

EL RGPD UE 2016/679 EN APLICACIÓN

Principios fundamentales de protección de datos (I)

En este boletín y siguientes trataremos un aspecto fundamental en la aplicación del RGPD tanto por parte de responsables del tratamiento como encargados del tratamiento.

El artículo 5 del RGPD establece los principios fundamentales que deben regir todo tratamiento de datos personales. Estos principios son esenciales para garantizar el respeto a los derechos de los interesados y la licitud del tratamiento. Su cumplimiento no es optativo: constituye una obligación legal para el responsable y, por extensión, para el encargado del tratamiento. El incumplimiento puede derivar en sanciones graves recogidas en el RGPD.

Los Principios del artículo 5.1 del RGPD que iremos abordando en sucesivos boletines son los siguientes:

- Licitud, lealtad y transparencia
- Limitación de la finalidad
- Minimización de datos
- Exactitud
- Limitación del plazo de conservación
- Integridad y confidencialidad.

El artículo 5.2 del RGPD establece, además, que el responsable del tratamiento debe cumplir con los principios anteriores y ser capaz de demostrar dicho cumplimiento, promoviendo la responsabilidad proactiva.

Contenido

1. Principios fundamentales de protección de datos (I).
2. Acceso indebido al historial clínico en un Servicio Público de salud.
3. ¿Quién y cuándo se puede acceder a un historial clínico? (II).
4. Riesgos para la protección de datos al utilizar servicios que convierten fotografías a formato *Ghibli* o similares para analizar la aplicación del derecho.
5. ¿Cómo puedo proteger mi dominio *web* ante un *Cybersquatting*? (II).



IMPORTANTE

El artículo 5 del RGPD establece principios esenciales para el tratamiento de datos personales, cuya observancia es obligatoria y su incumplimiento puede resultar en sanciones graves

SANCIONES DE LA AEPD

Acceso indebido al historial clínico en un Servicio Público de salud

En la resolución de la [AEPD](https://www.aepd.es/documento/ps-00250-2021.pdf) <https://www.aepd.es/documento/ps-00250-2021.pdf> se apercibe, a un Servicio Público de Salud, ya que no puede ser sancionado debido a un acceso ilícito a un historial clínico.

El reclamante manifiesta en su denuncia que se produjeron accesos indebidos a su historia clínica por parte de una trabajadora del Servicio Público de Salud. El acceso se realizó sin relación asistencial que lo justificara. En el escrito de reclamación se aportaron los certificados de accesos al historial clínico, que fueron solicitados a través de la vía judicial. La investigación acreditó que la trabajadora accedió reiteradamente a datos de salud del reclamante, considerados especialmente protegidos según el artículo 9 del RGPD.

El objeto de la reclamación se centró en la vulneración del principio de confidencialidad e integridad de los datos. La AEPD concluyó que el Servicio Público de Salud no implantó adecuadamente las medidas técnicas y organizativas necesarias. En la resolución se hace referencia a la falta de verificación por parte de la entidad reclamada del perfil de acceso del usuario.

Se han infringido por lo tanto el artículo 5.1.f RGPD del principio de confidencialidad e integridad de los datos y el artículo 32 del RGPD sobre la seguridad del tratamiento. Aunque no se impuso sanción económica por tratarse de una entidad pública, se dictó apercibimiento como medida correctiva.

El artículo 5.1.f del RGPD exige garantizar la seguridad de los datos personales, protegiéndolos contra el tratamiento no autorizado, pérdida, destrucción o daño accidental.



IMPORTANTE

Los accesos ilícitos se evitarían implementando controles efectivos de acceso bajo fines estrictamente asistenciales y realizando análisis de riesgos.

LA AEPD ACLARA

¿Quién y cuándo se puede acceder a un historial clínico? (II)

El acceso al historial clínico de un paciente está legitimado en la atención eficaz y eficiente para su salud, especialmente en casos de emergencia vital, tal y como lo indica la AEPD en su [guía para profesionales del sector sanitario](#). No obstante, el responsable del tratamiento tiene la obligación de adoptar las políticas de control de acceso, de registro y trazabilidad de dichos accesos para detectar cualquier diligencia que se pueda producir.

El acceso al historial clínico por parte de los profesionales sanitarios implica unos límites y garantías: está reservado exclusivamente al personal sanitario que participa directamente en la atención del paciente. Esto incluye médicos, enfermeros y residentes durante su formación, siempre que la finalidad sea asistencial. Solo se puede acceder a los datos necesarios para el tratamiento, y si no es imprescindible conocer la identidad del paciente, se debe evitar su visualización.

En centros sociosanitarios o privados concertados, también se permite el acceso si es necesario para prestar asistencia sanitaria a un paciente derivado a ese centro, pero limitado a la información imprescindible. Además, los Comités de Ética Asistencial pueden acceder a datos cuando sea necesario para emitir opiniones, siempre bajo acuerdo de confidencialidad. Solo cuando sea precisa la identificación del paciente para poder emitir el informe u opinión correspondiente, se podría acceder a ella.



IMPORTANTE

El principio de minimización de datos y el deber de secreto son pilares esenciales para evitar accesos ilícitos a los datos de salud del historial clínico.

ACTUALIDAD LOPD



Riesgos para la protección de datos al utilizar servicios que convierten fotografías a formato *Ghibli* o similares para analizar la aplicación del derecho

Fuente: [AEPD](#)

(7 de abril de 2025). La Agencia Española de Protección de Datos, en su labor de concienciación, ofrece consejos a la ciudadanía sobre los aspectos que deben tener en cuenta para la protección de sus datos personales.

En los últimos días se ha hablado mucho de una nueva práctica que podría poner en riesgo la protección de los datos personales de los usuarios: la utilización de aplicaciones y servicios en línea que permiten convertir fotografías personales en imágenes con estilo "Ghibli" o similares. Estas herramientas, aunque atractivas y aparentemente inofensivas, pueden tener implicaciones para la privacidad y seguridad de la información personal.

Los riesgos detectados para la protección de los datos personales tienen que ver con los siguientes aspectos:

1. **Acceso y tratamiento de datos personales:** Muchas de estas aplicaciones solicitan el acceso a la galería de fotos del dispositivo, lo que implica conceder el acceso tanto a datos personales propios como a los de terceras personas, no solo de la foto remitida, sino potencialmente de todas las fotos de la galería. Además, en algunos casos, las imágenes no se procesan exclusivamente en el dispositivo, sino que se suben a servidores externos, lo que incrementa el riesgo de exposición.
2. **Transparencia en el uso de los datos:** En ocasiones, las aplicaciones o servicios no proporcionan suficiente información sobre qué se hace con las imágenes una vez subidas, si se transmiten a otras entidades o cuánto tiempo se conservan.
3. **Almacenamiento y uso de imágenes:** En ciertos casos, los datos obtenidos de las fotografías podrían ser almacenados o reutilizados por las empresas desarrolladoras de las aplicaciones para fines comerciales o publicitarios, o para el entrenamiento de algoritmos.

Puede ver información relacionada en el siguiente enlace:

[Recomendación para usuarios en la utilización de chatbots con IA](#)

EL PROFESIONAL RESPONDE

¿Cómo puedo detectar una campaña de *Cybersquatting*?

(II)

El *cybersquatting*, tal y como vimos en el boletín pasado es una técnica que consiste en el registro malicioso de dominios similares al de una marca con fines fraudulentos. Debido a la multitud de combinaciones posibles (añadiendo, sustituyendo o eliminando caracteres), se recomienda el uso de herramientas automatizadas para detectar estos ataques.

Una primera opción es usar buscadores de dominios de proveedores de servicios de Internet (*ISP*). Al simular la compra de un dominio, estas herramientas generan variantes del nombre introducido e indican cuáles ya están registrados, lo que permite identificar posibles amenazas.

Existen herramientas online como, por ejemplo, *dnstwister* que permite introducir el dominio propio y genera un listado de variaciones, señalando cuáles han sido registradas. Además, indica si están aparcadas o asociadas a actividades de phishing, y permite descargar informes detallados.

Entre los fraudes más comunes en este tipo de ataques se encuentran: extorsión económica a la marca legítima, compra anticipada o una vez caducado el dominio original, campañas de *phishing* y daño reputacional intencionado.

Una buena acción para protegerse ante este tipo de ataques es monitorizar continuamente variantes del dominio similares al de la marca registrada y realizar comprobaciones manuales en el caso de que sea necesario.



IMPORTANTE

Este fraude puede afectar a cualquier empresa. La vigilancia activa de las variantes del dominio corporativo permite detectarlo a tiempo y tomar las medidas legales o técnicas más adecuadas.