

EL RGPD UE 2016/679 EN APLICACIÓN

Integridad y confidencialidad: garantías esenciales del tratamiento de datos

Uno de los principios básicos en los que se fundamenta el Reglamento General de Protección de Datos (RGPD) es garantizar la integridad y la confidencialidad de los datos personales.

El concepto de integridad que se recoge en el artículo 5.1.f del RGPD nos indica que los datos deben ser mantenidos por el responsable del tratamiento exactos y completos, sin realizar alteraciones no autorizadas. No se trata solo de evitar modificaciones indebidas, sino también de garantizar que las actualizaciones se realicen de forma controlada y trazable. Por ejemplo, una clínica médica debe asegurarse de que el historial de un paciente no pueda alterarse sin autorización y de que cualquier cambio quede registrado.

La confidencialidad que se recoge también en el artículo 5.1.f del RGPD se refiere a garantizar un acceso controlado y limitado a la información personal. Las empresas deben aplicar controles de acceso basado en roles y privilegios mínimos en el que los usuarios solamente accederán a la información estrictamente necesaria para su trabajo.

En definitiva, la integridad y la confidencialidad garantizan que los datos personales sean exactos, protegidos y accesibles solo para quien corresponda, asegurando un tratamiento responsable, seguro y conforme al RGPD.

Contenido

1. Integridad y confidencialidad: garantías esenciales del tratamiento de datos.
2. Sancionado un establecimiento hotelero con 9.000€ por el escaneado del DNI de los huéspedes.
3. Políticas de privacidad bajo el RGPD: el consentimiento informado en la era digital (II).
4. Laboratorio de Ciberseguridad.
5. Obligaciones clave de cumplimiento según la NIS2: una guía práctica.



IMPORTANTE

Prevenir accesos ilícitos exige firewalls, detección de intrusiones, monitorización continua y revocar permisos del personal laboral al cambiar funciones o al finalizar la relación laboral para proteger los datos.

SANCIONES DE LA AEPD

Sancionado un establecimiento hotelero con 9.000€ por el escaneado del DNI de los huéspedes

La Agencia Española de Protección de Datos (AEPD) en su [expediente sancionador](https://www.aepd.es/documento/ps-00421-2024.pdf) <https://www.aepd.es/documento/ps-00421-2024.pdf> impuso una multa de 9.000 euros a un establecimiento hotelero por incumplimiento del principio de minimización de datos.

El cliente presentó una reclamación ante la AEPD en la que alegaba que, al registrarse, se le exigió el escaneo completo de su DNI, ante su negativa, el personal copió manualmente sus datos personales.

En el proceso de investigación, la AEPD comprobó que el establecimiento llevaba a cabo el escaneo íntegro de los documentos de identidad de los huéspedes, conservando imágenes con datos que no son necesarios, como la fotografía, número de soporte o firma, alegando el cumplimiento del Real Decreto 933/2021 sobre registro documental de viajeros. Este Real Decreto solamente obliga a recabar determinados datos, sin exigir la copia completa.

La Agencia concluyó que se vulneró el principio de minimización de datos (art. 5.1.c del RGPD), puesto que trató información excesiva para el fin perseguido, además el procedimiento carecía de proporcionalidad, ya que existían medios menos intrusivos, como por ejemplo la verificación visual.

En la resolución, se le indica, además, que debe modificar su sistema de registro y eliminar los documentos de identidad escaneados almacenados en su sistema.

El incumplimiento de los principios generales supone tratar datos de forma indebida, vulnerar los derechos de los interesados y afrontar sanciones, responsabilidades legales y daños reputacionales.



IMPORTANTE

Se deberán evitar tratamientos innecesarios, limitar los datos recabados a lo estrictamente necesario y garantizar que sean pertinentes y justificables para la finalidad del tratamiento.

LA AEPD ACLARA

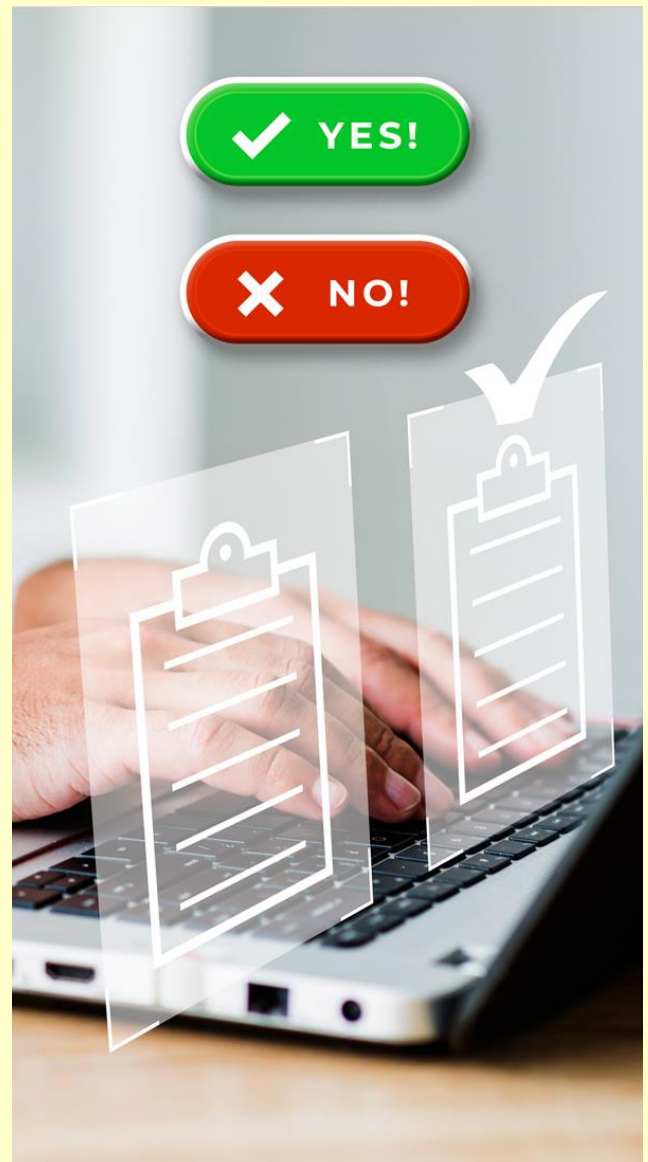
Políticas de privacidad bajo el RGPD: el consentimiento informado en la era digital (II)

Otro de los grandes cambios que introdujo el RGPD fue la regulación del consentimiento. Frente al modelo anterior, basado en la aceptación tácita o en la fórmula “He leído y acepto la política de privacidad”, el Reglamento exige que este consentimiento sea libre, informado, específico e inequívoco.

La AEPD, en su informe [sobre políticas de privacidad en Internet](#), detectó que numerosas empresas continúan recurriendo a mecanismos de aceptación globales, que agrupan todas las finalidades sin diferenciación. Este enfoque que incumple lo dispuesto en el RGPD compromete la validez del consentimiento.

El consentimiento informado requiere que el usuario conozca la identidad del responsable, las finalidades específicas del tratamiento, los tipos de datos que se van a recoger, el derecho a retirar el consentimiento, la existencia de decisiones automatizadas y los riesgos en transferencias internacionales sin garantías adecuadas. La AEPD recomienda ofrecer esta información directamente en el formulario de recogida de datos, de forma resumida pero clara, y detallar el resto en la política de privacidad.

Debe explicarse también cómo ejercer el derecho a retirar el consentimiento, facilitando un correo o formulario electrónico y garantizando que retirarlo sea tan sencillo como otorgarlo.



IMPORTANTE

Cuando el consentimiento se incluye dentro de una declaración más amplia, debe mostrarse de forma clara, separada y comprensible, para evitar ambigüedades o confusión.

ACTUALIDAD CIBERSEGURIDAD Y PRIVACIDAD

Laboratorio de Ciberseguridad

Fuente: [INCIBE](#)

España Digital 2026

El Laboratorio de Ciberseguridad tiene como misión principal incrementar la confianza digital y potenciar la ciberseguridad y la resiliencia en la industria (en colaboración con fabricantes e investigadores) a través de rigurosos ensayos en tecnologías emergentes como el 5G, los sistemas de control industrial, el Internet de las Cosas (IoT), la inteligencia artificial o los vehículos conectados. Como test center, posibilita que los centros de investigación, empresas y agentes del sector de la ciberseguridad puedan ensayar diferentes soluciones que estén desarrollando, reduciendo así el coste y el tiempo necesario para incorporar al mercado nuevos productos. El Laboratorio de Ciberseguridad actúa, además, como campo de pruebas donde expertos e investigadores pueden simular amenazas cibernéticas y desarrollar herramientas y estrategias para proteger nuestra infraestructura digital.

Objetivos

- **Elevar** la ciberseguridad y la resiliencia, además de aumentar la confianza digital en las tecnologías emergentes como las comunicaciones **5G**, el **Internet de las Cosas (IoT)** o la **Inteligencia Artificial (IA)**.
- **Posibilitar** que los centros de investigación, empresas y demás agentes relacionados puedan ensayar diferentes **soluciones** que estén desarrollando, reduciendo el coste y el tiempo necesario para poner en el mercado nuevos productos.

Puede ver información relacionada en el siguiente enlace:

[Evaluación de ciberseguridad de dispositivos conectados \(IoT\)](#)

[Evaluación de ciberseguridad de redes 5G](#)

EL PROFESIONAL RESPONDE

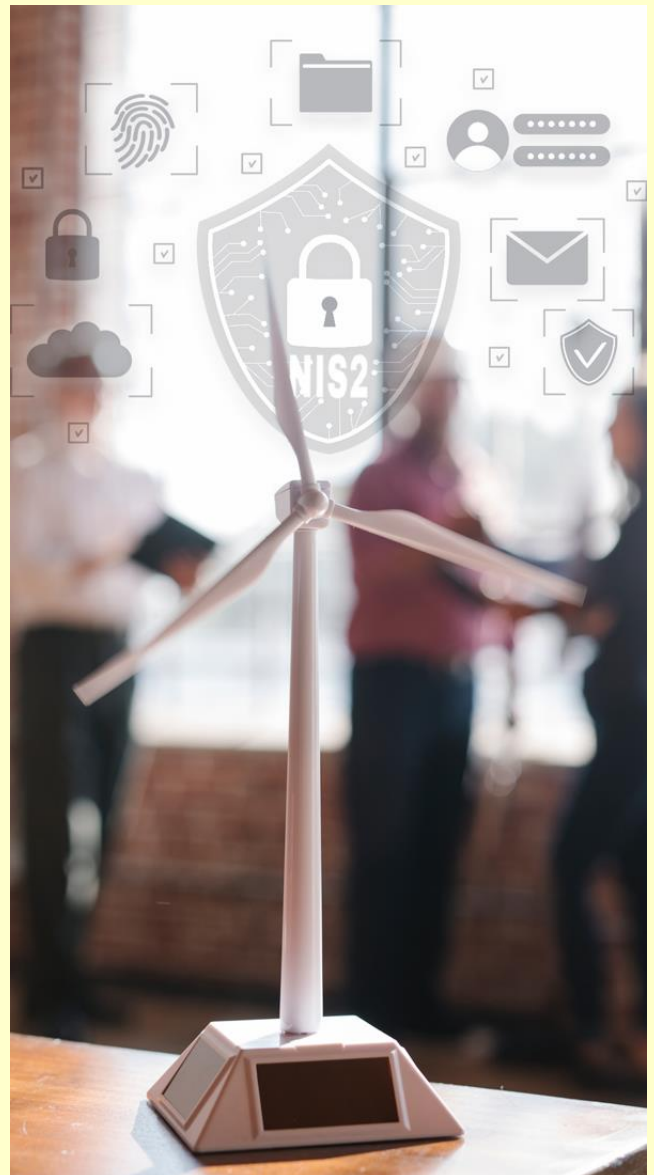
Obligaciones clave de cumplimiento según la NIS2: una guía práctica

La Directiva NIS2 marca un nuevo estándar en materia de ciberresiliencia en la Unión Europea, obligando a las organizaciones a adoptar un enfoque preventivo y estratégico.

El punto de partida es el análisis de riesgos, el cual, tiene que reflejar las amenazas reales que pueden afectar a la continuidad del servicio y la operación diaria de la organización, no solo riesgos teóricos. Por ejemplo, una compañía energética que gestiona redes de distribución debe identificar qué plataformas de supervisión son críticas y evaluar cómo un ciberataque podría interrumpir el suministro o afectar la seguridad física de los usuarios. Sobre esa base, la organización debe implantar medidas técnicas y organizativas proporcionadas, ya sea reforzando el control de accesos, estableciendo segmentación de redes o revisando la seguridad de proveedores que intervienen en el mantenimiento remoto de sistemas clave.

La directiva refuerza la detección y respuesta a incidentes, esto implica tiempos de reacción claros, equipos preparados y un flujo de comunicación eficaz, tanto dentro de la organización como con las autoridades competentes.

Otro pilar esencial es la continuidad de negocio: si un ataque inutiliza un sistema, deben existir planes para restaurar el servicio con rapidez y mantener las funciones esenciales.



IMPORTANTE

La NIS2 obliga a realizar revisiones y auditorías periódicas para garantizar una eficacia continua, incorporando la gobernanza y la seguridad como parte esencial de la gestión corporativa.