MEDIDAS DE RESPONSABILIDAD ACTIVA

El RGPD establece un catálogo de las medidas que los responsables, y en ocasiones los encargados, deben aplicar para garantizar que los tratamientos que realizan son conformes con el Reglamento y estar en condiciones de demostrarlo.

ANÁLISIS DE RIESGO

El RGPD ***condiciona la adopción de las medidas de responsabilidad activa al riesgo que los tratamientos puedan suponer para los derechos y libertades de los interesados***. Se maneja el riesgo de dos maneras:

- En algunos casos, prevé que determinadas medidas solo deberán aplicarse cuando el tratamiento suponga un alto riesgo para los derechos y libertados (por ejemplo, Evaluaciones de impacto sobre la Protección de Datos).
- En otros casos, las medidas deberán modularse en función del nivel y tipo de riesgo que el tratamiento conlleve (por ejemplo, con las medidas de Protección de Datos desde el Diseño o con las medidas de seguridad).

Obligaciones

Grandes organizaciones: como regla general, el análisis deberá llevarse a cabo utilizando alguna de las metodologías de análisis de riesgo existentes.

Organizaciones de menor tamaño y con tratamientos de poca complejidad: el análisis será el resultado de una reflexión, mínimamente documentada, sobre las implicaciones de los tratamientos en los derechos y libertades de los interesados. La reflexión deberá dar respuesta a cuestiones como las que se exponen a continuación. Cuanto mayor sea el número de respuestas afirmativas mayor sería el riesgo que podría derivarse del tratamiento. Si la respuesta a estas preguntas y otras del mismo tipo fuera negativa, es razonable concluir que la organización no realiza tratamientos que generen un elevado nivel de riesgo y que, por tanto, no debe poner en marcha las medidas previstas para esos casos.

- ¿Se tratan datos sensibles?
- ¿Se incluyen datos de una gran cantidad de personas?
- ¿Incluye el tratamiento la elaboración de perfiles?
- ¿Se cruzan los datos obtenidos de los interesados con otros disponibles en otras fuentes?
- ¿Se pretende utilizar los datos obtenidos para una finalidad para otro tipo de finalidades?

- ¿Se están tratando grandes cantidades de datos, incluido con técnicas de análisis masivo tipo big data?
- ¿Se utilizan tecnologías especialmente invasivas para la privacidad, como las relativas a geolocalización, videovigilancia a gran escala o ciertas aplicaciones del Internet de las cosas?

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

Obligaciones

Responsables y encargados deberán mantener un ***registro de operaciones de tratamiento*** en el que se contenga la información que establece el RGPD y que contenga cuestiones como:

- Nombre y datos de contacto del responsable o corresponsable y del Delegado de Protección de Datos si existiese
- Finalidades del tratamiento
- Descripción de categorías de interesados y categorías de datos personales tratados
- Transferencias internacionales de datos…
-

Están ***exentas las organizaciones que empleen a menos de 250 trabajadores***, a menos que el tratamiento que realicen pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional o incluya categorías especiales de datos o datos relativos a condenas e infracciones penales.

Recomendaciones

Las ***posibilidades para organizar el registro de actividades de tratamiento*** son:

- Partir de los ficheros que actualmente tienen notificados los responsables en el Registro General de Protección de Datos, detallando todas las operaciones que se realizan sobre cada conjunto estructurado de datos.
- En torno a operaciones de tratamiento concretas vinculadas a una finalidad básica común de todas ellas (por ejemplo, “gestión de clientes”, “gestión contable” o “gestión de recursos humanos y nóminas”) o con arreglo a otros criterios distintos.

MEDIDAS DE RESPONSABILIDAD ACTIVA II

PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO

- Estas medidas se incluyen dentro de las que debe aplicar el responsable ***con anterioridad al inicio del tratamiento y también cuando se esté desarrollando***.
- Este tipo de medidas reflejan muy directamente el enfoque de responsabilidad proactiva. Se trata de ***pensar en términos de protección de datos desde el mismo momento en que se diseña un tratamiento***, un producto o servicio que implica el tratamiento de datos personales.

Obligaciones

Desde el inicio, ***los responsables deben tomar medidas organizativas y técnicas*** para integrar en los tratamientos garantías que permitan aplicar de forma efectiva los principios del RGPD.

Los responsables deben adoptar ***medidas que garanticen que solo se traten los datos necesarios*** en lo relativo a la cantidad de datos tratados, la extensión del tratamiento, los periodos de conservación y la accesibilidad a los datos.

Medidas de seguridad

En el RGPD, los responsables y encargados establecerán las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado en función de los riesgos detectados en el análisis previo.

A tener en cuenta

Las ***medidas técnicas y organizativas deberán establecerse*** teniendo en cuenta:

- El coste de la técnica
- Los costes de aplicación
- La naturaleza, el alcance, el contexto y los fines del tratamiento
- Los riesgos para los derechos y libertades.

NOTIFICACIÓN DE "VIOLACIONES DE SEGURIDAD DE LOS DATOS"

El RGPD define las violaciones de seguridad de los datos, más comúnmente conocidas como "quiebras de seguridad", de una forma muy amplia, que incluye todo incidente que ocasione la ***destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos***. Sucesos como la pérdida de un ordenador portátil, el acceso no autorizado a las bases de datos de una organización (incluso por su propio personal) o el borrado accidental de algunos registros constituyen violaciones de seguridad a la luz del RGPD y deben ser tratadas como el Reglamento establece.

Obligaciones

Cuando se produzca una violación de la seguridad de los datos, el responsable debe notificarla a la autoridad de protección de datos competente, a menos que sea improbable que la violación suponga un riesgo para los derechos y libertades de los afectados.

La ***notificación de la quiebra*** a las autoridades debe producirse sin dilación indebida y, a ser posible, dentro de las 72 horas siguientes a que el responsable tenga constancia de ella.

La notificación ha de incluir un contenido mínimo:

- La naturaleza de la violación.
- Categorías de datos y de interesados afectados.
- Medidas adoptadas por el responsable para solventar la quiebra.
- Si procede, las medidas aplicadas para paliar los posibles efectos negativos sobre los interesados.

Los responsables deben documentar todas las violaciones de seguridad.

- En los casos en que sea probable que la ***violación de seguridad entrañe un alto riesgo para los derechos o libertades de los interesados***, la notificación a la autoridad de supervisión deberá complementarse con una ***notificación dirigida a estos últimos***.
- El ***objetivo de la notificación a los afectados*** es permitir que puedan tomar medidas para protegerse de sus consecuencias. Por ello, el RGPD requiere que se realice sin dilación indebida, sin hacer referencia ni al momento en que se tenga constancia de ella ni tampoco a la posibilidad de efectuar la notificación dentro de un plazo de 72 horas. El propósito es siempre que el interesado afectado pueda reaccionar tan pronto como sea posible.
- El RGPD añade a los contenidos de la notificación ***las recomendaciones sobre las medidas que pueden tomar los interesados*** para hacer frente a las consecuencias de la quiebra.

MEDIDAS DE RESPONSABILIDAD ACTIVA III

A tener en cuenta

- La ***valoración del riesgo de la quiebra es distinta del análisis de riesgos previo*** a todo tratamiento.

- Se trata de establecer hasta qué punto el incidente, por sus características, el tipo de datos a los que se refiere o el tipo de consecuencias que puede tener para los afectados puede causar un daño en sus derechos o libertades.

- ***Los daños pueden ser*** materiales o inmateriales, e ir desde la posible discriminación de los afectados como consecuencia de su uso por quien ha accedido a ellos de forma no autorizada hasta usurpación de identidad, pasando por perjuicios económicos o la exposición pública de datos confidenciales.

- Se considera que ***se tiene constancia de una violación de seguridad cuando*** hay una certeza de que se ha producido y se tiene un conocimiento suficiente de su naturaleza y alcance.

- La mera ***sospecha de que ha existido una quiebra*** o la constatación de que ha sucedido algún tipo de incidente sin que se conozcan mínimamente sus circunstancias no deberían dar lugar, todavía, a la notificación, dado que en esas condiciones no sería posible, en la mayoría de los casos, determinar hasta qué punto puede existir un riesgo para los derechos y libertades de los interesados.

- En casos de ***quiebras que por sus características pudieran tener gran impacto***, sí podría ser recomendable contactar con la autoridad de supervisión tan pronto como existan evidencias de que se ha producido alguna situación irregular respecto a la seguridad de los datos, sin perjuicio de que esos primeros contactos puedan completarse con una notificación formal más completa dentro del plazo legalmente previsto.

- Puede haber ***casos en que la notificación no pueda realizarse dentro de esas 72 horas***, por ejemplo, por la complejidad en determinar completamente su alcance. En esos casos, es posible hacer la notificación con posterioridad, acompañándola de una explicación de los motivos que han ocasionado el retraso.

- La información puede proporcionarse ***de forma escalonada*** cuando no sea posible hacerlo en el mismo momento de la notificación.

- El criterio de alto riesgo debe entenderse en el sentido de que sea probable que la violación de seguridad ocasione daños de entidad a los interesados. Por ejemplo, en casos en que se desvele información confidencial, como contraseñas o participación en determinadas actividades, se difundan de forma masiva datos sensibles o se puedan producir perjuicios económicos para los afectados.

La notificación a los interesados no será necesaria cuando:

- El responsable hubiera tomado medidas técnicas u organizativas apropiadas con anterioridad a la violación de seguridad, en particular las medidas que hagan ininteligibles los datos para terceros, como sería el cifrado.
- Cuando el responsable haya tomado con posterioridad a la quiebra medidas técnicas que garanticen que ya no hay posibilidad de que el alto riesgo se materialice.
- Cuando la notificación suponga un esfuerzo desproporcionado, debiendo en estos casos sustituirse por medidas alternativas como puede ser una comunicación pública.

MEDIDAS DE RESPONSABILIDAD ACTIVA IV

EVALUACIÓN DE IMPACTO SOBRE LA PROTECCIÓN DE DATOS

Obligaciones

- Los responsables de tratamiento deberán realizar una Evaluación de Impacto sobre la Protección de Datos (EIPD) con carácter previo a la puesta en marcha de aquellos tratamientos que sea probable que conlleven un alto riesgo para los derechos y libertades de los interesados.
- Cuando el análisis de riesgo que las organizaciones lleven a cabo sobre los tratamientos iniciados con anterioridad a la fecha de aplicación del RGPD indiquen que esos tratamientos presentan alto riesgo para los derechos o libertades de los interesados, los responsables deberán realizar una EIPD sobre esos tratamientos, a fin de estar en condiciones de poder adoptar las medidas adecuadas para adecuar esos tratamientos a las exigencias del RGPD.
- En los casos en que las EIPD hayan identificado un alto riesgo que, a juicio del responsable de tratamiento no pueda mitigarse por medios razonables en términos de tecnología disponible y costes de aplicación, el responsable deberá consultar a la autoridad de protección de datos competente. La consulta debe ir acompañada de la documentación que prevé el RGPD, incluyendo la propia Evaluación de Impacto, y la autoridad de supervisión puede emitir recomendaciones o ejercer cualquier otro de los poderes que el RGPD le confiere, entre ellos el de prohibir la operación de tratamiento.

A tener en cuenta

Lista indicativa de supuestos en que se considera que los tratamientos conllevan un alto riesgo:

- Elaboración de perfiles sobre cuya base se tomen decisiones que produzcan efectos jurídicos sobre los interesados o que les afecten significativamente de modo similar.
- Tratamientos a gran escala de datos sensibles.
- Observación sistemática a gran escala de una zona de acceso público.

Para valorar si un tratamiento se realiza a gran escala debe tenerse en cuenta (según el Grupo del Artículo 29, en su designación de Delegados de Protección de Datos):

- El número de interesados afectados, bien en términos absolutos, bien como proporción de una determinada población.

- El volumen de datos y la variedad de datos tratados.
- La duración o permanencia de la actividad de tratamiento.
- La extensión geográfica de la actividad de tratamiento.

Las autoridades de protección de datos están obligadas a confeccionar listas adicionales de tratamientos que requerirán una EIPD. La AEPD elaborará esa lista con anterioridad a la aplicación del RGPD, dado que tiene que ser sometida a la aprobación del futuro Comité Europeo de Protección de Datos y éste sólo se constituirá a partir de la fecha de aplicación del RGPD.

También está previsto que las autoridades puedan elaborar listas de tratamientos en los que no se precisa EIPD. La AEPD elaborará esa lista en las mismas condiciones que la correspondiente a tratamientos en que se deberá realizar Evaluación.

La existencia de estos listados no excluye el que los responsables deban realizar el correspondiente análisis de riesgo y, en caso de que concluyan que existe un alto riesgo para los derechos y libertades de los interesados, lleven a cabo una EIPD, aun cuando el tratamiento en cuestión no esté incluido en ninguna de las dos listas mencionadas. Como se ha dicho, el RGPD se basa en un principio de responsabilidad activa del responsable y es siempre en último extremo el responsable el que debe decidir qué medidas aplicar y cómo hacerlo. La intervención de las autoridades de supervisión o las previsiones del propio RGPD aclaran sus disposiciones o las especifican, pero no sustituyen la responsabilidad de quienes tratan los datos.

Es posible realizar una única EIPD para varios tratamientos similares que entrañen altos riesgos también similares.

Puede ser necesario llevar a cabo una nueva evaluación cuando cambien las condiciones del tratamiento o cuando varíen los riesgos asociados al mismo.