



INSTRUCCIÓN

Notificación de brechas de datos personales

CÓDIGO: PD-GEN-INS-005

Versión: 3.0

Fecha: 28/09/2021

Aprobado

Juan Ángel Morejudo Flores

 Castilla-La Mancha	INSTRUCCIÓN Notificación de brechas de datos personales	DIFUSIÓN LIMITADA	
		Código	PD-GEN-INS-005
		Versión	3.0
		Fecha	28/09/2021

Nombre		Fecha
Elaborado por:	Protección de Datos	01/02/2019
Revisado por:		



HISTÓRICO DEL DOCUMENTO			
Versión	Fecha	Descripción	Autor
1.0	01/02/19	Versión inicial	PD
2.0	12/03/21	Incluir fase de petición de información de la AEPD Incluir la realización de un informe único con anexos Incluir herramienta de la AEPD para comunicación a ciudadanos	PD
3.0	28/09/2021	Adaptación a la nueva guía para la notificación de brechas de datos personales de la AEPD	PD

Documento Verificable en www.jccm.es mediante
 Código Seguro de Verificación (CSV): C6EEB8B1E8337847C544EE

 Castilla-La Mancha	INSTRUCCIÓN Notificación de brechas de datos personales	DIFUSIÓN LIMITADA	
		Código	PD-GEN-INS-005
		Versión	3.0
		Fecha	28/09/2021

ÍNDICE

1. INTRODUCCIÓN	4
1.1 OBJETO	5
1.2 ÁMBITO DE APLICACIÓN.....	5
1.3 DEFINICIONES Y ACRÓNIMOS.....	5
1.3.1 <i>Definiciones</i>	5
1.3.2 <i>Acrónimos</i>	6
NOTIFICACIÓN DE BRECHAS DE SEGURIDAD	7
2.1 DETECCIÓN Y COMUNICACIÓN INTERNA DE LA BRECHA DE DATOS PERSONALES.....	7
2.2 REGISTRO Y VALORACIÓN DE LA BRECHA.....	8
2.3 GESTIÓN DE LA BRECHA DE SEGURIDAD	10
2.4 COMUNICACIÓN A LA AEPD.....	11
2.4.1 <i>Procedimiento general</i>	12
2.4.2 <i>Excepciones al procedimiento general</i>	12
2.5 COMUNICACIÓN A LOS AFECTADOS	12
2.6 RESPUESTA DE LA AEPD A LA NOTIFICACIÓN DE UNA BRECHA.....	13
2.7 REMISIÓN DE LAS COMUNICACIONES DE LA AEPD.....	14
ANEXO I COMUNICACIÓN A EL/LA DPD	15
ANEXO II MODELO DE REGISTRO DE BRECHAS DE DATOS PERSONALES	26
ANEXO III COMUNICACIÓN A LOS INTERESADOS	27
ANEXO IV ESQUEMA NOTIFICACIÓN DE BRECHAS DE DATOS PERSONALES	30



 Castilla-La Mancha	INSTRUCCIÓN Notificación de brechas de datos personales	DIFUSIÓN LIMITADA	
		Código	PD-GEN-INS-005
		Versión	3.0
		Fecha	28/09/2021

1. INTRODUCCIÓN

El Reglamento (UE) 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 (Reglamento General de Protección de Datos) pretende establecer un marco más sólido y coherente para la protección de datos en la Unión Europea, siendo aplicable desde el 25 de mayo de 2018.

Una de las grandes novedades del RGPD es el principio de responsabilidad proactiva que implica que el responsable del tratamiento debe aplicar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento. Por tanto, el responsable debe tener una actitud proactiva en los tratamientos que lleve a cabo.

Entre las medidas de responsabilidad proactiva el RGPD ha establecido la obligación de la notificación de las violaciones de seguridad, también llamadas brechas de seguridad, que puedan suponer un riesgo para los derechos y libertades de las personas físicas, a la autoridad de control competente, que en el caso de España se trata de la Agencia Española de Protección de Datos.

El concepto de brechas de seguridad relacionadas con los datos personales no es nuevo, sino que ya existe una cultura en las organizaciones impuesta por el Reglamento de desarrollo de la Ley Orgánica 15/1999, aunque dicha normativa no contemplaba la notificación a la Autoridad de Control.

Esta obligación está establecida en los artículos 33 y 34 del RGPD:

"1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. 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.

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

.....

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida."



 Castilla-La Mancha	INSTRUCCIÓN Notificación de brechas de datos personales	DIFUSIÓN LIMITADA	
		Código	PD-GEN-INS-005
		Versión	3.0
		Fecha	28/09/2021

Por tanto, este proceso de gestión de las brechas se debe integrar dentro de la política de información de las organizaciones, completando el proceso de gestión de incidentes.

1.1 Objeto

El objeto de la presente instrucción es permitir al responsable conocer con precisión el alcance de su obligación de notificación de las brechas de seguridad y facilitar su cumplimiento en plazo, determinando las funciones y responsabilidades de cada uno de los intervinientes y estableciendo la forma de actuar ante una brecha de datos personales en los tratamientos.

1.2 Ámbito de aplicación

Esta instrucción es de obligado cumplimiento en:

- a) La Administración regional
- b) Los organismos autónomos adscritos a la Administración regional, a excepción del Organismo Autónomo SESCOG que quedará sujeto a aquello que específicamente se refiera al mismo.
- c) El resto de entidades de Derecho Público vinculadas o dependientes, cuando ejerzan potestades administrativas.

1.3 Definiciones y acrónimos

1.3.1 Definiciones

Definición	Concepto
Incidente de seguridad	Un incidente de seguridad de la información se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información.
Ciberincidente	Un incidente de seguridad de la información se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información, cuando esta esté en soporte electrónico.
Violación de seguridad	Aunque el vocablo "violación" es el utilizado en la traducción al castellano del RGPD el término que se utiliza en la guía de la AEPD es el de "brechas de datos personales" que señala con carácter general a los incidentes que pueden afectar o afectan a la seguridad de la información y los datos personales



 Castilla-La Mancha	INSTRUCCIÓN Notificación de brechas de datos personales	DIFUSIÓN LIMITADA	
		Código	PD-GEN-INS-005
		Versión	3.0
		Fecha	28/09/2021

1.3.2 Acrónimos

Acrónimo	Concepto
AEPD	Agencia Española de Protección de Datos
CRPD	Comité Regional de Protección de Datos
DPD	Delegada/Delegado de Protección de Datos
RGPD	Reglamento General de Protección de Datos
SESCAM	Servicio de Salud de Castilla-La Mancha



Documento Verificable en www.jccm.es mediante
Código Seguro de Verificación (CSV): C6EEB8B1E8337847C544EE

 Castilla-La Mancha	INSTRUCCIÓN Notificación de brechas de datos personales	DIFUSIÓN LIMITADA	
		Código	PD-GEN-INS-005
		Versión	3.0
		Fecha	28/09/2021

2. NOTIFICACIÓN DE BRECHAS DE SEGURIDAD

El RGPD entiende por violaciones de seguridad de los datos de carácter personal como “todas aquellas violaciones 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”.

No tendrán consideración de brecha de datos personales sujetas a los artículos 33 y 34 del RGPD aquellos incidentes que:

- No afecten a datos de carácter personal
- No afecten a tratamientos de datos personales llevados a cabo por un responsable
- Ocurran en tratamientos llevados a cabo por una persona física en el ámbito doméstico

Las violaciones de seguridad pueden clasificarse, dependiendo de las dimensiones de seguridad a las que afecte, en:

- Violación de la confidencialidad: cuando se produce una revelación no autorizada o accidental de los datos personales, o el acceso a los mismos.
- Violación de la integridad: cuando se produce una alteración no autorizada o accidental de los datos personales.
- Violación de la disponibilidad: cuando se produce una pérdida de acceso accidental o no autorizada a los datos personales.

Cabe señalar que, dependiendo de las circunstancias, una violación puede afectar a más de una de las dimensiones de seguridad citadas.

2.1 Detección y comunicación interna de la brecha de datos personales

En cumplimiento de la normativa de protección de datos, según cómo y quién detecte la brecha de seguridad, se pueden dar los siguientes supuestos:

- Si se trata de un ciberincidente que afecte a datos personales detectado por un usuario con acceso a datos, el usuario debe notificarlo con la mayor brevedad posible a la Unidad de Protección de Datos, correo protecciondatos@jccm.es o a través del Servicio Integral de Gestión para Usuarios y Empleados: <https://sigue.jccm.es>.
- Si se trata de un ciberincidente que afecte a datos personales, descubierto mediante mecanismos de detección, como sistemas de alerta, antivirus, correlación de log, consumo inusual de recursos (red, cpu,) etc., el órgano con funciones de gestión de



 Castilla-La Mancha	INSTRUCCIÓN Notificación de brechas de datos personales	DIFUSIÓN LIMITADA	
		Código	PD-GEN-INS-005
		Versión	3.0
		Fecha	28/09/2021

ciberincidentes deberá comunicarlo a la mayor brevedad posible a la Unidad de Protección de Datos, , correo protecciondatos@jccm.es o a través del Servicio Integral de Gestión para Usuarios y Empleados: <https://sigue.jccm.es>.

- Si se trata de un incidente detectado por el encargado del tratamiento, actuará siguiendo lo establecido en el documento que regula su relación de encargado.
- Si se trata de un incidente que afecte a datos personales en soporte no automatizado, el usuario que lo detecte informará a la mayor brevedad posible a la Unidad de Protección de Datos, correo protecciondatos@jccm.es o a través del Servicio Integral de Gestión para Usuarios y Empleados: <https://sigue.jccm.es>.

La Unidad de Protección de Datos responderá confirmando la recepción del correo y remitirá la brecha de seguridad a los vocales del CRPD correspondientes.

2.2 Registro y valoración de la brecha

El responsable del tratamiento debe elaborar y mantener un registro de brechas de seguridad cuando estas afecten a datos personales. La inscripción en este registro se debe realizar con independencia de que la brecha sea notificada a la AEPD y/o a los afectados o no.

El contenido del registro de brechas de datos personales de cada Responsable del tratamiento contará, al menos, con la siguiente información:

- Código de la brecha
- Descripción breve de la brecha
- Información temporal de la brecha (fecha de detección, medios de detección, justificación de notificación tardía, fecha de inicio de la brecha, estado de resolución)
- Sobre la brecha:
 - a. Resumen del incidente.
 - b. Tipología (confidencialidad, integridad o disponibilidad).
 - c. Medio por el que se materializó la brecha.
 - d. Contexto.
 - e. Medidas preventivas aplicadas antes de la brecha.
- Sobre los datos afectados:
 - a. Categoría de los datos.
 - b. Categorías especiales de datos.
 - c. Número aproximado de registros de datos afectados.



 Castilla-La Mancha	INSTRUCCIÓN Notificación de brechas de datos personales	DIFUSIÓN LIMITADA	
		Código	PD-GEN-INS-005
		Versión	3.0
		Fecha	28/09/2021

- Sobre los sujetos afectados (perfil).
- Posibles consecuencias:
 - a. En brecha de confidencialidad.
 - b. En brecha de integridad.
 - c. En brecha de disponibilidad.
 - d. Naturaleza del impacto potencial sobre los sujetos.
 - e. Severidad de las consecuencias para los individuos.
 - f. Medidas tomadas para solucionar la brecha y minimizar el impacto con los afectados.
- Comunicación a la AEPD (fecha de la comunicación)
- Comunicación a los interesados (si se comunica: fecha, número de sujetos informados, medio utilizado, justificación para no informar y copia de la misma)

En anexo II se incluye un modelo de registro de brechas de datos personales

En un primer momento se cumplimentará toda aquella información que se conozca cuando se detecte la brecha, para posteriormente, durante su resolución documentar el proceso con toda la información que se vaya recopilando.

Valoración de la brecha:

El nivel de riesgo para los derechos y libertades de las personas físicas afectadas por la brecha es el aspecto principal a tener en cuenta para notificar una brecha a la AEPD y/o comunicarla a los afectados.

Los factores que se pueden utilizar para evaluar el riesgo en una brecha de datos personales son los siguientes:

- Tipo de brecha de datos personales
- Naturaleza, carácter sensible y el volumen de datos personales
- Facilidad de identificación de las personas
- Gravedad de las consecuencias para los derechos y libertades de las personas
- Características particulares del responsable de tratamiento
- Número de personas afectadas
- Consideraciones generales

Si tras la valoración se concluye que la brecha no entraña riesgo para los derechos y libertades de los afectados no será precisa la comunicación a la AEPD. En todo caso deberá documentarse esta tarea de valoración.



 Castilla-La Mancha	INSTRUCCIÓN Notificación de brechas de datos personales	DIFUSIÓN LIMITADA	
		Código	PD-GEN-INS-005
		Versión	3.0
		Fecha	28/09/2021

En los casos en que se concluya que la brecha entraña un alto riesgo para los derechos y las libertades de los titulares de los datos deberá procederse a la comunicación de la brecha a los afectados. En esta valoración debe tenerse en cuenta no la probabilidad de que se materialice la brecha sino la probabilidad de que tenga consecuencias para los interesados y el impacto que tendrían estas consecuencias.

Probabilidad	Muy alta	Obligación Comunicar Afectados			
	Alta				
	Baja	Valorar Comunicar afectados			
	Improbable ³⁴				
		Baja - Muy limitada	Media - Limitado	Alta - Significativo	Muy alta - Muy significativo
Severidad (Gravedad del impacto)					

(Tabla extraída de la Guía de la AEPD para la notificación de brechas de datos personales)

Para esta tarea el responsable del tratamiento contará con el asesoramiento del /la DPD, que utilizará para ese fin la herramienta creada al efecto por la AEPD.

2.3 Gestión de la brecha de seguridad

Dependiendo de las características de brecha de seguridad en los datos personales, se gestionará por:

- Los órganos con funciones de gestión de ciberincidentes.
- Los encargados de tratamiento, si así se recoge en los documentos donde se establece la relación responsable/encargado.
- Los responsables de los tratamientos.

La gestión de las brechas de seguridad deberá estar formalizada en un procedimiento interno. Este procedimiento podría tener en cuenta las siguientes medidas del artículo 32 del RGPD para gestionar el riesgo:

- Medidas orientadas a garantizar la confidencialidad, integridad y disponibilidad
- Medidas para garantizar la resiliencia de los sistemas y servicios de tratamientos, y para dotar de capacidad de restaurar la disponibilidad y el acceso a los datos personales de



 Castilla-La Mancha	INSTRUCCIÓN Notificación de brechas de datos personales	DIFUSIÓN LIMITADA	
		Código	PD-GEN-INS-005
		Versión	3.0
		Fecha	28/09/2021

forma rápida en caso de incidente físico o técnico

- La seudonimización y el cifrado de datos personales
- Los procesos de verificación, evaluación y valoración regulares de las medidas de seguridad

Además, se debe contemplar la gestión de los posibles errores, debilidades, vulnerabilidades o ataques que se pudieran derivar de las distintas medidas técnicas y organizativas que complementan estrategias de protección de datos por defecto, desde el diseño u otras garantías (los sistemas de garantías).



2.4 Comunicación a la AEPD

Si tras la valoración de la brecha se concluye que entraña riesgo a los derechos y libertades de los afectados, el responsable, a través del/la DPD, debe proceder a la notificación de la misma a la AEPD en un plazo no superior a las 72 horas a calcular desde que responsable es consciente de que el incidente de seguridad ha afectado a datos de carácter personal.

El/la 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, siempre de acuerdo con el procedimiento interno de gestión de brechas que deben tener aprobados los distintos órganos.

La comunicación de la brecha de seguridad se puede realizar de forma:

- Completa, cuando se conoce toda la información de la brecha. En cuyo caso debe estar relleno el campo de fecha de finalización en el formulario del Anexo I.
- Inicial, en caso de que en las primeras 72 horas no se tenga toda la información necesaria. Este tipo de comunicación se completa con más notificaciones parciales, si fuese necesario, y en todo caso siempre con la notificación final de la fecha de cierre de la brecha en el campo correspondiente del Anexo I. El plazo máximo de cierre de la brecha será no superior a 30 días desde la notificación inicial de la misma.

La comunicación de la brecha por parte del responsable al/la DPD deberá incluir, al menos, la siguiente documentación:

- Informe cronológico del incidente realizado por el responsable del tratamiento, junto con documentos que le den soporte.

 Castilla-La Mancha	INSTRUCCIÓN Notificación de brechas de datos personales	DIFUSIÓN LIMITADA	
		Código	PD-GEN-INS-005
		Versión	3.0
		Fecha	28/09/2021

- Anexo I "Formulario de notificación de brechas"
- Anexo II "Modelo de comunicación a los interesados" (si fuera necesario)

2.4.1 Procedimiento general

El Vocal del CRPD correspondiente notificará al/la DPD la documentación necesaria en tiempo y forma, esto es, con la antelación suficiente a las 72 horas siguientes en que la organización tenga conocimiento de que se ha producido dicha brecha, ya que antes del cumplimiento del plazo de 72 horas, se deberá haber realizado la notificación a la AEPD.

El vocal del CRPD deberá comunicarlo a través de la cuenta electrónica protecciondatos@jccm.es

El/la DPD, antes de notificar a la AEPD, deberá comprobar la correcta cumplimentación de los formularios y, en caso de duda, se pondrá en contacto con el responsable para cualquier aclaración e informará de ello al vocal del CRPD.

El/la DPD notificará la brecha de seguridad, a través de la vía "Sede Electrónica", a la Agencia Española de Protección de Datos, en un plazo máximo de 72 horas, contadas desde el momento en que el responsable tiene conocimiento de que se ha producido la brecha.

Una vez realizada la notificación a la AEPD, el/la DPD enviará al vocal el justificante de la notificación.

2.4.2 Excepciones al procedimiento general

En el caso de producirse brechas de seguridad de los datos personales contenidos en tratamientos de Radio Televisión Castilla-La Mancha, la notificación a la autoridad de control se realizará siguiendo el correspondiente procedimiento interno, debiendo enviar copia de la comunicación a la AEPD a la Unidad de Protección de Datos a través de la cuenta electrónica protecciondatos@jccm.es.

2.5 Comunicación a los afectados

La decisión de comunicar la brecha a los afectados podría derivar de diferentes supuestos:

1. Comunicación como consecuencia de la valoración de la necesidad por parte del responsable:

Si tras la valoración de la brecha se concluye que puede entrañar un alto riesgo para los



 Castilla-La Mancha	INSTRUCCIÓN Notificación de brechas de datos personales	DIFUSIÓN LIMITADA	
		Código	PD-GEN-INS-005
		Versión	3.0
		Fecha	28/09/2021

derechos y libertades de los titulares de los datos, el responsable del tratamiento deberá comunicar a los afectados la brecha, a la mayor brevedad posible (cualquier tardanza le resta efectividad, por lo que cualquier retraso debe justificarse por parte del responsable).

2. Comunicación como consecuencia de una orden de la AEPD.

Cuando la comunicación a las personas afectadas se produzca como consecuencia de una orden emitida por la Agencia Española de Protección de Datos, deberá materializarse la comunicación a los afectados sin dilación indebida y comunicar a la Agencia la confirmación de haber ejecutado la orden dentro del plazo de 30 días, salvo que se indique un plazo diferente en la orden.

En cualquier caso, el responsable del tratamiento guardará evidencia de la comunicación al interesado o los motivos de la imposibilidad de hacerlo.

Forma de realizar la comunicación

La comunicación a las personas afectadas se realizará de manera directa a cada uno de los afectados, en un lenguaje claro y sencillo.

Cuando la comunicación a los afectados suponga un esfuerzo desproporcionado con relación a los riesgos para los derechos y libertades que están sufriendo los interesados, se podrá realizar una comunicación indirecta a través de avisos públicos, como sitios web, tablón de anuncios, comunicados de prensa, etc...

En el Anexo III existe un modelo de comunicación a los afectados.

2.6 Respuesta de la AEPD a la notificación de una brecha

El responsable de tratamiento, tras notificar una brecha de datos personales, puede recibir por parte de la AEPD diversas comunicaciones o notificaciones electrónicas:

- Comunicación con información relativa al registro de la brecha de datos personales notificada
- Notificación con un requerimiento de información adicional sobre la brecha de datos personales o el tratamiento de datos personales. En el caso que se reciba este requerimiento se deberá atender en el plazo indicado siguiendo el procedimiento establecido para la remisión de la respuesta a la AEPD.
- Notificación con una orden para comunicar a los afectados la brecha de datos personales. Esta comunicación se deberá ejecutar en el plazo máximo indicado en la



 Castilla-La Mancha	INSTRUCCIÓN Notificación de brechas de datos personales	DIFUSIÓN LIMITADA	
		Código	PD-GEN-INS-005
		Versión	3.0
		Fecha	28/09/2021

misma y deberá notificarse a la AEPD su cumplimiento.

La confirmación del cumplimiento de la orden a la AEPD deberá incluir los siguientes detalles:

- Contenido de la comunicación a los afectados.
- Fecha o periodo en el que se ha ejecutado la comunicación.
- Número de sujetos comunicados.
- Medio utilizado para comunicar a los afectados.
- Justificación para optar por una comunicación pública de las establecidas en el art. 34.3.c) del RGPD en su caso.

El responsable, remitirá la información al/la DPD, siempre a través del vocal del CRPD, para que, a su vez, lo notifique a la AEPD por vía "Sede Electrónica".

2.7 Remisión de las comunicaciones de la AEPD

Las Comunicaciones que el DPD del Organismo Autónomo SESCOAM realice y reciba de la AEPD en el ejercicio de sus funciones deberán ser comunicadas simultáneamente a la Unidad de Protección de Datos de la Dirección General de Administración Digital al correo: protecciondatos@jccm.es o a través del Servicio Integral de Gestión para Usuarios y Empleados: <https://sigue.jccm.es>.



 Castilla-La Mancha	INSTRUCCIÓN Notificación de brechas de datos personales	DIFUSIÓN LIMITADA	
		Código	PD-GEN-INS-005
		Versión	3.0
		Fecha	28/09/2021

ANEXO I COMUNICACIÓN A EL/LA DPD



**FORMULARIO DE NOTIFICACIÓN BRECHAS DE DATOS PERSONALES A LA
 AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS**
 (Versión 3.0)



1.- Responsable del tratamiento			
Dirección: General, Secretaría General, Delegación Provincial, ...			
Dirección:			
Provincia:		C.P.:	
Localidad:		País:	
Teléfono(s):		e-mail:	

2.- Identificación del encargado <small>(RELLENAR EN LOS CASOS QUE UNA EMPRESA O ENTIDAD REALICE TODO O UNA PARTE DEL TRATAMIENTO EN NUESTRO NOMBRE)</small>			
¿Hay otra organización implicada en la brecha de seguridad?:			<input type="checkbox"/>
Ámbito de la Organización:	<input type="checkbox"/> Público <input type="checkbox"/> Privado		
Nombre de la Organización:			
CIF:			
Dirección:		C.P.:	
Provincia:		Localidad:	
Teléfono(s):		e-mail:	

3.- Datos de la notificación	
<input type="radio"/> Notificar una nueva brecha de datos <input type="radio"/> Modificar una notificación hecha con anterioridad para	
En su caso, datos de la notificación que se modifica:	
Registro de entrada:	
Fecha:	

 Castilla-La Mancha	INSTRUCCIÓN Notificación de brechas de datos personales	DIFUSIÓN LIMITADA	
		Código	PD-GEN-INS-005
		Versión	3.0
		Fecha	28/09/2021



**FORMULARIO DE NOTIFICACIÓN BRECHAS DE DATOS PERSONALES A LA
 AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS**
 (Versión 3.0)



Documento Verificable en www.jccm.es mediante
 Código Seguro de Verificación (CSV): C6EEB8B1E8337847C544EE

4.- Sobre el tratamiento	
4.1.- ¿Desde cuándo se viene realizando el tratamiento de datos afectado?	
<input type="radio"/> Tratamiento puntual o muy limitado <input type="radio"/> Entre 1 y 5 años	<input type="radio"/> Menos de 1 año <input type="radio"/> Más de 5 años
Número aproximado de personas físicas sobre las que se recoge, almacena o trata datos personales de otra forma, referido exclusivamente al tratamiento sobre el que se ha producido la brecha de datos personales.	
4.2.- El tratamiento sobre el que se ha producido la brecha incluye datos de personas:	
<input type="radio"/> Únicamente en España. nivel <input type="radio"/> Únicamente en España. nivel <input type="radio"/> Únicamente en España. nivel <input type="radio"/> A nivel	<input type="radio"/> En un único Estado miembro, pero no en <input type="radio"/> En más de un Estado <input type="radio"/> En más de un Estado miembro y a

5.- Sobre la brecha y sus consecuencias	
5.1.- El incidente ha sido:	
<input type="radio"/> Accidental o sin <input type="radio"/> Intencionalidad <input type="radio"/> Intencionado, para dañar al responsable, al encargado o a	
5.2.- El origen del incidente ha sido:	
<input type="radio"/> Interno: Personal o sistemas bajo el control del responsable de tratamiento <input type="radio"/> Externo: Otros, ajenos al responsable y	<input type="radio"/> Interno: Personal o sistemas bajo el control del encargado de tratamiento
5.2.- ¿Cómo ha ocurrido la brecha? Puede seleccionar varias opciones:	

 Castilla-La Mancha	INSTRUCCIÓN Notificación de brechas de datos personales	DIFUSIÓN LIMITADA	
		Código	PD-GEN-INS-005
		Versión	3.0
		Fecha	28/09/2021



**FORMULARIO DE NOTIFICACIÓN BRECHAS DE DATOS PERSONALES A LA
 AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS**
 (Versión 3.0)



Documento Verificable en www.jccm.es mediante
 Código Seguro de Verificación (CSV): C6EEB8B1E8337847C544EE

<input type="checkbox"/> Revelación verbal no autorizada
<input type="checkbox"/> Documentación perdida, robada o depositada en localización insegura
<input type="checkbox"/> Correo postal perdido o abierto
<input type="checkbox"/> Eliminación incorrecta de datos personales en formato papel
<input type="checkbox"/> Datos personales enviados por error (postal o electrónicamente)
<input type="checkbox"/> Datos personales eliminados/destruidos
<input type="checkbox"/> Abuso de privilegios de acceso por parte de empleado para extraer, reenviar o copiar datos personales.
<input type="checkbox"/> Datos personales residuales en dispositivos obsoletos
<input type="checkbox"/> Publicación no intencionada/autorizada
<input type="checkbox"/> Envío de email a múltiples destinatarios sin copia oculta/Lista distribución
<input type="checkbox"/> Dispositivo perdido o robado
<input type="checkbox"/> Ciberincidente: dispositivo cifrado/secuestro de información
<input type="checkbox"/> Ciberincidente: PHISHING/compromiso de cuenta de usuario
<input type="checkbox"/> Ciberincidente: acceso no autorizado a datos en sistema TI
<input type="checkbox"/> Incidencia técnica
<input type="checkbox"/> Modificación no autorizada de datos
<input type="checkbox"/> Datos personales mostrados al individuo incorrecto
Como consecuencia del incidente se ha visto afectada la:
<input type="checkbox"/> Confidencialidad: Personas u organizaciones que no están autorizadas, o no tienen el propósito legítimo para acceder a los datos, han podido acceder y/o extraerlos
<input type="checkbox"/> Disponibilidad: se ha destruido, perdido o cifrado los datos personales de forma que no pueden ser tratados
<input type="checkbox"/> Integridad: se han alterado los datos personales, siguen siendo accesibles, pero la sustitución de datos puede suponer un daño para las personas afectadas.
Solo en caso de brecha de confidencialidad. ¿Están los datos cifrados de forma segura, anonimizados o protegidos de forma que son ininteligibles para quien haya podido tener acceso, o no se puede identificar a las personas?
<input type="radio"/> Sí <input type="radio"/> No <input type="radio"/> Desconocido

 Castilla-La Mancha	INSTRUCCIÓN Notificación de brechas de datos personales	DIFUSIÓN LIMITADA	
		Código	PD-GEN-INS-005
		Versión	3.0
		Fecha	28/09/2021



**FORMULARIO DE NOTIFICACIÓN BRECHAS DE DATOS PERSONALES A LA
 AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS**
 (Versión 3.0)

Solo en caso de brecha de disponibilidad. ¿Se ha recuperado la disponibilidad de los datos personales de forma que pueden ser tratados con normalidad?		
<input type="radio"/> Sí <input type="radio"/> No <input type="radio"/> Todavía no, pero se recuperará en breve		
Solo en caso de brecha de integridad. Seleccione la opción más apropiada		
<input type="radio"/> Datos alterados, pero sin constancia de uso ilegal <input type="radio"/> Datos alterados y usados de forma ilegal o <input type="radio"/> Datos alterados y usados de forma ilegal o incorrecta.		
¿Cuáles podrían ser las consecuencias sobre las personas físicas?		
<input type="checkbox"/> Imposibilidad de ejercer algún derecho	<input type="checkbox"/> Imposibilidad para acceder a un servicio	<input type="checkbox"/> Usurpación de identidad
<input type="checkbox"/> Ser víctima de campañas de PHISHING/SPAMMING	<input type="checkbox"/> Pérdidas financieras	<input type="checkbox"/> Daños reputacionales
<input type="checkbox"/> Pérdida de confidencialidad de datos afectados por secreto profesional	<input type="checkbox"/> Daños psicológicos o físicos	<input type="checkbox"/> Pérdida de control sobre sus datos personales
<input type="checkbox"/> Otras consecuencias	<input type="checkbox"/> Aún desconocido	
¿En qué grado podrían afectar las consecuencias identificadas a las personas físicas?		
<input type="checkbox"/> 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		
<input type="checkbox"/> 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		
<input type="checkbox"/> 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.)		
<input type="checkbox"/> 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.)		
<input type="checkbox"/> Aún desconocido		
A fecha de esta notificación, ¿tiene constancia de que se haya materializado alguna de las consecuencias identificadas, con el grado indicado en la cuestión anterior?		



 Castilla-La Mancha	INSTRUCCIÓN Notificación de brechas de datos personales	DIFUSIÓN LIMITADA	
		Código	PD-GEN-INS-005
		Versión	3.0
		Fecha	28/09/2021



**FORMULARIO DE NOTIFICACIÓN BRECHAS DE DATOS PERSONALES A LA
 AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS**
 (Versión 3.0)

<input type="radio"/> Sí	<input type="radio"/> No	
Si aún no sea materializado ¿cómo valora la probabilidad de que se materialice sobre las personas afectadas?		
<input type="radio"/> Improbable	<input type="radio"/> Baja	<input type="radio"/> Alta
<input type="radio"/> Muy alta	<input type="radio"/> Desconocida	
RESUMEN DE LA BRECHA. BREVE DESCRIPCIÓN DE LO OCURRIDO Y LAS MEDIDAS CONCRETAS TOMADAS PARA MINIMIZAR EL DAÑO SOBRE LAS PERSONAS. EVITE INCLUIR DATOS PERSONALES Y FÓRMULAS DEL TIPO "Ver anexo". EN NINGÚN CASO LO AQUÍ ESCRITO PODRÁ SUPONER UNA MODIFICACIÓN SOBRE LO CONSIGNADO EN EL RESTO DEL FORMULARIO.		
<div style="border: 1px solid black; width: 100%; height: 100%;"></div>		

6.- Tipos de datos afectados		
Selecciones los tipos de datos que se han visto afectados, exclusivamente de personas físicas, marque todas las opciones aplicables:		
<input type="checkbox"/> Biométricos	<input type="checkbox"/> Datos básicos (Ej.: Nombre, Apellidos, fecha nacimiento)	<input type="checkbox"/> Sobre religión o creencia
<input type="checkbox"/> Imagen (Fotos/Vídeo)	<input type="checkbox"/> DNI, NIE, Pasaporte o cualquier documento identificativo	<input type="checkbox"/> Sobre condenas e infracciones penales
<input type="checkbox"/> Sobre afiliación sindical	<input type="checkbox"/> Datos económicos o financieros (sin medios de pago)	<input type="checkbox"/> Datos de medios de pago (Tarjeta bancaria, etc.)
<input type="checkbox"/> Sobre la vida sexual	<input type="checkbox"/> Datos de localización / geolocalización	<input type="checkbox"/> Datos de contacto
<input type="checkbox"/> Sobre origen racial o étnico	<input type="checkbox"/> Datos de perfiles (Ej.: en red social, solvencia, psicológico, etc.)	<input type="checkbox"/> Datos de salud (únicamente de empleados, los imprescindibles para relación laboral)
<input type="checkbox"/> Datos de salud (otros datos de salud)	<input type="checkbox"/> Sobre opinión política	<input type="checkbox"/> Genéticos



 Castilla-La Mancha	INSTRUCCIÓN Notificación de brechas de datos personales	DIFUSIÓN LIMITADA	
		Código	PD-GEN-INS-005
		Versión	3.0
		Fecha	28/09/2021



FORMULARIO DE NOTIFICACIÓN BRECHAS DE DATOS PERSONALES A LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

(Versión 3.0)

Credenciales de acceso o identificación (usuario y/o contraseña)

7.- Perfil de las personas afectadas (REFERIDO EXCLUSIVAMENTE A PERSONAS FÍSICAS. EN TÉRMINOS DE AFECTADOS NO COMPUTAN COMO TAL AQUELLOS QUE SEAN PERSONAS JURÍDICAS, YA SEAN CLIENTES, PROVEEDORES O CUALQUIER RELACIÓN QUE PUEDA MANTENER EL RESPONSABLE CON ELLOS)

Entre las personas afectadas, ¿hay menores?

Sí No Desconocido

Entre las personas afectadas, ¿hay miembro de colectivos vulnerables como supervivientes de violencia de género o en riesgo de exclusión social?

Sí No Desconocido

Las personas afectadas tienen los siguientes perfiles:

<input type="checkbox"/> Clientes/ciudadanos	<input type="checkbox"/> Usuarios	<input type="checkbox"/> Pacientes
<input type="checkbox"/> Suscriptores/potenciales clientes	<input type="checkbox"/> Estudiantes/alumnos	<input type="checkbox"/> Militares/policias
<input type="checkbox"/> Afiliados/asociados	<input type="checkbox"/> Empleados	<input type="checkbox"/> Otros:

En total, ¿Cuántas personas han visto sus datos afectados por la brecha? (Si desconoce el número exacto, indique un valor aproximado)(Indique una cifra superior a cero):

8.- Implicaciones transfronterizas

¿Hay personas afectadas por la brecha en otros Estados miembro de la Unión Europea?

Sí No Desconocido

En su caso, indique los estados en los que haya personas afectadas (A), el número de afectados por Estado y aquellos Estados en los que haya notificado (N) a otra autoridad de control

Estado	(A)	(N)	Número afectados	Estado	(A)	(N)	Número afectados

Documento Verificable en www.jccm.es mediante Código Seguro de Verificación (CSV): C6EEB8B1E8337847C544EE

 Castilla-La Mancha	INSTRUCCIÓN Notificación de brechas de datos personales	DIFUSIÓN LIMITADA	
		Código	PD-GEN-INS-005
		Versión	3.0
		Fecha	28/09/2021



FORMULARIO DE NOTIFICACIÓN BRECHAS DE DATOS PERSONALES A LA
AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

(Versión 3.0)

Alemania	<input type="checkbox"/>	<input type="checkbox"/>		Italia	<input type="checkbox"/>	<input type="checkbox"/>	
Bulgaria	<input type="checkbox"/>	<input type="checkbox"/>		Luxemburgo	<input type="checkbox"/>	<input type="checkbox"/>	
Dinamarca	<input type="checkbox"/>	<input type="checkbox"/>		Polonia	<input type="checkbox"/>	<input type="checkbox"/>	
Eslovenia	<input type="checkbox"/>	<input type="checkbox"/>		Rumanía	<input type="checkbox"/>	<input type="checkbox"/>	
Irlanda	<input type="checkbox"/>	<input type="checkbox"/>		Bélgica	<input type="checkbox"/>	<input type="checkbox"/>	
Lituania	<input type="checkbox"/>	<input type="checkbox"/>		Croacia	<input type="checkbox"/>	<input type="checkbox"/>	
Países Bajos	<input type="checkbox"/>	<input type="checkbox"/>		Eslovaquia	<input type="checkbox"/>	<input type="checkbox"/>	
República Checa	<input type="checkbox"/>	<input type="checkbox"/>		Finlandia	<input type="checkbox"/>	<input type="checkbox"/>	
Austria	<input type="checkbox"/>	<input type="checkbox"/>		Hungría	<input type="checkbox"/>	<input type="checkbox"/>	
Cipre	<input type="checkbox"/>	<input type="checkbox"/>		Letonia	<input type="checkbox"/>	<input type="checkbox"/>	
Francia	<input type="checkbox"/>	<input type="checkbox"/>		Malta	<input type="checkbox"/>	<input type="checkbox"/>	
Estonia	<input type="checkbox"/>	<input type="checkbox"/>		Portugal	<input type="checkbox"/>	<input type="checkbox"/>	
Grecia	<input type="checkbox"/>	<input type="checkbox"/>		Suecia	<input type="checkbox"/>	<input type="checkbox"/>	

9.- Información temporal de la brecha

Indique la fecha de detección de la brecha, entendida como la fecha en la que el responsable tiene constancia de que se han visto afectados datos personales

¿Conoce la fecha en la que se inició la brecha? En su caso, indique la fecha

- La fecha exacta
 Aproximada/Esti
 Desconocida

Justificación de notificación tardía (solo cumplimentar en el caso de notificación pasadas 72h desde la detección):

Plazo de 72 horas expirado fuera de la jornada laboral, fin de semana o

Problemas en medios

Inicialmente no se consideró susceptible de

Demora en el procedimiento de

No interferir en una investigación policial o



 Castilla-La Mancha	INSTRUCCIÓN Notificación de brechas de datos personales	DIFUSIÓN LIMITADA	
		Código	PD-GEN-INS-005
		Versión	3.0
		Fecha	28/09/2021



**FORMULARIO DE NOTIFICACIÓN BRECHAS DE DATOS PERSONALES A LA
 AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS**
 (Versión 3.0)



Documento Verificable en www.jccm.es mediante
 Código Seguro de Verificación (CSV): C6EEB8B1E8337847C544EE

La brecha se ha detectado mediante:
<input type="radio"/> Medios de detección propios del
<input type="radio"/> A través de la comunicación de
<input type="radio"/> Medios de comunicación: Se considera este caso cuando el responsable tiene constancia de la brecha mediante la comunicación recibida por una investigación de seguridad, un CERT, ...
<input type="radio"/> Detectado por un empleado del
<input type="radio"/> Tercero ajeno al tratamiento: Se considera en este caso cuando se tiene constancia de la brecha mediante la comunicación recibida por una investigación de seguridad, un CERT, ...
<input type="radio"/> Otros

10.- Medidas de seguridad antes de la brecha		
Marque las medidas de seguridad implementadas en la organización antes del suceso de la brecha (DEBERÁ PODER ACREDITAR LAS MEDIDAS MARCADAS ANTE UN EVENTUAL REQUERIMIENTO O DE LA AUTORIDAD DE CONTROL):		
<input type="checkbox"/> Políticas de protección de datos y seguridad <input type="checkbox"/> Registro de incidentes <input type="checkbox"/> Control de acceso lógico <input type="checkbox"/> Copias de seguridad / Plan de recuperación	<input type="checkbox"/> Formación en protección de datos y seguridad al nivel adecuado <input type="checkbox"/> Auditorías periódicas <input type="checkbox"/> Diferentes niveles de acceso a los datos <input type="checkbox"/> Automatización	<input type="checkbox"/> Sistemas informáticos actualizados <input type="checkbox"/> Control de acceso físico <input type="checkbox"/> Cifrado de datos <input type="checkbox"/> Ninguna de las anteriores
¿La brecha podría haberse evitado adoptando alguna medida de seguridad adicional?		
<input type="radio"/> Sí	<input type="radio"/> No	<input type="radio"/> Desconocido
¿El origen de la brecha es debido a un fallo, deficiencia o incumplimiento de alguna de las medidas de seguridad implementadas?		
<input type="radio"/> Sí	<input type="radio"/> No	<input type="radio"/> Desconocido
¿Existe un análisis de riesgos o evaluación de impacto en protección de datos documentado que justifique las medidas adoptadas?		
<input type="radio"/> Sí	<input type="radio"/> No	

 Castilla-La Mancha	INSTRUCCIÓN Notificación de brechas de datos personales	DIFUSIÓN LIMITADA	
		Código	PD-GEN-INS-005
		Versión	3.0
		Fecha	28/09/2021



**FORMULARIO DE NOTIFICACIÓN BRECHAS DE DATOS PERSONALES A LA
 AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS**
 (Versión 3.0)



Documento Verificable en www.jccm.es mediante
 Código Seguro de Verificación (CSV): C6EEB8B1E8337847C544EE

11.- Acciones tomadas tras el incidente			
¿Ha actualizado el registro de incidentes con los detalles relativos a la brecha de datos personales?			
<input type="radio"/> Sí <input type="radio"/> No <input type="radio"/> Desconocido			
¿Han adoptado tras el incidente nuevas medidas de seguridad que podrían haber evitado la brecha?			
<input type="radio"/> Sí <input type="radio"/> No <input type="radio"/> Desconocido			
¿Han establecido mejoras en los procedimientos y políticas de seguridad tras la brecha?			
<input type="radio"/> Sí <input type="radio"/> No <input type="radio"/> Desconocido			
En su caso, marque exclusivamente las nuevas medidas de seguridad o las que se hayan actualizado			
<input type="checkbox"/> Políticas de protección de datos y seguridad <input type="checkbox"/> Sistemas Informáticos actualizados <input type="checkbox"/> Auditorías periódicas <input type="checkbox"/> Control de acceso lógico <input type="checkbox"/> Cifrado de los datos <input type="checkbox"/> Anonimización	<input type="checkbox"/> Formación en protección de datos y seguridad al nivel adecuado <input type="checkbox"/> Registro de incidentes <input type="checkbox"/> Control de acceso físico <input type="checkbox"/> Niveles de acceso a los datos <input type="checkbox"/> Copia de seguridad <input type="checkbox"/> Ninguna de las anteriores		
¿Ha denunciado los hechos ante las Autoridades policiales y/o judiciales competentes por considerarlo constitutivo de delito, o se pretende hacerlo? (No es necesario adjuntar a la notificación de brecha de datos personales una copia de la denuncia, en su caso, se le podría requerir al responsable con posterioridad)			
<input type="radio"/> Sí <input type="radio"/> No			
¿Considera que se han tomado todas las acciones posibles y ha dado por resuelta la brecha?			
<input type="radio"/> Sí <input type="radio"/> No <input type="radio"/> Desconocido			
En caso afirmativo, indicar la fecha en la que se dio por resuelta la brecha:	<input style="width: 100px; height: 20px;" type="text"/>		
12.- Comunicación a los interesados (LA COMUNICACIÓN A LOS INTERESADOS DEBE SER EN UN LENGUAJE CLARO Y SENCILLO, INCLUIR DETALLES DE LO OCURRIDO, ASÍ COMO LOS DATOS DE A DÓNDE DIRIGIRSE PARA OBTENER MÁS INFORMACIÓN), LA POSIBLES CONSECUENCIAS DE LA BRECHA SOBRE ELLOS, LAS MEDIDAS ADOPTADAS PARA RESOLVER LA BRECHA Y LAS MEDIDAS ADOPTADAS Y PROPUESTAS PARA MINIMIZAR EL IMPACTO NEGATIVO DE LA BRECHA)			
¿Se ha comunicado la brecha a las personas afectadas en los términos anteriormente descritos?			
<input type="radio"/> Sí	<input type="radio"/> No, pero serán	<input type="radio"/> No serán	<input type="radio"/> Pendiente de

 Castilla-La Mancha	INSTRUCCIÓN Notificación de brechas de datos personales	DIFUSIÓN LIMITADA	
		Código	PD-GEN-INS-005
		Versión	3.0
		Fecha	28/09/2021



FORMULARIO DE NOTIFICACIÓN BRECHAS DE DATOS PERSONALES A LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

(Versión 3.0)

En su caso, fecha en la que se comunicó o se tiene previsto comunicar	<input type="text"/>
En su caso, número de personas comunicadas o que se tiene previsto comunicar	<input type="text"/>
En su caso, medio de comunicación utilizado o previsto	
<input type="checkbox"/> Telefónica o verbalmente <input type="checkbox"/> Comunicado público o publicación en web corporativa <input type="checkbox"/> Difusión en medios de comunicación	<input type="checkbox"/> Comunicación dirigida personalmente a cada afectado (postal, Email, SMS o similar) <input type="checkbox"/> Comunicación dirigida personalmente a cada afectado (postal, Email, SMS o similar) con garantía de entrega y lectura
En su caso, las personas afectadas no serán informadas porque...	
<input type="radio"/> No existe un riesgo alto para sus derechos <input type="radio"/> Daño reputacional para la organización <input type="radio"/> No interferir en una investigación	<input type="radio"/> No hay ninguna acción que puedan llevar a cabo para mitigar los daños <input type="radio"/> La comunicación supone un esfuerzo <input type="radio"/> Otros

13.- Notificación completa o por fases (Marque la opción más adecuada a la situación del responsable en el momento de la notificación)

- Esta notificación contiene toda la información que como responsable se ha podido recabar respecto a la brecha de seguridad. A todos los efectos, la autoridad de control puede
- Esta notificación es inicial a los efectos de cumplimiento con el plazo de notificación establecido en el RGPD. En el plazo máximo de 30 días se notificará información adicional.

INFORMACIÓN BÁSICA DE PROTECCIÓN DE DATOS	
Responsable	Dirección General Administración Digital
Finalidad	Notificación de las quebras de seguridad producidas en la Administración a la Agencia Española de Protección de Datos y a los interesados.
Legitimación	6.1.c) Cumplimiento de una obligación legal del Reglamento General de Protección de Datos. Reglamento General de Protección de Datos (RGPD). Art. 6.1.e) UE 2016/679 de 27 de abril de 2016.



 Castilla-La Mancha	INSTRUCCIÓN Notificación de brechas de datos personales	DIFUSIÓN LIMITADA	
		Código	PD-GEN-INS-005
		Versión	3.0
		Fecha	28/09/2021



**FORMULARIO DE NOTIFICACIÓN BRECHAS DE DATOS PERSONALES A LA
 AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS**
 (Versión 3.0)

Destinatarios	Existe cesión de datos
Derechos	Puede ejercer los derechos de acceso, rectificación o supresión de sus datos, así como otros derechos, tal y como se explica en la información adicional.
Información adicional	Disponible en la dirección electrónica: https://rat.castillalamancha.es/info/1125



Documento Verificable en www.jccm.es mediante
 Código Seguro de Verificación (CSV): C6EEB8B1E8337847C544EE

 Castilla-La Mancha	INSTRUCCIÓN Notificación de brechas de datos personales	DIFUSIÓN LIMITADA	
		Código	PD-GEN-INS-005
		Versión	3.0
		Fecha	28/09/2021

ANEXO II MODELO DE REGISTRO DE BRECHAS DE DATOS PERSONALES


 Castilla-La Mancha

REGISTRO BRECHAS DE DATOS PERSONALES DE
<ÓRGANO GESTOR RESPONSABLE DE LOS TRATAMIENTOS>

El RGPD define, de un modo amplio, las “brechas de datos personales” como “todas aquellas violaciones 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”.

En cumplimiento del artículo 33.5 del RGPD, el responsable del tratamiento debe elaborar y mantener un registro de brechas de seguridad cuando estas afecten a datos personales. La inscripción en este registro se debe realizar con independencia de que la brecha sea notificada a la AEPD y/o a los afectados o no.

Contenido de la información de la brecha:

- Identificación de la brecha
- Información sobre la brecha
- Información sobre los datos afectados
- Información sobre los sujetos afectados
 - Posibles consecuencias
 - Comunicación a la AEPD
 - Comunicación a los interesados



Documento Verificable en www.jccm.es mediante
 Código Seguro de Verificación (CSV): C6EEB8B1E8337847C544EE

 Castilla-La Mancha	INSTRUCCIÓN Notificación de brechas de datos personales	DIFUSIÓN LIMITADA	
		Código	PD-GEN-INS-005
		Versión	3.0
		Fecha	28/09/2021

ANEXO III COMUNICACIÓN A LOS INTERESADOS



FORMULARIO DE NOTIFICACIÓN DE BRECHAS DE DATOS PERSONALES A LOS INTERESADOS

(Versión 3.0)



Datos de contacto del interesado

Estimado ciudadano/a:

En cumplimiento del artículo 34 del Reglamento (UE) 679/2016, de 27 de abril, 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, le informamos que se ha producido una brecha de seguridad que afecta a sus datos personales:

Descripción general del incidente y momento en que se ha producido

Posibles consecuencias		
Brecha de confidencialidad:		
<input type="checkbox"/> Divulgación a terceros/difusión en internet	<input type="checkbox"/> Los datos pueden ser explotados con otros fines	<input type="checkbox"/> Enriquecimiento de otras bases de datos
<input type="checkbox"/> Otras:		
Brecha de integridad:		
<input type="checkbox"/> Datos han sido modificados aunque hayan quedado inservibles o irrecuperables	<input type="checkbox"/> Datos han sido modificados y utilizados para otros fines	
<input type="checkbox"/> Otras:		
Brecha de disponibilidad:		



 Castilla-La Mancha	INSTRUCCIÓN Notificación de brechas de datos personales	DIFUSIÓN LIMITADA	
		Código	PD-GEN-INS-005
		Versión	3.0
		Fecha	28/09/2021



**FORMULARIO DE NOTIFICACIÓN DE
BRECHAS DE DATOS PERSONALES A LOS INTERESADOS**

(Versión 3.0)

Posibles consecuencias	
<input type="checkbox"/> Imposibilidad de la prestación de un servicio a los interesados	<input type="checkbox"/> Deterioro de las condiciones de prestación de un servicio a los interesados
<input type="checkbox"/> Otras:	

Sobre los datos afectados	
Categoría de datos afectados:	
<input type="checkbox"/> Datos básicos.	<input type="checkbox"/> Credenciales de acceso o identificación.
<input type="checkbox"/> DNI, NIE y/o Pasaporte.	<input type="checkbox"/> Datos económicos o financieros.
<input type="checkbox"/> Sobre condenas e infracciones penales.	<input type="checkbox"/> Imágenes (foto/video).
<input type="checkbox"/> Datos de perfiles.	<input type="checkbox"/> Medios de pago (nº de tarjeta o cuenta bancaria).
<input type="checkbox"/> Otros:	
Categorías especiales de datos:	
<input type="checkbox"/> Sobre la religión o creencias.	<input type="checkbox"/> Sobre el origen racial.
<input type="checkbox"/> De salud de empleados.	<input type="checkbox"/> Sobre la afiliación sindical.
<input type="checkbox"/> Datos de salud de pacientes.	<input type="checkbox"/> Datos genéticos.
<input type="checkbox"/> Sobre la opinión política.	<input type="checkbox"/> Sobre la vida sexual.
<input type="checkbox"/> Otros:	<input type="checkbox"/> Datos biométricos.
Número aproximado de registros de datos personales afectados:	

Medidas adoptadas
Medidas adoptadas o propuestas para poner remedio a la brecha de seguridad de los datos personales
Si procede, medidas adoptadas para mitigar los posibles efectos negativos



 Castilla-La Mancha	INSTRUCCIÓN Notificación de brechas de datos personales	DIFUSIÓN LIMITADA	
		Código	PD-GEN-INS-005
		Versión	3.0
		Fecha	28/09/2021



**FORMULARIO DE NOTIFICACIÓN DE
BRECHAS DE DATOS PERSONALES A LOS INTERESADOS**

(Versión 3.0)

Así mismo le informamos que ya se ha procedido a su notificación a la Agencia Española de Protección de datos.

Si desea conocer más información sobre esta brecha puede ponerse en contacto con el/la Delegado/a de Protección de Datos:

Dirección postal:

Delegada de Protección de Datos
Dirección General de Administración Digital
Consejería de Hacienda y Administraciones Públicas
Calle Río Cifuentes S/N
45071 - Toledo

Dirección de correo electrónico:

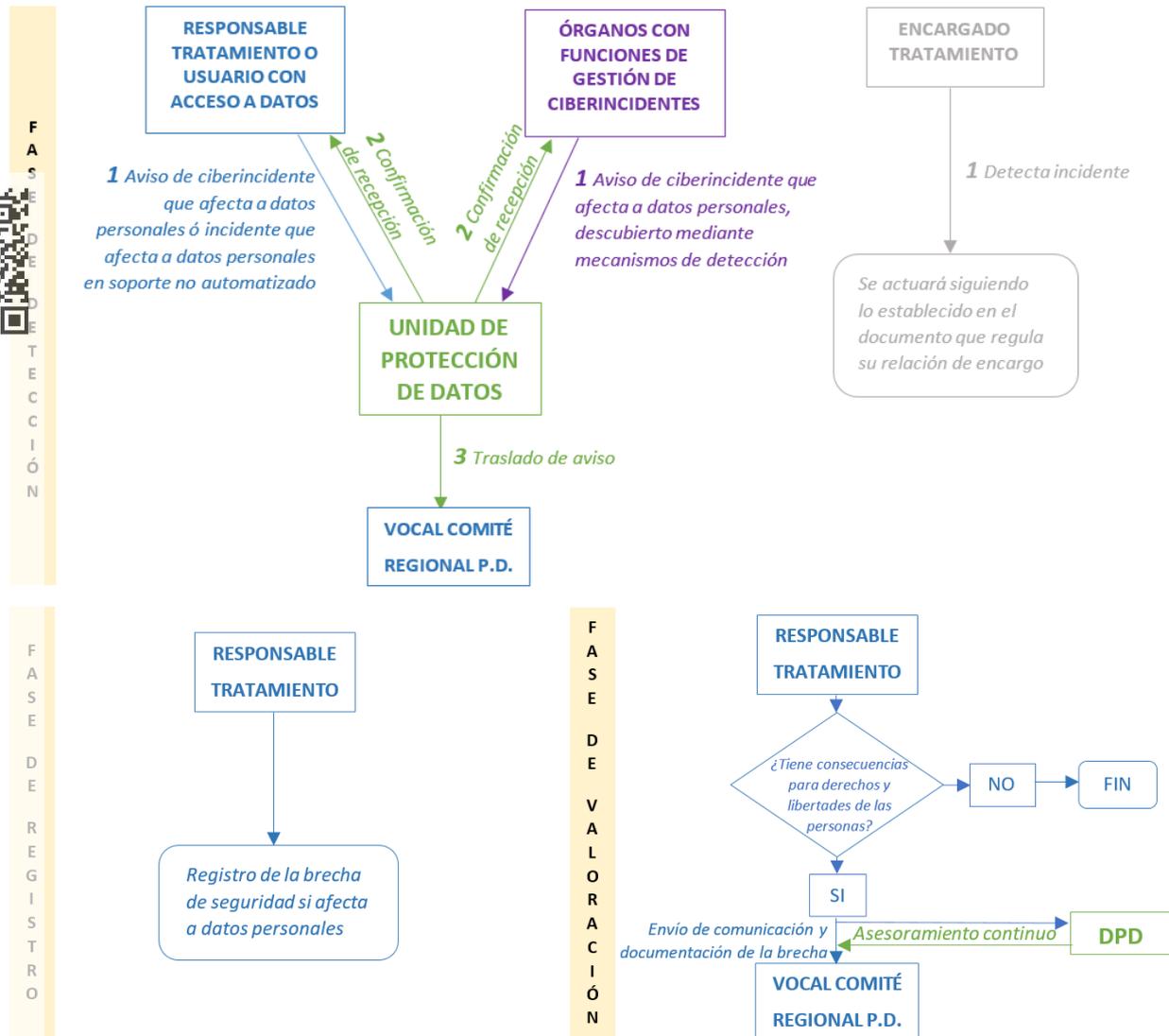
protecciondatos@jccm.es

En a

Edo:



ANEXO IV ESQUEMA NOTIFICACIÓN DE BRECHAS DE DATOS PERSONALES



Documento Verificable en www.jccm.es mediante
 Código Seguro de Verificación (CSV): C6EEB8B1E8337847C544EE



Castilla-La Mancha

INSTRUCCIÓN Notificación de brechas de datos personales

DIFUSIÓN LIMITADA

Código PD-GEN-INS-005

Versión 3.0

Fecha 28/09/2021

F
A
S
E
D
E
C
O
M
U
N
I
C
A
C
I
O
N

F
A
S
E
D
E
C
O
M
U
N
I
C
A
C
I
O
N

F
A
S
E
D
E
C
O
M
U
N
I
C
A
C
I
O
N



Documento Verificable en www.jccm.es mediante Código Seguro de Verificación (CSV): C6EEB8B1E8337847C544EE

