Procedimiento de notificación de brechas de seguridad

Todos los trabajadores que realizan un tratamiento de datos están obligados a adoptar medidas técnicas y organizativas que garanticen la protección de datos personales. El cumplimiento de las siguientes pautas respecto a la **notificación de violaciones o brechas de seguridad** en los datos personales está al alcance de todos y contribuye a reducir los riesgos inherentes de tales situaciones para los derechos y libertades de los interesados.

Cuando se sufre una brecha de seguridad se debe **recabar** una serie de **información** que será muy útil para decidir qué medidas tomar y qué acciones se emprenderán para cumplir los objetivos anteriores y para valorar la necesidad de notificar a la autoridad de control y afectados.

- Medio por el que se ha materializado la brecha, es decir, **qué ha ocurrido**; se ha perdido un dispositivo con datos personales, se ha producido un robo, se han publicado datos personales por error o se ha enviado a un destinatario equivocado, un ransomware ha cifrado un dispositivo, se ha producido una intrusión no autorizada en un sistema de información con datos personales, un empleado ha sido víctima de phishing, etc.
- **Origen de la brecha**, si ha sido interna o externa y su intencionalidad.
- **Categorías de datos**, si son datos básicos como credenciales o datos de contacto o si bien son categorías especiales como puedan ser datos de salud.
- **Volumen** de datos afectados, tanto en número de registros afectados como en número de personas afectadas.
- Categorías de **afectados**; clientes, empleados, estudiantes, abonados, pacientes, etc. Es importante identificar si se trata de colectivos vulnerables.
- Información temporal de la brecha; **cuándo se inició, cuándo se ha detectado y cuándo se resolvió o resolverá** la brecha de seguridad.

Ante el suceso de una brecha de seguridad, el personal habrá **de comunicarlo a la**

mayor brevedad al Delegado de Protección de Datos de la entidad, informando de la situación de la forma más completa posible, indicando los hechos que derivan en la brecha de seguridad y completando la información conforme con lo expuesto anteriormente.

Para ello, se cuenta con un **modelo de registro de incidencias** que estará a disposición de los empleados para su cumplimentación en caso de darse una brecha de seguridad.

Ante cualquier duda, contacte con el Responsable informatica@huesca.es o el Delegado de Protección de Datos Personales dpdhuesca@unive.es