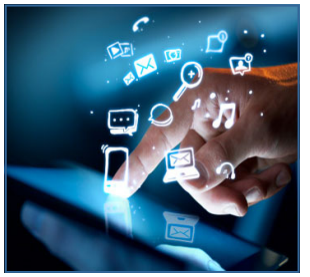

Privacidad en Internet

FEDERACIÓN
DE LA UNIÓN NACIONAL
DE CONSUMIDORES
Y AMAS DE HOGAR
DE ESPAÑA

Manual práctico para el consumidor y usuario nº 104

Privacidad y protección de datos en Internet

En el nuevo escenario digital se hace necesario asegurar la seguridad en todos los sectores, consiguiendo una mayor transparencia en el manejo de datos y en la soberanía tecnológica. En la actualidad los **servicios gratuitos más utilizados en Internet se prestan gracias a la información y los datos personales que los usuarios facilitan**, casi siempre **de forma inconsciente**, por lo que hay que **conocer los riesgos que implican para la privacidad**.

Por eso es necesario **proteger los datos personales** de los dueños de los dispositivos y de las personas con que se comunican (contactos, correos electrónicos, fotos, vídeos, etc.) para que no se pierdan o caigan en manos de otras personas. Pero también es muy importante cuidar de la privacidad e intimidad de los más pequeños.

Por eso es necesario conocer las novedades que presenta el nuevo **Reglamento General de Protección de Datos (RGPD)**, que establece **normas de protección coherentes y uniformes en toda Europa**, y se aplica a las empresas o personas jurídicas que tienen su sede en algún Estado miembro de la Unión Europea, así como a las empresas internacionales que realicen el tratamiento de datos relativos a personas de dichos países.

Además, el Reglamento establece estándares **más rigurosos sobre consentimiento**, se **amplían los derechos de las personas sobre el acceso, la portabilidad y la conservación**, e impone **multas considerables en caso de incumplimiento**.

La nueva normativa de protección de datos es **aplicable a partir del 25 de mayo de 2018**.

Para facilitar la privacidad de los usuarios, la Agencia Española de Protección de Datos (AEPD), la Oficina de Seguridad del Internauta (OSI) y el Instituto Nacional de Ciberseguridad (INCIBE), han elaborado una guía con una serie de recomendaciones importantes.

Protección de dispositivos

En primer lugar se **deben proteger los propios dispositivos**, especialmente los móviles, para **evitar pérdidas o robos**, y utilizar **sistemas de bloqueo de pantalla** como códigos numéricos, patrones u otros para impedir el acceso a la información que contienen.

Las **claves o contraseñas deben ser robustas**, es decir, **difíciles de descifrar**. Lo mejor es que tengan por lo menos ochos caracteres, compuestas por letras, números y símbolos del teclado, pero aleatorios, sin ningún significado concreto, y cambiarlas periódicamente.

Tampoco se debe usar la misma contraseña para varios servicios, porque si se accede a ella el riesgo para la información confidencial es mayor, ni compartirlas. Se pueden **usar patrones** que, con pequeñas variaciones, permiten generar muchas claves distintas y recordarlas fácilmente, o usar un **gestor de contraseñas**. Además, se pueden usar **programas de cifrado de información** para dificultar su acceso por personas no autorizadas.

También es necesario **realizar periódicamente copias de seguridad en otro soporte** para no perder nunca la información almacenada, en caso de pérdida o robo del dispositivo. Finalmente, es esencial **utilizar un buen antivirus**, que evite que ***apps* maliciosas** puedan eliminar o utilizar los datos almacenados sin conocimiento ni consentimiento del usuario.

Otro aspecto a tener en cuenta es la seguridad de las **redes públicas**, ya que **no cifran la información que transmiten** y no se sabe quién puede estar conectado, y quién puede tener acceso a la información. Por eso **no hay que realizar a través de ellas operaciones bancarias, compras online ni enviar información confidencial**.

Aplicaciones seguras

Nada es realmente gratuito en la web y, en muchos casos, las *apps* **comercializan los datos personales de los usuarios** sin que estos lo sepan. Por eso, para garantizar que las aplicaciones que se instalan en los dispositivos son seguras se deben **descargar sólo desde tiendas de apps oficiales**, que garantizan que han sido revisadas previamente. Y antes de instalarlas es necesario **consultar antes las valoraciones y comentarios de otros usuarios**, para comprobar que no presentan problemas de seguridad o de mal funcionamiento.

Hay que tener mucho **cuidado con las aplicaciones gratuitas** porque algunas, aparentemente inocentes, pueden tener **acceso a los datos más confidenciales**, por lo que hay que **revisar los permisos solicitados** (acceso a contactos, registro de llamadas, etc.) y en caso de duda no prestar el consentimiento para la instalación.

Aceptación de permisos en *apps* y redes sociales

Los usuarios están recibiendo una avalancha de mensajes similares como "**queremos seguir a tu lado**" o "**si no aceptas ya no podemos contactar contigo**", debido a la entrada en vigor del nuevo RGPD. A través de diversos medios como el correo electrónico, mensajes de texto, notificaciones al acceder a las apps o avisos en sitios webs y redes sociales sobre las ***cookies***, han solicitado **revisar las políticas de privacidad y protección de datos** y, de paso, continuar conectados a sus servicios.

Pero es muy importante **revisar en qué consisten estos cambios** y, sobre todo, **ayudar a los niños y jóvenes** en este proceso de revisión y darles buenos **consejos de privacidad en línea**. En la actualidad, muchos niños posan para

las cámaras o teléfonos móviles de sus padres, que cuelgan las fotos en redes sociales, por lo que tienen desde la infancia un **rastro digital** que va aumentando a medida que crecen y acceden a las nuevas tecnologías, donde se recogen **fotos, vídeos, comentarios, información de uso, geolocalización o perfiles online**, auténticos rastros que son difíciles de eliminar y que contribuirán más adelante a su **reputación online**.

El RGPD establece que cualquier **servicio que trate datos personales debe informar obligatoriamente al usuario** sobre quién lo hace, qué harán las empresas con ellos, por qué los tratan, cuánto tiempo los conservarán o a quién los comunicarán, información que, este caso los **padres de menores de 14 años** deben asegurarse de entender y, **si consideran que la información o permisos que solicita una *app* son excesivos para la funcionalidad que aporta, denegar la autorización**.

Además, hay que tener en cuenta que el RGPD **protege de manera especial los datos personales de los niños**, prohibiendo el empleo de esta información con fines de **mercadotecnia o elaboración de perfiles de personalidad o de usuario**, es decir, que **no es lícito comerciar con ellos**.

También hay que saber que el nuevo RGPD contempla el **derecho al olvido de los pequeños**, de manera que, aunque se hayan concedido determinados permisos a *apps* usadas por menores, es posible **revocar esos permisos o solicitar su rectificación**. Este derecho es muy útil si los **menores han concedido permisos de forma poco consciente** sobre los riesgos y, siendo ya mayores, desean revocarlos.

Asimismo, el RGPD regula el **derecho de oposición**, por el que los menores, sus padres o tutores legales pueden solicitar que **se retiren imágenes de aquéllos en plataformas online para las que no hayan dado antes su consentimiento**.

Qué tener en cuenta antes de conceder permisos

Así pues, antes de otorgar permisos en *apps* y redes sociales hay que tener en cuenta que **el consentimiento, con carácter general, debe ser libre, informado, específico e inequívoco, y en lenguaje comprensible, especialmente para los menores**.

No obstante, es muy probable que muchos niños, bombardeados por la **gran cantidad de alertas solicitando su consentimiento, hayan terminado aceptando las condiciones** que el servicio pedía sin recapacitar sobre sus riegos, para poder seguir utilizándolos. Por eso es recomendable que los padres **accedan a la configuración de los servicios que utilizan sus hijos**, como **redes sociales** (*Facebook, Instagram, Snapchat o YouTube*), **juegos online** y otras **aplicaciones en línea** de tipo lúdico, educativo o funcional.

En concreto, hay que **tratar de preservar**, en la medida de lo

posible, la información asociada a los siguientes permisos:

- **Visibilidad del menor a través de la información de registro o uso en la plataforma**, para que no se pueda localizar al niño en esa plataforma realizando una búsqueda a partir de su correo electrónico o su número de teléfono.

- **Información de actividad en tiempo real**, que proporciona a un posible acosador la posibilidad de actuar de forma impulsiva y perjudicial, sobre todo si esta información geoposiciona al menor.

- **Valorar la posibilidad de desactivar funciones como el historial de ubicaciones**, que muestra todos los lugares visitados, para evitar que se puedan trazar rutas habituales. Además, es aconsejable eliminar los datos que haya almacenado el servicio.

- **Acceso a cámara y a grabaciones de audio, imagen y vídeo**, ya que estos datos son los que permiten identificar con más facilidad a nuestros hijos y que con frecuencia son el objetivo de depredadores sexuales online. Por eso conviene ser restrictivos ya que, por ejemplo, una aplicación de juego online no necesariamente debe tener acceso a la galería del menor.

- **Registro del historial de búsqueda**, que puede dar información de gran valor tanto a proveedores con fines comerciales, como a terceros que puedan emplearla con fines malintencionados. Por ejemplo, una supuesta web de venta de entradas o calzado deportivo puede contactar con un niño si dispone de su historial de búsquedas y conoce sus preferencias, dándose casos de estafas online a menores.
- **Vinculación a datos bancarios o de tarjetas de crédito.** En muchas ocasiones, los dispositivos de los padres los utilizan o heredan los hijos, con cuentas o perfiles vinculados a información bancaria, con lo que pueden adquirir canciones en *Spotify* o mejoras para *Candy Crush* con un simple clic. En estos casos hay que estar atentos a estos permisos y supervisar cualquier compra que se haga desde móviles o tabletas.

- **Comprobar otra información del dispositivo**, como contactos, calendarios, actividad y otros datos almacenados en él. Como norma general es **conveniente inhabilitar** todas las aplicaciones que puedan recopilar información abusiva sobre los menores.

Cookies

Las cookies son archivos que **recogen y almacenas datos e información sorbe la navegación en Internet**, que se descargan y almacenan en los equipos informáticos. Las páginas

web que las utilizan están obligadas a **informar sobre su uso**, mediante un **mensaje sobreimpreso**, generalmente en la parte inferior de la pantalla, y un **enlace a otra página donde se detallen sus características**. Con esta información, los usuarios pueden decidir si las aceptan o no.

Además, los usuarios pueden **controlar el uso de las cookies mediante la configuración del navegador**, para rechazar todas, aceptar o rechazar las de determinadas páginas, aceptar sólo las de los sitios web visitados o hacer que todas se borren al cerrar el propio navegador.

Fallos de seguridad y protección de datos

Las tiendas online y las empresas que almacenen o traten **datos personales de sus usuarios** tienen obligación de adoptar medidas técnicas y organizativas que permitan garantizar **a los usuarios un nivel adecuado de seguridad**.

Además, desde la entrada en vigor del Reglamento Europeo de Protección de Datos, las **quiebras de seguridad** que afecten a los datos personales de los usuarios deberán comunicarse a la **Agencia Española de Protección de Datos en un plazo máximo de 72 horas**, junto con las medidas correctivas y preventivas adoptadas o propuestas.

Si los hechos suponen un **riesgo alto para los usuarios**, deberán comunicárselo junto con los datos del Delegado de Protección de Datos de la empresa, las consecuencias de la quiebra de seguridad y las medidas adoptadas o propuestas.

Derechos de los usuarios

Para asegurar la privacidad y la protección de los datos el RGPD otorga a los usuarios varios **derechos fundamentales**, que se pueden ejercer ante el Delegado de Protección de Datos y cuyo **ejercicio es gratuito**. Si no se atienden por la empresa, se puede acudir a la **Agencia Española de Protección de Datos (AEPD)**:

- **Derecho de información:** cuando se recaban datos de carácter personal el responsable del tratamiento debe informar de su **identidad**, los **fines que motivan la recogida**, especialmente si se trata de **elaborar perfiles**, **plazo de conservación** y su posible **cesión** o la **transferencia de datos a terceros**. Además, si los datos **no se han cedido voluntariamente**, se informará sobre su procedencia, incluso si se trata de fuentes de acceso público.

- **Derecho de acceso:** permite al usuario dirigirse al responsable del tratamiento para saber si se están tratando o no y obtener una copia de todos los datos almacenados o que se manejen y el uso que se hace de ellos y sus fines.

- **Derecho de rectificación:** el usuario puede pedir la rectificación de sus datos personales que sean incorrectos o estén incompletos, justificándolo en caso necesario.

- **Derecho de oposición:** el usuario puede oponerse a uno o varios tratamientos de sus datos en cualquier mo-

mento y sin ningún tipo de justificación (por ejemplo, cancelar el envío de emails informativos o publicitarios).

- **Derecho de supresión o "derecho al olvido":** en cualquier momento se puede solicitar la cancelación o borrado de los datos de una persona, eliminando de las bases de datos toda la información personal. SI la eliminación no fuese posible por motivos legales (por ejemplo, la conservación de facturas durante los plazos legales), se procederá al bloqueo de dichos datos y al borrado de los que no sean imprescindibles. En todo caso, se informará al solicitante de las medidas adoptadas.

- **Derecho a revocar el consentimiento:** también se puede retirar el consentimiento otorgado previamente para el tratamiento de datos con una determinada finalidad sin que esto suponga, a priori, una limitación en el uso de productos o servicios.

- **Derecho a la portabilidad de los datos:** el usuario puede solicitar que se le envíe una copia de los datos personales que le incumban en un formato de uso común o que se transfieran estos datos directamente a un tercero. No obstante, se puede limitar legalmente por motivos de interés público.

- **Derecho a no ser objeto de decisiones individuales automatizadas:** los responsables del tratamiento de datos no podrán tomar decisiones individualizadas de forma automática con los datos que dispongan de los usuarios, incluyendo la elaboración de perfiles, es decir, sin aceptación expresa del titular de dichos datos.

Internet Segura for Kids (is4K)

Para más información se puede contactar con **Internet Segura for Kids (IS4K), que es el Centro de Seguridad en Internet para menores de edad en España** y tiene por objetivo la promoción del uso seguro y responsable de Internet y las nuevas tecnologías entre los niños y adolescentes.

IS4K está liderado y coordinado por la **SESIAD (Secretaría de Estado para la Sociedad de la Información y Agenda Digital)**, con el **soporte de Red.es**, y ejecuta sus servicios a través del **INCIBE (Instituto Nacional de Ciberseguridad)**, en colaboración con otras entidades de referencia. En línea con la estrategia Europea BIK (*Better Internet for Kids*), forma parte de la red paneuropea INSAFE de Centros de Seguridad en Internet y está cofinanciado por la Comisión Europea.

Las principales tareas que tiene encomendadas son:

- **Sensibilizar y formar** a menores, jóvenes, familias, educadores y profesionales del ámbito del menor, a través del desarrollo de campañas, iniciativas y programas de ámbito nacional.
- **Ofrecer un servicio de línea de ayuda** con el que asesorar y asistir a menores, familias, educadores y profesionales del ámbito del menor sobre cómo hacer frente a los riesgos de Internet: contenidos perjudiciales, contactos dañinos y conductas inapropiadas.
- **Organizar el Día de Internet Segura** (*Safer Internet Day)* en España.
- **Reducir la disponibilidad de contenido criminal en Internet**, principalmente de **abuso sexual infantil**, dando soporte a las Fuerzas y Cuerpos de Seguridad del Estado.

PARA MÁS INFORMACIÓN:

Agencia Española de Protección de Datos (AEGPD): **https://www.aepd.es - Tlfs: 901.100.099 y 912.663.517.**

Oficina de Seguridad del Internauta (OSI): **https://www.osi.es/es**

Instituto Nacional de Ciberseguridad (INCIBE): **https://www.incibe.es - Tlfs: 912.127.626 y 987.877.189.**

Internet Segura for Kids (is4K): **https://www.is4k.es - Tlf: 900.116.116**.

Programa subvencionado por el
Ministerio de Sanidad, Consumo y Bienestar Social
Agencia Española de Consumo, Seguridad
Alimentaria y Nutrición (AECOSAN)

Federación UNAE 2018
C/ Villanueva, 8 - 3º
28001 Madrid
Tlf: 91-575.72.19
informacion@federacionunae.com
www.federacionunae.com

FEDERACIÓN
DE LA UNIÓN NACIONAL
DE CONSUMIDORES
Y AMAS DE HOGAR
DE ESPAÑA