Autoridad Independiente de Responsabilidad Fiscal

PROTECCIÓN DE DATOS

PROCEDIMIENTO DE GESTIÓN Y NOTIFICACIÓN DE BRECHAS DE SEGURIDAD

CONTROL DE VERSIONES

Nº de versión	Fecha	Motivo
V1	09/04/2019	Documento inicial

APROBADO POR

Nombre y cargo	José Luis Escrivá Belmonte, Presidente de la AIReF, previa deliberación favorable del Comité Directivo
Fecha	09/04/2019

Índice

1. Objeto y alcance

1.1 Objeto

Este documento tiene por objeto establecer el procedimiento para el registro, gestión y notificación de las brechas de seguridad que afecten a: (i) los datos de carácter personal, tal y como se definen en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (en adelante, Reglamento General de Protección de Datos o RGPD) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPD), y (ii) la información recogida en los sistemas TIC de la AIReF.

1.2 Alcance

El presente procedimiento será de aplicación a todo el personal de la AIReF, a los alumnos en prácticas (becarios) y, en lo que proceda, a los colaboradores externos.

2. Definiciones

Datos personales: Toda información sobre una persona física identificada o identificable (interesado). Se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como, por ejemplo, un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Tratamiento: Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Autoridad de control: Autoridad pública independiente de cada Estado miembro encargada de supervisar la aplicación del Reglamento General de Protección de Datos con el fin de proteger los derechos y libertades fundamentales de las personas físicas en lo que respeta al tratamiento y de facilitar la libre circulación de datos personales en la Unión Europea. En el caso de España, la autoridad de control principal es la Agencia Española de Protección de Datos (AEPD).

Brecha de la seguridad de los datos personales: Todo incidente 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.

Brecha de la seguridad de la información recogida en los sistemas TIC de la AIReF: Todo incidente de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos o información transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos o información.

Encargado del Tratamiento: Persona física o jurídica, autoridad pública, servicio u otro organismo que presta un servicio al responsable que conlleva el tratamiento de datos personales por cuenta de este.

Responsable del Tratamiento: Persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

Responsable de Seguridad: Persona designada por el Presidente de la AIReF para asegurar el mantenimiento de la seguridad de la información disponible en los sistemas TIC de la AIReF.

3. Detección e identificación de brechas de seguridad

3.1 Detección de brechas de seguridad

La existencia de una brecha de seguridad puede conocerse o detectarse a través de fuentes internas o externas.

Fuentes internas:

- Notificaciones de usuarios: presencia de 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 de información, etc.
- Alertas generadas por software antivirus.
- Consumos excesivos y repentinos de memoria de disco en servidores y equipos.
- Anomalías de tráfico de red o picos de tráfico en horas inusuales.
- Alertas de sistemas de detección/prevención de intrusión.
- Alertas de sistemas de correlación de eventos.
- Análisis de registros de conexiones realizadas a través de proxys corporativos o conexiones bloqueadas en los cortafuegos.
- Análisis de registro de servidores y aplicaciones con intentos de acceso no autorizados.
- Análisis de registros en herramientas de prevención de pérdida de datos.

Fuentes externas:

- Comunicación por un tercero (proveedor de servicios informáticos, proveedor de servicios de internet o fabricante de soluciones de seguridad).
- Comunicación por un cliente.
- Comunicación o notificación por organismos públicos como el Instituto Nacional de Ciberseguridad (INCIBE), el Centro Criptológico Nacional (CCN), Fuerzas y Cuerpos de Seguridad del Estado o incluso mediante información publicada en medios de comunicación.

Tipos de brechas de seguridad.

Las brechas de seguridad se pueden clasificar en las siguientes categorías:

- Brecha de confidencialidad: Partes no autorizadas o sin propósito legítimo para acceder a la información acceden a ella.
- Brecha de integridad: Se altera la información original y la sustitución de datos puede ser perjudicial para el individuo.
- Brecha de disponibilidad: No se puede acceder a los datos originales cuando es necesario. Puede ser temporal o permanente.

Niveles de criticidad de las brechas de seguridad.

- Crítico: Afecta a datos valiosos, gran volumen y en poco tiempo.
- Muy Alto: Dispone de capacidad para afectar a información valiosa en cantidad apreciable.
- Alto: Dispone de capacidad para afectar a información valiosa.
- Medio: Dispone de capacidad para afectar a un volumen apreciable de información.
- Bajo: Escasa o nula capacidad para afectar a un volumen apreciable de información.

3.2 Registro de brechas de seguridad

Se debe mantener un registro de todas las brechas de la seguridad que se produzcan.

Es importante que al registrar el incidente de seguridad se aporte toda la información posible sobre la naturaleza de la brecha, categoría de los datos y el número aproximado de registros afectados.

4. Respuesta a las brechas de seguridad

Una vez detectada, analizada y valorada la brecha de seguridad, se debe iniciar el proceso de gestión y respuesta.

El proceso de gestión y respuesta se desarrolla de la siguiente manera:

4.1 Contención del incidente

La contención del incidente que ocasiona la brecha de seguridad proporciona tiempo para desarrollar una estrategia de respuesta específica.

Las medidas de contención pueden ser inmediatas o de aplicación progresiva en función del desarrollo de la resolución del incidente. A continuación, se enumeran algunas de las medidas de contención que podrían ser de aplicación en función de cada caso:

- Impedir el acceso al origen de la divulgación: dominios, puertos, servidores, la fuente o los destinatarios de la divulgación.

- Suspender las credenciales lógicas y físicas con acceso a información privilegiada.
- Cambiar todas las contraseñas de usuarios privilegiados o hacer que los usuarios lo hagan de manera segura.
- Hacer una copia del sistema (clonado), hacer una copia bit a bit del disco duro que contiene el sistema y luego analizar la copia utilizando herramientas forenses.
- Aislar el sistema utilizado para revelar los datos con el fin de realizar un análisis forense con posterioridad.
- Si los datos han sido divulgados a servidores públicos, solicitar al propietario (o web master) que elimine los datos divulgados.
- Si no es posible eliminar los datos divulgados, proporcionar un análisis completo al departamento correspondiente o a quien ejerza dichas funciones.
- Vigilar la difusión de los documentos/datos filtrados en los diferentes sitios web y redes sociales, así como los comentarios y reacciones de los usuarios de internet.

4.2 Solución/erradicación

Una vez contenido el incidente, se necesita realizar tareas de erradicación, verificando que las medidas (provisionales o definitivas) son las idóneas para la erradicación del incidente, asegurando que la misma vulnerabilidad que ha producido el incidente no se vuelve a producir.

A continuación, se indican algunos ejemplos de tareas de erradicación:

- Definir el proceso de desinfección, basado en firmas, herramientas, nuevas versiones y revisiones de software y probarlo, para asegurar que funciona adecuadamente.
- Comprobar la integridad de todos los datos almacenados en el sistema mediante un sistema de hashes que permita garantizar que los ficheros no han sido modificados, prestando especial atención en relación con los ficheros ejecutables.
- Revisar la correcta planificación y actualización de los motores y firmas de antivirus.
- Análisis con antivirus de todo el sistema, los discos duros y la memoria.
- Restaurar conexiones y privilegios paulatinamente. Especial acceso restringido paulatino de máquinas remotas o no gestionadas.

4.3 Recuperación

Cuando se ha conseguido contener el incidente, debe procederse a solventar sus efectos y a identificar y mitigar todas las vulnerabilidades que hubiesen sido explotadas.

Además, se debe proceder a restablecer el servicio en su totalidad, confirmando su funcionamiento normal y evitando, en la medida de lo posible, que sucedan nuevos incidentes basados en la misma causa, mediante la adopción de medidas activas y controles periódicos y eficaces que permitan el seguimiento pormenorizado de los procesos de mayor riesgo.

5. Notificación y comunicación de las brechas de seguridad

5.1 Brechas de seguridad de los datos personales

5.1.1 Notificación a la Autoridad de Control

Cuándo se debe notificar

Tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una brecha de la seguridad de los datos personales debe, sin dilación y, a más tardar, dentro de las 72 horas siguientes a tener constancia, efectuar la correspondiente notificación por escrito a la Autoridad de Control (Agencia Española de Protección de Datos).

Los encargados del tratamiento también están obligados a notificar de forma inmediata al responsable del tratamiento las brechas de la seguridad de los datos personales de las que tengan conocimiento y como máximo en el plazo de 24 horas.

Qué debe contener la notificación

La notificación que hay que hacer a la Agencia Española de Protección de Datos o a la autoridad de control correspondiente deberá, como mínimo:

- Describir la naturaleza de la brecha de la seguridad de los datos personales, incluyendo, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.
- Comunicar el nombre y los datos de contacto del Delegado de Protección de Datos o de otro punto de contacto en el que pueda obtenerse más información.
- Describir las posibles consecuencias de la brecha de la seguridad de los datos personales.
- Describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la brecha de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si en el momento de la notificación no fuese posible facilitar toda la información, podrá facilitarse posteriormente de manera gradual en distintas fases. La primera

comunicación se realizará en las primeras 72 horas y, al menos, se realizará una comunicación final o de cierre cuando se disponga de toda la información relativa a la brecha.

Cómo debe realizarse la notificación

La notificación a la Agencia Española de Protección de Datos se realizará a través de:

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

A cada notificación se le asignará una referencia que se deberá mantener e incluir en las sucesivas comunicaciones relacionadas, si las hubiera.

5.1.2 Comunicación a los afectados

Cuándo se debe comunicar

La brecha de la seguridad de los datos personales se debe comunicar al interesado, también lo antes posible, en caso de que pueda entrañar un alto riesgo para sus derechos y libertades, de tal manera que pueda permitir a dicho interesado tomar las precauciones necesarias.

Es importante tener en cuenta que la comunicación al interesado no será necesaria si se cumple alguna de las condiciones siguientes:

- 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 brecha 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.

- 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.

Por tanto, la aplicación de sistemas de cifrado, que hacen ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, permiten no tener que realizar ningún tipo de comunicación a los interesados en caso de que se sufra un ataque de seguridad, a menos que, por motivos justificados, la Agencia Española de Protección de Datos o la autoridad de control correspondiente ordenase realizar el envío de la información directa o públicamente.

Qué debe contener la comunicación

La comunicación de la brecha de la seguridad a las personas físicas cuyos datos personales hayan sido afectados por ella debe producirse en un lenguaje claro y sencillo, y debe contener los siguientes aspectos mínimos:

- Una descripción de la naturaleza de la brecha de la seguridad de los datos personales.
- Las recomendaciones concretas para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la brecha.
- El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

Cómo debe realizarse la comunicación

La comunicación de la brecha de la seguridad de los datos personales deberá realizarse de forma pública en un medio de comunicación adecuado cuando suponga un esfuerzo desproporcionado ponerse en contacto con los interesados.

La finalidad de esta comunicación pública es que se informe de manera igualmente efectiva a los interesados.

Cuando el responsable todavía no haya comunicado al interesado el incidente de seguridad de los datos personales, la Agencia Española de Protección de Datos o la autoridad de control correspondiente, una vez considerada la probabilidad de que tal incidente entrañe un alto riesgo, podrá exigirle que lo haga directamente o a través de una comunicación pública o podrá decidir que se cumple alguna de las condiciones para poder evitar la comunicación.

Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la AEPD o autoridad de control correspondiente, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales.

5.1.3 Comunicación a las Fuerzas y Cuerpos de Seguridad del Estado

Cuando las brechas de seguridad puedan suponer la comisión de un delito, se deberán comunicar a las Fuerzas y Cuerpos de Seguridad del Estado.

5.2 Brechas de seguridad de la información de los sistemas TIC de la AIReF

Tan pronto como se tenga conocimiento de la existencia de una brecha de seguridad de la información recogida en los sistemas TIC de la AIReF, se notificará de forma inmediata y por escrito al responsable de seguridad, para que se proceda a la adopción de las correspondientes medidas.

6. Seguimiento y cierre de las brechas de seguridad

Una vez detectadas y gestionadas las brechas, se requieren las siguientes tareas:

Comunicación/ realización de un informe final sobre la brecha de seguridad

La comunicación es fundamental durante todo el ciclo de vida del proceso de repuesta y debe hacerse de manera continua a las partes involucradas.

A fin de cerrar la brecha de seguridad, se elaborará un informe final sobre la trazabilidad del suceso y su análisis valorativo. Dicho informe recopilará toda la información y documentación relativa a la brecha de manera que se facilite el estudio y revisión por terceros, incluida la dirección de la entidad. El informe contendrá la siguiente información:

- Alcance e impacto del incidente.
- Controles preventivos existentes.
- Acciones de respuesta tomadas para la resolución de la brecha.
- Acciones tomadas para la prevención de futuras brechas.
- Impacto en la resolución del incidente de las acciones de respuesta tomadas.
- Accidentes definidas para el seguimiento.

Cierre de la brecha de seguridad

Una vez las acciones derivadas de los procesos del plan de actuación han concluido y se han alcanzado los objetivos, se procederá al cierre de la brecha de seguridad.

7. Registro de brechas de seguridad

Fecha	Nombre y puesto de la persona que detecta la brecha	Tipo de brecha de seguridad	Consecuencias de la brecha de seguridad	Medidas propuestas o adoptadas