Procedimiento de brechas de seguridad

Protección de datos

Procedimiento de requisitos previos al tratamiento de datos

Procedimiento a seguir en el Ayuntamiento de Bolaños de Calatrava, para la correcta gestión de violaciones de seguridad, de conformidad con los artículos 33 y 34 del 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

Información del documento

Control de versiones

Versión	Fecha	Descripción de cambios
V 1.0	25/01/2022	Versión inicial del documento

Propiedad del documento

Propietario: Ayuntamiento de Bolaños de Calatrava

Elaborado: GRUPO CIES

Índice

1. Objeto

El presente documento tiene por objeto establecer un procedimiento de gestión de violaciones de seguridad, que afecten a los datos de carácter personal tratados por el Ayuntamiento de Bolaños de Calatrava, en adelante el Ayuntamiento, como Responsable de Tratamiento, de conformidad con los artículos 33 y 34 del 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

2. Alcance

El procedimiento descrito en el presente documento se aplicará a la totalidad de violaciones de seguridad que se produzcan en los datos de carácter personal, tratados por el Ayuntamiento.

2.1 ¿Qué es una violación de seguridad?

El Reglamento General de Protección de Datos define en su artículo 4 (12) lo que es una brecha de seguridad de los datos personales, entendiéndose como toda violación 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.

A modo enumerativo *-y no taxativo-*, pueden ser consideradas violaciones de seguridad las siguientes:

- Virus y malware maliciosos que afecten a los datos de carácter personal
- Robo y/o pérdida de equipos en los que se almacenen datos de carácter personal
- Incendios y otros accidentes que afecten a los datos de carácter personal
- Acceso a los datos de carácter personal por parte de personas no autorizadas
- Mandar un correo a varias personas sin CCO.
- Olvidar la agenda de contactos en un autobús.
- Perder el móvil o un usb corporativo.
- Acceso de un ciudadano a una notificación de otro en la sede electrónica.
- Apuntar nuestro usuario y contraseña en un post-it a la vista de los/as compañero/as.
- Una suplantación de identidad de un proveedor.
- El robo de nuestro usuario y contraseña del correo electrónico.
- Los accesos indebidos a la información.
- La publicación de listados de personas con el nombre, apellidos, DNI completo y otros datos personales sin que exista una base legal para ello…
- Otros…

2.2 ¿Qué no es una violación de seguridad?

- No afecten a datos personales, es decir, a datos que no sean de personas físicas identificadas o identificables.
- No afecten a tratamientos de datos personales llevados a cabo por un responsable o un encargado.
- Ocurran en tratamientos llevados a cabo por una persona física en el ámbito doméstico.

Un incidente de seguridad que no ha afectado a datos personales o tratamientos de datos personales, no es una violación de seguridad de los datos personales, dado que no podría producir daños sobre los derechos y libertades de las personas físicas cuyos datos son objeto del tratamiento, independientemente de otros perjuicios que pueda producir al responsable o encargado del tratamiento.

3. Procedimiento a seguir cuando se detecta una brecha de seguridad

En todo tratamiento debe determinarse el riesgo que para los derechos y libertades puede suponer que se materialice una violación de seguridad, es decir, un tratamiento no legítimo o accidental sobre los datos. El presente documento contiene los procedimientos para responder a las obligaciones que se desprenden del RGPD.

3.1. Detección

Un incidente puede ser detectado por:

- Medios de detección propios: sistema de monitorización etc.
- Personas empleadas en el Ayuntamiento
- Personas afectadas por el tratamiento
- Medios de Comunicación o externos como Redes Sociales
- Adjudicatarios o un prestador de servicio
- Cualquier tercero ajeno al tratamiento de datos personales

Los plazos de detección y resolución de una brecha de datos personales junto con los medios de detección son relevantes para determinar el nivel de riesgo para los derechos y libertades de las personas afectadas, es por ello por lo que, esta información quedará documentada en el Registro de Incidentes -Ver Anexo 01 Registro de Incidentes -:

- Fecha de detección: Fecha en la que el responsable de tratamiento tiene constancia de que un incidente ha afectado a datos personales, y es la fecha que establece el inicio de los plazos de notificación a la Autoridad de Control y a los afectados.
- Medios de detección: Medio a través del cual se ha tenido constancia de la brecha.
- Fecha de inicio de la brecha: Fecha de inicio del incidente que provoca la brecha de datos personales.

3.2. Descripción del incidente de seguridad

Para la correcta valoración de la violación de seguridad, el primer paso es la realización de una descripción de esta, teniendo en cuenta los siguientes factores:

- Información general del tratamiento

Se trata de información de carácter general sobre el tratamiento de datos personales que se ha visto afectados por la brecha de datos personales y permite estimar el riesgo inherente al tratamiento:

- Duración del tratamiento, permitiendo distinguir entre tratamientos puntuales y tratamientos de larga duración.
- Número total de personas cuyos datos forman parte del tratamiento afectado por la brecha de datos personales, aunque no necesariamente todos se hayan visto afectados por la brecha de datos personales.
- Ámbito geográfico del tratamiento, si se realiza sobre personas de la misma localidad, provincia, si es a nivel nacional y/o de otro Estado Miembro, o a nivel mundial.

- Origen e intencionalidad: Intencionalidad del incidente que ha causado la brecha:

  - Intencionado – Ejemplo: Ataque de un ciberdelincuente de diverso tipo, robo de un dispositivo.
  - Accidental o fortuito – Ejemplo: Envío de datos personales por error a destinatario incorrecto, pérdida de dispositivo, publicación no intencionada.

- Origen o ámbito del incidente:

  - Interno: Personal o sistemas bajo el control del responsable de tratamiento – Ejemplo: envío de datos personales a encargado de tratamiento incorrecto o extravío de dispositivo.
  - Externo: Otros, ajenos al responsable y encargado de tratamiento – Ejemplo: ciberataque o robo de dispositivos.

- Tipología

Uno de los parámetros más importantes a la hora de evaluar el nivel de riesgo de una brecha de datos personales es determinar con exactitud su tipología, es decir determinar a qué dimensión/es de seguridad de los datos personales ha afectado la brecha.

Integridad	Una alteración no autorizada o accidental de los datos personales
Disponibilidad	Pérdida de acceso accidental o no autorizada a los datos personales, o su destrucción
Confidencialidad	Revelación no autorizada o accidental de los datos personales, o su acceso.

- Categorías de datos y perfil de los afectados

El Ayuntamiento, determinará con precisión las categorías de datos personales afectadas, el número de personas afectadas y su perfil. Estos tres parámetros son fundamentales para poder determinar el nivel de riesgo para los afectados por la brecha de datos personales.

3.3. Valoración de la brecha de seguridad

Si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la

reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona física en cuestión.

Es por ello que, el Ayuntamiento deberá realizar una valoración del incidente de seguridad y proceder a determinar el nivel de riesgo para los derechos y libertades de las personas físicas y en función del riesgo tomar las opciones oportunas con el objetivo de protegerlos.

Con el objeto de evaluar el incidente de seguridad, se ha utilizado la metodología descrita por la autoridad de control – *Guía para la notificación de brechas de datos personales*-.

Para mantener el principio de responsabilidad actividad y poder evidenciar a la Autoridad de Control, el cumplimiento de lo establecido en el procedimiento se ha procedido a analizar el riesgo presentado en las violaciones de seguridad, con respecto a los derechos y libertades de las personas.

Criterios a Valorar

La toma de decisiones relacionada con la notificación de brechas de seguridad a la autoridad de control se evalúa en base a tres parámetros:

- Volumen de datos afectados
- Tipología de los datos
- Impacto de la brecha

Riesgo = Probabilidad (Volumen) x Impacto (Tipología x Impacto)

Probabilidad: Se trata de determinar si existe la posibilidad de que las consecuencias se materialicen con un nivel de severidad alto o muy alto.

Improbable	Cuando el responsable pueda garantizar que no puede materializarse el daño
Baja, alta y muy alta	cuando exista cierta probabilidad de materialización del daño.

Impacto: Para determinar el nivel de severidad debe tenerse en cuenta el daño que se puede producir al materializarse las consecuencias identificadas, considerando los siguientes niveles.

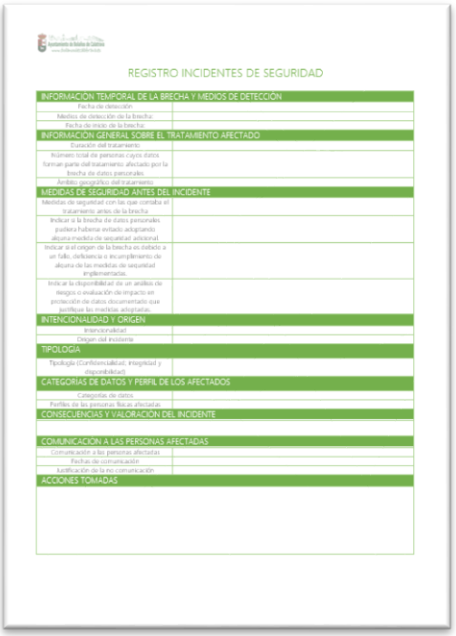
Muy alta	Las personas pueden enfrentar consecuencias muy significativas, o incluso irreversibles, que no pueden superar (exclusión o marginación social, dificultades financieras tales como deudas considerables o incapacidad para trabajar, dolencias psicológicas o físicas a largo plazo, muerte, etc.). Daña derechos fundamentales y libertades públicas de forma irreversible.
Alta	Las personas pueden enfrentar consecuencias significativas, 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.). En general cuando las consecuencias afectan a derechos fundamentales, pero pueden revertirse.
Media	Las personas pueden encontrar inconvenientes importantes, produciendo un daño limitado, 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.)
Baja	Las personas no se verán afectadas o pueden encontrar algunos inconvenientes muy limitados y reversibles que superarán sin ningún problema (tiempo de reingreso de información, molestias, irritaciones, etc.)

<table>
<tr><td rowspan="4">Probabilidad</td><td>Muy alta</td><td colspan="2" rowspan="2">Valorar comunicar a los afectados</td><td colspan="2" rowspan="2">Obligación de comunicar a las personas afectadas</td></tr>
<tr><td>Alta</td></tr>
<tr><td>Media</td><td colspan="2">Valorar comunicar a los afectados</td><td colspan="2">Obligación de comunicar a las personas afectadas</td></tr>
<tr><td>Baja</td><td colspan="4">Valorar comunicar a los afectados</td></tr>
<tr><td></td><td></td><td>Baja – Muy limitada</td><td>Media - Limitado</td><td>Alta - Significativo</td><td>Muy alta - Muy significativo</td></tr>
<tr><td></td><td></td><td colspan="4">Impacto/Gravedad</td></tr>
</table>

3.4. Registro de la brecha de seguridad

Con independencia de la necesidad de notificar a la Autoridad de Control sobre una brecha de datos personales, el artículo 33.5 del RGPD establece la obligación del responsable de tratamiento de documentar cualquier brecha, incluidos los hechos relacionados con la brecha, sus efectos y las medidas correctivas adoptadas.

Con el objeto de lograr un correcto desarrollo del procedimiento de brechas de seguridad, procederá a documentas el suceso en el Registro de Incidentes- *Ver Anexo 01 Registro de Incidentes-*.



REGISTRO INCIDENTES DE SEGURIDAD

INFORMACION TEMPORAL DE LA BRECHA Y MEDIOS DE DETECCION
Fecha de detección
Medios de detección de la brecha
Fecha de inicio de la brecha
INFORMACION GENERAL SOBRE EL TRATAMIENTO AFECTADO
Duración del tratamiento
Número total de personas cuyos datos forman parte del tratamiento afectado por la brecha de datos personales
Ámbito geográfico del tratamiento
MEDIDAS DE SEGURIDAD ANTES DEL INCIDENTE
Medidas de seguridad con las que contaba el tratamiento antes de la brecha
Indicar si la brecha de datos personales pudiera haberse evitado adoptando alguna medida de seguridad adicional.
Indicar si el origen de la brecha es debido a un fallo, deficiencia o incumplimiento de alguna de las medidas de seguridad implementadas.
Indicar la disponibilidad de un análisis de riesgos o evaluación de impacto en protección de datos documentario que justifique las medidas adoptadas
INTENCIONALIDAD Y ORIGEN
Intencionalidad
Origen del incidente
TIPOLOGIA
Tipología (Confidencialidad, integridad y disponibilidad)
CATEGORIAS DE DATOS Y PERFIL DE LOS AFECTADOS
Categorías de datos
Perfiles de las personas físicas afectadas
CONSECUENCIAS Y VALORACIÓN DEL INCIDENTE
COMUNICACIÓN A LAS PERSONAS AFECTADAS
Comunicación a las personas afectadas
Fechas de comunicación
Notificación de la no comunicación
ACCIONES TOMADAS

Extracto del Registro de Incidentes

3.5.Notificación a la Autoridad de Control

- Responsable de realizar la notificación y plazos

Tan pronto como el responsable del tratamiento-*Ayuntamiento*- tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, el responsable debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas. Si dicha notificación no es posible en el plazo de 72 horas, debe acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse información por fases sin más dilación indebida.

Si en el momento de la notificación no fuese posible por parte del Ayuntamiento cumplir con la obligación de facilitar toda la información necesaria, se realizará una notificación de tipo "inicial", antes de las 72 horas señaladas, rellenando el formulario con la información preliminar que se disponga, o en su caso las estimaciones preliminares sobre la brecha de datos personales.
Antes del plazo máximo de 30 días desde la notificación inicial, el responsable de tratamiento deberá completar toda la información mediante una "modificación" de la notificación anterior, incluida la decisión tomada sobre la comunicación de la brecha de datos personales a los afectados.

Cuando el Ayuntamiento, detecta una brecha de seguridad, respecto a los tratamientos sobre los que actúa como encargada del tratamiento, el Ayuntamiento, deberá remitir al Responsable del Tratamiento, toda la información necesaria para que pueda cumplir con sus obligaciones en tiempo y forma, de conformidad con lo establecidos en el contrato de encargado del tratamiento, Convenio u otros actos normativos en las que se regule el tratamiento de datos entre las partes.

- Contenido

El artículo 33 del RGPD establece que la notificación de brechas de datos personales a la Autoridad de Control deberá como mínimo:

- Describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y 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 del que pueda obtenerse más información.
- Describir las posibles consecuencias de la violación de la seguridad de los datos personales.
- Describir las medidas adoptadas o propuestas por el responsable del tratamiento 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.

3.6.Comunicación a las personas afectadas

Cuando sea probable que la brecha de datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el Ayuntamiento, comunicará la brecha de datos personales a los afectados sin dilación indebida –*Anexo 02 Comunicación afectados*–.
No siendo necesario comunicar la brecha de seguridad, en los siguientes supuestos:

- El responsable ha tomado medidas técnicas y organizativas adecuadas que evitan los riesgos anteriores, minimizan los daños a los derechos y libertades y/o los hacen reversibles.
- El responsable ha tomado con posterioridad a la brecha 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 para sus derechos y libertades se materialice.

La comunicación a los afectados debe realizarse sin dilación indebida.

3.7. Adopción de medidas

El Ayuntamiento, como Responsable del Tratamiento, debe determinar si las medidas de seguridad disponibles antes de la brecha de datos personales eran adecuadas al nivel de riesgo.

En caso necesario debe introducir medidas de seguridad adicionales o corregir fallos o deficiencias en las medidas de seguridad adoptadas.

4. Figuras implicadas

El Ayuntamiento, en calidad de responsable del tratamiento de acuerdo con la definición el artículo 4 del Reglamento (UE) General de Protección de Datos, le corresponde la gestión de brechas de seguridad, que se produzcan en el Ayuntamiento. No obstante, detectada una brecha de datos personales en la organización, y a efectos de una correcta y eficaz gestión, será necesaria la colaboración y actuación de distintas figuras:

- Responsable del tratamiento-*Ayuntamiento*-: Le corresponde aplicar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme al RGPD.

- Delegado de protección de datos (DPD): El RGPD encomienda al DPD la función de informar y asesorar al responsable o encargado de las obligaciones que les incumben, incluidas las relativas a la gestión y notificación de las brechas de datos personales, así como cooperar con la Autoridad de Control y actuar como punto de contacto de la Autoridad de Control para cuestiones relativas al tratamiento.

  El DPD por tanto deberá informar y asesorar al responsable/encargado del tratamiento respecto de:
  - La implantación de un proceso de gestión de brechas de datos personales en la organización.
  - La evaluación del riesgo y las consecuencias que puede suponer para los derechos y libertades de las personas una brecha de datos personales.
  - Las acciones adecuadas que se deben tomar para mitigar los efectos de la brecha de datos personales sobre las personas afectadas.
  - La necesidad de notificar la brecha de datos personales a la Autoridad de Control y en su caso a los interesados afectados, en el caso de encargados de tratamiento, la necesidad de notificar la brecha de datos personales al responsable.
  - El DPD actuará como punto de contacto con la Autoridad de Control en el proceso de notificación por parte del responsable de las brechas de datos personales, así como las respuestas a los requerimientos realizados por dicha Autoridad respecto a las mismas, siempre de acuerdo con el proceso de gestión de brechas implantado en la organización.

- Áreas/Departamentos del Ayuntamiento: Las áreas/departamentos deberán prestar su colaboración cuando así se les requiera para la gestión del incidente de seguridad.

5. Actualización del documento

La actualización del presente documento corresponde al delegado de Protección de Datos del Ayuntamiento de Bolaños.

6. Anexo documentos relacionados

En el presente apartado se referencian otros documentos relacionados con la atención el presente procedimiento de gestión de brechas de seguridad en el Ayuntamiento:

- Registro de Incidentes: Anexo 01 Registro de Incidentes.
- Modelo de notificación de las violaciones de seguridad a los afectados: Anexo 02 Modelo notificación de respuesta al afectado.

Ayuntamiento de Bolaños de Calatrava
www.bolanosdecalatrava.es

REGISTRO INCIDENTES DE SEGURIDAD

INFORMACIÓN TEMPORAL DE LA BRECHA Y MEDIOS DE DETECCIÓN	
Fecha de detección	
Medios de detección de la brecha:	
Fecha de inicio de la brecha:	
INFORMACIÓN GENERAL SOBRE EL TRATAMIENTO AFECTADO	
Duración del tratamiento	
Número total de personas cuyos datos forman parte del tratamiento afectado por la brecha de datos personales	
Ámbito geográfico del tratamiento	
MEDIDAS DE SEGURIDAD ANTES DEL INCIDENTE	
Medidas de seguridad con las que contaba el tratamiento antes de la brecha	
Indicar si la brecha de datos personales pudiera haberse evitado adoptando alguna medida de seguridad adicional.	
Indicar si el origen de la brecha es debido a un fallo, deficiencia o incumplimiento de alguna de las medidas de seguridad implementadas.	
Indicar la disponibilidad de un análisis de riesgos o evaluación de impacto en protección de datos documentado que justifique las medidas adoptadas.	
INTENCIONALIDAD Y ORIGEN	
Intencionalidad	
Origen del incidente	
TIPOLOGÍA	
Tipología (Confidencialidad; integridad y disponibilidad)	
CATEGORÍAS DE DATOS Y PERFIL DE LOS AFECTADOS	
Categorías de datos	
Perfiles de las personas físicas afectadas	
CONSECUENCIAS Y VALORACIÓN DEL INCIDENTE	
COMUNICACIÓN A LAS PERSONAS AFECTADAS	
Comunicación a las personas afectadas	
Fechas de comunicación	
Justificación de la no comunicación	
ACCIONES TOMADAS	

MODELO DE NOTIFICACIÓN DE VIOLACIONES DE SEGURIDAD A LAS PERSONAS AFECTADAS

DATOS DEL RESPONSABLE

Identidad:	
Dirección postal:	
Correo electrónico:	
Persona interlocutora en materia de	

DESCRIPCIÓN DE LA VIOLACIÓN DE SEGURIDAD

Descripción general del incidente	
Fecha del incidente	
Descripción de los datos e información personal afectados.	
Resumen de las medidas implantadas hasta el momento para controlar los posibles daños.	
Otras informaciones útiles a los afectados para que puedan proteger sus datos o prevenir posibles daños	

En _____, a _____ de _____ de 202_

Alcalde del Ayuntamiento de Bolaños de Calatrava

Fdo.