 PRINCIPE FELIPE <small>CENTRO DE INVESTIGACION</small>	PROTOCOLO NOTIFICACIÓN BRECHAS DE SEGURIDAD	Fecha:23/10/2019
		Versión: 1
		Página 1 de 11

Introducción

El Reglamento general de protección de datos (RGPD) introduce el requisito de que la violación de la seguridad de los datos personales (en adelante “brecha”) sea notificada a la autoridad nacional de supervisión competente y, en ciertos casos, también a las personas cuyos datos personales han sido afectados por la violación.

Para dar cumplimiento a dicho requisito, **Fundación de la Comunidad Valenciana Centro de Investigación Príncipe Felipe** (en adelante **CIPF**) ha elaborado un Protocolo interno de brechas de seguridad dirigido al personal con el fin de facilitar la gestión de las incidencias y brechas de seguridad y su notificación a la autoridad de control y a los interesados cuando sea necesario.

Aprobación del protocolo

El presente protocolo ha sido aprobado por la Dirección General del CIPF.

Modificación del protocolo

El presente protocolo puede ser modificado por la Dirección General del CIPF.

Objeto del protocolo

Constituye el objeto del presente documento establecer el protocolo destinado a garantizar el cumplimiento de lo establecido en el RGPD en relación con la notificación de brechas de seguridad a la Autoridad de Control y a los interesados.


Para ello se tendrá en cuenta lo siguiente:

A) ¿Qué es una violación de seguridad de los datos (quiebra de seguridad)?

El RGPD define las violaciones de seguridad de los datos, más comúnmente conocidas como "quiebras o brechas de seguridad", de una forma muy amplia, e incluye todo incidente 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.

Algunos ejemplos de sucesos que constituyen violaciones de seguridad son los siguientes:

- ✓ Pérdida o sustracción de un ordenador portátil
- ✓ Pérdida o sustracción de un terminal móvil
- ✓ El acceso no autorizado a las bases de datos de la organización (incluso por el propio personal cuando no cuente con autorización para ello)
- ✓ El borrado accidental de algunos registros

 PRINCIPE FELIPE CENTRO DE INVESTIGACION	PROTOCOLO NOTIFICACIÓN BRECHAS DE SEGURIDAD	Fecha:23/10/2019
		Versión: 1
		Página 2 de 11

A los efectos de este protocolo, debe quedar claro que la “violación” a la que se refiere el RGPD, solo se aplica en la medida en que afecte a datos de carácter personal, y en consecuencia dicho incidente pueda comprometer al Centro en el cumplimiento de los principios del RPGD.

Por tanto, se debe tener en cuenta que, aunque todas las brechas de datos personales son incidentes de seguridad, no todos los incidentes de seguridad son necesariamente brechas de datos personales.

B) Gestión de brechas de seguridad: detección e identificación y clasificación.


Para la gestión de las brechas de seguridad, se tendrán en cuenta los siguientes los pasos:

➤ Identificación del incidente:

Para poder valorar si un incidente constituye una brecha de seguridad es necesario en primer lugar identificar el incidente producido para poder determinar y valorar si afecta o no a datos de carácter personal.

La identificación de un incidente de seguridad puede producirse a través de varias formas:

- ✓ Cuando se detecte una quiebra de los controles, medidas y mecanismos de seguridad implantados en CIPF para proteger los datos personales, ya se trate de medidas físicas o lógicas, por ejemplo:
 - Incumplimiento o vulneración de las medidas y políticas adoptadas en la empresa como las políticas de mesas limpias (no dejar a la vista y alcance de personas no autorizadas información y datos), bloqueo de pantallas, accesos con usuario y contraseña, etc.
 - Vulneración de controles físicos como detección de intrusos, videovigilancia, control y registro de accesos a zonas determinadas, etc.
 - Archivos con caracteres inusuales, recepción de correos electrónicos con archivos adjuntos sospechosos, comportamiento extraño de dispositivos, imposibilidad de acceder a ciertos servicios, extravío/robo de dispositivos de almacenamiento o equipos con información.
 - Alertas generadas por software antivirus.
 - Consumos excesivos y repentinos de memoria o disco en servidores y equipos.
 - Anomalías de tráfico de red o picos de tráfico en horas inusuales.
 - Alertas de sistemas de detección/prevenición de intrusión (IDS/IPS).

 PRINCIPE FELIPE <small>CENTRO DE INVESTIGACION</small>	PROTOCOLO NOTIFICACIÓN BRECHAS DE SEGURIDAD	Fecha:23/10/2019
		Versión: 1
		Página 3 de 11

- ✓ Cuando se reciba una advertencia de fuentes externas, como, por ejemplo:
 - Advertencias procedentes de proveedores de servicios informáticos, proveedores de servicios de internet o fabricantes de soluciones de seguridad.
 - Advertencias procedentes de un cliente.
 - Comunicación o notificación que realicen a la empresa los distintos organismos públicos como el Instituto Nacional de Cyberseguridad (INCIBE), el Centro Criptológico Nacional (CCN), Fuerzas y Cuerpos de Seguridad del Estado.
 - Información publicada en medios de comunicación.

El análisis de las fuentes de información antes mencionadas permitirá determinar si se está ante un incidente de seguridad o no, así como su naturaleza, clase, tipo, si dicho incidente ha afectado a datos de carácter personal y por tanto constituye una “brecha de los datos de carácter personal” descrita en el RGPD, y el nivel de riesgo al que se enfrenta la organización.


➤ **Clasificación:**

Una vez identificada la incidencia y confirmado que constituye una brecha de datos de carácter personal, se deberá determinar si se trata de una brecha de confidencialidad, de integridad o de disponibilidad de los datos afectados. Concretamente:

- ✓ Si la brecha consiste en que personas no autorizadas o legitimadas acceden a la información y datos (**brecha de confidencialidad**). En este caso, la gravedad dependerá del alcance de la divulgación, es decir, el número potencial y el tipo de terceros que pueden haber accedido ilegalmente a la información.
- ✓ Si la brecha consiste en que se ha alterado información original y la sustitución de datos puede ser perjudicial para el individuo (**brecha de integridad**). La situación más grave ocurre cuando existen serias posibilidades de que los datos alterados se hayan utilizado de una manera que pueda dañar al individuo.
- ✓ Si la brecha consiste en que no se puede acceder a los datos originales cuando es necesario (**brecha de disponibilidad**). Puede ser temporal (los datos son recuperables pero tomará un periodo de tiempo y esto puede ser perjudicial para el individuo), o permanente (los datos no pueden recuperarse).

Una vez confirmado que el incidente constituye una brecha que afecta a datos personales se deberá informar de inmediato al Delegado de Protección de Datos del CIPF poniendo a su disposición la siguiente la siguiente información:

- ✓ Descripción de la naturaleza de la violación de la seguridad de los datos personales.

 PRINCIPE FELIPE CENTRO DE INVESTIGACION	PROTOCOLO NOTIFICACIÓN BRECHAS DE SEGURIDAD	Fecha: 23/10/2019
		Versión: 1
		Página 4 de 11

- ✓ Categorías y número aproximado de interesados afectados.
- ✓ Categorías y número aproximado de registros de datos personales afectados.
- ✓ Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.
- ✓ Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales y para mitigar los posibles efectos negativos.

El Delegado de Protección de Datos convocará, dentro del plazo máximo de 48 horas desde que tuvo lugar el incidente, al Comité de Protección de Datos, donde se valorará, sobre la base de la referida información, si la violación de seguridad constituye un riesgo para los derechos y las libertades de las personas físicas.

- **Valoración del riesgo para los afectados derivado de la brecha:**

Para la valoración del riesgo se tendrán en cuenta, entre otros, los siguientes factores:

- ✓ **La categoría o nivel de criticidad** respecto a la seguridad de los sistemas afectados. Siguiendo la clasificación genérica, se puede distinguir entre:
 - Crítico (afecta a datos valiosos, gran volumen y en poco tiempo)
 - Muy Alto (Cuando dispone de capacidad para afectar a información valiosa, en cantidad apreciable)
 - Alto (Cuando dispone de capacidad para afectar a información valiosa)
 - Medio (Cuando dispone de capacidad para afectar a un volumen apreciable de información)
 - Bajo (Escasa o nula capacidad para afectar a un volumen apreciable de información)
- ✓ **Naturaleza, sensibilidad y categorías de los datos personales afectados:**
 - Datos de escaso riesgo: datos de contacto, de educación, familiares, profesionales, biográficos
 - Datos de comportamiento: localización, tráfico, hábitos y preferencias
 - Datos financieros: transacciones, posiciones, ingresos, cuentas, facturas
 - Datos sensibles: de salud, biométricos, datos relativos a la vida sexual, etc.
- ✓ **Datos legibles/ilegibles:**
 - Datos protegidos mediante algún sistema de seudonimización (por ejemplo, cifrado o hash)

- ✓ **Volumen de datos personales, expresados en:**
 - cantidad (registros, ficheros, documentos) y/o
 - en periodos de tiempo (una semana, un año, etc.)

- ✓ **Facilidad de identificación de individuos:**
 - facilidad con la que se puede deducir la identidad de los individuos a partir de los datos involucrados en la brecha.


- ✓ **Severidad de las consecuencias para los individuos:**
 - Baja: Las personas no se verán afectadas o pueden encontrar algunos inconvenientes que superarán sin ningún problema (tiempo de reingreso de información, molestias, irritaciones, etc.).
 - Media: Las personas pueden encontrar inconvenientes importantes, que podrán superar a pesar de algunas dificultades (costos adicionales, denegación de acceso a servicios comerciales, miedo, falta de comprensión, estrés, dolencias físicas menores, etc.).
 - Alta: Las personas pueden enfrentar consecuencias importantes, que deberían poder superar aunque con serias dificultades (malversación de fondos, listas negras de los bancos, daños a la propiedad, pérdida de empleo, citación judicial, empeoramiento de la salud, etc.).
 - Muy alta: Las personas pueden enfrentar consecuencias significativas, o incluso irreversibles, que no pueden superar (exclusión o marginación social, dificultades financieras tales como deudas considerables o incapacidad para trabajar, dolencias psicológicas o físicas a largo plazo, muerte, etc.).

- ✓ **Características especiales de los individuos:**
 - Si afectan a individuos con características especiales o con necesidades especiales (menores, personas afectadas por alguna discapacidad).

- ✓ **Número de individuos afectados:**
 - Dentro de una escala determinada, por ejemplo, más de 100 individuos.

- ✓ **Características especiales del responsable del tratamiento (de la entidad en sí):**

En base a la actividad de la entidad.

 PRINCIPE FELIPE <small>CENTRO DE INVESTIGACION</small>	PROTOCOLO NOTIFICACIÓN BRECHAS DE SEGURIDAD	Fecha:23/10/2019
		Versión: 1
		Página 6 de 11

- ✓ **El perfil de los usuarios afectados**, su posición en la estructura organizativa de la entidad y, en su consecuencia, sus privilegios de acceso a información sensible o confidencial.
- ✓ **El número y tipología de los sistemas afectados.**
- ✓ **El impacto** que la brecha puede tener en la organización, desde los puntos de vista de la protección de la información, la prestación de los servicios, la conformidad legal y/o la imagen pública. Va a estar relacionado con la categoría o criticidad de los servicios afectados y personas afectadas. En este aspecto diferenciamos entre los siguientes impactos:
 - Bajo (perjuicio limitado)
 - Medio (perjuicio grave)
 - Alto (perjuicio muy grave)
- ✓ **Los requerimientos legales y regulatorios:** Notificación de la brecha a la autoridad de control y cualquier otra obligación de notificación, comunicación a Fuerzas y Cuerpos de Seguridad del Estado en caso de delito.

En general, el criterio de alto riesgo debe entenderse en el sentido de que sea probable que la violación de seguridad ocasione daños de entidad a los interesados. Por ejemplo, en casos en que se desvele información confidencial, como contraseñas o participación en determinadas actividades, se difundan de forma masiva datos sensibles o se puedan producir perjuicios económicos para los afectados.

C) Notificación a la Autoridad de Control:

Una vez realizada la valoración del riesgo, en caso de que se considere que **la brecha constituye un riesgo para los derechos y las libertades de las personas físicas**, el Delegado de Protección de Datos comunicará la violación de seguridad a la Autoridad de Protección de Datos (Agencia Española de Protección de Datos, AEPD) dentro del **plazo máximo de 72 horas** desde que tuvo lugar el incidente. Dicha comunicación se llevará a cabo mediante el trámite electrónico habilitado en la web de la sede de la AEPD.

<https://sedeagpd.gob.es/sede-electronica-web/vistas/formBrechaSeguridad/procedimientoBrechaSeguridad.jsf>

Si no fuera posible facilitar toda la información de manera simultánea, se aportará gradualmente sin dilación.

En caso de que la comunicación a la AEPD no tenga lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

En todo caso CIPF guardará copia de la notificación realizada a la AEPD y llevará a cabo cualquier acción que la AEPD solicite para la gestión de la brecha.

D) Notificación a los interesados:


Si de la valoración realizada por el Comité de Protección de Datos se concluye que **la violación de seguridad entraña alto riesgo para los derechos y libertades de las personas físicas**, se realizará la comunicación de la violación a los interesados a la mayor brevedad posible, acompañando la siguiente información en lenguaje claro y sencillo:

- Naturaleza de la violación de la seguridad de los datos personales.
- Nombre y datos de contacto del Delegado de Protección de Datos (o en otro caso, del responsable de seguridad, responsable de protección de datos o responsable del comité de protección de datos).
- Descripción de los posibles efectos o consecuencias de la violación de la seguridad.
- 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 y para mitigar los posibles efectos negativos.

La AEPD podrá exigir a CIPF que realice esta comunicación si todavía no se ha llevado a cabo cuando, a su criterio, exista un alto riesgo probable para los derechos y libertades de los interesados.

No será necesario realizar la comunicación a los interesados cuando el Comité de Protección de Datos (o en su caso la AEPD), verifique y constate que concurre alguna de las condiciones siguientes:

- ✓ Los datos ya se encontraban públicamente disponibles y su revelación no entraña ningún riesgo hacia el titular de los datos.
- ✓ Los datos personales afectados por la violación de la seguridad cuentan con medidas de protección técnicas y organizativas apropiadas, en particular si se han hecho ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado, minimización, disociación de datos, acceso a entornos de prueba sin datos reales, etc. Por ejemplo, es probable que no sea necesaria la notificación si se pierde un dispositivo móvil y los datos personales que contiene están cifrados. Sin embargo, sí que es posible que se requiera de notificación si esta fuera la única copia de los datos personales, o por ejemplo, la clave de cifrado en posesión del responsable estuviera comprometida.

 PRÍNCIPE FELIPE CENTRO DE INVESTIGACION	PROTOCOLO NOTIFICACIÓN BRECHAS DE SEGURIDAD	Fecha:23/10/2019
		Versión: 1
		Página 8 de 11

- ✓ Se han tomado medidas ulteriores que garanticen que ya no exista la probabilidad de alto riesgo para los derechos y libertades del interesado. Por ejemplo, mediante la identificación y puesta en marcha inmediatamente de las medidas contra la persona que ha accedido a los datos personales antes de que pudieran hacer algo con ellos.
- ✓ Cuando la comunicación suponga un esfuerzo desproporcionado a nivel técnico y organizativo. Por ejemplo, cuando los detalles de contacto se hayan perdido como resultado de la brecha, o aquellos casos en los que se tenga que desarrollar un nuevo sistema o proceso para realizar la notificación, o se requiera la dedicación excesiva de recursos internos para la identificación de los afectados. 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.

Para la notificación de la brecha de seguridad a los interesados CIPF utilizará el modelo que se adjunta como ANEXO I al presente protocolo.


E) Quiebras de gran impacto:

Con carácter general, la mera sospecha de que ha existido una quiebra o la constatación de que ha sucedido algún tipo de incidente sin que se conozcan mínimamente sus circunstancias no deberían dar lugar, todavía, a la notificación, dado que en esas condiciones no sería posible, en la mayoría de los casos, determinar hasta qué punto puede existir un riesgo para los derechos y libertades de los interesados.

No obstante, en casos de quiebras que por sus características pudieran tener gran impacto, sí podría ser recomendable contactar con la autoridad de supervisión tan pronto como existan evidencias de que se ha producido alguna situación irregular respecto a la seguridad de los datos, sin perjuicio de que esos primeros contactos puedan completarse con una notificación formal más completa dentro del plazo legalmente previsto.

F) Registro de la información:

Todos los hechos relacionados con la violación de seguridad quedarán registrados y deberán constar completamente documentados, incluidos los posibles efectos o consecuencias, las medidas correctivas adoptadas y las valoraciones realizadas por el Comité de Protección de Datos, especialmente en relación con la valoración del riesgo, la decisión de llevar a cabo o no las comunicaciones a la AEPD y a los interesados, la información aportada, el retraso en la realización de las comunicaciones en su caso y todas las circunstancias o condiciones que hayan servido de base a dichas valoraciones o que hayan incidido en el retraso o en la no realización de la comunicación. Esta documentación deberá conservarse a disposición de la Autoridad de Control para acreditar el cumplimiento por el Centro de todas las obligaciones señaladas.

 PRINCIPE FELIPE CENTRO DE INVESTIGACION	PROTOCOLO NOTIFICACIÓN BRECHAS DE SEGURIDAD	Fecha:23/10/2019
		Versión: 1
		Página 9 de 11

Obligaciones del personal

Todo el personal señalado en el apartado anterior tiene la obligación de conocer y cumplir la presente protocolo y normativas, medidas y procedimientos derivados de la misma.

El incumplimiento del presente protocolo o la normativa, medidas y procedimientos derivados de ésta podrá acarrear el inicio de medidas disciplinarias oportunas y, en su caso, las responsabilidades legales correspondientes.

Consultas

Cualquier consulta o sugerencia en relación con el presente protocolo, podrá ser consultada al Delegado de Protección de Datos.

Efectividad

Este documento forma parte de la normativa para cumplimiento del RGPD y entrará en vigor el día de su aprobación y quedará publicado para conocimiento y cumplimiento de todos los empleados en el sitio web del CIPF.

ANEXO I

MODELO NOTIFICACIÓN BRECHAS DE SEGURIDAD A LOS INTERESADOS¹

[INTERESADO DESTINATARIO]

[DIRECCIÓN]

[FECHA]

Asunto: Notificación de una violación de seguridad de datos personales

Estimado [INTERESADO]

Lamentamos informarle acerca de una violación de la seguridad de nuestros sistemas de información consistente en [INDICAR NATURALEZA DE LA VIOLACIÓN], la cual ha afectado a los datos personales que, sobre su persona, el Centro tiene almacenados y sometidos a tratamiento.

El incidente de seguridad ha causado los siguientes daños en relación con sus datos de carácter personal²:

- a. [INDICAR DAÑOS].

No obstante, le informamos de que hemos adoptado las siguientes medidas para poner remedio a la violación de seguridad y mitigar los posibles efectos negativos:


- b. [INDICAR MEDIDAS PARA PONER REMEDIO].
- c. [INDICAR MEDIDAS PARA MITIGAR LOS EFECTOS NEGATIVOS].

Asimismo, nos permitimos realizar le las siguientes recomendaciones que le rogamos encarecidamente lleve a cabo:

- a. [INDICAR MEDIDAS].

¹ Cuando la violación entrañe un alto riesgo para los derechos y libertades de las personas.

² Se advierte que, según la norma, la información que se contiene en este documento es la “mínima” a proporcionar al interesado, por lo que, se podrá valorar ofrecer una información mayor y más detallada. Además, se advierte que, según el RGPD, la información se describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d). Por lo que el responsable deberá tener en cuenta los términos utilizados en la comunicación.

 PRINCIPE FELIPE CENTRO DE INVESTIGACION	PROTOCOLO NOTIFICACIÓN BRECHAS DE SEGURIDAD	Fecha:23/10/2019
		Versión: 1
		Página 11 de 11

Puede obtener más información sobre la violación de seguridad y el daño producido en relación con sus datos de carácter personal, en cualquiera de los siguientes puntos de contacto:

- a. [INDICAR, POR EJ. UNA URL O UNA INTRANET].
- b. [DATOS DE CONTACTO DEL DELEGADO DE PROTECCIÓN DE DATOS O FIGURA RESPONSABLE DE SEGURIDAD, DE PROTECCIÓN DE DATOS O DEL COMITÉ DE PROTECCIÓN DE DATOS].

Le pedimos disculpas por cualquier inconveniente que esta violación de seguridad pueda causarle y nos ponemos a su disposición para apoyarle en todo lo que sea necesario.

Atentamente,

[NOMBRE]

Por y en nombre de [RESPONSABLE DEL TRATAMIENTO]³

³ Debería ser firmado por el Delegado de Protección de Datos o, en su caso, el responsable de seguridad de la organización o el responsable de protección de datos o del comité de protección de datos.