ORIENTACIONES PARA TRATAMIENTOS QUE IMPLICAN COMUNICACIÓN DE DATOS ENTRE ADMINISTRACIONES PÚBLICAS ANTE EL RIESGO DE BRECHAS DE DATOS PERSONALES

v. marzo 2023

RESUMEN EJECUTIVO

El objetivo de este documento es orientar a los responsables implicados en tratamientos que incluyen el intercambio de datos entre las Administraciones Públicas. Está dirigido específicamente a aquellos tratamientos que, por el alto volumen de datos personales que son tratados, y por la interconexión permanente entre sistemas de las Administraciones Públicas, pueden producirse brechas masivas de datos personales de alto riesgo para los derechos fundamentales. Para ello, ofrece orientaciones sobre cómo abordar la gestión de los riesgos para los derechos y libertades de las personas físicas que se podrían derivar de los posibles escenarios de brechas masivas.

Estas orientaciones abordan 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. Los responsables han de asumir que las brechas pueden producirse y que las medidas de seguridad no garantizan la protección total. Por lo tanto, los responsables han de implementar, desde el diseño de las operaciones de intercambio de datos, medidas específicas para minimizar el posible impacto personal y social de una brecha. 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.

Este documento está dirigido a responsables del tratamiento en el Sector Público y a sus delegados de protección de datos. Como material de ayuda, incluye una lista, no exhaustiva, de posibles medidas preventivas, de detección, de respuesta, de revisión y supervisión que se podrían implementar en el marco de este tipo de tratamientos.

Palabras clave: AAPP, intercambio, conectividad, riesgo, evaluación de impacto, brechas, responsabilidad proactiva, protección de datos, riesgo, impacto, protección de datos desde el diseño, privacidad, seguridad, coordinación.

ÍNDICE

I. OBJETIVOS Y DESTINATARIOS

Este documento está dirigido a responsables[1] del tratamiento en Administraciones Públicas y a sus delegados de protección de datos. Está orientado específicamente a aquellos tratamientos que, por el alto volumen de datos personales que son tratados, y por la interconexión permanente entre sistemas de las Administraciones Públicas, pueden producirse brechas masivas de datos personales de alto riesgo para los derechos fundamentales. En él se detallan los aspectos más relevantes en cuanto a la gestión de dichos riesgos.

Este documento no pretende replicar ni repetir lo establecido en la Guía para la notificación de brechas de datos personales de la AEPD, ni en la Gestión del riesgo y evaluación de impacto en tratamientos de datos personales sino simplemente particularizar el caso concreto de brechas masivas de datos personales en tratamientos de las Administraciones Públicas.

II. INTRODUCCIÓN

Los tratamientos de datos personales que suponen el acceso o la comunicación de grandes repositorios de datos entre múltiples responsables de las Administraciones Públicas (en adelante, AAPP) son comunes en el actual entorno de digitalización e interconectividad. Con frecuencia, en estos modelos de interoperabilidad de datos se integran otras fuentes de datos o grandes repositorios de datos del sector privado, entre los que pueden incluirse entidades de sectores estratégicos a nivel nacional, del sector de las telecomunicaciones, el sector financiero, el sector asegurador, el sector sanitario, proveedores de servicios de Internet, etc.

La interconexión de sistemas y el establecimiento de canales digitales permanentes entre administraciones hacen posibles estos tratamientos. Aunque estas infraestructuras 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. En este escenario es donde las soluciones técnicas y organizativas habituales, o de mínimos, pueden mostrar su fragilidad, más aún si tenemos en cuenta que un incidente puede producir un “efecto dominó”, generando quiebras en cadena de las medidas de seguridad en distintos intervinientes.

Por otro lado, 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 medidas que se podrían tomar para minimizar el impacto cuando el volumen de afectados es bajo, pueden resultar insuficientes cuando afectan a gran cantidad de personas físicas. Los efectos de una brecha masiva pueden generar un gran impacto a nivel social, afectar a las obligaciones de disponibilidad y resiliencia establecidas en el art. 32.1.b del Reglamento General de Protección de Datos (en adelante, RGPD) y, finalmente, pueden generar o ser utilizados para fomentar la desconfianza en los servicios o en la estructura de la Administración del Estado.

En definitiva, el análisis del impacto de brechas masivas de datos para los derechos fundamentales debe tomar una dimensión completamente distinta y añadirse nuevos

[1] El término “responsable” se utiliza en el sentido de responsable RGPD tal como se establece en el art.4.7 del RGPD. No confundir con la asignación de responsabilidades internas en una entidad (responsable de seguridad, responsable de RRHH, etc.) ni con una persona física (una situación excepcional que no aplica a las AAPP).

factores cuando se evalúa el efecto conjunto sobre una gran extensión de la población[2]. Según establece el art. 24.1 del RGPD, las medidas que se han de adoptar en un tratamiento para garantizar y poder demostrar su conformidad con el Reglamento deben tener en cuenta el ámbito, el contexto y los fines del tratamiento del tratamiento, debiendo atender, en particular, a la extensión de sujetos afectados por el mismo y al riesgo que supone para los derechos fundamentales.

En ese sentido, 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.

Cuando los responsables del tratamiento son entidades del sector público que realizan tratamientos para el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos o en el cumplimiento de una obligación legal, la posibilidad de un elevado impacto social es muy alto. Por lo tanto, el nivel de riesgo que supondría una brecha de datos personales en tratamientos llevados a cabo como resultado de la intercomunicación de datos entre diferentes responsables de este tipo es intrínsecamente es elevado. Y, en particular, la interconexión de infraestructuras para el acceso y el intercambio de datos multiplica la probabilidad de que se materialice una determinada amenaza.

En estos contextos es necesario tener en cuenta que el efecto acumulativo de las amenazas y vulnerabilidades del conjunto de tratamientos son, con frecuencia, no conocidas por todos sus intervinientes. Muchos no son conscientes que la materialización de una brecha en una operación de tratamiento de uno de los intervinientes puede afectar al resto de tratamientos del conjunto de intervinientes. En tal escenario, debe evitarse que la responsabilidad se diluya entre las organizaciones que participan en el tratamiento, que deben actuar de forma coordinada en la gestión de riesgos tanto para los derechos y libertades de las personas físicas como para el riesgo a nivel social.

Esto supone que deben aplicarse garantías de privacidad y medidas de seguridad, tanto técnicas como organizativas, adecuadas a estos escenarios complejos[3], específicas para gestionar el alto impacto social con relación a la protección de datos y de forma coordinada.

III. TRATAMIENTOS DE ALTA COMPLEJIDAD

Los tratamientos de datos personales en las AAPP son cada vez más complejos en cuanto al número de intervinientes, medios técnicos y tecnologías empleadas. Existen numerosos casos en los que en un tratamiento de datos personales participan múltiples organizaciones con distintos tipos de roles en relación con la protección de datos. Las relaciones entre organizaciones pueden ser las tradicionales de responsable a encargado del tratamiento, pero, con una mayor complejidad por la pluralidad de responsables intervinientes en lo relativo a la articulación de las garantías del artículo 28 del RGPD, en lo que afecta a las autorizaciones genéricas o específicas exigibles para su intervención y a las garantías que deben aportarse. En muchos casos dicha complejidad aumenta por la intervención de subencargados del tratamiento para la aportación de tecnologías. En muchos casos pueden producirse múltiples comunicaciones de datos entre organizaciones en las que todas ellas son responsables de un tratamiento distinto de esos datos personales. También pueden darse situaciones de corresponsabilidad que exijan acuerdos jurídicos

[2] Guía para la Gestión del riesgo y evaluación de impacto en tratamientos de datos personales: *"Cuando hay distintos factores de riesgo es necesario interpretar cómo dichos factores, considerados de forma independiente, podrían interactuar entre sí para incrementar el nivel de riesgo del tratamiento (factor de riesgo acumulado), mediante el análisis de sus dependencias y efectos combinados o las interacciones mutuas que existan entre ellos."*

[3] Art. 24 RGPD

específicos delimitando la responsabilidad de cada uno de los corresponsables, sin que ello pueda suponer una limitación o situaciones de vacío de responsabilidad.

A. AUTOMATIZACIÓN DEL INTERCAMBIO DE DATOS

El nivel de digitalización de las organizaciones permite que el intercambio de datos a gran escala sea realizado de forma muy dinámica y automatizada sin intervención humana. En la naturaleza de dichos tratamientos se encuentran establecidos canales digitales de forma continua y permanente. Algunos ejemplos de este tipo de canales pueden ser la publicación y consumo de servicios en Internet, en redes corporativas, en redes semiprivadas entre organizaciones o en redes privadas virtuales, puntos neutros, portales de acceso, etc.

B. ELEVADO VOLUMEN DE DATOS

Por lo general, el volumen de datos personales disponible en estas infraestructuras para el intercambio de datos puede ser muy elevado. En algunas de ellas pueden llegar a estar accesibles los datos de todos los ciudadanos de una Comunidad Autónoma, de España o de Europa. Una vulnerabilidad o debilidad en cualquiera de estas organizaciones podría poner en riesgo todo el tratamiento a lo largo de todas las organizaciones intervinientes, o incluso en otros tratamientos de esas mismas organizaciones.

IV. ESTIMACIÓN DEL RIESGO ANTE UNA BRECHA DE DATOS PERSONALES

Las medidas de seguridad son una obligación de medios, pero no de resultado[4]. En ese sentido, los responsables han de asumir que las brechas de datos personales pueden producirse. Por ello, y en cualquier tratamiento de datos personales es necesario estimar el riesgo que podría suponer para los derechos y libertades de las personas el que se materialice una brecha de datos personales. En tratamientos de datos personales de alta complejidad como los descritos en el apartado anterior, este aspecto es especialmente relevante por el impacto que puede suponer para los derechos fundamentales a nivel individual y social.

En el documento WP218 "*Statement on the role of a risk-based approach in data protection legal frameworks*", el Grupo de Trabajo del Artículo 29 indica:

> *"El enfoque basado en el riesgo va más allá de un estrecho "enfoque basado en el daño" que se concentra sólo en el daño y debe tener en cuenta todos los efectos adversos, tanto potenciales como reales, evaluados en una escala muy amplia que va desde el impacto en la persona afectada por el tratamiento en cuestión hasta un impacto social general (por ejemplo, la pérdida de confianza social)."*[5]

De la declaración anterior se concluye que es necesario gestionar el riesgo y tomar medidas con un enfoque que abarque todo el contexto del impacto las brechas de datos, lo que implica, al menos, en una doble perspectiva:

1. Gestionar el riesgo para los derechos y libertades de los individuos.
2. Gestionar el riesgo para la propia sociedad (o para un grupo representativo de ella).

[4] Comunicación Poder Judicial: El Tribunal Supremo establece que la obligación de las empresas de adoptar las medidas necesarias para garantizar la seguridad de los datos personales no puede considerarse una obligación de resultado.
[5] Traducción no oficial del documento original en inglés.

Por ejemplo, una brecha de datos personales que afectase a un porcentaje importante de la base de datos de identidad oficial de un país tiene un impacto social con unas consecuencias muy superiores a las que pueda sufrir cada individuo por separado[6]. La gran cantidad de personas afectadas supondría una quiebra en la confianza social que se tendría en ese medio de identificación, el colapso en los servicios y en la gestión administrativa. A su vez, las medidas de mitigación que sería necesario desplegar serían distintas y de una dimensión muy diferente de las adecuadas para mitigar el impacto sobre un solo individuo.

Siempre existen riesgos relacionados con las brechas de datos personales. Sin embargo, estos serán especialmente considerables en tratamientos de datos personales 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. Es muy importante tener en cuenta que el riesgo que pueden suponer brechas de datos personales en dichos tratamientos no depende tanto de que se traten categorías de datos sensibles y/o especialmente protegidos como de las consecuencias para los derechos fundamentales que se pueden derivar de un compromiso de la información[7].

Para estimar el impacto que pudiera tener una brecha de datos personales hay que plantearse las consecuencias que se derivarían de su materialización. Una forma de hacerlo es, antes que se produzca una brecha, 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.

Ante el resultado de dicho análisis, hay que determinar medidas adicionales para disminuir la probabilidad de que suceda la brecha. Sin embargo, solo implementando medidas para reducir la probabilidad de que se produzcan no es suficiente, la experiencia muestra que siempre quedará una probabilidad residual de materialización de la brecha. Los responsables han de asumir que la posibilidad de materialización de brechas de datos personales 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.

Hay que aceptar la realidad de que las brechas de datos personales se van a producir, antes o después. Por lo tanto, ante los posibles escenarios de materialización de distintos tipos de brechas hay que encontrar 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 de datos personales si se materializa.
- Qué medidas de protección de datos deberían estar implementadas a priori para minimizar el impacto personal y social que pudiera producir una brecha materializada.
- Qué medidas de respuesta deben estar previstas y deben ejecutarse a posteriori, una vez producida la brecha, para minimizar el impacto personal y social.

V. GESTIÓN DEL RIESGO DE UNA BRECHA DE DATOS PERSONALES

La gestión del riesgo para los derechos y libertades de los interesados y la evaluación de impacto para la protección de datos (en adelante, EIPD) son obligaciones del responsable del tratamiento, según los artículos 24 y 35 del RGPD. El responsable tiene el deber de garantizar una correcta evaluación del riesgo para los derechos fundamentales y la

[6] Noticia sobre la supuesta filtración de datos del Registro Nacional de Personas (Renaper) en Argentina.

[7] Por ejemplo, el compromiso de los datos de domicilio de un fichero de víctimas supervivientes de violencia de género tiene un alto impacto para los derechos fundamentales.

selección, la ejecución, la revisión y la actualización de las medidas apropiadas para garantizar el cumplimiento.

El responsable puede recibir asistencia de terceros para cumplir sus obligaciones, y en muchos casos debe reclamarla. Ya el artículo 28.3.f del RGPD establece la obligación de los encargados de facilitar esa asistencia cuando proceda. En concreto, el RGPD establece que el encargado "*ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado*". En el caso que nos ocupa, los encargados y, en su caso, los subencargados, deben asistir a los responsables en el cumplimiento de las obligaciones con relación a la gestión del riesgo para los derechos y libertades de las personas físicas. Esta asistencia se puede extender incluso a la preparación de evaluaciones de impacto en el ámbito de los servicios que los encargados vayan a aportar, con el fin de integrarlas en la EIPD del tratamiento de datos del responsable.

Por otro lado, el principio de responsabilidad proactiva, o "*accountability*", difícilmente podrá cumplirse si los medios técnicos que se emplean para implementarlo (su naturaleza[8]), no cuentan por sí mismos con las garantías adecuadas, es decir, no son "*accountables*" o demostrables con las evidencias objetivas adecuadas. Por lo tanto, el responsable tendrá la obligación de exigir la información y colaboración necesaria a encargados y proveedores tecnológicos para garantizar y de poder demostrar el cumplimiento de la norma.

Al ser un entorno muy complejo, en el que puede haber varios ámbitos de responsabilidad, es imprescindible una colaboración entre todos los intervinientes a la hora de gestionar los riesgos que supone un tratamiento de datos personales. La aplicación de garantías de privacidad y de medidas de seguridad evaluadas e implementadas en las entidades implicadas en un tratamiento, pero de forma independiente entre ellos, puede conducir a una pérdida de eficacia en la protección de los derechos fundamentales. 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.

Una eficaz y eficiente protección de datos va a exigir un esfuerzo coordinado y una aproximación combinada a la solución que dé cumplimiento al RGPD. La EIPD y las soluciones que gestionen las limitaciones y los riesgos a los derechos y libertades han de surgir de un trabajo común y su conclusión ha de ser única.

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. Que exista un interés público o una obligación legal para comunicar o permitir el acceso a los datos, no implica que tal comunicación o acceso se pueda realizar sin adoptar las medidas adecuadas. Un enfoque en el que el cedente de datos establece un canal de comunicación y confía exclusivamente en las medidas del destinatario para proteger el acceso a los datos deja la confidencialidad de los datos totalmente expuesta en caso de vulneración de los sistemas del cesionario.

[8] La naturaleza del tratamiento define el cómo se implementa éste: automatizado o no automatizado, las distintas operaciones en las que se divide, los intervinientes, la posibilidad y tipo de encargados y subencargados, las tecnologías en las que se apoya, si es en local o en la nube, etc.

VI. MEDIDAS APROPIADAS AL NIVEL DE RIESGO PARA LOS DERECHOS Y LIBERTADES

El art. 24 del RGPD establece que los responsables han de adoptar medidas apropiadas para garantizar y demostrar que sus tratamientos cumplen con la normativa de protección de datos. Las medidas apropiadas lo serán en función de las siguientes características del tratamiento:

- su naturaleza: cómo se implementan,
- su contexto: el entorno en el que se implementan,
- su ámbito: la extensión del tratamiento en categorías de datos, interesados, número de sujetos afectados, frecuencia y granularidad de datos, etc.,
- sus fines, y
- los riesgos para los derechos y libertades de los interesados identificados.

El análisis de un escenario potencial de brechas de datos personales parte del supuesto de que las garantías de seguridad han fallado. Por lo tanto, su gestión no puede estar basada exclusivamente en el ámbito de la ciberseguridad, sino que van a ser imprescindibles la adopción de medidas específicas para la protección de datos desde el diseño y por defecto, y además medidas para una gestión eficaz de las consecuencias de la brecha orientada a proteger los derechos fundamentales de las personas físicas.

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. Esto implica que el responsable ha de evaluar los riesgos que pueden aparecer, diseñar medidas orientadas a minimizar su probabilidad e impacto, y determinar en qué grado dichas medidas están gestionando apropiadamente los riesgos concretos en un proceso dinámico.

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. Por ello, en el caso de tratamientos de este tipo, todas estas medidas adicionales deben identificarse en el marco de la EIPD sobre los riesgos individuales y sociales a los derechos fundamentales de las personas y, si procede, realizar la oportuna consulta previa a la autoridad de control si fuera necesaria (art. 35 y 36 RGPD).

Las medidas apropiadas han de seleccionarse e implementarse desde el diseño de los tratamientos con el objeto de que todos los contextos de riesgo para los derechos y libertades sean considerados. Hay que tener en cuenta que algunas medidas serán más eficaces para evitar o mitigar el impacto directo sobre los individuos y otras medidas lo serán principalmente sobre el impacto social para los derechos fundamentales.

Es necesario aplicar un alto nivel de protección de datos por defecto. Es decir, en este contexto, las tradicionales estrategias de control de acceso con usuario y contraseña (por muy compleja que esta sea) son insuficientes, siendo necesario aplicar medidas adicionales adecuadas a los riesgos y teniendo en cuenta la protección de datos por defecto.

Una capa básica de medidas de seguridad como el control de acceso, explotación, supervisión de recursos externos, protección de servicios en la nube, monitorización de sistemas, planes de recuperación, etc. es absolutamente necesaria, pero no suficiente. Deben ser complementadas con medidas enfocadas a evitar los riesgos adicionales

identificados, en particular, a mitigar el impacto social en caso de que los riesgos se materialicen. En el caso concreto de las medidas de ciberseguridad, deberán estar también alineadas con las nuevas estrategias de ciberseguridad conocidas como "*zero trust*" o "mínimo privilegio".

La estrategia de mínimo privilegio requiere:

- Definición precisa de roles de usuario y sus necesidades de acceso.
- Verificación de identidad estricta para cada persona y dispositivo que intente acceder a un recurso de la red, incluyendo servicios que supongan el tratamiento de datos personales.
- Acceso con privilegios mínimos y mínima exposición de datos.
- Asumir las vulneraciones: limitar el daño y microsegmentar el acceso, también de forma temporal.

El modelo tradicional de protección del perímetro y confiar en el usuario o dispositivo interno no es suficiente y se ha demostrado ineficaz para evitar las brechas de datos personales en los últimos años. Desde el punto de vista de la responsabilidad proactiva y la protección de datos por defecto, es también claramente insuficiente.

La utilización de nubes, el acceso de proveedores y otras organizaciones desde fuera a los sistemas de la organización a través de redes privadas virtuales o también desde dentro, y en definitiva la deslocalización de los datos no permite delimitar o definir un perímetro concreto a proteger. Han sido frecuentes los casos en los que el compromiso de credenciales de sistemas de productividad en la nube, o de acceso a VPN corporativa, acaban produciendo brechas de datos personales con alto impacto sobre los derechos y libertades de las personas y también con alto impacto social.

Conviene recordar que el ENS (Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad), que está alineado con la estrategia de "mínimo privilegio", 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.

En su artículo 3 el ENS recuerda la aplicación de la normativa de protección de datos a aquellos sistemas que participen en tratamientos de datos personales. Esto incluye el análisis de riesgos orientado específicamente a protección de datos y, en su caso, la evaluación de impacto. Igualmente indica que prevalecerán las medidas a implantar como consecuencia de estos análisis en caso de resultar agravadas respecto a las que se determinen por el ENS. El RGPD no limita dichas medidas a las prescritas en el ENS sino a las que, en cada acaso, pudieran ser necesarias para la protección de los derechos y libertades de las personas.

Análogamente, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en su disposición adicional primera remite al ENS para la determinación de las que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, entendiéndose como un criterio de mínimos puesto que en último extremo las medidas determinadas por el ENS deben verse incrementadas si el resultado del análisis de riesgos en protección de datos así lo determina.

Para más concreción, el ENS en el punto 5.7.1 de su Anexo II, determina que cuando el sistema trate datos personales el responsable de seguridad recogerá los requisitos de protección de datos que sean fijados por el responsable o por el encargado del tratamiento, contando con el asesoramiento del delegado de protección de datos, y que sean necesarios implementar en los sistemas de acuerdo a la naturaleza, alcance, contexto y fines del mismo,

así como de los riesgos para los derechos y libertades de acuerdo a los establecido en los artículos 24 y 32 del RGPD, y de acuerdo a la evaluación de impacto en la protección de datos si se ha llevado a cabo. Esta medida es además aplicable a cualquier categoría de sistema.

Finalmente, hacemos referencia al art. 22 del Esquema Nacional de Interoperabilidad aprobado por Real Decreto 4/2010, que hace referencia al ENS.

VII. DELEGADOS DE PROTECCIÓN DE DATOS Y RESPONSABLES DE SEGURIDAD

El papel de los delegados de protección de datos (en adelante, DPD) es clave en casos de tratamientos de este tipo, como se deriva del art. 39 del RGPD. Los DPD de los distintos responsables deben estar coordinados y participar activamente y desde la misma concepción del tratamiento, en su diseño, implementación y también mientras el tratamiento esté operativo. Esto incluye la participación en la gestión de incidentes que puedan suponer una brecha de datos personales.

El asesoramiento de los DPD es fundamental, tanto en las fases iniciales de diseño del tratamiento, en la determinación de medidas aplicables y en las revisiones periódicas para determinar la aplicación de nuevas medidas en función de nuevos riesgos.

Además, deben establecerse mecanismos que articulen esta participación y que permitan que la información escale hasta los DPD cuando se produzca un incidente que pueda resultar en una brecha.

Deben ser consultados y tenidos en cuenta para el cumplimiento de las obligaciones de los responsables en casos de brechas de datos personales, incluida la evaluación del riesgo de una brecha, su gestión y respuesta y también la notificación a la autoridad de control y la comunicación a los afectados conforme a lo establecido en la normativa de protección de datos.

Los DPD han de trabajar estrechamente con los responsables de seguridad, y es especialmente importante en caso de un incidente de seguridad[9] para poder asesorar en cuanto a las medidas a tomar para proteger los derechos y libertades de los interesados tanto a corto plazo, en el marco de una brecha de datos personales, como a largo plazo, para implementar medidas de privacidad que minimicen el impacto para los sujetos de los datos o la sociedad en su conjunto.

En definitiva, contar con el asesoramiento del DPD es necesario para que los responsables puedan cumplir con sus obligaciones, incluyendo recopilar toda la información, analizarla y extraer las conclusiones relevantes para responder a la brecha, documentarla, notificarla y comunicar a los afectados si fuera necesario.

VIII. POLÍTICAS DE PROTECCIÓN DE DATOS

Ante estos escenarios complejos es necesario que la gobernanza y política de información de la entidad incluya una política de protección de datos. Una política de protección de datos es más que un documento, es una forma de actuar eficaz, eficiente y ejecutiva en el diseño y gestión de los distintos tratamientos. Esta política de protección de datos debe estar coordinada a alto nivel con los intervinientes en los tratamientos, especialmente con relación a:

- La intervención y la coordinación de los DPD.

[9] Los incidentes de seguridad pueden ser ciberincidentes, o no tener un componente “ciber”. La seguridad es más que la ciberseguridad.

- La realización de la gestión del riesgo y de la evaluación de impacto.
- La selección de medidas de privacidad y seguridad.
- La gestión de incidentes y la comunicación de los mismos entre intervinientes.
- La revisión y actualización de las medidas que garantizan el cumplimiento del RGPD.
- Los planes de continuidad y contingencia.
- La comunicación (art. 34 del RGPD) y la atención a los interesados.

Así mismo, resulta imprescindible la cooperación entre las autoridades de protección de datos y las que puedan tener atribuidas funciones de gobernanza respecto de tratamientos a los que sean aplicables estas orientaciones.

IX. MEDIDAS RECOMENDADAS

A continuación, se muestran algunas de las medidas preventivas, de detección, de respuesta y de revisión y supervisión que se podrían implementar. Esta lista no es exhaustiva ni exigible en su totalidad, pero sí son medidas a valorar en cada caso.

Algunos ejemplos de medidas preventivas son:

- 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, en el sentido indicado anteriormente, coordinadas entre los intervinientes en el tratamiento.
- Realizar ejercicios conjuntos en el que se planteen escenarios de brechas de datos personales.
- 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.
- Aumentar la intervención humana en la gestión de los accesos.
- Implementar políticas de cancelación o bloqueo de datos que no deben estar en los sistemas de producción.
- Estudiar estrategias de minimización de datos accesibles por Internet: anonimización, seudonimización, disminución de la granularidad o precisión de los datos, restricción de campos/atributos, agregación, adición de ruido, etc.
- Atendiendo a las políticas de acceso, establecer estrategias de minimización en el sentido anterior.
- Implementar estrategias de “mínimo privilegio”, con protección contra posibles ataques desde los sistemas interconectados basados también en la estrategia de “mínimo privilegio”.
- Establecer parámetros de monitorización o que impliquen requisitos de acceso adicional para la consulta de datos cuyas características personales puedan suponer un daño social adicional.
- Disponer en los planes de continuidad de negocio y resiliencia, que incluyan copias de seguridad de datos y también de continuidad de los tratamientos.
- Proteger las copias de seguridad con el mismo nivel de protección que sea aplicable a los datos y sistemas en producción.

- Disponer de copias de seguridad en sistemas independientes y separados de los de producción.
- Aplicar estrategias de segmentación de redes y sistemas, incluyendo protección de servicios expuestos, mediante DMZ u otras medidas adecuadas.
- Implementar estrategias de aislamiento entre sistemas que impidan la extensión de ransomware a toda la organización.
- Tener los sistemas de la infraestructura de servicios e interoperabilidad actualizados sin vulnerabilidades conocidas (servidores, máquinas virtuales, acceso a la nube, etc.)
- Evitar la utilización de nombres de usuario significativos, con patrones predecibles y/o otros identificadores como el NIF, DNI o correos electrónicos que puedan ser igualmente predecibles.
- Tener redactada e implementada una política de gestión de contraseñas actualizada, incluyendo la imposibilidad de utilizar contraseñas débiles y/o comprometidas en otras brechas de datos personales.
- Prohibir el uso de credenciales organizacionales genéricas (el mismo para múltiples usuarios de una organización). El usuario final que accede a datos, junto a la finalidad/justificación del acceso/consulta debe permear hasta el servicio que expone datos para que pueda aplicar políticas de acceso restrictivas.
- Tener y aplicar políticas de acceso a los datos diferenciadas por categorías de responsables, usuarios y tratamientos.
- Añadir un segundo y/o tercer factor de autenticación, sin que eso implique necesariamente tratamientos biométricos o en dispositivos móviles.

Algunos ejemplos de medidas de detección son:

- 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.
- Implementación de sistemas que permitan la detección y mitigación de ataques de enumeración/fuerza fruta.
- Implementación de sistemas que detecten intentos fallidos de acceso a datos, como por ejemplo consultas sistemáticas a DNI u otros datos que den como resultados intentos fallidos.
- Sistemas de detección de situaciones de exfiltración de datos.
- Implementar sistemas de alerta temprana que permitan conocer el ataque lo antes posible y en sus primeras fases a aquellos que tienen las obligaciones de actuar.
- Utilizar sistemas de detección basados en *honey-pots*.

Algunas medidas de respuesta que tienen que estar previstas:

- 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. Por ejemplo, el responsable debe saber de antemano cuál es la Autoridad de Control a la que se debe notificar, qué sucesos motivarán la ejecución del procedimiento, qué persona debe realizar la notificación a la autoridad de control, aprovisionar los medios técnicos o de cualquier índole necesarios para notificar.
- 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.
- En situaciones de gran impacto social, puede estar justificado la utilización de un comunicado público que podría ser un comunicado conjunto entre todos los responsables implicados en la brecha. En algunas situaciones podría ser ampliado a posteriori con comunicaciones individuales si fuera necesario.
- Notificación, en caso de ciberincidente, al CERT correspondiente y respuesta al ciberincidente siguiendo las indicaciones del CERT.
- Denuncia de los hechos a autoridades policiales/judiciales en caso de ilícitos.

Algunas medidas de supervisión y revisión son:

- 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.
- Reuniones periódicas entre los DPD y responsables de seguridad de las entidades intervinientes.
- Auditorias de privacidad (en función de cambios en la naturaleza, contexto, extensión, fines y riesgos del tratamiento art. 24.1) y de seguridad (estas últimas regulares art. 32.1d) en servicios que exponen datos personales a nivel de:
    - Evaluación de impacto del punto común de comunicación de datos.
    - Reevaluación de riesgo para los derechos y libertades individuales y sociales.
    - Grado de implementación de garantías de privacidad y medidas de seguridad.
    - Test de penetración[10].
    - Ataques por ingeniería social.
    - Nivel de respuesta de las medidas organizativas.
    - Procedimientos de gestión de incidentes de seguridad y brechas de datos personales (preventivos y reactivos).

[10] En el RGPD no se menciona explícitamente el requisito de auditoría de protección de datos, pero es un requisito implícito del principio de responsabilidad proactiva, en cuanto a que resulta una herramienta imprescindible para el cumplimiento de los artículos 24 y 32 del RGPD. En cuanto a auditorias de seguridad el ENS establece la obligación de realizarlas al menos cada dos años, cuando haya cambios sustanciales en los sistemas de información, y antes de la puesta en producción de nuevos elementos de software.

X. REFERENCIAS

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.

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

Gestión del riesgo y evaluación de impacto en tratamientos de datos personales.

Guía para la notificación de brechas de datos personales.

WP218 - Statement on the role of a risk-based approach in data protection legal frameworks – WP art. 28

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