

Módulo 2. Navegación sin sobresaltos

Módulo 2. Navegación sin sobresaltos



Imagen generada con IA (Midjourney) (CC BY-NC-SA
<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

En el módulo '**Navegación sin sobresaltos**', nos adentramos en el vasto y dinámico mar de internet, preparándonos para **navegar** de manera **segura** y **discreta**.

Descubrirás cómo manejar tu **identidad digital**, evitando que cada clic sea rastreado y cada interacción analizada. Este viaje te enseñará a configurar tus dispositivos y servicios online, protegiendo tu **privacidad** en **redes sociales** y aprovechando tus **derechos digitales** para controlar la información personal que circula en la red.

A lo largo de este módulo, no solo aprenderás a identificar amenazas, sino también a ejercer control sobre cómo y quién accede a tus datos en internet.

Obra publicada con **Licencia Creative Commons Reconocimiento Compartir igual 4.0 <<http://creativecommons.org/licenses/by-sa/4.0/>>**

Módulo 2. Navegación sin sobresaltos

2.1 El arte de navegar desapercibido

La habilidad de **navegar desapercibido** no es solo una cuestión de privacidad, sino un acto consciente de autoprotección. En una era donde cada clic puede ser rastreado y cada interacción analizada, la línea entre la seguridad y la privacidad se vuelve cada vez más difusa.

Este apartado se adentra en las estrategias para mantener el **control** sobre nuestra **identidad digital**, desde el dominio de técnicas de navegación anónima hasta la configuración de nuestros dispositivos y servicios online. Se trata de entender la importancia de nuestra **huella digital**, cómo se forma y las repercusiones que puede tener en nuestra vida diaria.

A través de herramientas y conocimientos, buscamos empoderar a los usuarios para que se conviertan en artistas de la discreción digital, capaces de manejar su presencia online con inteligencia y cautela. Adentrarse en el arte de navegar desapercibido es, por tanto, un viaje hacia la autonomía y la seguridad personal en internet.



Imagen generada con IA (Midjourney)
(CC BY-NC-SA
<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)



Tras tus pasos digitales



Imagen generada con IA (Midjourney)
(CC BY-NC-SA
<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

Al navegar por internet, dejamos **huellas**: datos que reflejan nuestros intereses, comportamientos y, en última instancia, nuestra **identidad**. Este rastro no solo incluye lo que deliberadamente compartimos, sino también los **datos acumulados** en el trasfondo, muchas veces sin nuestro conocimiento explícito. La formación de nuestra huella digital es un proceso constante e inevitable en el uso diario de internet. Sin embargo, el verdadero desafío radica en la **gestión consciente** de esta huella.

Los riesgos de una huella digital amplia y mal gestionada van desde la exposición a **publicidad** altamente dirigida hasta el **robo de identidad**. Entender y tomar medidas proactivas para minimizar nuestra huella digital no es solo una práctica de seguridad; es un paso hacia la reafirmación de nuestro derecho a la privacidad personal en un entorno digital cada vez más intrusivo.

Objetivos:

- Entender la naturaleza de la huella digital y cómo cada acción online contribuye a ella.
- Conocer los principales riesgos asociados con una huella digital amplia y cómo impacta nuestra privacidad e identidad digital.

Lecturas recomendadas:

- El 64% de la población deja en la red su huella digital <<https://cybersecuritynews.es/el-64-de-la-poblacion-deja-en-la-red-su-huella-digital/>> (CyberSecurity News). Un artículo que discute cómo la mayoría de las personas dejan un rastro digital en la red y los impactos potenciales de esto.
- Facebook pulveriza la teoría de los seis grados y la sitúa en menos de cinco <<https://www.europapress.es/sociedad/noticia-facebook-pulveriza-teoria-seis-grados-situa-menos-cinco-2011122164936.html>> (Europa Press). Este artículo explora cómo las redes sociales han cambiado nuestra percepción de la conexión global, reduciendo la distancia social entre las personas.

La privacidad en internet es un tema cada vez más relevante, y dos **actores** principales contribuyen a los riesgos más significativos: **los corredores de datos y los gigantes tecnológicos**.

Los **corredores de datos** recopilan y venden información personal sin el conocimiento de las personas involucradas. Estos datos pueden incluir detalles como nombre, dirección, correo electrónico, número de teléfono, y hasta el historial de navegación. Aunque algunos corredores de datos afirman obtener su información de fuentes públicas o de compras legítimas, la falta de transparencia en sus prácticas suscita preocupaciones sobre la privacidad de los usuarios.

Por otro lado, **los gigantes tecnológicos**, como Google, Facebook, y Amazon, conocidos como **FAANG (Facebook, Amazon, Apple, Netflix, y Google)**, también plantean riesgos de privacidad. Estas empresas poseen vastas cantidades de datos de usuarios, los cuales utilizan para personalizar servicios y publicidad dirigida a los usuarios individuales. Aunque esto puede

mejorar la experiencia del usuario, también plantea preocupaciones de privacidad.

Ambos actores, corredores de datos y gigantes tecnológicos, desempeñan un papel importante en la configuración de los riesgos de privacidad en internet.

¿Alguna vez te has preguntado **cuánto valen tus datos** en el vasto mercado de la información? La respuesta podría sorprenderte. No necesitas ser una celebridad o un personaje público para que tu información sea valiosa. Desde preferencias de compra hasta datos de localización, **toda información tiene un precio**.

Para entender mejor este fenómeno, te recomendamos ver el video "**¿Por qué me vigilas si yo no soy nadie?**" <<https://www.youtube.com/watch?v=NPE7i8wuupk>>, que arroja luz sobre cómo la vigilancia digital es omnipresente, afectando a todos, sin importar qué tan "insignificante" se considere una persona en el gran esquema de Internet.

Y si aún te preguntas "**¿Vamos a ver cuánto valen esos datos?**", la **infografía** de INCIBE: "**Lo que han pedido los ciberdelincuentes a los Reyes Magos**" <<https://www.incibe.es/ciudadania/formacion/infografias/lo-que-han-pedido-los-ciberdelincuentes-los-reyes-magos>> nos ofrece una perspectiva gráfica sobre **cómo y por qué la información personal es tan codiciada** en el mercado negro. Desde datos bancarios hasta identidades completas, la demanda es alta y el negocio, lucrativo.



Incibe <<https://www.incibe.es/ciudadania/formacion/infografias/lo-que-han-pedido-los-ciberdelincuentes-los-reyes-magos>> (Dominio público)

No te desanimes frente a los desafíos planteados. Las tecnologías alternativas están experimentando un renacimiento a medida que crece la conciencia sobre los problemas de privacidad y seguridad. De hecho, para todos los problemas enumerados anteriormente, encontramos excelentes soluciones para brindarnos más privacidad, seguridad y libertad en nuestra vida digital. Y ese es el propósito de este bloque de contenido: **brindarte soluciones.**

Esto es lo que necesitas:

1. Navegador seguro y centrado en la privacidad.
2. Motor de búsqueda privado.
3. Bloqueador de anuncios.
4. Gestor de contraseñas.
5. Mensajería segura y cifrada.
6. Correo electrónico privado.
7. Configurar la privacidad de los servicios.
8. Gestionar la privacidad en redes sociales.

El punto 4 ya fue visto en el bloque anterior, apartado "1.3 Guardianes de contraseñas seguras". El resto, lo cubriremos en este bloque de contenido.



Actividad de reflexión (opcional): En la piel de un corredor de datos

Descripción: Imagina que eres un corredor de datos por un día. ¿Qué tipo de información buscarías recopilar y por qué? ¿Cómo protegerías tu propia información si estuvieras al otro lado? Discute tus ideas en el foro, reflexionando sobre la ética y la privacidad.



Bajo el hechizo de los gigantes



Imagen generada con IA (Midjourney)
(CC BY-NC-SA
<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

Los servicios gratuitos en internet nos seducen constantemente, pero detrás de esta generosidad se esconde una verdad ineludible: **cuando el servicio es gratuito, el producto eres tú.** Los gigantes tecnológicos, maestros del hechizo digital, utilizan este modelo para recopilar exhaustivamente datos sobre nuestros hábitos, preferencias y secretos más íntimos, convirtiendo lo que compartimos -y a veces lo que no- en mercancía.

Conocer y entender los mecanismos de **rastreo** es el primer paso para reclamar nuestra **privacidad digital**. Desde ajustar las configuraciones de privacidad en nuestras cuentas hasta emplear herramientas que bloquean el rastreo, hay medidas que podemos tomar para protegernos.

Objetivos:

- Entender cómo y por qué somos rastreados en línea por grandes tecnológicas y anunciantes.

- Aplicar medidas prácticas para reducir el rastreo en línea y proteger nuestra privacidad digital.

Lecturas recomendadas:

- **Internet tracking: How and why we're followed online** <<https://us.norton.com/blog/privacy/internet-tracking>> (Norton). Explica el rastreo en internet y ofrece consejos para cubrir tus huellas digitales.
- **How does online tracking actually work?** <<https://robertheaton.com/2017/11/20/how-does-online-tracking-actually-work/>> (Robert Heaton). Detalla cómo los sitios web usan cookies para rastrearte y qué puedes hacer para protegerte.

Utilizando Google como caso de estudio, este apartado explora la **profundidad y el alcance del rastreo digital**, un fenómeno no exclusivo de Google, sino una práctica común entre otros gigantes como Facebook, Instagram, TikTok, y otros muchos más.

Para empezar a revisar el seguimiento de Google, el mejor sitio es la página principal de **Controles de Actividad** <<https://myaccount.google.com/activitycontrols>> de tu cuenta de Google. Si actualmente tienes iniciada sesión en Google en tu navegador, ese enlace debería llevarte directamente a él.

Si nos vas a acompañar en esta revisión de privacidad de tu cuenta Google, sería recomendable hacerlo con tu cuenta personal, en lugar de la corporativa (g.educaand.es), ya que el tratamiento de la información es diferente en ambas.

Los datos que Google tiene sobre ti están divididos en varias secciones:

1. Análisis de búsquedas y actividad web

Google registra cada búsqueda realizada y cada sitio visitado, creando un perfil detallado de intereses y comportamientos. Puedes revisar y gestionar esta información en la página de **Controles de Actividad en la Web y en Aplicaciones** <<https://myactivity.google.com/activitycontrols/webandapp>> . Podremos ver las páginas web que hemos visitado, las búsquedas web que realizamos y las aplicaciones que hemos abierto en nuestro teléfono Android (si está enlazado a dicha cuenta).



Actividad en la Web y en Aplicaciones

Tu Actividad en la Web y en Aplicaciones incluye la actividad que llevas a cabo en los servicios de Google, como Maps, la Búsqueda y Play. También puede incluir lo que haces en sitios web, aplicaciones y dispositivos que usan los servicios de Google o tus grabaciones de voz y audio. La actividad que conservas se utiliza para ofrecerte experiencias más personalizadas, como búsquedas más rápidas y recomendaciones de aplicaciones y contenido más útiles.

En esta página puedes ver tu actividad, eliminarla manualmente o eliminarla automáticamente.
[Más información](#)

A screenshot of the 'Activity in Web and Applications' page. It shows two main sections: 'Se guarda la actividad' (which is active) and 'Eliminación automática (desactivada)' (which is inactive). Below these are buttons for 'Gestionar verificación de Mi Actividad', 'Buscar actividad', 'Filtrar por fecha y producto', and an 'Eliminar' button. At the bottom, there's a summary bar for 'Hoy'.

Si hacemos clic en filtrar por fecha y producto, se nos abrirá una pantalla en la que podemos ver todas las aplicaciones que cubre este seguimiento, desde el Asistente de Google hasta Google Play Store.

Has seleccionado 0 productos	Seleccionar todo <input type="checkbox"/>
Android	<input type="checkbox"/>
Asistente	<input type="checkbox"/>
Ayuda	<input type="checkbox"/>
Búsqueda	<input type="checkbox"/>
Búsqueda de imágenes	<input type="checkbox"/>
Búsqueda de vídeos	<input type="checkbox"/>
Chrome	<input type="checkbox"/>
Discover	<input type="checkbox"/>
Google Analytics	<input type="checkbox"/>
Google Lens	<input type="checkbox"/>
Google Play Películas	<input type="checkbox"/>

Para eliminar toda la actividad, seleccionamos el enlace "Eliminar actividad", y elegimos, desde siempre.



Actividad en la Web y en Aplicaciones

Tu Actividad en la Web y en Aplicaciones incluye la actividad que llevas a cabo en los servicios de Google, como Maps, la Búsqueda y Play. También puede incluir lo que haces en sitios web, aplicaciones y dispositivos que usan los servicios de Google o tus grabaciones de voz y audio. La actividad que conservas se utiliza para ofrecerte experiencias más personalizadas, como búsquedas más rápidas y recomendaciones de aplicaciones y contenido más útiles.

En esta página puedes ver tu actividad, eliminarla manualmente o eliminarla automáticamente.
[Más información](#)

No se guarda la actividad >

El ajuste Actividad en la Web y en Aplicaciones está desactivado

Eliminación automática (desactivada) >

Elegir una opción de eliminación automática

Google protege tu privacidad y seguridad. [Gestionar verificación de Mi Actividad](#)

Buscar actividad

Filtrar por fecha y producto

Eliminar

Para desactivar este seguimiento, hacemos clic en el botón "Se guarda la actividad".



Actividad en la Web y en Aplicaciones

Tu Actividad en la Web y en Aplicaciones incluye la actividad que llevas a cabo en los servicios de Google, como Maps, la Búsqueda y Play. También puede incluir lo que haces en sitios web, aplicaciones y dispositivos que usan los servicios de Google o tus grabaciones de voz y audio. La actividad que conservas se utiliza para ofrecerte experiencias más personalizadas, como búsquedas más rápidas y recomendaciones de aplicaciones y contenido más útiles.

En esta página puedes ver tu actividad, eliminarla manualmente o eliminarla automáticamente.
[Más información](#)

Se guarda la actividad >
El ajuste Actividad en la Web y en Aplicaciones está activado
La función para guardar la actividad de audio está desactivada

Eliminación automática (desactivada) >
Elige una opción de eliminación automática

Google protege tu privacidad y seguridad. [Gestionar verificación de Mi Actividad](#)

Buscar actividad

Filtrar por fecha y producto

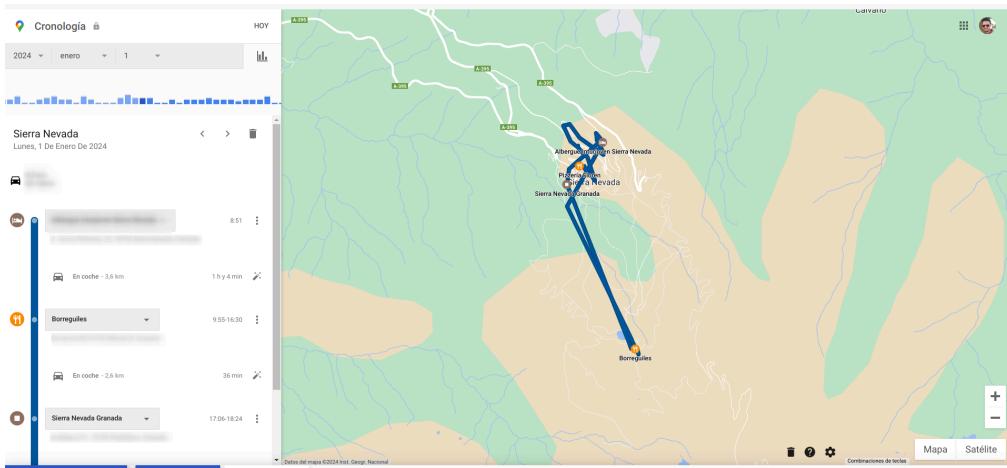
Eliminar

Hoy

2. Historial de ubicaciones

A través de nuestros dispositivos móviles, Google puede seguir nuestros movimientos, ofreciendo servicios basados en la ubicación, pero también compilando un historial detallado de nuestros hábitos y preferencias geográficas. Para ver y gestionar tu historial de ubicaciones, visita la [Línea de tiempo de Google Maps <https://www.google.com/maps/timeline>](https://www.google.com/maps/timeline).

En este caso los registros se muestran en un mapa; puedes ver los pequeños puntos que marcan los lugares en los que has estado y usar el menú desplegable, en la parte superior izquierda, para ver un rango de fechas más específico.



Si has realizado algún viaje mientras esta opción estaba activada, busca el punto en el mapa y haz clic en él. En el menú de la izquierda, podrás ver en detalle lo que hiciste, los sitios que visitaste, las horas, las fotografías que tomaste y mucha más información relevante. Aunque pueda parecer divertido al principio, una reflexión más profunda revela un serio problema de privacidad.

Para borrar estos datos de los registros de Google, haga clic en el ícono de la papelera en la parte inferior. Si, por el contrario, quieres desactivar el seguimiento y eliminar toda la actividad, puedes hacerlo en la página de **Controles de Actividad del Historial de ubicaciones** <https://myactivity.google.com/activitycontrols?settings=location&utm_source=my-activity> .

Controles de actividad

Los datos guardados en tu cuenta te permiten disfrutar de todos los servicios de Google de una forma más personalizada. Elige qué ajustes quieras que guarden datos en tu cuenta de Google.

The screenshot shows the 'Historial de ubicaciones' (Location History) section of the Google Activity Controls. It features a smartphone icon with a map and location pins. A red box highlights the 'Desactivar' (Disable) button, which is currently set to 'Activado' (Enabled). Below it, a note says 'Activado desde el 17 de abril de 2024'. Other sections visible include 'Dispositivos en esta cuenta' (Devices in this account), 'Eliminación automática (desactivada)' (Automatic deletion (disabled)), and 'Gestionar historial' (Manage history).

Más seguridad con Google
Tú controlas qué datos se guardan en tu cuenta. [Más información](#)

Más seguridad con Google
Tú controlas qué datos se guardan en tu cuenta. [Más información](#)

Historial de ubicaciones

Guarda los sitios a los que vas con tus dispositivos (aunque no estés usando ningún servicio específico de Google) para ofrecerte, por ejemplo, mapas personalizados o recomendaciones basadas en los sitios que has visitado. [Más información](#)

Activado
Activado desde el 17 de abril de 2024

[Desactivar](#)

Dispositivos en esta cuenta

Eliminación automática (desactivada)

Elige una opción de eliminación automática

Gestionar historial

Nota: La cronología de la versión web de Google Maps va a dejar de estar disponible. Es posible que para consultar tu cronología tengas que hacerlo a través de la aplicación Google Maps.

3. Historial de YouTube

Esta sección cubre, como dice su nombre, el Historial de búsquedas y reproducciones de YouTube. Tenemos la opción de borrar los registros a través del enlace **Gestionar actividad de Youtube <https://myactivity.google.com/product/youtube?utm_source=my-activity>** o de desactivar el seguimiento en la página de **Controles de actividad del Historial de ubicaciones <https://myactivity.google.com/activitycontrols?settings=youtube&utm_source=my-activity&fac=1>**.

Controles de actividad

Los datos guardados en tu cuenta te permiten disfrutar de todos los servicios de Google de una forma más personalizada. Elige qué ajustes quieras que guarden datos en tu cuenta de Google.

 Más seguridad con Google
Tú controlas qué datos se guardan en tu cuenta. [Más información](#)



Historial de YouTube
Guarda los videos de YouTube que ves y las búsquedas que realizas en YouTube para ofrecerte mejores recomendaciones, retomar sesiones y más. [Más información](#)

Activado Desactivar

Ajustes secundarios

Incluir los videos que ves en YouTube

Incluir las búsquedas que haces en YouTube

Incluir actividad de voz y audio de YouTube

Eliminación automática (desactivada)

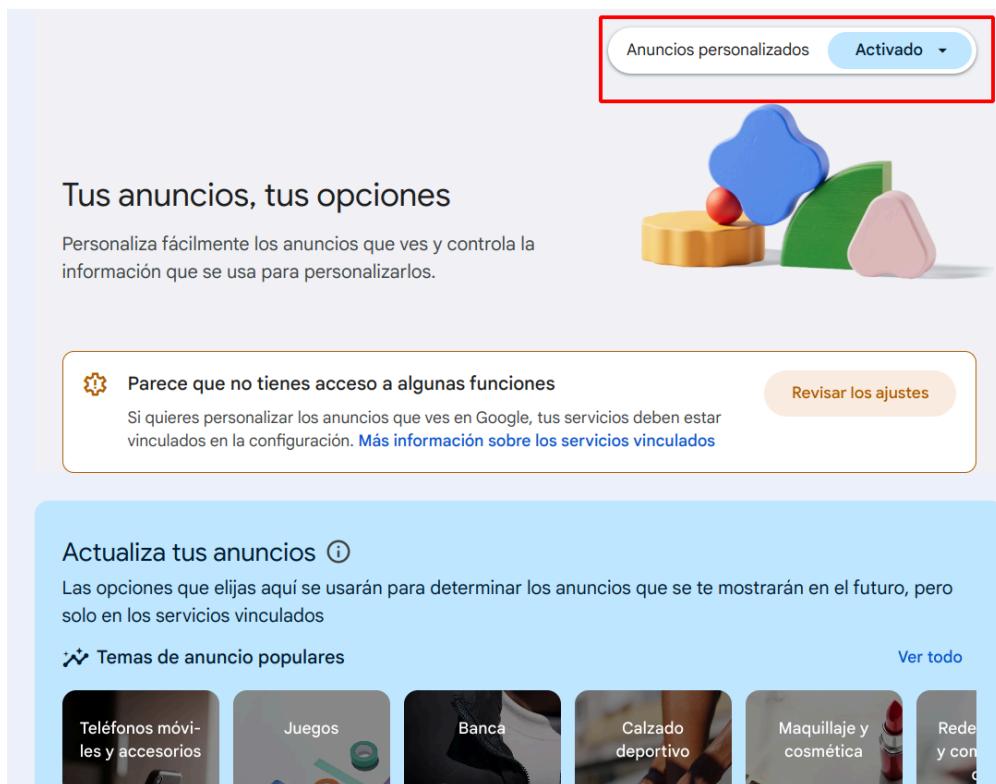
 Elige una opción de eliminación automática >

[Gestionar historial](#)

4. Anuncios dirigidos

Anteriormente estuvimos hablando de publicidad dirigida, veamos qué registra Google al respecto. Dirígete a **Mi centro de anuncios** https://go.skimresources.com/?id=100099X1555751&isjs=1&jv=15.5.0&sref=https%3A%2F%2Fwww.wired.com%2Fstory%2Fgoogle-tracks-you-privacy%2F&url=https%3A%2F%2Fadssettings.google.com%2Fauthenticate&xs=1&xtz=-120&xuuid=d1487914f1c050102bba5d019cad14c6&xjsf=other_click_contextmenu%20%5B2%5D

para ver el perfil publicitario que Google ha creado sobre ti. Igualmente, como hemos visto en las secciones anteriores, puedes eliminar la actividad y desactivar el seguimiento.



5. Dispositivos móviles

Todavía no hemos hablado de teléfonos móviles. Los principales datos que Google recopila a través de teléfonos se refieren a la ubicación, aunque obviamente también los rastrea a través de sus aplicaciones (Gmail, Google Docs, Google Maps), tal como lo hace en la web.

- En **Android**, ve al menú "Configuración" y luego selecciona "Google" para modificar algunas opciones de seguimiento de datos.
- En **iOS**, Google no tiene tanta "libertad" en el sistema operativo, como cabría esperar. Si abres la aplicación de Google para iOS, toca los tres puntos en la parte inferior derecha y luego elige Privacidad y Seguridad, ahí podrás evitar que Google rastree su ubicación en este dispositivo en particular.

Al sumergirnos en el universo de Google, hemos descubierto que almacena datos desde nuestras búsquedas web hasta nuestros movimientos en el mundo real. El debate se podría centrar en dos aspectos: primero, la **extensa cantidad de datos que Google recopila** sobre los usuarios; y segundo, el uso que Google da a esos datos. Mientras Google argumentará que esta recopilación de datos enriquece sus servicios, como personalizar recomendaciones de restaurantes, los usuarios podrían tener opiniones encontradas sobre estas prácticas.

Para comprender la razón detrás de este seguimiento, basta con observar a las cuentas anuales de la empresa. En 2023, **sus ingresos publicitarios ascendieron a \$237.85 billones <<https://fourweekmba.com/es/cuanto-dinero-gana-google-con-la-publicidad/>>**, lo que representa el 77,4% de sus ingresos totales para ese año. Los ingresos publicitarios de Google se generan principalmente a través de su motor de búsqueda y la plataforma YouTube, que juntos representaron más del 90% de sus ingresos publicitarios en 2023.

En resumen, **Google es fundamentalmente una empresa de publicidad**. El éxito del modelo de negocio proviene de su capacidad para crear un ecosistema de servicios y aplicaciones que ofrecen a los usuarios de manera gratuita. Para impulsar esos anuncios, el navegador Chrome (y el motor de búsqueda de Google) recopilan la mayor cantidad de datos posibles sobre los usuarios. Luego "monetizan" estos datos en forma de anuncios altamente dirigidos. **Cuanto más saben sobre ti, más dinero ganan.**

Aunque vivimos en una era donde la recolección de datos por parte de las grandes tecnologías es común, **no significa que tengamos que renunciar a los servicios que enriquecen nuestro día a día**, la clave reside en **tomar medidas proactivas** para proteger nuestra privacidad. Una de estas medidas es la que acabamos de ver, configurar adecuadamente nuestros servicios para minimizar el impacto en nuestra información personal.

A continuación, seguiremos profundizando en estas y otras estrategias, ofreciendo un enfoque práctico y efectivo.

Actividad (opcional): Exploración de privacidad digital

Descripción: Esta actividad guía a los participantes a través de la revisión y ajuste de las configuraciones de privacidad en sus cuentas de Google, enfocándose en entender qué datos son recopilados y cómo gestionarlos.

Pasos:

1. Acceder a la página de controles de actividad de Google.
2. Revisar y ajustar las configuraciones de recopilación de datos para cada categoría.
3. Desactivar el seguimiento de ubicación, actividad en la web y en aplicaciones.

Recursos necesarios:

- Enlace a controles de actividad:
<https://myaccount.google.com/activitycontrols>
[<https://myaccount.google.com/activitycontrols>](https://myaccount.google.com/activitycontrols)



Elige sabiamente



Imagen generada con IA (Midjourney)
(CC BY-NC-SA)

Nuestra selección de **herramientas digitales**, desde navegadores hasta motores de búsqueda, juega un rol fundamental en la protección de nuestra privacidad. Frente a la omnipresencia de grandes corporaciones tecnológicas, emergen **alternativas** diseñadas con un enfoque en la **seguridad** del usuario y el **respeto** por su **información personal**.

Este apartado se dedica a explorar estas opciones, destacando la necesidad de

<<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>>)

elegir conscientemente aquellas herramientas que no solo nos ofrecen una navegación eficiente, sino que también garantizan la confidencialidad de nuestros datos y minimizan el seguimiento no deseado.

Objetivos:

- Comprender la diferencia entre navegadores y motores de búsqueda, y cómo esta elección afecta nuestra privacidad.
- Identificar alternativas seguras a los navegadores y motores de búsqueda convencionales que priorizan la privacidad del usuario.

Lecturas recomendadas:

- **TOP +10: Seguridad, privacidad y navegación** <<https://ciberseguridadtips.com/cual-navegador-seguro-privado/>> (Ciberseguridad Tips). Una exploración de las mejores prácticas y herramientas para mejorar la seguridad y la privacidad en línea.
- **Los 6 Navegadores Más Seguros para Mantenerse a Salvo y Proteger Tu Privacidad en 2024** <<https://kinsta.com/es/blog/navegador-mas-seguro/>> (Kinsta). Un análisis de navegadores que ofrecen robustas características de seguridad y privacidad, ayudando a proteger tus datos personales.

A menudo, estos términos se usan indistintamente, pero tienen roles diferentes. El **navegador** es la aplicación que usamos para acceder y navegar

por internet, **Google Chrome**, **Mozilla Firefox**, **Safari**, entre otros. Por otro lado, el **motor de búsqueda** es el servicio usado dentro del navegador para buscar información en la web, utilizando palabras clave para obtener resultados relevantes. **Google**, **Bing** y **DuckDuckGo** son ejemplos de motores de búsqueda.

Simplificándolo, podemos decir que el navegador es la puerta de entrada a internet, y el motor de búsqueda es una herramienta que se encuentra dentro de esa puerta, ayudando a los usuarios a encontrar la información que necesitan en internet.

¿Cuál es el motor de búsqueda predeterminado de cada navegador? Aquí está la lista para todos los principales navegadores:

- **Chrome**: Google.
- **Firefox**: Google (antes Yahoo).
- **Edge**: Bing.
- **Internet Explorer**: Bing.
- **Safari**: Google.
- **Opera**: Google.

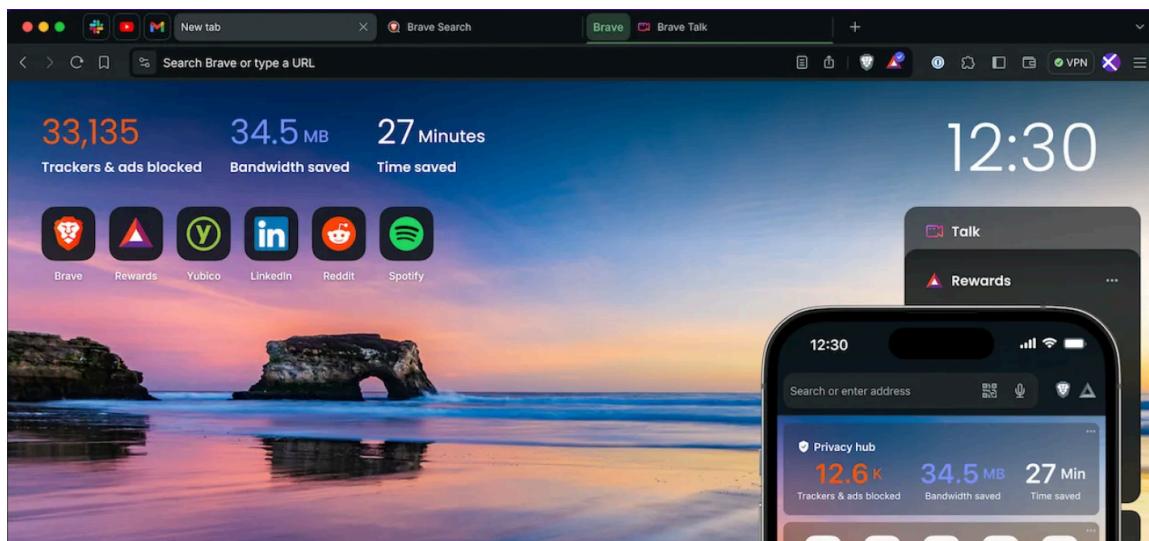
Aunque estas herramientas deberían proteger nuestra intimidad, lamentablemente, en muchas ocasiones son usadas para lo contrario. La buena noticia es que **podemos elegir qué navegador usar** y que **todos los navegadores estándar permiten cambiar el motor de búsqueda** que utilizan. A continuación, vamos a explorar las opciones que tenemos en cada una de ellas para proteger nuestra privacidad.

Los navegadores, a menos que se configuren correctamente, **contienen mucha información privada que puede ser explotada** (o simplemente

recopilada) por terceros:

- **Historial de navegación:** todos los sitios web que visitas.
- **Credenciales** de inicio de sesión: nombres de usuario y contraseñas.
- **Cookies y rastreadores:** los sitios que visitas.
- **Información de autocompletar:** nombres, direcciones, números de teléfono, etc.

Aquellos preocupados por su privacidad deberían considerar **alternativas** diseñadas específicamente con ese objetivo en mente. **Brave Browser** <<https://brave.com/>> es posiblemente el **navegador más seguro con una privacidad sencilla** y lista para usar. Tiene un bloqueador de anuncios integrado y protección de huellas digitales del navegador. Si estás interesado en conocer más sobre Brave, te recomendamos consultar **este artículo** <<https://www.xataka.com/tag/brave>> .



Brave Browser (Dominio público)

¿Prefieres seguir usando un navegador tradicional? Aún puedes mejorar tu privacidad online realizando algunos cambios, ajustando la configuración y usando algunos complementos.

¿Qué navegador elijo?

Todos los navegadores ofrecen ajustes de privacidad, pero varían en profundidad y facilidad de uso. **Mozilla Firefox** destaca por sus **robustas funciones de privacidad, seguridad** y su naturaleza de código abierto, desarrollado por una comunidad activa. Es considerado uno de los mejores

en términos de privacidad y seguridad entre los navegadores tradicionales, y además, es altamente personalizable.

Aunque Mozilla Firefox es uno de los navegadores más recomendables, lograr la máxima protección requiere ajustes y configuraciones extras. Para aquellos interesados en optimizar su privacidad, siguiendo esta **guía** <<https://restoreprivacy.com/firefox-privacy/>> podrán hacer de Firefox una fortaleza de privacidad.

Para quienes prefieran otras opciones o deseen evitar configuraciones complejas, **a continuación revisaremos ajustes imprescindibles en distintos navegadores.**

Quizás al leer el apartado anterior, has pensado que no necesitamos tomar medidas porque los navegadores tienen un modo incógnito. Sin embargo, el **modo incógnito** de los navegadores ha sido objeto de numerosos **mitos y malentendidos** en cuanto a su capacidad para proteger la privacidad en línea.

Existe una **creencia común** de que el uso del modo incógnito en los navegadores **garantiza una total privacidad en línea**. Sin embargo, esta **percepción es errónea**. Aunque el modo incógnito evita que el navegador almacene el historial de navegación, las cookies y los registros de búsqueda en el dispositivo local, no impide que los sitios web recopilen y utilicen datos sobre la actividad del usuario con fines como la publicidad dirigida y el seguimiento. Incluso, **Google ha confirmado que el modo incógnito no es privado** <<https://www.abc.es/tecnologia/google-confirma-modo-incognito-privado-eliminara-datos-20240402100631-nt.html>> .

¿Quiere decir esto que no debemos usar el modo incógnito? No necesariamente. Simplemente es importante entender que en lo que

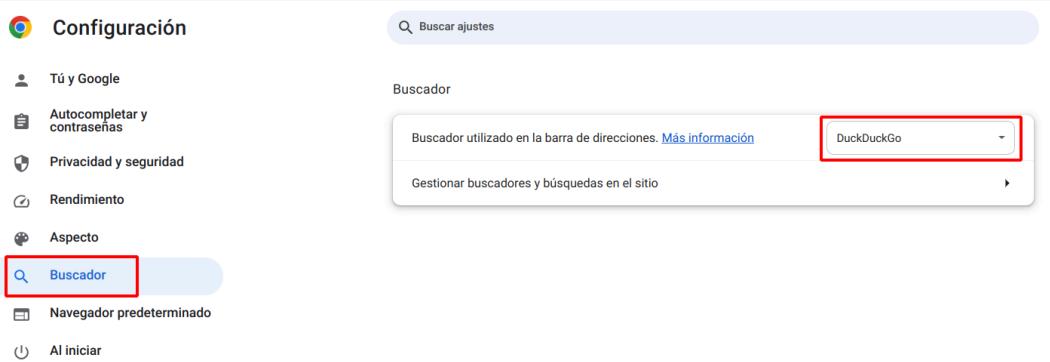
respecta a la privacidad, no nos garantiza la total confidencialidad de nuestros datos.

Vamos a por el **primer paso, cambiar el motor de búsqueda predeterminado por uno más respetuoso con nuestra privacidad**. Alternativas como **DuckDuckGo <<https://duckduckgo.com/>>**, un motor de búsqueda dedicado a proteger tu anonimato, presentan una opción muy interesante. Para conocer más sobre DuckDuckGo y su enfoque en la privacidad, puedes visitar **este enlace <<https://www.xataka.com/basics/duckduckgo-que-principales-diferencias-google>>**.

A continuación, veremos cómo cambiar el motor de búsqueda en algunos de los navegadores más populares:

- **Google Chrome:**

1. Abre Chrome y dirígete a Configuración.
2. Busca el apartado de "Buscador".
3. En el menú desplegable de "Buscador predeterminado", elige el que quieras usar.



Licencia: Dominio público

- **Mozilla Firefox:**

1. En Firefox, accede a Ajustes.
2. Entra en la sección de "Buscar".
3. En el menú desplegable de "Buscador predeterminado", elige el que quieras usar.



Licencia: Dominio público

- **Microsoft Edge:**

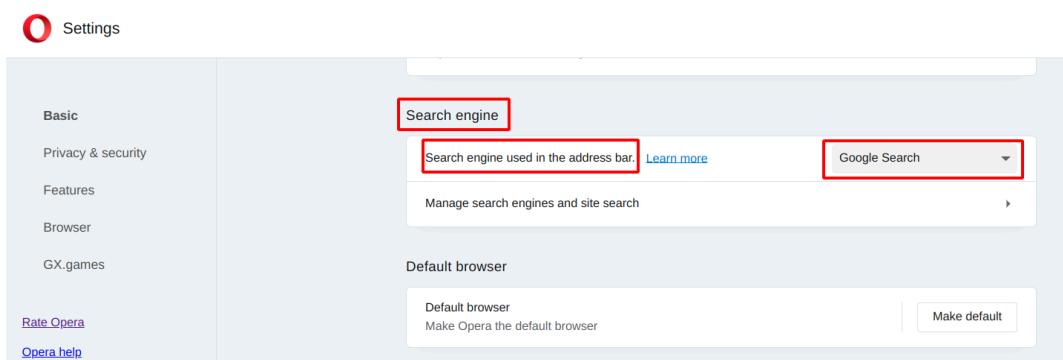
1. Abre Edge y ve a Configuración.
2. Selecciona "Privacidad, búsqueda y servicios".
3. Desplázate hasta "Barra de direcciones y búsqueda" y cambia el motor de búsqueda predeterminado.



Licencia: Dominio público

- **Opera:**

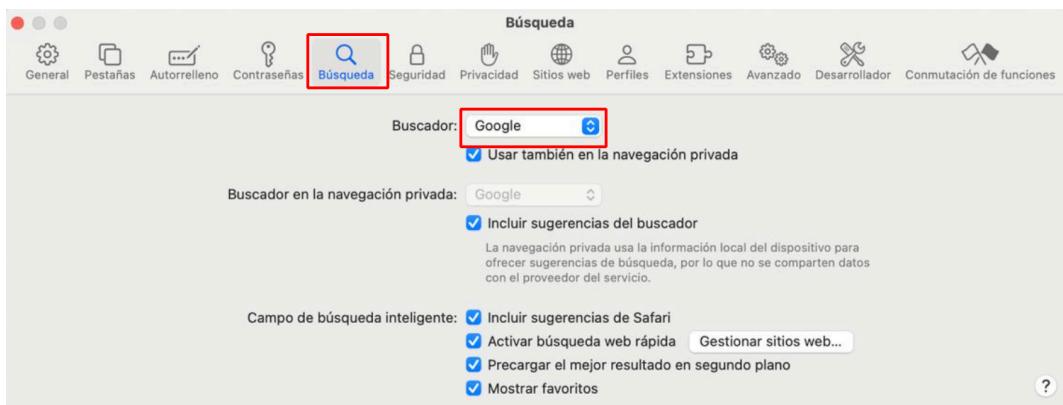
1. Abre Opera y ve a Configuración.
2. Busca la sección "Search engine".
3. En el menú desplegable de "Search engine used in the address bar.", elige el que quieras usar.



Licencia: Dominio público

- **Safari (en macOS):**

1. Abre Safari y dirígete a Ajustes.
2. Selecciona la pestaña "Búsqueda".
3. En el menú desplegable de "Buscador", elige el que quieras usar.



Licencia: Dominio público

Nota. Las instrucciones que se proporcionan pueden cambiar ligeramente en función de la versión del sistema operativo y del navegador.

A continuación, encontrarás cómo ajustar la configuración de privacidad en algunos de los navegadores más populares:

- **Google Chrome:** Accede a "Configuración" > "Privacidad y seguridad" para gestionar cookies y el rastreo.
- **Mozilla Firefox:** En "Opciones" > "Privacidad & Seguridad", Firefox ofrece controles detallados sobre el rastreo y las cookies.
- **Microsoft Edge:** Ve a "Configuración" > "Privacidad, búsqueda y servicios" para ajustar configuraciones relacionadas con la privacidad.
- **Safari:** En "Preferencias" > "Privacidad", Safari permite gestionar cookies y el rastreo.
- **Opera:** Ofrece configuraciones de privacidad en "Configuración" > "Privacidad y seguridad", incluyendo el bloqueo de anuncios y una VPN gratuita integrada.

Para cada navegador, considera las siguientes recomendaciones generales:

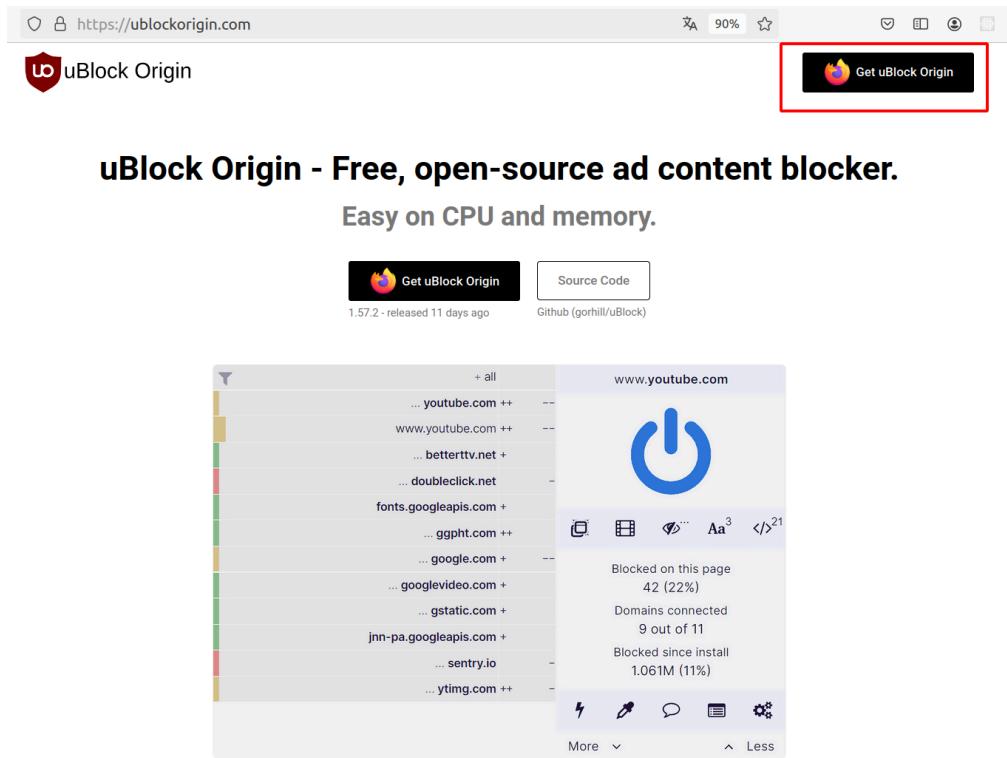
- **Bloquear cookies de terceros:** Limita el seguimiento de tus hábitos de navegación.
- **Activar la protección contra rastreo (Do not track):** Una función que te permite navegar por internet con mayor privacidad, solicitando a las páginas web que no rastreen tu actividad en línea.

- **Revisar las configuraciones de seguridad y privacidad regularmente:** Las actualizaciones del navegador pueden modificar estas configuraciones.

Los **anuncios** no son solo molestias visuales; son **herramientas de seguimiento**. Registran tu actividad en línea para crear perfiles detallados de usuario. Estos perfiles pueden ser utilizados para mostrarte publicidad dirigida o incluso ser vendidos a terceros. Además del rastreo, los anuncios pueden ser **vehículos para malware**. Algunos pueden contener scripts maliciosos que se activan al cargar la página, sin necesidad de clics por tu parte.

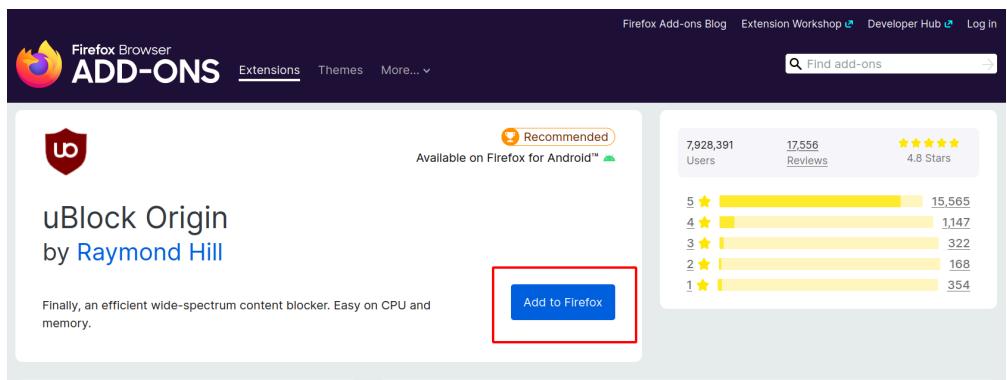
Existen **extensiones** para los navegadores **muy eficaces bloqueando la publicidad**, sin embargo, tenemos que elegir con cuidado, algunas recopilarán datos del usuario con fines de lucro y/o nos mostrarán anuncios "aprobados". La extensión **uBlock Origin** es una de las mas populares, está disponible para navegadores Firefox, Safari, Microsoft Edge, Chromium y Google Chrome. Funciona tanto en modo de navegación normal como en modo incógnito.

Para instalarla, hacemos clic en **uBlock Origin <<https://ublockorigin.com/>>** para acceder a la página web de la herramienta. Automáticamente detectará el navegador desde el que hemos accedido y nos mostrará un botón para instalarla:



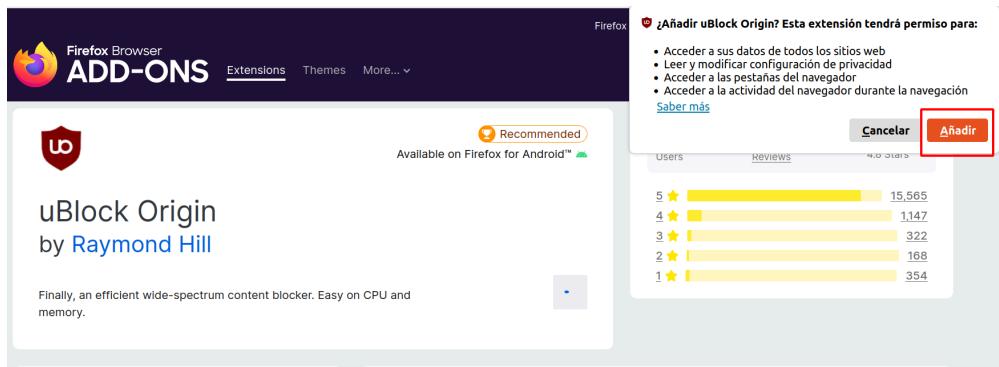
uBlock Origin (Dominio público)

Se nos abrirá una ventana con un botón para añadirla al navegador:



uBlock Origin (Dominio público)

Nos vuelve a preguntar si queremos añadirla al navegador:



uBlock Origin (Dominio público)

Si nos fijamos en la parte superior derecha del navegador, ya vemos la extensión instalada y activa:



uBlock Origin (Dominio público)

Navegamos por internet y veremos que aparece un número en el ícono de la extensión, es el número de ventanas publicitarias que ha bloqueado:



uBlock Origin (Dominio público)

Importante: "uBlock Origin" no es el mismo producto que "uBlock", que es un bloqueador de anuncios de nombre similar, que permite "anuncios aceptables" a cambio de un pago.

Actividad (opcional): Configuración de privacidad en acción

Descripción: Aprende a ajustar la configuración de privacidad en tu navegador favorito para mejorar tu seguridad en línea.

Pasos:

1. Selecciona tu navegador de uso diario.
2. Busca cómo ajustar la configuración de privacidad y seguridad.
3. Realiza los ajustes recomendados en los materiales.

Recursos necesarios:

- Conexión a internet.
- Navegador web.
- Acceso a los materiales del curso.



Recursos educativos



Imagen generada con IA (Midjourney) (CC BY-NC-SA
<<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>>)

Explora estos **recursos** para enseñar ciberseguridad: actividades, lecturas y más, diseñados para **promover** la **privacidad digital** entre nuestros estudiantes.

- **Doxing.** Infografía que explica qué es el doxing, sus riesgos y cómo protegerte de esta práctica. [Descargar la infografía <https://www.incibe.es/sites/default/files/docs/infografia-doxing-practica-revelar-informacion-terceros.pdf>](https://www.incibe.es/sites/default/files/docs/infografia-doxing-practica-revelar-informacion-terceros.pdf) .
- **Borra tu huella.** Vídeo con consejos prácticos para minimizar tu huella digital en internet. [Ver vídeo <https://www.youtube.com/watch?v=FT1FjR1XQ2w>](https://www.youtube.com/watch?v=FT1FjR1XQ2w) .
- **Identidad digital. ¿Quiénes somos en la red?** Reflexión sobre la importancia de nuestra identidad digital a través de un vídeo educativo. [Ver vídeo <https://www.youtube.com/watch?v=rNmXiYY9iHA>](https://www.youtube.com/watch?v=rNmXiYY9iHA) .

- **Cómo disminuir tu rastro en Internet.** Guía en PDF con estrategias para reducir tu huella digital. Descargar la guía [<https://www.incibe.es/sites/default/files/docs/c00-eg-disminuir_tu_rastro_0.1.pdf>](https://www.incibe.es/sites/default/files/docs/c00-eg-disminuir_tu_rastro_0.1.pdf).
 - **Servicios online, datos personales y derechos.** Explica la protección de datos personales en servicios online mediante un vídeo. Ver vídeo [<https://www.youtube.com/watch?v=agnTAcAlvKM>](https://www.youtube.com/watch?v=agnTAcAlvKM).
 - **Memory de la Privacidad.** Juego de memoria sobre conceptos de privacidad para aprender jugando. Acceso a la página del juego [<https://www.incibe.es/ciudadania/juegos/juegos-mesa/memory-privacidad>](https://www.incibe.es/ciudadania/juegos/juegos-mesa/memory-privacidad).
 - **Criptópolis. El juego de gestión y ciberseguridad.** Juego en PDF para aprender sobre ciberseguridad de forma lúdica. Descargar PDF [<https://www.incibe.es/sites/default/files/docs/osi-criptopolis.pdf>](https://www.incibe.es/sites/default/files/docs/osi-criptopolis.pdf).
 - **Configuraciones básicas de privacidad y seguridad en videoconsolas.** Guía con pasos para configurar la privacidad y seguridad en consolas de videojuegos. Ver guía [<https://www.incibe.es/ciudadania/formacion/actividades/configuracion-es-basicas-de-privacidad-y-seguridad-en-videoconsolas>](https://www.incibe.es/ciudadania/formacion/actividades/configuracion-es-basicas-de-privacidad-y-seguridad-en-videoconsolas).
 - **Interland.** Juego que fomenta compartir contenido con precaución. Acceso a la página del juego [<https://beinternetawesome.withgoogle.com/es-419_all/interland>](https://beinternetawesome.withgoogle.com/es-419_all/interland).
-

Obra publicada con Licencia Creative Commons Reconocimiento Compartir igual 4.0 <<http://creativecommons.org/licenses/by-sa/4.0/>>

Módulo 2. Navegación sin sobresaltos

2.2 Las redes sociales como contextos sensibles

Según los datos proporcionados por el **Instituto Nacional de Estadística <<https://ine.es/>>** (INE) en su último informe sobre el uso de redes sociales en España, el **83,6% de la población** total del país (39,7 millones de personas) **utiliza al menos una red social**.

Además, los usuarios españoles dedican **una media de 1 hora y 53 minutos al día** a estas plataformas, siendo las más utilizadas WhatsApp y Facebook, con un 91% y un 73,3% respectivamente, seguido de Instagram con un 71,7%. Otro dato interesante del informe es que **cada usuario** de redes sociales en España utiliza de **media 6 plataformas** diferentes.

Las redes sociales se han convertido en **plataformas esenciales** para la interacción humana, pero también en **espacios sensibles** donde la privacidad puede ser vulnerada. Este apartado se centra en **entender y mitigar los peligros** en estos espacios digitales, abordando desde la configuración de privacidad hasta estrategias de protección contra comportamientos malintencionados.



Imagen generada con IA (Midjourney)
(CC BY-NC-SA <<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>>)



Más que un perfil



Imagen generada con IA (DALL-E) (CC BY-NC-SA
<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

intrínsecas a su arquitectura social: la sobreexposición de información personal, la fluidez de la comunicación y la confianza en las relaciones online.

Ante estos desafíos, es necesario que adoptemos una postura proactiva para proteger nuestra **identidad digital**.

Objetivos:

- Comprender cómo las redes sociales recopilan y utilizan datos personales, y los riesgos asociados con la sobreexposición de información personal en plataformas digitales.
- Desarrollar una conciencia crítica sobre el impacto de nuestras interacciones en las redes sociales en nuestra privacidad.

Lecturas recomendadas:

Las **redes sociales**, vistas como extensiones de nuestra identidad, también pueden convertirse en **dobles filos digitales**. Ofrecen un espacio para la expresión y la interacción, pero también actúan como potentes **recolectores de datos** personales, diseminando nuestras huellas digitales en una red vasta e invisible llena de intereses comerciales.

Además, las redes sociales pueden ser utilizadas por cibercriminales para comprometer nuestra seguridad, explotando vulnerabilidades

- We need to rethink social media before it's too late <<https://www.theguardian.com/commentisfree/2020/sep/27/social-dilemma-media-facebook-twitter-society>> (The Guardian). Un artículo de The Guardian que reflexiona sobre la necesidad de replantear nuestro enfoque hacia las redes sociales para proteger la sociedad y la privacidad individual.
- **Privacidad en redes sociales: ¿Qué hacen realmente con nuestros datos?** <<https://intelectual.org/propiedad-intelectual-y-tecnologia/privacidad-redes-sociales-hacen-realmente-nuestros-datos/>> (Intelectual.org). Una mirada detallada de Intelectual.org sobre cómo las redes sociales gestionan y utilizan nuestra información personal, subrayando la importancia de la conciencia y la protección de la privacidad en el entorno digital.

Actividad (opcional): Descubre la información que compartes en redes sociales

Descripción: ¿Alguna vez te has detenido a considerar la cantidad de información personal que compartes en tus perfiles de redes sociales? Ya sea porque confías en la configuración de privacidad de tus perfiles o creas que la información que compartes no le interesa a nadie, te invitamos a reflexionar sobre lo siguiente:

- ¿Conoces a todos tus contactos en redes sociales? ¿Te sentirías cómodo compartiendo tus asuntos más privados con esas personas?
- ¿Estás al tanto de que las redes sociales pueden utilizar la información que publicas para fines publicitarios o compartirla con terceros?
- ¿Comprendes que la información que compartes puede ser de interés para una amplia gama de personas, incluidos los ciberdelincuentes?

Para tener una mejor comprensión del volumen de información que compartimos, te animamos a descargar tus datos de una red social. A continuación, te proporcionamos enlaces sobre cómo hacerlo en cada una de las principales plataformas:

- Para Facebook: **Instrucciones para descargar datos de Facebook** <<https://es-la.facebook.com/help/212802592074644>>

- Para Instagram: **Instrucciones para descargar datos de Instagram** <<https://es-la.facebook.com/help/instagram/181231772500920>>
- Para X (Twitter): **Instrucciones para descargar datos de Twitter** <<https://help.twitter.com/es/managing-your-account/accessing-your-x-data#:~:text=En%20la%20app%20de%20X%20para%20iOS%20o,Confirmar%20tu%20contrase%C3%B1a%2C%20luego%20pulsa%20Solicita%20tu%20archivo.>>
- Para TikTok: **Instrucciones para descargar datos de TikTok** <<https://support.tiktok.com/es/account-and-privacy/personalized-ads-and-data/requesting-your-data>>
- Para LinkedIn: **Instrucciones para descargar datos de LinkedIn** <<https://www.linkedin.com/help/linkedin/answer/a1340367/descargar-los-datos-de-tu-cuenta?lang=es-ES>>

Nota: Ten en cuenta que cada red social puede tener un proceso diferente para solicitar y recibir tus datos personales. Algunas plataformas pueden tardar varios días en procesar tu solicitud. Te recomendamos leer bien las instrucciones y tener paciencia.



Tu perfil a prueba de intrusos



La **privacidad** en las **redes sociales** es un tema muy relevante en la sociedad actual. Este apartado está dedicado a enseñarte cómo ajustar la configuración de seguridad y privacidad en tus redes sociales favoritas. Aprenderás a controlar quién ve tus publicaciones y cómo acceden a tu información personal.

Imagen generada con IA (Midjourney)
(CC BY-NC-SA
<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

A través de pasos claros y concisos, exploraremos opciones para **limitar la visibilidad** de tus publicaciones y regular el acceso a tus publicaciones. La meta es empoderarte para que ejerzas un control sobre tu perfil, convirtiéndolo en un refugio seguro.

Objetivos:

- Optimizar la configuración de privacidad y seguridad de los perfiles en redes sociales para proteger la información personal y limitar la visibilidad de las publicaciones.
- Implementar medidas de seguridad para proteger tu cuenta de accesos no autorizados y minimizar riesgos de sobreexposición digital.

Lecturas recomendadas:

- **Privacidad en las redes sociales: ¿Qué hacen realmente con nuestros datos?** <https://blog.internxt.com/es/privacidad-en-las-redes-sociales/> (Internxt Blog). Un análisis profundo sobre cómo las redes sociales gestionan y utilizan nuestra información personal, con énfasis en la importancia de proteger nuestra privacidad.
- **Social Media Security: What You Need to Know** <https://buffer.com/resources/social-media-security/> (Buffer). Explora los tipos de amenazas a la seguridad en redes sociales y ofrece consejos para proteger tu información personal.

La privacidad en las redes sociales se refiere a la protección y manejo de nuestra información personal divulgada en línea, como fotos, mensajes y datos de contacto. Al aumentar la cantidad de información compartida, crece el riesgo de su uso indebido o divulgación sin nuestro consentimiento.

La ciberseguridad, por su parte, se enfoca en resguardar nuestros dispositivos e información en línea de ataques cibernéticos, como virus, malware, phishing y otras amenazas. El incremento de la información compartida en redes eleva nuestra susceptibilidad a estos peligros.

La privacidad en redes sociales y la ciberseguridad están estrechamente relacionadas, sin medidas de seguridad adecuadas, nuestra privacidad puede verse comprometida. Por ejemplo, si no protegemos nuestras cuentas de redes sociales con una contraseña robusta, corremos el riesgo de que nuestra información sea accedida por personas no autorizadas.

¡Tenemos buenas noticias para ti! La mayoría de las medidas de seguridad esenciales para proteger tus cuentas en redes sociales ya las cubrimos en el módulo 1. Esto incluye la creación de contraseñas fuertes y únicas, la implementación de la autenticación de dos factores (2FA), y la actualización regular de las aplicaciones. Estas estrategias forman la base de una sólida defensa digital en cualquier plataforma.

Las únicas **medidas adicionales** para redes sociales, como la **prevención de estafas**, las abordaremos con más detalle en el **módulo 3**. Por lo tanto, ¡ya estás en buen camino para asegurar tus redes sociales contra accesos no autorizados y otros riesgos de seguridad!

Con la rapidez con la que cambian las políticas y funcionalidades de las plataformas sociales, crear guías detalladas sobre ajustes de privacidad podría resultar en información rápidamente desactualizada. Este apartado ofrece directrices generales y recursos específicos para asegurar tu privacidad online.

Directrices generales:

- **Personaliza tu configuración de privacidad.** Opta siempre por configuraciones personalizadas en lugar de las predeterminadas. Esto te permite tener un mayor control sobre quién ve tu información.
- **Revisa regularmente tu configuración de privacidad.** Las políticas y configuraciones de las plataformas cambian regularmente. Es importante revisar tus configuraciones de privacidad periódicamente para asegurarte de que siguen siendo efectivas.
- **Desactiva la geolocalización.** La ubicación puede revelar más información sobre ti de lo que podrías imaginar. Es recomendable desactivar esta función cuando no sea necesaria.

Ajustes de gestión de privacidad por plataforma:

Aquí encontrarás enlaces directos a las secciones de configuración de privacidad de las redes sociales más populares, que te permitirán ajustar tus preferencias específicas de manera efectiva:

- Para Facebook: **Configuración de privacidad** [<https://www.facebook.com/help/325807937506242>](https://www.facebook.com/help/325807937506242)
- Para X (Twitter): **Privacidad y seguridad** [<https://help.twitter.com/es/safety-and-security>](https://help.twitter.com/es/safety-and-security)
- Para Instagram: **Configuración de privacidad** [<https://help.instagram.com/325135857663734>](https://help.instagram.com/325135857663734)

- Para TikTok: **Privacidad y seguridad** <<https://support.tiktok.com/es/account-and-privacy/account-privacy-settings>>
- Para LinkedIn: **Configuración de privacidad** <<https://www.linkedin.com/help/linkedin/answer/a1342861>>

Para una guía más detallada, te recomendamos consultar el artículo de INCIBE: **Configuración de privacidad en redes sociales** <<https://www.incibe.es/ciudadania/tematicas/privacidad/configuraciones-redes-sociales>> (INCIBE).

Recursos adicionales:

Para profundizar en la gestión de tu privacidad en redes sociales, te sugerimos explorar los siguientes **vídeos educativos** proporcionados por la Agencia Española de Protección de Datos (AEPD), que ofrecen consejos prácticos y explicaciones sobre la importancia de proteger tu información:

- Facebook <<https://video-agpd.akamaized.net/configura-tu-privacidad/facebook.mp4>>
- Red social X <<https://www.youtube.com/watch?v=XWz-XJPfnwI>>
- Tiktok <<https://www.youtube.com/watch?v=MEzWcjI9a9c>>
- Instagram <<https://www.youtube.com/watch?v=6k3pxFaCDjM>>

Recuerda que la clave para mantener tu privacidad en redes sociales es una combinación de estar informado y tomar acciones proactivas.

Las aplicaciones de mensajería instantánea, como **WhatsApp** y **Telegram**, aunque no son redes sociales, ofrecen características sociales tales como la creación de grupos y canales. A continuación, te ofrecemos una guía para

ajustar la configuración de privacidad en estas aplicaciones y enlaces a recursos adicionales que te ayudarán a proteger tu información personal.

Para **ajustar la configuración de privacidad** en estas aplicaciones, sigue estos pasos generales:

- **WhatsApp:**

- Accede a "Configuración" en la aplicación.
- Elige "Cuenta" o "Privacidad" y ajusta quién puede ver tu información y publicaciones.

Para una guía más detallada, te recomendamos visitar esta **Guía de seguridad y privacidad de WhatsApp** <<https://www.incibe.es/ciudadania/blog/conoce-las-principales-funciones-de-seguridad-y-privacidad-de-whatsapp>> (INCIBE).

- **Telegram:**

- En "Configuración", busca "Privacidad y seguridad".
- Ajusta quién puede contactarte y ver tu información.

Para una guía más detallada, te recomendamos visitar el artículo **8 ajustes de privacidad en Telegram** <<https://lifehacker.com/8-telegram-privacy-settings-you-should-enable-immediate-1848931353>> (lifehacker).

Ajustes de gestión de privacidad por plataforma:

Es importante consultar la **documentación oficial** de ambas plataformas para obtener la información más actualizada sobre privacidad y seguridad:

- **Configuración de privacidad en WhatsApp** <https://faq.whatsapp.com/3307102709559968/?cms_platform=web>
- **Configuración de privacidad en Telegram** <<https://telegram.org/privacy/eu#4-keeping-your-personal-data-safe>>

Recursos Adicionales:

Para profundizar en la gestión de tu privacidad en las aplicaciones de mensajería, te sugerimos explorar los siguientes vídeos educativos proporcionados por la Agencia Española de Protección de Datos (AEPD), que te ayudarán a configurar las opciones de privacidad:

- **WhatsApp** <<https://www.youtube.com/watch?v=UbshtnCp0Vk>>

- **Telegram** [<https://video-agpd.akamaized.net/configura-tu-privacidad/telegram.mp4>](https://video-agpd.akamaized.net/configura-tu-privacidad/telegram.mp4)

Siguiendo estas recomendaciones y consultando la documentación oficial, podrás ajustar la privacidad en WhatsApp y Telegram para proteger tu información personal.

¿Recibiste alguna vez una **notificación de Facebook, Twitter, LinkedIn** u otra red social sobre **nuevas políticas de privacidad**? Sí, esas que solemos ignorar...

Estas notificaciones forman parte de uno de los requisitos que afectan directamente a la relación entre **protección de datos y redes sociales**: el deber de informar a los usuarios de los cambios en las políticas de privacidad, según lo establecido en el Reglamento General de Protección de Datos (RGPD) de la Unión Europea.

Actividad (opcional): Auditoría de privacidad digital

Descripción: Realiza una auditoría completa de tu configuración de privacidad en redes sociales para identificar y corregir posibles vulnerabilidades.

Pasos:

1. Elige una red social y accede a su configuración de privacidad.

2. Revisa y ajusta quién puede ver tus publicaciones y acceder a tu información personal.
3. Repite el proceso para otras redes sociales que utilices.

Recursos necesarios:

- Enlaces a guías de privacidad de Facebook, Instagram, Twitter, LinkedIn, y TikTok, proporcionadas en los materiales del curso.



Piensa antes de publicar

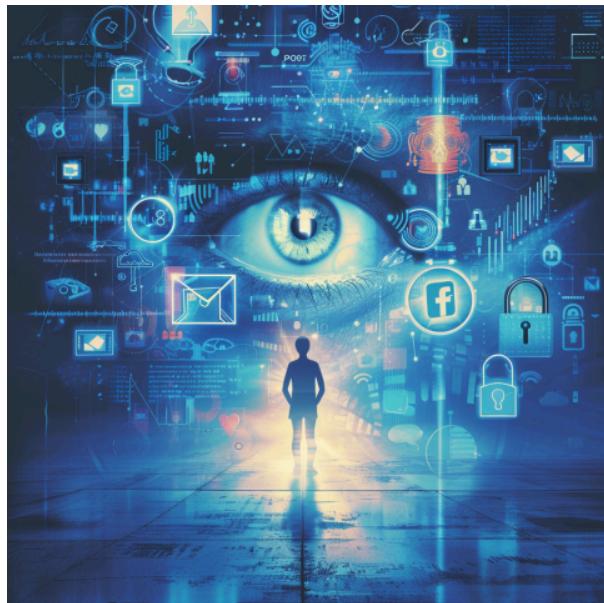


Imagen generada con IA (Midjourney)
(CC BY-NC-SA <<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>>)

Las redes sociales ponen a tu alcance distintos recursos para que puedas divulgar y compartir con otras personas la información que tú quieras, la cautela y el discernimiento son clave. Este apartado aborda la importancia de **pensar antes de publicar**. Cada vez que compartimos, no solo revelamos aspectos de nuestra vida, sino que también nos exponemos a riesgos que pueden comprometer nuestra **privacidad y seguridad**, afectar nuestra **reputación**, e incluso involucrar aspectos legales relacionados con la **propiedad intelectual**.

Las repercusiones de una publicación pueden ser más amplias de lo imaginado, afectando no solo al que publica sino también a terceros. Por ello, debemos adoptar una postura de **responsabilidad y respeto** al interactuar en las redes sociales, siempre conscientes del impacto de nuestras acciones en el entorno digital.

Objetivos:

- Desarrollar conciencia sobre los riesgos asociados a la publicación de información personal y de terceros en redes sociales.
- Fomentar prácticas responsables en el uso de redes sociales, respetando la privacidad y los derechos de propiedad intelectual.

Lecturas recomendadas:

- **Terminó presa por etiquetar a su ex cuñada en la red social** <<https://trome.com/viral/facebook-termino-presa-etiquetar-ex-cunada-red-social-2301/>> (Trome). Este artículo narra la historia de María González, quien fue encarcelada por un año tras etiquetar a su ex cuñada en publicaciones de Facebook, violando una orden de restricción.
- **Encarcelado por compartir en Facebook fotos de su ex novia desnuda** <https://www.abc.es/tecnologia/encarcelado-facebook-novia-201011160000_noticia.html> (ABC). Este caso destaca la historia de un joven que fue encarcelado por publicar fotos desnudas de su ex novia en Facebook.

En ocasiones publicamos contenidos en las redes sociales que nos parecen inofensivos, sin ser conscientes del grado de exposición al que nos sometemos, ni las consecuencias que pueden tener en nuestras vidas.

Algunos ejemplos de información que no deberíamos publicar:

- La **fecha de nacimiento completa**, aunque necesaria para crear un perfil, no debería estar visible para todos. Es un dato muy usado para el robo de identidad.

- La **ubicación actual** no se debe compartir públicamente para evitar indicar cuándo no estamos en casa o revelar rutinas personales.
- El **domicilio visible** puede aumentar el riesgo de robo en el hogar o suplantación de identidad.
- Compartir **número de móvil o correo electrónico** puede exponernos a ataques de ingeniería social, como spam o phishing, buscando acceder a información sensible.

Limitar la visibilidad de estos datos es una medida muy importante para nuestra seguridad en línea.

Cuando publicamos en redes sociales, la información puede escapar a nuestro control. Aunque borremos la publicación, como mínimo se ha quedado registrada en los servidores de la plataforma. Tenemos que ser conscientes del tipo de contenido que compartimos, ya que puede tener efectos negativos o no deseados.

Algunos ejemplos:

- **Publicaciones ofensivas o comentarios negativos** pueden tener consecuencias legales y dañar nuestra imagen personal y profesional.
- **El ciberacoso**, incluyendo burlas y difusión de mentiras, debe ser denunciado para proteger a las víctimas y los testigos.
- **Quejas laborales** en redes pueden afectar cómo los empleadores ven a sus trabajadores, impactando su relación laboral.
- **Fotos inapropiadas** pueden ser usadas en contra nuestra, perdiendo el control sobre cómo se distribuyen.
- **La propagación de noticias falsas** puede mermar nuestra credibilidad. Antes de publicar una noticia, comprueba sus fuentes.

Al compartir contenido en **redes sociales**, es fundamental reconocer la **propiedad intelectual** de los materiales publicados. Asegurarse de cumplir las **normativas y regulaciones** evita transgresiones legales, protegiendo así tanto los derechos de autor como nuestra reputación digital. Para más información sobre propiedad intelectual, visita el sitio del **Ministerio de Cultura y Deporte** [<http://www.culturaydeporte.gob.es/cultura-mecd/areas-cultura/propiedadintelectual/la-propiedad-intelectual.html> .](http://www.culturaydeporte.gob.es/cultura-mecd/areas-cultura/propiedadintelectual/la-propiedad-intelectual.html)

Las licencias de **Creative Commons** <<https://creativecommons.org/licenses/>> ofrecen flexibilidad para usar contenidos dentro de los marcos de la propiedad intelectual, permitiendo **copiar, distribuir, editar y crear** a partir de obras originales. Es crucial informarse sobre estas licencias. Podemos usar el **buscador de Creative Commons** <<https://search.creativecommons.org/>> para encontrar contenido libre bajo estas condiciones.



Actividad: Reflexión y búsqueda en redes sociales

Descripción: Imagina por un momento que decides irte de vacaciones con tu familia. Después de meses de planificación, finalmente llega el momento de relajarte y disfrutar. En tu entusiasmo, decides compartir en

tus redes sociales cada detalle: la foto del aeropuerto, el "check-in" en el hotel, las imágenes paradisíacas de la playa, e incluso un comentario sobre cuánto estás disfrutando el tiempo lejos de casa.

Sin embargo, mientras estás disfrutando del sol y el mar, en tu ciudad, alguien más ha estado atento a tus publicaciones. Esta persona no es un amigo ni un seguidor casual; es alguien que ha estado buscando oportunidades exactamente como esta. Mientras tú compartes tu alegría, ellos ven una oportunidad dorada: una casa vacía, lista para ser robada.

¿Es este el precio de compartir nuestra vida en línea? ¿Cómo podemos equilibrar el deseo de conectarnos y compartir con la necesidad de proteger nuestra privacidad y seguridad?

Después de reflexionar sobre este ejemplo, te invitamos a realizar una **búsqueda** rápida en redes sociales para **identificar publicaciones que podrían comprometer la privacidad o seguridad de los usuarios**.

Pasos:

- Accede a una red social de tu elección.
- Busca publicaciones que contengan información sensible, como ubicaciones específicas, datos personales o imágenes comprometedoras.
- Identifica al menos tres ejemplos y anota brevemente por qué podrían ser peligrosos.

Recursos necesarios:

- Dispositivo con conexión a internet.
- Acceso a una red social.



Recursos educativos



Imagen generada con IA (Midjourney) (CC BY-NC-SA
<<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>>)

Explora estos **recursos para** enseñar ciberseguridad: actividades, lecturas y más, diseñados para **promover** la **privacidad digital** entre nuestros estudiantes.

- **Muévete seguro por las redes sociales.** Infografía con consejos para moverte de manera segura en las redes sociales. [Descargar la infografía <https://www.incibe.es/sites/default/files/images/concienciacion/c4_pdf_rp_muevete_seguro_rrss.pdf>](https://www.incibe.es/sites/default/files/images/concienciacion/c4_pdf_rp_muevete_seguro_rrss.pdf).
- **Cómo las stories y otras publicaciones efímeras afectan a tu privacidad.** Vídeo educativo que explora cómo las publicaciones efímeras pueden impactar en la privacidad. [Ver vídeo <https://www.youtube.com/watch?v=tGU94h5kOkM>](https://www.youtube.com/watch?v=tGU94h5kOkM).
- **Guía de seguridad en redes sociales para familias.** Recurso que ofrece pautas de seguridad en redes sociales dirigidas a familias. [Acceder a la](#)

guía <<https://www.incibe.es/menores/materiales/guia-de-seguridad-en-redes-sociales-para-familias>> .

- ¡Carta! el juego de ciberseguridad para las redes sociales. Juego educativo sobre ciberseguridad en redes sociales dirigido a adolescentes. **Acceder al juego** <<https://www.incibe.es/menores/recursos/redes-sociales-en-la-adolescencia>> .
- Consejos para redes sociales. Documento PDF con recomendaciones para un uso seguro de las redes sociales. **Descargar PDF** <<https://www.incibe.es/sites/default/files/docs/redessociales.pdf>> .
- ¿Hacemos buen uso de las redes sociales?. Vídeo que plantea reflexiones sobre el uso responsable de las redes sociales. **Ver vídeo** <<https://www.youtube.com/watch?v=WMEk-bua9vA>> .
- Al día en Twitch. Artículo informativo sobre la plataforma de streaming Twitch. **Acceder al artículo** <<https://www.incibe.es/menores/blog/al-dia-en-twitch>> .
- Los menores eligen Instagram: ¿por qué les gusta tanto?. Análisis sobre la popularidad de Instagram entre los menores. **Acceder al análisis** <<https://www.incibe.es/menores/blog/los-menores-eligen-instagram-por-que-les-gusta-tanto>> .
- Qué es TikTok y por qué triunfa entre los menores. Artículo que explora la popularidad de la plataforma TikTok entre los jóvenes. **Leer el artículo** <<https://www.incibe.es/menores/blog/que-es-tiktok-y-por-que-triunfa-entre-los-menores>> .
- Tu hijo usa la app Snapchat: enséñale a manejarla con sentido común. Consejos para padres sobre el uso seguro de la aplicación Snapchat por parte de sus hijos. **Leer consejos** <<https://www.incibe.es/menores/blog/tu-hijo-usa-la-app-snapchat-ensenale-manejarla-con-sentido-comun>> .

Módulo 2. Navegación sin sobresaltos

2.3 Recuerda tus derechos

A lo largo de este módulo hemos explorado la importancia de la privacidad en nuestra navegación diaria por internet, aprendiendo a protegernos de amenazas y a manejar nuestras redes sociales con precaución. Pero, ¿qué sucede cuando encontramos información sobre nosotros en internet que nos perjudica, o deseamos eliminar una imagen o vídeo nuestro publicado sin nuestro consentimiento? ¿Qué ocurre con nuestros datos? Afortunadamente, contamos con **derechos digitales** que nos permiten tomar acción.

En este apartado, profundizaremos en cómo **ejercer nuestros derechos** para **controlar y proteger** nuestra **información personal en internet**.



Imagen generada con IA (Midjourney) (CC BY-NC-SA <<http://creativecommons.org/licenses/?lang=es>>)



Un vistazo a nuestros derechos en internet



Imagen generada con IA (Midjourney)
(CC BY-NC-SA
<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

En la Unión Europea, los usuarios tienen **derechos** en relación con su información personal en línea. Estos derechos no solo **salvaguardan nuestra información personal** sino que también aseguran nuestra capacidad para comunicarnos, expresarnos y participar en la sociedad digital de manera segura. A medida que avanzamos en este camino digital, es importante ser **conscientes** y estar **empoderados** sobre los **derechos que nos protegen** y **cómo podemos hacerlos valer**.

Objetivos:

- Concienciar sobre la importancia de los derechos digitales y la privacidad en internet.
- Revisar algunos de los derechos de los usuarios en internet.

Lecturas recomendadas:

- **Derecho al Olvido: Análisis del Caso Google España vs. AEPD y Mario Costeja** <https://cyberprotegidos.info/legislacion-y-politica/derecho-olvido-analisis-caso-google-espana-vs-aepd-mario-costeja/> (Cyber Protegidos). Una narrativa detallada sobre el caso que llevó al establecimiento del derecho al olvido en internet, destacando sus consecuencias y relevancia.
- **La UE publica un reglamento para proteger los derechos de los usuarios en el entorno digital** <https://diariolaleylareynext.es/dl/2022/11/02/la-ue-publica-un-reglamento-para-proteger-los-derechos-de-los-usuarios-en-el-entorno-digital> (Diario La Ley). Detalles sobre el nuevo reglamento de la Unión Europea diseñado para reforzar la protección de los derechos digitales de los usuarios.

El **derecho a la protección de datos** es el derecho de una persona a garantizar que su información personal se recopile, use y almacene de manera segura y responsable.

El **derecho a la privacidad** es el derecho de una persona a controlar quién tiene acceso a su información personal y cómo se utiliza. En internet, este derecho se ve afectado por la cantidad de información personal que compartimos en redes sociales, foros, blogs y otros sitios web. Para proteger nuestra privacidad, es importante ser conscientes de los riesgos y tomar medidas para proteger nuestra información personal.

El **derecho a la transparencia** es el derecho de una persona a saber cómo se utilizan y comparten sus datos personales en línea. Un artículo interesante sobre este derecho es el mencionado anteriormente, "La UE publica un Reglamento para proteger los derechos de los usuarios en el entorno digital <<https://diariolaleylaleynext.es/dl/2022/11/02/la-ue-publica-un-reglamento-para-proteger-los-derechos-de-los-usuarios-en-el-entorno-digital>> ", que describe cómo la Unión Europea está trabajando para garantizar que los usuarios tengan más control sobre su información personal en línea y puedan solicitar la eliminación de información incorrecta o irrelevante.

El **derecho al consentimiento informado** significa que una persona debe dar su consentimiento explícito antes de que se recopile, utilice o comparta su información personal. En línea, este derecho se ve afectado por las políticas de privacidad y los términos de uso de los sitios web y aplicaciones móviles. Para ejercer este derecho, es importante leer y comprender las políticas de privacidad y los términos de uso antes de utilizar un servicio en línea.

El derecho al olvido es el derecho de una persona a solicitar la eliminación de información personal en línea que ya no sea relevante o necesaria.

En los siguientes apartados exploraremos el **derecho de supresión ("al olvido")** en **buscadores de internet y redes sociales**, incluyendo cómo eliminar fotos y vídeos de una red social, profundizando en el ejercicio efectivo de nuestros derechos digitales.



Actividad de reflexión (opcional): El poder del consentimiento

Descripción: Reflexiona sobre la importancia del consentimiento informado en internet y cómo afecta a nuestra privacidad y control sobre los datos personales. Considera las veces que has dado consentimiento sin leer completamente los términos y cómo podrías tomar decisiones más informadas en el futuro.

Pasos:

1. Leer brevemente sobre el concepto de consentimiento informado en la web.
2. Analizar y reflexionar sobre las veces que hemos dado consentimiento sin leer completamente los términos.
3. Pensar en medidas para tomar decisiones más informadas en el futuro.

Recursos necesarios:

- Acceso a internet.

- Artículos o guías sobre consentimiento informado en línea.



Derecho de supresión ("al olvido")



Imagen generada con IA (Midjourney)

(CC

BY-NC-SA

<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>

El **derecho de supresión**, conocido como "**derecho al olvido**", permite a las personas controlar la difusión de su información personal en internet, especialmente en motores de búsqueda. Esto implica la capacidad de **evitar la exposición de datos personales** cuando su divulgación no cumple con los criterios de relevancia y adecuación establecidos por la normativa. En concreto, incluye el derecho a limitar la difusión universal e indiscriminada de datos personales en los buscadores generales cuando la información es obsoleta o ya no tiene relevancia ni interés público, aunque la publicación original sea legítima.

Objetivos:

- Entender el concepto y alcance del Derecho de Supresión ("derecho al olvido") y su importancia en la protección de la privacidad en internet.
- Aprender los procedimientos para ejercer el derecho al olvido en motores de búsqueda y redes sociales, considerando el equilibrio entre privacidad y acceso a la información.

Lecturas recomendadas:

- **Agencia Española de Protección de Datos: Derecho al olvido** <<https://www.aepd.es/areas-de-actuacion/internet-y-redes-sociales/derecho-al-olvido>> (AEPD). Un recurso oficial que proporciona una visión general sobre el derecho al olvido, incluyendo guías sobre cómo ejercer este derecho en el contexto de internet y redes sociales.
- **"El derecho al olvido en la era digital: desafíos legales y éticos"** <<https://www.castilholegalcorp.com/es/publicaciones/el-derecho-al-olvido-en-la-era-digital-desafios-legales-y-eticos/320/>> (Castillo Legal). Examina los retos legales y éticos que plantea el derecho al olvido en el entorno digital, destacando su impacto en la privacidad y la libertad de expresión.

Podrás ejercitar este derecho ante la persona responsable solicitando la supresión de tus datos de carácter personal cuando concurra alguna de las siguientes circunstancias:

- Si tus datos personales ya no son necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo.
- Si el tratamiento de tus datos personales se ha basado en el consentimiento que prestaste a la persona responsable, y retiras el mismo, siempre que el citado tratamiento no se base en otra causa que lo legitime.
- Si te has opuesto al tratamiento de tus datos personales al ejercitar el derecho de oposición en las siguientes circunstancias:
 - El tratamiento de la persona responsable se fundamentaba en el interés legítimo o en el cumplimiento de una misión de interés público, y no han prevalecido otros motivos para legitimar el tratamiento de tus datos.

- A que tus datos personales sean objeto de mercadotecnia directa, incluyendo la elaboración de perfiles relacionada con la citada mercadotecnia.
- Si tus datos personales han sido tratados ilícitamente.
- Si tus datos personales deben suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión Europea que se aplique a la persona responsable del tratamiento.
- Si los datos personales se han obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1 (condiciones aplicables al tratamiento de datos de los menores en relación con los servicios de la sociedad de la información).

La normativa de protección de datos establece que para ejercer el derecho de supresión (y, por tanto, el 'derecho al olvido') es imprescindible que el ciudadano se dirija en primer lugar a la entidad que está tratando sus datos, en este caso al buscador.

Pasos para ejercer el derecho de supresión:

1. Identifica la información personal que deseas suprimir.
2. Localiza los enlaces a la información personal que deseas suprimir y comprueba si pertenecen a buscadores de internet como Google, Bing o Yahoo.
3. Accede a los formularios de solicitud de supresión de los buscadores de internet. A continuación, te proporcionamos los enlaces a los formularios de solicitud de supresión de los principales buscadores de internet:
 - **Google**
<https://support.google.com/legal/troubleshooter/1114905?>

sjid=5774601044505015652-EU>

- **Bing <<https://www.bing.com/webmaster/tools/eu-privacy-request>>**
- **Yahoo <https://io.help.yahoo.com/contact/index?page=contactform&locale=es_ES&token=Zh%2FBBVqXzLHIbokbUqVWTUbuuQeXGkGFw6kaYtcsz3bJLmII3EUv0z8vEZziUaVM%2FeyBEjFUCaMU2WNiF1pt08EKxz55Rcv1x17V0EmPwqCwTMq3EFzwfnJNrIXz0JmkcIODVsGATkR7pX7Nwg%3D%3D&selectedChannel=email-icon&yid=>**

4. Completa el formulario de solicitud de supresión proporcionando la información personal necesaria y sigue las instrucciones indicadas en el formulario.
5. Espera a la respuesta del buscador de internet y, en caso de no estar satisfecho con la respuesta, puedes interponer una reclamación ante la Agencia Española de Protección de Datos (AEPD).

Es importante tener en cuenta que el derecho de supresión solo afecta a los resultados obtenidos en los buscadores de internet y no a las fuentes originales. Además, el derecho de supresión no garantiza la desaparición completa de la información personal de internet, sino únicamente la no visualización de la misma en los resultados de búsqueda realizados a través del nombre de la persona.

Las redes sociales más populares disponen de mecanismos establecidos para comunicar vulneraciones de la privacidad o contenidos inapropiados mediante sus propios formularios.

A continuación, detallamos algunos de los métodos que ofrecen:

- **Facebook:** Reportar fotos o videos que vulneran tu privacidad [<https://www.facebook.com/help/428478523862899>](https://www.facebook.com/help/428478523862899)
- **Twitter:** Formulario publicación de información privada [<https://help.twitter.com/forms/private_information>](https://help.twitter.com/forms/private_information)
- **Instagram:** Reportar contenido publicado por terceros [<https://help.instagram.com/122717417885747/?ref=hc_fnav>](https://help.instagram.com/122717417885747/?ref=hc_fnav)
- **TikTok:** Reportar contenido inapropiado [<https://support.tiktok.com/es/safety-hc/report-a-problem>](https://support.tiktok.com/es/safety-hc/report-a-problem)
- **YouTube:** Reportar contenido en YouTube [<https://support.google.com/youtube/answer/2802027>](https://support.google.com/youtube/answer/2802027)

Actividad (opcional): Egosurfing: Descubriendo tu huella digital

Descripción: Realiza **egosurfing** para explorar y reflexionar sobre la huella digital que has dejado en internet hasta ahora.

Pasos:

1. Utiliza varios motores de búsqueda para realizar egosurfing, buscando tu nombre completo **entre comillas**.
2. Revisa las imágenes y videos tuyas publicadas en la red social que más uses.
3. Identifica y anota los tipos de información sobre ti que son públicamente accesibles, prestando especial atención a cualquier contenido que consideres inadecuado o que prefieras que no esté disponible en línea.
4. Reflexiona sobre cómo esta información podría impactar tu vida personal y profesional, y considera si necesitas tomar medidas para mejorar tu privacidad online.
5. Para cada pieza de información inadecuada encontrada, utiliza los mecanismos proporcionados por motores de búsqueda y redes sociales para solicitar su retirada.

Recursos necesarios:

- Acceso a internet y a las principales redes sociales y motores de búsqueda.

- Un cuaderno o documento digital para registrar tus descubrimientos y acciones tomadas.



Recursos educativos



Imagen generada con IA (Midjourney) (CC BY-NC-SA
<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

Explora estos **recursos** para enseñar ciberseguridad: actividades, lecturas y más, diseñados para **promover** la **privacidad digital** entre nuestros estudiantes.

- **Derechos del ciudadano en Internet:** Este vídeo muestra los derechos que tenemos al utilizar Internet y la importancia de mantener nuestra privacidad en plataformas online. **Ver el vídeo** <https://www.youtube.com/watch?v=agnTAcAlvKM>.

- **La reputación de un menor se ve vulnerada tras publicarse un vídeo en redes sociales:** Análisis de un caso real que ilustra los peligros de la exposición en redes sociales. [Leer más <https://www.incibe.es/linea-de-ayuda-en-ciberseguridad/casos-reales/la-reputacion-de-un-menor-se-ve-vulnerada-tras-publicarse-un-video-en-redes-sociales>](https://www.incibe.es/linea-de-ayuda-en-ciberseguridad/casos-reales/la-reputacion-de-un-menor-se-ve-vulnerada-tras-publicarse-un-video-en-redes-sociales).
 - **Un famoso TikToker publica un vídeo viral de una menor sin su consentimiento:** Análisis de un caso real que explora las consecuencias legales y sociales de compartir contenido sin permiso. [Leer más <https://www.incibe.es/linea-de-ayuda-en-ciberseguridad/casos-reales/un-famoso-tiktoker-publica-un-video-viral-de-una-menor-sin-su-consentimiento>](https://www.incibe.es/linea-de-ayuda-en-ciberseguridad/casos-reales/un-famoso-tiktoker-publica-un-video-viral-de-una-menor-sin-su-consentimiento).
 - **Una empresa escanea el iris de menores a cambio de criptomonedas en un centro comercial:** Análisis de un caso real de invasión de la privacidad bajo el atractivo de la tecnología. [Leer más <https://www.incibe.es/linea-de-ayuda-en-ciberseguridad/casos-reales/una-empresa-escanea-el-iris-menores-cambio-de-criptomonedas-en-un-centro-comercial>](https://www.incibe.es/linea-de-ayuda-en-ciberseguridad/casos-reales/una-empresa-escanea-el-iris-menores-cambio-de-criptomonedas-en-un-centro-comercial).
 - **Una joven halla fotos suyas desnuda de cuando era menor de edad publicadas en Telegram:** Análisis de un caso real sobre la difusión no autorizada de imágenes personales. [Leer más <https://www.incibe.es/linea-de-ayuda-en-ciberseguridad/casos-reales/una-joven-halla-fotos-suyas-desnuda-de-cuando-era-menor-de-edad-publicadas-en-telegram>](https://www.incibe.es/linea-de-ayuda-en-ciberseguridad/casos-reales/una-joven-halla-fotos-suyas-desnuda-de-cuando-era-menor-de-edad-publicadas-en-telegram).
 - **Una menor es obligada a visualizar fotos y vídeos de abuso sexual infantil en WhatsApp:** Análisis de un caso real que muestra la gravedad de la exposición a contenidos inapropiados en las redes. [Leer más <https://www.incibe.es/linea-de-ayuda-en-ciberseguridad/casos-reales/una-menor-es-obligada-visualizar-fotos-y-videos-de-abuso-sexual-infantil-en-whatsapp>](https://www.incibe.es/linea-de-ayuda-en-ciberseguridad/casos-reales/una-menor-es-obligada-visualizar-fotos-y-videos-de-abuso-sexual-infantil-en-whatsapp).
 - **Una menor utiliza las redes sociales para publicar graves acusaciones sobre su exnovio:** Análisis de un caso real sobre el impacto de las redes sociales en las relaciones personales. [Leer más <https://www.incibe.es/linea-de-ayuda-en-ciberseguridad/casos-reales/una-menor-utiliza-las-redes-sociales-para-publicar-graves-acusaciones-sobre-su-exnovio>](https://www.incibe.es/linea-de-ayuda-en-ciberseguridad/casos-reales/una-menor-utiliza-las-redes-sociales-para-publicar-graves-acusaciones-sobre-su-exnovio).
-

Obra publicada con Licencia Creative Commons Reconocimiento Compartir igual 4.0 <<http://creativecommons.org/licenses/by-sa/4.0/>>

Módulo 2. Navegación sin sobresaltos

2.4 Actividades obligatorias

Manual de Supervivencia de Ciberseguridad



Imagen generada con IA (DALL-E) (CC BY-NC-SA
<http://creativecommons.org/licenses/?lang=es>)



Actividad 2.1: Manual de supervivencia de ciberseguridad II

Descripción: Esta actividad está diseñada para ayudarte a continuar con la elaboración de tu manual personal de ciberseguridad, desarrollando ahora el capítulo 2, que incorpora las medidas adicionales de seguridad y privacidad que hemos explorado en este módulo.

Pasos:

- **Selección de medidas de seguridad:**

- Revisa los contenidos del Módulo 2 y elige las medidas de seguridad y privacidad, estrategias y herramientas que consideres más relevantes para tu entorno digital.
- Justifica por qué has seleccionado cada medida y cómo se aplican a tus necesidades específicas.
- Añade a tu manual una sección que contenga una lista de las medidas seleccionadas con una breve descripción de cada una y los recursos necesarios para su implementación. Esta sección servirá como referencia rápida de las estrategias de seguridad que has considerado importantes.

- **Implementación de una medida de seguridad:**

- De las medidas seleccionadas, implementa al menos una en tu entorno digital actual.
- Describe el proceso de implementación y cómo has aplicado la medida, incluyendo cualquier dificultad que hayas encontrado y cómo la superaste.

- **Estado de madurez de mi seguridad digital:**

- Añade a tu manual una nueva sección que liste las medidas de seguridad y privacidad que ya has aplicado y las que están pendientes de implementación.
- Reflexiona sobre tu estado actual de seguridad digital y justifica tus decisiones y planes futuros para mejorar tu seguridad.

Recursos necesarios:

- Procesador de texto (Word, Google Docs, etc.).
- Acceso a los contenidos del Módulo 2.
- Herramientas y recursos de ciberseguridad mencionados en el módulo.
- Plantilla proporcionada en el aula virtual del curso.

Formato y entrega de la actividad: La actividad debe ser entregada en formato PDF a través del enlace habilitado en el aula virtual del curso.

Nota: Cada capítulo del manual se puede trabajar de manera independiente. No es necesario haber completado el capítulo 1 para realizar esta actividad.

Rúbrica de la actividad 2.1 **Aplicar**

	Nivel Alto	Nivel Medio	Nivel Básico
Selección de medidas	Se han identificado y seleccionado las	Se han identificado y seleccionado	No se ha incluido la sección. (0)

	Nivel Alto	Nivel Medio	Nivel Básico
seguridad pts) (2,5	estrategias y herramientas de manera completa y detallada, justificando claramente su relevancia y aplicación. (2.5)	estrategias y herramientas de manera adecuada, aunque las justificaciones son poco detalladas. (1.25)	
Implementación de una medida de seguridad	Se describe detalladamente la implementación de una medida, incluyendo las dificultades encontradas y cómo se superaron, reflejando un entendimiento profundo del proceso. (2.5)	La descripción de la implementación es adecuada, pero carece de detalles sobre las dificultades encontradas o posibles soluciones. (1.25)	No se ha incluido la sección o no se ha descrito la implementación de una medida. (0)
Estado de madurez de mi seguridad digital	Se ha incluido una sección detallada que refleja un análisis completo y una comprensión de la seguridad personal, mostrando claramente las medidas aplicadas y pendientes. (2.5)	La sección incluida muestra una comprensión adecuada de la seguridad personal, pero el análisis es superficial y necesita mayor profundidad. (1.25)	No se ha incluido la sección. (0)
Elaboración del manual	El manual incluye descripciones claras y recursos necesarios bien definidos. (2.5)	El manual incluye descripciones y recursos, pero no están completamente claros o son incompletos. (1.25)	No se ha elaborado el documento. (0)



Actividad obligatoria 2.2: Reflexión colaborativa sobre medidas de seguridad

Descripción: El propósito de esta tarea es fomentar la **reflexión colaborativa** sobre las medidas de seguridad propuestas en el módulo. Para ello, debes compartir tus experiencias en la **implementación** de alguna de las **medidas de seguridad y privacidad** presentadas en el módulo 2 y reflexionar sobre su efectividad en tu entorno digital. Además, se espera que comentes las contribuciones de tus compañeras y compañeros, ofreciendo tu perspectiva y posibles alternativas

de uso. Asegúrate de responder al menos a una entrada del foro para promover la interacción y el intercambio de ideas en el foro.

Considera enriquecer tus comentarios con preguntas estimulantes para promover una discusión más profunda y significativa.

Recursos necesarios:

- Acceso al foro del curso para la participación.

Formato y entrega de la actividad:

- Foro del módulo.

Rúbrica de la actividad 2.2 **Aplicar**

	Nivel 1	Nivel 2	Nivel 3
Participación activa en el foro (2,5 pts)	Se han compartido experiencias de manera detallada y constructiva, promoviendo la discusión. (2.5)	Se han compartido experiencias, pero de manera general o sin profundizar. (1.25)	No se han compartido experiencias en el foro. (0)
Reflexión sobre medidas implementadas (2,5 pts)	Se ha demostrado una reflexión profunda sobre las medidas implementadas, destacando su importancia. (2.5)	Se ha mostrado una reflexión básica sobre las medidas implementadas, sin detalles específicos. (1.25)	No se han compartido reflexiones sobre las medidas implementadas. (0)
Colaboración y apoyo a compañeras y compañeros (2,5 pts)	Se ha ofrecido apoyo constructivo y colaborativo a las reflexiones de las compañeras y compañeros. (2.5)	Se ha ofrecido apoyo a las compañeras y compañeros, pero de manera limitada o superficial. (1.25)	No se ha ofrecido apoyo ni colaboración a las compañeras y compañeros. (0)

	Nivel 1	Nivel 2	Nivel 3
Propuestas alternativas medidas de seguridad compañeras y compañeros pts) (2,5)	Se han presentado alternativas aplicables y bien fundamentadas a las medidas de seguridad, demostrando una comprensión profunda. (2.5)	Se han planteado alternativas a las medidas de seguridad; no obstante, estas requieren de un desarrollo más amplio o ejemplos que demuestren su aplicabilidad. (1.25)	No se han propuesto alternativas aplicables, sin aportar significativamente a la discusión sobre seguridad. (0)

Obra publicada con Licencia Creative Commons Reconocimiento Compartir igual 4.0
<http://creativecommons.org/licenses/by-sa/4.0/>

Módulo 2. Navegación sin sobresaltos

Otros formatos y autoría



Autoría

Título	Módulo 2 del curso "La Ciberseguridad en el ámbito educativo"
Descripción	El módulo " Navegación sin sobresaltos " proporciona herramientas y conocimientos detallados para una navegación segura y privada en internet. Los participantes aprenderán a gestionar su identidad digital y a configurar la privacidad de dispositivos y servicios online. También se abordan métodos para mantener una presencia discreta en redes sociales y se enfatiza la importancia de conocer y ejercer los derechos digitales para proteger la información personal.
Autor	Manuel Jesús Rivas Sánchez https://twitter.com/0xmrvias
Licencia	Creative Commons BY-NC-SA 4.0 https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es



Versión imprimible PDF



Este material está diseñado para ser leído y trabajado de manera interactiva en un ordenador, pero si quieres puedes descargártelo en [este enlace](https://raw.githubusercontent.com/0xmrvias/ciberseguridad-ambito-educativo-online/main/assets/PDF/modulo2.pdf) en formato pdf.

Obra publicada con Licencia Creative Commons Reconocimiento Compartir igual 4.0 <<http://creativecommons.org/licenses/by-sa/4.0/>>