GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

MATINAL IVAP

GESTIÓN DE BRECHAS DE DATOS PERSONALES(*)

19 de Octubre 2023

(*) Incidente de seguridad que afecta a datos personales

Índice de contenidos

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

NORMATIVA

Normativa

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

- **REGLAMENTO (UE) 2016/679** del Parlamento Europeo y del Consejo de Europa, de 27 de abril de 2016 relativo a la protección de las personas físicas en cuanto 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)
  - Directamente aplicable
  - Vigente desde mayo de 2016, plenamente exigible desde el 25 de mayo de 2018

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

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

- Autoridad de control de ámbito estatal: Agencia Española de Protección de Datos (*AEPD*).

Reglamento General de Protección de Dades - RGPD

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

Objeto:

- establece las normas relativas a la protección de las **personas físicas (*derechos y libertades*)** en cuanto al *tratamiento de los datos personales* y las *normas relativas a la libre circulación de tales datos*.
- El RGPD es una norma **directamente aplicable**, que no requiere de normas internas de trasposición ni tampoco, en la mayoría de los casos, de normas de desarrollo o aplicación.

Ámbito de aplicación:

- El presente Reglamento se aplica:
  - al tratamiento **total o parcialmente automatizado** de datos personales,
  - así como al tratamiento **no automatizado** de datos personales **contenidos** o **destinados a ser incluidos en un fichero.**
- No se aplica:
  - A las personas **jurídicas**, ni a las personas físicas **fallecidas**, ni al ejercicio de **actividades** exclusivamente **personales o domésticas**

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

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

La presente ley orgánica tiene por **objecto**:

a) **Adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679** y completar sus disposiciones.

El derecho fundamental de las personas físicas a la protección de datos personales, amparado por el **artículo 18.4 de la Constitución**, se ejercerá con arreglo al que se establece en el Reglamento (UE) 2016/679 y en esta ley orgánica.

b) **Garantizar los derechos digitales de la ciudadanía** conforme al mandato establecido en el artículo 18.4 de la Constitución.

Por ejemplo, el **RGPD** establece en su **artículo 8** "*Los Estados miembros podrán establecer por ley una edad inferior en tales fines (otorgar consentimiento a los dieciséis años), siempre que ésta no sea inferior a 13 años.*" y el **artículo 7 de la LOPDGDD** dictamina "***El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años***"

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

CONCEPTOS BASICOS

Conceptos básicos (art.4 RGPD)

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

«***Dato de carácter personal***»: ***Toda información sobre una persona física identificada o identificable*** (« el interesado»); Se considerará persona física identificable toda persona **cuya identidad pueda determinarse, directa o indirectamente**. En particular, mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de esta persona.

Ejemplos:

- ***Nombre y apellidos, NIF, Número de teléfono, Dirección IP de un dispositivo electrónico, Matrícula de vehículos, Registros de imagen o de voz de una persona, Número de expediente, Identificador de matrícula***
- ***Edad, Sexo, Municipio: si esa combinación identifica a una persona***
- ***Caso clínico específico***

Conceptos básicos (art.4 RGPD)

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

«***Categorías especiales de datos***»: **los datos personales que revelan el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.**

Ejemplos:

- ***Gestión de Recursos Humanos: datos afiliación sindical***
- ***Centros de salud y Hospitales: datos de salud***
- ***Gestión de Subvenciones: situaciones de especial vulnerabilidad (menores, víctimas de violencia de género, riesgo de exclusión…)***

Consulta AEPD 149/2019, N/REF 054388/2019 https://www.aepd.es/es/documento/2019-0149.pdf, que señala lo siguiente:

"*analizado el contexto, los riesgos y la afección a los derechos y libertades del titular de los datos, pueda incluirse en dichas categorías (especiales) información de diversa índole para otorgar la protección especial que se requiera en cada caso.*"

Conceptos básicos (art.4 RGPD)

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

«***Tratamiento***»: Cualquier **operación o conjunto de operaciones realizadas sobre datos personales** o conjuntos de datos personales, **ya sea por procedimientos automatizados o no**, como la recogida, grabación, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, confrontación o interconexionado, limitación, supresión o destrucción.

- ***Ejemplos de tratamientos en la Generalitat:***
  - ***Gestión de ayudas y subvenciones***
  - ***Divulgación de boletines y revistas***
  - ***Registro de entrada y salida***
  - ***Videovigilancia***
  - ***Gestión de ciudadanos en la sede electrónica***

¿Qué no seria un tratamiento de datos? *elaboración presupuestaria, mapas cartográficos…*

Conceptos básicos (art.4 RGPD)

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

«***Responsable del tratamiento***»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, **determine los fines y medios del tratamiento**;

Ejemplos:

- ***Ayuntamiento, Conselleria, Entidad del sector público, Diputación, Ministerio, etc.***
- ***En la GVA, cada conselleria y cada entidad del SPI***

«***Encargado del tratamiento***»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales **por cuenta del responsable** del tratamiento;

Ejemplos:

*Empresa, Entidad del sector público, incluso podrán atribuirse las competencias propias de un encargado a un determinado órgano de una administración pública, o un departamento del responsable, mediante la adopción de una norma reguladora de dichas competencias, que tendrá que incorporar el contenido exigido por el **artículo 28.3 del RGPD** (**encargo de tratamiento**).*

DGTIC

Conceptos básicos (art.4 RGPD)

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

***Artículo 28.3 RGPD**:*

*"El tratamiento por el encargado se regirá por un **contrato u otro acto jurídico (menor, convenio, encomienda de gestión)** con arreglo al Derecho de la Unión o de los Estados miembros, que **vincule al encargado respecto del responsable** y establezca:*

- *el objeto,*
- *la duración,*
- *la naturaleza y la finalidad del tratamiento,*
- *el tipo de datos personales y categorías de interesados,*
- *a elección del responsable, suprimirá o retornará todos los datos personales una vez finalice la prestación de los servicios de tratamiento*
- *i las obligaciones y derechos del responsable".*

PLIEGO PRESCRIPCIONES ADMINISTRATIVAS o TÉCNICAS

Conceptos básicos (art.4 RGPD)

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

DECRETO 133/2023, de 10 de agosto, del Consell, de aprobación del Reglamento orgánico y funcional de la Conselleria de Hacienda, Economía y Administración Pública

Disposiciones adicionales.

Tercera. Condiciones de actuación de la DGTIC en su condición de encargada de tratamiento de datos personales.

La DGTIC, de conformidad con lo establecido en el ***Decreto 80/2020, de 24 de julio, del Consell****, de atribución al centro directivo con competencias horizontales en tecnologías de la información y las comunicaciones, tiene el encargo del tratamiento de datos personales de los departamentos y los organismos autónomos de la Administración de la Generalitat.*

En el ejercicio de sus atribuciones, la Dirección General de Tecnologías de la Información y las Comunicaciones ***actuará como encargada de los tratamientos de datos personales que efectúan las consellerias y sus organismos autónomos como responsables del tratamiento en el ámbito de sus competencias.***

Asimismo, la DGTIC ***podrá recurrir a otro encargado del tratamiento, debiendo cumplir con lo estipulado en los apartados 2 y 4 del artículo 28 del Reglamento (UE) 2016/679****, del Parlamento Europeo y del Consell 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*

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

OBLIGACIONES DEL RESPONSABLE PARA VELAR POR LOS DERECHOS Y LIBERTADES DE LAS PERSONAS FÍSICAS

Obligaciones del responsable

El **RGPD** establece un conjunto de **obligaciones para el responsable** del tratamiento que vaya a llevarse a cabo, entre ellas las que se recogen en los siguientes artículos:

- ***Art. 24 Responsabilidades del responsable del tratamiento***
- ***Art. 25 Protección de datos desde el diseño y por defecto***
- ***Art. 32 Seguridad del tratamiento***
- ***Art. 35 Evaluación de impacto relativa a la protección de datos***

Obligaciones del responsable (art.24, 25 y 32)

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

Teniendo en cuenta:

- *El **estado** de la técnica, el **coste** de su aplicación*
- *TRATAMIENTO* (**naturaleza**, **ámbito, alcance**, **contexto**, **fines**)
- ***RIESGOS*** de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas

El **responsable** deberá:

Aplicar:

- en el *momento de determinar los medios*
- en el *propio tratamiento*

MEDIDAS *apropiadas*:

- *TÉCNICAS*
- *ORGANIZATIVAS*

Para garantizar un NIVEL de SEGURIDAD adecuado al RIESGO que existe y así se GARANTICEN los derechos y libertades de las personas afectadas por el tratamiento

Análisis de Riesgos

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

ANÁLISIS DE RIESGOS:

Proceso mediante el cual el responsable **identificará las amenazas** de su tratamiento y **optará por las medidas técnicas y organizativas más apropiadas** para **disminuir los riesgo** que puede suponer para sus derechos y libertades, tratar los datos de las personas afectadas.

Se estructura en las siguientes fases:

Una vez establecido el **nivel de riesgo**, y aunque este sea escaso, se deben establecer, las **medidas más apropiadas para minimizar dicho riesgo.**

Análisis de Riesgos

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

Tal como establece la LOPDGDD en su artículo 28:

2. *Para la adopción de las medidas a que se refiere el apartado anterior, los responsables y encargados del tratamiento tendrán en cuenta, en particular, los* ***mayores riesgos que podrían producirse*** *en los siguientes supuestos, cuando el tratamiento:*

- *pudiera generar* ***situaciones de discriminación***, ***usurpación de identidad o fraude***, ***pérdidas financieras***, *afectara a la* ***reputación***, ***pérdida de confidencialidad***, *etc.*
- *pudiera* ***privar*** *a los afectados de sus* ***derechos y libertades*** *o pudiera* ***impedirlos el ejercicio del control*** *sobre sus datos personales*
- *afectara a* ***categorías especiales de datos***
- *implicara una evaluación de aspectos personales de los afectados con el fin de* ***crear o utilizar perfiles personales*** *de estos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos*
- *utilizara datos de* ***grupos de afectados en situación de especial vulnerabilidad*** *y, en particular, de* ***menores de edad y personas con discapacidad.***
- *supusiera un* ***tratamiento masivo*** *que implica a un gran número de afectados o conlleva la recogida de una gran cantidad de datos personales.*

Análisis de Riesgos y Evaluación de Impacto

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

- Las **medidas** pueden ser **cualquier cosa**, **método o medio que el responsable pueda emplear;** desde la aplicación de soluciones técnicas avanzadas hasta la formación básica del personal, ***por ejemplo:***
  - ***la seudonimización de los datos personales***
  - ***disponer de sistemas de detección de programas maliciosos;***
  - ***establecer sistemas de gestión de la privacidad y la seguridad de la información;***
  - ***obligar contractualmente a los encargados del tratamiento a adoptar prácticas específicas de minimización de datos***
  - ***cerrar bajo llave documentación sensible (…)***
- Si se da el caso de que realizar un determinado tratamiento conlleva un **RIESGO ALTO** para los derechos y libertades de las personas afectadas, lo que se realizará además del ***AARR*** es un proceso que se identifica como **EVALUACIÓN DE IMPACTO EN PROTECCIÓN DE DATOS.**
- Este proceso también incluye la realización de un **ANALISIS DE RIESGOS**, pero incluye otras fases para **analizar el tratamiento a un mayor nivel de detalle** y así disponer de más conocimiento sobre el mismo. De este modo permite tanto **identificar mejor los riesgos** susceptibles de que se produzcan, como **elegir el conjunto de medidas** más apropiadas que ayude a minimizar dicho riesgo.

Medidas de Seguridad en los tratamientos

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

"***Disposición adicional primera-Medidas de Seguridad en el ámbito del sector público. (LOPDGDD)***

*1. El **Esquema Nacional de Seguridad**(*) incluirá las **medidas que deban implantarse** en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679*

*2. Los **responsables** enumerados en el artículo 77.1 (incluye las administraciones autonómicas) de esta ley orgánica **deberán aplicar a los tratamientos de datos personales las medidas de seguridad** que correspondan de las previstas en el Esquema Nacional de Seguridad(*).*

*En los casos en los que **un tercero preste un servicio** en régimen de concesión, encomienda de gestión o contrato, las **medidas de seguridad se corresponderán** con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad.“*

Las medidas del ENS a aplicar dependerán del nivel de riesgo resultante del AARR

(*) ***Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.***

ENS – Cumplimiento RD 311/2022 (I)

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

Artículo 2. Ámbito de aplicación.

Los pliegos de prescripciones administrativas o técnicas de los contratos que celebren las entidades del sector público incluidas en el ámbito de aplicación de este real decreto contemplarán todos aquellos requisitos necesarios para **asegurar la conformidad con el ENS de los sistemas de información en los que se sustenten los servicios prestados por los contratistas, tales como la presentación de las correspondientes Declaraciones o Certificaciones de Conformidad con el ENS**. Esta cautela se extenderá también a la cadena de suministro de dichos contratistas, en la medida que sea necesario y de acuerdo con los resultados del correspondiente análisis de riesgos.

ENS – Cumplimiento RD 311/2022 (II)

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

Artículo 38. Procedimientos de determinación de la conformidad con el Esquema Nacional de Seguridad.

1. Los sistemas de información comprendidos en el ámbito del artículo 2 serán objeto de un proceso para determinar su conformidad con el ENS. A tal efecto, **los sistemas de categoría MEDIA o ALTA precisarán de una auditoría para la certificación de su conformidad**, sin perjuicio de la auditoría de la seguridad prevista en el artículo 31 que podrá servir asimismo para los fines de la certificación, mientras que **los sistemas de categoría BÁSICA solo requerirán de una autoevaluación para su declaración de la conformidad**, sin perjuicio de que se puedan someter igualmente a una auditoria de certificación.

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

- Tanto si sólo hemos tenido que realizar el **AARR**, como si también hemos realizado una **EIPD**, debemos tener en cuenta que el ***riesgo 0/nulo NO EXISTE***.

- Sólo por llevar a cabo un tratamiento de datos personales existe un ***riesgo inherente***, que es el que perseguimos disminuir hasta un nivel de ***riesgo residual***, que sea admisible.

- Aunque consideremos que hemos aplicado todas las medidas posibles para evitar que se produzca cualquier incidente que pueda afectar a los derechos y libertades de las personas, debemos contar con que **en algún momento se producirá algún tipo de incidente sobre los datos personales**.

- Así es como nos encontramos con que se ha producido una **BRECHA DE DATOS PERSONALES** en nuestro tratamiento. Debemos estar preparados para actuar con diligencia.

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

BRECHAS DE DATOS PERSONALES

Brecha de datos personales

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

Concepto básico del RGPD:

«***violación de la seguridad de los datos personales***»*:* toda violación de la seguridad que ocasione

- la destrucción, pérdida o alteración accidental o ilícita de datos personales
  - transmitidos, conservados o tratados de otra forma,
    - la comunicación o acceso no autorizados a dichos datos;

Se están afectando las dimensiones: ***integridad, disponibilidad, confidencialidad***

La Agencia Española de Protección de Datos ha elaborado una "**Guía para notificación de brechas de datos personales**", en la que asigna el mismo significado a este conjunto de términos:

- "*violación de la seguridad de los datos personales*",
  - "*brecha de seguridad de los datos personales*",
    - "*brecha de seguridad*",
      - "*quiebra de seguridad*"
        - "*quiebra de seguridad de los datos personales*",
          - "***brecha de datos personales***" o simplemente "***brecha***".

Brecha de datos personales

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

Es importante **distinguir entre *incidente de seguridad* y *brecha***. No tendrán consideración de brecha aquellos incidentes que:

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

Por ejemplo **no pueden considerarse brechas:**

- el mero hecho de recibir correos electrónicos con malware o sospechosos de malware sin haberlo ejecutado
- detectar un sistema infectado con un virus
- sufrir un intento de ciberataque sin que se llegue a materializar

No obstante, **deben ser gestionadas como *incidentes de seguridad***

Brecha de datos personales

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

Ejemplos de brechas acontecidas en la GVA/SPI:

DESCRIPCIÓN BRECHA	NOTIFICACIÓN AEPD	NOTIFICACIÓN INTERESADOS
Archivo de documentación errónea en carpeta ciudadana		
Se publican datos personales no necesarios en un proceso selectivo de personal		
Pérdida por un funcionario instructor de un expediente disciplinario del CD con la documentación fuera de las dependencias de conselleria		
Remisión correo electrónico a ciudadan@s sin ocultar las direcciones de los destinatarios (Para en lugar de CCO)		
Pérdida o robo de un móvil en consulta hospital utilizada por un IP con datos identificativos y de contacto de las personas que participan en un ensayo clínico		
Recepción avisos de un tercero en una app personal, siendo que se ha dado de baja		
Duplicidad código CSV en resoluciones GVA		

Brechas de datos personales y seguridad en los tratamientos

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

Al implementar un tratamiento **se debe tener en cuenta** que:

- La **existencia del tratamiento** ya supone en sí mismo un **riesgo** para los derechos y libertades de las personas afectadas (*publicación listado admitidos en un proceso de selección, y una persona interesada se encuentra en una situación vulnerable*),
- Además será **obligatorio determinar también el riesgo** que para esos mismos derechos y libertades puede suponer el que **se materialice una brecha** de datos personales (*un tratamiento no autorizado o accidental sobre los datos).* Hay que **determinar el impacto** que podría tener un incidente que afectara al sistema de información, tanto con relación a:
  - la **materialización** de ataques, intrusiones o cualquier tipo de **proceso no autorizado**.
  - para el caso de **incidentes accidentales**, tanto tecnológicos como humanos, y los asociados a **eventos naturales**
  - cuando el **tratamiento no fuera automatizado**
- Por tanto, ***las medidas de mitigación han de estar orientadas a reducir las consecuencias que puede tener para las personas afectadas que se produzca una brechas de datos personales.***

Brechas de datos personales y seguridad en los tratamientos

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

https://www.youtube.com/watch?v=vTEs11IdvYE

https://www.aepd.es/prensa-y-comunicacion/blog/brechas-de-seguridad-el-top-5-de-las-medidas-tecnicas-que-debes-tener-en

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

GESTION DE BRECHAS DE DATOS PERSONALES

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

Ante cualquier suceso que pueda tener **consecuencias negativas para los derechos y libertades de los interesados**, el responsable de tratamiento ha de **reaccionar y mitigar dichas consecuencias**.

El proceso de **GESTIÓN DE BRECHAS** debe formar parte de la ***POLÍTICA DE PROTECCIÓN DE DATOS*** de la organización:

- Es un proceso que, con mayor o menor grado de madurez, **debe formar parte de la cultura de responsables y encargados** de tratamientos.
- Debe **actualizarse periódicamente y revisar/incorporar los procedimientos** para responder a las obligaciones que se desprenden del RGPD.
- En nuestro caso, las brechas **deberán ser puestas en conocimiento de la Delegación de Protección de Datos** por parte del **responsable/encargado** del tratamiento afectado, que actuará como intermediario entre la AEPD y el responsable/encargado.

Figuras implicadas en la gestión de brechas

Detectada una brecha de datos personales en la organización, y a efectos de una correcta y eficaz gestión, será **necesaria la colaboración y actuación de distintos intervinientes**:

RESPONSABLE DEL TRATAMIENTO:

- deberá **garantizar que se notifica la brecha** de datos personales a la autoridad competente sin dilación indebida
- también que **se comunicará la brecha de datos personales a los afectados** cuando sea necesario.
- deberá contar con el **asesoramiento del delegado de protección de datos**
- podrá contar con el **asesoramiento de expertos en materia de seguridad**
- puede **delegar en el encargado la gestión** de la brecha de datos personales, **si así consta en el encargo**, pero no olvidar que es su responsabilidad teniendo en cuenta que la delegación de funciones no implica delegación de responsabilidad.

Figuras implicadas en la gestión de brechas

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

ENCARGADO DEL TRATAMIENTO:

- le corresponde **informar al responsable** de tratamiento **sin dilación indebida** *(no se determina un plazo máximo exacto)* de las brechas de datos personales que afecten a los tratamientos encargados
- tiene la obligación de **ayudar al responsable a garantizar el cumplimiento de las obligaciones establecidas en el RGPD**, incluyendo la gestión, notificación y comunicación de las brechas de datos personales, si así se ha establecido en el *ENCARGO*
- La información al responsable de tratamiento **debe incluir los detalles necesarios para que el responsable pueda cumplir con sus obligaciones**, en particular la de evaluar el riesgo de la brecha de datos personales y en su caso notificarla a la Autoridad de Control y/o comunicar a los afectados.

Figuras implicadas en la gestión de brechas

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

DELEGADO DE PROTECCIÓN DE DATOS:

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

No obstante, la **responsabilidad** recae ineludiblemente en el **responsable** y **encargado** de tratamiento respecto de las obligaciones de cada uno de ellos.

Figuras implicadas en la gestión de brechas

GENERALITAT VALENCIANA

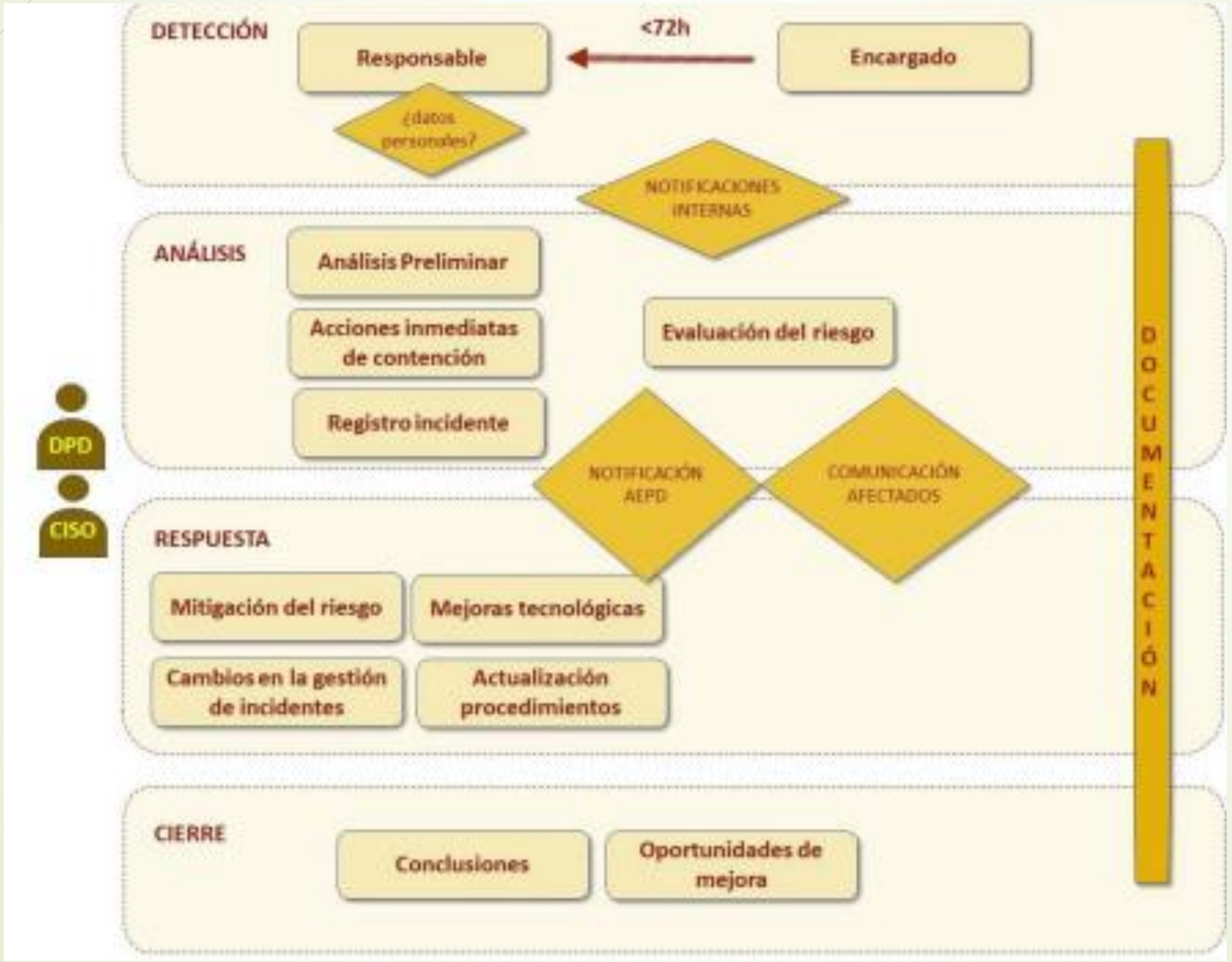
Delegació de Protecció Dades GVA

Figura	Funciones y responsabilidades
Responsable	• Implantación del proceso de gestión de brechas • Evaluación de las consecuencias para los derechos y libertades de las personas • Notificar la brecha de datos personales a la Autoridad de Control • Comunicar la brecha de datos personales a las personas afectadas
Encargado	• Informar al responsable de las brechas de datos personales que afecten a los tratamientos encargados • Ayudar al responsable en la gestión de la brecha de datos personales • Ejecutar las labores de notificación o comunicación de la brecha que tenga asignadas por contrato
Delegado de protección de datos	• Informar y asesorar al responsable/encargado del tratamiento sobre sus obligaciones y responsabilidades con relación a las brechas de datos personales • Cooperar con la Autoridad de Control en las cuestiones relativas a la gestión de la brecha de datos personales • Actuar como punto de contacto con la Autoridad de Control, en particular, en el proceso de notificación de la brecha de datos personales

PROCESO DE GESTIÓN DE BRECHAS

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA



GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

NOTIFICACIÓN DE BRECHAS DE DATOS PERSONALES

Artículos 33 y 34 RGPD

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

Artículo 33 Notificación de una violación de la seguridad de los datos personales a la autoridad de control

*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.*

*3. La **notificación** contemplada en el apartado 1 deberá, como mínimo:*

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

*b) 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;*

*c) describir las **posibles consecuencias** de la violación de la seguridad de los datos personales;*

*d) 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**.*

Artículos 33 y 34 RGPD

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

Artículo 33 Notificación de una violación de la seguridad de los datos personales a la autoridad de control (…)

*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.*

Artículos 33 y 34 RGPD

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

Artículo 34 Comunicación de una violación de la seguridad de los datos personales al interesado

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.*

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).

*3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes (****si bien la AEPD siempre podrá exigir que se realice dicha comunicación****):*

a) 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;*

b) 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 a que se refiere el apartado 1;*

c) ***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.*

Notificación de la brecha a la AEPD

(Asesora_brecha)

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

1. **La brecha se notificará** a la AEPD *salvo que el responsable pueda garantizar que es improbable que entrañe un riesgo para los derechos y libertades de las personas afectadas*.

Factores para evaluar el riesgo de una brecha:
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

2. Debe realizarse la **notificación** sin dilación indebida y **a más tardar a las 72 HORAS siguientes**, ***computando también las horas transcurridas durante fines de semana y festivos.*** Los procedimientos de gestión de brechas de responsables y encargados deben concretar el plazo, incluyéndolo incluso en el encargo de tratamiento.

3. Cuando en el momento de la notificación no se dispusiera de toda la información requerida, el RGPD prevé que la **información se facilite de manera gradual,** a la mayor brevedad y sin dilación. En el plazo de las 72 horas la AEPD prevé la posibilidad de realizar una **notificación de tipo INICIAL**.

4. Si se ha realizado este tipo de notificación, **se dispone de 30 DIAS** desde ese momento, **para completar toda la información** mediante una modificación de la notificación anterior generando así una **notificación de tipo COMPLETA**. ***Todos los plazos indicados en días en esta guía deben entenderse como días hábiles***.

5. La **notificación a la AEPD** estamos obligados a realizarla **de forma electrónica**, preferentemente usando el formulario de notificación de brechas de su sede electrónica.

Respuesta de la AEPD a la notificación de la brecha

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

Tras notificar una brecha de datos personales, el **responsable de tratamiento puede recibir por parte de la AEPD** diversas comunicaciones o notificaciones electrónicas, por ejemplo:

- **Comunicación** con información relativa al registro de la brecha de datos personales notificada.
- **Notificación con un requerimiento de información adicional** sobre la brecha de datos personales o el tratamiento de datos personales en cuestión en virtud de las funciones y potestades de esta Agencia a las que refiere el artículo 47 de la LOPDGDD así como el artículo 58 del RGPD.
- **Notificación con una orden para comunicar a los afectados la brecha** de datos personales en virtud del artículo 34.4 al considerar que el riesgo para los afectados es alto, en virtud de las funciones y potestades de esta Agencia a las que refiere el artículo 47 de la LOPDGDD así como el artículo 58 del RGPD.

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.
- 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 Agencia su ejecución** a través del registro electrónico. Con carácter general el plazo para la confirmación será de 30 días, aunque podría acortarse en función del nivel de riesgo.

Comunicación de la brecha a los afectados

El **RGPD no establece un plazo para realizar la comunicación a los afectados** pero si dictamina que sea a la **mayor brevedad posible**. Hay que tener en cuenta que una comunicación a destiempo puede tener el mismo efecto que una comunicación no realizada, por tanto todo retraso deberá justificarse

Factores a tener en consideración para decidir si debe realizarse la comunicación:

- 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 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.

La AEPD proporciona la herramienta **Comunica-Brecha RGPD** que ofrece ayuda a los responsables de tratamiento para la toma de decisiones en cuanto a la obligación de comunicar una brecha de datos personales a los afectados, quienes **en cualquier caso deben documentar las decisiones**.

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

CONTENIDO DE LA NOTIFICACIÓN DE BRECHAS

Contenido de la notificación brecha a la AEPD

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

Formulario de notificación de brechas de la AEPD: **SU CONTENIDO ES:**

A. CARÁCTER DE LA NOTIFICACIÓN:

- Nueva notificación (*Inicial o Completa*)
- Modificación de una brecha de datos personales ya notificada (*Completa*)

B. INFORMACIÓN GENERAL SOBRE EL TRATAMIENTO

- Duración del tratamiento
- Número total de personas cuyos datos forman parte del tratamiento afectado
- Ámbito geográfico del tratamiento (*localidad, provincia, nivel nacional y/o de otro estado miembro*)

C. INTENCIONALIDAD Y ORIGEN

- Intencionalidad de la brecha (*intencionado o accidental/fortuito*)
- Origen o ámbito de la brecha (*interno –responsable/encargado- o externo*)

D. TIPOLOGÍA

Afecta a:	Cuando produce una:
Confidencialidad	revelación no autorizada o accidental 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

Contenido de la notificación brecha a la AEPD

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

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		

Contenido de la notificación brecha a la AEPD

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

Suceso	Confidencialidad	Disponibilidad	Integridad
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 (phishing) / compromiso de cuenta de usuario o administrador	X	X	X
Ciberincidente: Acceso no autorizado a datos personales en un sistema de información ya 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		

Contenido de la notificación brecha a la AEPD

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

E. CATEGORÍAS DE DATOS Y PERFIL DE LOS AFECTADOS

Categorías de datos	Significado
Datos básicos	Nombre, apellidos o la fecha de nacimiento de los afectados
Datos de contacto	Número de teléfono, email o dirección física de las personas
Imágenes (foto/video)	Imágenes individuales o colectivas de las personas afectada
Documento identificativo	NIF, NIE, pasaporte, número de Seguridad Social o cualquier otro identificador a nivel nacional o extra nacional
Datos económicos o financieros	Datos referidos a nóminas, extractos bancarios, estudios económicos o cualquier otra información que pueda revelar información económica de los afectados
Datos de localización (datos de ubicación de la persona en un determinado momento o durante un periodo de tiempo)	Datos de posicionamiento, coordenadas o direcciones habituales (no residencia) de los afectados
Medios de pago (números de tarjeta o cuenta bancaria)	Información de los afectados referido a métodos de pago como números de tarjeta, cuentas bancarias, métodos de pago online como Paypal, bitcoins, etc.
Credenciales de acceso o identificación	Nombres de usuarios, contraseñas ya estén en claro, hasheadas o cifradas y datos como tarjetas de coordenadas o segundos factores de autenticación
Datos de perfiles	Perfiles de usuarios en redes o datos de perfilado psicosocial o que permitan realizar perfilados de personas físicas

Contenido de la notificación brecha a la AEPD

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

E. CATEGORÍAS DE DATOS Y PERFIL DE LOS AFECTADOS (…)

Categorías de datos	Significado
Sobre la vida sexual	Datos relativos a la salud sexual, hábitos, orientación o tendencias sexuales, así como información que permita inferirlo.
Religión o creencias	Religión que profesan los afectados, así como información sobre posturas religiosas, agnósticas o ateas
Origen racial o étnico	Información que refleje o permitan establecer el origen racial o la pertenencia a una determinada etnia de las personas
Datos de salud de empleados	Información sobre la salud que un responsable trate sobre sus empleados o personas con las que mantiene una relación laboral, como puedan ser partes de baja o informes sanitarios
Datos de salud de pacientes	Referido a la información que los responsables del sector sanitario dispongan de las personas
Opinión política	Información que refleje o permita averiguar la opinión o tendencias políticas de las personas
Datos genéticos	Características genéticas heredadas o adquiridas de una persona física que proporcionen una información única
	sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica
Datos sobre condenas e infracciones penales	Certificados de antecedentes penales o los certificados de delitos de naturaleza sexual
Datos biométricos	Características físicas, fisiológicas o conductuales de una persona física, que permita su identificación
Datos sobre afiliación sindical	Informan sobre la pertenencia o afiliación de una persona a un sindicato

Contenido de la notificación brecha a la AEPD

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

E. CATEGORÍAS DE DATOS Y PERFIL DE LOS AFECTADOS (…)

Perfiles de las personas físicas afectadas
Clientes / ciudadanos
Estudiantes / alumnos
Usuarios
Pacientes
Suscriptores / potenciales clientes
Afiliados / asociados
Fuerzas y Cuerpos de Seguridad del Estado
Empleados
Otros

Hay que tener en cuenta como **agravante del riesgo potencial** si el tratamiento se realiza sobre **datos de personas que pertenecen a un colectivo especialmente vulnerable** (*menores de edad, violencia de género, acoso, situaciones similares)*.

Siempre se debe determinar, aunque sea de forma aproximada, el **número de personas afectadas por la brecha**, teniendo en cuenta que no contabilizan las personas jurídicas. En último extremo se indicará el número total de personas sobre las que se tratan datos.

Contenido de la notificación brecha a la AEPD

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

F. CONSECUENCIAS

Se trata de realizar una valoración de los **riesgos potenciales que podrían padecer las personas afectadas** por la brecha, **en función de los datos** y de las **circunstancias concretas de la brecha**.

Consecuencias para los afectados
Imposibilidad de ejercer algún derecho o acceso a un servicio
Usurpación de la identidad
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

Para determinar el nivel de severidad **debe tenerse en cuenta el daño que se puede producir** si se materializan las consecuencias anteriores

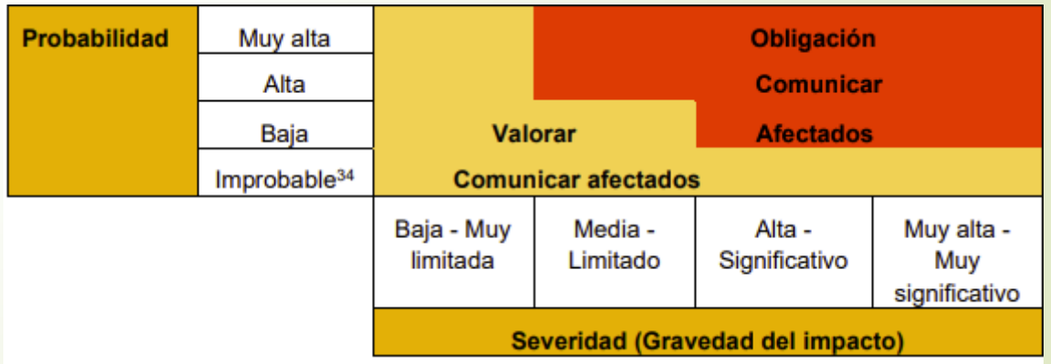
Contenido de la notificación brecha a la AEPD

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

F. CONSECUENCIAS

Nivel de severidad	Consecuencias para los afectados
Muy alta	Las personas pueden enfrentar consecuencias **muy significativas**, o incluso **irreversibles**, que no pueden superar (exclusión o marginación social, dificultades financieras tales como deudas considerables o incapacidad para trabajar, dolencias psicológicas o físicas a largo plazo, muerte, etc.). Daña **derechos fundamentales y libertades públicas** de forma irreversible
Alta	Las personas pueden enfrentar consecuencias **significativas**, que deberían poder superar, aunque con serias dificultades (malversación de fondos, listas negras de los bancos, daños a la propiedad, pérdida de empleo, citación judicial, empeoramiento de la salud, etc.). En general cuando las consecuencias afectan a derechos fundamentales, pero pueden revertirse
Media	Las personas pueden encontrar inconvenientes importantes, produciendo un daño **limitado**, que podrán superar a pesar de algunas dificultades (costos adicionales, denegación de acceso a servicios comerciales, miedo, falta de comprensión, estrés, dolencias físicas menores, etc.)
Baja	Las personas no se verán afectadas o pueden encontrar algunos inconvenientes **muy limitados y reversibles** que superarán sin ningún problema (tiempo de reingreso de información, molestias, irritaciones, etc.)



Contenido de la notificación brecha a la AEPD

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

G. RESUMEN DE LA BRECHA

En este apartado se debe **describir de forma concisa** los hechos acontecidos, así como **cualquier información que se considere relevante** y no se recoja en otros apartados del formulario.

H. INFORMACIÓN TEMPORAL DE LA BRECHA Y MEDIOS DE DETECCIÓN

Los **plazos de detección y resolución** de una brecha junto con los medios de detección **son relevantes** para **determinar el nivel de riesgo** para los derechos y libertades de las personas afectadas. Se informará:

- **Fecha de detección**: el responsable tiene conocimiento de que se ha producido una brecha y establece el inicio de los plazos de notificación a la AEPD y a los afectados
- **Si la fecha de la notificación supera las 72 horas** respecto a la detección existe un **conjunto de supuestos** entre los que se deberá seleccionar el que haya correspondido
- **Medios de detección de la brecha**: **propios** del responsable o encargado, comunicación de un **afectado**, **medios de comunicación**, **tercero ajeno** al tratamiento
- **Fecha de inicio de la brecha**: puede ser exacta o aproximada

Contenido de la notificación brecha a la AEPD

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

I. MEDIDAS DE SEGURIDAD ANTES DEL INCIDENTE

- Medidas de seguridad con las que contaba el tratamiento antes de la brecha: **se ofrecen opciones**
- Indicar si la brecha pudiera haberse evitado adoptando alguna **medida de seguridad adicional**
- Indicar si el **origen** de la brecha es debido a un fallo, deficiencia o incumplimiento de **alguna de las medidas de seguridad implementadas**
- Indicar la **disponibilidad de un análisis de riesgos o evaluación de impacto** en protección de datos documentado que justifique las medidas adoptadas

J. ACCIONES TOMADAS

- Si se ha actualizado el **registro de brechas** con los detalles correspondientes
- Si se han **mejorado y/o adoptado algunas de las medidas** del apartado anterior como nuevas medidas
- Si se han **establecido mejoras en los procedimientos y políticas de seguridad** tras la brecha
- Si se han **denunciado los hechos ante las Autoridades policiales y/o judiciales** competentes por considerarlo constitutivo de delito, o se pretende hacer
- Si el responsable considera que **se han tomado todas las acciones posibles y ha dado por resuelta la brecha**, indicando en que fecha

Contenido de la notificación brecha a la AEPD

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

K. COMUNICACIÓN A LOS AFECTADOS

- Si **se ha comunicado**, **fecha** en la que se realizó, **número de personas** comunicadas y **medio** utilizado
- Si **no lo ha hecho**, pero tiene decidido hacerlo, indicara la **fecha en que tiene previsto hacerlo**, **número** de personas que prevé informar y **medio** que utilizará para la comunicación
- Si **no lo ha hecho ni prevé hacerlo**, se indicarán los **motivos**. Se ofrecen varias opciones: *no hay alto riesgo, supone un esfuerzo desproporcionado, interferiría en una investigación, etc.*

*Para ayudar a la toma de decisión la AEPD proporciona la herramienta **Comunica-RGPD** que asesora al responsable sobre la acción que debe tomar en función de las características de la brecha.*

L. IDENTIFICACIÓN DE LOS INTERVINIENTES EN LA NOTIFICACION DE LA BRECHA

- **Solicitante:** persona física que rellena el formulario de notificación: **personal DPD con certificado electrónico**
- **Delegado de Protección de Datos o Persona de contacto**
- **Responsable del tratamiento**: además de sus datos identificativos se informa sector de actividad, tipo de organización, ámbito público o privado…
- **Encargado de tratamiento**: sus datos identificativos y si se trata de organización de ámbito público/ privado

M. DOCUMENTACIÓN ADJUNTA A LA NOTIFICACIÓN (informes, fotos, etc.)

Contenido de la notificación brecha a personas afectadas

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

La **comunicación** a las personas afectadas se realizará en un **lenguaje claro y sencillo**, con el siguiente contenido mínimo :

- **Datos de contacto del Delegado** de Protección de Datos, o en su caso, del punto de contacto en el que pueda obtenerse más información.
- **Descripción** general del incidente y **momento** en que se ha producido.
- Las posibles **consecuencias** de la brecha de datos personales.
- Descripción de los **datos** e información personal **afectados.**
- Resumen de las **medidas implantadas** hasta el momento para controlar los posibles daños.
- **Otras informaciones útiles** a los afectados para que puedan proteger sus datos o prevenir posibles daños.

La comunicación preferentemente se deberá realizar **de forma directa** al afectado, ya sea por *teléfono, correo electrónico, SMS, a través de correo postal, o a través de cualquier otro medio dirigido al afectado* que el responsable considere adecuado

Contenido de la notificación brecha a personas afectadas

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

- 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 por ejemplo
  - *sitios web como blogs corporativos, o*
  - *comunicados de prensa.*
- Estas técnicas podrían emplearse, también, **cuando no sea posible contactar con las personas afectadas** (por ejemplo, porque *ha habido pérdida de datos e imposibilidad para recuperarlos, o se desconocen los datos de contacto, o estos no están actualizados*) y esté debidamente justificado.

  En tal caso, el **aviso público** ocupará un lugar destacado, de forma que en ningún caso pueda pasar desapercibidos.

Régimen sancionador relativo a obligaciones artículos 33 y 34

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

- Las **notificaciones de brechas de datos personales** ante la Autoridad de Control es parte de la **responsabilidad proactiva de los responsables, o encargados** en su caso, demostrando diligencia en los tratamientos de datos.

- La notificación de brecha **no implica la imposición de una sanción**. Al contrario, una notificación, y en su caso comunicación, realizada en tiempo y forma, **es una evidencia de la diligencia** de la organización a la hora de ejecutar eficazmente la obligación de responsabilidad proactiva del RGPD.

- Sin embargo, el **no cumplir con las obligaciones de notificación a la AEPD y comunicación a los interesados sí está tipificado como infracción**:

  El **Titulo IX de la LOPDGDD** precisa el régimen sancionador y específicamente en relación con las brechas:

  - el **artículo 73** establece lo que se considera **infracciones graves**: *no informar el encargado al responsable*, *no notificar a la autoridad de control, no comunicar a los afectados si así lo ha requerido la AC, falta de adopción de medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado, no cumplir con las medias técnicas y organizativas que se hubieran implantado*

  - El **artículo 74** establece como **infracciones leves**: *la notificación incompleta, tardía o defectuosa a la autoridad de control, el incumplimiento de documentar cualquier brecha, no comunicar a los afectados cuando la brecha entraña un alto riesgo para los derechos y libertades de las personas*

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

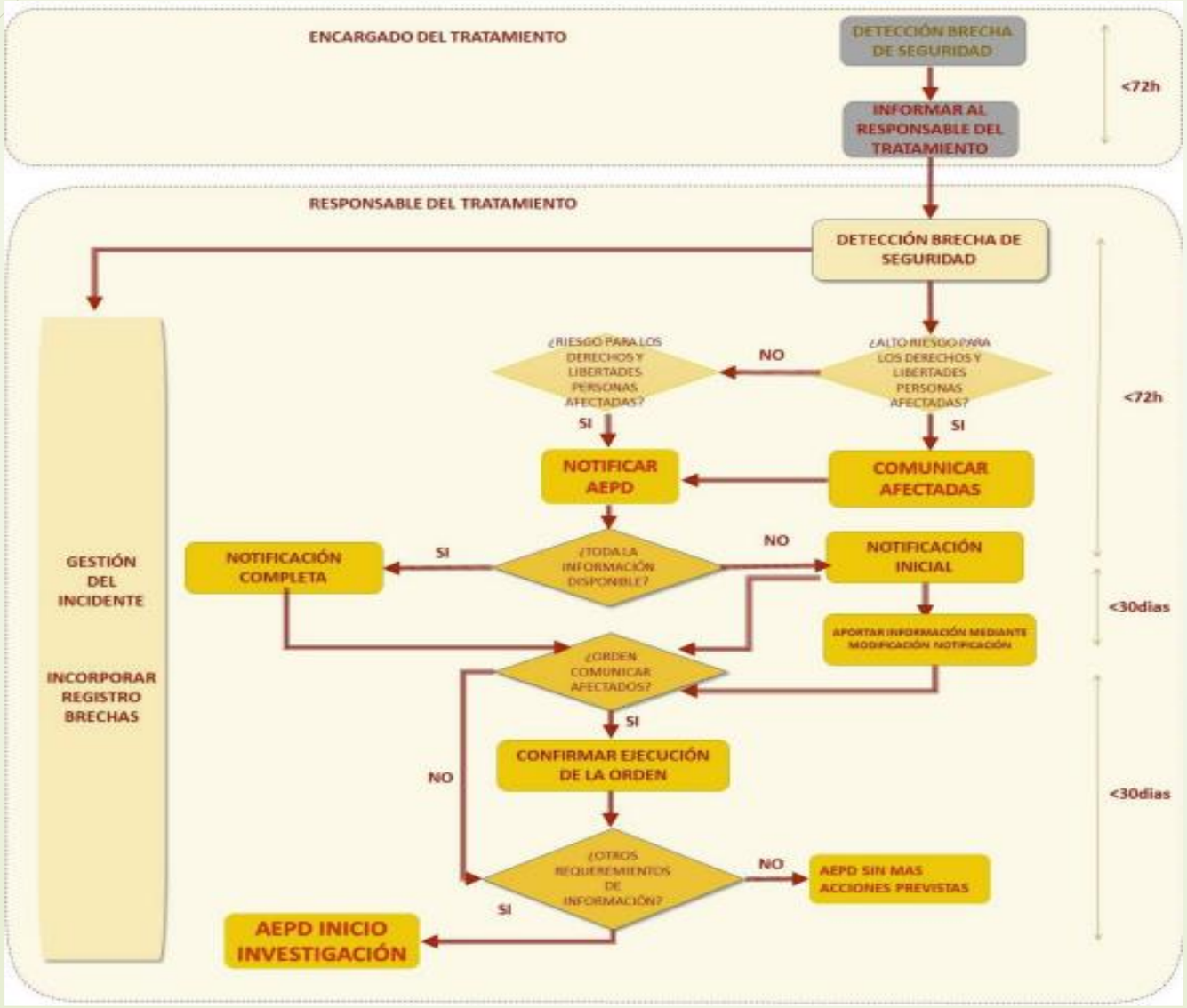
GESTIÓN DE BRECHAS

- El responsable del tratamiento **deberá documentar cualquier violación de la seguridad de los datos personales**, mediante un **registro interno** con el siguiente contenido mínimo: *fecha, hechos, efectos, medidas correctivas aplicadas.*
- Formulario de Notificación a la autoridad de control competente (AEPD), **A TRAVÉS DE LA DPD**, **sin dilación indebida y a más tardar en las 72 horas siguientes a la detección**, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas (ASESORA_BRECHA)
- El responsable del tratamiento deberá tener en consideración que, 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, la deberá **comunicar a la persona interesada sin dilación indebida** (COMUNICA_BRECHA)
- En la Generalitat, el **Centro de Seguridad TIC es el CSIRT-CV** y, por tanto, cuando se detecte **un incidente de seguridad** (*tanto si afecta a datos de carácter personal como si no*) el **responsable de seguridad de la organización**, o en su ausencia en quien delegue el responsable de la organización, **lo deberá notificar a este centro** a través del formulario que ofrecen en su página web https://www.csirtcv.gva.es/

Diagrama resumen de notificación de brecha

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA



Bibliografía

- *Reglamento General de Protección de Datos*
- *Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales*
- *GUIA AEPD para la notificación de brechas de datos personales*
- *Material de la AEPD respecto a medidas técnicas para evitar brechas de seguridad*
- *GUÍA AEPD Gestión del riesgo y evaluación de impacto en tratamientos de datos personales*

GENERALITAT VALENCIANA

Delegació de Protecció Dades GVA

Contacto con el DPD:

Delegado de protección de datos de la Generalitat y su sector público instrumental

dpdgeneralitat@gva.es

dpdsectorpublico@gva.es

Espacio de la Delegación de Protección de Datos en la intranet FUNCION@
(Conocimiento → Protección de Datos)

Formulario de notificación de brechas de la AEPD

Guía para la gestión de brechas