GUÍA PRÁCTICA

Evaluación de impacto relativa a la protección de datos

apdcat

Autoritat Catalana de Protecció de Dades

Índice de contenidos

1. Introducción

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento y la libre circulación de datos personales, en definitiva el Reglamento general de protección de datos (en adelante, RGPD o Reglamento), incorpora una nueva obligación para los responsables de tratamiento: evaluar el impacto de las operaciones de tratamiento en la protección de los datos personales, cuando sea probable que el tratamiento suponga un riesgo significativo para los derechos y las libertades de las personas.

En general, la reforma de la protección de datos en Europa propone un modelo de cumplimiento orientado a la gestión, que supere el modelo previo, de carácter demasiado formalista en algunos de sus aspectos. De la nueva regulación destaca el hecho de que hay que demostrar que se cumplen las obligaciones, y precisamente las evaluaciones de impacto relativas a la protección de los datos de carácter personal (en adelante, EIPD) se sitúan en el punto de partida para demostrar una gestión responsable de los tratamientos.

La ejecución de las EIPD debe basarse en métodos sistemáticos, a fin de que resulten objetivas, repetibles y comparables, y queden documentadas. Por ello, los contenidos de esta guía tienen como finalidad orientar en la forma de abordar la ejecución de las evaluaciones de impacto, de acuerdo con lo previsto en el RGPD.

Podemos clasificar los riesgos asociados a un tratamiento en dos tipos: los riesgos inherentes al tratamiento (como ha sido diseñado) y los riesgos asociados a la seguridad de los datos. El enfoque en el riesgo que propone el Reglamento exige analizar los riesgos y, si son demasiado altos, reducirlos.

Cuando los riesgos inherentes al tratamiento son demasiado altos, hay que modificar el tratamiento; esto se puede hacer, por ejemplo, evitando el tratamiento de algún tipo de dato especialmente sensible o restringiendo el acceso a ciertos tipos de datos.

El tratamiento de los riesgos asociados a la seguridad de los datos debe basarse en un análisis del riesgo asociado a la pérdida de la confidencialidad, la integridad y la disponibilidad de los datos. Las metodologías de análisis de riesgos estándar (por ejemplo, ISO y Magerit) son complejas y pueden ser difíciles de llevar a cabo por organizaciones pequeñas. En esta guía proponemos una metodología alternativa, que busca simplificar el análisis, pero sin reducir la exhaustividad de las medidas de control. Cuando el análisis de riesgos sugiere que el riesgo es demasiado alto, hay que aplicar controles de seguridad para reducirlo.

2. Introducción a las EIPD

Puntos clave

- Una evaluación de impacto en protección de datos (EIPD) es un procedimiento que pretende identificar y controlar los riesgos asociados a un tratamiento de datos.
- Es necesario hacer una EIPD cuando el tratamiento puede suponer un alto riesgo para los derechos y las libertades de las personas.

2.1 ¿Qué es una evaluación de impacto?

Una evaluación de impacto en protección de datos (EIPD) es un procedimiento que busca identificar y controlar los riesgos para los derechos y las libertades de las personas, asociados a un tratamiento de datos. Las EIPD también son instrumentos útiles en relación con el principio de responsabilidad proactiva[1].

El Reglamento establece los derechos que tienen las personas con respecto al tratamiento de sus datos (derecho a la información, etc.). Sin embargo, cuando se habla de los "riesgos para los derechos y las libertades de las personas" no nos limitamos a los derechos reconocidos por el Reglamento, sino a cualquier efecto que el tratamiento pueda tener sobre los derechos y las libertades fundamentales de las personas: derecho a la libertad de expresión, a la libertad de pensamiento, a la prohibición de sufrir discriminación, a la libertad de conciencia, a la libertad de religión, etc.

Al identificar los riesgos, debemos considerar cualquier impacto que el tratamiento pueda tener sobre las personas (físico, económico, emocional, etc.). Algunos impactos potenciales son:

- Imposibilidad de acceder a servicios u otras oportunidades
- Discriminación
- Robo de la identidad y otros fraudes
- Pérdidas económicas
- Daños a la reputación
- Daños físicos
- Pérdida de la confidencialidad
- Imposibilidad de ejercer algún derecho

Estos impactos pueden materializarse por dos razones principales. La primera es que el tratamiento, tal y como está diseñado, pueda dar lugar a estos impactos; ya sea por el tipo de datos que se tratan, por quien tiene acceso, por ejemplo, el potencial efecto del tratamiento, etc. La segunda está relacionada con la seguridad de los datos; en particular, la pérdida de la confidencialidad, la integridad o la disponibilidad de los datos.

Para controlar los riesgos inherentes al tratamiento, debemos establecer los controles necesarios para garantizar que el tratamiento se realiza de acuerdo con el RGPD. En

[1] *Accountability*, en su término en inglés.

particular, que es necesario y proporcional y que se establecen los mecanismos necesarios para que los interesados puedan ejercer sus derechos.

Para controlar los riesgos que afectan a la seguridad de los datos, hay que hacer un análisis que permita identificar y valorar los riesgos y, después, establecer las salvaguardas apropiadas a las valoraciones de riesgo.

2.2 ¿Cuándo hay que hacer una evaluación de impacto?

El RGPD exige que el responsable del tratamiento realice una EIPD, cuando el tratamiento puede conllevar un riesgo alto para los derechos y las libertades de las personas. El RGPD no describe qué se entiende por riesgo alto; se limita a dar una lista de tres casos en que la EIPD es obligatoria[1].

Dada la falta de especificidad del RGPD, seguiremos el procedimiento descrito en el GT29, que da una lista de nueve características de los tratamientos que pueden ser indicativas de un riesgo alto (véase más abajo). A mayor número de estas características, más probable es que un tratamiento presente un riesgo grave. Según el GT29, hay que hacer una EIPD cuando el tratamiento presenta dos o más, aunque indica que puede ser conveniente hacer el EIPD incluso en algunos casos en que solo presenta una.

1 **Evaluación o puntuación, incluidas la elaboración de perfiles y predicciones**
Especialmente en relación con el rendimiento laboral, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, ubicación o movimientos. Ejemplos:

- Una institución financiera que investiga a sus clientes en una base de datos de referencia de crédito.
- Una empresa biotecnológica que ofrece pruebas genéticas para evaluar y predecir los riesgos de padecer enfermedades.
- Una empresa que hace perfiles de comportamiento basados en la navegación web

2 **Toma de decisiones automatizada con efectos jurídicos o que afecta de manera similar y significativa a la persona física**

Por ejemplo, un tratamiento automatizado que puede dar lugar a exclusión o discriminación de las personas.

3 **Observación sistemática de un área de acceso público**

En este tratamiento, los datos se pueden recoger sin que los interesados sean conscientes de que se están recogiendo y de cómo se usarán.

4 **Datos sensibles**

Esto incluye las categorías especiales de datos mencionadas en el artículo 9 del RGPD:

- Origen racial o étnico
- Opiniones políticas o filosóficas
- Afiliación a un sindicato
- Datos genéticos
- Datos biométricos tratados con el fin de identificar a una persona de forma exclusiva

[1] RGPD, artículo 35.3.

- Datos relativos a la salud
- Datos relativos a la vida sexual o a la orientación sexual

También incluye:

- Datos relativos a condenas o a delitos penales
- Datos que aumentan el riesgo para los derechos y las libertades de las personas (como datos de comunicaciones electrónicas, datos de localización y datos financieros)
- Documentos personales, correo electrónico, diarios, notas de lectores de libros electrónicos e información personal incluida en aplicaciones de registro de actividades vitales.

5 Tratamiento de datos a gran escala

Para determinar si un tratamiento es a gran escala, hay que tener en cuenta los factores siguientes:

- El número de personas a las que se refieren los datos ya sea en términos absolutos o como proporción de la población subyacente
- El volumen o la variedad de datos
- La duración o permanencia de la operación de tratamiento
- La extensión geográfica de la operación de tratamiento

6 Conjuntos de datos que se han enlazado o combinado

7 Datos relacionados con personas vulnerables

Esto incluye todas las situaciones en las que se detecte un desequilibrio entre la posición del responsable del tratamiento y el interesado. Por ejemplo:

- Tratamiento de datos de empleados en relación con la gestión de recursos humanos
- Niños y personas mayores
- Personas con enfermedades mentales
- Solicitantes de asilo

8 Uso innovador de tecnologías

9 Tratamiento que en sí mismo impide el ejercicio de un derecho o el uso de un servicio o contrato

Por ejemplo:

- Tratamientos hechos en un espacio público que los transeúntes no pueden evitar.
- Consulta del historial de crédito de un cliente por parte de un banco, para decidir si le concede un crédito

Comentarios

- En versiones anteriores de la guía sobre EIPD del GT29 aparecía un supuesto adicional: la transferencia de datos fuera de la UE. En la revisión 1 se eliminó este supuesto.
- Según el artículo 35.4 del RGPD las autoridades de protección de datos deben publicar una lista de tratamientos para los que se debe hacer la EIPD. Hay una tendencia general de adoptar la propuesta del GT29.

Ejemplos

- Un hospital que trata datos sanitarios de sus pacientes.
  Criterios que son aplicables:
  - Datos sensibles.
  - Tratamiento a gran escala.
  - Datos relativos a personas vulnerables.
- Uso de cámaras para controlar el comportamiento de los conductores. Se prevé el uso de un sistema inteligente para seleccionar coches y reconocer matrículas.
  Criterios que son aplicables:
  - Observación sistemática.
  - Uso innovador de tecnologías.
- Una empresa que observa sistemáticamente las actividades de sus trabajadores: del puesto de trabajo, de la actividad en internet, etc.
  Criterios que son aplicables:
  - Observación sistemática.
  - Datos relativos a persones vulnerables.
- Recogida de datos públicos para elaborar perfiles.
  Criterios que son aplicables:
  - Evaluación o puntuación.
  - Tratamiento a gran escala.
  - Conjuntos de datos que se han enlazado o combinado.

Independientemente del riesgo que pueda tener un tratamiento, en los casos siguientes no es necesario hacer una EIPD:

- Cuando la naturaleza, el alcance, el contexto y las finalidades del tratamiento son muy similares a otro tratamiento para el que ya se ha hecho una EIPD.
- Cuando un tratamiento tiene una base jurídica en el derecho de la UE o de un estado miembro, y ya se ha hecho una EIPD en el momento de adoptar esta base jurídica.
- Cuando el tratamiento está incluido en una lista de tratamientos (publicada por la autoridad competente) que no requieren una EIPD. Por el momento, ni la APDCAT ni la AEPD han publicado esta lista.

Comentarios

- No es necesario hacer una EIPD si el RGPD no es de aplicación al tratamiento.
- El RGPD es de aplicación al tratamiento de datos personales realizado por una empresa u organización situada en la UE o en un lugar donde el derecho comunitario sea de aplicación, o por una empresa u organización situada fuera de la UE, si esta trata datos de personas residentes en la UE para actividades relacionadas con la oferta de bienes o servicios y para controlar el comportamiento.

Las operaciones de tratamiento pueden evolucionar rápidamente, lo que puede afectar a los riesgos y a la necesidad de ejecutar una EIPD, además de los cambios en el contexto del tratamiento. Por ejemplo, cambios en la estructura organizativa del responsable del tratamiento, o cambios sociales que incrementan el riesgo o la percepción que tenemos. Un ejemplo del último caso sería cuando la sociedad toma conciencia de que hay un grupo de personas que es vulnerable a sufrir discriminación.

Si la EIPD es obligatoria y no se ejecuta, los tratamientos quedan expuestos a unos riesgos no detectados. No habrán analizado ni valorado y, en consecuencia, no se habrán adoptado las medidas que deberían servir para mitigar los efectos negativos que las operaciones de tratamiento pueden tener para los derechos y las libertades de las personas. Según el artículo 83 del RGPD, no hacer una EIPD que es necesaria es una infracción sancionable.

2.3 ¿Cómo se hace una EIPD?

▪ ¿En qué momento debe hacerse la EIPD?

Hay que hacer la EIPD tan pronto como sea posible. En particular, para nuevos tratamientos hay que hacerla antes de empezar a tratar los datos. Esto está de acuerdo con la protección de datos en el diseño y por defecto, y permite hacer uso de la EIPD como herramienta para ayudar a la toma de decisiones en el diseño del tratamiento.

En el caso de una operación de tratamiento que ya está en marcha, conviene hacer una EIPD tan pronto como se detecte un riesgo grave para los derechos y las libertades de las personas. Conviene remarcar que las EIPD no son una tarea puntual, sino que implican un proceso continuo de revaluación. En particular, hay que reevaluar la necesidad de hacer una EIPD cuando se producen cambios significativos en la operación de tratamiento o en su contexto (organizativo o social).

▪ ¿Quién interviene en una EIPD?

El responsable del tratamiento es el actor principal, dado que es quien tiene la responsabilidad de que la EIPD se ejecute. Esto no quita que el responsable del tratamiento pueda delegar la EIPD, pero, en cualquier caso, es quien tiene la responsabilidad última.

El encargado del tratamiento, si lo hay, debe apoyar al responsable en el momento de hacer la EIPD.

El responsable del tratamiento debe buscar el consejo del delegado de protección de datos (DPD). Este consejo y las decisiones que tome deben quedar documentadas en la EIPD. En particular, el responsable del tratamiento debe pedir opinión al DPD en los aspectos siguientes:

- Determinar si hay que hacer una EIPD.
- La metodología que se usará en la EIPD.
- Determinar si conviene hacer la EIPD internamente o si es mejor externalizarla.

- Las medidas adoptadas para proteger los derechos y las libertades de las personas.
- Determinar si la EIPD se ha realizado correctamente y si las conclusiones satisfacen los requerimientos de protección de datos.

El responsable del tratamiento debe buscar la opinión de los interesados sobre la operación de tratamiento, cuando ello se considere apropiado. Si no se considera apropiado, hay que documentar el porqué; por ejemplo, porque buscar esta opinión tiene un coste desproporcionado, es impracticable o puede poner en riesgo la confidencialidad del plan de negocio.

La opinión de los interesados se puede recoger de diferentes maneras: encuestas, consulta a la persona representante de los trabajadores, etc. En cualquier caso, es necesario que el responsable del tratamiento tenga base legal para tratar cualquier dato personal que se genere al recoger estas opiniones.

Además de los actores anteriores, puede ser necesario que concurran una serie de agentes internos o externos a la organización, como pueden ser unidades o áreas específicas, expertos independientes, responsables de seguridad, etc.

¿Cuál es el contenido mínimo de una EIPD?

El resultado final de una evaluación de impacto no deja de ser un informe, o un conjunto de documentación, que recoge las características del tratamiento evaluado y las decisiones tomadas para mitigar los riesgos, de acuerdo con su identificación, análisis, valoración. En base a estos riesgos, también se valora la necesidad y la proporcionalidad de las operaciones de tratamiento.

El RGPD fija el siguiente contenido mínimo para una EIPD:

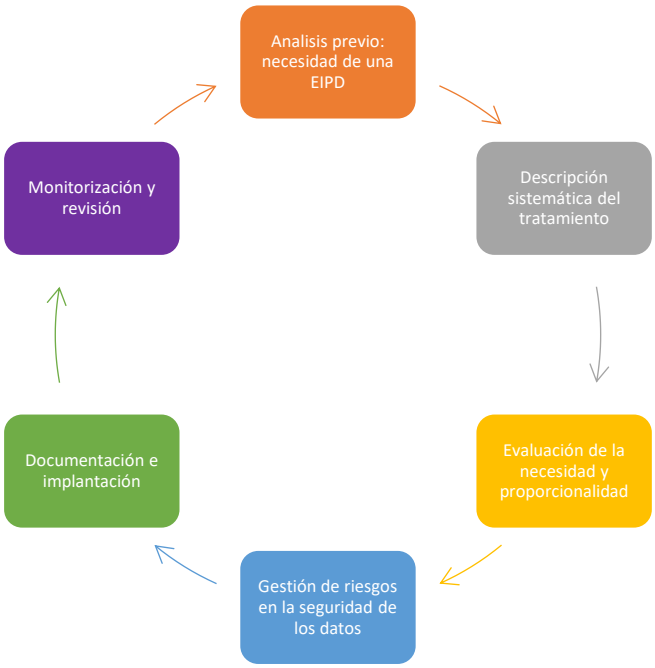
- Descripción de las operaciones de tratamiento.
- Evaluación de la necesidad y de la proporcionalidad del tratamiento.
- Evaluación del riesgo para los derechos y las libertades de las personas.
- Medidas adoptadas para mitigar los riesgos.

¿Cuáles son las fases de una EIPD?

La realización de una EIPD debe seguir un proceso sistemático, objetivo, repetible y comparable. En esta guía, proponemos una metodología estructurada en seis fases:

1. Necesidad de hacer una EIPD. Aunque esta parte debería ser un análisis previo a la EIPD, para que quede constancia de que se ha analizado la necesidad de hacerla, será la primera sección en la plantilla de EIPD que proponemos. Esta parte es especialmente interesante cuando se concluye que no es necesario hacer el EIPD.
2. Descripción sistemática del tratamiento. La descripción del tratamiento y el contexto en que tiene lugar es esencial para determinar los riesgos que conlleva.
3. Evaluación de la necesidad y la proporcionalidad del tratamiento. Cualquier tratamiento de datos tiene una finalidad. Hay que diseñar el tratamiento que sea menos intrusivo para alcanzar este fin (necesidad) y es necesario que el beneficio del tratamiento sea superior a potenciales perjuicios (proporcionalidad).
4. Gestión de riesgos en la seguridad de los datos. Se evalúa el riesgo sobre los derechos y las libertades de las personas que puede tener la vulneración de la seguridad de los datos. El riesgo se deriva del impacto y de la probabilidad de que la vulneración se produzca. Cuanto más alto sea el riesgo, más exhaustivos deben ser los controles para reducirlo.

5. Documentación e implantación. El resultado de una EIPD es un documento que describe los análisis hechos en los puntos anteriores. Las medidas adoptadas para salvaguardar los derechos y las libertades de las personas se deben implementar en el sistema de tratamiento.
6. Monitorización y revisión. La EIPD no se acaba cuando se completa la documentación y la implantación. Las EIPD necesitan un proceso de monitorización para detectar cambios en los riesgos (ya sea a consecuencia de cambios en el tratamiento o en la percepción de riesgo de la sociedad), que pueden requerir que se revise la EIPD o, incluso, que se rehaga.



2.4 ¿Qué se debe hacer si la EIPD concluye que el riesgo es alto?

Según el artículo 36, si la EIPD concluye que el tratamiento conlleva un alto riesgo, el responsable del tratamiento debe consultar a la autoridad de control antes de iniciar el tratamiento.

Una vez la autoridad de control tiene toda la documentación necesaria, debe responder por escrito en un plazo de ocho semanas. Este plazo se puede ampliar seis semanas más, de acuerdo con la complejidad del tratamiento.

En el contexto de una consulta previa, la autoridad de protección de datos puede utilizar cualquiera de los poderes recogidos en el artículo 58 del RGPD, tanto los de investigación como los correctivos. Por ejemplo "imponer una limitación temporal o definitiva del tratamiento, incluida la prohibición ".

.

3. Descripción sistemática del tratamiento

Puntos clave

- Es esencial dar una descripción sistemática del tratamiento, para conocer los riesgos potenciales que implica.
- Proponemos una lista de preguntas que ayudarán al responsable de los datos a hacer esta descripción; se remarcan los aspectos más relevantes desde el punto de vista de los riesgos.

Para poder determinar de forma precisa qué riesgos pueden afectar a un tratamiento, hay que conocer con detalle el tratamiento y el contexto donde se produce. Proponemos la siguiente lista de preguntas, como una guía que el responsable del tratamiento puede usar para describir el tratamiento. El objetivo de las preguntas es poner en relieve aspectos que pueden ser clave en el momento de determinar los riesgos del tratamiento[1].

3.1 ¿Cuál es el tratamiento de datos?

El objetivo de esta pregunta es delimitar la operación de tratamiento que se está considerando, a la vez que se hace una primera descripción.

¿Qué operaciones de tratamiento se pueden evaluar en una EIPD?

Una EIPD puede hacer referencia a una o a múltiples operaciones de tratamiento, si son similares en términos de tipos de datos, alcance, contexto, finalidad y riesgos.

También se puede hacer una EIPD para evaluar el impacto que tiene una aplicación o plataforma de tratamiento. Esto no exime al responsable del tratamiento que haga uso de esta aplicación o plataforma, de realizar una EIPD adaptada a su caso, pero la puede basar en la de la aplicación.

Ejemplos

- Un hospital gestiona datos médicos de los pacientes: historial médico, datos de contacto, etc.
- El sistema de recursos humanos de una empresa gestiona datos personales de sus empleados: datos de contacto, datos bancarios, retribuciones, periodos de baja y de vacaciones.

3.2 ¿Cuál es la finalidad del tratamiento?

Según el RGPD, la finalidad de un tratamiento debe ser explícita, legítima y determinada antes de recoger los datos.

Guidelines for SME on the security of personal data processin, ENISA, diciembre 2016.

La obligación del responsable de especificar la finalidad del tratamiento antes de iniciarlo ayuda a los interesados a entender el uso que se hará de sus datos; de este modo, permite que los interesados tomen decisiones informadas en relación con el uso de sus datos. Aparte, evita que, una vez recogidos, los datos se usen con otros fines.

El principio de limitación de la finalidad está estrechamente relacionado con otros principios, como el de licitud, lealtad y transparencia. La transparencia exige que los interesados tengan conocimiento del uso que se hace de sus datos. No se puede evaluar la licitud y la lealtad de un tratamiento si no se conoce su finalidad.

Ejemplo

- Una empresa trata los datos de sus clientes con el fin exclusivo de cumplir con sus obligaciones contables.
- El departamento de marketing de una empresa quiere hacer uso de los datos de sus clientes para enviar publicidad.

Aunque en los casos anteriores los datos tratados pueden ser los mismos, la finalidad es muy distinta. Esto hace que la base legal del tratamiento también sea diferente. En el primer caso, el responsable de los datos hace el tratamiento para cumplir con una obligación legal. En el segundo caso, el consentimiento es una base legal más apropiada.

3.3 ¿Tipos y características de los datos a tratar?

Aunque esta pregunta está relacionada con la operación de tratamiento (pregunta 1), conviene especificar claramente cuáles son los tipos y las características de los datos a tratar. Esto tiene importancia a la hora de determinar los riesgos asociados a la operación de tratamiento, sus bases legales y la forma de obtener el consentimiento.

Las características más relevantes de los datos son:

- Fuente de los datos

Conviene especificar si los datos se han obtenido directamente del interesado o de una tercera parte y, si es así, especificarla.

- Plazo de conservación

Los datos no deben conservarse más tiempo del necesario para alcanzar la finalidad del tratamiento.

- Datos especialmente sensibles

El RGPD habla de *categorías especiales* de datos personales para referirse a los tipos de datos que, por su naturaleza, presentan unos riesgos mayores para los derechos y las libertades de las personas. El RGPD limita el tratamiento que se puede hacer de estos datos. Los siguientes tipos de datos forman parte de las categorías especiales de datos:

- Origen étnico o racial
- Opiniones políticas
- Convicciones religiosas o filosóficas
- Afiliación sindical
- Datos genéticos
- Datos biométricos capaces de identificar de manera unívoca a una persona
- Datos relativos a la salud

- Datos relativas a la vida o a la orientación sexual de una persona

Pese a no estar contenidas dentro de las categorías especiales, el tratamiento de datos relacionados con condenas o infracciones penales también está sujeto a más restricciones.

Del mismo modo, los datos de personas vulnerables (en particular, los menores) también reciben una protección especial.

- Uso con una finalidad diferente de la que motivó la recogida

Si se quieren utilizar datos con una finalidad distinta de la que motivó la recogida, hay que aplicar ciertos controles para garantizar que la nueva finalidad es compatible.

3.4 ¿Qué actores intervienen en el tratamiento?

Aparte de los actores esenciales a los que el RGPD hace referencia (el responsable y el encargado del tratamiento, los interesados y el DPD), el tratamiento se puede ver condicionado por otros actores. Conviene determinar cuáles son y qué roles y responsabilidades tienen en el tratamiento

3.5 ¿Cuáles son los procesos de tratamiento?

Los datos se pueden tratar de forma automatizada, de forma manual o con una combinación de ambas; lo puede hacer el responsable del tratamiento o delegarlo en un encargado; se puede hacer con los medios propios del responsable del tratamiento o con medios proporcionados por un encargado (por ejemplo, en la nube).

Hay una estrecha relación entre los medios que se utilizan para tratar los datos y los riesgos del tratamiento. Aparte, el uso de algunas tecnologías puede tener implicaciones que entran en conflicto con otros aspectos del RGPD. Por ejemplo, el uso de una nube podría implicar la transferencia de datos fuera de las fronteras de la UE, que el RGPD limita.

3.6 ¿Dónde se hace el tratamiento de los datos?

Siguiendo el criterio del GT29, no consideramos que el tratamiento de datos fuera de la UE sea un factor en el momento de determinar si es necesario hacer una EIPD. Esto no quiere decir que no sea un factor importante a la hora de ejecutar la EIPD.

La transferencia de datos personales a un tercer país u organización internacional donde el RGPD no es de aplicación puede hacer que los interesados vean reducida la protección de sus datos. Por eso el RGPD restringe estas transferencias, que sólo se pueden hacer si se da una de las condiciones siguientes:

- La Comisión Europea considera que el tercer país, territorio, sector de un país u organización internacional ofrece un nivel de protección adecuado. En septiembre de 2019 la lista de países reconocidos es: Andorra, Argentina, Canadá (organizaciones comerciales), Estados Unidos (limitado al Privacy Shield), Guernsey, Isla de Man, Islas Faroe, Israel, Japón, Jersey, Nueva Zelanda, Suiza y Uruguay.
- Si el responsable o el encargado proporcionan las garantías adecuadas y los interesados disponen de derechos exigibles y acciones legales efectivas. Las garantías adecuadas pueden ser aportados por:
    - Un instrumento jurídicamente vinculante y exigible entre autoridades u organismos públicos.
    - Normas corporativas vinculantes, de acuerdo con el artículo 47 del RGPD.
    - Cláusulas tipo de protección de datos adoptadas por la Comisión.
    - Cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión.

- Un código de conducta de acuerdo con el artículo 42 del RGPD, junto con compromisos vinculantes y exigibles del responsable o del encargado del tratamiento en el tercer país, de aplicar las garantías adecuadas.

- Es de aplicación alguna de las excepciones relacionadas en el artículo 49 del RGPD.
  - El interesado ha dado su consentimiento a la transferencia.
  - La transferencia es necesaria para ejecutar un contrato entre el interesado y el responsable.
  - La transferencia es necesaria para ejecutar un contrato, en interés del interesado, entre el responsable del tratamiento y una tercera parte.
  - La transferencia es necesaria por razones de interés público.
  - La transferencia es necesaria para formular, ejercer o defender reclamaciones.
  - La transferencia es necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado está incapacitado para dar su consentimiento.
  - La transferencia se hace desde un registro público que tiene por objeto facilitar información al público y que está abierto a la consulta del público en general.

4. Necesidad y proporcionalidad del tratamiento

Puntos clave

- Es necesario que el tratamiento sea eficaz para lograr su finalidad.
- Un tratamiento es necesario cuando el fin no se pueda lograr de una forma menos intrusiva.
- Un tratamiento es proporcional cuando los beneficios son superiores a los perjuicios potenciales.

En la descripción del tratamiento hecha anteriormente, se ha fijado su finalidad. Ahora hay que evaluar la proporcionalidad y la necesidad del tratamiento, en relación con esta finalidad.

Así pues, hay que evaluar si el tratamiento descrito en la sección anterior es idóneo para alcanzar la finalidad, si hay una alternativa para que sea menos lesivo para los derechos y las libertades de las personas y si el beneficio que se obtiene del tratamiento es superior a los potenciales perjuicios que puede tener sobre las personas.

En la evaluación de la necesidad y la proporcionalidad, hay que seguir la guía que establecen los principios básicos que deben regir cualquier tratamiento de datos personales (art. 5 RGPD). En particular, tienen una incidencia directa los principios de licitud, lealtad, minimización de datos, limitación del plazo de conservación de los datos y exactitud.

Aparte de evaluar los principios anteriores, para establecer la necesidad y la proporcionalidad de un tratamiento resulta indispensable identificar los riesgos para los derechos y las libertades de las personas que implica el tratamiento, el nivel de estos riesgos y, si es necesario, proponer medidas para mitigarlos. En la sección 6 se analizan los riesgos desde el punto de vista de la seguridad de la información; es decir, qué efectos puede tener sobre las personas una pérdida de la confidencialidad, la integridad o de la disponibilidad de la información. El análisis que hacemos en esta sección pretende determinar el impacto que tiene el tratamiento sobre las personas, si se produce tal y como está planeado; es decir, sin tener en cuenta factores externos que lo puedan alterar.

4.1 Evaluación de la finalidad del tratamiento

▪ Tratamiento con una finalidad diferente de la que motivó la recogida

En general, los datos deben tratarse exclusivamente con la finalidad para la que se han recogido. Si se quieren tratar datos con una finalidad diferente, es necesario que la nueva finalidad sea compatible con la inicial, a menos que se dé una de las condiciones siguientes[1]:

- Se ha obtenido el consentimiento de los interesados para el nuevo tratamiento.

[1] Articulo 6.4 RGPD.

- El tratamiento está basado en el derecho de la Unión o de los Estados miembros que constituya una medida para salvaguardar los objetivos indicados en el artículo 23:
    - seguridad nacional
    - defensa
    - seguridad pública
    - prevención, investigación, detección y procesamiento de delitos penales
    - otros objetivos importantes de interés público
    - la protección de la independencia judicial y de los procedimientos judiciales
    - la prevención, investigación, detección y procesamiento de infracciones en normas deontológicas
    - la protección del interesado o de los derechos y libertades de otros
    - la ejecución de demandas civiles

Compatibilidad de finalidades

Para evaluar si una nueva finalidad es compatible con la finalidad que motivó la recogida de datos, hay que tener en cuenta los aspectos siguientes:

- Las posibles relaciones entre la nueva finalidad y la finalidad inicial.
- El contexto en el que se han recogido los datos. En particular, si el interesado puede anticipar el nuevo tratamiento.
- La naturaleza de los datos. En particular, con respecto a categorías especiales (art. 9 RGPD) y datos de condenas y delitos penales (art. 10 RGPD).
- Las posibles consecuencias del nuevo tratamiento.
- Si hay garantías adecuadas.

Como norma general, si la nueva finalidad es muy distinta a la inicial y no es una finalidad que los interesados puedan prever, o puede tener un impacto injustificado sobre las personas, debe considerarse incompatible con la finalidad inicial.

El tratamiento de datos personales con finalidad de archivo en el interés público, con finalidad de investigación científica o histórica o con finalidad estadística se considera compatible con la finalidad inicial[1].

4.2 Principio de licitud y lealtad

Licitud

Para que un tratamiento sea lícito, es necesario que le sea de aplicación alguno de los siguientes supuestos que dan una base legal al tratamiento:

- El interesado ha dado su consentimiento para el tratamiento de sus datos personales, para una o varias finalidades específicas.
- El tratamiento es necesario para ejecutar un contrato en el que el interesado es parte o para aplicar medidas precontractuales.
- El tratamiento es necesario para cumplir una obligación legal aplicable al responsable del tratamiento.
- El tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física.
- El tratamiento es necesario para cumplir una misión hecha en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

[1] Artículo 5.1 RGPD.

- El tratamiento es necesario para satisfacer los intereses legítimos del responsable del tratamiento o de un tercero, siempre que no prevalezcan los intereses o los derechos y libertades fundamentales del interesado (en particular, cuando el interesado es un menor).

Aparte, es necesario que el uso de los datos que hagan el responsable y el encargado del tratamiento sea lícito en un sentido amplio. Por ejemplo, el uso que hagan no puede:

- Incurrir en ningún ilícito (civil o penal).
- Infringir la normativa del copyright.
- Infringir acuerdos contractuales.

A la hora de elegir la base legal sobre la que se debe fundamentar el tratamiento, hay que tener en cuenta la finalidad y el contexto. Se debe elegir la base legal que encaja mejor con las circunstancias. No hay una base legal mejor o más importante que las otras. Puede ser, incluso, que el tratamiento se pueda acoger a más de una base legal. En este caso, hay que especificar todas las bases legales al principio.

Algunas de las bases legales tienen una finalidad específica: un contrato con el interesado, una obligación legal, proteger los intereses vitales de una persona y el interés público. Si el tratamiento se hace con alguna de estas finalidades, la base legal apropiada es obvia.

Si el tratamiento se hace con otros fines, entonces la base legal puede no ser tan obvia. En muchos casos puede haber la opción de elegir entre intereses legítimos y consentimiento. Si se utiliza el interés legítimo como base legal, se mantiene el control del tratamiento; pero hay que demostrar que está dentro de lo que las personas pueden razonablemente esperar y que no les causa daños injustificados. Si se utiliza el consentimiento como base legal, se da a los interesados control total sobre el uso de sus datos (incluida la posibilidad de que retiren el consentimiento y que no se pueda continuar tratando sus datos).

Conviene elegir la base legal adecuada desde el principio. Si después de iniciar el tratamiento se descubre que la base legal era inadecuada, puede ser difícil cambiarla por otra. Incluso si se ha podido aplicar desde el principio, puede que los interesados no entiendan este cambio.

Ejemplo

Una organización decide tratar datos personales sobre la base del consentimiento. Después de recoger el consentimiento de los interesados e iniciar el tratamiento, hay una persona que quiere retirar el consentimiento. La organización, que quiere seguir tratando los datos, decide continuar el tratamiento sobre la base del interés legítimo.

En este caso, se ha hecho creer a los interesados que controlaban el tratamiento de sus datos, cuando realmente no era así. La organización habría tenido que dejar claro desde el principio que el tratamiento se fundamentaba en el interés legítimo y, en esta situación, debería dejar de tratar los datos cuando se retira el consentimiento.

Tratamiento de datos de menores

Los menores necesitan una protección especial en el tratamiento de sus datos, porque pueden no ser conscientes de los riesgos que conlleva.

En particular, cuando el tratamiento está relacionado con la oferta directa de servicios de la sociedad de la información a niños y la base legal es el consentimiento, el RGPD establece una edad mínima de 16 años para que el consentimiento sea válido. Si el menor

tiene menos de 16 años, es necesario que el consentimiento lo dé o lo autorice el titular de la patria potestad.

Los estados miembros pueden reducir la edad mínima para dar consentimiento, pero no puede ser inferior a 13 años. En el caso español, la edad se ha fijado en 14 años.

La tabla siguiente muestra las edades mínimas para dar consentimiento en el contexto de la oferta directa de servicios de la sociedad de la información:

Edad mínima de consentimiento (a julio de 2019)[1]

13	14	15	16
Bélgica	Austria	Republica Checa	Alemania
Dinamarca	Bulgaria	Francia	Croacia
Estonia	España		Eslovaquia
Finlandia	Italia		Eslovenia
Letonia	Lituania		Grecia
Malta	Chipre		Holanda
Portugal			Hungría
Reino Unido			Irlanda
Suecia			Luxemburgo
			Polonia
			Rumanía

Tratamiento de categorías especiales de datos

Los datos de categorías especiales son más sensibles y necesitan más protección. Cuando se tratan estos datos, además de determinar una base legal para el tratamiento, hay que determinar cuál de las condiciones del artículo 9 es la que permite tratarlas:

- El interesado ha dado su consentimiento explícito para el tratamiento con una finalidad específica, salvo que el derecho de la UE o del estado miembro no lo permita.
- El tratamiento es necesario para cumplir obligaciones o para ejercer derechos en el ámbito del derecho laboral y de la seguridad y la protección social.
- El tratamiento es necesario para proteger intereses vitales del interesado o de otra persona, y el interesado no está capacitado para dar el consentimiento.
- El tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física.
- El tratamiento es legítimo y con garantías, hecho por una asociación sin ánimo de lucro de carácter político, filosófico, religioso o sindical, siempre que el tratamiento afecte personas con las que mantienen contactos en relación con estas finalidades y los datos no se comuniquen a terceros sin el consentimiento de los interesados.
- El tratamiento hace referencia a datos que el interesado ha hecho públicas.
- El tratamiento es necesario para formular, ejercer o defender reclamaciones, o cuando los tribunales actúan en su función judicial.
- El tratamiento es necesario por razones de interés público esencial.
- El tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social.
- El tratamiento es necesario por razones de interés público en el ámbito de la salud pública.

[1] www.betterinternetforkids.eu/en_US/web/portal/practice/awareness/detail?articleId=3017751.

- El tratamiento es necesario con el fin de archivo con interés público, investigación científica o histórica, o con finalidad estadística.

La base legal elegida para el tratamiento no restringe las bases legales para el tratamiento de datos de categoría especial. Por ejemplo, el uso del consentimiento como base legal no implica el uso de consentimiento explícito como base para el tratamiento de datos de categorías especiales. Sin embargo, hay casos en que el enlace entre uno y otro es probable. Por ejemplo, si la base legal es el interés vital, es probable que la base para el tratamiento de categorías especiales sea la misma.

Tratamiento de datos penales

Aunque no es una categoría especial de datos, los datos sobre condenas o infracciones penales también gozan de una protección especial. El tratamiento de estos datos sólo está permitido bajo la supervisión de las autoridades o cuando lo autorice el derecho de la unión o de un estado miembro. Además, se establece que los registros exhaustivos de condenas criminales sólo se pueden mantener bajo control de la autoridad.

Validez del consentimiento

Cuando la base legal de un tratamiento es el consentimiento, para que sea válido es necesario que se cumplan las condiciones siguientes:

- El responsable debe poder demostrar que lo ha recogido.
- La solicitud de consentimiento es inteligible, de fácil acceso y en un lenguaje claro.
- La ejecución de un contrato no puede supeditarse a recibir el consentimiento respecto de datos personales no necesarios para ejecutar el contrato.
- Se ha informado a los interesados de la posibilidad de retirar el consentimiento en cualquier momento.

La retirada del consentimiento no afecta a la validez de los tratamientos hechos antes de retirarlo.

- Lealtad

Un tratamiento es leal si hace un uso de los datos que sea previsible para los interesados (en relación con la finalidad del tratamiento) y no se derivan consecuencias adversas para los interesados que no sean justificables.

4.3 Principio de minimización

El principio de minimización de datos determina que los datos deben ser adecuados (suficientes para cumplir con la finalidad del tratamiento de forma adecuada), relevantes (tienen relación con la finalidad del tratamiento) y limitadas a lo estrictamente necesario para cumplir con la finalidad del tratamiento. Este es un punto clave para justificar la necesidad.

Para cumplir el principio de minimización, es necesario identificar cuál es la mínima información necesaria para cumplir con la finalidad de un tratamiento. Se debe recoger esta información mínima y no más.

Aparte del tipo de datos que se tratan, el nivel de detalle de estos datos también es esencial en el momento de determinar si se cumple el principio de minimización. Los datos deben tener un nivel de detalle que sea relevante para la finalidad del tratamiento.

Puede que los datos relevantes para el tratamiento varíen según la persona o el grupo de personas. En este caso, hay que ajustar los datos recogidos a los que son relevantes en cada caso.

Hay que revisar de forma periódica que los datos almacenados siguen siendo relevantes y adecuados para la finalidad del tratamiento, y borrar cualquier dato que no lo sea.

En cuanto a la adecuación de los datos, hay que garantizar que sean útiles para alcanzar la finalidad del tratamiento. No se tienen que tratar datos insuficientes o incompletos para la finalidad pretendida.

4.4 Principio de limitación del plazo de conservación

Los datos personales no se conservarán más tiempo del estrictamente necesario para cumplir con la finalidad del tratamiento. Asegurarse de que se borran los datos personales cuando dejan de ser necesarios reduce el riesgo de que se conviertan en irrelevantes, excesivos o inexactos.

De acuerdo con el artículo 30.1, cuando sea posible hay que establecer y documentar unos periodos estándar de retención para los diferentes tipos de datos. También conviene asegurarse de que la organización tiene los procedimientos necesarios para revisar y hacer efectivos estos periodos de retención.

El reglamento no especifica cuánto tiempo se deben conservar los datos. Es el responsable del tratamiento quien fijará el periodo de retención, de acuerdo con las necesidades del tratamiento. No se conservarán los datos de forma indefinida, en previsión de que puedan ser necesarios en el futuro.

Los datos se pueden conservar indefinidamente con la finalidad de archivo en interés público, con la finalidad de investigación científica o histórica, o con la finalidad estadística. En estos casos, hay que garantizar que se implantan las medidas técnicas y organizativas necesarias para garantizar el principio de minimización. Técnicas tales como la anonimización o la pseudonimización de los datos tienen una particular relevancia en este contexto.

4.5 Principio de exactitud

El tratamiento de datos inexactos puede afectar negativamente a las personas. El principio de exactitud pide que los datos sean exactos y que se tomen las medidas adecuadas para garantizar que los que sean inexactos se actualicen o se borren sin dilación.

4.6 Riesgos del tratamiento

Cualquier tratamiento de datos puede tener efectos negativos sobre los derechos y las libertades de las personas. Para paliar estos efectos, el RGPD propone un enfoque basado en el riesgo. Las medidas para proteger los derechos y las libertades de las personas deben ser proporcionales al riesgo asociado al tratamiento.

Típicamente, la evaluación del riesgo se hace desde el punto de vista de la organización que trata los datos. Es decir, se centra en los efectos negativos sobre el responsable o el encargado del tratamiento. El RGPD cambia este punto de vista y busca evaluar el riesgo del tratamiento sobre las personas.

La seguridad de la información es el punto central en las evaluaciones de riesgo. Es decir, normalmente se evalúan los potenciales efectos negativos de una violación de seguridad en el tratamiento. Ahora bien, un tratamiento puede afectar a los derechos y las libertades de las personas, aunque no se haya producido ninguna violación de la seguridad. Por ejemplo, un tratamiento puede ser discriminatorio en sí mismo o puede favorecer la aparición de prácticas discriminatorias. Esta sección se centra en esta última visión: la evaluación del riesgo de un tratamiento tal como ha sido diseñado.

Comentario

Conviene notar que cualquier tratamiento de datos, sean personales o no, puede tener efectos negativos sobre las personas. A la hora de hacer una EIPD, sólo nos interesan los efectos derivados del uso de datos personales.

Por ejemplo, un tratamiento que se basa en datos agregados (por lo tanto, no personales) puede tener un efecto significativo sobre un grupo de personas.

Los efectos negativos que un tratamiento puede tener sobre las personas dependen del tratamiento concreto que se está haciendo. A continuación, damos algunos ejemplos. Ahora bien, es el responsable del tratamiento quien determinará los efectos negativos potenciales.

- pérdida de tiempo
- enojo
- augmento de los costes
- falta de comprensión
- estrés
- Imposibilidad de acceder a servicios u otras oportunidades
- discriminación
- robo de identidad y otros fraudes
- pérdidas económicas
- daños psicológicos
- daños para la reputación
- daños físicos
- afectación de la salud
- pérdida del trabajo
- daños físicos o psicológicos graves

En el momento de determinar los efectos que un tratamiento puede tener sobre las personas, conviene tener en cuenta algunas características del tratamiento, tales como:

- El tipo de datos personales. El tratamiento de categorías especiales de datos, tales como el origen racial o étnico, los datos médicos o datos sobre las preferencias políticas, son claros indicadores de potenciales efectos negativos sobre los derechos y las libertades de las personas. Ahora bien, cabe destacar que otros tipos de datos que no forman parte de las categorías especiales también pueden tener un impacto importante. Por ejemplo, localizaciones, información financiera, etc.
- El grado de sensibilidad del tratamiento. Más allá del tipo de datos tratados, el tipo de tratamiento también puede indicar potenciales impactos. Por ejemplo, cuando el tratamiento tiene como objetivo la monitorización de personas.
- La cantidad de datos personales tratados sobre cada individuo. Cuanto mayor sea esta cantidad, mayor serán los potenciales efectos negativos sobre las personas.
- La actividad del responsable del tratamiento. Por ejemplo, si la actividad del responsable de tratamiento está relacionada con la salud o las finanzas, ya podemos entrever que el impacto puede ser alto.
- Las características de los interesados. Si los interesados forman parte de un grupo con necesidades especiales (por ejemplo, menores o autoridades), hay que tener un cuidado especial a la hora de determinar los efectos potenciales del tratamiento.

El RGPD establece la conveniencia de tener en cuenta la opinión de los interesados en el momento de hacer una EIPD. Ya que la evaluación del riesgo se centra en las personas (y no en la organización que hace el tratamiento), este es un punto donde resulta interesante recoger la opinión de los interesados: los potenciales efectos negativos, el nivel de impacto, las amenazas y las probabilidades de que estas amenazas se materialicen.

- Impacto

Una vez identificados los potenciales efectos negativos, hay que determinar qué impacto tienen. Consideramos cuatro niveles de impacto: bajo, medio, alto y muy alto.

Impacto	Descripción
Bajo	Los interesados pueden sufrir algunas molestias menores, que pueden superar sin problemas (por ejemplo, pérdida de tiempo, enojo, etc.)
Medio	Los interesados pueden encontrar inconvenientes importantes, que pueden superar con algunas dificultades (por ejemplo, aumento de costes, falta de comprensión, estrés, daños físicos, imposibilidad de acceder a algún servicio, etc.)
Alto	Los interesados pueden sufrir consecuencias importantes, que pueden superar con dificultades importantes (por ejemplo, discriminación, robo de la identidad, pérdidas económicas, daños psicológicos, daños por la reputación, daños físicos, empeoramiento de la salud, pérdida del trabajo etc.)
Muy alto	Los interesados pueden sufrir consecuencias graves que no pueden superar (por ejemplo, daños físicos o psicológicos graves, muerte, etc.)

Al igual que antes, la responsabilidad de hacer un cálculo preciso del nivel de impacto recae sobre el responsable del tratamiento.

- Amenazas y probabilidad

Aunque un tratamiento puede tener efectos negativos sobre una persona, estos efectos no se materializan siempre. Para evaluar el riesgo asociado a un potencial efecto negativo, hay que estimar la probabilidad de que se materialice.

Consideramos tres niveles de probabilidad:

- Bajo. Es improbable que el impacto se materialice.
- Medio. Es posible que el impacto se materialice.
- Alto. Es probable que el impacto se materialice.

Esta probabilidad se podría estimar de forma directa. Ahora bien, sin un análisis de las circunstancias en que el impacto es materializa, la estimación puede ser poco precisa. Por ello, estimaremos la probabilidad según las amenazas.

Una amenaza es cualquier circunstancia que tiene el potencial de materializar uno de los efectos negativos descritos anteriormente. Una vez determinadas las amenazas, hay que calcular en qué medida es probable. Aunque esta estimación también es subjetiva, está mejor fundamentada.

- Determinación del riesgo

El nivel de riesgo asociado resulta de combinar la gravedad del impacto con la probabilidad de que se materialice. Dado que las últimas se han calculado de forma cualitativa, la estimación del riesgo también será cualitativa.

En el momento calcular el nivel de riesgo es fundamental tomar el punto de vista de los interesados. Desde el punto de vista del responsable o del encargado del tratamiento, un impacto de mucha gravedad podría ser aceptable, si la probabilidad es pequeña; y el responsable podría decidir asumir el coste asociado a este evento. Ahora bien, el punto de vista de las personas afectadas suele ser diferente, ya que el impacto recae sobre ellas. Esto hace que, en general, no quieran impactos con gravedad muy alta, aunque la probabilidad sea baja, ya que reponerse de estos impactos podría ser muy difícil, o incluso imposible. Además, aunque pueda haber personas dispuestas a aceptar un impacto de gravedad muy alto, si la probabilidad es baja no es apropiado que el responsable del tratamiento tome esta decisión.

Proponemos la tabla de cálculo de riesgo siguiente. De acuerdo con lo expuesto, si el potencial impacto es muy alto, el riesgo será alto independientemente de la probabilidad.

Probabilidad	Alta	Riesgo medio	Riesgo alto	Riesgo alto	Riesgo alto
	Mediana	Riesgo bajo	Riesgo medio	Riesgo alto	Riesgo alto
	Baja	Riesgo bajo	Riesgo bajo	Riesgo medio	Riesgo alto
		Bajo	Medio	Alto	Muy alto
		Impacto			

- Reducción de los riesgos

Salvo que el riesgo sea bajo, hay que buscar medidas para reducirlo. Esto es especialmente necesario en los casos de riesgo alto o muy alto. Si no es posible reducir un riesgo alto, antes de comenzar el tratamiento se debe consultar a la autoridad de protección de datos competente sobre la idoneidad del tratamiento.

Las medidas que se pueden tomar dependen del tratamiento y es tarea del responsable del tratamiento encontrar las más adecuadas. Algunas medidas pueden ser:

- Evitar la recogida de ciertos tipos de datos.
- Reducir el alcance del tratamiento.
- Formar al personal para que haga un uso apropiado de la información.
- Anonimizar o pseudonimizar los datos.
- Tener una política clara para compartir datos.

En el caso del riesgo asociado a la seguridad de la información, es habitual calcular un riesgo inicial (sin controles de seguridad) y un riesgo residual (con los controles implementados para reducir el riesgo inicial). Esto es posible porque los controles de seguridad no alteran la esencia del tratamiento. Sin embargo, en el caso del riesgo asociado al tratamiento como está diseñado, las medidas para reducirlo son, básicamente, modificaciones del diseño del tratamiento. Modificar el diseño de forma separada a la descripción del tratamiento hecha en la sección anterior haría que la descripción inicial no fuera precisa. Esto no es conveniente y, por tanto, hay que adaptar las secciones anteriores de la EIPD a los cambios hechos al tratamiento y volver a calcular el riesgo. Esto hace que hacer una EIPD no sea una tarea lineal.

Ejemplo

Una empresa pone en marcha un proceso de selección para contratar personal. El objetivo de este proceso de selección es elegir a la persona más adecuada para hacer un trabajo.

En un sentido amplio de la palabra, cualquier proceso de selección discrimina. No obstante, queremos que esta discriminación esté justificada por la capacitación de las personas y no por motivos espurios.

Puede que por motivos de comunicación con los candidatos se recoja información del lugar de residencia. Un evaluador con acceso a esta información puede dejar fuera (discriminar) a los candidatos que vivan en zonas marginales. Si calificamos el impacto de esta potencial discriminación de alto y le asignamos una probabilidad media, resulta un riesgo alto. Hay que buscar medidas para reducirlo.

Conviene notar que conocer el domicilio de residencia no es necesario para evaluar la capacitación del candidato. Por lo tanto, una medida para reducir el riesgo sería privar a los evaluadores de esta información.

4.7 Necesidad y proporcionalidad del tratamiento

Una vez evaluados los principios de protección de datos y analizados cuáles son los riesgos para los derechos y las libertades de las personas, el responsable tiene la información necesaria para evaluar la necesidad y la proporcionalidad del tratamiento.

Un tratamiento sólo tiene sentido si logra su finalidad. Por lo tanto, justificar la eficacia del tratamiento es un primer paso esencial para justificar la necesidad.

Para justificar que un tratamiento es necesario, hay que mostrar que no hay ningún otro tratamiento que sea, al mismo tiempo, efectivo y menos lesivo para los derechos y las libertades de las personas.

Para justificar que un tratamiento es proporcional, es necesario mostrar que el beneficio que se obtiene del tratamiento es superior a los perjuicios potenciales sobre las personas. En la justificación de la proporcionalidad, conviene tener en cuenta el análisis de riesgos realizado en la sección anterior.

4.8 Opinión de los interesados

El responsable del tratamiento debe buscar la opinión de los interesados sobre la operación de tratamiento. La necesidad y la proporcionalidad del tratamiento es un punto especialmente interesante para buscar la opinión de los interesados. Si no se considera apropiado buscarla, hay que documentar el porqué. Por ejemplo, porque tiene un coste desproporcionado o porque puede poner en riesgo la confidencialidad del plan de negocio.

5. Protección de los derechos de las personas

Puntos clave

- El Reglamento establece una serie de derechos que permiten a las personas conocer e intervenir en el tratamiento de sus datos.
- A la hora de evaluar el impacto del tratamiento, es esencial garantizar que las personas pueden ejercer estos derechos.

Los principios fundamentales a qué se refiere el artículo 5 del Reglamento se materializan en una serie de derechos que se establecen en el capítulo 3: transparencia, información y acceso a los datos personales, rectificación y supresión, limitación y oposición.

Estos derechos dan a los interesados la posibilidad de conocer el tratamiento y de intervenir. La transparencia y el derecho a la información son necesarios para que los interesados sean conscientes de cómo se tratan sus datos. Los derechos de acceso, rectificación y supresión permiten que los interesados controlen sus datos. Los derechos de limitación y oposición dan a los interesados control sobre el tratamiento.

Es esencial garantizar que las personas pueden ejercer los derechos que tienen reconocidos en el Reglamento. El objetivo de esta sección es evaluar los mecanismos establecidos para garantizarlo.

5.1 Transparencia

El Reglamento habla de la transparencia como una propiedad transversal, que debe estar presente en el momento de informar a las personas interesadas.

Más concretamente, la transparencia exige que cualquier comunicación con los interesados sea concisa, inteligible y de fácil acceso, y que utilice un lenguaje claro y sencillo. Especialmente, cuando esta comunicación esté dirigida a un niño.

También exige que las solicitudes de los interesados se tramiten en un tiempo razonable. En particular, el reglamento establece un periodo de un mes, que se puede ampliar (previa notificación dentro del plazo de un mes) en dos meses adicionales, si lo justifica la complejidad o el número de solicitudes.

Finalmente, la transparencia exige que, si no se tramita la solicitud de un interesado, el responsable informe sin dilación de este hecho y de las razones, así como de la posibilidad de presentar una reclamación a una autoridad de control y de ejercer acciones judiciales.

En el curso de una solicitud de un interesado, y en el caso de que el responsable tenga dudas respecto de la identidad del solicitante, el representante puede pedir la información necesaria para confirmar la identidad.

.

5.2 Derecho de información

El derecho de información establece que los interesados tienen el derecho a estar informados de la recogida y posterior tratamiento que se hace de sus datos. Este es un

derecho esencial para que, sin esta información, el resto de los derechos no pueden hacerse efectivos.

El derecho de información establece que el responsable tiene que dar la información siguiente a los interesados:

- La identidad y los datos de contacto del responsable.
- Los datos de contacto del delegado de protección de datos (si los hay).
- La finalidad del tratamiento.
- La base legal del tratamiento.
- El interés legítimo del responsable, si esta es la base legal del tratamiento.
- Los destinatarios o categorías de destinatarios de los datos.
- El plazo de conservación de los datos o el criterio empleado para determinarlo.
- La intención de transmitir los datos fuera de la UE, si procede.
- La decisión de la Comisión Europea respecto de la suficiencia de la seguridad que ofrece el país u organización destinataria.

Aparte, para garantizar que los interesados conocen sus derechos y saben cómo ejercerlos, es necesario que el responsable del tratamiento les informe que tienen los derechos siguientes:

- Derecho de acceso a los datos.
- Derecho de rectificación y supresión.
- Derecho de limitación del tratamiento.
- Derecho de oposición al tratamiento.
- Derecho a la portabilidad de los datos.
- Derecho a revocar el consentimiento (si esta es la base legal del tratamiento).
- Derecho a presentar una reclamación ante una autoridad de control.

Y, asimismo:

- Que la comunicación de los datos es un requisito legal o contractual, si procede.
- La existencia de decisiones automatizadas.

En el caso de datos que no se han recogido directamente del interesado, debe informar de su procedencia.

Cuando los datos se recogen directamente de los interesados, hay que dar la información anterior en el mismo momento de recogida. Cuando los datos no se recogen directamente de los interesados, hay que informar:

- En un período razonable de tiempo y no superior a un mes.
- Si nos comunicamos con los interesados, como muy tarde en el momento de la primera comunicación.
- Si se quieren comunicar los datos a terceros, antes de comunicarlos.

Hay algunas exenciones a la obligación de informar, que dependen de cómo se han recogido los datos:

- Si los datos se han obtenido directamente del interesado, no existe la obligación de informarle si ya dispone de la información.
- Si los datos no se han obtenido directamente del interesado, no es necesario informarle si se da alguna de las siguientes condiciones[1]: el interesado ya dispone de esta información, la comunicación es imposible o supone un esfuerzo desproporcionado, así está regulado por una norma de la UE o de los Estados

[1] RGPD, artículo 14.5.

miembros o la información tiene carácter confidencial sobre la base del secreto profesional.

No obstante, en caso de que no se informe, hay que justificarlo.

5.3 Derecho de acceso

El interesado tiene el derecho de obtener del responsable del tratamiento la confirmación de que se están tratando sus datos y, en este caso, el derecho de acceso a los datos personales y a la información siguiente:

- La finalidad del tratamiento.
- Las categorías de datos tratados.
- Los destinatarios de los datos.
- El plazo de conservación de los datos.
- Los derechos a rectificar y suprimir los datos.
- Los derechos a limitar y oponerse al tratamiento.
- El derecho a reclamar ante una autoridad de control.
- Si los datos no se han obtenido del interesado, el origen de los datos.
- La existencia de decisiones automatizadas, si procede.
- Garantías en la transferencia de datos fuera de la UE, si procede.

Aparte de conocer qué información se debe transmitir a los interesados, hay que asegurarse de que se dan las condiciones para hacer efectivo el derecho de acceso.

- ¿Cómo se reconoce una solicitud válida?
  El Reglamento no dice cómo se deben hacer las solicitudes de acceso. Es decir, se pueden dirigir a cualquier trabajador, por cualquier medio y no necesitan ninguna frase del tipo "solicitud del derecho de acceso". Por esta razón, hay que asegurarse de que el personal que interacciona con los interesados tiene los conocimientos suficientes para identificar las solicitudes.
- ¿Hay que establecer un procedimiento para hacer las solicitudes?
  Es recomendable establecer un procedimiento estándar para hacer las solicitudes. Esto facilita las cosas tanto al responsable como los interesados. Sin embargo, las solicitudes son igualmente válidas, aunque no utilicen este procedimiento.

La transparencia se aplica a los procedimientos diseñados para garantizar el derecho de acceso.

- La información debe ser concisa, inteligible, fácilmente accesible y en un lenguaje claro y sencillo.
- Las solicitudes se deben tramitar en un plazo de un mes.
- Si la complejidad o el número de solicitudes lo requiere, este plazo puede ampliarse en dos meses. No obstante, hay que informar a los interesados antes de que finalice el primer mes.
- Si hay duda sobre la identidad de la persona que hace la solicitud, se puede pedir la información necesaria para confirmar la identidad.
- La solicitud debe ser gratuita. El responsable únicamente las puede cobrar (o desestimar) si son infundadas o excesivas.

5.4 Derecho de rectificación

El Reglamento establece el derecho de las personas a que se rectifique la información personal que no sea exacta. Sin embargo, en el momento de determinar si una información es exacta también puede intervenir la percepción personal. Esto hace que el ejercicio de este derecho pueda tener una cierta complejidad.

Si se recibe una solicitud de rectificación, hay que hacer los pasos necesarios para comprobar si la información es precisa y, si procede, rectificarla.

Mientras se está comprobando si los datos son exactos, el interesado puede pedir que se limite el tratamiento[1].

Por la transparencia, si el resultado de la comprobación es que la información ya es exacta y, por tanto, no hay que rectificarla, se informará al interesado. Hay que explicarle la decisión e informarle de la posibilidad de recurrir a la autoridad de protección de datos competente.

Según el artículo 19, si el responsable ha compartido los datos, tiene que tomar las medidas adecuadas (teniendo en cuenta los costes y la tecnología disponible) para informar a los destinatarios sobre la petición de rectificación.

5.5 Derecho de supresión

Según el Reglamento, las personas tienen el derecho a que se borre la información cuando se da alguno de los casos siguientes:

- Los datos ya no son necesarios en relación con la finalidad para la que se recogieron.
- El Interesado retira su consentimiento y no hay ninguna otra base legal para el tratamiento.
- El Interesado se opone al tratamiento y no hay ningún otro factor superior que lo legitime.
- Los datos se han tratado sin una base legal.
- Los datos se tienen que borrar de acuerdo con una obligación legal que afecta al responsable.
- Los datos se utilizan para ofrecer servicios de la sociedad de la información a niños.

Si el responsable ha compartido los datos, es necesario que tome las medidas adecuadas (teniendo en cuenta los costes y la tecnología disponible) para informar a los destinatarios sobre la petición.

El derecho de supresión no es de aplicación los casos siguientes:

- Para ejercer el derecho a la libertad de expresión y de información.
- Para cumplir una obligación legal o en el interés público.
- Con el fin de archivo en interés público, con finalidad de investigación científica o histórica, y con finalidad estadística (si el cumplimiento de estas finalidades se viera afectado por la supresión de los datos).
- Para presentar, ejercer o defender reclamaciones legales.

5.6 Derecho a limitar el tratamiento

El artículo 18 da a las personas el derecho a limitar el tratamiento de sobre datos, en los casos siguientes:

- El interesado ha pedido la rectificación sobre datos y el responsable está verificando si son exactos.
- Los datos se han tratado sin una base legal.
- El interesado necesita que el responsable guarde los datos para iniciar, ejercer o defender una reclamación.

[1] RGPD, artículo 18.

- El Interesado se ha opuesto al tratamiento y el responsable está evaluando si los motivos legítimos del responsable prevalecen sobre los del interesado.

La noción de tratamiento es muy general: incluye, entre otros, recogida, análisis, diseminación y supresión de datos. Es importante que se tengan en cuenta todas las formas de tratamiento, en el momento de limitarlo.

Si el responsable ha compartido los datos, es necesario que tome las medidas adecuadas (teniendo en cuenta los costes y la tecnología disponible) para informar a los destinatarios sobre la petición.

5.7 Derecho a la portabilidad de datos

Según el artículo 20, las personas tienen el derecho a expedir los datos que han facilitado al responsable del tratamiento en los siguientes casos:

- Si el tratamiento está basado en el consentimiento, o es necesario para ejecutar un contrato o para aplicar medidas precontractuales.
- El tratamiento se hace con mecanismos automatizados.

El derecho a la portabilidad de datos no se limita a los datos que las personas han dado de forma explícita; también afecta a los datos que se han recogido de la observación de las personas. Por Ejemplo, el registro de búsqueda que una persona ha hecho en un buscador o la información de localización recogida de un GPS.

Los datos se deben transmitir en un formato estructurado de uso común y que sea de fácil lectura mecánica.

El derecho a la portabilidad de datos no debe afectar negativamente a otras personas. En particular:

- Si los datos personales contienen información de una tercera persona, hay que evaluar si esta última puede ver afectados sus derechos y libertades.
- Si los datos están asociados a varias personas (por ejemplo, una cuenta bancaria compartida), hay que buscar el consenso de todos los Interesados.

5.8 Derecho de oposición

Según el artículo 21, las personas tienen el derecho a oponerse al tratamiento de la información cuando este tratamiento se hace en base a:

- El interés público o el ejercicio de los poderes, públicos conferidos al responsable del tratamiento.
- El interés legítimo del responsable del tratamiento.

En este caso, el responsable debe cesar en el tratamiento, salvo que acredite motivos legítimos que prevalezcan sobre los derechos del Interesado.

El Reglamento habla de las situaciones siguientes:

- Oposición al tratamiento con fines de marketing. En este caso, el responsable debe detener el tratamiento sin excepciones.
- Oposición al tratamiento con finalidades de investigación científica o histórica, o con finalidad estadística. En este caso, el responsable puede continuar el tratamiento si está justificado por el interés público.

5.9 Derecho a no ser objeto de decisiones automatizadas

Según el artículo 22, las personas tienen derecho a no ser objetivo de decisiones basadas únicamente en el tratamiento automatizado (incluida la elaboración de perfiles), si tienen efectos jurídicos o tienen un efecto significativo, a menos que:

- Sea necesario para ejecutar un contrato entre el interesado y el responsable.
- Esté autorizado por el derecho de la Unión o de un estado miembro.
- El interesado haya dado su consentimiento explícito.

El interesado siempre tendrá derecho a obtener intervenciones humanas, a expresar su punto de vista y a impugnar la decisión.

Estas decisiones automatizadas sólo pueden hacer uso de categorías especiales de datos si existe el consentimiento explícito del Interesado, o si el tratamiento se hace para proteger los intereses vitales del interesado o de otra persona.

6. Riesgos en la seguridad de los datos

De acuerdo con el RGPD, las medidas empleadas para proteger la información deben ser apropiadas al riesgo para los derechos y las libertades de las personas. En sección 4.6 se han evaluado los riesgos asociados al tratamiento, tal como está diseñado. En esta sección, se busca evaluar los riesgos desde el punto de vista de la seguridad de la información; es decir, los riesgos que presenta el tratamiento cuando no se hace según el diseño inicial.

Seguimos el proceso descrito en la sección 4.6: Partiendo de la descripción del tratamiento hecho con anterioridad, evaluaremos cual es el impacto potencial sobre las personas y cuál es la probabilidad de que este impacto se materialice. Esto nos permitirá calcular el riesgo inicial. Si el riesgo es demasiado grande, hay que aplicar controles (medidas de protección) para reducirlo. Estas medidas pueden buscar reducir la gravedad de un impacto o la probabilidad de que se materialice.

El RGPD busca una solución que sea lo más completa posible. En particular, cita las siguientes medidas de protección a considerar (entre otras)[1]:

- Pseudonimización y encriptación de los datos.
- Medidas para garantizar la confidencialidad, integridad, disponibilidad y la resiliencia de los sistemas de tratamiento y los servicios.
- En caso de incidente, medidas para recuperar la disponibilidad y el acceso a los datos personales en un tiempo adecuado.
- Un proceso continuo de prueba y evaluación de la efectividad de las medidas propuestas para garantizar la seguridad del tratamiento.

Los tres primeros puntos hacen referencia a las medidas de protección. Las medidas del primer punto buscan reducir la probabilidad de que el impacto se materialice, mientras que las medidas del tercer punto buscan reducir la severidad del impacto. El segundo punto es más general y engloba todo tipo de medidas. El último punto hace referencia a que el proceso de gestión de riesgo no es un proceso puntual, sino que se debe hacer un seguimiento de los riesgos y de la efectividad de los controles.

En cuanto a la metodología de análisis de riesgos, las hay que tienen un amplio reconocimiento, tales como: ISO 27005:2013, OCTAVE, NIST SP 800-30 y Magerit. Ahora bien, hacer un análisis de riesgos utilizando estas metodologías puede ser un proceso complejo. Por ejemplo, en Magerit debemos:

1. Identificar los activos del sistema (que pueden ser información, servicios, software, hardware, comunicaciones, instalaciones, etc.), especificando la relación de dependencia que existe entre ellos y evaluarlos.
2. Identificar amenazas relevantes para nuestro sistema y caracterizarlas según la probabilidad de que se materialicen y la degradación que causan.
3. Identificar los controles que hay que desplegar en el sistema y calificar su eficacia frente a las amenazas identificadas previamente.

Con el objetivo de hacer la evaluación de riesgos más asequible, esta guía propone un método simplificado[2]. Si una organización tiene la capacidad suficiente para abordar alguna de las metodologías de análisis de riesgos mencionadas anteriormente, conviene que lo

[1] RGPD, artículo 32.1.
[2] Basado en la guía "Guidelines for SMEs on the security of personal data processing", ENISA.

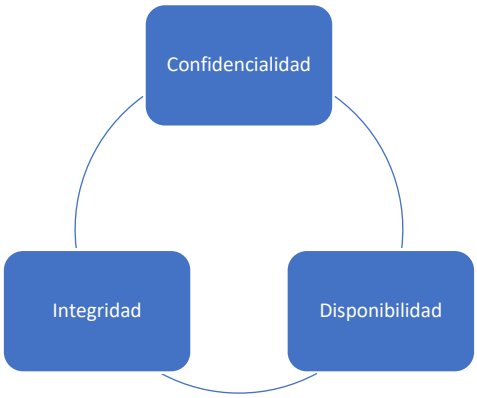
haga, pero sin perder de vista que el objetivo es evaluar el riesgo sobre las personas (no sobre la organización).

6.1 Breve introducción a la seguridad de la información

Entendemos por seguridad de la información el conjunto de medidas (técnicas, organizativas, etc.) que se toman para proteger la información que se trata en un sistema contra el acceso no autorizado, la revelación, la modificación y la destrucción.

El triángulo CIA es un modelo de seguridad de la información muy conocido. Hace referencia a tres propiedades esenciales en la seguridad de la información: confidencialidad, integridad y disponibilidad (*availability*, en inglés).

- Confidencialidad. Sólo pueden acceder a la información las personas, entidades o procesos que han sido previamente autorizados.
- Integridad. Sólo pueden modificar la información las personas, entidades o procesos que han sido previamente autorizados.
- Disponibilidad. La información debería estar disponible cuando una persona, entidad o proceso autorizado la pida.



Las tres propiedades anteriores son básicas. Ahora bien, hay modelos que las complementan con otras propiedades derivadas. Por ejemplo, en el ENS se habla también de autenticidad y trazabilidad. En nuestra estimación de riesgo nos limitaremos a las tres propiedades básicas.

6.2 Impacto

El primer paso para evaluar el riesgo es determinar la gravedad de los efectos sobre los derechos y las libertades de las personas que puede causar la pérdida de la confidencialidad, la integridad o de la disponibilidad de los datos. Cabe destacar que mientras que normalmente se mide el impacto sobre la organización, aquí medimos el impacto sobre las personas.

En el momento de evaluar el impacto, se deben considerar todos los posibles casos de pérdida de la confidencialidad, de la integridad y de la disponibilidad. Para facilitar esta tarea, se plantean diferentes escenarios en los que se pierde alguna de estas propiedades.

Escenarios en los que hay pérdida de confidencialidad:

- Pérdida o robo de un ordenador que contiene datos personales.
- Envío por error de datos personales a personas no autorizadas.
- Posibilidad de acceder de forma no autorizada a la cuenta de una persona.
- Un error de configuración en una web expone los datos personales de sus usuarios.

- Robo de información de las instalaciones del responsable o del encargado del tratamiento.
- Un empleado de un centro médico consulta de forma no autorizada el expediente de un paciente.

Escenarios en los que hay pérdida de la integridad:

- Un empleado modifica por error los datos de un cliente.
- Un error en la red de comunicaciones altera los datos mientras están en tránsito.
- Por motivos operacionales, una empresa mantiene varias copias de los datos, pero un cambio en alguna de las copias no se propaga a las otras.
- Pérdida de parte de un expediente, como consecuencia de un fallo en el sistema de tratamiento.

Escenarios en los que hay pérdida de la disponibilidad:

- Un archivo se corrompe o se borra y no hay una copia de seguridad.
- Se pierde un expediente del que solo había una copia en papel.
- Un servicio de consulta de datos deja de estar disponible (por ejemplo, el servicio para acceder a los registros electrónicos de salud).

De acuerdo con la sección 6.2, el impacto sobre las personas de la pérdida de la seguridad de los datos puede ser bajo, medio, alto o muy alto. Para fijar el valor, hay que tener en cuenta las características del tratamiento. Las situaciones siguientes incrementan el riesgo:

- El tratamiento de datos de categorías especiales u otros datos especialmente sensibles (información financiera, localización, etc.).
- La monitorización de personas.
- El tratamiento de datos de grupos con necesidades especiales (menores, autoridades, etc.).
- El Tratamiento de gran cantidad de datos de cada persona.

Como resultado, tendremos un impacto por la pérdida de la confidencialidad, uno por la pérdida de la integridad y uno por la pérdida de la disponibilidad. También podemos calcular el impacto global del sistema de tratamiento, como el máximo de los Impactos anteriores.

6.3 Probabilidad inicial

El riesgo se calcula de acuerdo con el impacto que tiene la pérdida de las propiedades de seguridad (confidencialidad, integridad y disponibilidad) y de la probabilidad de que este impacto se materialice. El objetivo de esta sección es estimar esta probabilidad.

Con el objetivo de mantener el análisis simple, la estimación de la probabilidad no se basará en un inventario del sistema. Esto requiere identificar los activos, las amenazas y las vulnerabilidades. Nuestra estimación se basa en la identificación de algunas características del sistema de tratamiento que lo hacen más susceptible de sufrir ataques.

Consideramos características del sistema de tratamiento de los tipos: hardware y software, procesos de tratamiento, personas que intervienen en el tratamiento y otras características.

Hardware y software

P1. ¿El sistema de tratamiento está conectado a sistemas externos a la organización?

La conexión con sistemas externos a la organización incrementa la exposición a amenazas. Por ejemplo, la información puede ser capturada o modificada maliciosamente mientras está en tránsito.

Ejemplos:

- El sistema de tratamiento de un hospital está conectado con el sistema público de seguridad social y con los sistemas de aseguradoras privadas.
- Las estaciones de trabajo que forman parte del sistema de tratamiento tienen acceso a internet.

P2. ¿Alguna parte del tratamiento se hace a través de internet?

La interacción con los interesados a través de internet expone al sistema de tratamiento a amenazas externas, tales como *phishing*, *SQL injection*, *man-in-the-middle attacks*, *DoS* y *XSS*. Estas amenazas pueden comprometer el sistema de tratamiento y afectar a las propiedades de seguridad de los datos (confidencialidad, integridad y disponibilidad).

Permitir que los trabajadores accedan al sistema de tratamiento a través de internet también incrementa la exposición a ataques externos y, aparte, incrementa la posibilidad de que los trabajadores hagan un mal uso de la información (accidental o intencionada).

Ejemplos:

- Tienda online, banca online, etc.
- Se utiliza el correo electrónico en el tratamiento.
- Los administradores del sistema de tratamiento pueden hacer tareas de mantenimiento o supervisión a través de internet.
- El acceso al sistema de tratamiento desde un espacio público puede facilitar que personas ajenas a la organización puedan observarlas.

P3. ¿Falta de seguimiento de un documento de buenas prácticas relevante en el diseño o la configuración del sistema de tratamiento?

Si el sistema de tratamiento no está bien diseñado o los elementos que lo componen no están configurados adecuadamente, los riesgos para la seguridad de los datos se incrementan. Hay multitud de guías de buenas prácticas en seguridad con diferente temática (red, equipos, etc.).

Ejemplos:

- Hay que diseñar la red siguiendo un documento de buenas prácticas que incluya elementos tales como cortafuegos, segmentación de la red y uso de VPN.
- Hay que hacer uso de un documento de buenas prácticas, en el momento de configurar el sistema operativo. Esto implica medidas como el uso de antivirus y no permitirse el uso de contraseñas inseguras.
- Hay que dimensionar el sistema de tratamiento pensando en las necesidades computacionales, de comunicación y de almacenamiento que se anticipan También hay que dotarlo del personal suficiente.
- Hay que hacer uso de un documento de buenas prácticas, en el momento de configurar el software. Por ejemplo, cómo configurar un servidor web para hacerlo más seguro.
- Hay que usar una metodología de desarrollo que tenga en cuenta la seguridad de los datos durante todo el ciclo de vida de la aplicación.

P4. ¿Falta de seguimiento de un documento de buenas prácticas relevante en el mantenimiento, la monitorización y la respuesta a incidentes del sistema de tratamiento?

Es esencial hacer un mantenimiento y una monitorización adecuada del sistema. El mantenimiento se debe hacer tanto de los dispositivos como del software. Monitorizar el sistema no sólo permite analizar un incidente una vez se ha producido, sino que también ayuda a detectar comportamientos sospechosos con el fin de evitar que el incidente tenga lugar, o para reducir su impacto.

Ejemplos:

- No aplicar las actualizaciones de seguridad del sistema operativo puede dar lugar a nuevos vectores de ataque.
- La falta de copias de seguridad regulares puede dar lugar a la pérdida de información en caso de incidente.

P5. ¿Hay una falta de seguridad física en las instalaciones donde tiene lugar el tratamiento?

La seguridad física de las instalaciones de tratamiento es esencial. Sin esta, no se puede garantizar la seguridad del sistema de tratamiento (ya sea electrónico o no).

Ejemplos:

- El CPD no está debidamente protegido con un sistema que impide el acceso a las personas no autorizadas.
- Las limitaciones de espacio han hecho que parte del archivo en papel se haya distribuido en diferentes áreas, que no garantizan la seguridad.
- El CPD no está protegido contra accidentes naturales e industriales (por ejemplo, fallos eléctricos, inundaciones).
- Se hace uso de un servicio en la nube sin tener garantías de que las instalaciones del proveedor están suficientemente protegidas.

Uso del sistema de Tratamiento

P6. ¿Hay una falta de claridad en la definición de los roles y las responsabilidades de los trabajadores?

Una falta de claridad en la definición de los roles y las responsabilidades puede dar lugar a un uso descontrolado de los datos (ya sea accidental o intencionado).

Ejemplos:

- Un trabajador de una oficina bancaria sólo debería consultar los datos de sus clientes.
- Los trabajadores son responsables de destruir la información (digital o no) de forma segura, cuando deja de ser necesaria.
- Los trabajadores son responsables de mantener la seguridad de los datos, cuando los comunican a alguna otra persona u organización.

P7. ¿Hay falta de claridad en la definición de los usos aceptables de los sistemas de tratamiento?

Cuando los usos aceptables de los sistemas de tratamiento no están definidos claramente, se incrementa el riesgo de hacer un mal uso y de introducir vulnerabilidades al sistema.

Ejemplos:

- La instalación de software de compartición de ficheros puede dar lugar a la compartición involuntaria de archivos.
- La instalación de software por parte de usuarios no administradores puede dar lugar a un mantenimiento deficiente.
- Visitar páginas web maliciosas podría ser una fuente de entrada de software malicioso y de robo de datos.

P8. ¿Puede el personal conectar dispositivos externos al sistema?

La conexión de dispositivos externos al sistema de tratamiento es una puerta a la entrada de software malicioso, de introducción de vulnerabilidades, etc. Aparte, también facilita la extracción de información.

Ejemplos:

- El personal conecta su teléfono o su lápiz de memoria a los puertos USB del ordenador.
- El personal puede utilizar sus dispositivos para efectuar tareas relacionadas con el tratamiento (BYOD).

P9. ¿Falta un procedimiento adecuado de registro y supervisión de las actividades relacionadas con el tratamiento?

La falta de un registro de las actividades (*log file*) puede incrementar las malas prácticas del personal y, a la vez, dificulta la investigación de los incidentes que se han producido.

Ejemplos:

- Se pueden consultar los expedientes de clientes / pacientes sin que quede un registro.
- Aunque se genera un registro de actividades, no se monitoriza.
- No hay constancia de las personas que entran en el CPD.

Personas

P10. ¿El personal recibe permisos que no son necesarios para cumplir las tareas que tiene encomendadas?

Cuanto mayor sea la base de personas que tienen acceso a unos datos, mayor es la probabilidad de que se produzca un abuso. Para evitar esto, es esencial que el sistema controle el acceso al sistema del personal y autorice sólo los accesos que son estrictamente necesarios para cumplir las tareas que tiene encomendadas.

Ejemplos:

- El acceso al historial clínico de un paciente debería estar limitado a los profesionales que lo tratan.

P11. ¿Se ha externalizado alguna parte del tratamiento a un encargado?

La externalización del tratamiento o parte del tratamiento a un encargado supone una pérdida de control sobre los datos. Hay que elegir un encargado que pueda ofrecer un nivel alto de seguridad y definir claramente sus responsabilidades.

Ejemplos:

- Se utiliza una nube para realizar parte del tratamiento.
- Se contratan unos servicios especializados para analizar unos datos.

P12. ¿Hay una falta de conocimiento del personal respecto del uso adecuado del sistema, de aspectos de seguridad de los datos o de las limitaciones de uso que impone el RGPD?

Una falta de conocimientos sobre el uso que se espera del sistema, sobre seguridad de la información o sobre las obligaciones y limitaciones que impone el RGPD puede dar lugar a malas prácticas.

Ejemplos:

- La falta de conocimientos en seguridad puede hacer que el personal que trata los datos sea más propenso a seguir las instrucciones de un correo de *phishing*.
- El personal debe recordar la necesidad de guardar los documentos físicos bajo las condiciones de seguridad adecuadas.

Otras características

P13. ¿Han sufrido la empresa u otras empresas del sector ataques últimamente?

La existencia de ataques anteriores se debe tomar como una advertencia de potenciales ataques futuros. Conviene tomar las medidas necesarias para evitar que ataques similares tengan éxito.

P14. ¿Se han recibido quejas de alguna persona respecto de la estabilidad o la seguridad del sistema de tratamiento últimamente?

La presencia de errores en el sistema de tratamiento incrementa la probabilidad de sufrir un ataque. Del mismo modo, las advertencias respecto de potenciales fallos en la seguridad del sistema també pueden indicar una probabilidad más alta de sufrir ataques.

Ejemplos:

- Al entrar datos incorrectos en un formulario, la aplicación de tratamiento muestra un error y finaliza de forma inesperada.
- Se ha recibido la notificación de un usuario de que el sistema es vulnerable a algún ataque específico.

P15. ¿Se tratan datos de especial interés o datos de un número muy grande de usuarios?

La presencia masiva de datos y la presencia de datos de especial interés son una motivación extra para posibles atacantes.

Ejemplo:

- Una gran empresa que almacena datos personales y financieros sobre clientes (por ejemplo, número de tarjeta de crédito).

Cada respuesta afirmativa en alguno de los apartados de las tablas anteriores indica un incremento de la probabilidad de que se materialice un impacto sobre la seguridad de los datos. Para estimar la probabilidad inicial (sin controles de seguridad), contamos el número de respuestas afirmativas y aplicamos la siguiente tabla:

Respuestas afirmativas	Probabilidad inicial
0 - 4	Baja
5 – 9	Media
10 - 15	Alta

6.4 Riesgo inicial

Una vez estimada el impacto y la probabilidad inicial, ya podemos dar la estimación del riesgo inicial (sin los controles de seguridad). Seguimos la misma tabla que hemos utilizado en la sección 4.6.

Probabilidad	Alta	Riesgo medio	Riesgo alto	Riesgo alto	Riesgo alto
	Media	Riesgo bajo	Riesgo medio	Riesgo alto	Riesgo alto
	Baja	Riesgo bajo	Riesgo bajo	Riesgo medio	Riesgo alto
		Bajo	Medio	Alto	Muy alto
		Impacto			

El resultado de esta sección es un cálculo del riesgo para cada una de las propiedades de seguridad (confidencialidad, integridad, disponibilidad), así como una medida de riesgo global (el máximo de los riesgos anteriores).

6.5 Controles de seguridad

Una vez calculado el riesgo inicial, hay que determinar qué controles (medidas para mejorar la seguridad) se aplican. Si el cálculo muestra un riesgo alto, hay que aplicar controles de seguridad para reducirlo; en caso contrario, esto no es imprescindible. Ahora bien, es recomendable aplicar unos controles mínimos de acuerdo con el riesgo estimado.

Los controles actúan sobre el riesgo de formas diversas: evitando que un incidente se produzca; reduciendo el impacto de un incidente, si se produce; facilitando la recuperación en caso de incidente; etc. Podemos encontrar diferentes listas de controles. Aquí hacemos uso de los controles del ENS (Esquema Nacional de Seguridad).

En el momento de determinar los controles de seguridad a aplicar, el ENS sólo tiene en cuenta el impacto. Es decir, la necesidad y la intensidad con que es necesario aplicar un control depende del impacto asociado a las diferentes propiedades de seguridad. En el ENS se consideran las siguientes propiedades: confidencialidad (C), integridad (I), disponibilidad (D), autenticidad (A) y trazabilidad (T). También se considera la categoría del sistema, que es el máximo de los Impactos de las propiedades anteriores. En nuestro caso, nos hemos limitado a la confidencialidad (C), la integridad (I), la disponibilidad (D) y el sistema.

Nuestro objetivo es reducir el riesgo, y esto se puede hacer tanto reduciendo el impacto como la probabilidad. En general, los controles se clasifican según el objetivo que tienen. Los controles preventivos y disuasivos reducen la probabilidad de un incidente, Mientras que los controles correctivos, de recuperación y compensatorios reducen el impacto. En el ENS, los controles son bastante complejos y, en general, tienen efecto tanto sobre el impacto como sobre la probabilidad.

Como guía a la hora de decidir los controles necesarios, proponemos los dos criterios siguientes:

- Para reducir el impacto, aplicaremos los controles de acuerdo con las dimensiones de seguridad que se ven afectadas por el control. La intensidad con la que hay que aplicar el control se determinará de acuerdo con el impacto de la dimensión de seguridad.

- Para reducir la probabilidad, hay que reducir el número de preguntas de la sección 6.3 que tienen respuesta afirmativa.

La mejor manera de hacerlo es evitar la casuística a qué se refiere la pregunta. Por ejemplo, una respuesta afirmativa a la pregunta "Q2. ¿Se hace alguna parte del tratamiento a través de internet?" Se puede transformar en negativa, si desconectamos el sistema de internet y forzamos que el tratamiento se haga in situ.

Cuando no sea posible evitar completamente la casuística de las preguntas, hay que aplicar controles de seguridad para reducir la probabilidad de que haya un ataque. La tabla siguiente muestra los controles que pueden tener efecto sobre cada una de las preguntas de la sección 6.3

.

Control	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15
[org.1]			×	×											
[org.2]						×	×								
[org.3]												×			
[org.4]					×	×	×	×		×					
[op.pl.2]			×	×											
[op.pl.3]			×												
[op.pl.4]			×												
[op.pl.5]			×												
[op.acc.1]					×					×					
[op.acc.2]					×					×					
[op.acc.3]						×				×					
[op.acc.4]					×					×					
[op.acc.5]					×					×					
[op.acc.6]					×				×						
[op.acc.7]		×							×						
[op.exp.1]					×	×									
[op.exp.2]			×												
[op.exp.3]			×												
[op.exp.4]				×											
[op.exp.5]				×											
[op.exp.6]		×	×	×				×							
[op.exp.7]				×											
[op.exp.8]									×						
[op.exp.9]				×											
[op.exp.10]									×						
[op.exp.11]			×												
[op.ext.1]											×				
[op.ext.2]											×				
[op.ext.3]															
[op.cont.1]			×								×				
[op.cont.2]			×	×											
[op.cont.3]			×	×											
[op.mon.1]	×	×		×	×				×						
[op.mon.2]			×												
[mp.if.1]					×				×						
[mp.if.2]					×				×						

Control	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15
[mp.if.3]					×										
[mp.if.4]					×										
[mp.if.5]					×										
[mp.if.6]					×										
[mp.if.7]					×				×						
[mp.if.8]					×										
[mp.per.1]						×	×					×			
[mp.per.2]						×						×			
[mp.per.3]												×			
[mp.per.4]												×			
[mp.per.5]												×			
[mp.eq.1]					×										
[mp.eq.2]				×											
[mp.eq.3]			×		×										
[mp.eq.4]			×		×										
[mp.com.1]	×	×													
[mp.com.2]	×	×													
[mp.com.3]	×	×													
[mp.com.4]				×											
[mp.com.5]	×	×													
[mp.si.1]					×										
[mp.si.2]					×										
[mp.si.3]					×										
[mp.si.4]					×										
[mp.si.5]					×										
[mp.sw.1]			×												
[mp.sw.2]			×												
[mp.info.2]						×				×					
[mp.info.3]	×	×			×										
[mp.info.4]			×												
[mp.info.5]									×						
[mp.info.6]						×				×					
[mp.info.7]				×	×										
[mp.s.1]		×				×									
[mp.s.2]	×	×													
[mp.s.3]	×	×													
[mp.s.4]	×														

Estos criterios constituyen una guía para ayudar a determinar los controles necesarios. Sin embargo, en el momento de calcular el riesgo residual, hay que justificar el efecto que tienen estos controles sobre el impacto y sobre la probabilidad.

- Política de seguridad [org.1] (sistema)

La política de seguridad es un documento de alto nivel que establece los principios básicos de seguridad en una organización.

Nivel: bajo, medio, alto

La política de seguridad debe establecer de forma clara, como mínimo lo siguiente:

- Los objetivos de la organización.
- El marco legal en que se desarrollan las actividades.
- Los roles y las funciones de seguridad, que deben definir los deberes y responsabilidades de cada uno y el procedimiento para la designación y renovación.
- Comités de coordinación de la seguridad (miembros y responsabilidades).
- Directrices para la estructuración de la información de seguridad.

Normativa de seguridad [org.2] (sistema)

Riesgo: bajo, medio, alto

Es necesario disponer de una serie de documentos que describan:

- El uso correcto de equipos, servicios e instalaciones.
- Qué se considera uso inapropiado.
- Las responsabilidades del personal respecto del cumplimiento o de la violación de estas normas (derechos, deberes y medidas disciplinarias).

Procedimientos de seguridad [org.3] (sistema)

Riesgo: bajo, medio, alto

Es necesario disponer de una serie de documentos que describan:

- Cómo desarrollar las tareas habituales.
- Quién tiene que hacer cada tarea.
- Cómo identificar comportamientos anómalos e informar de ello.

Proceso de autorización [org.4] (sistema)

Riesgo: bajo, medio, alto

Hay que establecer un proceso formal de autorizaciones que abarque todos los elementos del sistema:

- Uso de las instalaciones (habituales y alternativas).
- Entrada de equipos en producción.
- Entrada de aplicaciones en producción.
- Establecimiento de enlaces con otros sistemas.
- Utilización de medios de comunicación (habituales y alternativos).
- Utilización de soportes de información.
- Utilización de equipos móviles.

Arquitectura de seguridad [op.pl.2] (sistema)

Riesgo: bajo, medio, alto

La seguridad del sistema debería ser objeto de planteamiento integral, como mínimo en:

- Documentación de las instalaciones (área y puntos de acceso).
- Documentación del sistema (equipos, redes y puntos de acceso al sistema).
- Esquema de líneas de defensa (cortafuegos, DMZ, tecnologías para prevenir vulnerabilidades).

- Sistema de identificación y autenticación.
- Controles técnicos internos.

Adquisición de nuevos componentes [op.pl.3] (sistema)

Riesgo: bajo, medio, alto

Hay que establecer un procedimiento formal para planificar la adquisición de nuevos componentes del sistema, que debe:

- Ser conforme a las conclusiones del análisis de riesgos.
- Seguir la arquitectura de seguridad.
- Prever las necesidades técnicas, de formación y de financiación.

Dimensionamiento [op.pl.4] (D)

Riesgo: medio, alto

Estudio previo a la puesta en marcha del sistema, que incluya las necesidades de:

- Tratamiento.
- Almacenamiento.
- Comunicación.
- Personal (cantidad y calificación).
- Instalaciones y medios auxiliares.

Componentes certificados [op.pl.5] (sistema)

Riesgo: alto

Hay que utilizar sistemas, productos o equipos con funcionalidades de seguridad certificadas por entidades independientes de solvencia reconocida.

Identificación [op.acc.1] (sistema[1])

Riesgo: bajo, medio, alto

Hay que asignar un identificador singular a cada entidad que acceda al sistema.

Requerimientos de acceso [op.acc.2] (ICAT)

Riesgo: bajo, medio, alto

- Sólo pueden utilizar los recursos del sistema las entidades que disponen de derechos de acceso suficientes.
- Los derechos de acceso se deben establecer de acuerdo con el responsable de cada recurso y siguiendo la política y la normativa de seguridad.
- Hay que controlar, particularmente, el acceso a los componentes del sistema y los archivos de configuración.

[1] En el ENS, las propiedades son AT.

- Segregación de funciones y tareas [op.acc.3] (ICAT)

Riesgo: medio, alto

Necesidad de concurrencia de dos o más personas para realizar tareas críticas.

- Proceso de gestión de derechos de acceso [op.acc.4] (ICAT)

Riesgo: bajo, medio, alto

Los derechos de acceso de cada usuario se deben asignar de acuerdo con:

- Mínimo privilegio.
- Necesidad de conocer.
- Únicamente el personal competente puede modificar los derechos de acceso, de acuerdo con los criterios establecidos por el responsable.

- Mecanismo de autenticación [op.acc.5] (ICAT)

Riesgo: baja, medio, alto

- Se acepta cualquier mecanismo de autenticación.
- Las contraseñas deben estar bajo el control exclusivo del usuario.
- El usuario debe reconocer la recepción y aceptar las obligaciones (custodia diligente e información inmediata, en caso de pérdida).
- Los autenticadores deben renovarse periódicamente, de acuerdo con la política de la organización.
- Los autenticadores se deben retirar y desactivar cuando la entidad (persona, equipo o proceso) acabe su relación con el sistema.

Riesgo: medio, alto

- No se recomienda utilizar contraseñas.
- Se recomienda utilizar dispositivos físicos (*tokens*), lógicos (certificados digitales) o biométricos.
- Si se emplean contraseñas, hay que aplicar políticas rigurosas de calidad y renovación.

Riesgo: alto

- Los autenticadores se suspenderán automáticamente, si no se utilizan.
- No se admiten contraseñas.
- Se exige el uso de dispositivos físicos o biometría.
- Es necesario que los dispositivos físicos hagan uso de algoritmos acreditados.
- Se debe utilizar preferentemente productos certificados.

- Acceso local [op.acc.6] (ICAT)

Uno acceso local es el que se hace desde dentro de las propias instalaciones.

Riesgo: bajo, medio, alto

- Hay que evitar los ataques que, a pesar de no dar acceso, puedan revelar información del sistema.
- Hay que bloquear el acceso después de un número fijado de intentos fallidos.
- Hay que registrar los intentos de acceso (con éxito y fallidos).
- En el momento del acceso, el sistema debe informar al usuario a cerca de sus obligaciones.

Riesgo: medio, alto

- Se debe informar al usuario del último acceso con su identidad.

Riesgo: alto

- El acceso se debe limitar por fecha y hora.
- Hay que definir puntos donde el usuario debe renovar la autenticación.

Acceso remoto [op.acc.7] (ICAT)

Un acceso remoto es el que se hace desde fuera de las instalaciones de la organización.

Riesgo: bajo, medio, alto

- Hay que proteger el acceso de la misma manera que se hace en el acceso local.
- Hay que proteger las comunicaciones.

Riesgo: medio, alto

- Es necesario establecer una política que especifique qué tareas se pueden hacer remotamente y hay que autorizar al usuario previamente.

Inventario de activos [op.exp.1] (sistema)

Riesgo: bajo, medio, alto

- Se debe mantener un registro de los activos del sistema que describa la tipología e identifique al responsable.

Configuración de seguridad [op.exp.2] (sistema)

Riesgo: bajo, medio, alto

Los equipos deben configurarse antes de que empiecen a operar, de manera que:

- Se borren cuentas y contraseñas estándar.
- Se aplique la regla de la mínima funcionalidad.
- Se aplique la regla de seguridad por defecto.

- Gestión de la configuración [op.exp.3] (sistema)

Riesgo: medio, alto

La configuración del sistema se debe gestionar de forma continua, de manera que:

- En todo momento se mantiene la regla de funcionalidad mínima.
- En todo momento se mantiene la regla de seguridad por defecto.
- El sistema se adapta a las nuevas necesidades.
- El sistema reacciona a las vulnerabilidades reportadas.
- El sistema reacciona a incidencias.

- Mantenimiento [op.exp.4] (sistema)

Riesgo: bajo, medio, alto

- Hay que respetar las especificaciones de los fabricantes en cuanto a la instalación y el mantenimiento de los sistemas.
- Hay que hacer un seguimiento continuo de los comunicados de defectos.
- Es necesario disponer de un sistema para analizar, priorizar y aplicar las actualizaciones de seguridad.

- Gestión de cambios [op.exp.5] (sistema)

Riesgo: medio, alto

Se debe mantener un control continuo de los cambios realizados en el sistema:

- Todos los cambios anunciados por el fabricante se deben analizar, para determinar su conveniencia.
- Antes de aplicar cambios en producción, se deben comprobar en un equipo que no esté en producción.
- Los cambios se deben planificar, para reducir el impacto sobre la prestación de servicios.
- Los cambios que supongan un riesgo alto se deben aprobar explícitamente.

- Protección contra código malicioso [op.exp.6] (sistema)

Riesgo: bajo, medio, alto

- Es necesario disponer de mecanismos de prevención y reaccionar contra código malicioso.

- Gestión de incidentes [op.exp.7] (sistema)

Riesgo: medio, alto

Se dispondrá de un proceso para hacer frente a los incidentes de seguridad.

- Procedimiento de notificación.
- Registro de evidencias.

- Registro de la actividad de los usuarios [op.exp.8] (sistema[1])

Riesgo: alto

Hay que registrar todas las actividades de los usuarios del sistema, de manera que:

- Indique quien hace una actividad, cuando la hace y sobre qué datos.
- Incluya la actividad de los usuarios, de los operadores y de los administradores.
- Consten las actividades realizadas y los intentos fallidos.

- Registro de la gestión de incidentes [op.exp.9] (sistema)

Riesgo: medio, alto

Hay que registrar todas las actuaciones relacionadas con la gestión de incidencias:

- El informe inicial, las actuaciones y las modificaciones en el sistema.
- Las evidencias que puedan sustentar o hacer frente a una demanda judicial.
- Como resultado del análisis de incidentes, se deben revisar los eventos auditables.

- Protección de los registros de actividad [op.exp.10] (sistema[2])

Riesgo: alto

Hay que proteger los registros del sistema, de manera que:

- Se determinará el período de retención de los registros.
- Se debe asegurar la fecha y hora.
- El personal no autorizado no debe poder modificar los registros.
- Las copias de seguridad, si las hay, deben tener los mismos requerimientos.

- Protección de las claves criptográficas [op.exp.11] (sistema)

Las claves criptográficas se protegerán durante todo su ciclo de vida: generación, transporte al punto de explotación, custodia durante la explotación, archivo y destrucción.

Riesgo: bajo, medio, alto

- Los medios de generación deben estar aislados de los de explotación.
- Las claves archivadas deben estar en soportes aislados de los de explotación.

Riesgo: medio, alto

- Hay que utilizar herramientas certificadas (algoritmos, programas, dispositivos).

- Contratación y acuerdos de nivel de servicio [op.ext.1] (sistema)

Riesgo: medio, alto

[1] En el ENS la propiedad es T.
[2] En el ENS la propiedad es T.

- Antes de emplear recursos externos, hay que establecer contractualmente las características del servicio y las responsabilidades de las partes. En particular, hay que establecer la calidad mínima del servicio y las consecuencias de un incumplimiento.

Gestión diaria [op.ext.2] (sistema)

Riesgo: medio, alto

Para a la gestión diaria del sistema, es necesario:

- Un sistema para medir el cumplimiento de las obligaciones de servicio.
- Mecanismos y coordinación para hacer las tareas de mantenimiento de los sistemas afectados por el acuerdo.
- Mecanismos y coordinación en caso de incidencias.

Medios alternativos [op.ext.3] (D)

Riesgo: alto

Hay que prever que el servicio esté provisto con medios alternativos, si el servicio contratado no está disponible. El servicio alternativo debe ofrecer las mismas garantías.

Continuidad del servicio [op.cont.1] (D)

Riesgo: medio, alto

Hay que hacer un análisis de lo siguiente:

- Requerimientos de disponibilidad de cada servicio, según su impacto.
- Elementos críticos para cada servicio.

Plan de continuidad [op.cont.2] (D)

Riesgo: alto

Hay que establecer un plan de continuidad en caso de interrupciones de los servicios ofrecidos con los medios habituales:

- Se deben identificar funciones, responsabilidades y actividades a realizar.
- Hay que prever medios alternativos para continuar ofreciendo los servicios.
- Todos los medios alternativos deben estar planificados y materializados en contratos o acuerdos con los proveedores correspondientes.
- Todas las personas afectadas deben recibir formación específica.
- El plan de continuidad se integrará con otros planes de continuidad en materias ajenas a la seguridad.

Pruebas periódicas [op.cont.3] (D)

Riesgo: alto

Hay que hacer pruebas periódicas para detectar y corregir los errores o las deficiencias que pueda haber en el plan de continuidad.

- Detección de intrusiones [op.mon.1] (sistema)

Riesgo: alto

Se debe disponer de herramientas de detección y prevención de intrusiones.

- Sistema de métricas [op.mon.2] (sistema)

Riesgo: alto

Hay que establecer un conjunto de indicadores que mida la seguridad del sistema en los aspectos siguientes:

- Grado de implantación de las medidas de seguridad.
- Eficacia y eficiencia de las medidas de seguridad.
- Impacto de los incidentes de seguridad.

- Áreas separadas y control de acceso [mp.if.1] (sistema)

Riesgo: bajo, medio, alto

- El equipamiento se instalará en áreas separadas específicas para su función.
- Hay que controlar el acceso a las áreas indicadas, de manera que solo se pueda acceder por las entradas previstas y vigiladas.

- Identificación de las personas [mp.if.2] (sistema)

Riesgo: bajo, medio, alto

- Hay que identificar a todas las personas que acceden a los locales donde haya equipamiento del sistema informático.
- Hay que registrar la entrada y la salida de personas.

- Condicionamiento de los locales [mp.if.3] (sistema)

Riesgo: bajo, medio, alto

Los locales donde se ubican los sistemas de información y sus componentes deben disponer de elementos adecuados para hacer eficaz el funcionamiento del equipamiento instalado.

- Condiciones de temperatura y humedad.
- Protección contra las amenazas identificadas en el análisis de riesgo.
- Protección del cableado contra incidentes fortuitos o deliberados.

- Energía eléctrica [mp.if.4] (D)

Riesgo: bajo

Los locales donde se ubican los sistemas de información y sus componentes deben disponer de la energía eléctrica necesaria para funcionar, de manera que se garantice:

- El suministro de energía eléctrica.
- El funcionamiento correcto de las luces de emergencia.

Riesgo: bajo, medio, alto

En caso de fallo del suministro general, hay que garantizar el suministro eléctrico de los sistemas, con el tiempo suficiente para hacer una apagada ordenada y salvaguardando la información.

- Protección contra incendios [mp.if.5] (D)

Riesgo: bajo, medio, alto

Los locales donde se ubican los sistemas de información y sus componentes se deben proteger contra incendios fortuitos o deliberados.

- Protección contra inundaciones [mp.if.6] (D)

Riesgo: medio, alto

Los locales donde se ubican los sistemas de información y sus componentes se deben proteger contra incidentes fortuitos o deliberados causados por el agua.

- Registro de entrada y de salida de equipamiento [mp.if.7] (sistema)

Riesgo: bajo, medio, alto

Se debe mantener un registro detallado de la entrada y la salida de equipamiento, que incluya la identificación de la persona que autoriza el movimiento.

- Instalaciones alternativas [mp.if.8] (D)

Riesgo: alto

Hay que garantizar que hay instalaciones alternativas para poder trabajar, y que están disponibles, si las habituales no están disponibles. Las instalaciones alternativas deben disponer de las mismas garantías que las habituales.

- Caracterización del puesto de trabajo [mp.per.1] (sistema)

Riesgo: medio, alto

- Hay que definir las responsabilidades relacionadas con la seguridad en cada puesto de trabajo.
- Hay que definir las condiciones que deben satisfacer a las personas que ocupen cada puesto de trabajo (en particular, respecto a la confidencialidad).

- Hay que tener en cuenta las condiciones anteriores en la selección del personal, incluida la verificación de su vida laboral, formación y otros datos.

Deberes y obligaciones [mp.per.2] (sistema)

Riesgo: bajo, medio, alto

Hay que informar a cada persona que trabaje en el sistema de los deberes y las responsabilidades en materia de seguridad:

- Las medidas disciplinarias.
- Las obligaciones tanto en el periodo de desarrollo del trabajo como en el caso de finalización o traslado.
- El deber de confidencialidad respecto de los datos a qué tiene acceso.

Para el personal contratado a través de un tercero, hay que establecer:

- Los deberes y obligaciones del personal.
- Los deberes y obligaciones de cada parte.
- El procedimiento para resolver incidentes relacionados con el incumplimiento de las obligaciones.

Concienciación [mp.per.3] (sistema)

Riesgo: bajo, medio, alto

Hay que hacer las acciones necesarias para concienciar regularmente al personal acerca de su papel para que la seguridad del sistema alcance el nivel exigido. En particular, hay que recordar:

- La normativa relativa al buen uso de los sistemas.
- La identificación de incidentes, actividades o comportamientos sospechosos que hay que reportar.
- El procedimiento para informar de incidentes de seguridad.

Formación [mp.per.4] (sistema)

Riesgo: bajo, medio, alto

Hay que formar regularmente al personal en todas las materias necesarias para el desarrollo de sus funciones, en particular respecto de lo siguiente:

- Configuración del sistema.
- Detección y reacción a incidentes.
- Gestión de la información en cualquier soporte. Hay que abarcar, como mínimo, las actividades siguientes: almacenamiento, transferencia, copia, distribución y destrucción.

Personal alternativo [mp.per.5] (D)

Riesgo: alto

Hay que garantizar la disponibilidad de otras personas que puedan hacerse cargo de las funciones, si el personal habitual no está disponible. El personal alternativo debería estar sometido a las mismas garantías que el habitual.

- Puesto de trabajo vaciado [mp.eq.1] (sistema)

Riesgo: bajo, medio, alto

Se exigirá que los puestos de trabajo permanezcan vacíos, sin más material en la mesa que el necesario para la actividad que se está haciendo en cada momento.

Riesgo: medio, alto

El material debe guardarse en un lugar cerrado.

- Bloqueo del puesto de trabajo [mp.eq.2] (sistema)

Riesgo: medio, alto

El puesto de trabajo se debe bloquear al cabo de un tiempo de inactividad y es necesario requerir la autenticación del usuario para continuar la actividad

Riesgo: alto

Pasado un tiempo, superior al anterior, se deben cerrar las sesiones abiertas desde el puesto de trabajo.

- Protección de portátiles [mp.eq.3] (sistema)

Riesgo: bajo, medio, alto

Los equipos que abandonan las instalaciones se deben proteger adecuadamente:

- Hay que hacer un inventario de los equipos portátiles, con la identificación de la persona responsable y un control regular de que los equipos están bajo su control.
- Hay que establecer un canal para informar de pérdidas o sustracción.
- Es necesario que haya un sistema de protección perimetral, que minimice la visibilidad exterior y controle el acceso cuando el equipo se conecte a redes, en particular a redes públicas.
- Hay que evitar, en la medida de lo posible, que el equipo tenga claves de acceso remoto a la organización.

Riesgo: alto

- El equipo debe disponer de detectores de violación que permitan saber si el equipo ha sido manipulado.
- La información de nivel alto que tiene almacenada se debe cifrar.

- Medios alternativos [mp.eq.4] (D)

Riesgo: medio, alto

- Hay que garantizar la disponibilidad de medios alternativos de tratamiento de la información, si los habituales fallan. Estos medios alternativos deben estar sujetos a las mismas garantías de protección.
- Hay que establecer un tiempo máximo para que los equipos alternativos entren en funcionamiento.

- Perímetro seguro [mp.com.1] (sistema)

Riesgo: bajo, medio, alto

- Es necesario disponer de un cortafuegos que separe la red interna del exterior. Todo el tráfico debe pasar a través del cortafuegos, que solo debe permitir los flujos previamente autorizados.

Riesgo: alto

- El cortafuegos debe constar de dos o más equipos de diferentes fabricantes en cascada.
- Es necesario disponer de sistemas redundantes.

- Protección de la confidencialidad [mp.com.2] (C)

Riesgo: medio, alto

- Hay que utilizar una VPN, cuando la comunicación pase por fuera del dominio de seguridad.
- Hay que utilizar algoritmos acreditados por el CCN.

Riesgo: alto

- Preferentemente, hay que utilizar dispositivos de hardware para establecer y utilizar la VPN.
- Preferentemente, hay que utilizar productos certificados.

- Protección de la autenticidad y de la integridad [mp.com.3] (IA)

Riesgo: bajo, medio, alto

- Hay que garantizar la autenticidad del otro extremo de un canal de comunicación, antes de intercambiar información.
- Hay que prevenir ataques activos y garantizar que, como mínimo, se detectan. Se consideran ataques activos: la alteración de la información en tránsito, la introducción de información espuria y el secuestro de la sesión por una tercera parte.

Riesgo: medio, alto

- Hay que utilizar una VPN, cuando la comunicación pase por fuera del dominio de seguridad.
- Hay que utilizar algoritmos acreditados por el CCN.

Riesgo: alto

- Hay que valorar positivamente el uso de dispositivos de hardware en el momento de establecer la VPN.
- Preferentemente, hay que utilizar productos certificados.

Segregación de redes [mp.com.4] (sistema)

La segregación de redes limita la propagación de los incidentes de seguridad, que quedan restringidos al entorno donde tienen lugar.

Riesgo: alto

La red se debe segmentar, de manera que haya:

- Control de entrada de los usuarios a cada segmento.
- Control de salida de la información de cada segmento.
- Los puntos de interconexión (físico o lógico) deben estar particularmente asegurados, mantenidos y monitorizados.

Medios alternativos [mp.com.5] (D)

Riesgo: alto

Hay que garantizar que hay medios de comunicación alternativos si los habituales fallan, y que están disponibles. Es necesario que los medios alternativos:

- Estén sujetos a las mismas garantías de protección que los habituales.
- Garanticen un tiempo máximo de entrada en funcionamiento.

Etiquetado [mp.si.1] (C)

Riesgo: bajo, medio, alto

- Los soportes de información se etiquetan de manera que, sin revelar el contenido, indique el nivel de seguridad de la información contenida.
- Los usuarios deben estar capacitados para entender el significado de las etiquetas.

Criptografía [mp.si.2] (IC)

Esta medida se aplica, en particular, a todos los dispositivos extraíbles (CD, DVD, discos USB y otros análogos).

Riesgo: medio, alto

Hay que aplicar mecanismos criptográficos que garanticen la integridad y la confidencialidad de la información contenida.

Riesgo: alto

- Hay que utilizar algoritmos acreditados por el CCN.
- Hay que utilizar, preferentemente, productos certificados.

Custodia [mp.si.3] (sistema)

Riesgo: bajo, medio, alto

Hay que aplicar la diligencia y el control adecuados a los soportes de información que están bajo la responsabilidad de la organización.

- Hay que garantizar el control de acceso con medidas físicas, lógicas o ambas.
- Hay que garantizar que se respetan las exigencias de mantenimiento del fabricante.

Transporte [mp.si.4] (sistema)

Riesgo: bajo, medio, alto

El responsable de sistemas debe garantizar que, mientras se desplazan, los dispositivos están bajo control y que se cumple con los requisitos de seguridad. Hay que:

- Disponer de un registro de salida que identifique al transportista que recibe el soporte.
- Disponer de un registro de entrada que identifique al transportista que lo entrega.
- Disponer de un procedimiento que compare entradas y salidas. Si se detecta algún incidente, se deben activar las alarmas.
- Utilizar medios criptográficos de acuerdo con [mp.si.2].
- Gestionar las claves de acuerdo con [op.exp.11].

Borrado y destrucción [mp.si.5] (C)

Riesgo: medio, alto

El borrado y destrucción del soporte de la información se debe aplicar a cualquier tipo de equipo susceptible de almacenar información.

- Los soportes que se deben reutilizar o entregar a otra organización deben ser objeto de un borrado seguro.
- Hay que destruir los soportes de forma segura, cuando la naturaleza del soporte no permita un borrado seguro y así lo requiera el procedimiento asociado a la información contenida.

- Desarrollo de aplicaciones [mp.sw.1] (sistema)

Riesgo: medio, alto

- El desarrollo de aplicaciones debe hacerse sobre un sistema diferente y separado del de producción. No debe haber herramientas o datos de desarrollo en el entorno de producción.
- Hay que aplicar una metodología de desarrollo reconocida, que:
  - Tome en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida.
  - Trate específicamente los datos utilizados en las pruebas.
  - Permita la inspección del código fuente.
- Los elementos siguientes deben ser parte integral del diseño del sistema:
  - Mecanismos de identificación y autenticación.
  - Mecanismos de protección de la información tratada.
  - La generación y el tratamiento de pistas de auditoría.
- Las pruebas no se deben hacer con datos reales, a menos que se asegure el nivel de seguridad correspondiente.

- Aceptación y puesta en servicio [mp.sw.1] (sistema)

Riesgo: bajo, medio, alto

Antes de pasar a producción, hay que comprobar que la aplicación funciona correctamente:

- Se debe comprobar que se cumplen los criterios de aceptación en materia de seguridad y que no se deteriora la seguridad de los otros componentes del servicio.
- Las pruebas se deben realizar en un entorno aislado (preproducción).
- Las pruebas no se deben hacer con datos reales, a menos que se pueda garantizar la seguridad.

Riesgo: medio, alto

Antes de la puesta en funcionamiento, se deben hacer las inspecciones siguientes:

- Análisis de vulnerabilidades.
- Pruebas de penetración.

Riesgo: alto

Antes de la puesta en funcionamiento, hay que:

- Hacer un análisis de la coherencia en la integración de los procesos.
- Considerar la posibilidad de hacer una auditoría del código fuente.

- Calificación de la información [mp.info.2] (C)

Riesgo: bajo, medio, alto

- Para calificar la información, hay que tener en cuenta su naturaleza.

- La política de seguridad la debe establecer el responsable de cada información.
- La política de seguridad debe contener los criterios que determinan el nivel de seguridad requerido.
- Con los criterios anteriores, el responsable de cada información debe asignar a cada información el nivel de seguridad requerido.
- El responsable de cada información debe tener en exclusiva la potestad de modificar el nivel de seguridad requerido.

Riesgo: medio, alto

Hay que redactar los procedimientos que describan cómo etiquetar y tratar la información, según su nivel de seguridad. En particular, como hay que hacer:

- El control de acceso.
- El almacenamiento.
- Las copias.
- El etiquetado de soportes.
- La transmisión telemática.

Cifrado de la información [mp.info.3] (C)

Riesgo: medio, alto

- La información con un nivel alto de confidencialidad debe ser cifrada, durante el almacenamiento y la transmisión. Sólo debería estar en claro cuando se esté utilizando.
- El uso de criptografía en las comunicaciones se debe hacer de acuerdo con [mp.com.2].
- El uso de criptografía en los soportes se debe hacer de acuerdo con [mp.si.2].

Firma electrónica [mp.info.4] (IA)

La firma electrónica garantiza la autenticidad del firmante y la integridad del contenido. También es un mecanismo de prevención del repudio.

Riesgo: bajo

Se puede utilizar cualquier medio de firma electrónica.

Riesgo: medio, alto

Los medios de firma electrónica deben ser proporcionales a la calificación de la información tratada. En cualquier caso, hay que utilizar:

- Algoritmos acreditados por el CCN.
- Certificados reconocidos, preferentemente.
- Dispositivos seguros de firma, preferentemente.

Se debe garantizar la verificación y la validación de la firma. Con esta finalidad:

- Se debe adjuntar a la firma toda la información pertinente: certificados y datos de verificaciones y de validación.
- Se debe proteger la firma con un sello temporal.
- El organismo que recoge los documentos firmados debe verificar y validar la firma, en el momento de recepción.

Riesgo: alto

- Hay que utilizar certificados reconocidos.
- Hay que utilizar dispositivos seguros de creación de firmas.
- Hay que utilizar, preferentemente, productos certificados.

Sellos temporales [mp.info.5] (T)

Riesgo: alto

Los sellos temporales evitan la posibilidad de repudio posterior:

- Se deben aplicar a la información que pueda ser utilizada como evidencia electrónica en el futuro.
- Los datos para verificar la fecha se tienen que tratar con la misma seguridad que la información.
- Hay que utilizar productos certificados o servicios externos admitidos.

Limpieza de documentos [mp.info.6] (C)

Riesgo: bajo, medio, alto

El proceso de limpieza de documentos debe eliminar toda la información adicional que haya en campos ocultos, metadatos, comentarios o revisiones anteriores, salvo que esta información pertenezca al receptor.

Esta medida es especialmente relevante cuando el documento se difunde ampliamente.

Copias de seguridad [mp.info.7] (D)

Riesgo: medio, alto

Hay que hacer copias de seguridad que permitan recuperar datos perdidos accidental o intencionadamente.

Las copias deben tener la misma seguridad que los datos iniciales. En particular, hay que considerar la necesidad de que estén cifradas.

Las copias deben contener:

- Información de trabajo de la organización.
- Las aplicaciones en explotación, incluidos los sistemas operativos.

- Los datos de configuración, servicios, aplicaciones, equipos y otros análogos.
- Las claves utilizadas para preservar la confidencialidad de la información.

Protección del correo electrónico [mp.s.1] (sistema)

Riesgo: bajo, medio, alto

- La información distribuida por correo electrónico se debe proteger, tanto el cuerpo como los anexos.
- Se debe proteger la información de enrutamiento de mensajería y establecimiento de conexiones.
- Se debe proteger la organización de problemas que se materializan por correo electrónico: spam, software malicioso (virus, gusanos, etc.), código.
- Se deben establecer normas para el uso apropiado del correo electrónico. Estas normas deben tener: limitaciones de uso y actividades de formación y concienciación.

Protección de servicios y aplicaciones web [mp.s.2] (sistema)

Riesgo: bajo, medio, alto

Cuando la información tenga algún tipo de control de acceso, hay que garantizar la imposibilidad de acceder a la información sin autenticarse. En particular, hay que:

- Evitar que el servidor ofrezca acceso a los documentos por vías alternativas.
- Prevenir ataques de manipulación de URL.
- Prevenir ataques de manipulación de galletas.
- Prevenir ataques de Inyección de código.
- Prevenir los intentos de escalada de privilegios.
- Prevenir los ataques de XSS.
- Prevenir los ataques de manipulación de servidores intermedios (*proxy*) y de caché.

Protección contra la denegación de servicio [mp.s.3] (D) (impacto, probabilidad)

Riesgo: medio, alto

Se tienen que establecer medidas preventivas y reactivas contra los ataques de denegación de servicio:

- Dotar el sistema de la capacidad suficiente para atender la carga prevista.
- Desplegar tecnologías para prevenir los ataques conocidos.

Riesgo: alto

- Hay que establecer un sistema de detección de los ataques de denegación de servicio.
- Es necesario establecer procedimientos para reaccionar a los ataques, incluida la comunicación con el proveedor de comunicaciones.
- Hay que impedir que se lancen ataques desde las propias instalaciones.

- Medios alternativos [mp.s.9] (D) (impacto)

Riesgo: alto

Hay que garantizar que hay medios alternativos si los habituales fallan, y que están disponibles. Estos medios alternativos deben tener las mismas garantías de protección que los habituales.

6.6 Cálculo del riesgo residual

Una vez establecidos los controles de seguridad, es necesario determinar cómo afectan al riesgo. En general, los controles de seguridad se clasifican según el objetivo que tienen: preventivo, de detección, correctivo, disuasivo, de recuperación y compensatorio. A la hora de calcular el riesgo, el efecto de los controles se traduce en una reducción del impacto o de la probabilidad de un incidente.

En la sección anterior hemos dado unas pautas para seleccionar los controles a aplicar, de acuerdo con el impacto y la probabilidad. Estas pautas son meramente indicativas y no se traducen en una reducción directa del impacto o de la probabilidad de un incidente. Es el responsable del tratamiento quien deberá decidir qué controles hay que aplicar y justificar los efectos que estos controles tienen sobre el impacto y la probabilidad.

El riesgo residual se calcula a partir del impacto y la probabilidad residuales, utilizando la tabla de la sección 4.6. Si el riesgo residual es alto, hay que proponer nuevos controles para reducirlo. Si no es posible reducirlo, antes de iniciar el tratamiento se debe consultar a la autoridad de protección de datos competente sobre su idoneidad.