Protección de datos.
Universidad de Sevilla

# Procedimiento de Notificación, Gestión y Respuesta de Violación de Seguridad en el Tratamiento de Datos Personales.

## I.- Introducción.

**Concepto de Violación de Seguridad en el Tratamiento de Datos Personales**:

Cualquier suceso que ocasione destrucción, pérdida, alteración, comunicación o acceso no autorizado a datos de carácter personal, ya sea de forma accidental o intencionada.

Este procedimiento forma parte de las medidas organizativas y técnicas de seguridad para los tratamientos de datos personales que se realicen en la Universidad de Sevilla, PARA LA SALVAGUARDA DE LOS DERECHOS Y LIBERTADES DE LOS INTERESADOS.

**Normativa:**

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD);

Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad.

Art. 4.12 RGPD. ***Violación de la seguridad de los datos personales: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos;***

Responsabilidad proactiva: notificación de las violaciones de seguridad que pueden suponer un riesgo para los derechos y libertades de las personas físicas, a la Autoridad de Control.

**¿Qué posibles incidencias podemos tener que den lugar a una violación de seguridad en el tratamiento de datos personales?:**

1) Acceso ilegítimo a los datos. Confidencialidad:

   Cualquier actuación que tenga como consecuencia un **acceso ilegítimo** a los datos personales.

   Modificación de los permisos de acceso o accesos no autorizados a la información de datos personales

   Accesos físico no autorizados a las áreas donde se ubiquen los sistemas y soportes informáticos o documentación (Centros de Procesos de Datos, oficinas, consultas médicas, salas de diagnóstico, etc.).
   Conocimiento por terceros del identificador de usuario y contraseña etc.

2) Modificación no autorizada de los datos. Integridad.

**Alteración** de los datos personales y el tratamiento con datos alterados/inexactos puede suponer un daño para los afectados.

3) Eliminación de los datos. Disponibilidad.

Se han **destruido, perdido o cifrado** datos personales, de forma que no pueden ser tratados.
Pérdida de información personal (documentación o dispositivos informáticos).

**Objetivos del Procedimiento**:

Se trata de una medida organizativa relacionada con el cumplimiento del RGPD y la LOPDyGDD, que consiste en establecer un procedimiento para la gestión de violaciones de seguridad en el tratamiento de datos personales, para la protección de los derechos y libertades de los afectados.

En el propio RGPD, se establecen los pasos a seguir, para realizar una adecuada gestión en estos casos. (Art. 33 y 34).

## II.-Procedimiento de Notificación, Gestión y Respuesta de Violación de Seguridad en el Tratamiento de Datos Personales.

Todo el procedimiento de notificación de violaciones de seguridad en el tratamiento de datos personales, se desarrollará con la ayuda y asistencia de la Oficina de Protección de datos ( dpd@us.es)

1) Identificación de una posible violación de seguridad en el tratamiento de datos personales. Esta identificación la puede realizar el Responsable Delegado, Responsable Tecnológico, Interesado, Autoridad de Control, Personal de la US (PAS o PDI) o cualquier persona o usuario afectado.
2) La persona que haya identificado la posible violación de seguridad, lo pondrá en conocimiento del Responsable Delegado (RD) y/o Responsable Tecnológico (RT) del Tratamiento de Datos, a la mayor brevedad.
3) El Responsable delegado o Responsable tecnológico reciben la notificación de la posible violación de seguridad en el tratamiento de datos personales (por un usuario, interesado, encargado..) En el caso de los encargados de tratamiento, en los anexos en donde se establecen las cláusulas que van a regir el tratamiento que van a realizar por cuenta de la US, es imprescindible introducir una cláusula que regule este tema, e indicar un plazo para que el encargado del tratamiento notifique al Responsable la posible violación de seguridad.

4) El Responsable comprueba que realmente se trata de una violación de seguridad de datos personales.

5) Si la comprobación resulta positiva entonces, el Responsable debe, a la mayor brevedad, notificar la violación a la Delegada de Protección de Datos, (dpd@us.es) utilizando para ello el formulario establecido al efecto:

   https://osi.us.es/sites/osi/files/doc/pd/procedimientos/impresodocumetarbrechaseguridad.docx

   En este formulario se recoge toda la información preceptiva requerida por la normativa que posteriormente se ha de comunicar a la Autoridad de Control competente (Consejo de Trasparencia y Protección de Datos de Andalucía).
   Es preciso señalar, que la violación de seguridad se debe notificar a la Autoridad de Control competente sin dilación indebida (a más tardar 72 horas desde tener constancia de ella) y además si la violación de seguridad entraña un alto riesgo para los derechos y libertados de los interesados, se le comunicará también a los mismos.

6) La violación de seguridad en el tratamiento de datos personales será valorada y analizada por la Oficina de Protección de datos junto con los responsables de seguridad de la información de la US.

7) La Oficina de Protección de Datos ( DPD) procederá, en su caso, a la comunicación de la violación de seguridad a la autoridad de control competente.

8) Comunicación a los interesados afectados. Cuando la violación de seguridad entrañe un alto riesgo para los derechos y libertados de los interesados, se comunicará también a los mismos.

   Con el fin de valorar la necesidad o no de comunicar la violación a los interesados, y tener más indicadores para la toma de la decisión adecuada, la Agencia de Protección de datos ha elaborado dos herramientas, denominadas Comunica Brecha RGPD y Asesora Brecha RGPD, con el objeto de ayudar a la decisión sobre la realización las notificaciones a la autoridad de control por un lado y de la comunicación a los afectados por otro. Estas herramientas han sido integradas en la página web del Consejo de Transparencia y Protección de Datos de Andalucía.
   Esta valoración se realizará con la asistencia de la Oficina de Protección de Datos de la US.

   8.1) Qué comunicar a los interesados:

   a) Naturaleza de la violación de la seguridad de datos personales. (categoría de datos afectados, tipo de incidencia…)

b) Nombre y los datos de contacto del delegado de protección de datos y/o de otro punto de contacto en el que pueda obtenerse más información;
c) Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales;
d) Descripción de las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

8.2) Cómo comunicarlo

La comunicación a los interesados será expresada en un lenguaje claro y sencillo, conteniendo. La notificación se realizará, a ser posible, de una sola vez, pero, si esto no fuera viable, se podrá hacer de manera gradual, siempre indicando la referencia de la primera notificación, con el fin de hacer un seguimiento de la misma.

En el caso de que tras el análisis de la brecha, fuera necesaria la comunicación al afectado, ésta se deberá realizar de forma directa al afectado, ya sea por teléfono, correo electrónico, SMS, a través de correo postal, o a través de cualquier otro medio dirigido al afectado que se considere adecuado.

Para la comunicación se podrá utilizar el formulario que se recoge en el siguiente enlace:

https://osi.us.es/sites/osi/files/doc/pd/procedimientos/formulario_comunicacion_afectadosdef.docx

8.3) Cuando NO comunicar a los afectados:

Supuestos en los que no es necesario la comunicación a los interesados:

a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;

b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;

c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

9) Cierre y registro de la brecha de Seguridad.-

El responsable o corresponsable del tratamiento, con el apoyo y asesoramiento de la Oficina de Protección de datos, realizará un informe final en el que se detalle la

trazabilidad del suceso, vicisitudes, análisis valorativo y particularmente el impacto final, que sirva para extraer conclusiones que ayuden en el futuro. Si la brecha ha tenido su origen en un encargado de tratamiento, éste deberá proporcionar toda la información para el informe.

Toda la documentación que derive de la gestión de la violación de seguridad se deberá incluir en la correspondiente petición de la **aplicación lopdyens**, con el fin de no perder la trazabilidad de lo ocurrido y de las medidas adoptadas.

Enlace a lopdyens:

https://lopdyens.us.es/login?back_url=https%3A%2F%2Flopdyens.us.es%2F