Procedimiento de Gestión de Incidentes de Seguridad (GDPR)

Gonvarri Industries

PROC-CORP-05

Contenido:

1. Objetivo

El Objetivo del presente documento es establecer y comunicar a todas las áreas de Gonvarri Industries (a partir de ahora, GI) el procedimiento para notificar y gestionar de manera estándar los incidentes que puedan comprometer la seguridad de los Datos de Carácter Personal en posesión de GI, en cumplimiento del Reglamento General de Protección de Datos (GDPR).

En este sentido, el reglamento (EU) 2016/679 del Parlamento Europeo y del Consejo de la Unión Europea, aprobado el 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de esos datos, y por el que se deroga la Directiva 95/46/EC (Reglamento general de protección de datos), establece que los incidentes de seguridad que afecten a Datos de Carácter Personal deben ser documentados y notificados.

2. Alcance

La presente Política es de aplicación a todas las sociedades dentro del Espacio Económico Europeo que conforman el Grupo Gonvarri Industries, participadas mayoritariamente, directa o indirectamente, por su sociedad matriz, Gonvarri Corporación Financiera, S.L.U. y a todo el personal del Grupo Gonvarri Industries en el ejercicio de sus funciones y responsabilidades, y en todos los ámbitos profesionales en los que representen al Grupo, entendiendo por tales a los administradores, directivos, empleados y colaboradores del Grupo GI, cualquiera que sea su cargo o responsabilidad.

En todo caso, la actuación del Grupo respeta la legislación vigente en cada jurisdicción, por lo que en algunas de éstas los principios expuestos en la presente política pueden ser sustituidos por leyes, regulaciones y normativas vigentes más restrictivas.

3. Términos y Definiciones

- **Afectado/Interesado:** Titular de los datos objeto de incidente.
- **Área Encargada del Tratamiento:** Unidad responsable que trata los datos asociados al tratamiento que corresponda.
- **Comité de Privacidad**: Unidad máxima de reporte en materia de Privacidad.
- **Datos de Carácter Personal:** Cualquier información concerniente a personas físicas identificadas o identificables.
- **Encargado de privacidad:** Persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

- **Incidente:** Cualquier anomalía que suponga la destrucción, perdida o alteración accidental o ilícita de datos de carácter personal transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos.

- **Responsable de Privacidad:** Es el principal encargado de controlar y supervisar el cumplimiento de la normativa de privacidad y protección de datos en la organización.

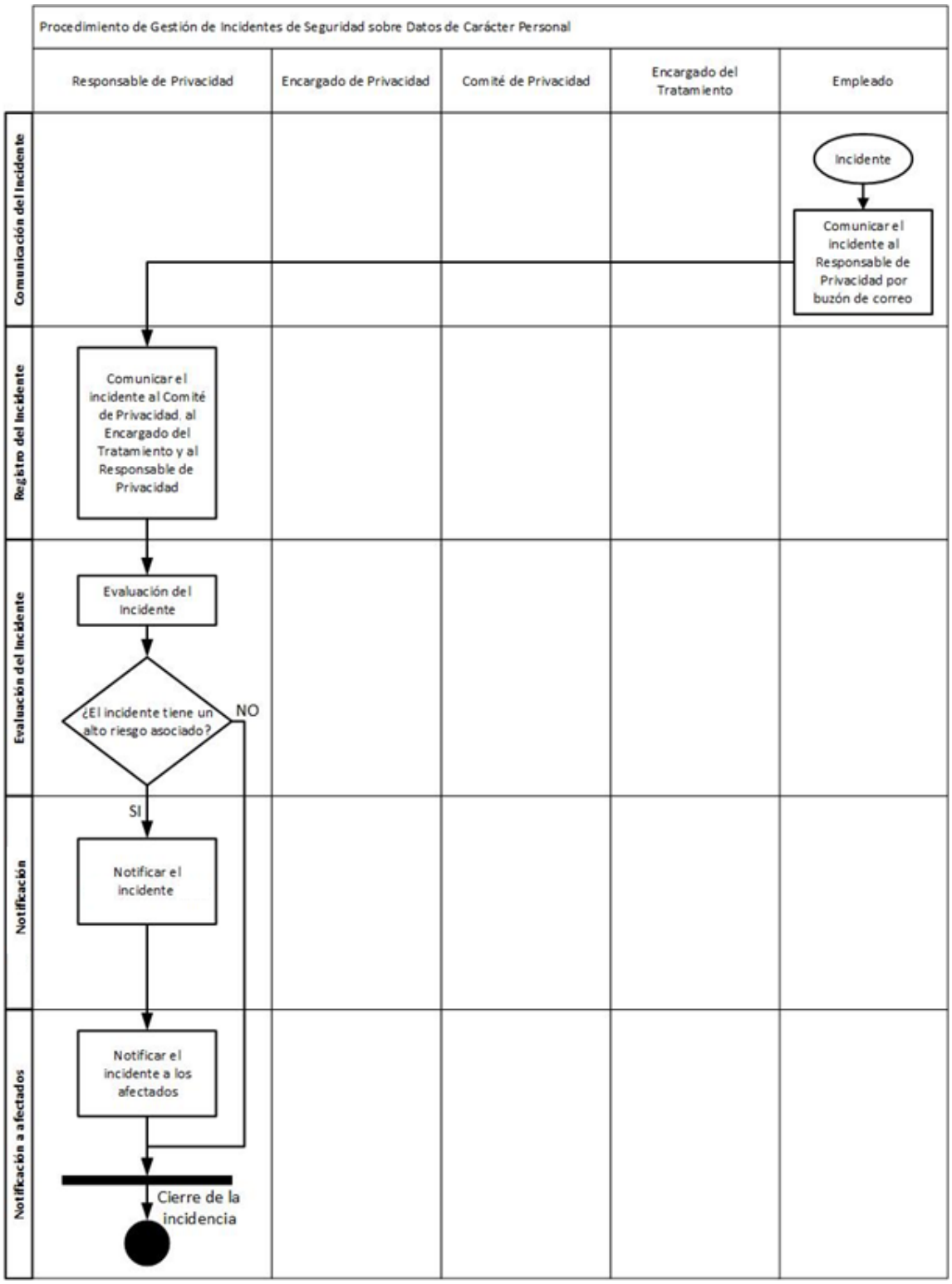
- **Titular de los datos:** Persona a la que pertenecen los datos.

- **Tratamiento de datos:** Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

4. Procedimiento de Gestión de Incidentes de Seguridad sobre Datos de Carácter Personal

El presente procedimiento se ejecutará ante cualquier incidente que afecte a la seguridad de los Datos de carácter personal. En cualquier caso, se llevarán a cabo las acciones descritas en los apartados “4.1 Comunicación del Incidente”, “4.2 Registro del Incidente” y “4.3 Evaluación del Incidente”, ejecutándose las acciones descritas en el apartado “4.4. Notificación del Incidente” en los casos en que el incidente de seguridad suponga un riesgo alto para los derechos y libertades de los afectados.

A continuación, se muestra gráficamente el flujo general seguido en el procedimiento de gestión de incidentes de seguridad sobre Datos de Carácter Personal:


Procedimiento de Gestión de Incidentes de Seguridad sobre Datos de Carácter Personal
Responsable de Privacidad
Encargado de Privacidad
Comité de Privacidad
Encargado del Tratamiento
Empleado
Comunicación del Incidente
Registro del Incidente
Evaluación del Incidente
Notificación
Notificación a afectados
Incidente
Comunicar el incidente al Responsable de Privacidad por buzón de correo
Comunicar el incidente al Comité de Privacidad, al Encargado del Tratamiento y al Responsable de Privacidad
Evaluación del Incidente
¿El incidente tiene un alto riesgo asociado?
NO
SI
Notificar el incidente
Notificar el incidente a los afectados
Cierre de la incidencia

4.1 Comunicación del Incidente

- Todo el personal está obligado a comunicar cualquier incidencia de seguridad relativa a los datos de carácter personal al Encargado de Privacidad. Dicha notificación se realizara mediante el buzón de correo electrónico Privacy.Incidents@Gonvarri.com o bien a través del formulario ubicado en la web corporativa.

- Las incidencias pueden aparecer en todas las actividades relacionadas con el manejo y gestión de información en formato físico o bases de datos lógicas que almacenen datos de carácter personal, así como en el desarrollo de las actividades que afecten a la seguridad de los datos contenidos en las mismas.

- A continuación, citamos algunos ejemplos de incidencias:

    - Crear una base de datos de carácter personal sin realizar la solicitud de registro en la Autoridad de Control.
    - Recabar datos de carácter personal sin la autorización del afectado y sin informarle de sus derechos.
    - Uso de los datos de carácter personal con una finalidad diferente a la registrada en la Autoridad de Control.
    - Intento o violación del control de acceso físico y de BBDD.
    - Alterar BBDD (borrado, modificación o inclusión de datos que atente contra la calidad de la BBDD).
    - Sacar datos en soportes sin la autorización pertinente.
    - Sacar datos en soportes diferentes a los autorizados en el registro de la base de datos.
    - Incumplir lo establecido en el Documento de Seguridad para la recuperación de datos.
    - Incumplir los plazos establecidos para resolver y contestar las solicitudes para ejercer los derechos del interesado.
    - Usar ilícitamente datos de carácter personal.
    - Ejecutar el proceso de recuperación de datos.
    - Gestionar incorrectamente los backups.
    - Perdida de activo material (Teléfono de trabajo, portátiles, etc).
    - Imposibilidad de acceder al sistema con nuestro usuario/contraseña habitual.
    - Contraseña de acceso posiblemente comprometida.
    - Comportamiento anormal del sistema (información incompleta o irreal, fallos inesperados, etc.).

- Las incidencias relativas a datos de carácter personal no se limitan al tratamiento automatizado, sino que también incluyen los medios de tratamiento no automatizado. Así pues, las incidencias que afecten a dichos medios, como por ejemplo la pérdida de listados en papel con datos de carácter personal, deberán ser también obligatoriamente reportadas y registradas por el sistema descrito en el presente apartado.

4.2 Registro del Incidente

Una vez se ha comunicado el incidente de seguridad, se realizarán las siguientes acciones:

- El Responsable de Privacidad registrará formalmente dicho incidente de seguridad. En este sentido, se detallará al menos la siguiente información:

    - Tipo de Incidencia.
    - Descripción de la Incidencia.
    - Fecha y hora de la notificación.
    - Usuario que reporta la incidencia.

- En el caso de que sea necesario, el Responsable de Privacidad se coordinará con el Encargado de Privacidad para el análisis del incidente de seguridad. Adicionalmente, el Responsable de Privacidad podrá solicitar soporte técnico de responsables de departamentos durante la fase de análisis del incidente.

4.3 Evaluación del Incidente

Una vez se ha registrado el incidente de seguridad, se realizarán las siguientes acciones:

- El Responsable de Privacidad se encargará de evaluar el incidente de seguridad.

- En caso de que el Responsable de Privacidad lo considere oportuno, en base a la criticidad del incidente, podrá convocar al Comité de Privacidad con el fin de evaluar el impacto del incidente en el grupo.

- La categoría o nivel de criticidad del incidente respecto a la seguridad de la información afectada. Siguiendo la clasificación genérica, podemos 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).

Adicionalmente pueden existir escenarios técnicos que pueden dar lugar a un incidente:

- 0-day (vulnerabilidad no conocida): Vuln0erabilidad que permite a un atacante el acceso a los datos en la medida en que es una vulnerabilidad desconocida. Esta vulnerabilidad estará disponible hasta que el fabricante o desarrollador la resuelva.

- APT (ataque dirigido): Se refiere a diferentes tipos de ataques dirigidos normalmente a recabar información fundamental que permita continuar con ataques más sofisticados. En esta categoría se encuadraría por ejemplo una campaña de envío de email con software malintencionado a empleados de una empresa hasta conseguir que alguno de ellos lo instale en su equipo y proporcione una puerta de entrada al sistema.

- Denegación de servicio (DoS/DDoS): Consiste en inundar de tráfico un sistema hasta que no sea capaz de dar servicio a los usuarios legítimos del mismo.

- Acceso a cuentas privilegiadas: El atacante consigue acceder al sistema mediante una cuenta de usuario con privilegios avanzados, lo que le confiere libertad de acciones. Previamente deberá haber conseguido el nombre de usuario y contraseña por algún otro método, por ejemplo, un ataque dirigido.

- Código malicioso: piezas de software cuyo objetivo es infiltrase o dañar un ordenador, servidor u otro dispositivo de red con finalidades muy diversas. Una de las posibilidades para que el código dañino alcance a una organización es que un usuario lo instale de forma involuntaria.

- Compromiso de la información: Recoge todos los incidentes relacionados con el acceso y fuga, modificación o borrado de información no pública.

- Robo y/o filtración de datos: Se incluye en esta categoría la pérdida/robo de dispositivos de almacenamiento con información.

- Desfiguración (Defacement): Es un tipo de ataque dirigido que consiste en la modificación de la página web corporativa con la intención de colgar mensajes reivindicativos de algún tipo o cualquier otra intención. La operativa normal de la web queda interrumpida, produciéndose además daños reputacionales.

- Explotación de vulnerabilidades de aplicaciones: Cuando un posible atacante logra explotar con éxito una vulnerabilidad existente en un sistema o producto consiguiendo comprometer una aplicación de la organización.

- Ingeniería social: Son técnicas basadas en el engaño, normalmente llevadas a cabo a través de las redes sociales, que se emplean para dirigir la conducta de una persona u obtener información sensible. Por ejemplo, el usuario es inducido a pulsar sobre un enlace haciéndole pensar que es lo correcto.

En el caso de que se produzcan algunos de estos supuestos, se deberá notificar el incidente de seguridad a:

- La Autoridad de control
- Los afectados.

4.4 Notificación del Incidente

4.4.1. Notificación a la Autoridad de control

Como se ha comentado anteriormente, 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 en las 72 horas siguientes a tener constancia, efectuar la correspondiente notificación a la Autoridad de Control. Se considera que se tiene constancia de una brecha de seguridad cuando hay una certeza de que se ha producido y se tiene conocimiento suficiente de su naturaleza y alcance.

El criterio a tener en cuenta para determinar si un incidente ha producido "una brecha de la seguridad de los datos personales" se recoge en el propio RGPD, e incluye "todas aquellas brechas de la seguridad que ocasionen 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.

Esta comunicación se realizará con el modelo de comunicación descrito en el Anexo II, y deberá contener la siguiente información:

Datos identificativos y de contacto de:

- Entidad / Responsable del tratamiento
- Delegado de Protección de Datos (si está designado) o persona de contacto.
- Indicación de si se trata de una notificación completa o parcial. En caso de tratarse de una notificación parcial indicar si se trata de una primera notificación o una notificación complementaria.

Información sobre la brecha de seguridad de datos personales:

- Fecha y hora en la que se detecta.
- Fecha y hora en la que se produce el incidente y su duración.
- Circunstancias en que se haya producido la brecha de seguridad de datos personales (por ejemplo, pérdida, robo, copia, etc.)
- Naturaleza y contenido de los datos personales en cuestión.
- Resumen del incidente que ha causado la brecha de seguridad de datos personales (con indicación de la ubicación física y del soporte de almacenamiento).
- Posibles consecuencias y efectos negativos en los afectados.
- Medidas técnicas y organizativas que se hayan adoptado por parte del responsable del tratamiento según el apartado 33.2d) del RGPD.

- Categoría de los datos afectados y número de registros afectados.

- Categoría y número de individuos afectados.

- Posibles cuestiones de carácter transfronterizo, indicando la posible necesidad de notificar a otras autoridades de control.

- 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 notificación se realizará en las primeras 72h, y al menos se realizará una comunicación final o de cierre cuando se disponga de toda la información relativa al incidente.

- Cuando el responsable realice la primera notificación deberá informar si proporcionará más información a posteriori. También podrá aportar información adicional mediante comunicaciones intermedias a la autoridad de control bajo petición de esta, o cuando el responsable considere adecuado actualizar la situación de la misma.

- Cuando la notificación inicial no sea posible en el plazo de 72 horas, la notificación deberá realizarse igualmente a posteriori, y en ella deberán constar y justificarse los motivos de la dilación.

- Las notificaciones deben ser sean claras, concisas y que incluyan la información necesaria para que puedan ser analizadas adecuadamente.

4.4.2. Identificación de la Autoridad de control

Cuando un incidente pueda afectar a los datos de personas en más de un Estado miembro, el responsable debe realizar una evaluación sobre cuál es la autoridad principal a la que deberá realizar la notificación y, en caso de duda, se debe como mínimo, notificar a la autoridad de control local donde la brecha ha tenido lugar. Actuará como autoridad de control principal, la del establecimiento principal o la del único establecimiento del responsable.

Los criterios para identificar el establecimiento principal son:

- Lugar donde tenga la sede principal el responsable.
- Lugar donde se toman las decisiones sobre fines y medios.

En el siguiente enlace publicado por el WP29, figura la información de contacto para cada autoridad de control:

20180419_NationalDa
taProtectionAuthoritie

4.4.3. Notificación a los afectados

Al igual que en el aparatado anterior, en el caso de que se produzca un incidente de seguridad que suponga un riesgo alto para los derechos y libertades de los afectados, este deberá comunicarse a los afectados con el objetivo de permitir a estos la toma de medidas para protegerse de las consecuencias del incidente.

El Responsable de Privacidad es el encargado de notificar a los afectados el incidente, debiendo comunicarlo a los mismos en un tiempo prudencial.

La notificación se realizará mediante email, SMS, correo postal o por teléfono e incluirá la siguiente información:

1. Datos de contacto del Delegado de Protección de Datos, o en su caso, del punto de contacto en el que pueda obtenerse más información.
2. Descripción general del incidente y momento en que se ha producido.
3. Las posibles consecuencias de la brecha de la seguridad de los datos personales.
4. Descripción de los datos e información personal afectados.
5. Resumen de las medidas implantadas hasta el momento para controlar los posibles daños.

Otras informaciones útiles a los afectados para proteger sus datos o prevenir posibles daños.

4.5 Excepción a la notificación / comunicación

No será necesaria la notificación a la Autoridad de Control cuando el responsable pueda demostrar, de forma fehaciente, que la brecha de la seguridad de los datos personales no entraña un riesgo para los derechos y las libertades de las personas físicas.

Por ejemplo, si los datos ya se encontraban públicamente disponibles y su revelación no entraña ningún riesgo hacia el titular de los datos.

Asimismo, no será necesaria la comunicación a los afectados cuando:

- El responsable ha tomado medidas técnicas y organizativas adecuadas, como que los datos no sean inteligibles para personas o máquinas no autorizadas con anterioridad a la brecha de seguridad de datos personales (mediante el uso de: cifrados de datos de última generación, 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.

- El responsable ha tomado con posterioridad a la brecha de seguridad de datos personales las medidas de protección que mitiguen total o parcialmente el posible impacto para los afectados y garanticen que ya no hay posibilidad de que el alto riesgo se materialice. 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 notificación a los afectados 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. Ante esta situación, se realizará la notificación de manera pública a través de los canales establecidos por el responsable.

5. Responsabilidades

Se adjunta a continuación una matriz de asignación de responsabilidades (RACI) dentro del proceso de gestión de incidentes de seguridad sobre datos de carácter personal. En esta matriz se asigna en cada una de las tareas, una o más responsabilidades representadas por una letra:

- R (Responsable): Este rol corresponde a quien efectivamente realiza la tarea.
- A (Encargado): Este rol se responsabiliza de que la tarea se realice y es el que debe rendir cuentas sobre su ejecución.
- C (Consultado): Este rol posee alguna información o capacidad necesaria para realizar la tarea.
- I (Informado): Este rol debe ser informado sobre el avance y los resultados de la ejecución de la tarea.

Tareas / Recurso	Comité de Privacidad	Responsable de Privacidad	Encargado de Privacidad	Área Encargada del Tratamiento	Empleado
Comunicar el incidente	**I**	**I**	**I**	**I**	**R / A**
Registrar el incidente	**I**	**R / A**	**I / C**	**I**	
Evaluar el incidente	**I/C**	**R / A**	**I / C**	**I/C**	
Notificar a la Autoridad de Control	**I**	**R / A**	**I**	**I**	
Notificar a los Afectados	**A**	**R**	**I**	**I**	

6. Idioma

La presente Norma se publica en idioma español e inglés, siendo prevalente el primero, en caso de divergencia entre ambas.

7. Control de versión y documento

Versión	Fecha	Descripción	Elabora	Supervisa
Versión 1	19 de Octubre de 2018	Versión inicial del documento	Daniel Lluch	Comité de Cumplimiento

8. Aprobación y entrada en vigor

Esta norma ha sido aprobada por el Comité de Cumplimiento del Grupo Gonvarri Industries el día 31 de Octubre de 2018, y entra en vigor 30 días naturales después del día de su aprobación. A partir de la entrada en vigor quedan derogadas las disposiciones previas existentes en su caso que regulen el mismo contenido.

FIRMADA POR EL COMITÉ DE CUMPLIMIENTO

ANEXO

Formulario de Notificación de Brechas de Seguridad (AEPD)

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

FORMULARIO NOTIFICACIÓN
BRECHAS DE SEGURIDAD

1. Datos de la notificación

Tipo de notificación: ○ Inicial, ○ Adicional, ○ Completa
Referencia notificación inicial:_____ Fecha notificación inicial:_____

2. Identificación del Delegado de Protección de Datos o persona de contacto

NIF/NIE: _____ Nombre:_____
Apellidos:_____ Cargo:_____
Dirección:_____ C.P.:_____
Provincia:_____ Localidad:_____
Teléfono(s):_____/_____ e-mail:_____

3. Identificación del responsable del tratamiento

Nombre de la Organización: _____
Tipo de Organización: ○ Privada, ○ Pública
CIF:_____ Dirección distinta del DPD o persona de contacto:☐
Dirección:_____ C.P.:_____
Provincia:_____ Localidad:_____
Teléfono(s):_____/_____ e-mail:_____

4. Identifiación del encargado del tratamiento

¿Hay otra organización implicada en la brecha de seguridad?☐
Nombre de la Organización: _____
Tipo de Organización: ○ Privada, ○ Pública
CIF:_____
Dirección:_____ C.P.:_____
Provincia:_____ Localidad:_____
Teléfono(s):_____/_____ e-mail:_____

5. Información temporal de la brecha

Fecha detección de la brecha: _____ ○ Exacta, ○ Estimada.
Medios de detección de la brecha:

_____
_____
_____

Justificación de notificación tardía (notificación pasadas 72h desde la detección):

_____
_____
_____

Fecha inicio de la brecha: _____ ○ Exacta, ○ Estimada.
¿Está resuelta la brecha? ☐ Fecha de resolución: _____ ○ Exacta, ○ Estimada.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

FORMULARIO NOTIFICACIÓN
BRECHAS DE SEGURIDAD

6. Sobre la brecha

Resumen del incidente:

_____

_____

_____

Tipología:

- ☐ Brecha de confidencialidad (acceso no autorizado)
- ☐ Brecha de integridad (modificación no autorizada)
- ☐ Brecha de disponibilidad (desaparición o pérdida)

Medio por el que se ha materializado la brecha:

☐ Datos personales residuales en dispositivos obsoletos.	☐ Documentación perdida, robada o depositada en localización insegura.	☐ Eliminación incorrecta de datos personales en formato papel.
☐ Hacking.	☐ Malware (e.j. ransomware).	☐ Phishing.
☐ Correo perdido o abierto.	☐ Dispositivo perdido o robado.	☐ Publicación no intencionada.
☐ Datos personales mostrados al individuo incorrecto.	☐ Datos personales enviados por error.	☐ Revelación verbal no autorizada de datos personales.

☐ Otros:_____

Contexto:

○ Interna (acción no intencionada)	○ Interna (acción intencionada)
○ Externa(acción no intencionada)	○ Externa (acción intencionada)
○ Otros:	

Medidas preventivas aplicadas antes de la brecha:

_____

_____

_____

_____

7. Sobre los datos afectados

Categoría de datos afectados:

☐ Datos básicos	☐ Credenciales de acceso o identificación	☐ Datos de contacto
☐ DNI, NIE y/o Pasaporte	☐ Datos económicos o financieros	☐ Datos de localización
☐ Sobre condenas e infracciones penales	☐ Otros: _____	

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

FORMULARIO NOTIFICACIÓN BRECHAS DE SEGURIDAD

Categorías especiales de datos:

☐ Sobre el orígen racial ☐ Sobre la opinión política
☐ Sobre la religión o creencia ☐ Sobre la afiliación sindical ☐ Sobre la vida sexual
☐ De salud ☐ Genéticos ☐ Biométricos
☐ Desconocidos ☐ Otros: _____

Número aproximado de registros de datos personales afectados:

8. Sobre los sujetos afectados

Perfil de los sujetos afectados:

☐ Clientes ☐ Usuarios ☐ Empleados ☐ Suscriptores
☐ Estudiantes ☐ Pacientes ☐ Otros: _____

Número aproximado de personas afectadas:

9. Posibles consecuencias

Brecha de confidencialidad:

☐ Divulgación a terceros /difusión en internet ☐ Los datos pueden ser explotados con otros fines
☐ Enriquecimiento de otras bases de datos ☐ Otras: _____

Brecha de integridad:

☐ Datos han sido modificados aunque hayan quedado inservibles o irrecuperables ☐ Datos han sido modificados y utilizados para otros fines
☐ Otras: _____

Brecha de disponibilidad:

☐ Imposibilidad de la prestación de un servicio a los interesados ☐ Deterioro de las condiciones de prestación de un servicio a los interesados
☐ Otras: _____

Naturaleza del impacto potencial sobre los sujetos:

☐ Pérdida de control sobre sus datos personales ☐ Limitación de sus derechos ☐ Discriminación
☐ Usurpación de identidad ☐ Fraude ☐ Pérdidas financieras
☐ Reidentificación no autorizada ☐ Perdida de confidencialidad de datos afectados por secreto profesional
☐ Daños a la reputación ☐ Otras: _____

Severidad de las consecuencias para los individuos: ○ Baja ○ Media ○ Alta ○ Muy alta

Medidas tomadas para solucionar la brecha y minimizar el impacto sobre los afectados:

_____
_____
_____
_____
_____

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

FORMULARIO NOTIFICACIÓN
BRECHAS DE SEGURIDAD

10. Comunicación a los interesados

¿Se ha comunicado la brecha a los interesados?

○ Si — Fecha en la que se informó: _____

Número de sujetos informados: _____

Medios o herramientas de comunicación: _____

○ No, pero serán informados — Fecha en la que se informará: _____

○ No serán informados — Justificación para no informar: _____

○ Pendiente de decidir

(Adjuntar contenido de la comunicación a los interesados)

11. Implicaciones trasfronterizas

¿Hay sujetos de otros Estados miembros de la UE afectados por la brecha? ☐

Marque los Estados que puedan estar afectados (A) y aquellos a los que haya notificado(N) la misma brecha de seguridad:

A	N		A	N		A	N	
☐	☐	Alemania	☐	☐	Austria	☐	☐	Bélgica
☐	☐	Bulgaria	☐	☐	Chipre	☐	☐	Croacia
☐	☐	Dinamarca	☐	☐	España	☐	☐	Eslovaquia
☐	☐	Eslovenia	☐	☐	Estonia	☐	☐	Finlandia
☐	☐	Gran Bretaña	☐	☐	Grecia	☐	☐	Hungría
☐	☐	Irlanda	☐	☐	Italia	☐	☐	Letonia
☐	☐	Lituania	☐	☐	Luxemburgo	☐	☐	Malta
☐	☐	Países Bajos	☐	☐	Polonia	☐	☐	Portugal
☐	☐	Rep. Checa	☐	☐	Rumania	☐	☐	Suecia

12. Documentos adjuntos

(Adjuntar documentos)

En_____,a___de_____20__


Gonvarri
Industries