UNIVERSIDAD DE ALMERÍA

PROCEDIMIENTO DE GESTIÓN DE INCIDENTES Y NOTIFICACIÓN DE BRECHAS DE SEGURIDAD EN DATOS DE CARÁCTER PERSONAL

Comisión de Seguridad Informática y Protección de Datos

21/09/2022

CONTROL DE CAMBIOS

Versión	Fecha	Cambios	Revisado	Aprobado
1.0	2018	Versión inicial		
2.0	2022	Versión adaptada a la nueva Guía para la notificación de brechas de datos personales de la Agencia Española de Protección de Datos	Junio 2021	
3.0	2022	Revisado en la Comisión de Seguridad Informática y Protección de Datos	30/03/2022	
3.1	2022	Aprobado por la Comisión de Seguridad Informática y Protección de Datos		21/09/2022

1. OBJETO

El presente documento constituye una normativa interna de obligado cumplimiento para el personal de Universidad de Almería (en adelante, UAL).

El objeto de este documento es desarrollar el procedimiento establecido por parte de la UAL, en relación con la gestión de incidentes de seguridad que puedan afectar a la confidencialidad, integridad o disponibilidad de los datos de carácter personal, así como la notificación - en caso de concebirse como brecha o violación de seguridad- a la Autoridad de Control en protección de datos y la comunicación a las personas físicas afectadas.

Los artículos 33 y 34 del RGPD exponen la necesidad de que las organizaciones integren dentro de sus políticas un proceso de gestión de brechas de datos personales que concrete cómo la organización va a dar cumplimiento a sus obligaciones con respecto a las brechas de seguridad.

Este proceso constituye una de las medidas organizativas más importantes a la hora de salvaguardar los derechos y libertades de los interesados a través de medidas de seguridad de los tratamientos.

Las notificaciones de brechas de datos personales ante la Autoridad de Control son parte de la responsabilidad proactiva de la UAL. La notificación de brechas realizada de acuerdo con el RGPD no implica necesariamente la imposición de una sanción. Al contrario, una notificación y comunicación en tiempo y forma, en el caso de que la Autoridad de Control inicie actuaciones previas de investigación, es una evidencia de la diligencia de la organización a la hora de ejecutar eficazmente la obligación de responsabilidad proactiva requerida por el RGPD. Sin embargo, el no cumplir con las obligaciones de notificación a la Autoridad y comunicación a los interesados sí está tipificado como infracción.

Específicamente en relación con las brechas de datos personales, el artículo 73 de la LOPDGDD establece como **infracciones graves**, entre otras:

"*q) El incumplimiento del deber del encargado del tratamiento de notificar al responsable del tratamiento las violaciones de seguridad de las que tuviera conocimiento.*

r) El incumplimiento del deber de notificación a la autoridad de protección de datos de una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679.

s) El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos de conformidad con lo previsto en el artículo 34 del Reglamento (UE) 2016/679 si el responsable del tratamiento hubiera sido requerido por la autoridad de protección de datos para llevar a cabo dicha notificación.

f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679.

g) El quebrantamiento, como consecuencia de la falta de la debida diligencia, de las medidas técnicas y organizativas que se hubiesen implantado conforme a lo exigido por el artículo 32.1 del Reglamento (UE) 2016/679."

Por otra parte, el artículo 74 de la LOPDGDD establece como **infracciones leves**:

"*m) La notificación incompleta, tardía o defectuosa a la autoridad de protección de datos de la información relacionada con una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679.*

n) El incumplimiento de la obligación de documentar cualquier violación de seguridad, exigida por el artículo 33.5 del Reglamento (UE) 2016/679.

ñ) El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos que entrañe un alto riesgo para los derechos y libertades de los afectados, conforme a lo exigido por el artículo 34 del Reglamento (UE) 2016/679, salvo que resulte de aplicación lo previsto en el artículo 73 s) de esta ley orgánica."

2. LEGISLACIÓN Y GUÍAS DE REFERENCIA

Las referencias tenidas en cuenta para la redacción de esta normativa han sido principalmente:

- 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD).

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

También se han tenido en cuenta las siguientes guías:

- Guía de la AEPD para la notificación de brechas de datos personales
- *Guidelines 01/2021 on Examples regarding Data Breach Notification* del Comité Europeo de Protección de Datos.
- Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679 del Grupo de trabajo sobre protección de datos del artículo 29.

3. ROLES Y RESPONSABILIDADES

En el contexto del presente procedimiento, se definen las siguientes responsabilidades, sin perjuicio de los roles y responsabilidades:

- **Responsable del tratamiento = UAL**

  Deberá aplicar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme al RGPD:

  - implantar del proceso de gestión de brechas;
  - garantizar que se notifica la brecha de datos personales a la autoridad competente sin dilación indebida, y también que se comunicará la brecha de datos personales a los afectados cuando sea necesario;
  - evaluar las consecuencias para los derechos y libertades de las personas;
  - contar con el asesoramiento del Delegado de Protección de Datos.

- **Encargado del tratamiento = tercero/prestador de servicio con acceso a datos**

  En caso de que el incidente o brecha de seguridad se produzca por parte de un tercero que trate datos por cuenta de la UAL (encargado del tratamiento), este deberá:

- informar al responsable de tratamiento sin dilación indebida de las brechas de datos personales que afecten a los tratamientos encargados, sin perjuicio de las obligaciones adicionales que pueda haber adquirido en virtud del contrato de encargo de tratamiento;
- ayudar a la UAL a garantizar el cumplimiento de las obligaciones establecidas en el RGPD, incluyendo la gestión, notificación y comunicación de las brechas de datos personales;
- ejecutar las labores de notificación o comunicación de la brecha que tenga asignadas por contrato.

- **Delegado de Protección de Datos = Comisión de Seguridad Informática y Protección de Datos**

  Debe supervisar y asesorar en materia de cumplimiento de la legislación en materia de protección de datos. Su rol dentro de este procedimiento debe ser:

  - el asesoramiento y apoyo a las tareas de valoración del incidente y las posibles consecuencias al afectado;
  - actuar como portavoz único ante la Autoridad de Control y ser la persona que atenderá cualquier cuestión, duda, derecho o denuncia de los interesados afectados por el incidente de seguridad en cualquiera de los tratamientos de datos personales realizado por la UAL;
  - asesorar sobre la evaluación del riesgo y las consecuencias que puede suponer para los derechos y libertades de las personas una brecha de datos personales;
  - asesorar sobre la necesidad de notificar la brecha de datos personales a la Autoridad de Control y en su caso a los interesados afectados;
  - supervisar las acciones de mejora para asegurar la eficacia de las medidas y la validez de las lecciones aprendidas.

- **Responsable = Órgano con competencias en tecnologías de la información y las comunicaciones**

  Será el encargado de la resolución efectiva de los incidentes que se produzcan y que estén relacionados con los sistemas automatizados de la entidad.

- **Usuarios de los sistemas de información**

  Todos los usuarios de los sistemas de información de la UAL que utilicen equipamiento informático y accedan o traten información de carácter personal para la realización de sus funciones y tareas tienen la responsabilidad de conocer y cumplir el presente procedimiento.

4. ¿QUÉ ES UNA BRECHA O VIOLACIÓN DE SEGURIDAD EN PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL?

El artículo 4.12 RGPD define, de un modo amplio, las **"violación 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".***

No tendrán consideración de violación o brecha de seguridad de datos personales, a los efectos de la obligación de notificación a la Autoridad de Control y comunicación a los afectados, aquellos incidentes que:

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

Por otro lado, tal y como manifiesta la AEPD en su Guía (pág. 8), ***"no todos los incidentes de seguridad son necesariamente brechas de datos personales y no solo los ciberincidentes pueden ser brechas de datos personales. A su vez, no toda acción que suponga una vulneración de la normativa de protección de datos puede ser considerada una brecha de datos personales".***

Por tanto, es necesario establecer un criterio para que la UAL determine los parámetros a considerar para valorar cuándo el incidente se concibe como una brecha o violación de la seguridad de los datos de carácter personal.

5. FASES EN LA GESTIÓN Y NOTIFICACIÓN DE BRECHAS DE SEGURIDAD

El proceso de gestión y notificación de incidentes se compone de las siguientes fases. Tal como se ha referido, es necesario conocer qué ha ocurrido y de qué forma las medidas de seguridad han funcionado o paliado los hechos para establecer si realmente se ha producido o no una violación de la seguridad de los datos.

FASE 1 – DETECCIÓN Y ALERTA

Cualquier empleado, proveedor u otra persona, puede informar a la UAL de la existencia de un incidente que pudiera afectar a la seguridad de los datos de carácter personal.

Si la brecha de datos personales es detectada por el encargado del tratamiento, éste deberá remitir al responsable toda la información necesaria para que pueda cumplir con sus obligaciones en tiempo y forma.

El incidente de seguridad deberá ser comunicado, inmediatamente, a la **Comisión de Seguridad Informática y Protección de Datos** a través del email consulta.comision.seguridad@ual.es.

FASE 2 – REGISTRO DEL INCIDENTE

El incidente será registrado e irá documentándose el proceso con toda la información que se vaya recopilando. La información relativa a las decisiones tomadas sobre la notificación a la Autoridad de Control competente y la comunicación a los afectados (incluida una copia de la comunicación si hubiera de realizarse) debe recogerse también en este registro de forma detallada.

La información a registrar, mínimamente, será:

- Fecha y hora de la detección.
- Detección. [empleado, colaborador, 3º de confianza, externo].
- Naturaleza del evento de seguridad de los datos personales.
- Descripción breve.
- Sistema afectado.
- Unidad organizativa o unidades organizativas potencialmente afectadas.

En la medida de lo posible, y aunque sea información imprecisa o sin verificar, deberá también solicitarse información para poder evaluar la severidad del incidente. Por ese motivo, se recogerá además la siguiente información:

- Tipo y número aproximado por categoría de interesados afectados [menores, empleados, afiliados a sindicatos, etc.].
- Categorías y número aproximado de registros de datos personales afectados [DNI, nombre y apellidos, direcciones, matrículas, credenciales, etc.].
- Nivel de certeza de los hechos conocidos: [Sin evidencias / Indicios de evidencia / Evidencias contrastables].

Es necesario destacar que, es posible que durante el primer registro del incidente no se disponga de toda la información descrita, en cuyo caso deberá de solicitarse más información y la investigación del incidente para poder cumplimentar, al menos, con información aproximada los campos requeridos.

En el **ANEXO I** se recoge un modelo de formulario para registro de incidentes y brechas de seguridad de la información.

FASE 3 – ACTUACIONES DE CONTENCIÓN Y RECUPERACIÓN FRENTE A LOS INCIDENTES INFORMÁTICOS O ELECTRÓNICOS.

Frente a los incidentes de seguridad, principalmente, los que afectan a los sistemas de información automatizados (informáticos o electrónicos) se precisará la intervención inmediata del Responsable de Seguridad, a los efectos de llevar a cabo las siguientes actuaciones:

Contención

La contención del incidente supondrá la toma de decisiones rápidas y adopción de medidas, técnicas y organizativas, como puede ser cerrar un sistema, aislarlo de la red, deshabilitar ciertas funciones, etc.

Una vez aplicadas de las medidas, se debe verificar el correcto funcionamiento de estas, confirmando su idoneidad para la eliminación del incidente.

Se debe considerar también si las medidas aplicadas son de carácter temporal o si forman parte de una solución definitiva, y el sistema y/o la información afectada ha vuelto de nuevo de modo efectivo a su estado original.

Recuperación

Solucionado el incidente o la brecha de seguridad, y verificada la eficacia de las medidas adoptadas, se restablecerá el servicio en su totalidad, confirmando su funcionamiento normal y evitando en la medida de lo posible que sucedan nuevos incidentes basados en la misma causa. Esto será crucial para categorizar con carácter final la severidad del incidente de seguridad en protección de datos personales, y poder así valorar si estamos ante una brecha de seguridad.

Frente al resto de incidentes de seguridad que no estén relacionados con los sistemas automatizados, se estará igualmente a lo mencionado en los apartados anteriores de Contención y Recuperación.

FASE 4 – VALORACIÓN DE LOS INCIDENTES Y BRECHAS DE SEGURIDAD

La valoración del incidente se realizará por parte de la Comisión de Seguridad Informática y Protección de Datos.

4.1 TIPOLOGÍA BRECHA DE SEGURIDAD

Tal y como afirma la AEPD[1], uno de los parámetros más importantes a la hora de evaluar una brecha de datos personales es determinar con exactitud su tipología, es decir determinar a qué dimensión/es de seguridad de los datos personales ha afectado la brecha:

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

Fuente: AEPD, Guía para la notificación de brechas de datos personales, p. 32.

[1] Guía AEPD p. 32.

En segunda instancia, se podrá recatalogar el evento de seguridad atendiendo a los criterios establecidos por el punto 5.2., en lo que respecta a la modificación de la severidad del evento de privacidad.

Confidencialidad: Una brecha afecta a la confidencialidad cuando los datos personales de un tratamiento han podido ser accedidos por terceros sin permiso. Esto incluye, por ejemplo, los casos de intrusión en sistema de información con acceso y/o exfiltración de datos personales, el envío de datos personales por error, la pérdida de dispositivos o documentación con datos personales, malware de tipo ransomware con exfiltración de datos, etc. Es importante saber si los datos personales afectados estaban (total o parcialmente) cifrados de forma segura, anonimizados o protegidos de forma que sean ininteligibles para quien haya tenido acceso a dichos datos o lo pueda tener en el futuro. Si es así, las consecuencias de la brecha de confidencialidad quedan en gran medida mitigadas reduciendo o incluso anulando los riesgos derivados del incidente.

- Ejemplo: brechas causadas por pérdida o robo de dispositivos móviles cuyos elementos de almacenamiento están cifrados con un algoritmo no comprometido y el acceso al dispositivo protegido por una contraseña fuerte y difícilmente deducible, se puede considerar que los riesgos asociados a la pérdida de confidencialidad de los datos están apropiadamente mitigados.
- Ejemplo: brechas causadas por la exfiltración de un fichero de base de datos de usuarios conteniendo nombre de usuario, contraseña, datos de contacto y dirección:
    - Si las contraseñas de los usuarios están protegidas con un algoritmo de hash considerado criptográficamente seguro, de forma que son ininteligibles para quien ha tenido acceso a la base de datos, el riesgo quedaría parcialmente mitigado. Si el algoritmo de hash no se considera criptográficamente seguro (md5, sha1…) la mitigación del riesgo no es efectiva.
    - Si el fichero de base de datos exfiltrado estaba totalmente cifrado mediante un algoritmo criptográficamente seguro y la clave de cifrado no está comprometida, el riesgo queda mitigado de forma que en algunos casos se puede considerar que es prácticamente nulo

Disponibilidad: Una brecha afecta a la disponibilidad de los datos personales cuando han estado inaccesibles de forma temporal o permanente para quien legítimamente debe poder tratarlos o acceder a ellos. Esta situación puede ocurrir por sucesos que afecten a los datos

personales en sí mismos o también por sucesos que afecten a los sistemas utilizados para su tratamiento.

Es importante determinar si la disponibilidad se ha podido recuperar o está en vías de recuperación, dado que recuperar los datos y los sistemas de tratamiento es la vía para mitigar el daño que pueden producir este tipo de brechas de datos personales.

- Ejemplo: brechas causadas por malware tipo ransomware en las que se pueda descartar con certeza la exfiltración de datos y se pueden reestablecer los datos personales y medios de tratamiento sin que afecte significativamente a los servicios prestados, se puede considerar que el riesgo se ha mitigado adecuadamente. En el caso de que la recuperación de los datos y/o tratamientos se prolongue en el tiempo afectando significativamente a los servicios prestados, por ejemplo, al no existir o no funcionar sistemas de respaldo de datos y procesos, se puede concluir que el riesgo no solo no ha quedado mitigado, sino que se está materializando y causando perjuicios de diversa consideración a los interesados.
- Ejemplo: brechas causadas por malware tipo ransomware en las que se pueda descartar con certeza la exfiltración de datos y se pueden reestablecer los datos personales y medios de tratamiento sin que afecte significativamente a los servicios prestados, se puede considerar que el riesgo se ha mitigado adecuadamente.
- Ejemplo: En brechas causadas por la pérdida o destrucción accidental de datos personales, el riesgo se considerará mitigado cuando exista un plan de recuperación que incluya una copia actualizada y recuperable de los datos y se pueda reestablecer la prestación del servicio sin haber causado perjuicios a los interesados.

Integridad: Una brecha afecta a la integridad cuando se han alterado los datos personales de forma ilegítima y el tratamiento de esos datos personales puede causar un daño a los afectados.

- Por ejemplo, un tercero ha modificado en la base de datos de la organización la información relativa a los datos bancarios de los empleados que se utilizan para el pago de las nóminas, o un alumno modifica las calificaciones en la base de datos. Cuando se producen brechas de datos personales de integridad, la UAL debe determinar si el tratamiento de los datos alterados ilegítimamente puede causar o ha causado algún daño a los afectados y en su caso si el daño se puede revertir.

- Ejemplo: Para mitigar las brechas de integridad causadas por la modificación de ficheros se puede implementar herramientas de control de la integridad de los archivos que se basan en calcular el hash de cada fichero que se vigila y cuando es modificado, aunque sea un solo bit de alguno de estos archivos el sistema periódicamente vuelve a calcular el hash de cada uno y al compararlo detectará la modificación y emitirá un aviso.
- Ejemplo: Se podrá mitigar el riesgo de una brecha de integridad en las bases de datos contando con controles de acceso, alertas y registros ante modificaciones. Además, implementando sistemas que auditen de forma continua los accesos de lectura y escritura a estas bases de datos.

SUCESO	Confidencialidad	Disponibilidad	Integridad
Revelación verbal no autorizada	x		
Documentación perdida, robada o depositada en localización insegura	x	x	
Correo postal perdido o abierto	x	x	
Eliminación incorrecta de datos personales en papel		X	
Datos personales enviados por error de forma electrónica o en papel	X		
Datos personales eliminados o destruidos		X	
Abuso de privilegios de acceso por parte de miembro (ejemplo: empleado) para extraer, reenviar o copiar datos personales	X		
Datos personales residuales en dispositivos obsoletos	X		
Publicación no intencionada/autorizada	X		
Envío de correo electrónico a múltiples destinatarios sin copia oculta o en una lista de distribución visible	X		
Dispositivo perdido o robado	x	X	
Ciberincidente: Dispositivo ha sido cifrado / secuestro de la información	x	X	
Ciberincidente: Suplantación de identidad (pishing) / compromiso de cuenta de usuario y administrador	x	X	X
Ciberincidente: Acceso no autorizado a datos personales en un sistema de información y a sea corporativo o de un servicio en Internet	x	x	X
Incidencia técnica	x	x	X
Modificación no autorizada de datos			X
Datos personales mostrados al individuo incorrecto	X		

4.2 CRITERIOS DE VALORACIÓN

Para estimar, desde la perspectiva del afectado, qué riesgo supone para los derechos y libertades de las personas físicas, se establecerán criterios de valoración según los tipos de daños en las tres dimensiones de la seguridad. A continuación, se establecen los criterios de valoración del riesgo para los derechos fundamentales y libertades de las personas físicas:

Naturaleza, sensibilidad y categorías de los datos personales afectados

- Datos de escaso riesgo: datos de contacto, de educación, familiares, profesionales, biográficos
- Datos de comportamiento: localización, tráfico, hábitos y preferencias
- Datos financieros: transacciones, posiciones, ingresos, cuentas, facturas
- Datos sensibles: de salud, biométricos, datos relativos a la vida sexual, etc.

Datos legibles/ilegibles

- Datos protegidos mediante algún sistema de seudonimización (por ejemplo, cifrado o hash).

Volumen de datos personales

- Expresados en cantidad (registros, ficheros, documentos) y/o en periodos de tiempo (una semana, un año, etc.)

Facilidad de identificación de individuos

- La facilidad con la que se puede deducir la identidad de los individuos a partir de los datos involucrados en la brecha.

Severidad de las consecuencias para los individuos

Nivel de severidad	Consecuencias para los interesados
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.)
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.)
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
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

Fuente: AEPD, Guía para la notificación de brechas de datos personales, p. 38.

La AEPD indica que, en caso de no haberse materializado el daño, se deberá estimar esta probabilidad, es decir, la posibilidad de que las consecuencias se materialicen con un nivel de severidad alto o muy alto.

<table>
<tr><td rowspan="4">Probabilidad</td><td>Muy alta</td><td colspan="4" rowspan="3">Obligación de comunicar a los afectados</td></tr>
<tr><td>Alta</td></tr>
<tr><td>Baja</td></tr>
<tr><td>Improbable[2]</td><td colspan="4">Valorar si comunicar a los afectados</td></tr>
<tr><td></td><td></td><td>Baja – Muy limitada</td><td>Media – Limitado</td><td>Alta – Significativo</td><td>Muy alta – Muy significativo</td></tr>
<tr><td></td><td></td><td colspan="4">Severidad (Gravedad del impacto)</td></tr>
</table>

Fuente: AEPD, Guía para la notificación de brechas de datos personales, p. 39.

Será improbable cuando el responsable pueda garantizar que no puede materializarse el daño; y baja, alta y muy alta cuando exista cierta probabilidad de materialización del daño.

Cuando la severidad para las personas afectadas por la brecha de datos personales sea alta o muy alta, el responsable de tratamiento deberá comunicar la brecha de datos personales a los afectados, excepto si puede garantizar que no existe probabilidad de que se materialice el daño. Además, en situaciones de severidad media o daño limitado, cuando la probabilidad de que dicho daño se materialice sea alta o muy alta, también se deberá comunicar a los afectados.

Características especiales de los individuos

- Si afectan a individuos con características especiales o con necesidades especiales.

Número de individuos afectados

[2] El responsable puede garantizar que no existe probabilidad

- Dentro de una escala determinada, por ejemplo, más de 100 individuos.

Características especiales del responsable del tratamiento (de la entidad en sí)

- En base a la actividad de la entidad.

El perfil de los usuarios afectados

- Su posición en la estructura organizativa de la entidad y, en su consecuencia, sus privilegios de acceso a información sensible o confidencial.

El número y tipología de los sistemas afectados

- Se tendrá en cuenta el número de sistemas afectados, así como del tipo de sistemas.

El impacto

El impacto que la brecha puede tener en la organización, desde los puntos de vista de la protección de la información, la prestación de los Servicios, la conformidad legal y/o la imagen pública. Va a estar relacionado con la categoría o criticidad de los servicios afectados y personas afectadas. En este aspecto diferenciamos entre los siguientes impactos:

- Bajo (perjuicio limitado)
- Medio (perjuicio grave)
- Alto (perjuicio muy grave)

Los requerimientos legales y regulatorios

Notificación de la brecha a la autoridad de control y cualquier otra obligación de notificación, comunicación a Fuerzas y Cuerpos de Seguridad del Estado en caso de delito.

Según la evaluación de riesgos realizada sobre la violación de la seguridad de los datos y, atendiendo a los criterios establecidos respecto a quién notificar, se establecen las pautas para la notificación a cada una de las partes interesadas con las que comunicarse.

El Consejo de Transparencia y Protección de Datos de la Junta de Andalucía dispone de un procedimiento para la notificación de una violación de la seguridad de los datos personales a la autoridad de control.

Para la gestión y notificación de incidentes de ciberseguridad el Centro Criptográfico Nacional (CCN-CERT) dispone de la herramienta LUCÍA (Listado Unificado de Coordinación de Incidentes y Amenazas).

La AEPD dispone de la herramienta Comunica-Brecha RGPD para la toma de decisiones en cuanto a la obligación de comunicar una brecha de datos.

4.3 EJEMPLOS PRÁCTICOS PARA SABER SI NOTIFICAR O NO A LA AUTORIDAD DE CONTROL

A) BRECHA DE CONFIDENCIALIDAD

VIOLACIÓN DE LA CONFIDENCIALIDAD		
Escenario de riesgo	**Consecuencias posibles para el interesado**	**Tipo de notificación requerida**
La información filtrada o extraviada se encuentra cifrada o almacenada en formato ininteligible y, por tanto, no podrá ser procesable o utilizada para ninguna finalidad. El dispositivo extraviado es gestionable de forma remota y puede ser borrado. Sería reevaluado como evento o incidencia de privacidad.	No se generan daños al interesado al no poderse tratar los datos afectados	• No se requiere notificación a la Autoridad de Control. • No se requiere notificación al interesado o interesados.
	La información filtrada tiene escaso valor y no permite su explotación de forma maliciosa al no poder localizar a los interesados y generar acciones contra ellos.	• Se requiere notificación a la Autoridad de Control. • No se requiere notificación al interesado o interesados.
La información filtrada o extraviada no se encuentra protegida y podrá ser tratable.	Daño reputacional que afecte a su honor o intimidad. (P.ej. información relacionada con el ámbito familiar, la personalidad, aficiones, etc. que pueda afectar negativamente al afectado en el entorno familiar, social o laboral) (Alto riesgo)	• Se requiere notificación a la Autoridad de Control. • Se requiere notificación al interesado o interesados.
	Daños que impactan en la solvencia patrimonial del afectado. (P.ej. información que permita la suplantación de identidad y la contratación o compra de productos en nombre del afectado o bien la sustracción de dinero, bienes o inmuebles). (Alto riesgo)	• Se requiere notificación a la Autoridad de Control. • Se requiere notificación al interesado o interesados.
	El afectado debe asumir consecuencias judiciales. (P.ej. información relativa a la investigación de posibles infracciones o estado de situación de la gestión del patrimonio) (Alto riesgo)	• Se requiere notificación a la Autoridad de Control. • Se requiere notificación al interesado o interesados.
	Daño a su estado de salud. (P.ej. información relativa a su estado de salud o cualquier otra circunstancia personal que pueda afectar al interesado y causarle consecuencias negativas de carácter físico o psicológico como consecuencia de su revelación (Depresión, ansiedad, estrés, etc.) (Alto riesgo)	• Se requiere notificación a la Autoridad de Control. • Se requiere notificación al interesado o interesados.

B) BRECHA DE INTEGRIDAD

VIOLACIÓN DE LA INTEGRIDAD		
Escenario de riesgo	**Consecuencias posibles para el interesado**	**Tipo de notificación requerida**
La información alterada o modificada dispone de copia de seguridad y se ha garantizado su restauración. Sería reevaluado como evento o incidencia de privacidad.	No se generan daños al interesado al no verse dañados los datos afectados tras aplicar las medidas de contención y recuperación.	• No se requiere notificación a la Autoridad de Control. • No se requiere notificación al interesado o interesados.
La información alterada o modificada no dispone de copia de seguridad, pero se puede reconstruir si vuelve a ser procesada. Sería reevaluado como evento o incidencia de privacidad.	No se generan daños de integridad al interesado al poder volver al estado anterior al incidente. Debe valorarse si se producen daños en disponibilidad por el tiempo en el que los datos no están accesibles.	• No se requiere notificación a la Autoridad de Control por daños en integridad. Deberá evaluarse por daños en disponibilidad. • No se requiere notificación al interesado o interesados.
La información alterada o modificada no dispone de copia o ha sido procesada de forma incorrecta alterando el resultado de los tratamientos realizados sobre el interesado.	Daño reputacional que afecte a su honor o intimidad. (Alto riesgo)	• Se requiere notificación a la Autoridad de Control. • Se requiere notificación al interesado o interesados.
	Daños que impactan en la solvencia patrimonial del afectado. (Alto riesgo)	• Se requiere notificación a la Autoridad de Control. • Se requiere notificación al interesado o interesados.
	El afectado debe asumir consecuencias judiciales (Sanciones, indemnizaciones, embargos, etc). (Alto riesgo)	• Se requiere notificación a la Autoridad de Control. • Se requiere notificación al interesado o interesados.
	Daño a su estado de salud. (Alto riesgo)	• Se requiere notificación a la Autoridad de Control. • Se requiere notificación al interesado o interesados.

C) BRECHA DE DISPONIBILIDAD

VIOLACIÓN DE LA DISPONIBILIDAD		
Escenario de riesgo	**Consecuencias posibles para el interesado**	**Tipo de notificación requerida**
La información no accesible dispone de copia de seguridad y existen planes de contingencia para la vuelta a la normalidad. La duración de la indisponibilidad no afecta a los tratamientos. Sería reevaluado como evento o incidencia de privacidad.	No se generan daños al interesado al no poderse tratar los datos afectados durante el tiempo que dura la indisponibilidad de los datos o los sistemas donde estos se procesan.	• No se requiere notificación a la Autoridad de Control. • No se requiere notificación al interesado o interesados.
La información filtrada o extraviada no es recuperable o su restauración supone un tiempo de indisponibilidad que afecta seriamente al tratamiento necesario.	Daño reputacional que afecte a su honor o intimidad. (Alto riesgo)	• Se requiere notificación a la Autoridad de Control. • Se requiere notificación al interesado o interesados.
	Daños que impactan en la solvencia patrimonial del afectado. (Alto riesgo)	• Se requiere notificación a la Autoridad de Control. • Se requiere notificación al interesado o interesados.
	El afectado debe asumir consecuencias judiciales (Sanciones, indemnizaciones, etc).	• Se requiere notificación a la Autoridad de Control. • Se requiere notificación al interesado o interesados.
	Daño a su estado de salud. (Alto riesgo)	• Se requiere notificación a la Autoridad de Control. • Se requiere notificación al interesado o interesados.

FASE 5 – NOTIFICACIÓN A LAS AUTORIDADES, INTERESADOS Y OTRAS PARTES INTERESADAS

5.1 NOTIFICACIÓN A LA AUTORIDAD DE CONTROL

Siempre que sea probable que la brecha constituya un riesgo para los derechos y libertades de las personas, deberá realizarse sin dilación la notificación al Consejo de Transparencia y Protección de Datos de Andalucía por parte de la Comisión de Seguridad Informática y Protección de Datos.

No es obligatorio notificar todas las brechas de datos personales, dado que el RGPD prevé una excepción a esta obligación cuando, conforme al principio de responsabilidad proactiva, el responsable pueda garantizar que es improbable que la brecha de datos personales entrañe un riesgo para los derechos y libertades de las personas físicas.

La notificación se realizará, a más tardar, **72 horas después de que se haya tenido constancia** de ella y una vez se haya valorado la obligación de tenerla que efectuar por los riesgos que supone.

La AEPD indica[3] que *"El plazo de 72 horas empieza a calcularse desde el instante en que el responsable de tratamiento tenga **constancia** de que el incidente de seguridad **ha afectado a datos personales, incluyendo las horas trascurridas durante fines de semana y días festivos".***

Cuando en el momento de la notificación se disponga de toda la información relevante para la gestión y resolución de la brecha de datos personales, incluida la decisión sobre la comunicación de la brecha a los afectados, se realizará **una notificación de tipo "completa"**, dado que no está previsto que el responsable de tratamiento tenga que aportar información adicional. Alternativamente, cuando en el momento de la notificación no fuese posible cumplir con la obligación de facilitar toda la información necesaria, el RGPD prevé que la información se facilitará de manera gradual, a la mayor brevedad y sin dilación.

En la notificación se deberá incluir, al menos, la siguiente información:

- Describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados

[3] Guía AEPD p. 18.

afectados, y las categorías y el número aproximado de registros de datos personales afectados;

- Comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;
- Describir las posibles consecuencias de la violación de la seguridad de los datos personales;
- Describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.
- Informará sobre la intención o no de notificar a los afectados. Este punto permitirá a la Autoridad de Control valorar si concurre alguna circunstancia que exime de la notificación al afectado o si, por el contrario, se corre un alto riesgo y debe notificarse al afectado.

En caso de que no fuese posible facilitar toda la información en un primer reporte, podrán realizarse notificaciones graduales que incorporen la información requerida según se disponga de ella.

La notificación se realizará conforme a lo dispuesto en el apartado *"Notificación de una violación de la seguridad de los datos personales a la autoridad de control"* que el Consejo de Transparencia y Protección de Datos de Andalucía tiene disponible en su página web: https://www.ctpdandalucia.es/area-de-proteccion-de-datos/notificacion-violacion-la-seguridad-los-datos-personales-a-la-autoridad-control

En el **ANEXO II** se adjunta el **formulario del Consejo de Transparencia y Protección de Datos de Andalucía** para la **comunicación de brechas de seguridad.**

5.2 NOTIFICACIÓN A LOS AFECTADOS

El artículo 34 del RGPD establece que cuando sea probable que la brecha de datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable de tratamiento deberá comunicar la brecha a los afectados sin dilación indebida.

La comunicación se realizará por el Responsable del tratamiento.

No será necesaria la notificación al afectado cuando:

- "*el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado*" [art. 34.3.a) RGPD].
- *"el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado* [art. 34.3.b) RGPD]. Ejemplo, en casos de suplantación de identidad cuando se pueda garantizar el proceso de renovación de credenciales y fuerce a los interesados afectados a establecer una nueva contraseña. La AEPD cita como ejemplos la identificación y puesta en marcha inmediatamente de medidas como la revocación, cancelación o bloqueo de credenciales de acceso o certificados digitales comprometidos, o mediante el restablecimiento de los servicios y copias de seguridad de los datos de forma que no puedan comprometerse otros datos personales.
- "*suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados"* [art. 34.3.c) RGPD]. La Comisión de Seguridad Informática y Protección de Datos valorará si la notificación supone un esfuerzo desproporcionado y, por tanto, se empleará una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados. En este caso, se deberá coordinar el medio de comunicación a utilizar y el contenido del mensaje con el Dpto. Relaciones Institucionales.

La AEPD indica[4] diversos factores a tener en consideración para decidir si se ha de realizar la comunicación a las personas afectadas:

- Cuáles son las obligaciones legales y contractuales.
- Qué riesgos comporta para los derechos y libertades de las personas la pérdida de confidencialidad, integridad o disponibilidad de sus datos personales, de los servicios asociados a dichos datos personales, así como del compromiso de la identidad o

[4] Guía AEPD p. 26

identificación de los interesados. En particular, los perjuicios a sus derechos fundamentales, los daños físicos, daños reputacionales, fraudes, etc.

- Hasta qué punto los daños producidos serán irreversibles, se puede evitar o mitigar los daños inmediatos y los posibles perjuicios posteriores.

En caso de decidir realizar la comunicación a los afectados, esta se realizará sin dilación indebida, una vez se haya notificado la violación a la Autoridad de Control.

La AEPD indica[5] que *"Cualquier dilación en la comunicación a los afectados le resta efectividad, por lo que una comunicación a destiempo puede llegar a tener el mismo efecto que una comunicación no realizada. Por tanto, todo retraso en la comunicación inmediata a los interesados cuando esta sea necesaria ha de justificarse".*

En todo caso, si la comunicación se produce como consecuencia de una orden emitida por la Autoridad de Control, deberá materializarse la comunicación a los afectados sin dilación indebida y comunicar la confirmación de haber ejecutado la orden dentro del plazo de 30 días, salvo que se indique un plazo diferente en la orden.

No obstante, si después del análisis correspondiente se concluye que es necesario comunicar a los interesados, pero se prevé que la comunicación a los interesados puede comprometer el resultado de una investigación en curso, la comunicación podría posponerse siempre bajo la supervisión de la Autoridad de Control.

La comunicación a los afectados describirá, en un lenguaje claro y sencillo, la naturaleza de la violación de privacidad y contendrá, al menos, la siguiente información:

- Nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
- Describir las posibles consecuencias de la violación de la seguridad de los datos personales.
- Describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

[5] Guía AEPD p. 27.

Téngase en cuenta, según señala la AEPD, que "***Una comunicación incompleta*** *(sin el contenido mínimo), de difícil acceso o realizada a las personas incorrectas no es efectiva, por lo que una comunicación en estas condiciones* ***podría llegar a considerarse una comunicación no realizada****".*

5.3 NOTIFICACIÓN A LOS EMPLEADOS, COLABORADORES U OTRAS PARTES INTERESADAS

Cualquier incidente que suponga una violación o brecha de seguridad catalogada como "Crítica" será notificada a los empleados y, en su caso, al encargado de tratamiento si lo hubiera, a colaboradores o terceras personas relacionadas o vinculadas con la actividad, por parte del Responsable del Tratamiento.

Con ello, se pretende que el personal de UAL sea conocedor de los hechos y pueda estar informado de primera mano.

La comunicación se realizará de forma coordinada y simultánea a la realizada a las personas afectadas. La comunicación describirá, en un lenguaje claro y sencillo, la naturaleza de la violación de privacidad, así como el posicionamiento corporativo en relación con la violación ocurrida.

De igual forma, se valorará el envío de una comunicación similar a otras entidades colaboradoras u otras partes interesadas que deban conocer lo sucedido y ser informados por UAL de la violación de privacidad acaecida, así como el posicionamiento corporativo en relación a la violación ocurrida.

FASE 6 - SEGUIMIENTO

Mientras no se tenga constancia fehaciente que la violación de datos ha sido completamente resuelta y que el riesgo para los afectados no ha sido eliminado o reducido a niveles de riesgo residual aceptable, no se podrá cerrar el asunto.

Asimismo, la UAL ha de estar preparada para recibir y atender los posibles requerimientos, órdenes o comunicaciones que la Autoridad de Control pueda realizar en relación con la brecha de datos personales notificada.

La AEPD indica en su Guía[6] que:

- En caso de recibir un requerimiento de información adicional, el responsable de tratamiento deberá atenderlo en el plazo indicado en el requerimiento y remitiendo la información a través de registro electrónico, indicando que se trata de un registro relacionado con un procedimiento en tramitación e indicando el tipo de documento "contestación a requerimiento".
- En caso de recibir una orden de comunicación a los afectados, el responsable de tratamiento dispondrá del plazo indicado en esa orden para confirmar a la Autoridad de Control su ejecución.

La violación de datos personales, en tanto no se clasifique como "definitivamente resuelta", será tratada en las diferentes reuniones que se convoquen en relación con asuntos relacionados con la seguridad de la información.

FASE 7 - LECCIONES APRENDIDAS

Esta fase tiene por objetivo solventar posibles deficiencias en la gestión de incidentes o incorporar mejoras que permitan una mejor respuesta en las siguientes ejecuciones. Debe de servir por tanto para:

- Depurar errores o actualizar información que se haya evidenciado obsoleta.
- Detectar nuevos mecanismos de control que puedan ser necesarios o mejorar los ya existentes.
- Revisar la eficacia del proceso de gestión.
- Analizar la información forense que todavía esté pendiente de procesar y que pueda aportar mejoras.
- Comunicar los resultados del proceso y realizar una valoración final del incidente.

[6] Guía AEPD sobre violaciones de seguridad, p. 25.

ANEXO I. MODELO DE FORMULARIO PARA REGISTRO DE INCIDENTES Y BRECHAS DE SEGURIDAD DE LA INFORMACIÓN

HOJA DE REGISTRO DE INCIDENTES	**Nº _____**
Responsable del tratamiento:	
¿El incidente ha tenido afectación en un encargado de tratamiento? □ Sí □ No	
Nombre de la organización	
Datos de persona de contacto:	
Información adicional:	
Información del incidente	
Fecha/Hora del incidente:	
Fecha/hora de detección:	
Medios de detección del incidente:	
Origen del incidente: □ Interno □ Externo	
¿Se ha comunicado el incidente a la Autoridad de Control? □ Sí □ No	
¿Se ha comunicado el incidente a los afectados? □ Sí □ No	
Persona que realiza la comunicación:	
¿Se ha resuelto el incidente? □ Sí □ No	**Fecha/hora resolución:**
Resumen del incidente:	
Tipología del incidente: □ Confidencialidad □ Integridad □ Disponibilidad	
Categoría de los datos afectados:	
□ Datos básicos □ Credenciales de acceso/identificación □ DNI/NIE/Pasaporte □ Datos de contacto □ Datos económicos/financieros □ Datos de localización □ Otros:	
Datos o informaciones especiales:	
□ Datos de religión o creencia □ Datos de salud □ Datos de opinión política □ Datos de origen racial □ Datos de afiliación sindical □ Datos sobre vida sexual □ Datos genéticos □ Datos biométricos □ Datos sobre condenas e infracciones penales □ Otros:	
Categorías de personas afectadas	
□ Clientes □ Usuarios □ Empleados □ Proveedores □ Potenciales clientes/usuarios □ Suscriptores □ Estudiantes □ Menores □ Personas en riesgo de exclusión □ Pacientes □ Otros:	
Volumen de datos afectados: en nº de registros _____ en nº de afectados _____	

Relación de medidas correctivas y preventivas adoptadas

ANEXO II. FORMULARIO DE NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD DE DATOS PERSONALES

La Junta de Andalucía tiene a disposición de los usuarios el procedimiento de "Notificación de una violación de la seguridad de los datos personales a la autoridad de control" (https://www.juntadeandalucia.es/servicios/sede/tramites/procedimientos/detalle/19261.html) que permite realizar el trámite por internet o presencialmente rellenando el siguiente formulario:

Consejo de Transparencia y Protección de Datos de Andalucía

CONSEJO DE TRANSPARENCIA Y PROTECCIÓN DE DATOS DE ANDALUCÍA

NOTIFICACIÓN

FORMULARIO PARA NOTIFICAR UNA VIOLACIÓN DE SEGURIDAD DE LOS DATOS PERSONALES A LA AUTORIDAD DE CONTROL. (Código de procedimiento: 19261)

☐ **COMPLETA.** Contiene toda la información sobre las causas y efectos de la violación de seguridad, la resolución de la misma y, en su caso, sobre la notificación a interesados, sin que esté previsto aportar más información.

☐ **INICIAL.** La información será complementada posteriormente, de forma única o gradual, conforme se vaya conociendo toda la información sobre las causas y efectos de la violación de seguridad, la resolución de la misma y, en su caso, sobre la notificación a interesados.

☐ **COMPLEMENTARIA.** (Indique la fecha de la notificación inicial: .....)

¿Da por finalizada la remisión de notificaciones complementarias? ☐ SÍ ☐ NO

1. DATOS DEL RESPONSABLE DEL TRATAMIENTO

TIPO:

☐ INSTITUCIÓN AUTONÓMICA
☐ ADMINISTRACIÓN AUTONÓMICA
☐ ENTIDAD DE DERECHO PÚBLICO O PRIVADO DEPENDIENTE DE LA ADMINISTRACIÓN AUTÓNOMICA
☐ OTROS
☐ UNIVERSIDAD DEL SISTEMA UNIVERSITARIO ANDALUZ
☐ ADMINISTRACIÓN LOCAL
☐ ENTIDAD DE DERECHO PÚBLICO O PRIVADO DEPENDIENTE DE LA ADMINISTRACIÓN LOCAL

DENOMINACIÓN DEL ÓRGANISMO O ENTIDAD:							NIF:
DOMICILIO: TIPO DE VÍA:	NOMBRE DE LA VÍA:						
NÚMERO:	LETRA:	KM EN LA VÍA:	BLOQUE:	PORTAL:	ESCALERA:	PLANTA:	PUERTA:
ENTIDAD DE POBLACIÓN:		MUNICIPIO:			PROVINCIA:	PAÍS:	CÓD. POSTAL:
TELÉFONO:	CORREO ELECTRÓNICO:						

2. IDENTIFICACIÓN Y DATOS DE CONTACTO DEL DPD

APELLIDOS Y NOMBRE (1):						SEXO: ☐H ☐M	DNI/NIE/NIF:
DOMICILIO: TIPO DE VÍA:	NOMBRE DE LA VÍA:						
NÚMERO:	LETRA:	KM EN LA VÍA:	BLOQUE:	PORTAL:	ESCALERA:	PLANTA:	PUERTA:
ENTIDAD DE POBLACIÓN:		MUNICIPIO:			PROVINCIA:	PAÍS:	CÓD. POSTAL:
TELÉFONO:	CORREO ELECTRÓNICO:						

(1)Se deberá identificar al DPD, en caso de ser persona física, o a la persona física que representa al DPD o coordina/dirige sus funciones.

3. DATOS DEL ENCARGADO DE TRATAMIENTO (En caso de estar relacionado con la violación de seguridad)

DENOMINACIÓN:							DNI/NIE/NIF:
DOMICILIO: TIPO DE VÍA:	NOMBRE DE LA VÍA:						
NÚMERO:	LETRA:	KM EN LA VÍA:	BLOQUE:	PORTAL:	ESCALERA:	PLANTA:	PUERTA:
ENTIDAD DE POBLACIÓN:		MUNICIPIO:			PROVINCIA:	PAÍS:	CÓD. POSTAL:
TELÉFONO:	CORREO ELECTRÓNICO:						

4. INFORMACIÓN TEMPORAL SOBRE LA VIOLACIÓN DE SEGURIDAD

FECHA DE INICIO:	☐ EXACTA	☐ ESTIMADA	☐ DESCONOCIDA
FECHA DE DETECCIÓN:	☐ EXACTA	☐ ESTIMADA	

MEDIOS DE DETECCIÓN [2]:

JUSTIFICACIÓN DE LA NOTIFICACIÓN TARDÍA (Si se ha realizado pasadas 72 horas desde la detección):

¿ESTÁ RESUELTA EN EL MOMENTO DE LA NOTIFICACIÓN?	☐ SÍ ☐ NO	
EN SU CASO, FECHA DE RESOLUCIÓN:	☐ EXACTA	☐ ESTIMADA

(2) Si para este o para el resto de campos descriptivos le resulta insuficiente el espacio, puede ampliarlo anexando documentación complementaria.

5. DATOS SOBRE LA VIOLACIÓN DE SEGURIDAD (Puede marcarse más de una casilla por apartado)

RESUMEN DEL INCIDENTE:

TIPOLOGÍA:

☐ RELATIVA A LA CONFIDENCIALIDAD (Acceso o difusión no autorizados)	☐ RELATIVA A LA INTEGRIDAD (Modificación no autorizada)	☐ RELATIVA A DISPONIBILIDAD (Desaparición o pérdida)

MEDIO POR EL QUE SE HA MATERIALIZADO:

☐ DISPOSITIVO PERDIDO, ROBADO O DESECHADO	☐ DOCUMENTACIÓN PERDIDA, ROBADA O EN LOCALIZACIÓN INSEGURA	☐ CORREO PERDIDO O ABIERTO
☐ HACKING, MALWARE O PHISHING	☐ ELIMINACIÓN INCORRECTA DE DATOS EN FORMATO PAPEL	☐ DATOS PERSONALES MOSTRADOS A LA PERSONA INCORRECTA
☐ PUBLICACIÓN NO INTENCIONADA	☐ REVELACIÓN VERBAL NO AUTORIZADA DE DATOS PERSONALES	☐ DATOS PERSONALES ENVIADOS POR ERROR
☐ OTROS MEDIOS:		

CONTEXTO:

☐ INTERNO (acción no intencionada)	☐ INTERNO (acción intencionada)	☐ EXTERNO (acción no intencionada)	☐ EXTERNO (acción intencionada)
☐ OTRO:			

MEDIDAS PREVENTIVAS TOMADAS ANTES DE LA VIOLACIÓN DE SEGURIDAD:

6. SOBRE LOS DATOS AFECTADOS (Puede marcarse más de una casilla por apartado)			
DE CONOCERLO, INDIQUE LAS CATEGORÍAS DE LOS DATOS AFECTADOS:			
☐ DATOS BÁSICOS	☐ DNI, NIE y/o PASAPORTE	☐ CREDENCIALES DE ACCESO O IDENTIFICACIÓN	☐ DATOS DE CONTACTO
☐ DATOS DE PERFILES	☐ SOBRE CONDENAS E INFRACCIONES PENALES	☐ DATOS ECONÓMICOS O FINANCIEROS	☐ DATOS DE LOCALIZACIÓN
☐ OTRO:			
DE CONOCERLO INDIQUE LAS CATEGORÍAS ESPECIALES DE DATOS AFECTADOS:			
☐ ORIGEN ÉTNICO O RACIAL	☐ OPINIONES POLÍTICAS	☐ CONVICCIONES RELIGIOSAS O FILOSÓFICAS	☐ AFILIACIÓN SINDICAL
☐ DATOS BIOMÉTRICOS	☐ DATOS GENÉTICOS	☐ DATOS RELATIVOS A LA SALUD	☐ DATOS RELATIVOS A LA VIDA SEXUAL U ORIENTACIÓN SEXUAL
☐ OTRO:			
INDIQUE, SI ES POSIBLE, EL NÚMERO APROXIMADO O EL RANGO DE REGISTROS DE DATOS PERSONALES AFECTADOS:			

7. SOBRE LAS PERSONAS AFECTADAS (Puede marcarse más de una casilla por apartado)			
DE CONOCERLO INDIQUE LAS CATEGORÍAS ESPECIALES DE DATOS AFECTADOS:			
☐ CLIENTES	☐ ESTUDIANTES	☐ USUARIOS	☐ PACIENTES
☐ EMPLEADOS	☐ SUSCRIPTORES	☐ MENORES	☐ PERSONAS ESPECIALMENTE VULNERABLES
☐ OTRO:			
INDIQUE, SI ES POSIBLE, EL NÚMERO APROXIMADO O EL RANGO DE PERSONAS AFECTADAS:			

8. POSIBLES CONSECUENCIAS DE LA VIOLACIÓN DE SEGURIDAD (Puede marcarse más de una casilla por apartado)		
SOBRE LA CONFIDENCIALIDAD:		
☐ DIVULGACIÓN A TERCEROS/DIFUSIÓN EN INTERNET	☐ UTILIZACIÓN DE DATOS PARA OTROS FINES	☐ ALIMENTACIÓN DE OTRAS BASES DE DATOS
☐ OTRAS:		
SOBRE LA INTEGRIDAD:		
☐ LOS DATOS HAN SIDO MODIFICADOS, SIN CONOCER CON QUÉ FINALIDAD	☐ LOS DATOS HAN SIDO MODIFICADOS Y HAN QUEDADO INSERVIBLES O IRRECUPERABLES	☐ LOS DATOS HAN SIDO MODIFICADOS Y UTILIZADOS INDEBIDAMENTE
☐ OTRAS:		
SOBRE LA DISPONIBILIDAD:		
☐ IMPOSIBILIDAD DE LA PRESTACIÓN DE UN SERVICIO A LOS INTERESADOS	☐ DETERIORO DE LA PRESTACIÓN DE UN SERVICIO A LOS INTERESADOS	
☐ OTRAS:		
NATURALEZA SOBRE EL IMPACTO POTENCIAL SOBRE LOS AFECTADOS:		
☐ PÉRDIDA DE CONTROL SOBRE SUS DATOS	☐ LIMITACIÓN DE SUS DERECHOS	☐ DISCRIMINACIÓN
☐ USURPACIÓN DE IDENTIDAD	☐ FRAUDE	☐ PÉRDIDAS FINANCIERAS
☐ REIDENTIFICACIÓN NO AUTORIZADA	☐ PÉRDIDA DE SECRETO PROFESIONAL	☐ DAÑOS A LA REPUTACIÓN
☐ OTRAS:		
SEVERIDAD DE LAS CONSECUENCIAS PARA LOS AFECTADOS:		
☐ BAJA	☐ MEDIA	☐ ALTA	☐ MUY ALTA
MEDIDAS TOMADAS PARA SOLUCIONAR LA BRECHA Y MINIMIZAR EL IMPACTO SOBRE LOS AFECTADOS:		

9. COMUNICACIÓN A LOS INTERESADOS

¿SE HA COMUNICADO LA VIOLACIÓN DE SEGURIDAD A LOS INTERESADOS?

☐ SÍ [3] ☐ NO, PERO SE LE COMUNICARÁ ☐ NO SE LE VA A COMUNICAR ☐ PENDIENTE DE DECIDIR

EN SU CASO, FECHA EN LA QUE SE INFORMÓ O SE TIENE PREVISTO INFORMAR: .....

EN SU CASO, NÚMERO DE PERSONAS A LAS QUE SE INFORMÓ O SE TIENE PREVISTO INFORMAR: .....

EN SU CASO, MEDIOS O HERRAMIENTAS PARA LA COMUNICACIÓN: .....

EN SU CASO, JUSTIFICACIÓN PARA NO INFORMAR O POR QUÉ AÚN NO SE HA INFORMADO:

(3) En su caso, anexe a esta notificación copia del modelo de comunicación realizada a los interesados.

10. OTRAS NOTIFICACIONES REALIZADAS Y OTROS ÁMBITOS AFECTADOS

¿SE HA COMUNICADO LA VIOLACIÓN DE SEGURIDAD A OTRA AUTORIDAD DE CONTROL O ENTIDAD CON COMPETENCIAS AL RESPECTO?

☐ SÍ ¿A CUÁL?

☐ NO

SI EXISTEN OTRAS COMUNIDADES AUTÓNOMAS O PAÍSES DE LA UNIÓN EUROPEA AFECTADOS POR LA VIOLACIÓN, INDÍQUELOS:

11. DOCUMENTACIÓN QUE SE ADJUNTA

Presento la siguiente documentación:

☐ .....

☐ .....

☐ .....

DOCUMENTOS EN PODER DE LA ADMINISTRACIÓN DE LA JUNTA DE ANDALUCÍA

Ejerzo el derecho a no presentar los siguientes documentos que obran en poder de la Administración de la Junta de Andalucía o de sus Agencias, e indico a continuación la información necesaria para que puedan ser recabados:

	Documento	Consejería/Agencia y Órgano	Fecha de emisión o presentación	Procedimiento en el que se emitió o en el que se presentó
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

DOCUMENTOS EN PODER DE OTRAS ADMINISTRACIONES

Ejerzo el derecho a no presentar los siguientes documentos que obran en poder de otras Administraciones Públicas, e indico a continuación la información necesaria para que puedan ser recabados:

	Documento	Administración Pública y Órgano	Fecha de emisión o presentación	Procedimiento en el que se emitió o en el que se presentó
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

12. DATOS DE LA PERSONA QUE REALIZA LA COMUNICACIÓN

APELLIDOS Y NOMBRE :	SEXO: ☐H ☐M	DNI/NIE/NIF:

CARGO, PUESTO DE TRABAJO O RELACIÓN DE LA PERSONA QUE REALIZA LA COMUNICACIÓN CON EL ORGANISMO O ENTIDAD:

TELÉFONO:	CORREO ELECTRÓNICO:

13. PRESENTACIÓN, LUGAR, FECHA Y FIRMA

PRESENTO la presente notificación, solicitando su admisión por parte del Consejo de Transparencia y Protección de Datos de Andalucía, y **DECLARO** que son ciertos los datos consignados en ella y la documentación que se adjunta a la misma, así como que he leído la información sobre protección de datos personales que figura en el formulario y que se ha informado al DPD y a los responsables del tratamiento la realización de la presente notificación.

En ..... a ..... de ..... de .....

LA PERSONA QUE REALIZA LA COMUNICACIÓN

Fdo.: .....

CONSEJO DE TRANSPARENCIA Y PROTECCIÓN DE DATOS DE ANDALUCÍA.

Código Directorio Común de Unidades Orgánicas y Oficinas: ☐☐☐☐☐☐☐☐☐☐

INFORMACIÓN BÁSICA SOBRE PROTECCIÓN DE DATOS

En cumplimiento de lo dispuesto en el Reglamento General de Protección de Datos, le informamos que:

a) El Responsable del tratamiento de sus datos personales es el Consejo de Transparencia y Protección de Datos de Andalucía cuya dirección es Conde de Ibarra, 18. 41004 – Sevilla. ctpdandalucia@juntadeandalucia.es

b) Podrá contactar con el Delegado de Protección de Datos en la dirección electrónica dpd.ctpda@juntadeandalucia.es, consecuencia de lo establecido en la Ley 1/2014, de Transparencia Pública de Andalucía, el Reglamento (UE) 2016/679 General de Protección de datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

c) Los datos personales que nos indica se incorporan a la actividad de tratamiento Gestión de las notificaciones de violaciones de seguridad, con la finalidad de gestionar, evaluar y realizar el seguimiento de las notificaciones de violaciones de seguridad realizadas por los responsables de tratamientos, de acuerdo con el artículo 33 del Reglamento General de Protección de Datos; la licitud de dicho tratamiento se basa en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento y de una obligación legal aplicable al responsable del tratamiento, consecuencia de lo establecido en el artículo 6.1.c) y e) Reglamento (UE) 2016/679 General de Protección de datos y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

d) Puede usted ejercer sus derechos de acceso, rectificación, supresión, portabilidad de sus datos, y la limitación u oposición a su tratamiento y a no ser objeto de decisiones individuales automatizadas, como se explica en la siguiente dirección electrónica: https://www.ctpdandalucia.es/datos personales, donde podrá encontrar el formulario recomendado para su ejercicio.

e) El Consejo de Transparencia y Protección de Datos de Andalucía contempla la cesión de datos a organismos competentes en seguridad, como fuerzas y cuerpos de seguridad del estado, a otras autoridades de control en materia de protección de datos personales en la Unión Europea, al Comité Europeo de Protección de Datos, a equipos de respuesta ante emergencias informáticas (CERT) o a otras autoridades públicas previstas legalmente.

La información adicional detallada, así como el formulario para la reclamación y/o ejercicio de derechos se encuentra disponible en la siguiente dirección electrónica: https://www.ctpdandalucia.es/datospersonales.