Plan de respuesta a incidentes

DocClar · Versión 1.1 · 11 de octubre de 2026
Responsable: Dmytro Shelest · seguridad@docclar.com

Qué hacemos ante una violación de la seguridad de los datos personales que tratamos por cuenta de un cliente, o ante la sospecha de una. Desarrolla la cláusula 12 del contrato de encargo del tratamiento.

1. Cómo nos enteramos

- El autocontrol diario de seguridad avisa a quien dirige el servicio en cuanto uno de sus controles falla.
- Cualquier persona del equipo que vea algo extraño lo comunica de inmediato a quien dirige el servicio.
- Cualquiera puede escribir a seguridad@docclar.com, también quien investiga vulnerabilidades (página «Divulgación responsable» de nuestra web).

2. Registrar

Anotamos la fecha y la hora en que tenemos conocimiento del incidente: desde ese momento corre el plazo de 48 horas para avisar al cliente. Anotamos también qué se ha observado y quién lo ha visto.

3. Contener

Usamos las medidas que hagan falta de las que tenemos preparadas:

- retirar el acceso de una persona: todas sus sesiones dejan de valer a la vez;
- pausar la cola de trabajo, para que no se procese ni se entregue nada mientras se investiga;
- renovar el secreto de sesión de la aplicación de revisión, para que todo el equipo tenga que volver a entrar;
- cambiar las claves y credenciales afectadas, que están en el llavero del sistema operativo;
- restaurar una copia de seguridad cifrada (antes se guarda una copia del estado actual).

4. Evaluar

Determinamos qué ha pasado, qué encargos y qué clientes están afectados, qué categorías de datos y cuántos interesados y registros, aproximadamente, y qué consecuencias puede tener.

5. Avisar al cliente en un máximo de 48 horas

Avisamos a cada cliente afectado sin dilación indebida y en todo caso en un máximo de 48 horas desde que tenemos conocimiento, con la información del artículo 33.3 del RGPD de que dispongamos: la naturaleza de la violación, las categorías y el número aproximado de interesados y de registros afectados, las posibles consecuencias, las medidas adoptadas o propuestas y un punto de contacto (seguridad@docclar.com). Si no tenemos toda la información a la vez, la damos por fases.

6. Colaborar

El cliente, como responsable del tratamiento, decide si notifica a la autoridad de control (el artículo 33 del RGPD le da 72 horas desde que tiene conocimiento) y a los interesados (artículo 34). Le ayudamos con

la información y con las evaluaciones de impacto y consultas previas que necesite (artículos 35 y 36).

7. Corregir y documentar

Corregimos la causa, comprobamos con el autocontrol que las medidas vuelven a funcionar y documentamos el incidente: los hechos, sus efectos y las medidas tomadas. Si cambia alguna medida, actualizamos el documento «Medidas de seguridad» y nuestra web.

Contacto

Seguridad: seguridad@docclar.com. Responsable: Dmytro Shelest.