PROTOCOLO PARA LAS VIOLACIONES DE LA SEGURIDAD

Una violación de seguridad es cualquier incidencia 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.

Notificar la violación a la AC

Plazo para la notificación

- Sin dilación indebida.
- Máximo de 72 horas desde que se haya tenido constancia.
- Pasadas las 72 horas, se deberá acompañar de una justificación motivada.

Obligación de notificar la violación

Es obligatorio para cualquier RT, siempre que la violación de seguridad pueda producir daños o perjuicios a INTERESADOS o terceros en el transcurso del tratamiento de datos, tales como:

- Pérdida de control sobre los datos personales.
- Restricción de los derechos.
- Discriminación.
- Usurpación de identidad.
- Pérdidas financieras.
- Reversión no autorizada de la seudonimización.
- Daño para la reputación.
- Pérdida de la confidencialidad de los datos sujetos al secreto profesional.
- Cualquier otro perjuicio económico o social significativo para la persona física.

Razones para no notificar la violación

- Cuando sea improbable que la vulneración de los datos personales constituya un riesgo para los derechos y las libertades de los INTERESADOS.
- Esta improbabilidad debe basarse atendiendo al principio de responsabilidad proactiva: ser capaz de demostrar el cumplimiento de todos los principios del tratamiento: Licitud, Limitación de los fines, Minimización de los datos, Exactitud, Limitación del plazo de conservación, Integridad y Confidencialidad.

Contenido de la notificación

- La naturaleza y contexto de la violación.
- Los posibles efectos y consecuencias de la violación.
- Las medidas correctivas adoptadas o propuestas por el RT para remediar y mitigar los efectos ocasionados.
- Cuando sea posible:

- Las categorías y número de INTERESADOS afectados.
- Las categorías y número de registros afectados.
- Si es el caso, la identidad y los datos de contacto del DPO u otros contactos para obtener más información.
- Si no es posible facilitar toda la información en una comunicación, se notificará por etapas sin dilación indebida.

Comunicar la violación al INTERESADO

Plazo para la notificación

- Sin dilación indebida.

Obligación de notificar la violación

- Es obligatorio para cualquier RT, cuando sea probable que presente un ALTO RIESGO para los derechos y libertades del INTERESADO.
- Cuando al RT le sea exigido por la AC.

Razones para no notificar la violación

- Cuando se han adoptado medidas técnicas y organizativas de protección apropiadas para hacer ininteligibles los datos a personas no autorizadas y que estas se han aplicado a los datos afectados.
- Cuando se han tomado medidas posteriores que garantizan que ya no sea probable un ALTO RIESGO para los derechos y libertades del INTERESADO.
- Cuando supusiera un esfuerzo desproporcionado. En este caso, se podrá optar por una comunicación pública que sea igualmente efectiva para informar al INTERESADO.

Contenido de la notificación

- Una descripción de la naturaleza de la violación.
- Las posibles consecuencias de la violación.
- Las medidas correctivas adoptadas o propuestas por el RT para remediar y mitigar los efectos ocasionados.
- Si es el caso, la identidad y los datos de contacto del DPO u otros contactos para obtener más información.

Casuística de violaciones de seguridad

Se puede producir una violación de la seguridad cuando, por cualquier motivo, sea intencionado o no, se vulnere la seguridad de los datos o se prevea que pueda entrañar un ALTO RIESGO para los derechos y libertades de las personas físicas.

Acceso a datos no autorizado

- Encargo del tratamiento sin el contrato correspondiente.
- Acceso indiscriminado a impresoras, fotocopiadoras, etc.
- Acceso no autorizado a información confidencial. Por ejemplo, a datos de nóminas, currículums, embargos, imágenes de videovigilancia, etc.
- Acceso no autorizado a los sistemas informáticos.

Comunicación de datos no autorizada

- Transmisión ilícita de datos a un DESTINATARIO.
- Vulneración del secreto profesional.
- Publicación de imágenes sin autorización del INTERESADO.
- Envío de correos electrónicos masivos sin ocultar los destinatarios (copia oculta).
- TRANSFERENCIA internacional de datos sin estar sujeta a una Decisión de suficiencia de la UE o garantías adecuadas de protección de datos.

Alteración de datos

- Modificación de datos malintencionada.
- Falsificación de datos.
- Recuperación ineficaz de copias de respaldo.

Pérdida de información

- Extravío u olvido de soportes.
- Robo o sustracción de información.
- Desinstalación de aplicaciones informáticas.
- Por causas del transporte.
- Reorganización de la empresa.
- Destrucción de datos
- No usar destructora de papel o de soportes digitales.
- Incendio, inundación u otras causas ajenas a la empresa.

Ausencia de medidas de seguridad

- Antivirus, *antispam*, *antimalware*, *antiransomware*, *fireware*, cifrado, seudonimización, etc.
- Identificación y autentificación para acceder a los sistemas informáticos.
- Mecanismos de seguridad para acceder al mobiliario o a departamentos con datos personales.
- Disposición de datos a la vista de personas no autorizadas (recepción, monitores, mesas, etc.).