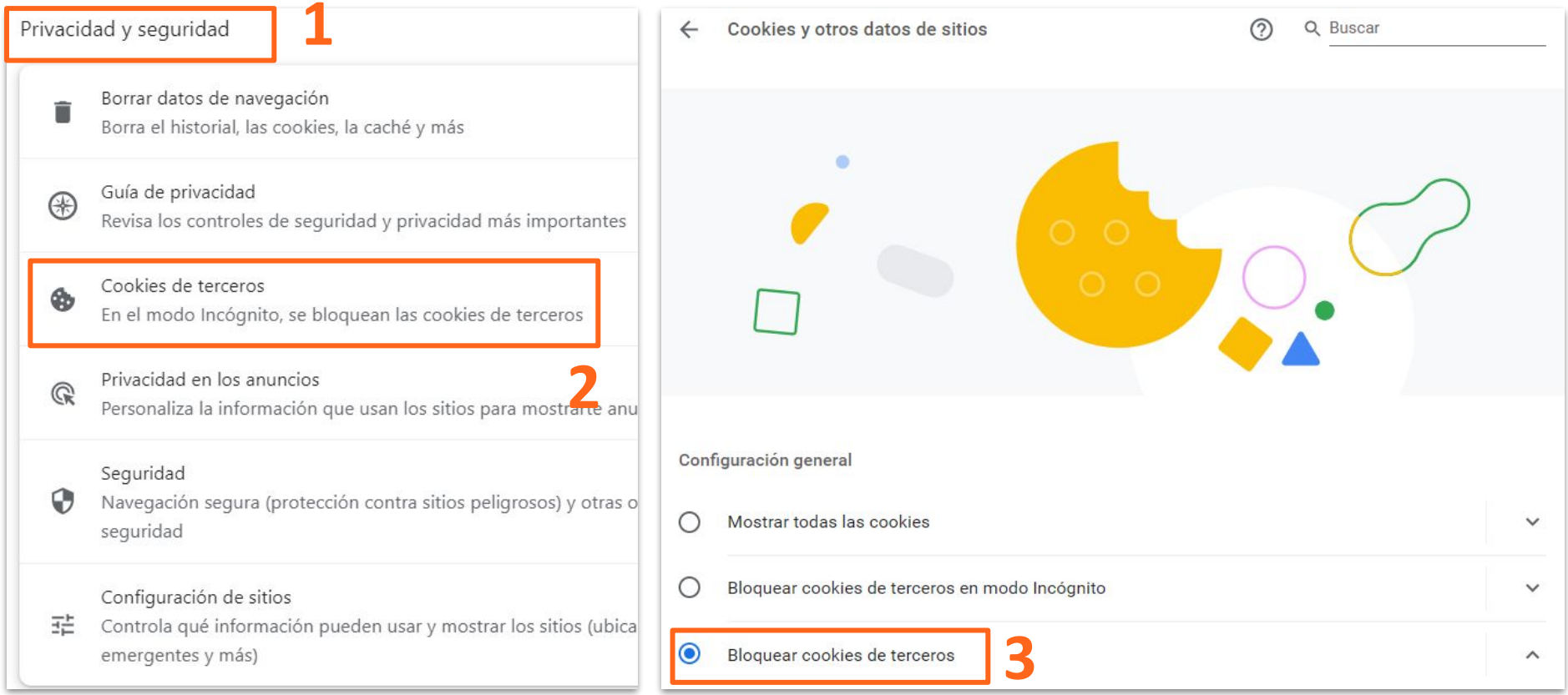
Recuperado de:
https://www.eff.org/deeplinks/2021/09/https-actually-everywhere

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.

GOOGLE CHROME

3. Bloquea las cookies de terceros

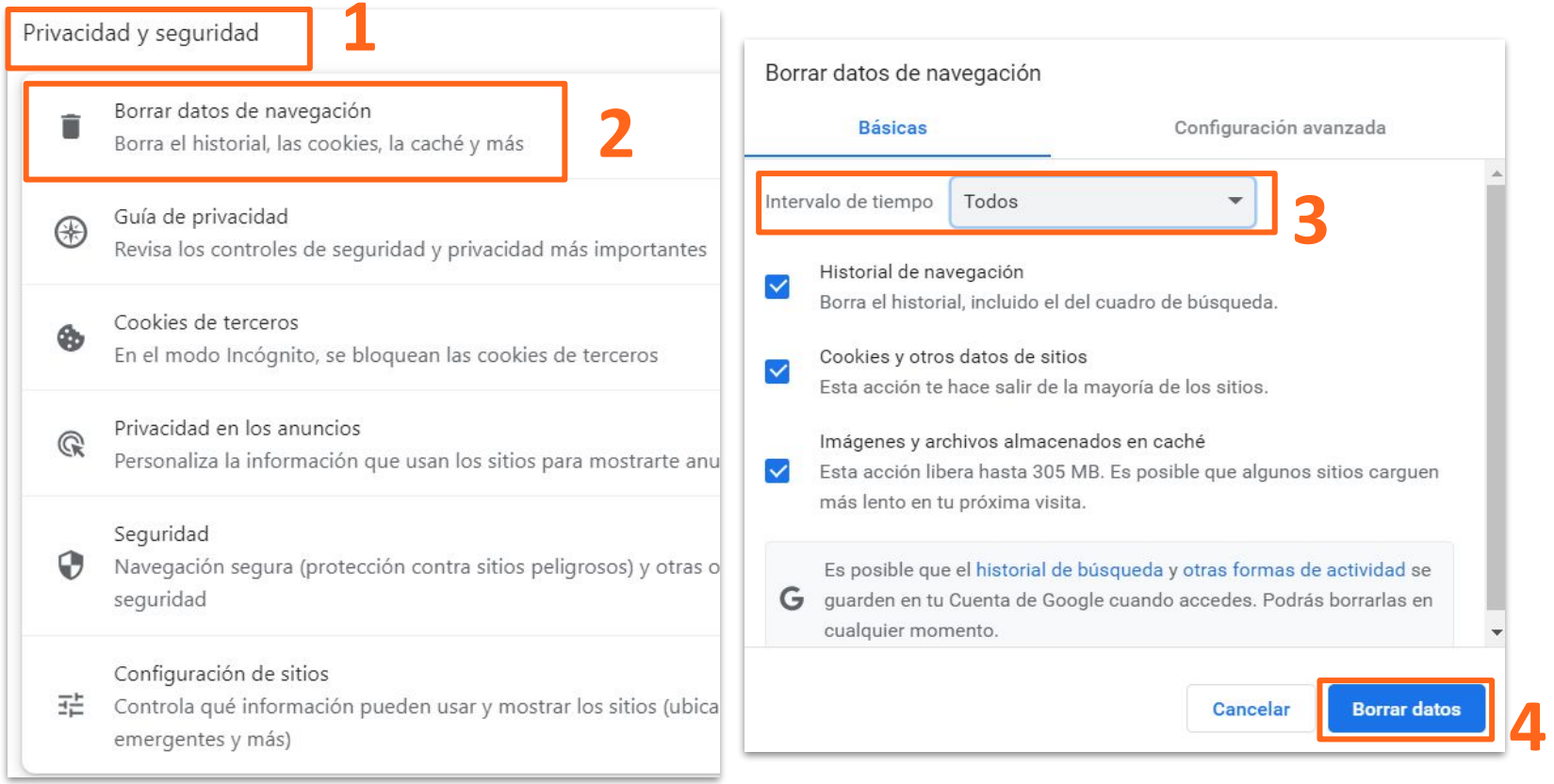
- ➔ Ingresa al apartado de “Privacidad y Seguridad” del panel de configuración de tu navegador: (Menú > Configuración > Privacidad y Seguridad)
- ➔ Haz clic en “Cookies de terceros”
- ➔ Haz clic en la opción “Bloquear cookies de terceros” para activarla



GOOGLE CHROME

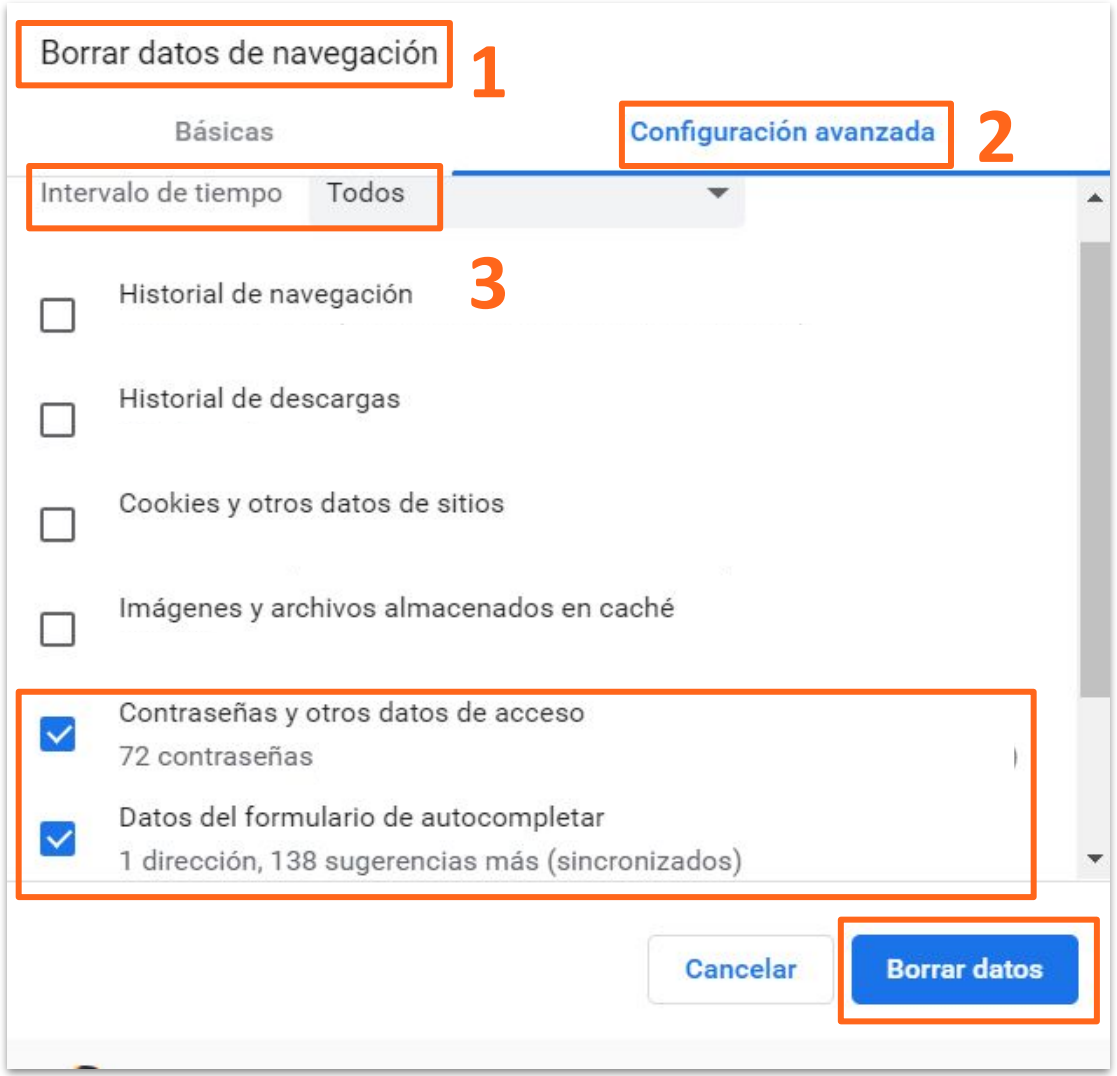
4. Borra los datos de navegación

- ➔ 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”



GOOGLE CHROME

5. Borra contraseñas almacenadas



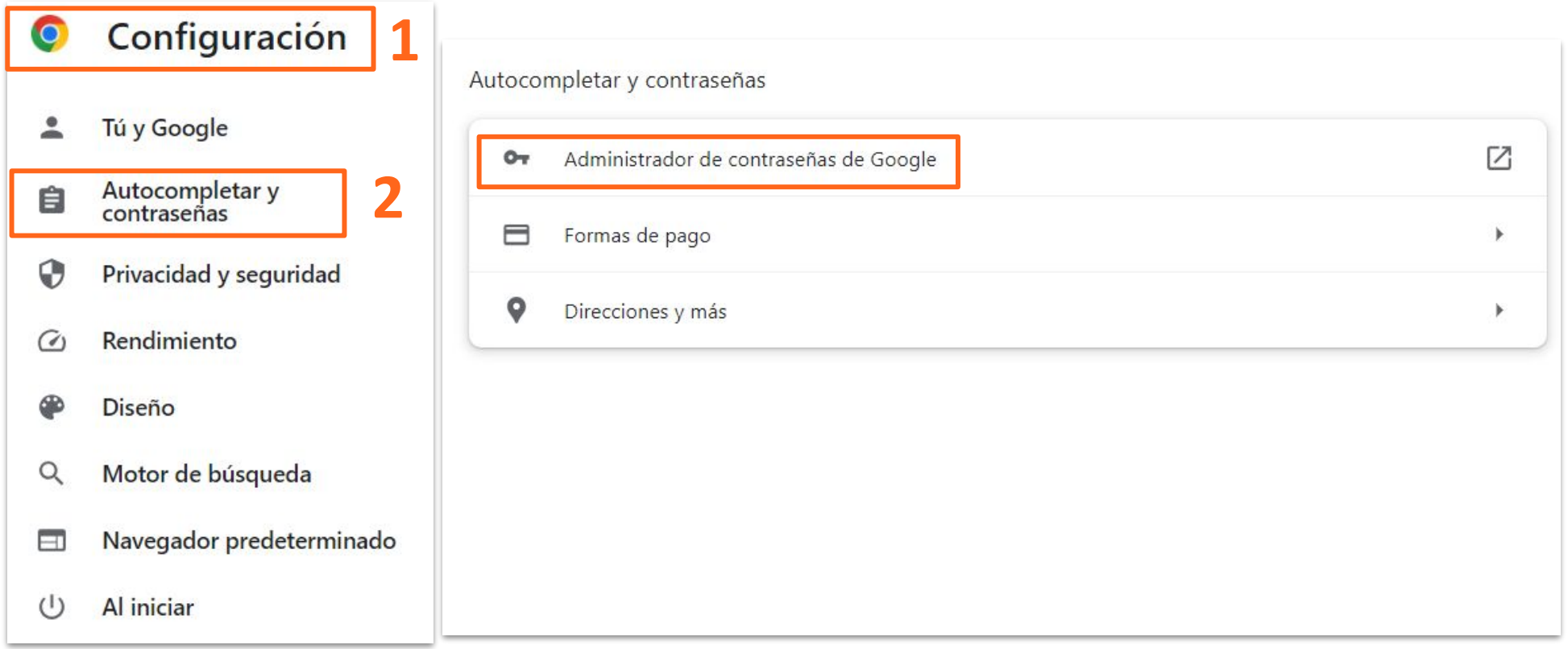
- ➔ Ingresa al apartado de “Borrar datos de navegación” del panel de configuración de tu navegador:

  (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 autocompletar”
- ➔ Haz clic en Borrar Datos

GOOGLE CHROME

6. Desactiva la sugerencia de almacenar contraseñas

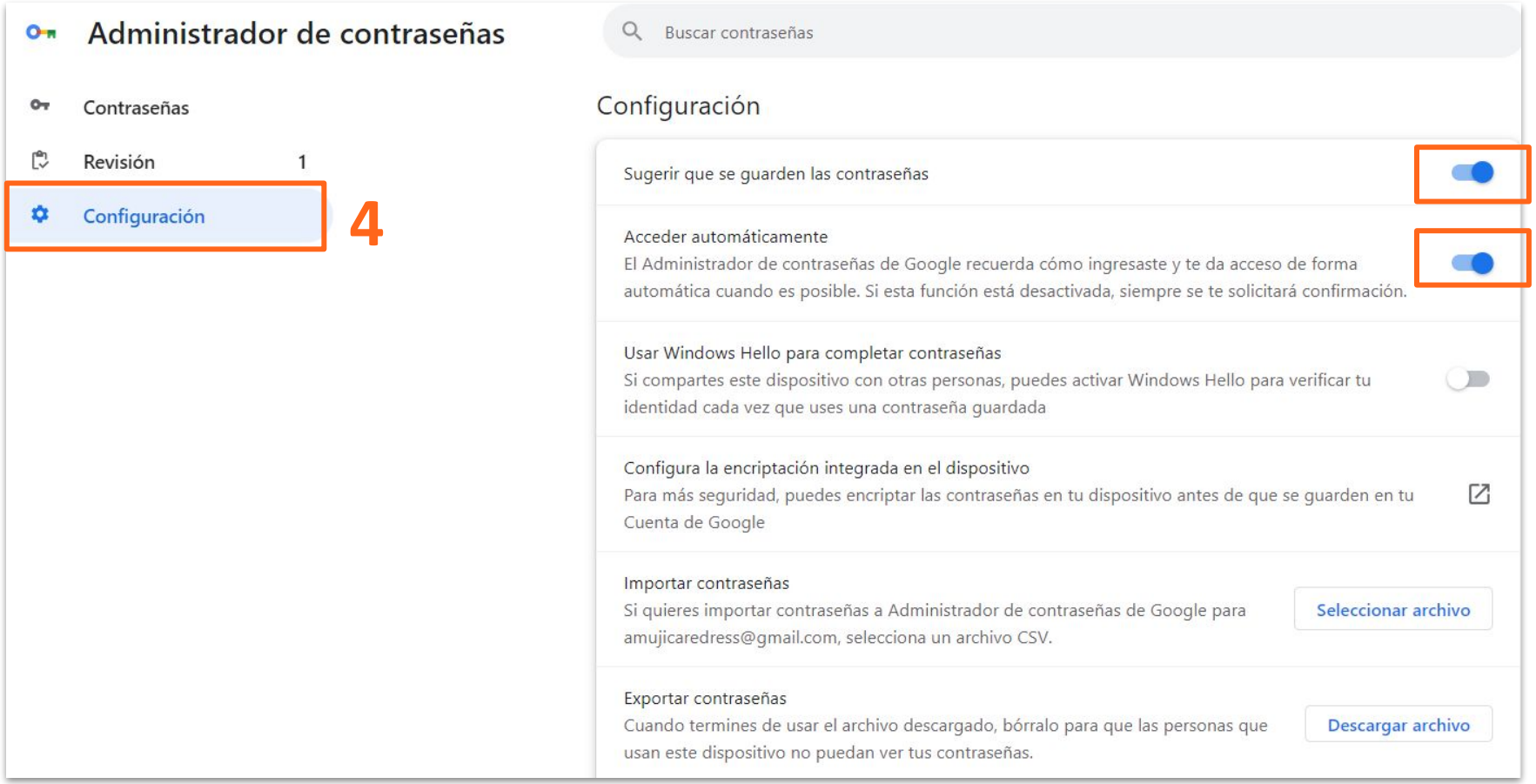
- ➔ Ingresa al apartado de “Autocompletar y contraseñas” del panel de configuración de tu navegador (Menú > Configuración > Autocompletar y contraseñas)
- ➔ Haz clic en “Administrador de contraseñas de Google”



GOOGLE CHROME

6. Desactiva la sugerencia de almacenar contraseñas

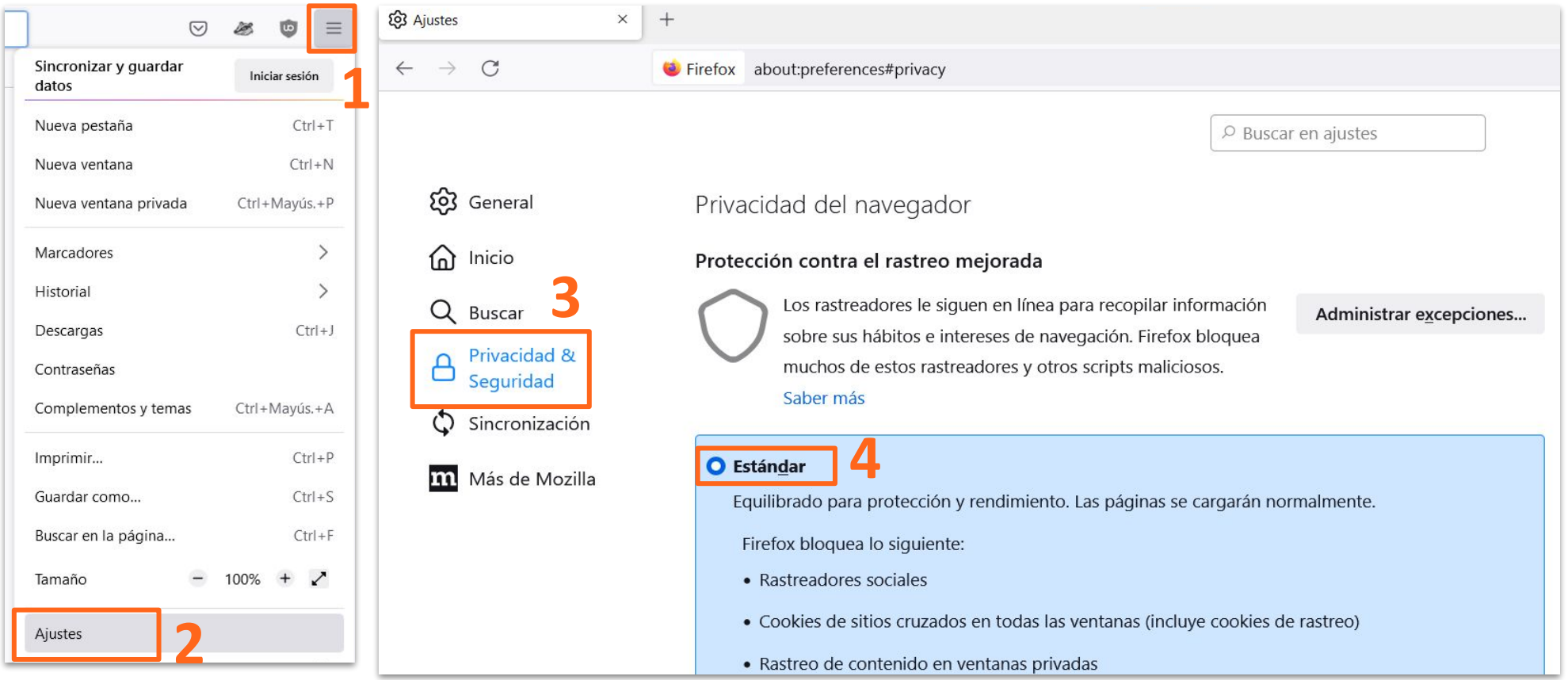
- ➔ Haz clic en “Configuración”
- ➔ Deshabilita las opciones: “Sugerir que se guarden las contraseñas” y “Acceder automáticamente”



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”



MOZILLA FIREFOX

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”

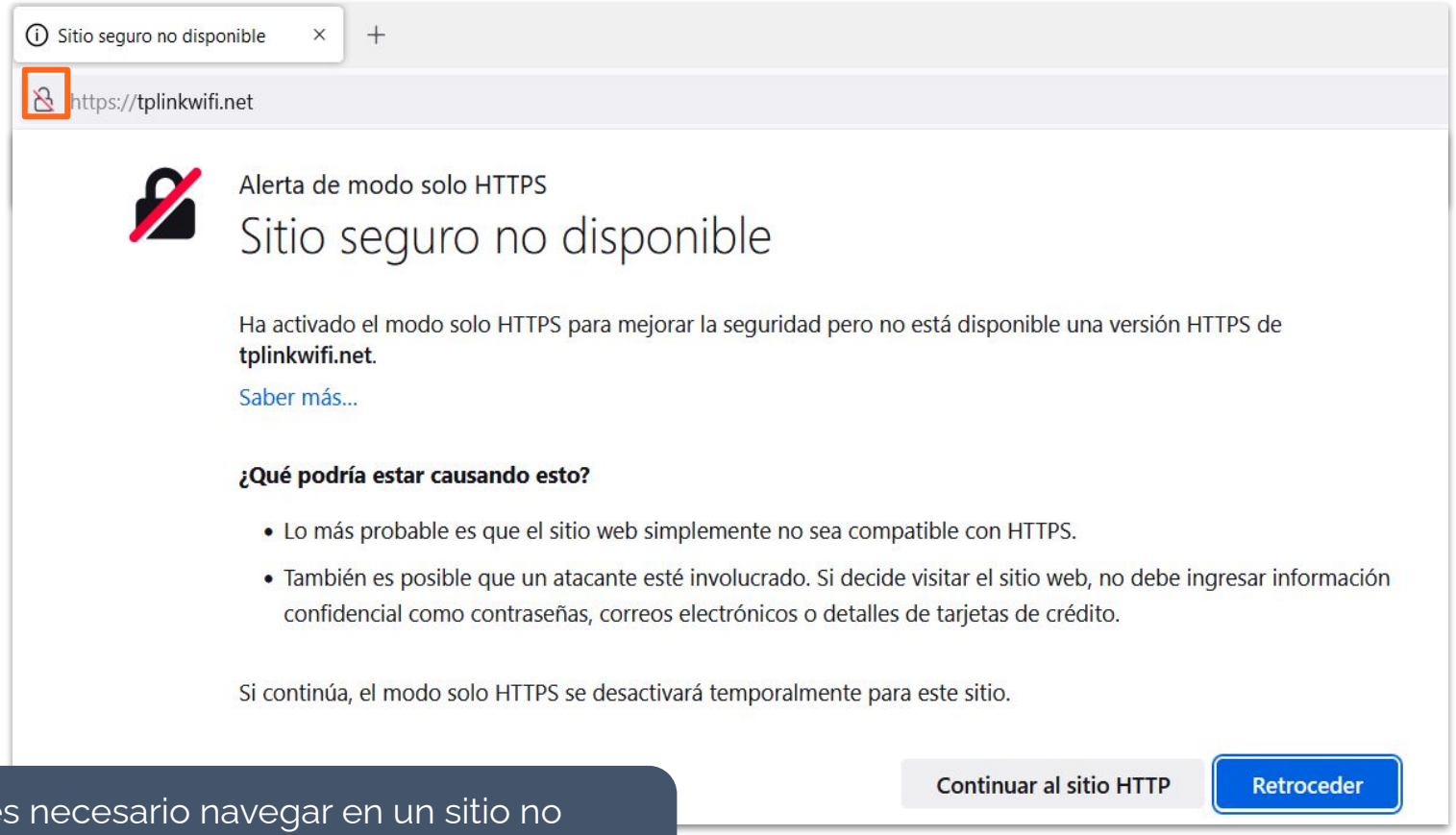


MOZILLA FIREFOX

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

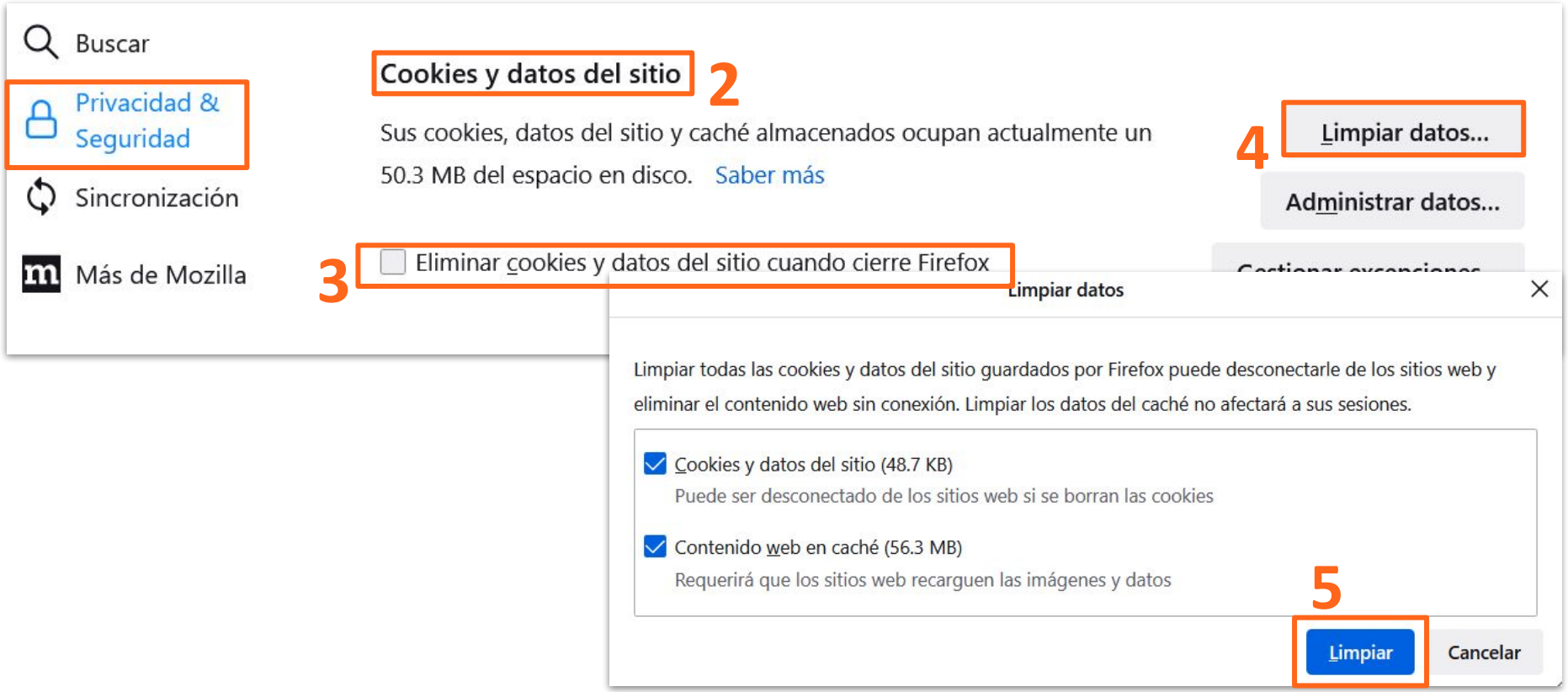


Nota: Si es necesario navegar en un sitio no seguro (sin https), puedes hacer clic en el botón "**Continuar al sitio HTTP"**, para acceder a él.

MOZILLA FIREFOX

3. Borra los datos de navegación y cookies

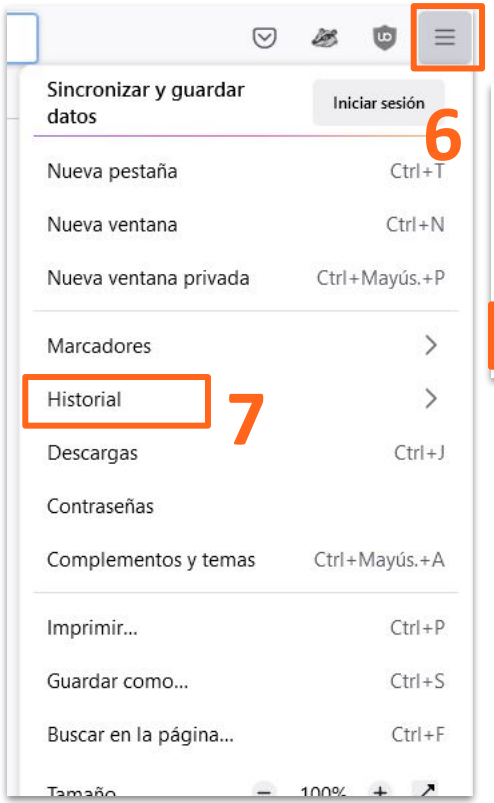
- ➔ Ingresa al apartado de “Privacidad y Seguridad” del panel de ajustes de tu navegador: (Menú ☰ > Ajustes > Privacidad y Seguridad)
- ➔ En “Cookies y datos del sitio” habilita la opción “Eliminar cookies y datos del sitio cuando cierre Firefox”
- ➔ Haz clic en “Limpiar datos” > “Limpiar” para eliminar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

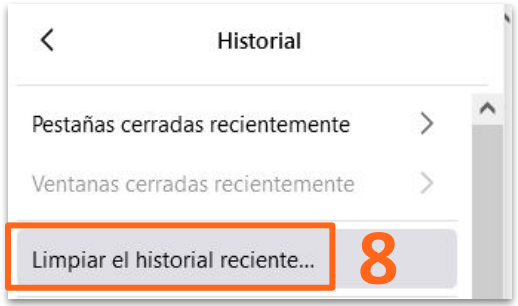


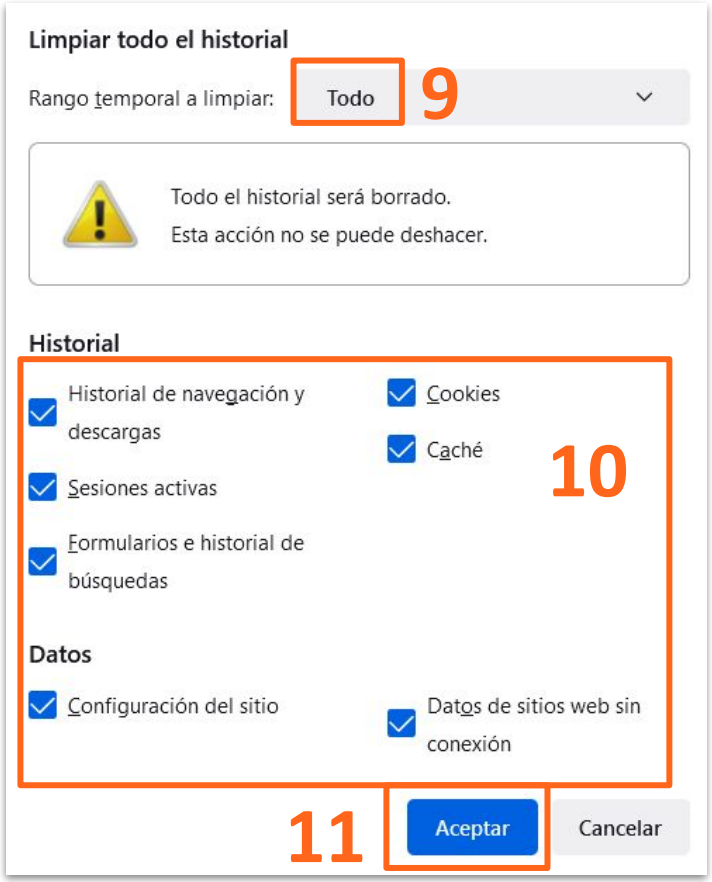
MOZILLA FIREFOX

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”



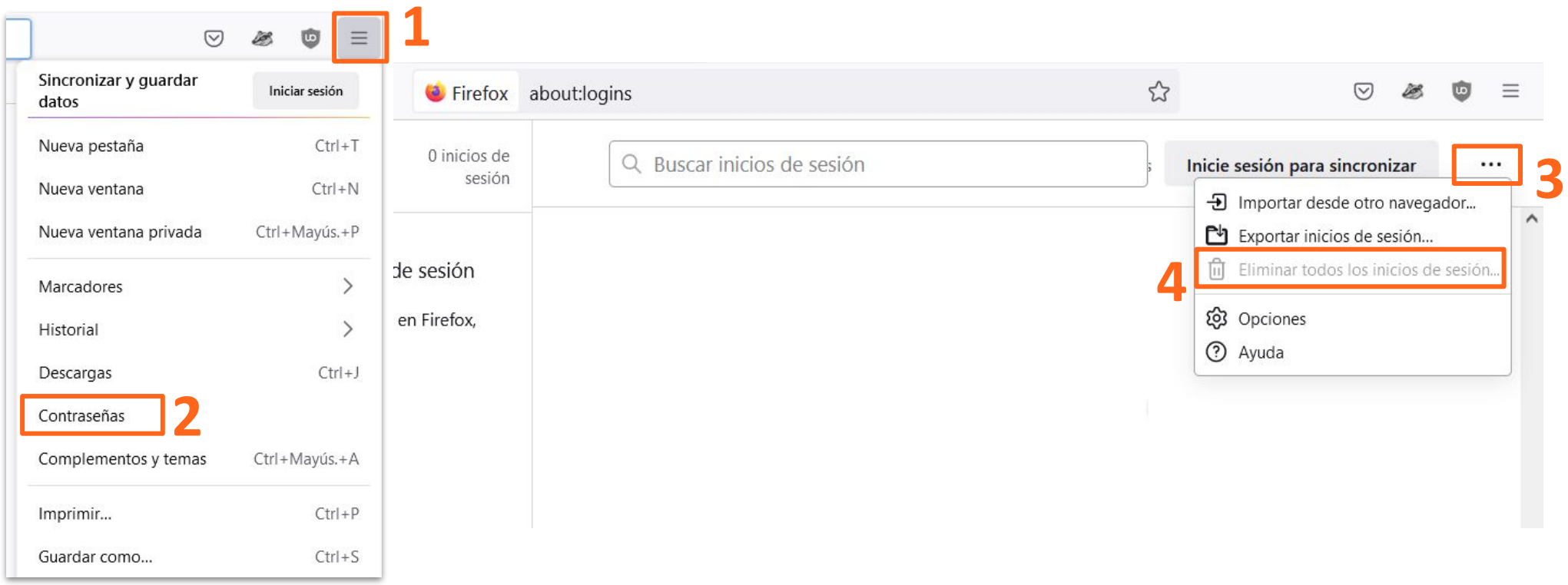




MOZILLA FIREFOX

4. Borra contraseñas almacenadas

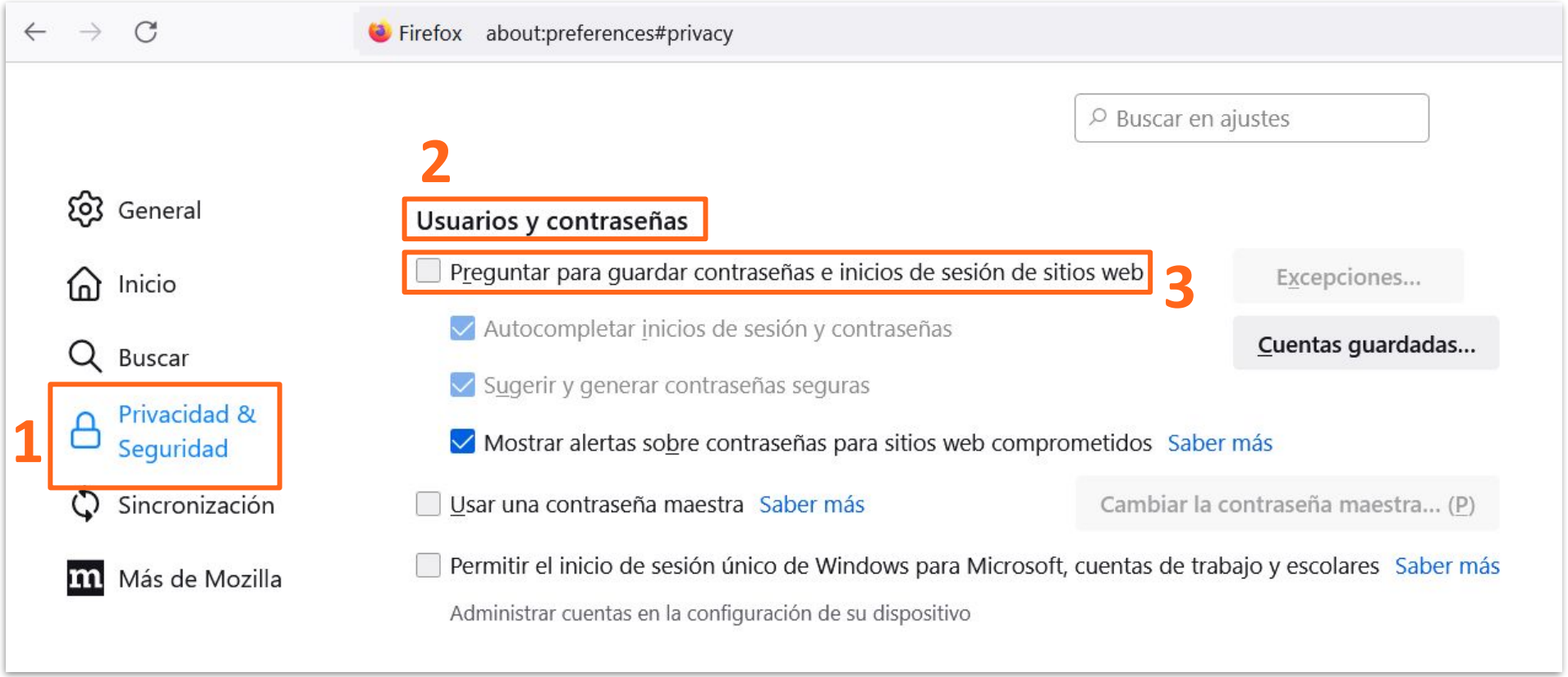
- ➔ Ingresa al apartado de “Contraseñas” de tu navegador: (Menú ☰ > Contraseñas)
- ➔ Se abrirá el administrador de “Inicio de Sesión y Contraseñas” de Firefox.
- ➔ En el menú de ajustes haz clic en “Eliminar todos los inicios de sesión”



MOZILLA FIREFOX

5. Desactiva la sugerencia de almacenar contraseñas

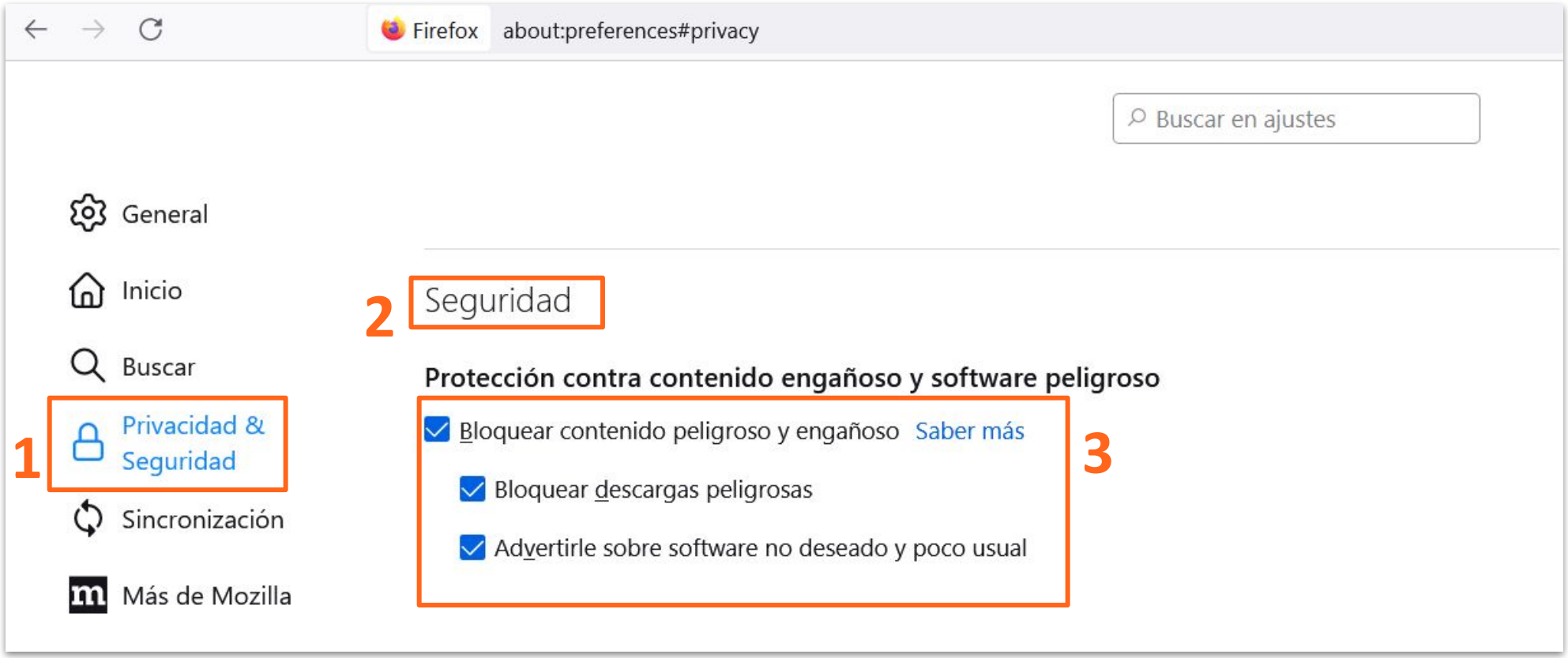
- ➔ Ingresa al apartado de “Privacidad y Seguridad” del panel de ajustes de tu navegador: (Menú ☰ > Ajustes > Privacidad y Seguridad)
- ➔ En “Usuarios y contraseñas” desactiva la opción “Preguntar para guardar contraseñas e inicios de sesión de sitios web”



MOZILLA FIREFOX

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.



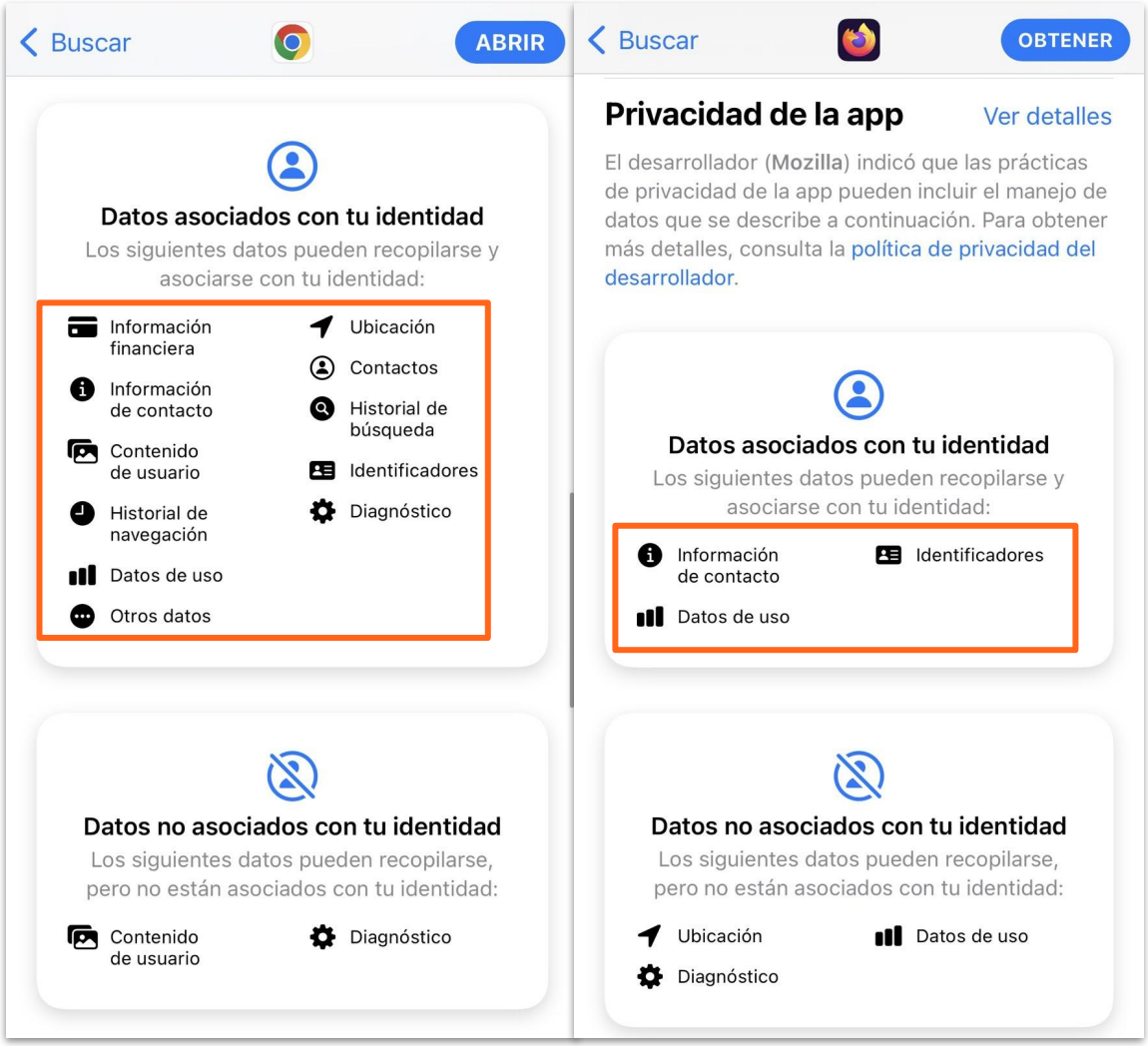
Total Cookie Protection funciona mediante la creación de un **"tarro de cookies"** asignado para cada sitio web que visites.

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/

MOZILLA FIREFOX

Privacidad de los datos - Google Chrome vs. Mozilla Firefox



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

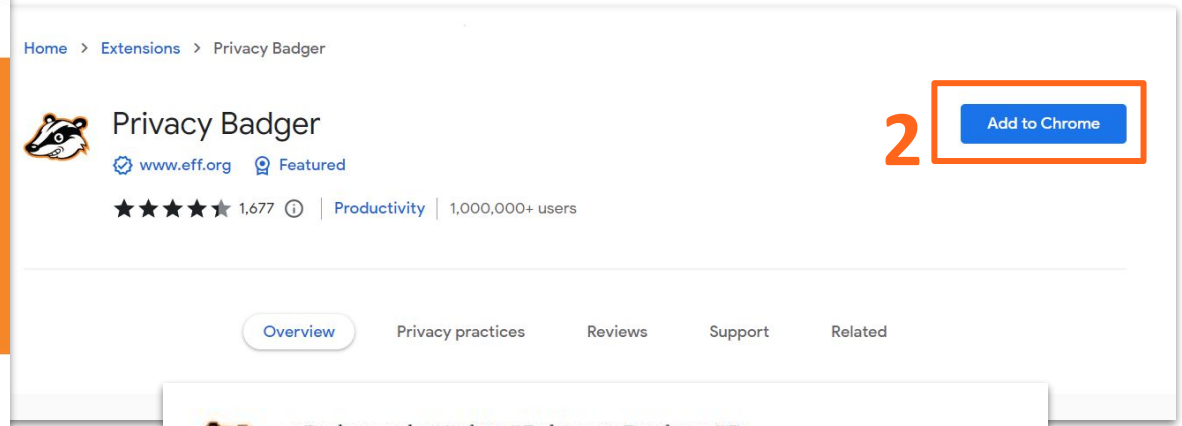
En temas de privacidad de datos, ésta es una de las razones por las cuales recomendamos el uso de Mozilla Firefox como navegador seguro

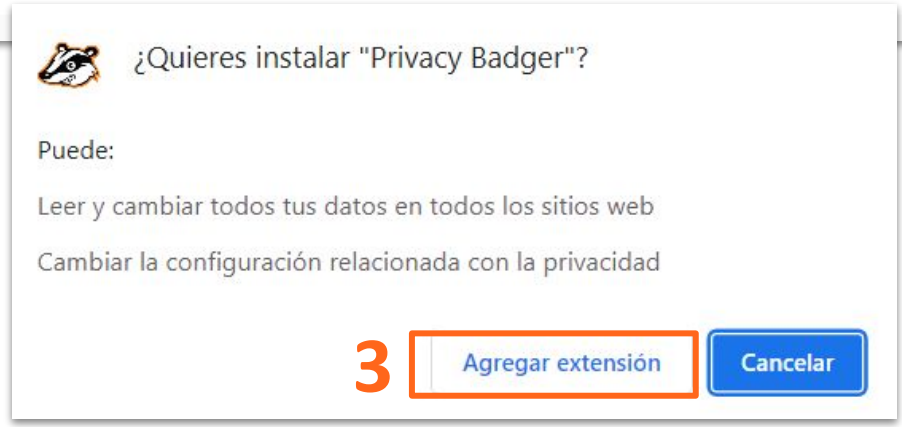
EXTENSIÓN: Privacy Badger

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”



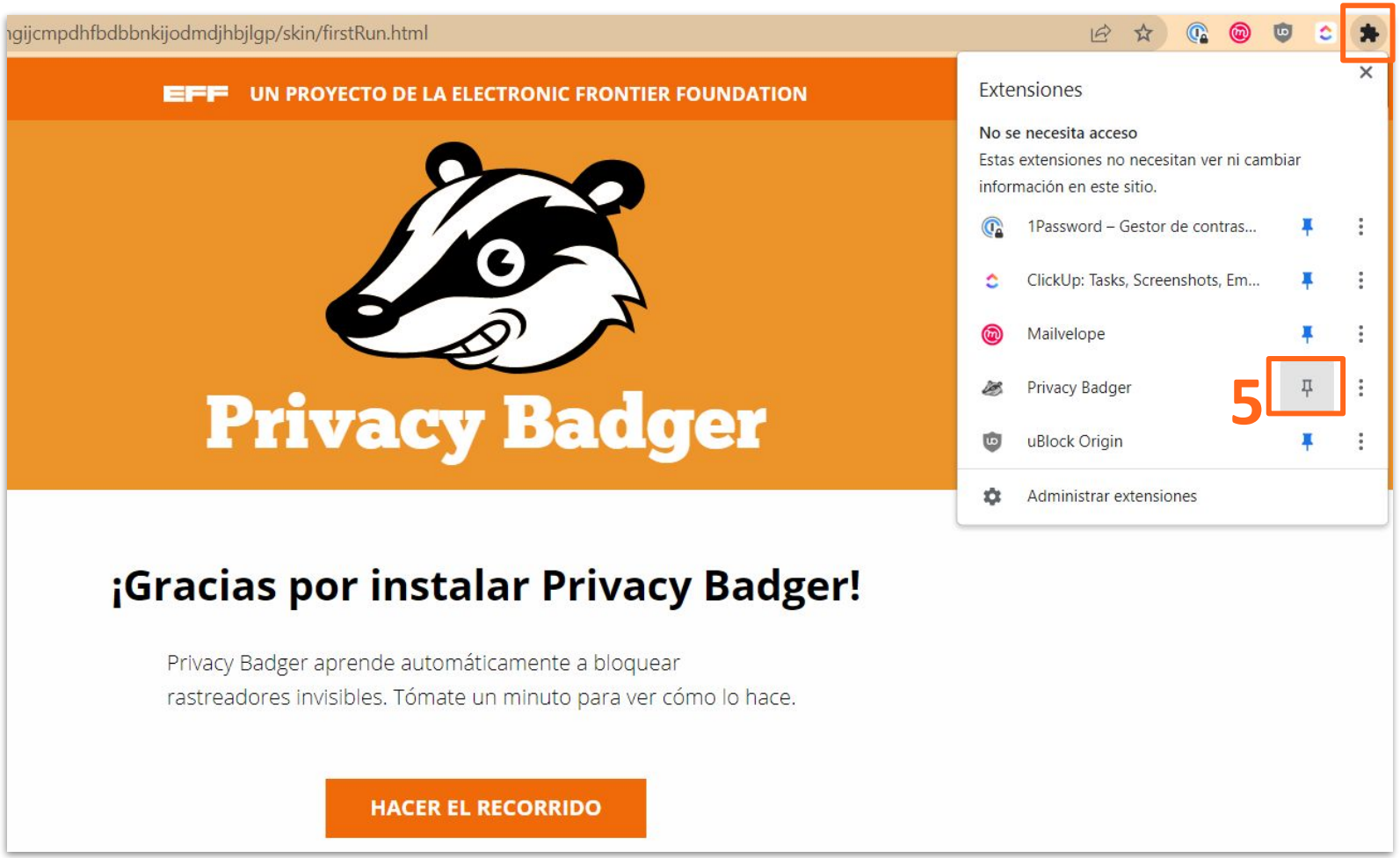




EXTENSIÓN: Privacy Badger

Instalación en Google Chrome

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

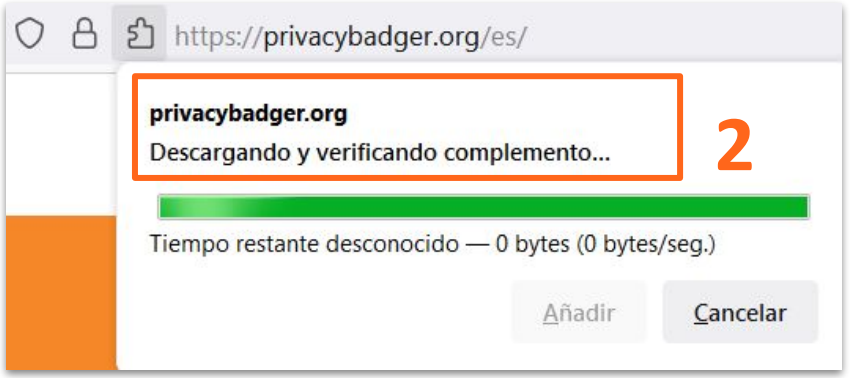


EXTENSIÓN: Privacy Badger

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

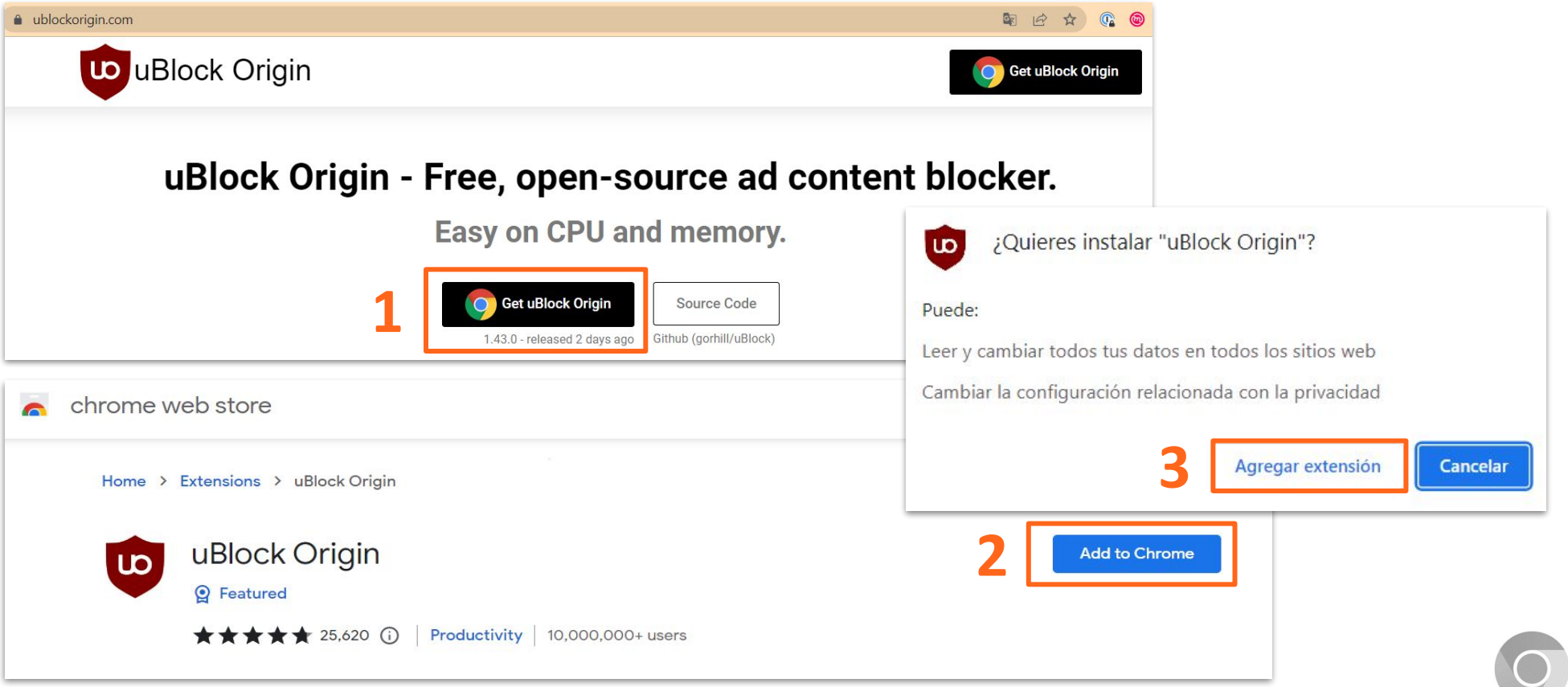
➔ Habilita los permisos para mantenerla en la barra de tareas y haz clic en aceptar



EXTENSIÓN: uBlock Origin

Instalación en Google Chrome

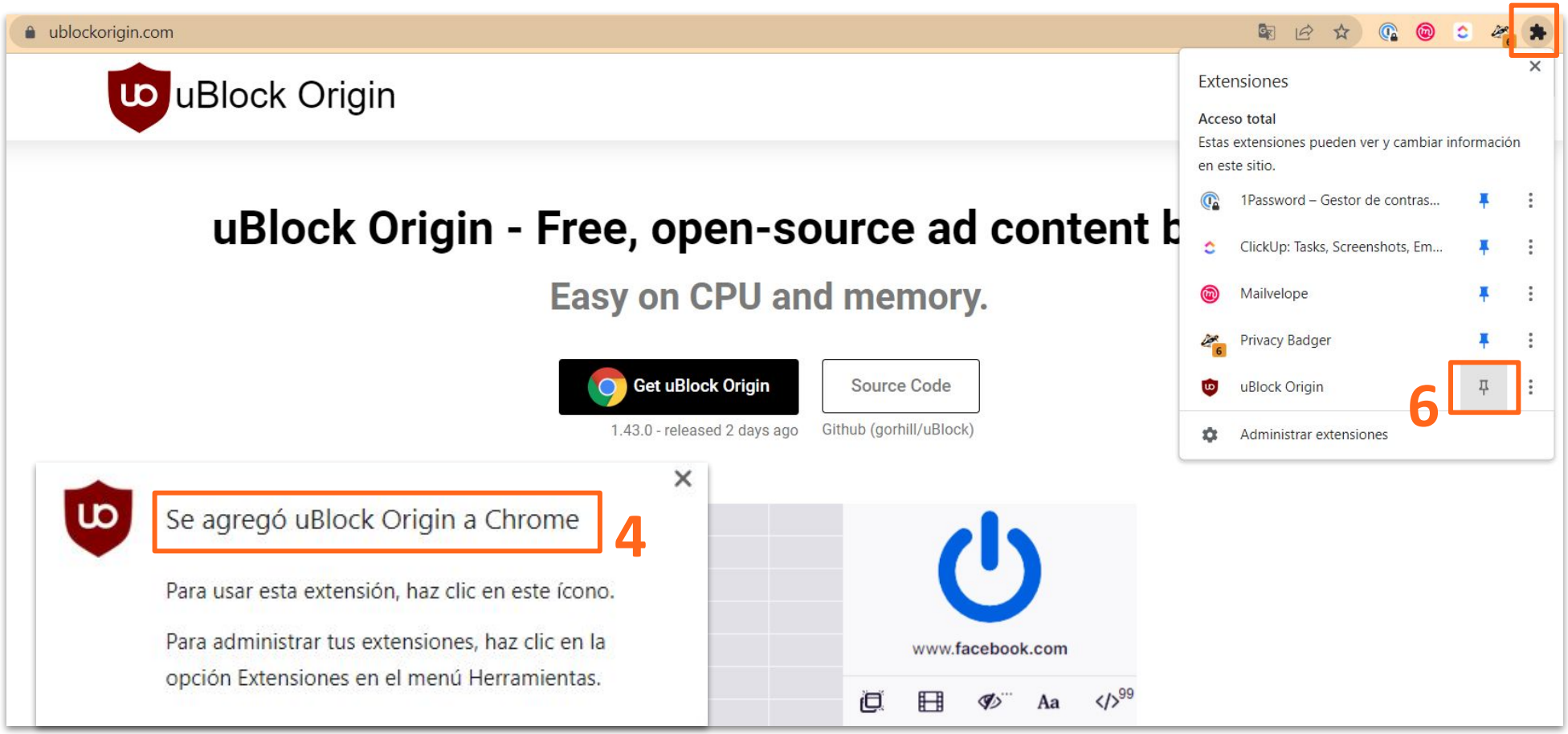
- ➔ Ingresa a https://github.com/gorhill/uBlock#ublock-origin
- ➔ Haz clic en “Get uBlock Origin”
- ➔ Serás dirigido a la Chrome web store. Haz clic en “Add to Chrome”
- ➔ Habilita los permisos haciendo clic en “Agregar extensión”



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



EXTENSIÓN: uBlock Origin

Instalación en Mozilla Firefox

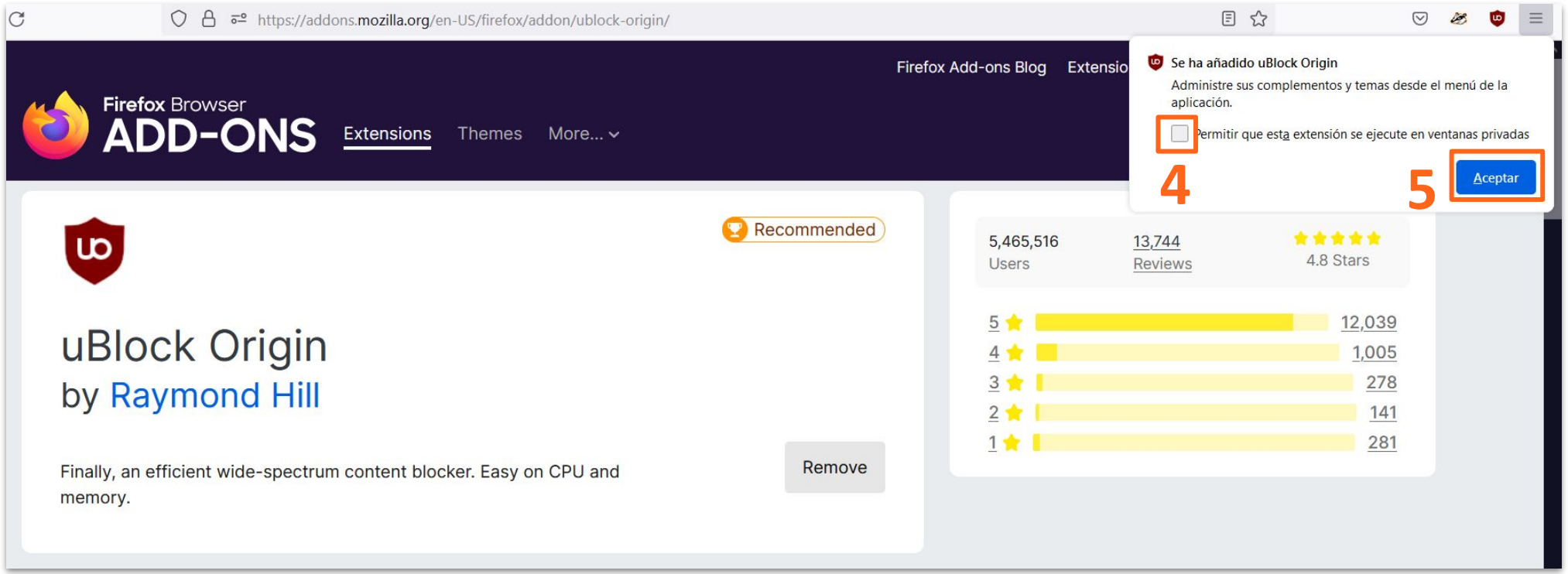
- ➔ Ingresa a https://github.com/gorhill/uBlock#ublock-origin
- ➔ Haz clic en “Obtener uBlock Origin”
- ➔ Serás dirigido a la Firefox Browser ADD-ONS. Haz clic en “Add to Firefox”
- ➔ Espera a que se descargue y Haz clic en “Añadir”



EXTENSIÓN: uBlock Origin

Instalación en Mozilla Firefox

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

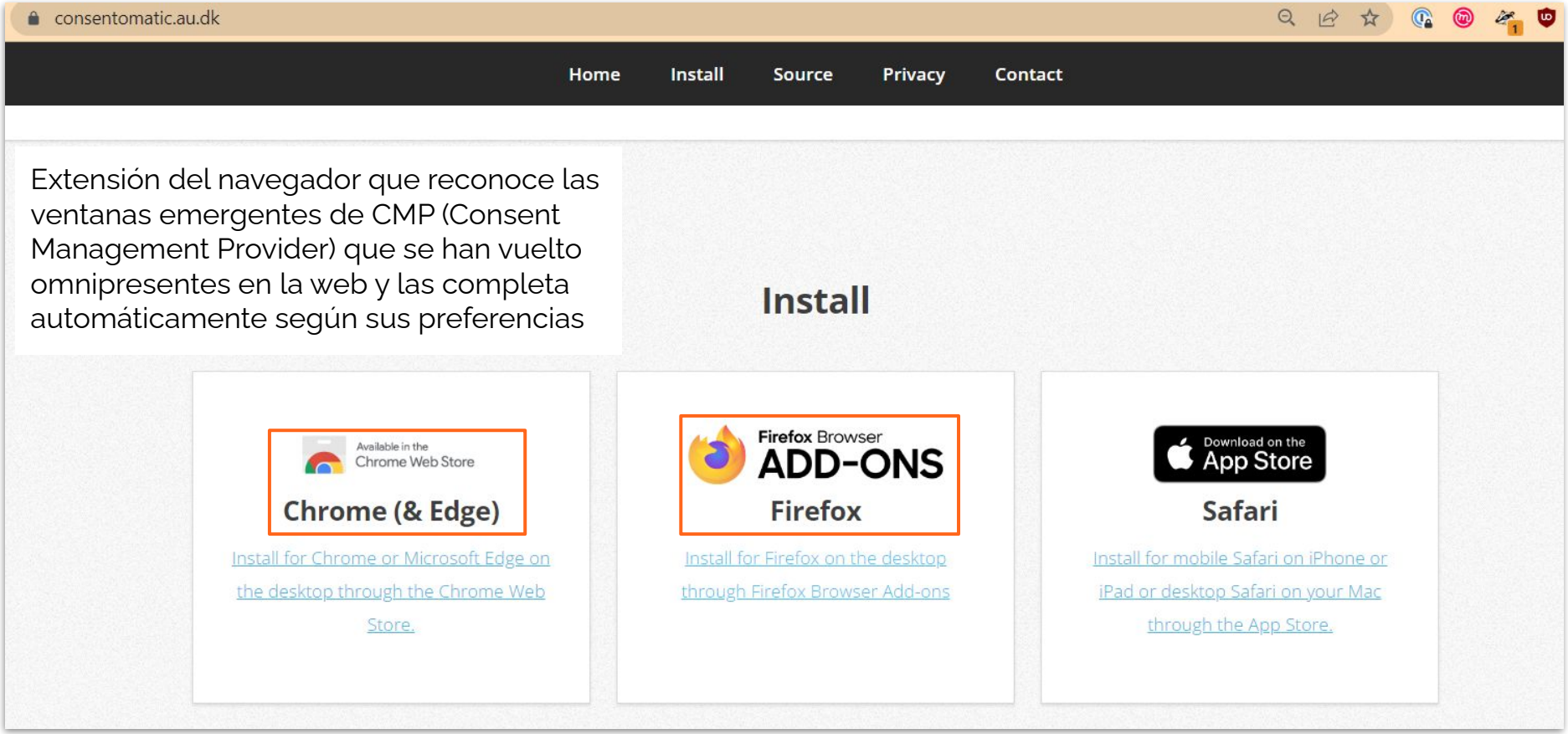


EXTENSIÓN: Conset O-Matic

CAVI AARHUS UNIVERSITY

Instalación

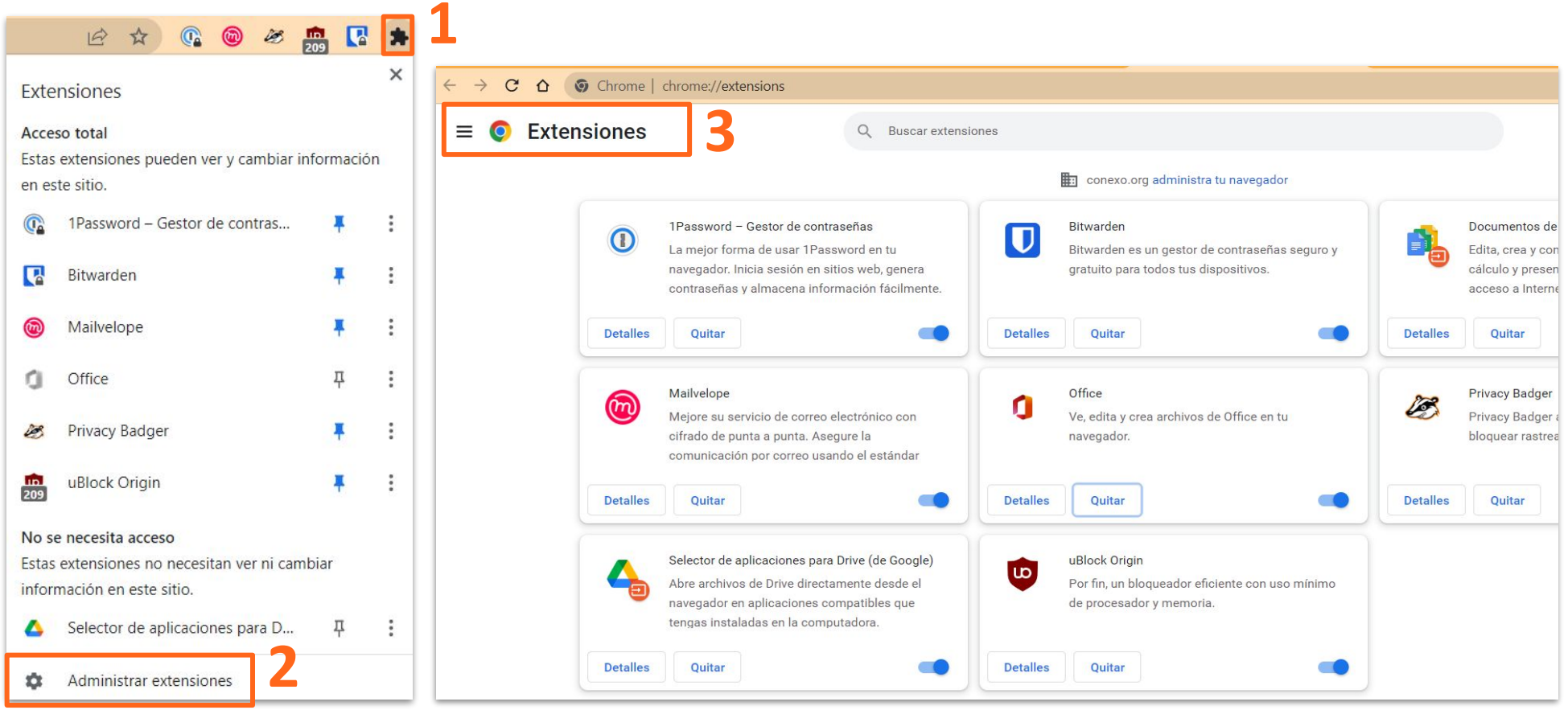
- ➔ Ingresa a https://consentomatic.au.dk/
- ➔ Selecciona la versión de tu navegador
- ➔ Habilita los permisos, instala la extensión y fíjala en tu barra de tareas del navegador



EXTENSIONES

Revisar Administrador de Extensiones (Chrome)

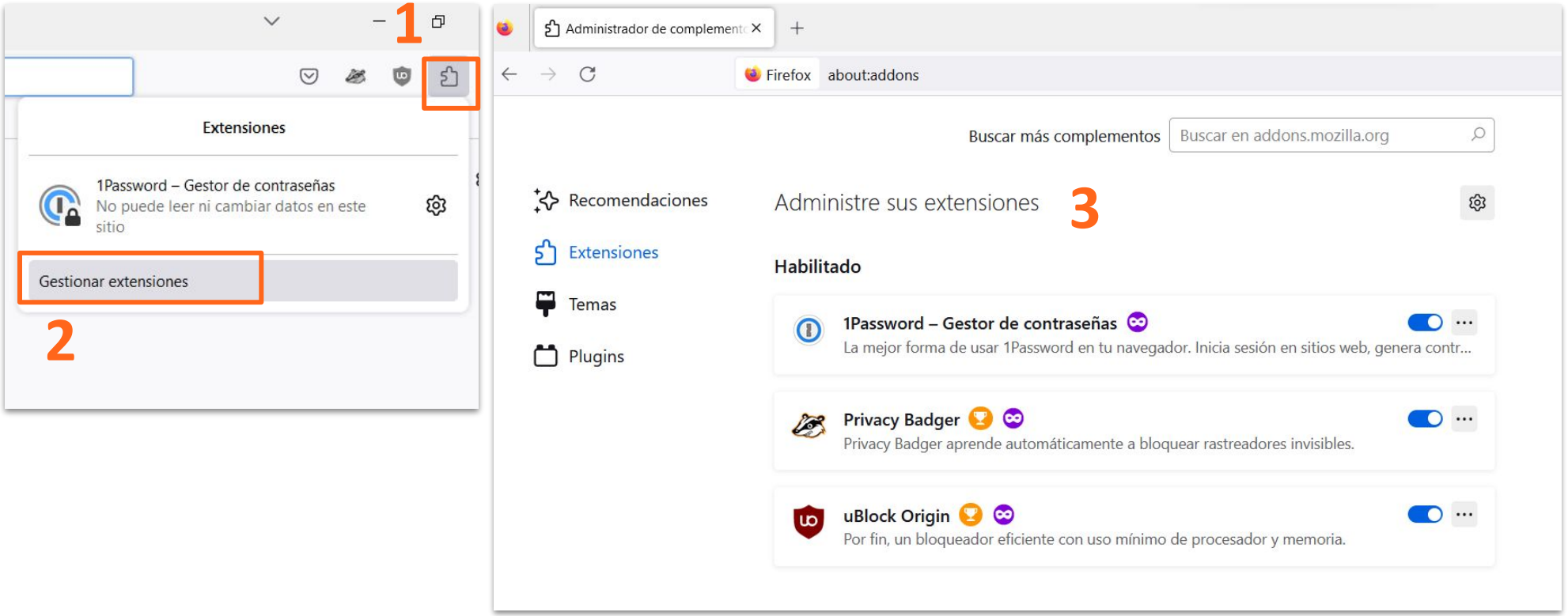
Te recomendamos que accedas al Administrador de extensiones de tu navegador y validez que las instaladas, fueron autorizadas por ti. Recientemente se han realizado investigaciones sobre extensiones que se instalan en tu navegador sin consentimiento y acceden a toda tu información de navegación



EXTENSIONES

Revisar Administrador de Extensiones (Firefox)

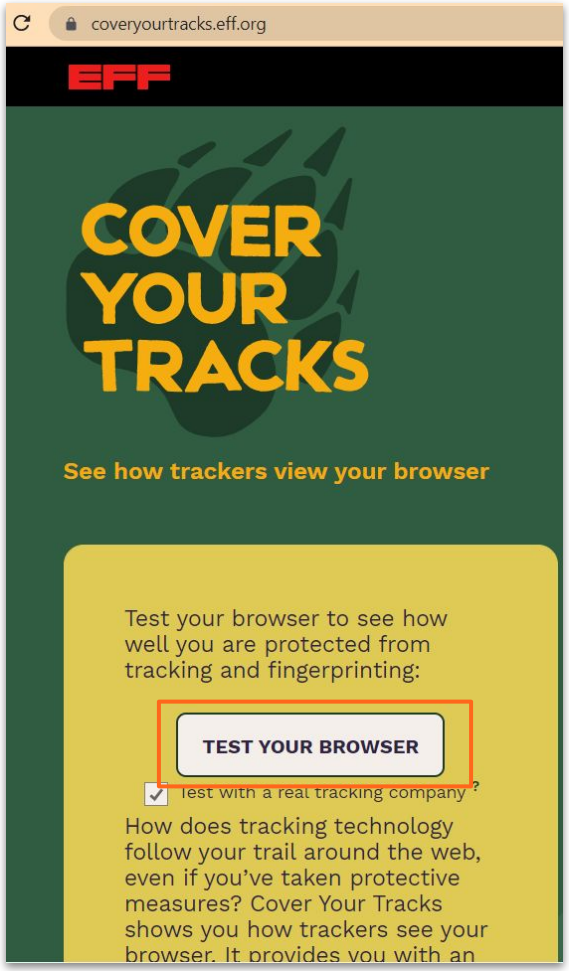
Te recomendamos que accedas al Administrador de extensiones de tu navegador y validez que las instaladas, fueron autorizadas por ti. Recientemente se han realizado investigaciones sobre extensiones que se instalan en tu navegador sin consentimiento y acceden a toda tu información de navegación

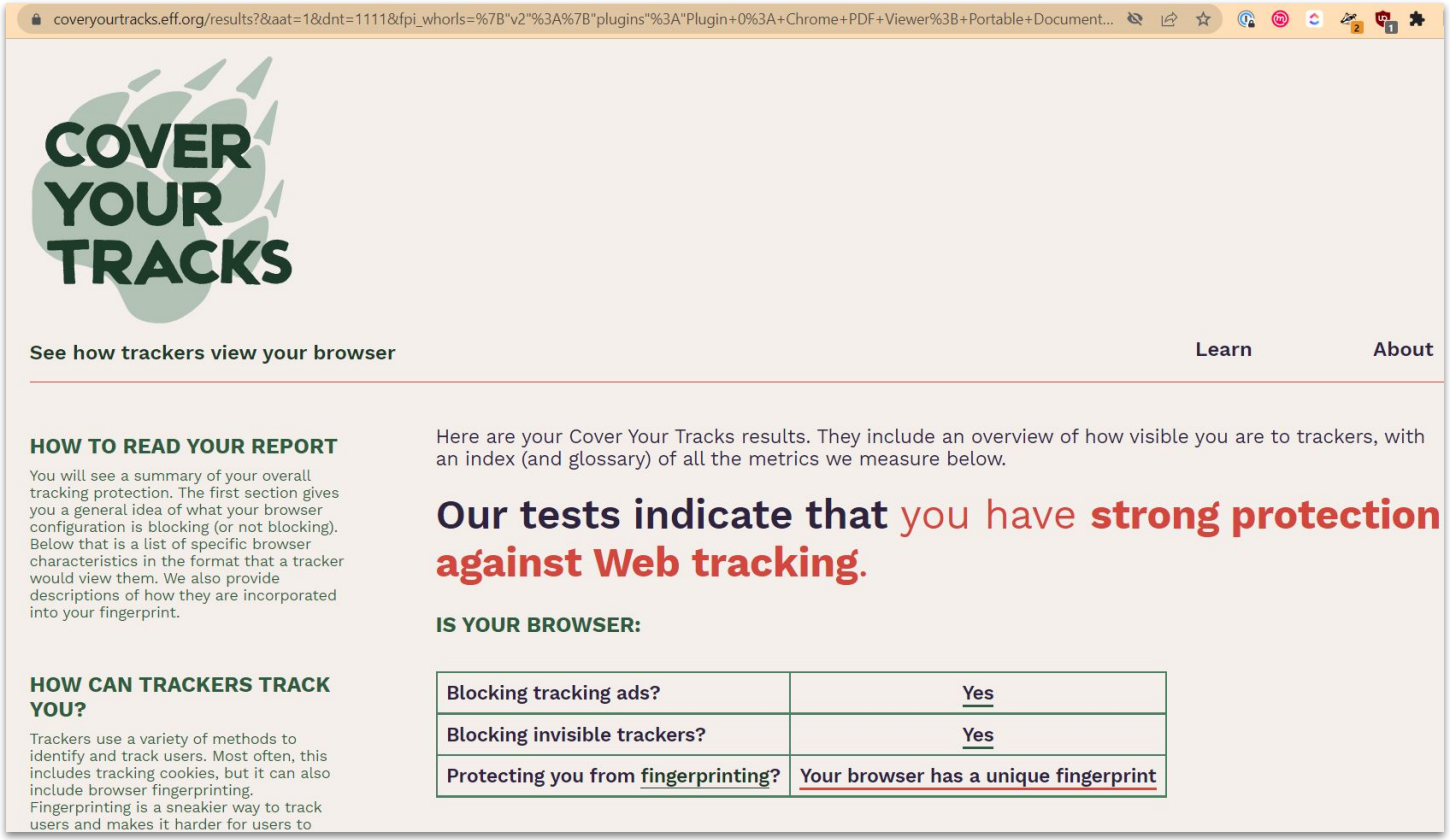


SEGURIDAD DE TU NAVEGADOR

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





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 ProntonPass.
- ➔ 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.

