

EL RGPD UE 2016/679 EN APLICACIÓN

Principio de exactitud y actualización de datos personales

Uno de los principios fundamentales del RGPD es el principio de exactitud de datos, que supone que los datos personales deben ser exactos y, en el caso de que sea necesario, mantenerse actualizados.

El responsable del tratamiento ha de disponer medidas razonables con las que se pueda verificar la calidad de los datos, según el contexto y los fines para los que se recogieron. Para garantizar la exactitud de los datos durante el proceso de recogida, por ejemplo, se pueden incorporar mecanismos de validación. Así mismo, puede implantar procedimientos de evaluación y revisión habilitando canales para que los interesados actualicen su información.

La utilización de una base de datos personales que no sean exactos o estén desactualizados pueden provocar riesgos para los derechos y libertades, esto son algunos de ellos.

- Decisiones erróneas con efectos jurídicos negativos para el interesado, por ejemplo, la denegación de un crédito.
- Daños económicos como pérdidas financieras, cobros indebidos o perjuicios por exclusión de servicios.
- Pérdida de confidencialidad al comunicar información a destinatarios incorrectos al tener los datos desactualizados.

Contenido

1. Principio de exactitud y actualización de datos personales.
2. Sancionada con 40.000 euros una entidad de prevención de riesgos laborales y vigilancia de la salud por vulnerar la confidencialidad de los datos de salud.
3. Privacidad por defecto: recomendaciones prácticas para responsables y encargados del tratamiento (II).
4. Inyección NoSQL: Cómo una entrada maliciosa puede comprometer tu aplicación.
5. Decálogo de Ciberseguridad: Centro Criptológico Nacional.



IMPORTANTE

El responsable comunicará a los destinatarios toda rectificación, supresión o limitación, salvo imposibilidad o esfuerzo desproporcionado, e informará al interesado.

SANCIONES DE LA AEPD

Sancionada con 40.000 euros una entidad de prevención de riesgos laborales y vigilancia de la salud por vulnerar la confidencialidad de los datos de salud

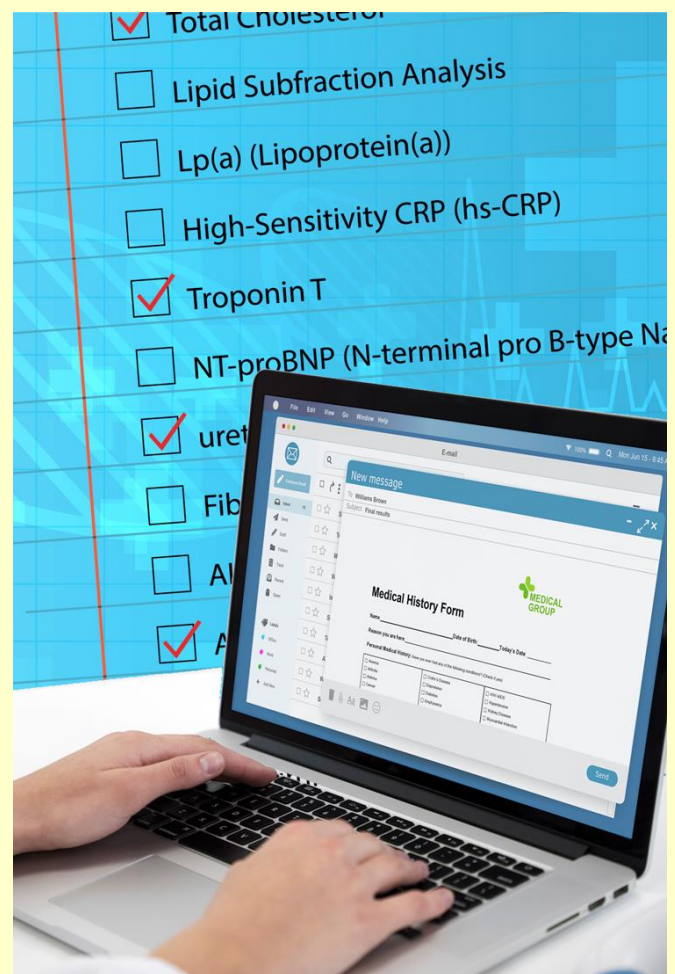
La Agencia Española de Protección de Datos (AEPD) en el [expediente sancionador https://www.aepd.es/documento/ps-00106-2024.pdf](https://www.aepd.es/documento/ps-00106-2024.pdf) impuso una multa de 40.000 euros por vulnerar el principio de integridad y confidencialidad de los datos.

El reclamante que interpuso la denuncia manifestó que, tras acudir a un reconocimiento médico por parte de la empresa de Servicio de Prevención sancionada, un compañero le advirtió que después de que, al descargar su propio informe desde la web del Servicio de Prevención, el documento contenía por error pruebas médicas del reclamante. Ante esta situación, el delegado de protección de datos de la entidad reconocía la incidencia, se eliminó el documento y se solicitó al tercero que destruyera la información que había recibido de forma indebida.

En su proceso de investigación la AEPD constató que el acceso a los datos de salud se produjo por un error humano en la mecanización del escaneado, al haberse anexo por error pruebas médicas al informe de otro paciente.

En el escrito de reclamaciones la AEPD valoró positivamente la exposición de las medidas aplicadas por la reclamada antes del suceso, tales como formación inicial y continua al personal sanitario de el uso de las herramientas y campañas periódicas de sensibilización.

La vulneración del principio de integridad y confidencialidad de los datos personales constituye una infracción muy grave.



IMPORTANTE

las actuaciones correctivas a posteriori no eximen de la responsabilidad por la infracción ya cometida.

LA AEPD ACLARA

Privacidad por defecto: recomendaciones prácticas para responsables y encargados del tratamiento (II)

Aplicar el principio de protección de datos por defecto implica adoptar decisiones concretas en el diseño, configuración y operación de sistemas y procesos.

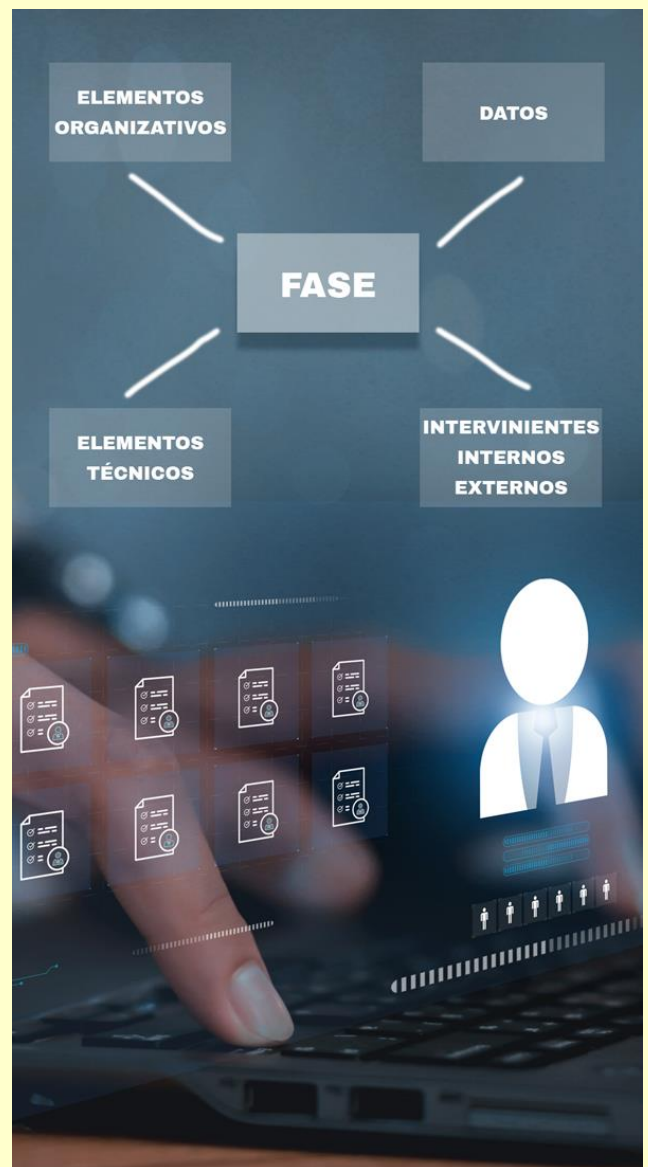
En primer lugar, en [la guía de la AEPD](#), se recomienda establecer perfiles de usuario con privilegios mínimos, configurando el acceso solo a los datos imprescindibles. Asimismo, deben limitarse los formularios para evitar campos innecesarios, restringiendo el uso de datos opcionales o sensibles.

Otra medida fundamental es implementar sistemas que controlen por defecto la visibilidad de datos personales, como la configuración de privacidad de cuentas o plataformas digitales. Por ejemplo, los ajustes iniciales deben ocultar datos frente a terceros salvo que el usuario los habilite de forma expresa.

La guía también destaca la importancia de definir políticas de retención automatizadas, asegurando la supresión o anonimización de datos una vez alcanzada su finalidad.

Desde el punto de vista organizativo, es necesario formar al personal en los principios de privacidad por defecto, y documentar las decisiones adoptadas como parte del principio de responsabilidad proactiva.

Estas recomendaciones permiten a los responsables y encargados cumplir con el RGPD de manera eficiente, demostrando diligencia ante cualquier requerimiento de la autoridad de control o de los interesados.



IMPORTANTE

Por defecto, el tratamiento debe configurarse para que solo se recaben los datos estrictamente necesarios para la finalidad.

ACTUALIDAD CIBERSEGURIDAD Y PRIVACIDAD

Inyección NoSQL: Cómo una entrada maliciosa puede comprometer tu aplicación

Fuente: [INCIBE](#)

Publicado el 20/06/2025

Dada la creciente proliferación de las bases de datos NoSQL en aplicaciones modernas, es fundamental que los desarrolladores y los equipos de seguridad comprendan los riesgos asociados con las inyecciones NoSQL. Este artículo analiza las amenazas y el impacto de estas vulnerabilidades, las técnicas que los atacantes utilizan para descubrir y explotar puntos débiles en las aplicaciones y las mejores prácticas para protegerse contra estos tipos de ataque. A través de una estrategia de defensa en profundidad, que combina validación de entradas, consultas seguras, controles de acceso estrictos y monitorización continua, las organizaciones podrán fortalecer la seguridad de sus aplicaciones frente a las inyecciones NoSQL y mitigar los riesgos asociados.

A diferencia de las bases de datos SQL tradicionales, que utilizan un lenguaje estructurado (SQL) para realizar consultas, las bases de datos NoSQL pueden manejar estructuras de datos no relacionales y permiten consultas más flexibles y, a menudo, menos estrictas. Por ejemplo, en las bases de datos NoSQL, las consultas pueden variar significativamente en su formato, desde documentos JSON en MongoDB, hasta consultas basadas en grafos en Neo4j. Esta flexibilidad, combinada con la falta de tipado estricto y validación en algunas implementaciones, puede llevar a fallos de seguridad significativos.

A menudo, los desarrolladores y equipos de seguridad subestiman los riesgos de seguridad asociados con las bases de datos NoSQL debido a la falta de conocimientos especializados y a la **suposición errónea de que las inyecciones relacionadas con las BBDD son un problema exclusivo de SQL**. Sin embargo, en la categoría de inyecciones del OWASP, esta vulnerabilidad ocupa la tercera posición. [El 94% de las aplicaciones evaluadas presentaron algún tipo de inyección, con una tasa máxima de incidencia del 19% y una tasa media de incidencia del 3%, acumulando un total de 274,000 ocurrencias.](#)

Las inyecciones NoSQL, que afectan a las bases de datos NoSQL, como MongoDB, CouchDB, o Cassandra, ocurren cuando un atacante manipula las entradas de usuario para alterar las consultas que se realizan a una base de datos NoSQL. Los ataques de inyección NoSQL pueden ocurrir en diferentes partes de una aplicación en comparación con las inyecciones SQL tradicionales. Mientras que las inyecciones SQL se ejecutan típicamente dentro del motor de la base de datos, las variantes NoSQL pueden ejecutarse en la capa de aplicación o en la capa de base de datos, dependiendo de la API NoSQL utilizada y el modelo de datos. Por lo general, estos ataques se llevan a cabo donde la cadena maliciosa es analizada, evaluada o concatenada en una llamada de API NoSQL (...)

Puede ver información relacionada en el siguiente enlace:

[Inyección NoSQL: Cómo una entrada maliciosa puede comprometer tu aplicación](#)

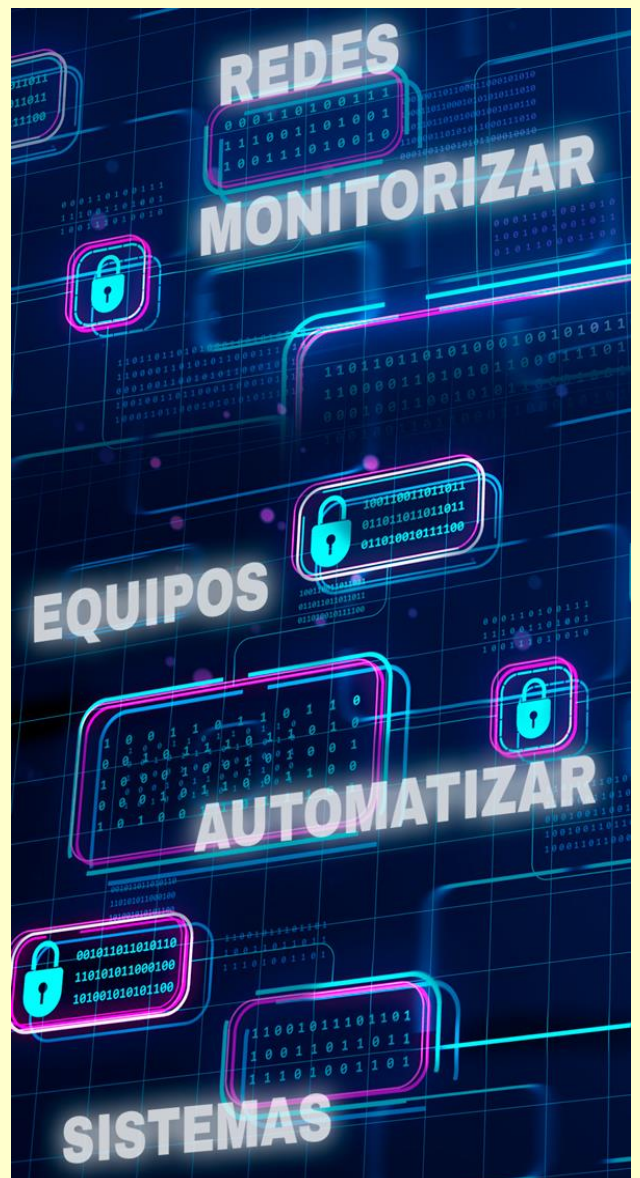
EL PROFESIONAL RESPONDE

Decálogo de Ciberseguridad: Centro Criptológico Nacional

El Centro Criptológico Nacional (CCN) es el organismo adscrito al Centro Nacional de Inteligencia. Actúa como autoridad pública para armonizar el uso de procedimientos de cifrado, proteger las tecnologías de la información en el marco de la administración pública, orientar la compra coordinada de soluciones criptográficas y formar a los especialistas de la Administración.

En la página web del CCN encontramos en el apartado de comunicación un [Decálogo de ciberseguridad](#) que supone una herramienta muy útil para que las entidades apliquen medidas de seguridad en el ámbito de la ciberseguridad y minimizar así los riesgos a los que todas las empresas públicas y privadas estamos expuestos. Los 10 puntos del decálogo son:

- 1º Aumentar la capacidad de vigilancia de las redes y los sistemas.
- 2º Monitorización y correlación de eventos.
- 3º Política de seguridad corporativa restrictiva.
- 4º Configuraciones de seguridad en todos los componentes de la red corporativa.
- 5º Uso de productos, equipos y servicios confiables y certificados.
- 6º Automatizar e incrementar el intercambio de información.
- 7º Compromiso de la Dirección con la ciberseguridad.
- 8º Formación y sensibilización de usuarios.
- 9º Atenerse a la legislación y buenas prácticas.
- 10º Trabajar como si los sistemas estuviesen comprometidos.

**IMPORTANTE**

Las entidades deben realizar un ajuste progresivo en sus activos con: autenticación, cifrado, segregación, monitorización y auditorías en ciberseguridad.