Análisis y gestión de riesgos de los datos personales

El análisis de riesgos es el proceso de identificar y evaluar la probabilidad e impacto derivados de que una amenaza se materialice, y la gestión de esos riesgos tiene como objetivo establecer las acciones que prevengan, reduzcan o eviten en la medida de lo posible la materialización de esas amenazas y que permita minimizar a un nivel aceptable la exposición a los riesgos.

Identificar y evaluar los riesgos son las tareas iniciales del proceso de gestión de riesgos. Asegurar la correcta identificación de los riesgos a los que están expuestas las actividades de tratamiento es una parte clave para poder realizar una evaluación completa. La no identificación de riesgos implica que estos no se evalúan y no se tratan, y el tratamiento podría estar más expuesto al potencial riesgo. Esto conlleva las siguientes acciones:

1. Identificar el origen de los potenciales riesgos a los que puede estar expuestos los datos personales durante todo el ciclo de vida de su tratamiento
2. Analizar los factores y elementos que determinan el nivel de riesgo
3. Valorar las consecuencias de que el riesgo se materialice, teniendo en cuenta la probabilidad de que un evento no deseado se produzca y el impacto de que ello puede tener

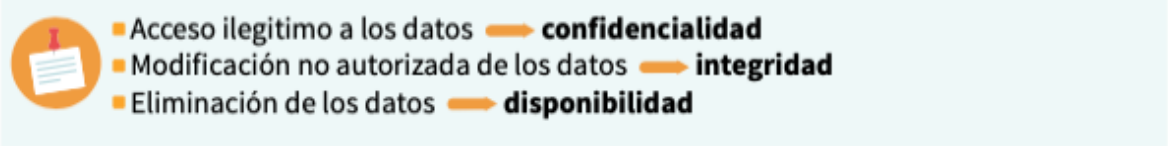
El último paso de la gestión de riesgos es tratar de reducir la explosión al riesgo mediante la aplicación de medidas de control (medidas organizativas, técnicas y de seguridad) que disminuyan la probabilidad y/o el impacto.

Identificar los riesgos

En esta etapa se deben identificar los potenciales escenarios de riesgo que pueden afectar a los datos personales que se van a tratar y a los derechos y libertades de los interesados. Se entiende por riesgo la probabilidad y el impacto de que una amenaza se materialice, siendo una amenaza cualquier elemento o factor que potencialmente pueda provocar un daño o perjuicio.

RIESGO = PROBABILIDAD X IMPACTO

Las amenazas generalmente pueden ser de diferentes tipos (desastres naturales, errores o fallos, ataques intencionados, etc.). Sin embargo, desde la perspectiva de la normativa de protección de datos personales existen amenazas que afectan a las tres dimensiones de la seguridad: confidencialidad, integridad y disponibilidad.



Fuente: Agencia Española de Protección de Datos

Para identificar todas las amenazas a las que puede estar expuestos los tratamientos de los datos personales hay que tener en cuenta todo el ciclo de vida de los datos, identificando todos los escenarios en el que se pueda producir un daño o una violación de los datos y/o de los derechos y libertades de los interesados.

Tipo de amenaza	Amenaza	¿Qué preguntas se pueden formular para identificar la amenaza?
 Acceso ilegítimo a los datos	▪ Perdidas de dispositivos móviles ▪ Fuga de información ▪ Acceso intencionado por parte de personal no autorizado ▪ Ataques intencionados (hacking, suplantación de identidad, etc.) ▪ Uso ilegítimo de datos personales	▪ *¿Los **dispositivos móviles y de almacenamiento** están cifrados?* ▪ *¿Existen **métodos para extraer la información** durante la operación de tratamiento?* ▪ *¿Está expuesta la información al **acceso por parte de terceros** no autorizados? ¿**Existe un mecanismo** para dar acceso a los datos únicamente al personal autorizado?* ▪ *¿La operación de tratamiento es susceptible de **ataques de hacking?** ¿es susceptible de **ataques de phishing** o de otros métodos de suplantación de identidad?* ▪ *¿Existe una adecuada gestión de la configuración de los **parámetros de seguridad** de los elementos (elementos de red, SO y BBDD)* ▪ *¿Existe una **base legitimadora** para la actividad de tratamiento? ¿las **finalidades de las actividades** de tratamiento son necesarias y proporcionales?*
 Modificación no autorizada de los datos	▪ Ataque para la suplantación de identidad ▪ Errores en los procesos de recopilación y captura de información ▪ Modificación no autorizada de datos intencionada ▪ Uso ilegítimo de datos personales	▪ *¿Existen **credenciales o mecanismos de control** que limiten el acceso a personal no autorizado? ¿Se **revisa periódicamente la actividad** realizada por los usuarios cuando acceden a los sistemas?* ▪ ***¿Existen** controles sobre la integridad de la información durante el proceso de captura de datos? ¿se **identifica adecuadamente al interesado** que proporciona los datos?* ▪ *¿Los **datos son modificables** únicamente por el personal autorizado?* ▪ *¿La actividad de tratamiento sobre los datos son acordes a las finalidades para las cuales existe una **base legitimadora?** ¿se puede realizar un perfilado o una operación de tratamiento que no esté alineada con las finalidades de la operación de tratamiento?*
 Eliminación de los datos	▪ Corte de suministro eléctrico o fallos en servicios de comunicaciones ▪ Error humano o ataque intencionado que provoca borrado o pérdida de datos ▪ Desastres naturales	▪ *¿Un **fallo de suministro eléctrico** puede implicar la pérdida de datos? ¿Un fallo en los servicios de comunicaciones puede ocasionar una pérdida de datos?* ▪ *¿Los datos pueden ser **eliminados únicamente por el personal autorizado**? ¿Existen **copias de seguridad?*** ▪ *¿Están los sistemas que **almacenan datos en ubicaciones expuestas** a la posibilidad de que se produzca un desastre natural? ¿Existe **réplica de los datos** en diferentes ubicaciones?*

Ejemplo de amenazas en función de su tipología
Fuente: Agencia Española de Protección de Datos

Evaluar los riesgos

La evaluación de riesgos consiste en valorar y estimar la probabilidad y el impacto de que la amenaza se materialice. Existen distintos criterios para valorar y cuantificar los riesgos y estimar el nivel de impacto y su probabilidad. Dicha evaluación puede ser cualitativa o cuantitativa, y se pueden basar en estándares.

Aquí se propone realizar una evaluación de los riesgos en la que se analicen en primer lugar los riesgos inherentes al tratamiento de los datos y, tras la definición de los controles o medidas de seguridad y su aplicación, se evalúen los riesgos residuales a los que quedará expuesto el tratamiento y que deberán se aceptables para garantizar un nivel de seguridad adecuado teniendo en cuenta el coste de la tecnología que se vaya a emplear, de su aplicación, de la naturaleza, el alcance, el contexto y los fines del tratamiento, y de los riesgos para los derechos y libertades de los interesados.

El riesgo inherente es aquel intrínseco a cada actividad de tratamiento, sin tener en cuenta la medidas o controles que mitiguen o reduzcan el nivel de exposición de los datos a las amenazas. El cálculo de riesgo inherente será el producto de la probabilidad de que la amenaza se materialice por el impacto de los datos que se pueden producir al materializarse la amenaza.

Escala de valores para el cálculo de la probabilidad:

- Probabilidad despreciable: posibilidad de ocurrencia muy baja, sucede de forma fortuita. Se valorará con 1.
- Probabilidad limitada: posibilidad de ocurrencia baja, sucede de forma ocasional. Se valorará con 2.
- Probabilidad significativa: posibilidad de ocurrencia alta, sucede con bastante frecuencia. Se valorará con 3.
- Probabilidad máxima: posibilidad de ocurrencia muy elevada, sucede con mucha frecuencia. Se valorará con 4.

Escala de valores para el cálculo del impacto:

- Impacto despreciable: impacto muy bajo, sus consecuencias son prácticamente despreciables sin impacto sobre el interesado. Se valorará con 1.
- Impacto limitado: impacto bajo, sus consecuencias suponen un daño menor sin impacto sobre el interesado. Se valorará con 2.
- Impacto significativo: impacto alto, sus consecuencias suponen un daño elevado con impacto sobre el interesado. Se valorará con 3.
- Impacto máximo: impacto muy alto, sus consecuencias suponen un daño muy elevado con un impacto crítico sobre el interesado. Se valorará con 4.

Las consecuencias del impacto pueden producir daños de diferente tipo, aquí se van a considerar tres dimensiones diferentes de posibles daños sobre el interesado:

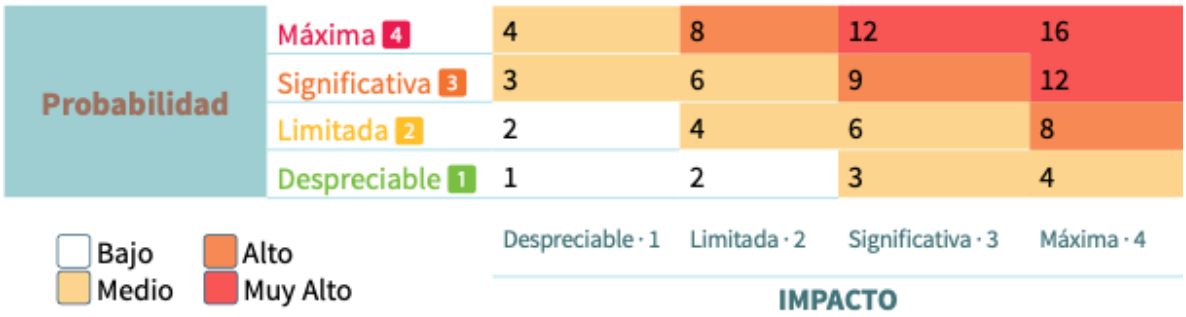
a) Daño físico: acciones que pueden ocasionar un daño en la integridad física del interesado.
b) Daño material: acciones que pueden ocasionar pérdidas económicas, patrimoniales, laborales, etc.
c) Daño moral: acciones que pueden ocasionar un daño moral o mental en el interesado, como una depresión, fobias, acoso, etc.

Para evaluar el impacto se tendrá en cuenta el tipo de daños y el perjuicio que puede causar. En la siguiente tabla se pueden ver ejemplos de los niveles de impacto.

	Ejemplos de posibles daños físico, material o moral
Despreciable: *Los interesados no se verán prácticamente afectados o encontrarán alguna pequeña inconveniencia*	▪ Molestias o irritación. ▪ Se incumplen obligaciones materiales sin perjuicios relevantes. ▪ No se priva de los derechos y libertades.
Limitado: *Los interesados podrán encontrar inconveniencias no significativas*	▪ Estrés o padecimientos físico menores. ▪ Costes extra, denegación de acceso a algunos servicios o incumplimiento de obligaciones materiales con perjuicios económicos. ▪ Se priva de los derechos y libertades de los interesados, por ejemplo, por difamación de un interesado por divulgación de datos personales.
Significativo: *Los interesados encontrarán consecuencias significativas, que deberían poder superar sin dificultades serias.*	▪ Empeoramiento del estado de salud o agresiones físicas. ▪ Apropiación indebida de fondos, pérdida del empleo o incumplimiento de obligaciones materiales con perjuicios económicos relevantes. ▪ Se agrede contra los derechos y libertades de los interesados, por ejemplo, una citación judicial, entrar en una lista de morosidad o divulgación de datos personales con impacto significativo en la reputación del interesado.
Máximo: *Los interesados encontrarán consecuencias significativas o incluso irreversibles, que podrán no llegar a superarse.*	▪ Agresiones físicas con consecuencias irreparables. ▪ Asunción de una deuda inafrontable, imposibilidad de volver a trabajar o incumplimiento de obligaciones materiales con perjuicios económicos irreparables. ▪ Se agrede significativamente contra los derechos y libertades de los interesados, por ejemplo, padecimiento psicológico con consecuencias a largo plazo o irreparables por la divulgación de datos sensibles.

Fuente: Agencia Española de Protección de Datos

Para poder determinar el riesgo inherente, asignando los valores indicados más arriba para cada una de las escalas de probabilidad e impacto (valores de 1 o despreciable a 4 o valor máximo), multiplicaremos para cada amenaza identificadas el valor de la probabilidad por el valor del impacto. El resultado será una matriz de riesgos como la siguiente:



Fuente: Agencia Española de Protección de Datos

El resultado de esta matriz nos mostrará el riesgo inherente, estimado la probabilidad por al impacto de que una amenaza se materialice. Este riesgo se puede clasificar según los siguientes niveles:

- Riesgo bajo: valores entre 1 y 2
- Riesgo medio: valores entre 3 y 6
- Riesgo alto: valores entre 7 y 9
- Riesgo muy alto: valores entre 10 y 16

Ejemplo de valoración del riesgo inherente:

Tipo de amenaza	Amenaza	Riesgo	Probabilidad	Impacto	Riesgo inherente
Acceso ilegítimo a los datos	Fuga de información	Terceras personas acceden a los datos vulnerado su confidencialidad	Significativa Valoración: 3	Significativo Valoración: 3	Alto Valoración: 9
	Operaciones de tratamiento no autorizadas	Uso ilegítimo de los datos que vulneran los derechos de los interesados	Máxima Valoración: 4	Limitado Valoración: 2	Alto Valoración: 8
Modificación no autorizada de los datos	Ataque de software malicioso (Ciberataque)	Se modifican los datos perdiendo su integridad	Significativa Valoración: 3	Limitado Valoración: 2	Medio Valoración: 6
	Operaciones de tratamiento que modifican los datos de forma ilegítima	Uso ilegítimo de los datos que vulneran los derechos de los interesados	Máxima Valoración: 4	Significativo Valoración: 3	Muy Alto Valoración: 12

Indisponibilidad de los datos	Corte del suministro eléctrico que impide el acceso a los datos	Imposibilidad de acceso a los datos porque no están disponibles	Limitada Valoración: 2	Limitado Valoración: 2	Medio Valoración: 4
	Ciberataque que impide acceder a los datos	Imposibilidad de acceso a los datos porque no están disponibles	Significativa Valoración: 3	Significativo Valoración: 3	Alto Valoración: 9

Gestionar los riesgos

El siguiente paso que hay que realizar es tratar estos riesgos para reducirlos a niveles aceptables. Esto lo conseguiremos aplicando las medias de control o seguridad adecuadas que permitan reducir la probabilidad y/o el impacto asociados a los riesgos inherentes.

Para reducir o mitigar el nivel de riesgo se puede pueden realizar las siguientes acciones:

1. Reducir el riesgo mediante la aplicación de medidas de control
2. Transferir riesgo a un tercero. Por ejemplo, se puede contratar un seguro que cubra las consecuencias materiales de materializarse los riesgos
3. Anular el riesgo no realizando el tratamiento de datos. Por ejemplo, si el riesgo es muy elevado y no hay forma de mitigarlo o reducirlo, se se puede decidir no iniciar el tratamiento de los datos

También es posible que el nivel de riesgo inherente esté dentro de los márgenes que se consideran aceptables, en cuyo caso se puede decidir que es necesario implementar controles adicionales.

En el supuesto que se decida por reducir el riesgo, que es la práctica más habitual, se deberán aplicar medidas de control que reduzcan los riesgos a un nivel aceptable que permita realizar el tratamiento con garantías en cuanto a la seguridad de los datos y los derechos y las libertades de los interesados. Estas medidas de control pueden ser de índole organizativa (por ejemplo, decidir qué usuarios están autorizados a tratar los datos, definir protocolos para la gestión de incidentes de seguridad o gestionar vulnerabilidades) y técnica (por ejemplo, qué controles de acceso de aplica, cifrado de los datos, realización de copias de seguridad, etc.)

Una vez aplicadas estas medidas de control, el riesgo que aún persista y que hemos considerado aceptable se denomina riesgo residual. Para el cálculo del riesgo residual se tendrán en cuenta las medidas de control a la hora de cuantificar la probabilidad y el impacto de que las amenazas se materialicen.

Ejemplo de valoración de riesgo residual:

Tipo de amenaza	Amenaza	Riesgo	Control	Probabilidad	Impacto	Riesgo residual
Acceso ilegítimo a los datos	Fuga de información	Terceras personas acceden a los datos vulnerado su confidencialidad	Acceso a usuarios autorizados mediante el uso de credenciales y MFA	Despreciable Valoración: 1	Significativo Valoración: 3	Medio Valoración: 3
	Operaciones de tratamiento no autorizadas	Uso ilegítimo de los datos que vulneran los derechos de los interesados	Acceso a usuarios autorizados mediante el uso de credenciales y MFA	Despreciable Valoración: 1	Limitado Valoración: 2	Bajo Valoración: 2
Modificación no autorizada de los datos	Ataque de software malicioso (Ciberataque)	Se modifican los datos perdiendo su integridad	Utilización de sistema antivirus de última generación	Despreciable Valoración: 1	Limitada Valoración: 2	Bajo Valoración: 2
	Operaciones de tratamiento que modifican los datos de forma ilegítima	Uso ilegítimo de los datos que vulneran los derechos de los interesados	Acceso a modificar los datos sólo a los perfiles de usuario autorizados	Despreciable Valoración: 1	Significativo Valoración: 3	Medio Valoración: 3
Indisponibilidad de los datos	Corte del suministro eléctrico que impide el acceso a los datos	Imposibilidad de acceso a los datos porque no están disponibles	Utilización de sistemas de alimentación ininterrumpida	Despreciable Valoración: 1	Limitado Valoración: 2	Bajo Valoración: 2
	Ciberataque que impide acceder a los datos	Imposibilidad de acceso a los datos porque no están disponibles	Utilización de sistema antivirus de última generación	Limitada Valoración: 2	Significativo Valoración: 3	Medio Valoración: 6