

EL RGPD UE 2016/679 EN APLICACIÓN

Plazos de Conservación: seguridad jurídica y reducción de riesgos

Los datos personales no deben conservarse más tiempo del estrictamente necesario para cumplir con la finalidad para la que fueron recogidos. El responsable del tratamiento debe cumplir este principio de limitación del plazo de conservación, que se encuentra recogido en el artículo 5.1.e del RGPD.

La aplicación práctica de este principio supone que las entidades han de documentar los plazos en políticas internas, y establecer procedimientos de revisión y supresión de los datos personales. Mantener bases de datos sin necesidad no solo incrementa los riesgos de seguridad, sino que también puede suponer una infracción sancionable.

Un ejemplo claro lo encontramos en el sector sanitario: el artículo 17.1 de la Ley 41/2002, básica reguladora de la autonomía del paciente establece que la historia clínica debe conservarse, con carácter general, durante un mínimo de cinco años contados desde la fecha de alta de cada proceso asistencial. Una vez transcurrido dicho plazo, y salvo que otra norma exija su conservación, los datos deben eliminarse o anonimizarse para fines estadísticos o de investigación.

Las entidades tienen que planificar cuánto tiempo mantendrán cada categoría de datos y suprimirlos o anonimizarlos una vez transcurrido dicho periodo.

Contenido

1. Plazos de Conservación: seguridad jurídica y reducción de riesgos.
2. Sancionado un centro especial de empleo por incluir a un trabajador en un grupo de WhatsApp sin consentimiento.
3. Políticas de privacidad bajo el RGPD: el reto de informar de forma clara y comprensible (I).
4. El Centro Criptológico Nacional resuelve las dudas más frecuentes sobre su Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC).
5. Alta dirección bajo NIS2: responsabilidad y oportunidad.



IMPORTANTE

En las políticas de privacidad es obligatorio informar a los interesados sobre los plazos de conservación de sus datos, ya sea indicando un periodo exacto o explicando el criterio que se aplicará para decidirlo.

SANCIONES DE LA AEPD

Sancionado un centro especial de empleo por incluir a un trabajador en un grupo de WhatsApp sin consentimiento

La Agencia Española de Protección de Datos (AEPD) en su [expediente sancionador https://www.aepd.es/documento/ps-00393-2024.pdf](https://www.aepd.es/documento/ps-00393-2024.pdf) impuso una multa a un centro especial de empleo por un uso indebido de WhatsApp como canal corporativo de comunicación con su personal laboral.

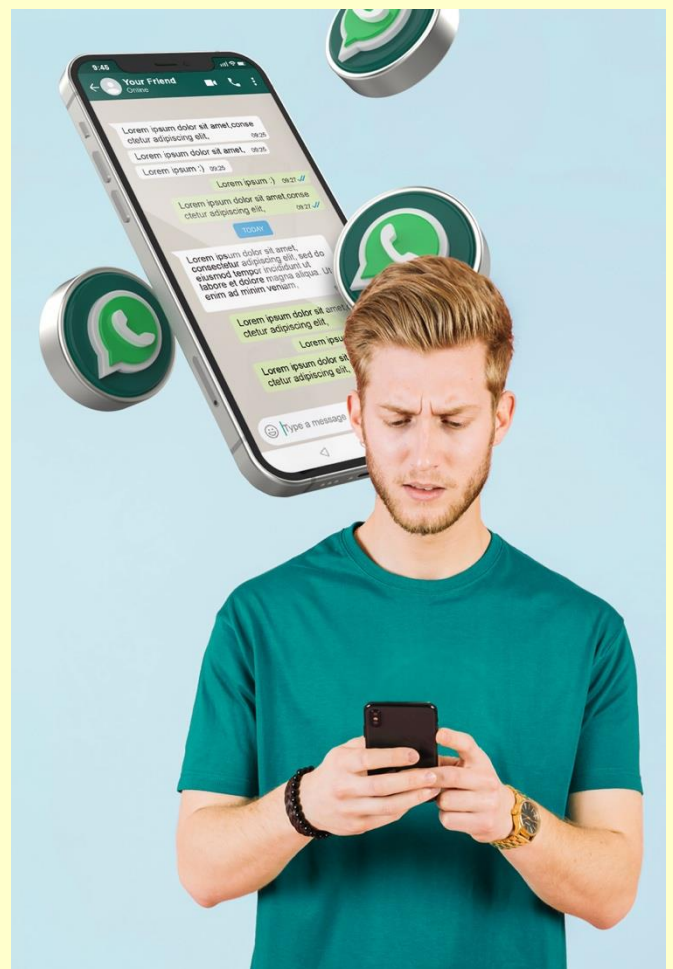
El reclamante fue contratado como teleoperador en la modalidad de teletrabajo. La coordinadora le incluyó sin solicitar el consentimiento, ni proporcionarle un dispositivo corporativo en un grupo de WhatsApp corporativo para informar sobre asuntos de índole laboral y organizativo. En la reclamación señala también, que tenía una recepción continua de notificaciones y llamadas fuera del horario laboral.

La AEPD constató que el número de teléfono personal se trató sin contar con un consentimiento válido ni con otra base legal legitimadora para el tratamiento de los datos personales. Además, existía una exposición del número de teléfono con el resto de los compañeros/as mezclando asuntos laborales con mensajes personales con lo que se vulneró el principio de licitud.

El centro especial de empleo, en su escrito de alegaciones, no acreditó el ofrecimiento de canales alternativos como medio de comunicación.

La AEPD calificó la conducta como infracción muy grave del artículo 6.1.(RGPD), imponiendo una sanción de 2.000 euros.

El consentimiento del interesado es la aceptación libre, específica, informada e inequívoca para permitir el tratamiento de datos personales.



IMPORTANTE

El tratamiento de datos personales de empleados/as requiere una base jurídica clara, proporcionalidad estricta y respeto pleno al derecho de desconexión.

LA AEPD ACLARA

Políticas de privacidad bajo el RGPD: el reto de informar de forma clara y comprensible (I)

En el apartado de [Publicaciones y resoluciones/Guías de la AEPD](#) encontramos el informe sobre Políticas de Privacidad en Internet. La AEPD analiza en esta guía las políticas de privacidad y formularios de recogida de datos personales de diversas entidades pertenecientes a los sectores: hoteles, transporte, comercio electrónico y seguros.

El objetivo de la guía es realizar un estudio del cumplimiento del deber de informar al interesado cuando se obtienen sus datos personales, haciendo especial referencia al tratamiento de los datos personales basado en el consentimiento, así como el modo de obtener el consentimiento.

Con carácter general, se detectan que los textos son demasiados extensos y no facilitan que el usuario pueda finalizar la lectura y la comprenda. Las bases legítimas del tratamiento no se explican correctamente, puesto que a veces, se incluye, por ejemplo, como interés legítimo lo que en realidad se trata de una ejecución de un contrato. En cuanto al lenguaje utilizado se han encontrado expresiones demasiado genéricas que no aportan información al interesado, siendo utilizadas para dar una apariencia de cumplimiento de normativa aplicable.

En la guía se dan recomendaciones respecto al deber de informar que recogeremos en sucesivos boletines.

Política de Privacidad

[Nombre de la empresa] ("Empresa", "nosotros", "nos") está comprometida con la protección de la privacidad de sus datos personales. Esta Política de Privacidad ("Política") describe cómo recopilamos, utilizamos y divulgamos sus datos personales cuando utiliza nuestro sitio web, aplicaciones móviles u otros servicios (en conjunto, los "Servicios").

1. Información que recopilamos

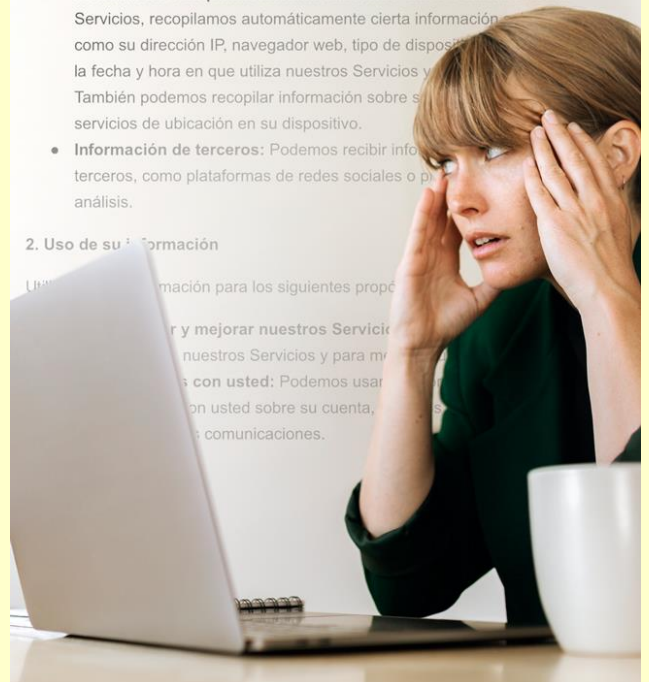
Recopilamos los siguientes tipos de información sobre usted:

- **Información que nos proporciona:** Esto incluye su nombre, dirección de correo electrónico, número de teléfono, dirección postal, información de pago y otra información que nos proporciona cuando se registra para una cuenta, utiliza nuestros Servicios o se comunica con nosotros.
- **Información recopilada automáticamente:** Cuando utiliza nuestros Servicios, recopilamos automáticamente cierta información como su dirección IP, navegador web, tipo de dispositivo, la fecha y hora en que utiliza nuestros Servicios y su ubicación. También podemos recopilar información sobre su uso de nuestros servicios de ubicación en su dispositivo.
- **Información de terceros:** Podemos recibir información de terceros, como plataformas de redes sociales o proveedores de análisis.

2. Uso de su información

Utilizamos su información para los siguientes propósitos:

- Para proporcionar y mejorar nuestros Servicios.
- Para personalizar nuestros Servicios y para mejorarlos.
- Para comunicarnos con usted: Podemos usar su información para comunicarnos con usted sobre su cuenta, nuestros Servicios y nuestras comunicaciones.



IMPORTANTE

Quando los datos se recogen directamente, debe informarse al interesado en ese momento; si se obtienen indirectamente, la información debe facilitarse en un mes o en la primera comunicación.

ACTUALIDAD CIBERSEGURIDAD Y PRIVACIDAD

El Centro Criptológico Nacional resuelve las dudas más frecuentes sobre su Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC)

Fuente: [CCN-CERT](#)

Publicado el 04/08/2025

Con el objetivo de resolver todas las dudas sobre el **Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC)**, el **Centro Criptológico Nacional** del **Centro Nacional de Inteligencia** ha habilitado en [la página web del CPSTIC](#) dos nuevas secciones de Preguntas Frecuentes (también conocidas por sus siglas en inglés FAQ, Frequently Asked Questions).

La sección [FAQ CPSTIC](#) ofrece respuestas claras y actualizadas a las consultas más habituales sobre el Catálogo, su objetivo, los productos y servicios que recoge, y también sobre el procedimiento de inclusión de productos o servicios o sobre los beneficios asociados.

La sección [FAQ FABRICANTES](#) está dirigida a todas las organizaciones inmersas en el proceso de inclusión de un producto o servicio en el Catálogo. En ella se abordan temáticas como las certificaciones válidas, el Informe de Análisis Diferencial (IAD), el periodo de validez de la cualificación o las acciones a llevar a cabo en el caso de tener nuevas versiones de productos disponibles.

Estas nuevas secciones de consulta facilitan la comprensión del catálogo y sus procesos, y fomentan una colaboración más eficiente entre todos los actores implicados en este Catálogo, que ofrece un conjunto de productos y servicios de seguridad de las tecnologías de la información y la comunicación de referencia, cuyas funcionalidades de seguridad han sido certificadas. Es, por tanto, una herramienta clave para las entidades públicas y para las empresas privadas que prestan servicios a la Administración.

Puede ver información relacionada en el siguiente enlace:

[FAQ CPSTIC: Catálogo de Productos y Servicios de Seguridad TIC\)](#)

[FAQ CPSTIC-FABRICANTES: Catálogo de Productos y Servicios de Seguridad TIC\)](#)

EL PROFESIONAL RESPONDE

Alta dirección bajo NIS2: responsabilidad y oportunidad

La NIS2 es la directiva europea que refuerza la ciberseguridad, dirigida a operadores esenciales y proveedores clave, entre otros, tales como energía, transporte, salud, agua, infraestructuras digitales; servicios financieros y fabricación de productos claves.

En el artículo 20 “Gobernanza” de la NIS2, se recoge uno de los aspectos fundamentales de la directiva europea, y es el papel protagonista que se otorga al órgano de dirección de las entidades, puesto que establece obligaciones explícitas para ellos.

La norma recoge entre otras obligaciones, la exigencia a los administradores de la aprobación de políticas de gestión del riesgo de seguridad cibernética y su supervisión. Es decir, tienen que velar porque la implementación de esas políticas de gestión del riesgo sea efectiva.

Otro aspecto relevante, es que los miembros de gestión de las entidades esenciales e importantes han de formarse obligatoriamente de manera periódica en ciberseguridad, con el fin de que adquieran los conocimientos y aptitudes suficientes para permitirles identificar los riesgos y evaluar las prácticas de gestión de riesgos de ciberseguridad y su impacto en los servicios prestados por la entidad.



IMPORTANTE

La NIS2 refuerza la gobernanza exigiendo a la alta dirección supervisar riesgos, garantizar la formación y asumir responsabilidad directa en ciberseguridad.