DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Cuadernos DivalData

Cuadernos dirigidos a delegados,
responsables y especialistas en protección
de datos personales

Cuaderno nº 35 | Mayo 2023

RIESGOS ANTE LA COMUNICACIÓN MASIVA DE DATOS ENTRE ADMINISTRACIONES PÚBLICAS

Í N D I C E

Riesgos ante la comunicación masiva de datos entre Administraciones Públicas

Os invitamos a trasladarnos aquellas temáticas que resulten de vuestro interés para los próximos boletines informativos. Estas peticiones deberán dirigirse a:

Diputación de Valencia

Dpto. de Protección de Datos y Seguridad de la Información

Pl. de Manises, 4 46003 Valencia

email: dpdsi@dival.es

SUSCRIPCIONES

Si deseas suscribirte a nuestra publicación accede al siguiente

enlace

INTRODUCCIÓN

Como consecuencia del actual entorno de **digitalización, interconectividad e interoperabilidad**, nos encontramos con tratamientos de datos personales que suponen el acceso o la comunicación de grandes repositorios de datos entre múltiples responsables de las Administraciones Públicas.

Estos tratamientos que suponen un alto volumen de datos conectados de forma permanente, obligan a considerar ciertos **riesgos** en materia de privacidad, como las **brechas masivas de datos personales** que suponen un alto riesgo para los derechos fundamentales.

Se aborda la necesidad de gestionar tanto los riesgos para los **derechos y libertades de los individuos** como el riesgo para la propia **sociedad** o para un grupo representativo de ésta, derivado del compromiso de **masivas cantidades de datos personales.**

Estas infraestructuras, que no tienen por qué ser muy complejas técnicamente, sí lo suelen ser organizativamente por implicar a múltiples actores que pueden tener distintas esferas de responsabilidad. El número de puntos débiles, donde pueden ocurrir posibles fallos o errores, aumenta y de la misma forma se incrementa la posibilidad de materialización de una brecha.

Una gestión eficaz de los riesgos implica la **actuación coordinada de los distintos implicados** en el tratamiento, un estudio conjunto de los distintos escenarios de brechas masivas en caso de fallo de las medidas de seguridad, y la adopción, coherente y en el ámbito de las distintas responsabilidades, de los procedimientos, técnicas de protección de datos y medidas de seguridad específicas y adecuadas para minimizar su impacto sobre los derechos fundamentales.

"La interconexión de sistemas y el establecimiento de canales digitales permanentes hacen posibles los tratamientos de datos que suponen el acceso o la comunicación de grandes repositorios de datos entre múltiples responsables de las Administraciones Públicas".

"El impacto para los derechos y libertades que podría tener una brecha de datos en estos entornos, debido a que pueden afectar a un gran volumen de población, es mayor que la suma del impacto que puede tener en cada uno de los interesados.".

BRECHAS MASIVAS DE DATOS

"Una brecha de datos personales es un incidente de seguridad que ocasiona la destrucción, pérdida o alteración accidental o ilícita de los datos personales tratados por un responsable, o bien la comunicación o acceso no autorizados a los mismos".

Una **brecha de datos personales** es un incidente de seguridad que ocasiona la **destrucción, pérdida o alteración accidental o ilícita de los datos personales** tratados por un responsable, o bien la comunicación o acceso no autorizados a los mismos.

Una brecha de datos personales puede tener una serie de efectos adversos considerables en las personas, susceptibles de ocasionar **daños y perjuicios físicos, materiales o inmateriales**; por lo que hay que intentar evitarlas y en caso de que sucedan gestionarlas adecuadamente, especialmente cuando puedan poner en riesgo los derechos y libertades de las personas físicas.

El artículo 33 del Reglamento (UE) 2016/679 General de Protección de Datos (en adelante, RGPD) impone a los responsables de un tratamiento de datos personales la **obligación de notificar a la autoridad de control** competente las brechas de datos personales cuando sea probable que constituyan un riesgo para los derechos y libertades de las personas.

El responsable de tratamiento debe valorar el nivel de riesgo de una brecha de datos personales y notificarla a la autoridad de control cuando exista tal riesgo, y además **cuando el riesgo sea alto el responsable también deberá comunicar la brecha a las personas afectadas** conforme al artículo 34 del RGPD.

El plazo para notificar a la autoridad de control es de **72 horas** desde que la organización tiene constancia de la brecha.

Los tratamientos de datos personales en las Administraciones Públicas (en adelante, AAPP) son cada vez **más complejos** en cuanto al número de intervinientes, medios técnicos y tecnologías empleadas. En el caso de la interoperabilidad administrativa el **nivel de riesgo** que supondría una brecha de datos personales es de un elevado impacto social **muy alto**, dado que la interconexión de infraestructuras multiplica la probabilidad de que se materialice una amenaza. El **impacto** para los

derechos y libertades que podría tener una brecha de datos en estos entornos, debido a que pueden afectar a **un gran volumen de población**, es mayor que la suma del impacto que puede tener en cada uno de los interesados.

Las consecuencias de una brecha masiva de datos personales en el ámbito de las AAPP han de ser evaluadas desde una **doble perspectiva**: por un lado, sobre los derechos fundamentales del individuo y, por otro lado, por el impacto que podría suponer para la garantía del interés público y sus efectos sobre los derechos fundamentales de la propia sociedad.

Una correcta gestión implica establecer, **previamente** a la materialización de una brecha que afecte a los derechos fundamentales, las **medidas y acciones** que se deben adoptar en el caso de que dicha brecha llegue a producirse.

Una gestión eficaz de los riesgos implica la **actuación coordinada** de los distintos implicados en el tratamiento, un **estudio conjunto** de los distintos escenarios de brechas masivas en caso de fallo de las medidas de seguridad, y la adopción, coherente y en el ámbito de las distintas responsabilidades, de los **procedimientos, técnicas de protección de datos y medidas de seguridad específicas y adecuadas** para minimizar su impacto sobre los derechos fundamentales.

"En el caso de la interoperabilidad administrativa el nivel de riesgo que supondría una brecha de datos personales es de un elevado impacto social muy alto, dado que la interconexión de infraestructuras multiplica la probabilidad de que se materialice una amenaza".

"Una correcta gestión implica establecer, previamente a la materialización de una brecha que afecte a los derechos fundamentales, las medidas y acciones que se deben adoptar en el caso de que dicha brecha llegue a producirse".

CÓMO GESTIONAR LOS RIESGOS ANTE UNA POSIBLE BRECHA MASIVA

Los **riesgos**, aunque siempre estén presentes, serán **especialmente considerables** en tratamientos llevados a cabo por grandes organizaciones públicas y privadas que estén dando servicio a gran parte de los ciudadanos, y aun mucho más si están interconectadas.

Para **estimar el impacto** que pudiera tener una brecha de datos personales hay que plantearse las **consecuencias que se derivarían de su materialización**. Para ello, pueden plantearse los posibles escenarios de materialización de un compromiso de los datos personales, determinar sus consecuencias, y evaluar cómo afecta a los derechos y libertades de los interesados, sobre todo si se trata de consecuencias irreversibles en sus derechos fundamentales.

“Para estimar el impacto que pudiera tener una brecha de datos personales hay que plantearse las consecuencias que se derivarían de su materialización”.

Tras el análisis, hay que determinar **medidas adicionales para disminuir la probabilidad** de que suceda la brecha. No obstante, se debe asumir que **la posibilidad de materialización siempre existe** y que hay una probabilidad residual de materialización que no se puede eliminar, por lo que hay que considerar **medidas específicas para eliminar, disminuir o revertir el impacto** de la misma sobre el interesado cuando esta se produzca.

Por ello, hay que encontrar la respuesta, al menos, a las siguientes preguntas **desde el diseño del tratamiento y previamente a su implementación**:

- Qué **impacto** personal y social puede tener una brecha si se materializa.
- Qué **medidas de protección** de datos deberían estar implementadas a priori para minimizar el impacto.
- Qué **medidas de respuesta** deben estar previstas y deben ejecutarse a posteriori, una vez producida la brecha.

"Sea cuales sean los roles de los intervinientes, las medidas y garantías de protección de datos deben ser implementadas de forma transversal a través de la cooperación de las organizaciones que intervienen".

Sea cuales sean los **roles de los intervinientes**, las medidas y garantías de protección de datos deben ser **implementadas de forma transversal** a través de la cooperación de las organizaciones que intervienen.

Por ejemplo, en una situación de comunicación de datos entre responsables de la AAPP, las medidas y garantías deberán ser establecidas tanto por las entidades que comunican o permiten el acceso a los datos (**cedentes**) como por las entidades que los reciben o consultan (**destinatarios**) independientemente de los roles que adopten con relación al RGPD.

Asimismo, el RGPD **no requiere una simple acumulación de acciones**, sino que reclama aquellas que de forma objetiva permitan disminuir impactos sobre derechos fundamentales y/o probabilidades de que se produzcan, en particular, aquellas orientadas a la gestión de las brechas de datos personales. El acumular medidas sin saber qué problemas solucionan, cómo interactúan entre sí y cuál es su efectividad real, además de no gestionar los riesgos, puede crear **vulnerabilidades adicionales**.

Conviene recordar que el **ENS** (Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad), que tiene por objetivo la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, y que está alineado con el **RGPD** y la **LOPDGDD** (Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales), aplica a sistemas de información de AAPP y cualquier entidad privada que preste servicio a una AAPP. Por ejemplo, el ENS también es de obligado cumplimiento para los sistemas de información de entidades privadas que actúen como encargados o subencargados del tratamiento de AAPP.

MEDIDAS RECOMENDADAS POR LA AEPD

Las medidas técnicas y organizativas que se adopten han de estar dirigidas específicamente a **minimizar los riesgos identificados** para los derechos y libertades de las potenciales brechas de datos personales.

La AEPD propone el siguiente listado de medidas, no siendo exhaustiva ni exigible en su totalidad, pero sí son medidas a valorar en cada caso. A continuación, se extraen algunas de las más relevantes:

Medidas **preventivas**:

- Disponer de un marco de coordinación de los DPD de las entidades involucradas.
- Realizar un análisis conjunto de las implicaciones de los tratamientos que involucran a distintas entidades.
- Disponer de políticas de protección de datos.
- Realizar ejercicios conjuntos en el que se planteen escenarios de brechas de datos.
- Categorizar datos que en un momento dado puedan ser considerados de especial sensibilidad.
- Identificar conjuntos de datos de mayor impacto que no deban ser accesibles por medios exclusivamente automatizados.

Medidas de **detección**:

- Establecimiento de cuotas o límites de consulta por usuario/cuenta y también por organización, acordes al uso legítimo de los mismos, incluyendo la monitorización de tales accesos.
- Gestionar de forma específica las consultas/accesos desde IP geolocalizadas en áreas geográficas fuera del ámbito de las organizaciones o no habituales, IP basadas en redes de anonimización o IP comprometidas.

"Las medidas técnicas y organizativas que se adopten han de estar dirigidas específicamente a minimizar los riesgos identificados para los derechos y libertades de las potenciales brechas de datos personales".

"La AEPD propone el siguiente listado de medidas, no siendo exhaustiva ni exigible en su totalidad, pero sí son medidas a valorar en cada caso".

Medidas de **respuesta**:

- Disponer de planes de respuesta a incidentes que incluyan la gestión y rápida respuesta a brechas de datos personales.
- Disponer de procedimientos que permitan que los incidentes de seguridad escalen de forma rápida tanto al DPD como a los círculos de decisión de la organización.
- Establecimiento de canales ágiles, efectivos y probados de comunicación de brechas entre las entidades intervinientes.
- Procedimiento de notificación de brechas de datos personales a las autoridades competentes que concrete todos los aspectos fundamentales.
- Procedimiento y recursos para la comunicación a los afectados, que adelante en cada situación cómo se va a comunicar una brecha masiva a los interesados afectados, en qué situaciones se producirá tal comunicación, medio para comunicar, plazos para proteger de forma efectiva los derechos de los interesados, recomendaciones para los interesados en función de los distintos escenarios de brechas, situaciones que pueden justificar el retraso de la comunicación, etc.

Medidas de **supervisión y revisión**:

- Procedimientos establecidos para determinar cambios de contexto en responsables y tratamientos de similar naturaleza: brechas producidas, cambios tecnológicos, novedades normativas nacionales, europeas e internacionales, evolución social o política, factores geoestratégicos, etc.
- Establecimiento de canales de comunicación efectivos entre las entidades intervinientes sobre los eventos anteriores.
- Auditorías de privacidad.

MATERIAL COMPLEMENTARIO

- Orientaciones para tratamientos que implican comunicación de datos entre Administraciones Públicas ante el riesgo de brechas de datos personales de la Agencia Española de Protección de Datos. Consulta este enlace.
- Gestión del riesgo y evaluación de impacto en tratamientos de datos personales de la Agencia Española de Protección de Datos. Consulta este enlace.
- Guía para la notificación de brechas de datos personales de la Agencia Española de Protección de Datos. Consulta este enlace.

NOTICIAS

La AEPD publica **nuevas notícias** en relación a las Administraciones públicas**:**

1. **LA AEPD PUBLICA POR PRIMERA VEZ EL LISTADO DE ADMINISTRACIONES PÚBLICAS INCUMPLIDORAS CON SUS REQUERIMIENTOS**. El objetivo de esta lista se encuentra en garantizar el derecho fundamental a la protección de datos. La lista está compuesta por Administraciones Públicas que no cumplen con los requerimientos de información remitidos por la Agencia, así como aquellas que no adecúan el tratamiento de datos a la legalidad y no acreditan las medidas correctivas impuestas. Tanto la falta de respuesta a los requerimientos como no acreditar que se han cumplido las medidas ordenadas para garantizar la protección de datos de los ciudadanos suponen infracciones clasificadas como muy graves. Vid. Noticia en este enlace.

2. **ORIENTACIONES PARA LA REALIZACIÓN DE UNA EVALUACIÓN DE IMPACTO PARA LA PROTECCIÓN DE DATOS EN EL DESARROLLO NORMATIVO**. El objetivo de este documento es aborda la necesidad de realizar una evaluación de impacto desde el diseño cuando la medida legislativa implica el tratamiento de datos personales, aportando consejos y recomendaciones para llevarla a cabo. Dirigido a los organismos de las Administraciones Públicas que promuevan proyectos normativos que impliquen tratamientos de datos personales y a sus delegados de protección de datos, el documento analiza los requisitos previos que hay que analizar para saber si hay que hacer esa evaluación de impacto, cómo debe realizarse en caso afirmativo y qué aspectos que se deben tener en cuenta para evaluar la calidad de la misma. Vid. guía en este enlace.