Castilla-La Mancha

INSTRUCCIÓN
Notificación de brechas de datos personales

Versión: 5.0

Fecha: 10/09/2025

Aprobado
Firmado digitalmente el 15-09-2025 Director General de la Oficina del Dato

Vicepresidencia Primera
Oficina del Dato
c/ Río Cabriel, 12 – Edificio CIE III
45071 - Toledo

Tel. 925 26 7703
Correo-e: oficinadeldato@jccm.es

www.castillalamancha.es

	Nombre	Fecha
Elaborado por:	Protección de Datos	01/02/2019
Revisado por:	Delegada de Protección de Datos	05/09/2025

HISTÓRICO DEL DOCUMENTO			
Versión	**Fecha**	**Descripción**	**Autor**
1.0	01/02/19	Versión inicial	Protección de Datos
2.0	12/03/21	Inclusión fase de petición de información de la AEPD Inclusión la realización de un informe único con anexos Inclusión herramienta de la AEPD para comunicación a ciudadanos	Protección de Datos
3.0	28/09/2021	Adaptación a la nueva guía para la notificación de brechas de datos personales de la AEPD	Protección de Datos
4.0	07/12/2023	Adaptación a la nueva estructura de la Junta de Comunidades de Castilla-La Mancha y al Decreto 55/2023, de 6 de junio, por el que se establece la política de protección de datos en la Administración de la Junta de Comunidades de Castilla-La Mancha	Protección de Datos
5.0	10/09/2025	Adaptación a la nueva estructura de la Junta de Comunidades de Castilla-La Mancha y modificación de algunos apartados por cuestiones de eficiencia	Protección de Datos

Castilla-La Mancha

1. INTRODUCCIÓN 4
1.1 Objeto 5
1.2 Ámbito de aplicación 5
1.3 Definiciones, acrónimos y referencias 6
1.3.1 Definiciones 6
1.3.2 Acrónimos 6
1.3.3 Referencias 6
2. Notificación de brechas de DATOS PERSONALES 8
2.1 Detección y comunicación interna de la brecha de datos personales 8
2.2 Registro y valoración de la brecha 9
2.2.1 Registro de brechas de datos personales 9
2.2.2 Valoración de necesidad de notificación 11
2.3 Gestión de la brecha de datos personales 12
2.4 Comunicación a la AEPD 13
2.5 Comunicación a los afectados 15
2.5.1 Supuestos para la notificación a los interesados: 15
2.5.2 Forma de realizar la comunicación 15
2.6 Respuesta de la AEPD a la notificación de una brecha 16
2.7 Comunicación del SESCAM 17
ANEXO I FORMULARIO DE NOTIFICACIÓN A LA AEPD 18
Anexo II: registro de brechas de datos personales 28
Anexo III: Modelo de comunicación al afectado 29

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:

Artículo 33:

"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.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo."

Artículo 34:

"1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida."

1.1 Objeto

El objeto de la presente instrucción es regular la obligación de los órganos gestores de notificar las brechas de datos personales que pudieran ocurrir en los tratamientos de los que son responsables facilitando su cumplimiento en tiempo y forma, 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 SESCAM que quedará sujeto a aquello que específicamente se refiera al mismo.

c) El resto de las entidades de Derecho Público vinculadas o dependientes, cuando ejerzan potestades administrativas.

1.3 Definiciones, acrónimos y referencias

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 ciberincidente 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

1.3.2 Acrónimos

Acrónimo	Concepto
AEPD	Agencia Española de Protección de Datos
DPD	Delegada/Delegado de Protección de Datos
RGPD	Reglamento General de Protección de Datos
LOPDyGDD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
SESCAM	Servicio de Salud de Castilla-La Mancha

1.3.3 Referencias

Los siguientes documentos son aplicables en la medida que se indique en el documento, correspondiéndose sus versiones y fechas con las vigentes en el momento de aplicación de este; el resto se han usado simplemente a modo de consulta.

Referencias
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
Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Guía para la notificación de brechas de datos personales (AEPD)
Sede electrónica de la AEPD: trámite de brechas de datos personales
Herramienta de la AEPD: Comunica-Brecha RGPD
Herramienta de la AEPD: Asesora Brecha

2. NOTIFICACIÓN DE BRECHAS DE DATOS PERSONALES

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 de los datos personales 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 DPD, 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 ciberincidentes deberá comunicarlo a la mayor brevedad posible a la DPD, 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 DPD, correo protecciondatos@jccm.es o a través del Servicio Integral de Gestión para Usuarios y Empleados: https://sigue.jccm.es.

La DPD responderá confirmando la recepción del correo e informará de la brecha de datos personales a los referentes de protección de datos correspondientes por la misma vía.

2.2 Registro y valoración de la brecha

2.2.1 Registro de brechas de datos personales

Se creará un registro de brechas de datos personales por cada una de las siguientes entidades:

- Presidencia.
- Consejerías.
- Organismos Autónomos.
- Entidades de derecho público.

La creación de este registro se realizará por medio de los referentes de protección de datos correspondientes.

Los responsables pertenecientes a cada uno de los organismos anteriores, a través de los referentes de protección de datos, deberán mantener actualizado dicho registro en relación con las brechas que afecten a los tratamientos de los que son responsables.

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 sea notificada.

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.
- 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.

- Comunicaciones a la AEPD (fecha de la comunicación, enlace al justificante y al documento, si procede).
- Comunicación a los interesados:
    - Si se comunica: fecha, número de interesados que han sido informados, medio utilizado y enlace al documento.
    - Si no se comunica justificación para no informar.

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.

2.2.2 Valoración de necesidad de notificación

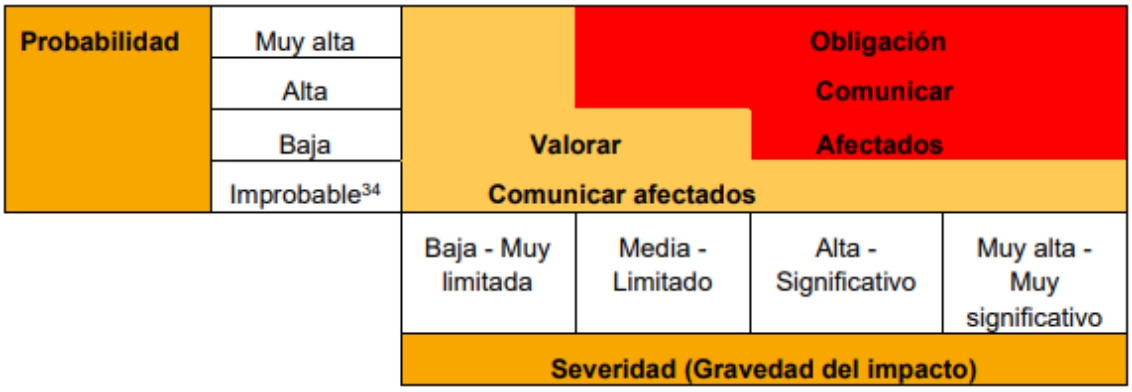
El nivel de riesgo para los derechos y libertades de las personas físicas afectadas por la brecha es el aspecto principal a tener en cuenta para notificar o no una brecha a la AEPD y/o comunicarla a los afectados.
Los factores que se pueden utilizar para evaluar el riesgo en una brecha de datos personales 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, que debe quedar documentada por el responsable, se concluye que la brecha no entraña riesgo para los derechos y libertades de los afectados, no será precisa la comunicación a la AEPD ni a los interesados. Para esta tarea el responsable debe contar con el

asesoramiento de la DPD y utilizar la herramienta Asesora Brecha disponible en la web https://www.aepd.es/guias-y-herramientas/herramientas. A su vez la DPD podrá contar con la asistencia del correspondiente referente de protección de datos.

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, que debe quedar documentada, 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.



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

Para esta tarea el responsable debe contar con el asesoramiento de la DPD y utilizar la herramienta Comunica Brecha-RGPD disponible en la web https://www.aepd.es/guias-y-herramientas/herramientas. A su vez la DPD podrá contar con la asistencia del correspondiente referente de protección de datos.

2.3 Gestión de la brecha de datos personales

Dependiendo de las características de brecha de datos personales, en la gestión de ésta podrán participar, teniendo en cuenta sus competencias:

- Los órganos con funciones de gestión de ciberincidentes.
- Los encargados de tratamiento. En este caso habrá que tener en cuenta si el encargado o subencargados han estado implicados en la brecha, si se requiere su participación o si son parte de la solución de la brecha.
- Los responsables de los tratamientos.

- Los referentes de protección de datos.
- Otros órganos de la Administración que por competencia presten algún servicio al responsable del tratamiento. En este caso habrá que tener en cuenta si han estado implicados en el hecho que produce la brecha, se requiere su participación o son parte de la solución de la brecha.
- La DPD, en su función de asesoramiento al responsable y supervisión del cumplimiento de la normativa de protección de datos.

Las secretarías generales, en el caso de las Consejerías, y los órganos directivos, en el caso de los organismos públicos, deberán aprobar un procedimiento de detección y gestión de las brechas de datos personales.

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 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 implementan 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 la DPD, deberá proceder a la notificación de ésta a la AEPD en un plazo no superior a las 72 horas a calcular desde que el responsable es consciente de que el incidente de seguridad ha afectado a datos de carácter personal. Para esta notificación el responsable enviará la información de la brecha a la DPD utilizando el Anexo I.

La DPD actuará como punto de contacto con la AEPD en el proceso de notificación por parte del responsable de las brechas de datos personales, y dicha función debe estar reflejada en el procedimiento interno de gestión de brechas de datos personales.

La comunicación de la brecha de datos personales se puede realizar de forma:

- Completa, cuando se conoce toda la información de la brecha. En cuyo caso debe estar cumplimentado el campo de fecha de finalización en el formulario del Anexo I.
- Inicial, en caso de que en las primeras 72 horas no se disponga de 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 a 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, si procede.
- Anexo I "Formulario de notificación de brechas".
- Anexo II "Modelo de comunicación a los interesados", si procede.

El procedimiento es el siguiente:

El responsable del tratamiento a través del referente de protección de datos correspondiente, notificará a la DPD en el correo protecciondatos@jccm.es, 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 por parte de la DPD.

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.

La DPD notificará la brecha de datos personales, 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 responsable del tratamiento afectado, el justificante de la notificación con copia al referente de protección de datos correspondiente.

2.5 Comunicación a los afectados

2.5.1 Supuestos para la notificación a los interesados:

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

- 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 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 demora le resta efectividad, por lo que los retrasos deberán ser justificados por parte del responsable).

  Para esta tarea el responsable debe contar con el asesoramiento de la DPD y utilizará la herramienta Comunica Brecha-RGPD disponible en la web https://www.aepd.es/guias-y-herramientas/herramientas. A su vez la DPD podrá contar con la asistencia del correspondiente referente de protección de datos.

- 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, a través de la DPD, la confirmación de haber ejecutado la orden dentro del plazo de 30 días, salvo que se indique un plazo diferente en la orden recibida.

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

2.5.2 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 II 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 a través de la DPD, puede recibir por parte de la AEPD diversas comunicaciones o notificaciones electrónicas con información relativa al registro de la brecha de datos personales notificada. Las más comunes son las siguientes:

- Comunicación 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.
- Comunicación 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 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.
- Comunicación de la AEPD indicando que no están previstas más acciones en relación con este acto de comunicación de brecha de datos personales.

El responsable del tratamiento enviará de forma inmediata la comunicación recibida de la AEPD a la DPD con copia a su referente de protección de datos.

En el caso de que la notificación de la AEPD implique respuesta por parte del responsable, este podrá solicitar el asesoramiento de la DPD. A su vez la DPD podrá contar con la asistencia del correspondiente referente de protección de datos. Una vez determinada la respuesta a enviar, remitirá la información la DPD para que lo notifique a la AEPD por vía "Sede Electrónica". La DPD enviará el justificante de la notificación a la AEPD al responsable con copia al referente de protección de datos.

2.7 Comunicación del SESCAM

El delegado de protección de datos de SESCAM deberá notificar al órgano competente en materia de protección de datos, semestralmente, el número de brechas de datos personales ocurridas en los tratamientos responsabilidad de los órganos gestores del SESCAM al correo electrónico: protecciondatos@jccm.es o a través del Servicio Integral de Gestión para Usuarios y Empleados: https://sigue.jccm.es.

ANEXO I FORMULARIO DE NOTIFICACIÓN A LA AEPD

Datos de la notificación

☐ Notificar una nueva brecha de datos personales

☐ Esta notificación es completa

☐ Esta notificación es inicial

☐ Modificar una notificación anterior

☐ Nº de registro de la notificación a modificar

☐ Fecha de notificación anterior

Sobre el tratamiento

¿Desde cuándo se viene realizando el tratamiento de datos afectado?

☐ Es un tratamiento puntual

☐ Menos de 1 año

☐ Entre 1 y 5 años

☐ Mas 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

El tratamiento sobre el que se ha producido la brecha incluye datos de personas:

☐ Únicamente en España, nivel local/municipal

☐ Únicamente en España, nivel provincial/autonómico

☐ Únicamente en España, nivel nacional

☐ En un único Estado miembro, pero no en España

☐ En más de un Estado miembro

☐ En más de un Estado miembro y a terceros Países

☐ A nivel mundial

Sobre la brecha y sus consecuencias

El incidente ha sido:

☐ Accidental o sin intencionalidad

☐ Intencionado, para dañar al responsable, al encargado o a las personas afectadas

☐ Desconocido

El origen del incidente ha sido:

☐ Interno: Personal o sistemas bajo el control del responsable de tratamiento

☐ Interno: Personal o sistemas bajo el control del encargado de tratamiento

☐ Externo: Otros, ajenos al responsable y encargado de tratamiento

¿Cómo puede haber ocurrido? Puede seleccionar varias opciones:

☐ Revelación verbal no autorizada

☐ Documentación perdida, robada o depositada en localización insegura

☐ Correo postal perdido o abierto

☐ Eliminación incorrecta de datos personales en formato papel

☐ Datos personales enviados por error (postal o electrónicamente)

☐ Datos personales eliminados/destruidos

☐ Abuso de privilegios de acceso por parte de empleado para extraer, reenviar o copiar datos personales

☐ Datos personales residuales en dispositivos obsoletos

☐ Publicación no intencionada/autorizada

☐ Envío de email a múltiples destinatarios sin copia oculta/lista distribución

☐ Dispositivo perdido o robado

☐ Ciberincidente: dispositivo cifrado/secuestro de información

☐ Ciberincidente: PHISHING/compromiso de cuenta de usuario

☐ Ciberincidente: acceso no autorizado a datos en sistema TI

☐ Incidencia técnica

☐ Modificación no autorizada de datos

☐ Datos personales mostrados al individuo incorrecto

Como consecuencia del incidente se ha visto afectada la:

☐ 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

Referido específicamente a los datos afectados por la 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?

☐ Sí

☐ No

☐ Desconocido

☐ Disponibilidad: se ha destruido, perdido o cifrado los datos personales de forma que no pueden ser tratados

Referido específicamente a los datos afectados por la brecha de disponibilidad. ¿Se ha recuperado la disponibilidad de los datos personales de forma que pueden ser tratados con normalidad?

☐ Sí

☐ No

☐ Todavía no, pero se recuperará en breve

☐ Integridad: se han alterado los datos personales, siguen siendo accesibles, pero la sustitución de datos puede suponer un daño para las personas afectadas

Referido específicamente a los datos afectados por la brecha de integridad. Seleccione la opción más apropiada:

☐ Datos alterados, pero sin constancia de uso ilegal o incorrecto

☐ Datos alterados y usados de forma ilegal o incorrecta, pero con posibilidad de revertir/recuperar los daños

☐ Datos alterados y usados de forma ilegal o incorrecta, sin posibilidad de revertir/recuperar los daños

¿Cuáles podrían ser las consecuencias sobre las personas físicas?

☐ Imposibilidad de ejercer algún derecho

☐ Imposibilidad para acceder a un servicio

☐ Usurpación de identidad

☐ Ser víctima de campañas de PHISHING/SPAMMING

☐ Pérdidas financieras

☐ Daños reputacionales

☐ Pérdida de confidencialidad de datos afectados por secreto profesional

☐ Daños psicológicos o físicos

☐ Pérdida de control sobre sus datos personales

☐ Otras consecuencias

☐ Aún desconocido

¿En qué grado podrían afectar las consecuencias identificadas a las personas físicas?

☐ 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

☐ 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.)

☐ 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.)

☐ 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

☐ 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?

☐ Sí

☐ No

Como valora la probabilidad de que el daño anterior se materialice sobre las personas afectadas con la severidad indicada

☐ Improbable

☐ Baja

☐ Alta

☐ Muy alta

☐ Desconocida

Introduzca una breve descripción de lo ocurrido. Evite incluir datos personales, fórmulas del tipo "ver anexo" y en ningún caso lo aquí escrito podrá suponer una modificación sobre lo consignado en el resto del formulario (entre 100 y 1500 caracteres).

Tipos de datos afectados

Selecciones los tipos de datos que se han visto afectados, exclusivamente de personas físicas, marque todas las opciones aplicables:

☐ Biométricos

☐ Datos básicos (Ej.: Nombre, Apellidos, fecha nacimiento)

☐ Sobre religión o creencia

☐ Imagen (Fotos/Vídeo)

☐ DNI, NIE, Pasaporte o cualquier documento identificativo

☐ Sobre condenas e infracciones penales

☐ Sobre afiliación sindical

☐ Datos económicos o financieros (sin medios de pago)

☐ Datos de medios de pago (Tarjeta bancaria, etc.)

☐ Sobre la vida sexual

☐ Datos de localización

☐ Datos de contacto

☐ Sobre origen racial o étnico

☐ Datos de perfiles (Ej.: en red social, solvencia, psicológico, etc.)

☐ Datos de salud (únicamente de empleados, los imprescindibles para relación laboral

☐ Datos de salud (otros datos de salud)

☐ Sobre opinión política

☐ Genéticos

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

Perfil de las personas afectadas, referido exclusivamente a personas físicas

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:

☐ Clientes/ciudadanos

☐ Estudiantes/alumnos

☐ Usuarios

☐ Pacientes

☐ Suscriptores/potenciales clientes

☐ Afiliados/asociados

☐ Militares/policías

☐ Empleados

☐ Otros

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

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

☐ Sí

☐ No

☐ Desconocido

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?

☐ La fecha exacta

☐ Aproximada / estimada

☐ Desconocida

La brecha se ha detectado mediante:

☐ Medios de detección implementados proactivamente por el responsable o encargado del tratamiento

☐ Comunicación de algún afectado

☐ Algún medio de comunicación

☐ La advertencia de un miembro de la organización del responsable o el encargado

☐ Un tercero ajeno

☐ Otros

Justificación de información tardía, si procede:

☐ Plazo de 72h expira fuera de la jornada laboral, durante el fin de semana o en vacaciones

☐ Problemas en medios técnicos propios para efectuar la notificación

☐ Inicialmente no se consideró susceptible de notificación a la autoridad de control

☐ Demora en el procedimiento de gestión de la brecha de datos personales

☐ No interferir en investigación policial / judicial en curso

☐ Otros

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 D ELA AUTORIDAD DE CONTROL):

☐ Políticas de protección de datos y seguridad

☐ Formación en protección de datos y seguridad al nivel adecuado

☐ Los sistemas informáticos se mantienen actualizados

☐ Registro de incidentes

☐ Auditorías periódicas

☐ Control de acceso físico

☐ Control de acceso lógico

☐ Niveles de acceso a los datos

☐ Cifrado de datos

☐ Copias de seguridad

☐ Anonimización

☐ Ninguna de las anteriores

¿La brecha podría haberse evitado adoptando alguna medida de seguridad adicional?

☐ Sí

☐ No

☐ Desconocido

¿Se ha producido el incidente por algún fallo, deficiencia o incumplimiento de las medidas de seguridad implementadas?

☐ Sí

☐ No

☐ Desconocido

¿Dispone de un análisis de riesgos documentado que justifique las medidas adoptadas previamente al incidente?

☐ Sí

☐ No

Acciones tomadas tras el incidente

¿Ha actualizado el registro de incidentes con la información de esta brecha de datos personales?

☐ Sí

☐ No

¿Ha adoptado tras el incidente nuevas medidas de seguridad que podrían haber evitado la brecha?

☐ Sí

☐ No

¿Ha adaptado / mejorado sus procedimientos y políticas de seguridad?

☐ Sí

☐ No

Marque exclusivamente las nuevas medidas de seguridad y las que se hayan actualizado, si procede:

☐ Políticas de protección de datos y seguridad

☐ Formación en protección de datos y seguridad al nivel adecuado

☐ Los sistemas informáticos se mantienen actualizados

☐ Registro de incidentes

☐ Auditorías periódicas

☐ Control de acceso físico

☐ Control de acceso lógico

☐ Niveles de acceso a los datos

☐ Cifrado de datos

☐ Copias de seguridad

☐ Anonimización

☐ Ninguna de las anteriores

¿Ha puesto el incidente en conocimiento de las autoridades policiales / judiciales por considerar que es constitutivo de delito?

☐ Sí

☐ No

¿Considera que ha tomado todas las acciones posibles y da por resuelta la brecha?

☐ Sí, con fecha _____

☐ No

Comunicación a los afectados por la brecha de datos personales (LA COMUNICACIÓN DE LA BRECHA 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?

☐ Sí

Fecha en la que se informó:

Número de personas informadas:

Medio por el que se ha informado:

☐ Telefónica o verbalmente

☐ Comunicación dirigida personalmente a cada afectado (postal, Email, SMS o similar)

☐ Comunicación dirigida personalmente a cada afectado (postal, Email, SMS o similar) con garantía de entrega y lectura

☐ Comunicado público o publicación en web corporativa

☐ Difusión en medios de comunicación

☐ No, pero serán informados

A más tardar, las personas afectadas serán informadas en la siguiente fecha:

Medio por el que se informará:

☐ Telefónica o verbalmente

☐ Comunicación dirigida personalmente a cada afectado (postal, Email, SMS o similar)

☐ Comunicación dirigida personalmente a cada afectado (postal, Email, SMS o similar) con garantía de entrega y lectura

☐ Comunicado público o publicación en web corporativa

☐ Difusión en medios de comunicación

☐ No serán informados

Las personas afectadas no serán informadas por:

☐ No existe un riesgo alto para sus derechos y libertades

☐ No hay ninguna acción que puedan llevar a cabo para mitigar los daños para mitigar los daños que les causará la brecha d datos personales

☐ El daño reputacional para la organización sería muy elevado

☐ La comunicación supone un esfuerzo excesivo

☐ No interferir en una investigación policial/judicial en curso

☐ Otros

Castilla-La Mancha

Encargado del tratamiento

¿Hay implicado un encargado de tratamiento en la brecha de datos personales?

☐ Sí

Tipo de organización:

☐ Pública

☐ Privada

Nombre:

CIF:

Calle y número:

País:

Código postal:

Provincia:

Localidad:

☐ No

INFORMACIÓN BÁSICA DE PROTECCIÓN DE DATOS	
Responsable	Oficina del Dato
Finalidad	Notificación de las brechas de datos personales producidas en los tratamientos de la JCCM (salvo SESCAM) 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.
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**

ANEXO II: 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
- Comunicaciones a la AEPD
- Comunicación a los interesados

Castilla-La Mancha

ANEXO III: MODELO DE COMUNICACIÓN AL AFECTADO

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>

Las posibles consecuencias para las personas afectadas son las siguientes:

☐ Imposibilidad de ejercer algún derecho.

☐ Imposibilidad para acceder a un servicio.

☐ Usurpación de identidad.

☐ Ser víctima de campañas de PHISHING/SPAMMING.

☐ Pérdidas financieras.

☐ Daños reputacionales.

☐ Pérdida de confidencialidad de datos afectados por secreto profesional.

☐ Daños psicológicos o físicos.

☐ Pérdida de control sobre sus datos personales.

☐ Otras consecuencias.

☐ Aún desconocido.

Las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales son las siguientes:

☐ Políticas de protección de datos y seguridad.

☐ Formación en protección de datos y seguridad al nivel adecuado.

☐ Los sistemas informáticos se mantienen actualizados.

☐ Registro de incidentes.

☐ Auditorías periódicas.

☐ Control de acceso físico.

☐ Control de acceso lógico .

☐ Niveles de acceso a los datos.

☐ Cifrado de datos.

☐ Copias de seguridad.

☐ Anonimización.

☐ Otras…….

Si procede, las medidas adoptadas para mitigar los posibles efectos negativos:

……

……..

Si desea conocer más información sobre esta brecha puede ponerse en contacto con la delegada de protección de datos:

<u>Dirección postal:</u>

Delegada de Protección de Datos

Vicepresidencia Primera

Oficina del Dato

C/ Río Cabriel, 12 – Edificio CIE III

45071 - Toledo

<u>Dirección de correo electrónico:</u>

protecciónd atos@jccm.es

<firma>