¿Qué es la privacidad digital?

En internet circula una enorme cantidad de información, entre la que se encuentran los datos personales de los usuarios. Al hacer acciones tan simples como usar un navegador, colgar una foto en una red social o dejar un comentario en un blog o un foro, estamos dejando una información personal que deja un rastro en la red.

Por ello, es muy importante saber **qué es la privacidad digital** y cómo se puede aumentar la seguridad de nuestros datos en internet.

1 Significado y concepto

Comenzamos viendo el **significado de privacidad digital**. Este término se refiere al derecho de los usuarios a proteger sus datos en la red y decidir qué información está visible para el resto.

Del mismo modo que una persona quiere que se respete la privacidad en su casa o en su trabajo, también tiene el derecho a evitar que otros accedan a sus datos personales en internet sin su consentimiento.

El **concepto de privacidad digital** es relativamente joven, ya que está unido a la aparición y desarrollo de internet y las telecomunicaciones. De hecho, hasta hace poco no existía una regulación clara al respecto.

Características de la privacidad digital

La privacidad digital se define por una serie de **características**:

- Se refiere a toda la información de un usuario que circula por internet. Además de datos personales como el nombre, DNI, teléfono, domicilio, etc.
- Las particularidades de internet también hacen que la privacidad se refiera a imágenes, vídeos, correo electrónico, geolocalización, historial de navegación, IP o cualquier otro dato que permita la identificación de un usuario en la red.
- No se limita al uso de páginas web o redes sociales, sino que también se refiere a la transmisión de datos a través de tiendas online, aplicaciones, servicios de mensajería instantánea, etc.

1.1.1 Protección de datos

Para poder recabar datos de usuarios en internet se exige una serie de requisitos que veremos en profundidad más adelante. De momento, te adelantamos que entre los requisitos se encuentra la identificación de los responsables del tratamiento, obtener consentimiento explícito del usuario o comunicar la finalidad con la que se usará la información, entre otras.

1.1.2 Identidad digital

La **identidad digital o huella digital** se define como el rastro que una persona deja en internet. Al publicar una foto, escribir en un blog, dejar comentarios en una web… en definitiva, casi cualquier acción que se realiza en internet deja un rastro.

Está relacionado con la intimidad digital, que asiste a los usuarios con el objetivo de salvaguardar aquella información que quieren mantener en el ámbito privado, fuera del alcance de internet.

La ley establece que la persona debe tener el control de la información personal que circula por la red, lo cual nos lleva al siguiente punto.

1.1.3 Derecho al olvido

El usuario tiene derecho a solicitar que se elimine de internet aquella información que no quiere que sea vista por otros usuarios. Es lo que se denomina como derecho al olvido en internet. El requisito para proceder a su eliminación es que se trate de **información desactualizada, no pertinente o excesiva**, sin importar que en su día fuera veraz.

Por ejemplo, una persona aparece en Google como autor de un delito cometido hace muchos años, por el cual ya ha pagado y se encuentra rehabilitado totalmente. Esa información le puede perjudicar, por ejemplo de cara a conseguir un trabajo, por lo que puede hacer uso de este derecho.

1.1.4 Protección de datos de menores

La edad mínima para que los menores puedan prestar consentimiento para tratar sus datos personales en internet es de **14 años**. Antes de esa edad, el consentimiento debe ser otorgado por sus padres o tutores.

1.1.5 Testamento digital

Los familiares o herederos de una persona pueden **solicitar que se elimine la información personal del fallecido**, siempre y cuando éste no lo haya prohibido expresamente en vida. Esto incluye cualquier tipo de datos, desde fotos o perfiles de redes sociales, hasta cuentas bancarios o contraseñas de acceso a servicios web.

1.1.6 Desconexión digital

La privacidad digital también llega hasta el ámbito del trabajo. La desconexión digital implica que los trabajadores no tienen obligación de responder llamadas o correos electrónicos una vez que haya finalizado su horario de trabajo

1.1.7 Proveedores de servicios de internet

Por su parte, los proveedores de servicios debe ofrecer el acceso de los usuarios a la red sin ningún tipo de discriminación. Asimismo, han de garantizar que el acceso a la red se realiza en las máximas condiciones de seguridad.

Ventajas y desventajas

Ventajas de la privacidad digital:

- Aumentar la seguridad de la información y protege frente a fraudes, ciberataques como hackeos o suplantación de identidad.
- Decidir cuál es nuestra identidad digital, es decir, la imagen que internet proyecta de nosotros al resto de usuarios
- Permitir que solo accedan a nuestros datos aquellos usuarios, empresas o proveedores de servicios a los que hayamos otorgado nuestro consentimiento.
- Adecuar a nuestro perfil y nuestros intereses los contenidos, productos o servicios que se nos ofrecen.
- Concienciar cada vez más a la gente sobre la importancia de proteger los datos personales en internet.

Desventajas de la privacidad digital:

- Internet es una red inmensa, en la que circula una cantidad ingente de datos. POr tanto, tratar de controlar todo este flujo de información no es una objetivo realista. Como se suele decir, sería como poner puertas al campo.
- Entra en conflicto con los intereses de grandes empresas y corporaciones. Muchas de estas compañías tienen un enorme poder y prefieren hacer frente al pago de multas antes que hacer caso a las normas sobre privacidad que dictan los gobiernos.
- Todavía existe mucha gente que no comprende la importancia de proteger la información digital. Muchas personas siguen aceptando términos y condiciones de uso sin leerlas.
- A las generaciones pasadas les cuesta adaptarse a las nuevas exigencias en este campo, ya que la era digital avanza rápidamente y no espera por nadie.

Problemas y riesgos

La publicación de información sensible en internet puede acarrear diversos **problemas relacionados con la privacidad digital.**

- **Datos personales**: facilitar información como el el nombre real, teléfono o el DNI es un gran error ya que podría dar pie a una suplantación de identidad.
- **Correo electrónico**: dejar la dirección del email en cualquier sitio aumenta las posibilidades de recibir gran cantidad de spam o correo no deseado.
- **Datos bancarios**: nunca se deben dar los datos bancarios a nadie que no sea de total confianza, o de lo contrario podrías poner en riesgo tu dinero.
- **Ubicación geográfica**: otros datos como la dirección de tu domicilio o decir si estás o no en casa podría poner en riesgo tu vivienda, además de tu seguridad y la de los que viven contigo.
- **Fotografías y vídeos**: hay que tener mucho cuidado con qué tipo de fotografías se envían y dónde se publican. No sería la primera vez que extorsionan a alguien con fotos de índole sexual o que alguien pierde su trabajo por imágenes comprometidas.

Hablando más de términos y prácticas concretas, estos serían algunos de los principales **riesgos de la privacidad digital**:

- **Phishing**: es un método de abuso informático que consiste en conseguir información confidencial de manera fraudulenta para suplantar la identidad de un usuario.
- **Spam**: se define como la recepción masiva de correos electrónicos no deseados.
- **Virus y troyanos**: son programas que se cuelan en el ordenador del usuario para llevar a cabo acciones no solicitadas: robo de información, borrado de datos, etc. Pueden ir camuflados dentro de programas o aplicaciones aparentemente inofensivos.
- **Ciberacoso**: el cyberbulling o acoso virtual consiste en el uso de internet o las redes sociales para amenazar, acosar o chantajear a una persona.

Privacidad en internet

A continuación vemos cómo cumplir con estos requisitos en páginas web, redes sociales, aplicaciones o servicios de mensajería.

1.1.8 Páginas web

Para cumplir con la normativa sobre privacidad digital, las páginas web que recaben información personal de usuarios deben informar sobre su Política de privacidad, Política de cookies y Aviso legal.

Política de privacidad

La política de privacidad es el texto legal que informa al usuario sobre la forma en la que se van a tratar sus datos personales. Debe ser colocada en un apartado específico y claramente visible de la web.

En la política de privacidad se debe informar sobre:

- Identidad del responsable del tratamiento de datos
- Información del usuario que se va a recabar
- Finalidad con la que se recaba dicha información
- Período durante el cual los datos del usuarios se mantendrán en la base de datos
- Si los datos del usuario se van a ceder a terceros
- Si se produce alguna brecha de seguridad
- La manera de efectuar los derechos ARSULIPO (antiguos derechos ARCO), esto es, los derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad u oposición.

Política de cookies

Las **cookies** son archivos que se instalan en el navegador del usuario para conocer su historial de navegación. Se suele utilizar en marketing para ofrecer contenidos, productos o servicios relacionados con los intereses del usuario.

Para poder colocar una cookie en el navegador del usuario es necesario haber obtenido **consentimiento** expreso. Es decir, ya no sirve con el consentimiento tácito o por omisión, sino que éste debe ser efectivo, voluntario e inequívoco. Por ejemplo, marcando una casilla de aceptación.

Por otro lado, la intención de usar las cookies del usuario se debe presentar mediante una **doble capa informativa**. En la primera capa simplemente se indica que la web utiliza cookies de terceros, con un link a la segunda capa, en la que se informa más detalladamente sobre la finalidad, si se van a ceder a terceros o el tiempo de permanencia en la base de datos.

Como norma general, para colocar cualquier cookie es necesario el consentimiento expreso del usuario, pero esto no siempre es así. No será necesario, por ejemplo, en el caso de cookies de entrada de usuario, de seguridad, de reproducción multimedia o de autentificación.

Aviso legal

El aviso legal es un texto que se debe incluir en la web siempre y cuando se trate de:

- Páginas corporativas
- Webs o blogs que tengan publicidad
- Tiendas online
- Portales que ofrezcan prestación de algún tipo de servicio

En el aviso legal se debe incluir la siguiente información:

- Nombre de la empresa/usuario y datos de contacto
- DNI, NIF o NIE
- Número del Registro Mercantil, en caso de estar dado de alta como sociedad
- Información sobre autorizaciones administrativas obligatorias obtenidas
- En caso de ejercer una profesión regulada, se debe facilitar los datos del Colegio Profesional, título académico o normas deontológicas relativas al ejercicio de la profesión.

1.1.9 Privacidad en correos electrónicos

La normativa actual sobre protección de datos obliga a incluir un **texto legal** en los correos electrónicos de índole corporativa o comercial. Este texto legal debe ser incluido en la firma del correo electrónico e informar sobre la identidad del emisor, la finalidad del correo, la cesión de datos o las vías para ejercer los derechos.

Por otro lado, en los casos en los que se comunique información privada o secreta, será necesario incluir un aviso o **cláusula de confidencialidad** (aunque en muchos casos esta cláusula ya queda pactada mediante contrato.

El correo electrónico es otra de las herramientas que pueden ver comprometida la privacidad digital. A pesar de que muchos de estos sistemas utilizan **sistemas de cifrado** parcial (STARTTLS, STS o SMTP) o avanzados (SPF, DMARC o DKIM), sigue siendo más que recomendable tomar una serie de precauciones a la hora de usarlos:

- Usar una contraseña robusta (mayúsculas, minúsculas, mezcla de caracteres alfanuméricos) y sistemas de cifrado
- Emplear un sistema de autentificación en dos capas, si la herramienta lo permite.
- No facilitar información personal por email.
- Eliminar sin abrir los correos procedencia desconocida.

- Evitar abrir los emails sospechosos, aunque procedan de alguien conocido.
- Hacer backups o copias de seguridad de los correos.

Por otra parte, una de las grandes dudas sobre privacidad digital en este caso se refiere al **correo electrónico en el trabajo**. Las últimas sentencias establecen ciertos límites a este acceso. Un jefe no podrá acceder al correo personal de un trabajador, pero sí podrá acceder al correo electrónico corporativo, siempre que el trabajador haya sido avisado previamente.

1.1.10 Aplicaciones móviles y privacidad digital

Al igual que una página web, cualquier aplicación móvil que obtenga información personal de los usuarios debe informar sobre ello en un lugar visible. En cualquier caso, existen una serie de consejos para garantizar la privacidad digital en el uso de apps móviles:

- Descargar solo aplicaciones oficiales y desde los sitios oficiales
- Usar apps como eRule, que permiten analizar la seguridad de las apps instaladas (o que se vayan a instalar) en el dispositivo.
- Leer siempre la política de privacidad para saber a qué datos tendrá acceso la app.
- Repasar la configuración de privacidad de la aplicación una vez que haya sido instalada.
- Desconfiar de aquellas apps que soliciten acceder a contenidos que, en ningún caso, resultan imprescindibles para el correcto funcionamiento de la aplicación.
- Eliminar las aplicaciones que ya no uses.

1.1.11 ¿Cómo proteger tu privacidad en las redes sociales?

Las **redes sociales** son unas de las plataformas de internet más usadas. Hoy en día casi todo el mundo usa Facebook, Twitter o Instagram, y mucha gente lo hace sin pensar en las consecuencias negativas que estas herramientas podrían tener para su privacidad digital.

A continuación te mostramos cómo puedes mantener la seguridad de tus perfiles en redes sociales y evitar que se haga un uso malintencionado de tus imágenes o datos personales.

Facebook

Accede a la **configuración de privacidad en Facebook**. Desde ahí podrás ajustar numerosos parámetros, por ejemplo:

- Quién puede ver tu perfil o tus publicaciones.
- Administrar bloqueos de usuarios.

- Decidir quién puede enviarte solicitudes de amistad.
- Gestionar quién te puede etiquetar o quién puede publicar en tu muro.
- Poner límite al acceso de otras aplicaciones a tu perfil de Facebook.
- Visibilidad de anuncios.
- Elegir si quieres que tu perfil se vea en las búsquedas realizadas fuera de la web (por ejemplo, en motores de búsqueda como Google).
- Cambiar la privacidad de las fotografías.

Twitter

Del mismo, modo, desde la **configuración de Twitter** se pueden configurar los siguientes parámetros:

- Poner el perfil público privado.
- Modificar el nombre de usuario, contraseña, teléfono o email.
- Cambiar la configuración de privacidad de las imágenes.
- Administrar contactos.
- Bloquear o silenciar usuarios.
- Permitir que te encuentren por la dirección de email.
- Activar o desactivar la información sobre la ubicación.
- Elegir si quieres recibir anuncios personalizados
- Decidir si quieres que Twitter sepa desde qué dispositivos se accede.
- Aceptar o no si se quiere que Twitter comparta la información con sus socios.

Instagram

Instagram recaba información con un triple objetivo: conocer comportamientos de usuarios, saber el uso que se hacen de los dispositivos y compartir esa información con sus socios comerciales.

Para configurar la privacidad en Instagram hay que entrar en la aplicación y hacer clic en la sección “Configuración”. Desde aquí se pueden modificar aspectos como:

- Poner el perfil en público o privado.

- Configurar la privacidad de la Historias de Instagram o Instagram Stories.
- Eliminar fotos o decidir quién las puede ver.
- Bloquear o desbloquear usuarios.
- Habilitar o deshabilitar comentarios en las publicaciones.
- Desactivar o eliminar la cuenta

Casos prácticos

A continuación vemos cómo puedes **configurar tu privacidad digital** en algunos de los portales o servicios más importantes de internet.

Google

Existen tres maneras diferentes de configurar la privacidad en Google. Lo puedes hacer a través del Panel de Control, de la sección “Mi actividad” o desde el apartado “Información personal y privacidad”:

Entre las opciones está la posibilidad de:

- Controlar los datos que el resto de usuarios pueden ver sobre ti.
- Elegir el tipo de información que Google guarda sobre tu actividad.
- Configurar las preferencias para la visualización de anuncios.
- Decidir si quieres que Google utilice tu nombre o imagen en textos con finalidad comercial.

Mucha gente también se pregunta si existe la posibilidad de eliminar información de los resultados de búsqueda de Google. Y la respuesta es sí. De hecho, es una posibilidad asistida por el derecho al olvido. Para ello, es necesario enviar una solicitud a Google.

Youtube

Una de las plataformas más conocidas de Google es Youtube, un servicio en el que millones de usuarios publican y comparten vídeos.

Entrando en el apartado de configuración del usuario en Youtube se puede:

- Gestionar información relacionada con la cuenta, como privacidad del contenido, seguidores, anuncios, etc.
- Controlar el acceso de otras aplicaciones o dispositivos.

- Determinar preferencias de la cuenta relativos a suscripción a servicios, pagos, etc.
- Realizar análisis para detectar brechas de seguridad o privacidad.

Además, desde la configuración de Youtube también puedes modificar otros aspectos como:

- Notificaciones: suscripciones a tu canal, a otros canales, información sobre novedades del servicio, etc.
- Historial y privacidad: historial de navegación en la plataforma, vídeos añadidos a favoritos, listas de reproducción, etc.
- Videos: decidir si quieres que sean públicos (accesibles a todo el mundo), privados (solo para suscriptores) u ocultos (exclusivos para quienes tienen el enlace del vídeo).

10 consejos para proteger tu privacidad en Internet

Te damos 10 **trucos para proteger tu privacidad digital**. Sigue estos consejos para mantener tus datos personales seguros y protegidos:

1. Lee las condiciones antes de ceder cualquier tipo de información en internet o darte de alta en un servicio.
2. No compartas información personal en webs o redes sociales (nombre real, DNI, dirección) ni fotos que te puedan comprometer de alguna manera.
3. En las redes sociales, acepta solicitudes de amistad solo de personas que conozcas o perfiles de confianza.
4. No te registres a servicios mediante tu perfil de redes sociales, ya que dicho servicio podría acceder a la información de tus redes. Hazlo mejor mediante dirección de correo electrónico.
5. Configura la privacidad de tu perfil en las plataformas o servicios en los que te hayas registrado.
6. Utiliza sistemas de cifrado seguro de contraseñas como Last Pass.
7. Elimina de forma periódica tu historial de navegación o configura el navegador para que no almacene esta información.
8. Evita conectarte a internet a través de redes Wi-Fi públicas no seguras: hoteles, locutorios, aeropuertos.
9. Recuerda cerrar sesión siempre, sobre todo cuando entres en tu cuenta desde un dispositivo al que otros podrían tener acceso.

10. Desconecta el GPS de tu teléfono móvil cuando no lo estés usando, ya que evitarás que se sepa dónde estás en cada momento.

1.1.12 ¿Cómo hacer una cuenta de Twitter privada?

Debes seguir los siguientes pasos:

1. Inicia sesión.
2. Pincha encima de tu foto de perfil y después en “Configuración”.
3. Ve a “Seguridad y Privacidad”
4. En “Privacidad de los Tweets”, marca la casilla “Proteger mis Tweets”.

En todo caso, los usuarios que te siguen podrán seguir viendo tus tweets. Si quieres evitar que alguien en concreto acceda a los contenidos de tu perfil, deberás bloquear a ese usuarios.

1.1.13 ¿Se pueden desactivar las cookies del navegador?

Sí, en cualquier momento puedes eliminar o borrarlas desde el propio navegador.

1.1.14 ¿Cómo solicitar que se elimine mi información de una base de datos?

En sus Políticas de privacidad todo responsable del tratamiento debe informar al usuario sobre las vías para ejercer sus derechos de acceso, rectificación, limitación del tratamiento u oposición.

1.1.15 ¿Cómo proteger la información personal en aplicaciones móviles?

Es importante que sigas estos consejos:

- Utiliza un bloqueo de pantalla para evitar que otras personas puedan manejar el dispositivo.
- Descarga apps seguras desde portales oficiales
- Haz copias de seguridad en otros dispositivos
- Instala un antivirus

1.1.16 ¿Un medio de comunicación puede publicar una fotografía de mis redes sociales?

Si prevalece el interés público general o es con fines informativos, SÍ. También si tu imagen es meramente accesoria dentro del significado de la foto. Por ejemplo, si tu imagen aparece en una manifestación o en un mitin de un partido político durante la campaña electoral.

1.1.17 ¿Puede mi jefe acceder a mi correo electrónico?

Al correo personal, **NO**.

Pero como hablamos de jefes es obvio que nos referimos al correo corporativo. En este caso hay sentencias que avalan que el empresario puede acceder al correo electrónico corporativo de sus trabajadores, siempre que éstos hayan sido informados previamente.

1.1.18 ¿Qué es la seguridad digital?

Se refiere a la protección de los equipos y herramientas que forman parte de una estructura computacional y, en especial, de la información contenida en dicha estructura.