PROCEDIMIENTO DE GESTIÓN Y NOTIFICACIÓN DE VIOLACIONES DE SEGURIDAD

1 ¿Cuál es el objeto de este documento?

Este documento describe el procedimiento que debe seguirse para identificar, detectar, gestionar y, en su caso, notificar las violaciones de seguridad que se produzcan en relación con datos personales.

2 ¿Qué es una violación de seguridad?

Todo quebrantamiento de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de cualquier otra forma, o la comunicación o acceso no autorizados a dichos datos.

3 ¿Cómo deben notificar los usuarios las violaciones de seguridad que detecten?

Cualquier usuario que detecte una violación de la seguridad de los datos personales (**potencial o consumada**), deberá comunicarla a través del sistema de tickets existente. Dicha comunicación deberá recoger la información indicada en la ADDENDA I.

4 ¿Cómo deben actua cuando se comunica una violación de seguridad?

Departamento de Sistemas, el Responsable de Seguridad Físico y el DPD

Cuando el Departamento de Sistemas o el Responsable de Seguridad Físico, conforme a lo indicado en el punto anterior, tengan conocimiento de una posible violación de seguridad, deberán analizar la información aportada sobre la violación de seguridad, con el fin de verificar si la misma afecta a datos de carácter personal de personas físicas y las posibles consecuencias derivadas de ello. A tal fin, obtendrá toda la información que sea posible sobre los siguientes aspectos:

I. Naturaleza y descripción de la violación de la seguridad.

II. Las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

III. Posibles consecuencias de la violación de la seguridad de los datos personales.

En caso de que el Departamento de Sistemas o el Responsable de Seguridad Físico, según le corresponda a cada uno por el tipo de incidencia producida, comprueben que la violación de seguridad **NO** ha afectado ni puede afectar a datos personales, cumplimentará el documento que se incluye en la ADDENDA II, remitirá copia del mismo al Delegado de Protección de Datos (DPD) y conservará el original, debidamente archivado, dando por cerrado el incidente a efectos de protección de datos.

En caso de que se compruebe que la violación de seguridad **SÍ** ha afectado o puede afectar a datos personales, remitirá un correo electrónico al DPD informando del hecho, con toda la información de que disponga.

En este último caso, el Departamento de Sistemas o el Responsable de Seguridad Físico, dependiendo del tipo de violación de Seguridad, y el DPD valorarán conjuntamente si, en efecto, se ha producido una violación de la seguridad de los datos personales. Esta valoración también se efectuará con la participación del Departamento de Asesoría Jurídica:

a) Si concluyesen que no se ha producido una violación de la seguridad de los datos personales, cumplimentarán y firmarán el documento que se incluye en la ADDENDA II, debiendo archivarlo debidamente.

DEPARTAMENTO DE ASESORÍA JURÍDICA
lopd@nebrija.es
www.nebrija.com

b) Si concluyesen que sí se ha producido una violación de la seguridad de los datos personales:

a. Decidirán si, a su juicio, se debe informar del hecho a la autoridad de control o, en su caso, al interesado.

b. Decidirán qué medidas han de adoptarse o proponerse 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.

En caso de que se concluya que, efectivamente, se ha producido una violación de la seguridad de los datos personales, cumplimentarán el modelo previsto en la ADENDA III y lo elevarán a la dirección de la entidad, para que adopte una decisión sobre la notificación del hecho.

5 ¿Cómo debe actuar la entidad una vez disponga de toda la información?

En caso de que se confirme que la violación de seguridad ha afectado a datos personales, la entidad, a través del DPD, lo comunicará a la Agencia Española de Protección de Datos, cumplimentando la ADDENDA IV de este procedimiento y remitiéndola a través de la sede electrónica de la AEPD:

https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/canalesAcceso.jsf;jsessionid=6B11401115464D9E5E88F54187ACD4E2

Esta comunicación debe hacerse sin dilación indebida o, a más tardar y, de ser posible, antes de 72 horas después de que haya tenido constancia de la violación de la seguridad. Se exceptúa del deber de cumplir este plazo el caso de que sea improbable que la violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. No obstante, si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

A la hora de practicar la notificación sin dilación indebida, deberán tenerse en cuenta, en particular, los siguientes factores

a) La naturaleza y gravedad de la violación de la seguridad de los datos personales.

b) Sus consecuencias y efectos adversos para el interesado.

c) Las restantes circunstancias de la violación, inclusive si los datos personales se hallaban protegidos mediante las medidas técnicas adecuadas, limitando eficazmente la probabilidad de usurpación de identidad u otras formas de uso indebido

Si, por cualquier motivo justificado, no fuera posible facilitar toda la información simultáneamente, se facilitará de manera gradual sin dilación indebida.

6 ¿Cómo deben documentarse de modo interno las violaciones de seguridad?

El Departamento de Sistemas o los Responsables de Seguridad Físicos, dependiendo del tipo de incidencia, documentarán cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas.

Esto se hará de conformidad con lo establecido en el apartado 9.2 del Documento denominado “DOCUMENTO DE SEGURIDAD DE LOS FICHEROS CON DATOS DE CARÁCTER PERSONAL (INTRODUCCIÓN GENERAL)”. En concreto, una vez generado el “tickect” por el usuario que ha detectado la violación de seguridad, este le llegará al Departamento de Sistemas, que procederá a resolver la misma si esta afecta al tratamiento automatizado de datos personales. Por el contrario, si la violación de seguridad afecta al tratamiento de datos en soporte papel, se dará traslado de la misma al Responsable de Seguridad Físico de la entidad Nebrija que corresponda para que proceda a su resolución, en caso de que sea posible.

El sistema de tickets deberá recoger toda la información indicada en la ADDENDA III cuando la violación de seguridad afecte a datos de carácter personal. En el supuesto de que no registre toda la información necesaria, el Departamento de Sistemas deberá registrar la misma, utilizando para ello el modelo que se adjunta en la ADDENDA III de este documento.

Los documentos en que se hayan registrado las violaciones de seguridad de datos personales serán debidamente custodiados por el Responsable de Seguridad Informático.

7 La notificación de violaciones de seguridad

¿La notificación de violaciones de seguridad a la AEPD puede tener consecuencias para la entidad?

Efectivamente, la notificación puede dar lugar a una intervención de la AEPD, de conformidad con las funciones y poderes que le reconoce la ley.

8 ¿Deben notificarse las violaciones de seguridad a los afectados?

Como regla general, no deben comunicarse a las personas afectadas.

No obstante, como excepción, la violación de seguridad se debe comunicar a los interesados, sin dilación indebida, cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para sus derechos y libertades. Dicha decisión será adoptada, en su caso, por la Dirección de la entidad, tras haber escuchado el parecer del DPD.

Asimismo, la AEPD, una vez considerada la probabilidad de que la violación entrañe un alto riesgo, podrá exigir a la entidad que comunique al interesado la violación de la seguridad de los datos personales, aunque se hubiese decidido lo contrario.

9 ¿Cómo deben notificarse las violaciones de seguridad a los afectados, en su caso?

La comunicación al interesado, en su caso se podrá efectuar a través de cualquier medio que permita acreditarla y contendrá en un lenguaje claro y sencillo la siguiente información:

a) La descripción de la naturaleza de la violación de la seguridad de los datos personales.

b) El nombre y los datos de contacto del DPD o de otro punto de contacto en el que pueda obtenerse más información.

c) Describir las posibles consecuencias de la violación de la seguridad de los datos personales.

d) Describir las medidas adoptadas o propuestas 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. Se deben incluir aquí las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación.

La comunicación a los interesados, en su caso, debe realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la AEPD, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continuas o similares.

10 ¿Existen excepciones al deber de notificar las violaciones de seguridad a los afectados?

La comunicación al interesado no será necesaria si se cumple alguna de las condiciones siguientes:

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

b) La entidad ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se materialice el alto riesgo para los derechos y libertades del interesado.

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.

11 ¿Los encargados del tratamiento deben notificar también las violaciones de seguridad?

En caso de que quien detecte una violación de la seguridad de los datos personales actúe en calidad de encargado del tratamiento, lo notificará sin dilación indebida al responsable del tratamiento.

A tal fin, el encargado del tratamiento deberá cumplimentar el formato previsto en la ADDENDA IV y remitirla al responsable del tratamiento por e-mail sin dilación indebida.

El presente procedimiento debe ser dado a conocer, mediante su envío por e-mail, a todos los usuarios y encargados del tratamiento de la entidad, dejando constancia documental, mediante un acuse de recibo, de que dicha comunicación se ha producido.

Fecha de solicitud / / **Hora:**

ADDENDA I. COMUNICACIÓN DE POSIBLE VIOLACIÓN DE LA SEGURIDAD DE LOS DATOS PERSONALES

PERSONA QUE NOTIFICA LA POSIBLE VIOLACIÓN DE LA SEGURIDAD:

Nombre y apellidos:

DNI o documento equivalente:

Puesto / Departamento:

PERSONA A QUIEN SE NOTIFICA:

Nombre y apellidos:

DESCRIPCIÓN Y EFECTOS DE LA POSIBLE VIOLACIÓN DE LA SEGURIDAD:

COMENTARIOS / OBSERVACIONES:

En a de de

Firma del solicitante

DEPARTAMENTO DE ASESORÍA JURÍDICA
lopd@nebrija.es
www.nebrija.com

Fecha de solicitud / / **Hora:**

ADDENDA II. CIERRE DE INCIDENTE DE SEGURIDAD POR NO HABER AFECTADO A DATOS PERSONALES

PERSONA QUE NOTIFICÓ EL INCIDENTE:

Nombre y apellidos:

Fecha y hora en que se notificó el incidente:

DESCRIPCIÓN DE LAS CAUSAS DE CIERRE DEL INCIDENTE:

Comprobaciones realizadas que han llevado a decidir el cierre del incidente:

Firma del Responsable de Seguridad Informático/ Responsable de Seguridad Físico

Firma del DPD (en caso de haber intervenido):

En a de de

Firma del solicitante

DEPARTAMENTO DE ASESORÍA JURÍDICA
lopd@nebrija.es
www.nebrija.com

Fecha de solicitud / / **Hora:**

ADDENDA III. REGISTRO DE VIOLACIÓN DE LA SEGURIDAD DE LOS DATOS PERSONALES

DATOS

Descripción de la violación de seguridad:

Categorías de datos personales afectados (si es posible precisarlo):

Categorías y número aproximado de interesados afectados (si es posible precisarlo):

Categorías y número aproximado de registros afectados (si es posible precisarlo):

Posibles consecuencias derivadas de la violación de la seguridad:

Medidas ya adoptadas para poner remedio a la violación de seguridad y mitigar sus efectos:

Medidas propuestas para poner remedio a la violación de seguridad y mitigar sus efectos:

¿Procede comunicar el hecho a la autoridad de control? ☐ **SI** ☐ **NO**

Indicar motivos:

¿Procede comunicar el hecho a los interesados? ☐ **SI** ☐ **NO**

Indicar motivos:

Firma del Responsable de Seguridad Informático/ Responsable de Seguridad Físico

Firma del DPD (en caso de haber intervenido):

En a de de

Firma del solicitante

DEPARTAMENTO DE ASESORÍA JURÍDICA
lopd@nebrija.es
www.nebrija.com

Fecha de solicitud / / **Hora:**

ADDENDA VI. NOTIFICACIÓN DE VIOLACIÓN DE LA SEGURIDAD DE LOS DATOS PERSONALES

DATOS

Nombre de la entidad: CIF:

Identificación del DPD: Datos de contacto del DPD:

Descripción de la violación de seguridad:

Categorías de datos personales afectados (si es posible precisarlo):

Categorías y número aproximado de interesados afectados (si es posible precisarlo):

Categorías y número aproximado de registros afectados (si es posible precisarlo):

Posibles consecuencias derivadas de la violación de la seguridad:

Medidas ya adoptadas para poner remedio a la violación de seguridad y mitigar sus efectos:

Medidas propuestas para poner remedio a la violación de seguridad y mitigar sus efectos:

¿Se estima que procede comunicar el hecho a los interesados? ☐ **SI** ☐ **NO**

Indicar motivos:

Nombre del representante legal de la entidad:

Cargo:

Firma del solicitante

En a de de

Firma del solicitante

DEPARTAMENTO DE ASESORÍA JURÍDICA
lopd@nebrija.es
www.nebrija.com