

Procedimiento específico para notificar brechas de seguridad de datos personales

10/03/2026

Este **procedimiento** tiene por objeto incrementar la agilidad y eficacia en la respuesta ante posibles incidentes de **seguridad**, que puedan afectar a **datos personales**. De modo que sustituye a otros canales informales previos.



¿QUÉ ES UNA BRECHA DE SEGURIDAD?

Una brecha de seguridad es toda violación de la seguridad que ocasione o pueda ocasionar la destrucción, pérdida o alteración accidental o ilícita de datos personales; incluida la comunicación o acceso no autorizado a datos personales.

Las brechas de seguridad pueden ser, entre otras:

- **Brechas de confidencialidad:** personas no autorizadas acceden a la información, pudiendo verla, copiarla o modificarla.
- **Brechas de Integridad:** la información se modifica o altera de forma que puede perjudicar a las personas afectadas.
- **Brechas de disponibilidad:** la información desaparece o se pierde. Puede ser de forma temporal (si los datos pueden recuperarse) o permanente (si los datos no pueden recuperarse).

Su origen puede ser accidental, debido a fallos técnicos o errores humanos, intencional o debida a ciberataques.

Ejemplos comunes: envío de correos con datos sensibles a destinatarios erróneos; pérdida de portátiles u otros dispositivos electrónicos con información personal propia o de terceros; ser víctima de ataques externos a través de phishing, hackeo de cuentas de correo o bases de datos universitarias; transmisión indebida de documentos con información personal en soporte físico o de forma electrónica (por correo electrónico o redes sociales de mensajería).

¿CÓMO ACTUAR EN CASO DE DETECTAR UN POSIBLE INCIDENTE?

Toda persona miembro de la comunidad universitaria, o ajena a ella, que detecte una posible exposición accidental o ilícita de datos personales de los que sea responsable la Universidad, ya sea en soportes físicos o digitales, deberá comunicarlo a la Universidad de Granada a la mayor brevedad posible, para que se pueda proceder al análisis y valoración del incidente y, en su caso, adoptar las medidas necesarias de control y respuesta.

Los pasos para ello son los siguientes:

1º) Acceder a la **sede electrónica de la UGR**. Se puede acceder con:

- Con certificado digital
- Con usuario y clave web propios de UGR
- Con Cl@ve

2º) Comunicar el incidente a través del procedimiento: "**Notificación de brechas de seguridad**", ubicado dentro del catálogo de "Protección de datos personales y transparencia". Se podrán aportar documentos adjuntos, para acreditar y facilitar el análisis de lo alegado.

MÁS INFORMACIÓN:

- El **Protocolo** de notificación de brechas de seguridad de datos personales de la Universidad de Granada
- Información sobre **protección de datos**
- Contacto del responsable de seguridad de la información de la UGR: **@email**
- Contacto de la Delegada de Protección de Datos de la UGR: **@email**
- Contacto de la Oficina de Protección de Datos de la UGR: **@email**
- Contacto del Responsable del Tratamiento de la UGR: **@email**
- Contacto del Responsable de la Información de la UGR: **@email**