

Navegadores

Los navegadores son aplicaciones informáticas muy útiles que nos permiten visualizar las páginas web, transformando el texto plano y sin formato que almacenado en servidores web en las páginas web interactivas y con apariencias y estilos elaborados que todos conocemos. Debido a su naturaleza realizan muchas conexiones a internet para pedir la información y que podamos navegar, pero también hacen conexiones por su cuenta por diversos motivos con los servidores de la empresa que los desarrolla. Esto está explicado en sus términos de uso, fácilmente accesibles en su About y en sus páginas de internet, pero los usuarios no siempre prestan atención cuando simplemente pretenden bajar un navegador que les permita acceder a internet. Cada navegador es distinto, y normalmente no recogen información sobre las webs que visitamos, sino que se centran más en metainformación de cómo usamos el navegador, fallos de ejecución, que elementos de interfaz son muy usados (o no usados nunca), etc. Pero no siempre es así, y hay casos en los que pueden recoger información no solo sobre las páginas que visitamos sino sobre la información que escribimos. Lo que es más, la configuración por defecto de unos y otros es diferente, y hay algunas que son más intrusivas respecto a nuestra privacidad, por lo que conviene revisar nuestra configuración y asegurarnos de que no estamos compartiendo información que no queremos sin ser conscientes de ellos.

Chrome

Información que el navegador Chrome envía a Google:

- Instalación: Durante la instalación genera un token que utiliza para medir el porcentaje de descargas del instalador que finalmente son instalados. se borra después de la instalación y no guarda información personal, pero no es opcional.
- Identificador RLZ: es una cadena codificada, sin información identificadora que informa a Google sobre de donde fue descargado Chrome y en qué semana fue instalada. Es utilizada en el primer uso del navegador y durante campañas promocionales de Chrome para medir su éxito. La codificación es en código abierto proporcionado por Google, y es posible deshabilitar que se mande esta cadena.
- Estadísticas de uso: envía un identificador único del cliente y preferencias de usuario, logs de las métricas de uso y fallos de ejecución. En concreto las métricas que recoge son: preferencias, clicks de botones, uso de memoria RAM, dirección de la página si introduces la dirección por voz/visitas una página de suplantación de identidad o malware, tu sistema operativo y fabricante y modelo de tu ordenador. Es opcional y está habilitada por defecto.
- Predicciones de Omnibox: envía el texto escrito en la barra de dirección según se va escribiendo. Es opcional y está habilitado por defecto
- Página no encontrada: envía el texto escrito en la barra de dirección tras recibir una respuesta de "Servidor no encontrado". Es opcional y está habilitado por defecto.
- Traducción: si utilizas la herramienta de traducción de Chrome, enviará el texto que quieras traducir a Google.
- Localización: si utilizas la función de localización, que permite compartir tu ubicación con una página web, Chrome envía la información de red local a Google para estimar tu ubicación. Esto puede incluir: ID de la antena móvil más cercana, fortaleza de señal wifi, e IP asignada a tu dispositivo.
- Reconocimiento de voz: si utilizas el reconocimiento de voz para introducir búsquedas o direcciones, envía la grabación de tu voz, tu idioma por defecto, y la configuración gramática de la página para la que estás usando el reconocimiento por voz. Google usa esta información para convertir la grabación en texto. Si tienes activadas las estadísticas de uso e informes de

errores, manda información adicional, como URL de la página, sistema operativo, y fabricante y modelo del procesador y hardware de audio.

- Autocompletado de formularios: envía información a Google acerca de las páginas que tienen formularios web, incluida una URL hasheada y detalles sobre la estructura del formulario. También envía si has escrito en el formulario, aunque no la información que has escrito, salvo que decidas almacenarlo en tu cuenta Google usando sincronización.
- Actualizaciones automáticas (Win/Mac): en estos dos sistemas operativos Chrome envía periódicamente información sobre la frecuencia de uso de Chrome, y detalles sobre la versión de Chrome y del Sistema Operativo. Es posible deshabilitarlo pero a cambio tienes que deshabilitar las actualizaciones automáticas y preocuparte tú de mantenerlo actualizado, lo cual puede ser un riesgo de seguridad.
- Sincronización: si tienes activada la sincronización, Chrome por defecto sincroniza todo con tu cuenta Google: apps, extensiones, preferencias, auto completar, historial de Omnibox, marcadores, contraseñas y pestañas abiertas.

A partir de 2012 Google comenzó a dar soporte para la cabecera HTTP Do Not Track (DNT), pero es una opción que está deshabilitada por defecto. Google es transparente con qué información recoge, pero la configuración por defecto de Chrome es más intrusiva que la de otros navegadores.

Firefox

Información que el navegador Firefox envía a Mozilla:

- Actualizaciones: una vez al día, envía tu versión del navegador, preferencias de lenguaje, sistema operativo y versión del mismo. Es opcional y está habilitado por defecto, deshabilitarlo puede ser un riesgo de seguridad.
- Bloqueo de add-ons: para proteger de add-ons maliciosos, y una vez al día, envía tu versión del navegador, sistema operativo y versión del mismo, tu localización, número total de peticiones, hora de la última petición, hora actual, dirección IP, y la lista de add-ons que tienes instalados. Es opcional y está habilitado por defecto, deshabilitarlo puede ser un riesgo de seguridad.
- Página de inicio por defecto: tiene unos snippets en la parte superior, debajo de la barra de búsqueda. Una vez al día recoge información de uso de los mismos, idioma y versión de Firefox. Almacenan esta información durante 60 días. Para que la información de los snippets sea relevante, una vez al mes Mozilla envía tu navegador el país desde el que estás usando Firefox (en base a tu dirección IP), y el navegador almacena esta información localmente, para después elegir que snippets mostrar.
- Firefox Health Report: utilizado para proporcionar al usuario información sobre la estabilidad y rendimiento del navegador, así como consejos si está teniendo problemas. Envía información sobre el hardware del dispositivo en el que está instalado, sistema operativo, versión de Firefox, número y tipo de addons, temporización de eventos del navegador, renderización, restauración de sesiones, duración de sesiones, antigüedad de perfil, número de crashes y número de páginas visitadas. No envía URLs de páginas visitadas. Es opcional y está habilitado por defecto.
- Seguridad: de manera automática comprueba páginas maliciosas o que están suplantando identidad, add-ons maliciosos, y certificados SSL de terceros. Para ello comprueba los certificados de páginas seguras con terceros, comprobando su validez. Cada 30 minutos descarga las listas de SafeBrowsing de Google para bloquear accesos y descargas de páginas maliciosas o de suplantación de identidad. Cuando descargas ejecutables que no aparecen en estas listas, Firefox manda metainformación, incluida la URL asociada al archivo al servicio SafeBrowsing. Es opcional y está habilitado por defecto.

- **Telemetría:** estadísticas de uso del navegador, rendimiento, uso y responsividad de la interfaz, consumo de RAM, y configuración del hardware. También recoge tu dirección de IP. Las transmite usando SSL para mejorar el desarrollo de futuras versiones de Firefox. Una vez recibidas son agregadas y puestas a disposición de los desarrolladores, tanto empleados de Mozilla como contribuidores públicos. Si tienes telemetría activada, algunos experimentos a corto plazo pueden recolectar información de páginas visitadas. Es opcional y está deshabilitado por defecto. No obstante en versiones nightly, de desarrollo y beta si que está activado por defecto.
- **Celdas:** si utilizas esta opción en las nuevas pestañas, Firefox envía a Mozilla información sobre número de clicks, impresiones, dirección IP, información de localización, e información sobre las celdas (posición y tamaño de la rejilla).
- **Búsqueda por defecto:** para elegir tu mejor buscador por defecto, envía una vez una petición a Mozilla para averiguar tu país en base a tu IP. Firefox recibe esta información y la almacena localmente, y la utiliza para determinar qué buscador utilizar por defecto.
- **Sincronización:** si eliges utilizar sincronización, las opciones que elijas sincronizar (pestañas, marcadores, historial, contraseñas, addons, preferencias) son enviadas a los servidores de Mozilla mediante SSL para poder sincronizar entre dispositivos.

En 2009 Firefox fue el primer navegador en implementar las cabeceras HTTP Do Not Track (DNT). Mozilla es transparente en cuanto a qué información recoge y cómo la usa, y la configuración por defecto de Firefox no es intrusiva, y además pregunta/informa antes de enviar información personal.

En general encuentre esto <http://www.omicrono.com/2015/06/esta-web-te-resume-los-terminos-y-condiciones-de-uso-que-nunca-lees/>

Términos y condiciones de microsoft

Política de privacidad-> <https://www.microsoft.com/en-us/privacystatement/default.aspx?intsrc=client- -windows- -7.14- -go-privacy&setlang=es>

Condiciones de uso-> <https://www.microsoft.com/en-us/servicesagreement/?intsrc=client- -windows- -7.14- -go-eula&setlang=es>

http://wikis.fdi.ucm.es/ELP/Terminos_y_condiciones_de_Microsoft
He aquí la página de la wiki con los términos de microsoft.

Contrato de servicios de Microsoft

- Privacidad de los servicios
 - Microsoft **recopila datos directamente**, por ejemplo, cuando un usuario crea una cuenta de Microsoft, envía una consulta de búsqueda de Bing, habla con un comando de voz a Cortana, carga un documento en OneDrive o se pone en contacto con nosotros para obtener ayuda. También obtienen datos de terceros.

- Microsoft utiliza los datos que recoge y el uso de los mismos para proporcionar los servicios que ofrece. También pueden utilizar los datos para comunicarse con un usuario.
- **Utilizan los datos recaudados para ayudar a hacer los anuncios más relevantes para los usuarios.** No utilizan lo que contiene un correo electrónico, chat, vídeo llamadas o correo de voz, ni documentos, fotos u otros archivos personales con este fin.
- **Comparten los datos personales de los usuarios** con su consentimiento o para completar cualquier transacción o proporcionar un servicio que haya solicitado o autorizado el usuario. También compartimos los datos con filiales y subsidiarias controladas por Microsoft, con los proveedores que trabajan en nuestro nombre, o para responder a un proceso legal.
- Los usuarios pueden ver o editar sus datos personales en línea para muchos servicios de Microsoft. También pueden tomar decisiones acerca de la recogida y uso de sus datos de Microsoft.
- Los usuarios pueden inhabilitar la recepción de anuncios basados en sus intereses por parte de Microsoft visitando su [página de no participación](#).
- **Microsoft utiliza cookies y tecnologías similares para ofrecer sus servicios y ayudar a recopilar datos.** También utilizan balizas web para ayudar a entregar las cookies y recopilar datos de uso y rendimiento de nuestros servicios. Sus servicios pueden incluir balizas web y cookies de proveedores de servicios de terceros.
- Los usuarios tienen una serie de herramientas para controlar las cookies, balizas web y otras tecnologías similares.
- Contenido de los servicios
 - El contenido personal de un usuario **seguirá siendo de su propiedad** y estará bajo su responsabilidad.
 - Si un usuario comparte su contenido con otras personas, acepta expresamente que toda persona con quien lo haya compartido puede utilizar, guardar, grabar, reproducir, transmitir, mostrar, comunicar y eliminar dicho contenido.
 - Microsoft no tiene responsabilidad alguna respecto del contenido de los usuarios o del material que otras personas carguen, almacenen o compartan mediante sus Servicios.
 - Para proporcionar los servicios a los usuarios, con justificación de protección y mejora de los productos y servicios de Microsoft, **se concede a Microsoft una licencia de propiedad intelectual e industrial universal y libre de regalías** (pagos por la autoría de una obra) para utilizar el contenido.

- **No utilizan lo que los usuarios expresan en mensajes de correo electrónico, chat, videollamadas o correo de voz ni en documentos, fotos u otros archivos personales con el fin de personalizar anuncios** para usted.
- Código de conducta
 - Se prohíbe el contenido, el material o las acciones que infrinjan los Términos y condiciones y al aceptarlos queda obligado a cumplir las siguientes reglas:
 - No realizar actividades ilegales.
 - No participar en actividades que exploten, dañen o amenacen con dañar a menores de edad.
 - No enviar correo no deseado.
 - No mostrar o utilizar públicamente los Servicios para compartir contenido u otro material inapropiado.
 - No participar en actividades falsas o engañosas.
 - No eludir de forma dolosa las restricciones en materia de acceso a los Servicios o disponibilidad de estos.
 - No participar en actividades que pudieran dañarle a usted, a otras personas o a los Servicios.
 - No infringir los derechos de otras personas o entidades.
 - No participar en actividades que vulneren la privacidad de otras personas o entidades.
 - No ayudar a otros individuos a infringir estas reglas.
 - Microsoft se reserva el derecho de **rechazar el contenido de los usuarios** si excede los límites de almacenamiento o tamaño de archivo permitidos por el Servicio.
 - Microsoft se reserva el derecho de **adoptar medidas contra los usuarios** que infrinjan las reglas mencionadas, como la interrupción de los servicios, el cierre de la cuenta de Microsoft o la eliminación de contenidos.

Lightbeam (Firefox) -> Hacer algo visual para mostrar que al conectarte a una web hay un árbol de conexiones “extra” que desconocemos

Para hacer esto alguien que vaya a llevar el portatil (Asumo que miguel o alex.. jaja) se descargue el plugin para firefox este de aqui <https://www.mozilla.org/es-ES/lightbeam/> para luego hacer la prueba en clase