apdcat
Autoritat Catalana de Protecció de Dades

Evaluación de impacto relativa a la protección de datos

Actualización: julio 2025

Colección guías. Núm. 4

Generalitat de Catalunya

© Barcelona, 2024

El contenido de este informe es titularidad de la Autoridad Catalana de Protección de Datos y está sujeto a la licencia de Creative Commons BY-NC-ND.

La autoría de la obra se reconocerá a través de la inclusión de la siguiente mención:

Obra titularidad de la Autoridad Catalana de Protección de Datos.

Licenciada bajo licencia CC BY-NC-ND.

La licencia presenta las siguientes particularidades:

Se permite libremente:

Copiar, distribuir y comunicar públicamente la obra, bajo las siguientes condiciones:

- Reconocimiento: Se debe reconocer la autoría de la obra de la forma especificada por el autor o el licenciador (en todo caso, no de forma que sugiera que tiene o da apoyo a su obra).
- No comercial: No se puede utilizar esta obra para fines comerciales o promocionales.
- Sin obras derivadas: No se puede alterar, transformar o generar una obra derivada a partir de esa obra.

Aviso: Al reutilizar o distribuir la obra, es necesario que se mencionen claramente los términos de la licencia de esta obra.

El texto completo de la licencia se puede consultar en https://creativecommons.org/licenses/by-nc-nd/4.0/deed.es.

Índice

1. Introducción 7
2. Introducción a las EIPD 8
2.1 ¿Qué es una evaluación de impacto? 8
2.2 ¿Cuándo hay que hacer una evaluación de impacto? 9
2.3 ¿Cómo se hace una EIPD? 14
2.3.1 ¿En qué momento hay que hacer la EIPD? 14
2.3.2 ¿Quién interviene en una EIPD? 14
2.3.3 ¿Cuál es el contenido mínimo de una EIPD? 15
2.3.4 ¿Cuáles son las fases de una EIPD? 15
2.4 ¿Qué hay que hacer si la EIPD concluye que el riesgo es alto? 17
3. Descripción sistemática del tratamiento 18
3.1 ¿Cuál es el tratamiento de datos? 18
3.2 ¿Cuál es la finalidad del tratamiento? 19
3.3 ¿Tipos y características de los datos a tratar? 19
3.3.1 Fuente de los datos 20
3.3.2 Plazo de conservación 20
3.3.3 Datos especialmente sensibles 20
3.3.4 Uso con una finalidad diferente de la que motivó la recogida 21
3.4 ¿Qué actores intervienen en el tratamiento? 21
3.5 ¿Cuáles son los procesos de tratamiento? 21
3.6 ¿Dónde se hace el tratamiento de los datos? 21
4. Necesidad y proporcionalidad del tratamiento 23
4.1 Evaluación de la finalidad del tratamiento 24
4.1.1 Tratamiento con una finalidad diferente de la que motivó la recogida 24
4.1.2 Compatibilidad de finalidades 24
4.2 Principio de licitud y lealtad 25
4.2.1 Licitud 25
4.2.2 Lealtad 28
4.3 Principio de minimización 29

4.4 Principio de limitación del plazo de conservación 29
4.5 Principio de exactitud 30
4.6 Riesgos del tratamiento 30
4.6.1 Impacto 32
4.6.2 Amenazas y probabilidad 33
4.6.3 Determinación del riesgo 33
4.6.4 Reducción de los riesgos 34
4.7 Necesidad y proporcionalidad del tratamiento 35
4.8 Opinión de las personas interesadas 36
5. Protección de los derechos de las personas 36
5.1 Transparencia 36
5.2 Derecho de información 37
5.3 Derecho de acceso 39
5.4 Derecho de rectificación 40
5.5 Derecho de supresión 40
5.6 Derecho a limitar el tratamiento 41
5.7 Derecho a la portabilidad de datos 42
5.8 Derecho de oposición 42
5.9 Derecho a no ser objeto de decisiones automatizadas 43
6. Riesgos en la seguridad de los datos 43
6.1 Breve introducción a la seguridad de la información 45
6.2 Impacto 45
6.3 Probabilidad inicial 47
6.4 Riesgo inicial 52
6.5 Controles de seguridad 52
6.5.1 Política de seguridad [org.1] (sistema) 55
6.5.2 Normativa de seguridad [org.2] (sistema) 56
6.5.3 Procedimientos de seguridad [org.3] (sistema) 56
6.5.4 Proceso de autorización [org.4] (sistema) 56
6.5.5 Arquitectura de seguridad [op.pl.2] (sistema) 57
6.5.6 Adquisición de nuevos componentes [op.pl.3] (sistema) 57

6.5.7 Dimensionamiento [op.pl.4] (D) 58
6.5.8 Componentes certificados [op.pl.5] (sistema) 58
6.5.9 Identificación [op.acc.1] (sistema) 58
6.5.10 Requerimientos de acceso [op.acc.2] (ICAT) 59
6.5.11 Segregación de funciones y tareas [op.acc.3] (ICAT) 59
6.5.12 Proceso de gestión de derechos de acceso [op.acc.4] (ICAT) 59
6.5.13 Mecanismo de autenticación para usuarios externos [op.acc.5] (ICAT) 60
6.5.14 Mecanismo de autenticación para usuarios internos [op.acc.6] (ICAT) 60
6.5.15 Inventario de activos [op.exp.1] (sistema) 62
6.5.16 Configuración de seguridad [op.exp.2] (sistema) 62
6.5.17 Gestión de la configuración de la seguridad [op.exp.3] (sistema) 62
6.5.18 Mantenimiento y actualizaciones de seguridad [op.exp.4] (sistema) 63
6.5.19 Gestión de cambios [op.exp.5] (sistema) 63
6.5.20 Protección contra código malicioso [op.exp.6] (sistema) 64
6.5.21 Gestión de incidencias [op.exp.7] (sistema) 64
6.5.22 Registro de la actividad de les persones usuarias [op.exp.8] (sistema) 65
6.5.23 Registro de la gestión de incidencias [op.exp.9] (sistema) 65
6.5.24 Protección de les claves criptográficas [op.exp.10] (sistema) 66
6.5.25 Contratación y acuerdos de nivel de servicios [op.ext.1] (sistema) 66
6.5.26 Gestión diaria [op.ext.2] (sistema) 66
6.5.27 Protección de la cadena de suministro [op.ext.3] (sistema) 66
6.5.28 Interconexión de sistemas [op.ext.4] (sistema) 67
6.5.29 Protección de servicios en la nube [op.nub.1] (sistema) 67
6.5.30 Análisis de impacto [op.cont.1] (D) 67
6.5.31 Plan de continuidad [op.cont.2] (D) 68
6.5.32 Pruebas periódicas [op.cont.3] (D) 68
6.5.33 Medios alternativos [op.cont.4] (D) 68
6.5.34 Detección de intrusiones [op.mon.1] (sistema) 69
6.5.35 Sistema de métricas [op.mon.2] (sistema) 69
6.5.36 Vigilancia [op.mon.3] (sistema) 69
6.5.37 Áreas separadas y control de acceso [mp.if.1] (sistema) 70

6.5.38 Identificación de les personas [mp.if.2] (sistema) 70
6.5.39 Acondicionamiento de los locales [mp.if.3] (sistema) 70
6.5.40 Energía eléctrica [mp.if.4] (D) 70
6.5.41 Protección contra incendios [mp.if.5] (D) 71
6.5.42 Protección contra inundaciones [mp.if.6] (D) 71
6.5.43 Registro de entrada y de salida de equipamiento [mp.if.7] (sistema) 71
6.5.44 Caracterización del puesto de trabajo [mp.per.1] (sistema) 71
6.5.45 Deberes y obligaciones [mp.per.2] (sistema) 72
6.5.46 Concienciación [mp.per.3] (sistema) 72
6.5.47 Formación [mp.per.4] (sistema) 72
6.5.48 Puesto de trabajo vaciado [mp.eq.1] (sistema) 73
6.5.49 Bloqueo del puesto de trabajo [mp.eq.2] (sistema) 73
6.5.50 Protección de portátiles [mp.eq.3] (sistema) 73
6.5.51 Otros dispositivos conectados a la red [mp.eq.4] (C) 74
6.5.52 Perímetro seguro [mp.com.1] (sistema) 74
6.5.53 Protección de la confidencialidad [mp.com.2] (C) 74
6.5.54 Protección de la autenticidad y de la integridad [mp.com.3] (IA) 75
6.5.55 Segregación de flujos de información [mp.com.4] (sistema) 75
6.5.57 Etiquetado [mp.si.1] (C) 76
6.5.58 Criptografía [mp.si.2] (IC) 76
6.5.59 Custodia [mp.si.3] (sistema) 77
6.5.60 Transporte [mp.si.4] (sistema) 77
6.5.61 Borrado y destrucción [mp.si.5] (C) 77
6.5.62 Desarrollo de aplicaciones [mp.sw.1] (sistema) 78
6.5.63 Aceptación y puesta en servicio [mp.sw.1] (sistema) 78
6.5.64 Calificación de la información [mp.info.2] (C) 79
6.5.65 Firma electrónica [mp.info.3] (IA) 79
6.5.66 Sellos temporales [mp.info.4] (T) 80
6.5.67 Limpieza de documentos [mp.info.5] (C) 80
6.5.68 Copias de seguridad [mp.info.6] (D) 80
6.5.69 Protección del correo electrónico [mp.s.1] (sistema) 81

6.5.70 Protección de servicios y aplicaciones web [mp.s.2] (sistema)..... 81
6.5.71 Protección de la navegación web [mp.s.3] (sistema)..... 82
6.5.72 Protección contra la denegación de servicio [mp.s.4] (D) (impacto, probabilidad) 82
6.6 Cálculo del riesgo residual 83

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 con respecto 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 tratamientos: evaluar el impacto de las operaciones de tratamiento en la protección de los datos personales, cuando sea probable que el tratamiento comporte 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 y al riesgo, 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, siendo una tarea de responsabilidad proactiva.

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 manera 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 (tal 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 tratar 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.
- Hay que 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 en cuanto al tratamiento de sus datos (derecho a la información, etc.). Ahora bien, 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 otros oportunidades.
- Discriminación.
- Suplantación de la identidad y otros fraudes.
- Pérdidas económicas.
- Daños a la reputación.
- Daños físicos.
- Pérdida de la confidencialidad.

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

- Imposibilidad de ejercer algún derecho.

Estos impactos se pueden materializar por dos razones principales. La primera es que el tratamiento, tal como está diseñado, pueda dar lugar a estos impactos; ya sea por el tipo de datos que se tratan, por quien tiene acceso a ellos, por 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 particular, que es necesario y proporcionado y que se establecen los mecanismos necesarios para que las personas interesadas puedan ejercer sus derechos.

Para controlar los riesgos que afectan a la seguridad de los datos, es necesario 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 ejecute 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 los que la EIPD es obligatoria[2].

Dada la falta de especificidad del RGPD, seguiremos el procedimiento que describe la guía WP248 del GT29[3], que da una lista de nueve características de los tratamientos que pueden ser indicativas de un riesgo alto (ver más abajo). A mayor número de estas características, más probable es que un tratamiento presente un riesgo grave. Según esta lista, hay que hacer una EIPD cuando el tratamiento presenta dos o más, aunque indica que puede ser conveniente hacer la EIPD incluso en algunos casos en que solo presenta una.

[2] RGPD, articulo 35.3

[3] Ratificada por el Comité Europeo de Protección de Datos, que sustituye al GT29, en su primera sesión.

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 sufrir 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 las personas interesadas sean conscientes de que se están recogiendo y de cómo se usarán.

4. Datos sensibles.

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

   - Origen racial o étnico.
   - Opiniones políticas o filosóficas.
   - Pertenencia a un sindicato.
   - Datos genéticos.
   - Datos biométricos tratados con la finalidad de identificar una persona de forma unívoca.
   - Datos relativos a la salud.
   - Datos relativos a la vida sexual o la orientación sexual.

   También incluye:

   - Datos relativos a condenas o 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 que se detecte un desequilibrio entre la posición del responsable del tratamiento y la persona interesada. Por ejemplo:

   - Tratamiento de datos del personal en relación a la gestión de recursos humanos.
   - Menores y personas mayores.
   - Personas con enfermedades mentales.
   - Personas 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 peatones no pueden evitar.
   - Consulta del historial de crédito de unoa persona usuaria por parte de un banco, para decidir si le concede un crédito.

Comentarios

- En versiones anteriores de la guía sobre AIPD 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 hay que hacer la AIPD. Hay una tendencia general a adoptar la propuesta del GT29. Este es el caso de la autoridad catalana (APDCAT) y de la española (AEPD).

Ejemplos

- Uno hospital que trata datos sanitarios de pacientes.
  Criterios que son de aplicación:
  - Datos sensibles.
  - Tratamiento a grande escala.
  - Datos relativos a personas vulnerables.
- Uso de cámaras para controlar el comportamiento de las personas conductoras. Se prevé el uso de un sistema inteligente para seleccionar coches y reconocer matrículas.
  Criterios que son de aplicación:
  - Observación sistemática.
  - Uso innovador de tecnologías.
- Una empresa que observa sistemáticamente las actividades de su personal, del lugar de trabajo, de la actividad en internet, etc.
  Criterios que son de aplicación:
  - Observación sistemática.
  - Datos relativos a personas vulnerables.
- Recogida de datos públicos para elaborar perfiles.
  Criterios que son de aplicación:
  - 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 parecidos 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. Ahí, 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 uno lugar donde el derecho comunitario sea de aplicación, o por una empresa u organización situada fuera de la UE, si ésta trata datos de personas residentes en la UE para actividades relacionadas con la oferta de bienes, servicios y para controlar el comportamiento.

Las operaciones de tratamiento pueden evolucionar rápidamente, lo que puede afectar a los riesgos y la necesidad de ejecutar una EIPD, así como 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 se 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?

2.3.1 ¿En qué momento hay que hacer 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 por 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 reevaluación. 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).

2.3.2 ¿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 existe, debe apoyar al responsable a la hora 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 documentados en la EIPD. En particular, el responsable del tratamiento debe pedir opinión al DPD en los siguientes aspectos:

- Determinar si es necesario hacer una EIPD.
- La metodología a usar 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 hecho correctamente i si las conclusiones satisfacen los requerimientos de protección de datos.

El responsable del tratamiento debe buscar la opinión de les personas interesadas sobre la operación de tratamiento, cuando esto se considere apropiado. Si no se considera apropiado, hay que documentar el porqué; por ejemplo, por qué buscar esta opinión tiene un

coste desproporcionado, es impracticable o puede poner en riesgo la confidencialidad del plan de negocio.

La opinión de les personas interesadas se puede recoger de diferentes maneras: encuestas, consulta a representantes del personal, 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.

Aparte 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, personas expertas, responsables de seguridad, etc.

2.3.3 ¿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.

2.3.4 ¿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 hay que hacer la EIPD.

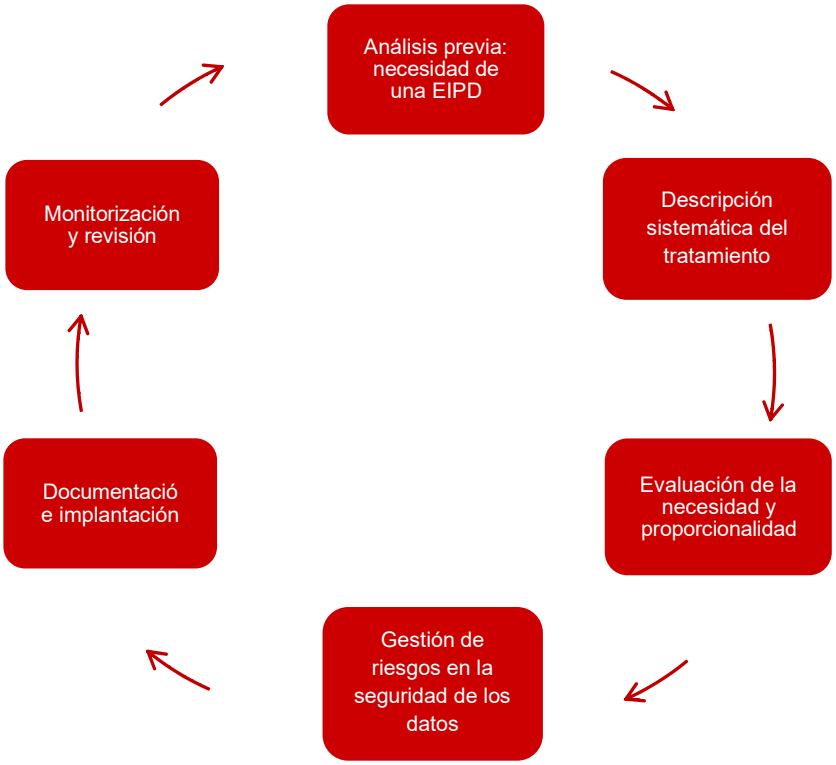
2. Descripción sistemática del tratamiento. La descripción del tratamiento y el contexto en que tiene lugar es esencial para determinar los riesgos que comporta.

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 esta finalidad (necesidad) y es necesario que el beneficio del tratamiento sea superior a los 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 realizados en los puntos anteriores. Las medidas adoptadas para salvaguardar los derechos y las libertades de las personas deben implementarse 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 hay que 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 que 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, como 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 esmerada qué riesgos pueden afectar a un tratamiento, es necesario 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 utilizar para describir el tratamiento. El objetivo de las preguntas es poner de relieve aspectos que pueden ser clave a la hora de determinar los riesgos del tratamiento[4].

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 tipo 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 hacer una EIPD adaptada a su caso, pero la puede basar en la de la aplicación.

[4] *Guidelines for SME on the security of personal data processin*, ENISA, Diciembre 2016

Ejemplos

- Un hospital gestiona datos médicos de pacientes: historial médico, datos de contacto, etc.
- El sistema de recursos humanos de una empresa gestiona datos personales de su personal: 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.

La obligación del responsable de especificar la finalidad del tratamiento antes de iniciarlo ayuda a las personas interesadas a entender el uso que se hará de sus datos; de esta manera, permite que las personas interesadas tomen decisiones informadas respecto del uso de sus datos. Además, evita que, una vez recogidos, los datos se usen con otras finalidades.

El principio de limitación de la finalidad está estrechamente relacionado con otros principios, como el de licitud, lealtad y transparencia. La transparencia exige que las personas interesadas conozcan el 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.

Ejemplos

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

Aunque en los casos anteriores los datos tratados pueden ser los mismos, la finalidad es muy diferente. 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, una base legal posible es el consentimiento.

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 manera de obtener consentimiento.

Las características más relevantes de los datos son:

3.3.1 Fuente de los datos

Conviene especificar si los datos se han obtenido directamente de la persona interesada o bien de un tercero y, si es así, especificarlo.

3.3.2 Plazo de conservación

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

3.3.3 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 mayores riesgos 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 inequívoca a una persona.
- Datos relativos a la salud.
- Datos relativos a la vida o la orientación sexual de una persona.

A pesar de no estar contenidos 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, menores) también reciben una protección especial.

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

Si se quieren utilizar datos con una finalidad diferente de la que motivó su 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, las personas interesadas y el delegado DPD), el tratamiento puede verse 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).

Existe una estrecha relación entre los medios que se utilizan para tratar los datos y los riesgos del tratamiento. Además, 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, algo 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 a la hora de determinar si es necesario hacer una EIPD. Ahora bien, 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 las personas interesadas 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 siguientes condiciones:

- La Comisión Europea considera que el tercer país, territorio, sector de un país u organización internacional ofrece un nivel de protección adecuado. La lista de países reconocidos es: Andorra, Argentina, Canadá (organizaciones comerciales), Estados Unidos (limitado al Marco de Trabajo de Privacidad), Guernsey, Isla de Man, Islas

Feroe, Israel, Japón, Jersey, Nueva Zelanda, Reino Unido, República de Corea, Suiza y Uruguay.

- Si el responsable o el encargado proporcionan las garantías adecuadas y las personas interesadas disponen de derechos exigibles y acciones legales efectivas. Las garantías adecuadas pueden ser aportadas 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 adoptados 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.

    - La persona interesada ha dado el consentimiento a la transferencia.
    - La transferencia es necesaria para ejecutar un contrato entre la persona interesada y el responsable.
    - La transferencia es necesaria para ejecutar un contrato, en interés de la persona interesada, 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 de la persona interesada o de otras personas, cuando la persona interesada está incapacitada per 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 alcanzar su finalidad.
- Uno tratamiento es necesario cuando la finalidad no se pueda alcanzar de manera menos intrusiva.
- Uno tratamiento es proporcionado cuando los beneficios son superiores a los perjuicios potenciales.

En la descripción del tratamiento realizada 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, en su caso, 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, de 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

4.1.1 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, salvo que se dé una de las condiciones siguientes[5]:

- Se ha obtenido el consentimiento de las personas interesadas del nuevo tratamiento.
- 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.
    - Protección de la independencia judicial y de los procedimientos judiciales.
    - Prevención, investigación, detección y procesamiento de infracciones en normas deontológicas.
    - La protección de la persona interesada o de los derechos y libertades de otros.
    - La ejecución de demandas civiles.

4.1.2 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 la persona interesada puede anticipar el nuevo tratamiento.
- La naturaleza de los datos. En particular, en cuanto a categorías especiales (art. 9 RGPD) y a datos de condenas y delitos penales (art. 10 RGPD).
- Las posibles consecuencias del nuevo tratamiento.
- Si hay garantías adecuadas.

[5] Articulo 6.4 RGPD.

Como norma general, si la nueva finalidad es muy diferente de la inicial y no es una finalidad que las personas interesadas pueden 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 [6].

4.2 Principio de licitud y lealtad

4.2.1 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:

- La persona interesada ha dado su consentimiento per al tratamiento de sus datos personales, para una o varias finalidades específicas.
- El tratamiento es necesario para ejecutar un contrato en el que la persona interesada 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 de la persona interesada 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.
- El tratamiento es necesario para satisfacer los intereses legítimos del responsable del tratamiento o de un tercero, siempre que no prevalezcan los intereses o derechos y libertades fundamentales de la persona interesada (en particular, cuando es menor).

Además, 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.

[6] Articulo 6.4 RGPD.

A la hora de escoger la base legal sobre la que se debe fundamentar el tratamiento, hay que tener en cuenta su finalidad y contexto. Hay que elegir la base legal que encaja mejor con las circunstancias. No hay una base legal mejor o más importante que las demás. 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 de buen comienzo.

Algunas de las bases legales tienen una finalidad específica: un contrato con la persona interesada, 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 otras finalidades, 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 las personas interesadas control total sobre el uso de sus datos (incluida la posibilidad de que retiren el consentimiento y que no se pueda seguir 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 ser que las personas interesadas de que no entiendan este cambio.

Ejemplo

Una organización decide tratar datos personales sobre la base del consentimiento. Después de recoger el consentimiento de las personas interesadas 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 las personas interesadas 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.

4.2.1.1 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 menores 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, cal que el consentimiento lo dé o lo autorice la persona 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.

4.2.1.2 Tratamiento de categorías especiales de datos

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

- La persona interesada 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 de la persona interesada o de otra persona, y la persona interesada no está capacitada para dar el consentimiento.
- 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 a personas con las que mantienen contactos en relación con estas finalidades y los datos no se comuniquen a terceros, sin el consentimiento de las personas interesadas.
- El tratamiento hace referencia a datos que la persona interesada ha hecho públicos.
- 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 personal, 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.

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

La base legal escogida 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 los que el enlace entre uno y otro es probable. Por ejemplo, si la base legal es el interés vital, es probable que la base per al tratamiento de categorías especiales sea la misma.

4.2.1.3 Tratamiento de datos penales

A pesar de no ser 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 públicas o cuando lo autorice el derecho de la unión o del estado miembro. Además, se establece que los registros exhaustivos de condenas criminales sólo pueden mantenerse bajo control de la autoridad.

4.2.1.4 Validez del consentimiento

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

- 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 a datos personales no necesarios para ejecutar el contrato.
- Se ha informado a las personas interesas de la posibilidad de retirar el consentimiento en cualquier momento.

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

4.2.2 Lealtad

Un tratamiento es leal si hace un uso de los datos que sea previsible para las personas interesadas (en relación con la finalidad del tratamiento) y no se derivan consecuencias adversas para las personas interesadas 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 limitados a lo estrictamente necesario para cumplir la finalidad del tratamiento. Este es un punto clave a la hora de 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. Hay que 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 a la hora 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 ser 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 continúan 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 deben tratar datos insuficientes o incompletos para la finalidad pretendida.

4.4 Principio de limitación del plazo de conservación

Los datos personales no deben conservarse 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 es necesario 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 cuándo tiempo deben conservarse los datos. Es el responsable del tratamiento quien debe fijar su periodo de retención, de acuerdo con las necesidades del

tratamiento. No se deben conservar los datos de forma indefinida, en previsión de que puedan ser necesarios en el futuro.

Los datos pueden conservarse indefinidamente con finalidad de archivo en interés público, con finalidad de investigación científica o histórica, o con finalidad estadística. En estos casos, hay que garantizar que se implantan las medidas técnicas y organizativas necesarias para garantizar el principio de minimización. Técnicas 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 las que sean inexactas 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 y 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 debe determinar sus efectos negativos potenciales.

- Pérdida de tiempo.
- Enfado.
- Aumento de los costes.
- Falta de comprensión.
- Estrés.
- Imposibilidad de acceder a servicios u otras oportunidades.
- Discriminación.
- Robo de la 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.

A la hora de determinar los efectos que un tratamiento puede tener sobre las personas, conviene tener en cuenta algunas características del tratamiento, como:

- El tipo de datos personales. El tratamiento de categorías especiales de datos, 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, hay que remarcar 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 más grande 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 las personas interesadas. Si las personas interesadas forman parte de un grupo con necesidades especiales (por ejemplo, menores o autoridades públicas), es necesario 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 les personas interesadas a la hora 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 les personas interesadas: los potenciales efectos negativos, el nivel de impacto, las amenazas y las probabilidades de que estas amenazas se materialicen.

4.6.1 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	Las personas interesadas pueden sufrir algunas molestias menores, que pueden superar sin problemas (por ejemplo, pérdida de tiempo, enfado, etc.)
Medio	Las personas interesadas 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	Las personas interesadas pueden sufrir consecuencias importantes, que pueden superar con dificultades importantes (por ejemplo, discriminación, robo de la identidad, pérdidas económicas, daños psicológicos, daños para la reputación, daños físicos, empeoramiento de la salud, pérdida del trabajo etc.)
Muy alto	Las personas interesadas 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 cuidadoso del nivel de impacto recae sobre el responsable del tratamiento.

4.6.2 Amenazas y probabilidad

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

Consideramos tres niveles de probabilidad:

- Baja. Es improbable que el impacto se materialice.
- Media. Es posible que el impacto se materialice.
- Alta. 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 se materializa, la estimación puede ser poco cuidadosa. 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.

4.6.3 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 manera cualitativa, la estimación del riesgo también será cualitativa.

A la hora de calcular el nivel de riesgo es fundamental tomar el punto de vista de las personas interesadas. 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; el responsable podría decidir asumir el coste asociado a este suceso. Ahora bien, el punto de vista de las personas afectadas acostumbra a 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 rehacerse de estos impactos podría ser muy difícil, o incluso imposible. Además, aunque pueda haber personas dispuestas a aceptar un impacto de gravedad muy alta, 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.

	Impacto			
Probabilidad	Bajo	Medio	Alto	Muy alto
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

4.6.4 Reducción de los riesgos

A menos 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 hay que consultar 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 de compartición de 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. Ahora bien, en el caso del riesgo asociado al tratamiento tal como está diseñado, las medidas para reducirlo son, básicamente, modificaciones del diseño del tratamiento. Modificar su diseño de forma separada a la descripción del tratamiento hecha en la sección anterior haría que la descripción inicial no fuera esmerada. Eso no es conveniente y, por tanto, hay que adaptar las secciones anteriores de la EIPD a los cambios realizados en el tratamiento y volver a calcular el riesgo. Eso fa que hacer una EIPD no sea uno 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 uno sentido amplio de la palabra, cualquier proceso de selección discrimina. Ahora bien, queremos que esta discriminación esté justificada por la capacitación de las personas y no por motivos espurios.

Puede ser 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 y candidatas 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 de las candidaturas. Por lo tanto, una medida para reducir el riesgo sería privar a las personas evaluadoras 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 alcanza su finalidad. Por lo tanto, justificar la eficacia del tratamiento es un primer paso esencial para justificar su necesidad.

Para justificar que un tratamiento es necesario, hay que mostrar que no hay otro tratamiento que sea, a la vez, efectivo y menos lesivo para los derechos y las libertades de las personas.

Para justificar que un tratamiento es proporcional, hay que 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 riesgo realizado en la sección anterior.

4.8 Opinión de las personas interesadas

El responsable del tratamiento debe buscar la opinión de les personas interesadas sobre la operación de tratamiento. La necesidad y la proporcionalidad del tratamiento es un punto especialmente interesante para buscar la opinión de las personas interesadas. Si no se considera apropiado buscarla, hay que documentar el porqué. Por ejemplo, por qué tiene un coste desproporcionado o por qué 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 que 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 las personas interesadas la posibilidad de conocer el tratamiento y de intervenir. La transparencia y el derecho a la información son necesarios para que las personas interesadas sean conscientes de cómo se tratan sus datos. Los derechos de acceso, rectificación y supresión permiten que las personas interesadas controlen sus datos. Los derechos de limitación y oposición dan a las personas interesadas 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 a la hora de informar a las personas interesadas.

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

También exige que las solicitudes de las personas interesadas se tramiten en un tiempo razonable. En particular, el reglamento establece un periodo de un mes, que puede ampliarse (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 una persona interesada, 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 una persona interesada, y en el caso de que el responsable tenga dudas respecto de la identidad de la persona solicitante, la persona representante puede solicitar la información necesaria para confirmar la identidad.

5.2 Derecho de información

El derecho de información establece que las personas interesadas tienen derecho a estar informadas de la recogida y posterior tratamiento que se hace de sus datos. Este es un derecho esencial porque, sin esta información, el resto de derechos no se pueden hacer efectivos.

El derecho de información establece que el responsable debe dar la siguiente información a las personas interesadas:

- La identidad y los datos de contacto del responsable.
- Los datos de contacto del delegado de protección de datos (si existe).
- La finalidad del tratamiento.
- La base legal del tratamiento.
- El interés legítimo del responsable, si esta es la base legal del tratamiento.
- Las personas destinatarias o categorías de destinatarios de los datos.
- El plazo de conservación de los datos o el criterio utilizado 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 las personas interesadas 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 ha recogido directamente de la persona interesada, hay que informar de la procedencia.

Cuando los datos se recogen directamente de las personas interesadas, se dará la información anterior en el mismo momento de recogida. Cuando los datos no se recogen directamente de las personas interesadas, hay que informar:

- En un período razonable de tiempo y superior a un mes.
- Si nos comunicamos con las personas interesadas, 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 de la persona interesada, no existe la obligación de informarla si ya dispone de la información.
- Si los datos no se han obtenido directamente de la persona interesada, no hay que informarle a si se da alguna de las siguientes condiciones1: la persona interesada 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 miembros o la información tiene carácter confidencial sobre la base del secreto profesional.

Ahora bien, en caso de que no se informe, hay que justificarlo.

5.3 Derecho de acceso

La persona interesada 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 tratadas.
- Las personas destinatarias 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 de la persona interesada, el origen de los datos.
- La existencia de decisiones automatizadas, en su caso.
- Garantías en la transferencia de datos fuera de la UE, si procede.

Aparte de conocer qué información se debe transmitir a les personas interesadas, 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 o trabajadora, 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 las personas interesadas tiene los conocimientos suficientes para identificar las solicitudes.

¿Es necesario 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 a las personas interesadas. Ahora bien, las solicitudes son igualmente válidas aunque no utilicen este procedimiento.

La transparencia es de aplicación 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 deben tramitarse en un plazo de un mes.

[7] RGPD, article 14.5.

- Si la complejidad o el número de solicitudes lo requiere, este plazo se puede ampliar en dos meses. Ahora bien, hay que informar a las personas interesadas antes de que finalice el primer mes.
- Si hay duda sobre la identidad de la persona que hace la solicitud, se puede solicitar la información necesaria para confirmar su identidad.
- La solicitud debe ser gratuita. El responsable únicamente puede cobrarlas (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. Ahora bien, a la hora 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 dar los pasos necesarios para comprobar si la información es cuidadosa y, si procede, rectificarla.

Mientras se está comprobando si los datos son exactos, la persona interesada puede pedir que se limite el tratamiento[7].

Por la transparencia, si el resultado de la comprobación es que la información ya es exacta y, por lo tanto, no hay que rectificarla, se debe informar a la persona interesada. 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, debe tomar las medidas adecuadas (teniendo en cuenta los costes y la tecnología disponible) para informar a las personas destinatarias 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 por la que se recogieron.
- La persona interesada retira su consentimiento y no hay ninguna otra base legal para el tratamiento.

[7] RGPD, articulo 18

- La persona interesada se opone al tratamiento y no hay otro factor superior que la legitime.
- Los datos se han tratado sin una base legal.
- Los datos deben borrarse de acuerdo con una obligación legal que afecta al responsable.
- Los datos se utilizan para ofrecer servicios de la sociedad de la información a menores.

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 las personas destinatarias sobre la petición.

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

- Para ejercer el derecho a la libertad de expresión y de información.
- Para cumplir una obligación legal o en el interés público.
- Con la finalidad 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 sus datos, en los siguientes casos:

- La persona interesada ha pedido la rectificación de sus datos y el responsable está verificando si son exactos.
- Los datos se han tratado sin una base legal.
- La persona interesada necesita que el responsable guarde los datos para iniciar, ejercer o defender una reclamación.
- La persona interesada se ha opuesto al tratamiento y el responsable está evaluando si los motivos legítimos del responsable prevalecen sobre los de La persona interesada.

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, a la hora 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 las personas destinatarias sobre la petición.

5.7 Derecho a la portabilidad de datos

Según el artículo 20, las personas tienen el derecho a solicitar 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 medios automatizados.

El derecho a la portabilidad de datos no se limita a les datos que les 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 búsquedas que una persona ha hecho en un buscador o la información de localización recogida de un GPS.

Los datos deben transmitirse 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 todas las personas interesadas.

5.8 Derecho de oposición

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

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

En este caso, el responsable cesará el tratamiento, salvo que acredite motivos legítimos que prevalezcan sobre los derechos de la persona interesada.

El Reglamento habla de las tres situaciones siguientes:

- Oposición al tratamiento con fines de marketing. En este caso, el responsable debe atisbar el tratamiento sin excepción.

- Oposición al tratamiento con finalidad 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 el derecho a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado (incluida la elaboración de perfiles), si tienen efectos jurídicos o tienen un efecto significativo, salvo que:

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

La persona interesada siempre tendrá derecho a obtener intervención humana, 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 de la persona interesada, o si el tratamiento se hace para proteger los intereses vitales de la persona interesada 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 la sección 4.6 se han evaluado los riesgos asociados al tratamiento, tal y 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 realizado con anterioridad, evaluaremos cuál 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)[8]:

- 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 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 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, algunas tienen un amplio reconocimiento, como: ISO 27005:2013, OCTAVE, NIST SP 800-30 y Magerit. Ahora bien, hacer un análisis de riesgos empleando 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.), especificar la relación de dependencia que existe entre ellos y evaluarlos.
2. Identificar las amenazas relevantes para nuestro sistema y caracterizarlas según la probabilidad de que se materialicen y la degradación que causan.
3. Identificar los controles a desarrollar 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[9]. Si una organización tiene la capacidad suficiente para abordar alguna de las metodologías de análisis de riesgos mencionadas anteriormente, conviene que lo haga, pero sin perder de vista que el objetivo es evaluar el riesgo sobre las personas (no sobre la organización).

[8] RGPD, articulo 32.1.

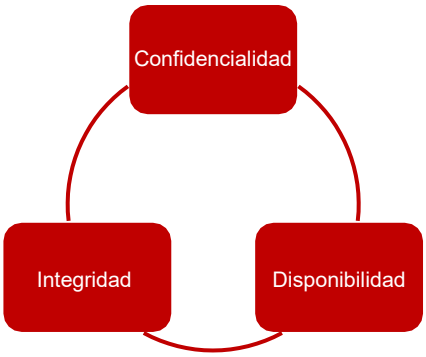
[9] Basado en la guía "*Guidelines for SMEs on the security of personal data processing*", ENISA.

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 de 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 ha de 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, de la integridad o de la disponibilidad de los datos. Cabe remarcar que mientras que normalmente se mide el impacto sobre la organización, aquí mediremos el impacto sobre las personas.

A la hora 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 las personas usuarias.
- Robo de información de las instalaciones del responsable o del encargado 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 o empleada modifica por error los datos de un cliente o clienta.
- Un error en la red de comunicaciones altera los datos mientras están en tráfico.
- Por motivos operacionales, una empresa mantiene varias copias de los datos, pero un cambio en alguna de las copias no se propaga a las demás.
- 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 fichero es corrompe o se borra y no hay una copia de seguridad.
- Se pierde un expediente del que sólo 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 a 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 siguientes situaciones incrementan el riesgo:

- El tratamiento datos de categorías especiales u otros datos especialmente sensibles (información financiera, localizaciones, 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 requeriría 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

¿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. Pudiendo ser la información capturada o modificada maliciosamente mientras está en tráfico. Eso se produce, por ejemplo, cuando se han contratado servicios en la nube, teletrabajando se realizan conexiones a los sistemas de la organización, o se permiten accesos a través de internet a la red interna para conectarse a bases de datos corporativas, entre otros motivos.

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

La interacción con las personas interesadas a través de internet expone el sistema de tratamiento a amenazas externas, 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 el personal acceda al sistema de tratamiento a través de internet también incrementa la exposición a ataques externos y, además, incrementa la posibilidad de que el personal haga un mal uso de la información (accidental o intencionado).

Algunos ejemplos de este tipo de tratamiento pueden ser los tratamientos que hacen uso del correo electrónico, aquellos en que el mantenimiento o la supervisión se hace a través de internet o bien el uso de servicios en la nube como son Google Drive, Microsoft OneDrive, Amazon Web Services, Microsoft Azure, entre otros.

¿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. Para garantizar un buen diseño y una buena configuración del sistema de tratamiento hay multitud de guías de buenas prácticas en seguridad con diferentes temáticas como pueden ser para diseño de una red local, cortafuegos, segmentación de la red, redes privadas virtuales (VPN), configuración del sistema operativo, antivirus, uso de contraseñas seguras, factores múltiples de autenticación (MFA), etc.

Disponer de un documento de buenas prácticas ayuda a dimensionar el sistema de tratamiento de datos teniendo en cuenta las necesidades computacionales, de comunicación, de seguridad y de almacenamiento. También permite configurar correctamente el software, aplicar una metodología de desarrollo que priorice la seguridad de los datos durante todo el ciclo de vida de la aplicación, utilizar aplicaciones seguras en la nube o establecer criterios sobre el uso y la tipología de datos que se pueden gestionar en este entorno, entre otras actuaciones.

Hardware y software

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

Disponer de un documento de buenas prácticas que recoja estos aspectos es esencial para garantizar el mantenimiento, monitorización y un plan de respuesta a incidentes del sistema adecuados. El mantenimiento debe realizarse tanto de los dispositivos y hardware como del software. La monitorización permite analizar un incidente una vez se ha producido y ayuda a detectar comportamientos sospechosos a fin de evitar que el incidente ocurra, o para reducir su impacto. El plan de respuesta a incidentes permite contar con un enfoque sistemático para abordar y gestionar los incidentes de seguridad.

Este documento de buenas prácticas puede recoger importantes tareas como la aplicación de actualizaciones de seguridad del sistema operativo, la realización de copias de seguridad regulares, el uso de sistemas automáticos de detección o correlación de eventos de seguridad, así como la realización periódica de auditorías para la revisión de vulnerabilidades y la seguridad general, entre otros.

¿Existe una falta de seguridad física en las instalaciones donde tiene lugar el tratamiento?

La seguridad física de las instalaciones de tratamiento es esencial. Sin embargo, no se puede garantizar la seguridad del sistema de tratamiento (ya sea electrónico o no). Esto puede darse, por ejemplo, cuando el CPD no está debidamente protegido con un sistema que impida el acceso a las personas no autorizadas o no está protegido contra accidentes naturales e industriales (fallos eléctricos, inundaciones, etc.), cuando el archivo se ha distribuido en diferentes áreas de forma que no se pueda garantizar de seguridad o cuando se realiza otros supuestos.

Uso del sistema de tratamiento

¿Existe una falta de claridad en la definición de los roles y las responsabilidades del personal?

Una falta de claridad en la definición de los roles y responsabilidades puede dar lugar a un uso descontrolado de los datos (ya sea accidental o intencionado). Por ejemplo, un trabajador sólo debería consultar los datos que le son necesarios para realizar sus tareas. También debe ser responsable de destruir la información cuando ya no sea necesaria, así como de garantizar su seguridad cuando se comunica a otra organización o persona, entre otras.

¿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 claramente definidos, se incrementa el riesgo de hacer un mal uso y de introducir vulnerabilidades en el sistema. Por ejemplo, la instalación de un software de compartición de archivos podría comportar la compartición involuntaria de información o acceder a páginas web maliciosas podría facilitar la entrada de software malicioso y de robo de datos, entre otros riesgos.

¿Puede el personal conectar dispositivos externos al sistema?

La conexión de dispositivos externos (teléfono móvil, memoria USB, etc.) al sistema de tratamiento puede representar un riesgo de seguridad, dado que puede facilitar la entrada de software malicioso, la introducción de vulnerabilidades y la extracción no autorizada de información. Por ello, es imprescindible establecer una política clara que regule el uso de dispositivos externos por parte del personal de la organización.

¿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 favorecer las malas prácticas del personal y dificultar la investigación de incidentes una vez se han producido, dada la falta de trazabilidad, tal y como establece el Esquema Nacional de Seguridad (ENS). Esto compromete la capacidad de detectar, analizar y responder a posibles amenazas. Por tanto, es necesario disponer de un registro adecuado que permita conocer quién accede a los sistemas de información y asegurar que las actividades registradas sean monitorizadas de manera efectiva.

Personas que intervienen en el tratamiento

¿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.

¿Se ha externalidad alguna parte del tratamiento a un encargado?

El encargado es la persona física o jurídica, autoridad pública, servicio u organismo que presta al responsable un servicio que comporta el tratamiento de datos personales por cuenta de éste. Por ejemplo, una empresa o entidad pública que ofrece un servicio de alojamiento de información en sus servidores o el gestor de un servicio público municipal, entre otros supuestos.

La externalización del tratamiento o parte del tratamiento a un encargado supone una pérdida de control sobre los datos. Es necesario escoger un encargado que ofrezca

garantías suficientes respecto de la implantación y el mantenimiento de las medidas de seguridad apropiadas, y definir claramente sus responsabilidades.

¿Existe una falta de conocimiento del personal respecto del uso adecuado del sistema, de aspecto 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. Así, por ejemplo, el personal podría ser más propenso a seguir las instrucciones de un correo de phishing o, a la hora de guardar documentos, no ser consciente de garantizar su seguridad, entre otras situaciones.

Otras características

¿Ha sufrido la empresa o otras empresas del sector ataques últimamente?

La existencia de ataques anteriores debe servir como lección para identificar vulnerabilidades y reforzar la seguridad, así como advertencia de potenciales ataques futuros.

¿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. De la misma manera, les advertencias respeto a potenciales fallos en la seguridad del sistema también pueden indicar una probabilidad más alta de sufrir ataques.

¿Se tratan datos de especial interés o datos de un número muy grande de personas usuarias?

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

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 tabla siguiente:

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

6.4 Riesgo inicial

Una vez estimado 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 usado en la sección 4.6.

	Impacto			
Probabilidad	Bajo	Medio	Alto	Muy alto
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

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) deben aplicarse. 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).

A la hora de determinar los controles de seguridad a aplicar, el ENS solo tiene en cuenta el impacto. Es decir, la necesidad y la intensidad con que hay que 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 su 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 debe determinarse 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 la que hace referencia 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	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15
[org.1]			x	x											
[org.2]						x	x								
[org.3]												x		x	
[org.4]					x	x	x	x		x	x				
[op.pl.2]			x	x											
[op.pl.3]			x												
[op.pl.4]			x												
[op.pl.5]			x												
[op.acc.1]					x					x					
[op.acc.2]					x					x					
[op.acc.3]						x				x					
[op.acc.4]					x					x					
[op.acc.5]		x			x					x			x		
[op.acc.6]					x				x				x		
[op.exp.1]					x	x									
[op.exp.2]				x											
[op.exp.3]				x		x				x				x	x
[op.exp.4]					x	x				x					
[op.exp.5]					x										
[op.exp.6]		x	x	x				x							
[op.exp.7]				x									x		
[op.exp.8]						x			x						
[op.exp.9]				x											
[op.exp.10]									x						
[op.ext.1]											x				
[op.ext.2]											x				
[op.ext.3]	x										x				
[op.ext.4]	x	x									x				
[op.nub.1]	x	x	x	x											
[op.cont.1]			x								x				
[op.cont.2]			x	x											
[op.cont.3]			x	x											
[op.cont.4]	x	x				x					x				x
[op.mon.1]	x	x		x	x				x				x		
[op.mon.2]			x											x	
[op.mon.3]				x									x		
[mp.if.1]					x				x						
[mp.if.2]					x				x						
[mp.if.3]					x										
[mp.if.4]					x										

Control	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15
[mp.if.5]					x										
[mp.if.6]					x										
[mp.if.7]					x				x						
[mp.per.1]						x	x					x			
[mp.per.2]						x						x			
[mp.per.3]												x			
[mp.per.4]												x			
[mp.eq.1]					x										
[mp.eq.2]				x											
[mp.eq.3]			x		x										
[mp.eq.4]	x	x					x	x				x			
[mp.com.1]	x	x													
[mp.com.2]	x	x													x
[mp.com.3]	x	x													x
[mp.com.4]				x									x		
[mp.si.1]					x										
[mp.si.2]					x										
[mp.si.3]					x										
[mp.si.4]					x										
[mp.si.5]					x										
[mp.sw.1]			x												
[mp.sw.2]			x												
[mp.info.2]						x				x					
[mp.info.3]			x												
[mp.info.4]									x						
[mp.info.5]						x				x					
[mp.info.6]				x	x										
[mp.s.1]		x				x									
[mp.s.2]	x	x													
[mp.s.3]	x	x													
[mp.s.4]	x	x												x	

Estos criterios constituyen unas guías para ayudar a determinar los controles necesarios. Ahora bien, a la hora de calcular el riesgo residual, hay que justificar el efecto que tienen estos controles sobre el impacto y sobre la probabilidad.

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

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

6.5.2 Normativa de seguridad [org.2] (sistema)

Nivel: bajo, medio, alto

Hay que 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 violación de estas normas (derechos, deberes y medidas disciplinarias).

6.5.3 Procedimientos de seguridad [org.3] (sistema)

Nivel: bajo, medio, alto

Hay que disponer de una serie de documentos que describan:

- Cómo desarrollar las tareas habituales.
- Quién debe hacer cada tarea.
- Cómo identificar comportamientos anómalos e informar de ello.
- Cómo tratar la información en función del nivel de seguridad.

6.5.4 Proceso de autorización [org.4] (sistema)

Nivel: 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.
- Utilización de servicios de terceros.

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

Nivel: bajo, medio, alto

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

- Documentación de las instalaciones (áreas 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.

Nivel: medio, alto

- Sistema de gestión, relativo a planificación, organización y control.

Nivel: alto

- Sistema de gestión de la seguridad con mejora continua.
- Controles técnicos internos, incluyendo la validación de datos de entrada, salida y datos intermedios.

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

Nivel: bajo, medio, alto

Es necesario 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.

6.5.7 Dimensionamiento [op.pl.4] (D)

Nivel: bajo, 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.

Nivel: medio, alto

- Mejora continua de la gestión de la capacidad.

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

Nivel: medio, alto

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

6.5.9 Identificación [op.acc.1] (sistema[10])

Nivel: bajo, medio, alto

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

Nivel: medio, alto

- Lista actualizada de usuarios y privilegios.

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

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

Nivel: bajo, medio, alto

- Sólo pueden utilizar los recursos del sistema las entidades que disponen de derechos de acceso suficientes.
- Los derechos de acceso deben establecerse 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 a los ficheros configuración.

Nivel: alto

- Los privilegios de acceso deben poder ser mantenidos de forma individual.

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

Nivel: medio, alto

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

Nivel: alto

- Segregación rigurosa de personas y tareas.

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

Nivel: bajo, medio, alto

Los derechos de acceso de cada usuario deben asignarse de acuerdo con:

- Acceso prohibido sin autorización expresa.
- Mínimo privilegio.
- Necesidad de conocer.
- Únicamente el personal competente puede modificar los derechos de acceso, de acuerdo con los criterios establecidos por el responsable.
- Política específica de acceso remoto.

6.5.13 Mecanismo de autenticación para usuarios externos [op.acc.5] (ICAT)

Nivel: bajo, medio, alto

Requisitos para el personal que tiene acceso a la información:

- Identificación fidedigna de los usuarios.
- El usuario debe conocer y aceptar sus obligaciones (custodia diligente e información inmediata en caso de pérdida).
- Las contraseñas de acceso deben de estar para el control exclusivo del usuario.
- Los autenticadores se han de renovar periódicamente, de acuerdo con la política de la organización.
- Los autenticadores se han de deshabilitar cuando la entidad (persona, equipo o proceso) acaba su relación con el sistema.
- La información previa a la autenticación debe de ser mínima.
- El número de intentos permitidos estará limitado.
- Se dará información al usuario de sus derechos y obligaciones inmediatamente después de acceder al sistema.

Y además uno de los siguientes requisitos:

- La contraseña como un mecanismo de autenticación, con una complejidad y robustez mínima.
- Contraseña de un solo uso (OTP) como complemente a la contraseña de autenticación.
- Acceso con certificado digital.
- Acceso con certificado digital en dispositivo físico.

Nivel: medio, alto

- Registro de accesos con éxito y fallidos y además se informará al usuario del último acceso realizado con su identificador.

6.5.14 Mecanismo de autenticación para usuarios internos [op.acc.6] (ICAT)

Nivel: bajo, medio, alto

Requisitos para el personal que tiene acceso a la información:

- Aceptación por parte del usuario de la política de seguridad.

- El usuario debe reconocer la recepción y aceptar las obligaciones (custodia diligente e información inmediata, en caso de pérdida).
- Las palabras de paso deben estar bajo el control exclusivo del usuario.
- Los autenticadores deben renovarse periódicamente, de acuerdo con la política de la organización.
- Los autenticadores deben deshabilitarse (con la posibilidad de regeneración) si hay sospecha de pérdida.
- Los autenticadores deben retirarse y deshabilitarse cuando la entidad (persona, equipo o proceso) termina su relación con el sistema.
- La información previa a la autenticación debe ser mínima.
- Número de intentos permitidos limitado.
- Información al usuario de sus derechos y obligaciones inmediatamente después de tener acceso.
- Y además uno de los siguientes requisitos:
    - Contraseña como mecanismo de autenticación, con complejidad y robustez mínima.
    - Contraseña desechable (OTP) como complemento a la contraseña de autenticación.
    - Acceso con certificado digital.
    - Acceso con certificado digital en dispositivo físico.
- Y además:
    - Doble factor de autenticación por acceso desde a través de zonas no controladas.
    - Acceso remoto (autorizado, cifrado, habilidad sólo cuando sea necesario y con registros de auditoría).

Nivel: medio, alto

- Registro de accesos con éxito y fallidos y se informará al usuario del último acceso realizado con su identificador.

Nivel: alto

- Limitación de la ventana de acceso.
- Suspensión por no utilización.

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

Nivel: bajo, medio, alto

- Se debe mantener un registro de los activos del sistema que describe su tipología e identifica al responsable.

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

Nivel: bajo, medio, alto

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

- Se borren cuentas y palabras de paso estándar.
- Se aplique la regla de la mínima funcionalidad.
- Se aplique la regla de seguridad por defecto.
- Máquinas virtuales configuradas en modo seguro, como si fueran máquinas físicas.

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

Nivel: bajo, medio, alto

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

- En todo momento se mantiene la regla de funcionalidad mínima.
- En todo momento se mantiene la regla de mínimo privilegio.
- El sistema se adapta a las nuevas necesidades.
- El sistema reacciona a las vulnerabilidades reportadas.
- El sistema reacciona a incidencias.
- Configuración de seguridad solamente editable por personal autorizado.

Nivel: medio, alto

- Mantenimiento periódico de la configuración (verificación periódica y lista de servicios).

Nivel: alto

- Responsabilidad de la configuración.
- Copias de seguridad.

6.5.18 Mantenimiento y actualizaciones de seguridad [op.exp.4] (sistema)

Nivel: bajo, medio, alto

- Hay que respetar las especificaciones de los fabricantes con respecto a la instalación y el mantenimiento de los sistemas.
- Hay que disponer de un sistema para analizar, priorizar y aplicar las actualizaciones de seguridad.
- Mantenimiento solo realizable por personal autorizado.

Nivel: medio, alto

- Pruebas de preproducción.

Nivel: alto

- Prevención de fallos.

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

Nivel: medio, alto

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

- Los cambios se planificarán para reducir el impacto sobre la prestación de los servicios afectados.
- La información a registrar para cada petición de cambio será suficiente para que quien deba autorizarlos no tenga dudas al respecto y permita gestionarlo hasta su desestimación o implementación.
- Las pruebas de preproducción, siempre que sea posible realizarlas, se efectuarán en equipos equivalentes a los de producción, al menos en los aspectos específicos del cambio.
- Mediante un análisis de riesgos se determinará si los cambios son relevantes para la seguridad del sistema. Aquellos cambios que impliquen un riesgo de nivel ALTO tendrán que ser aprobados, explícitamente, previamente a su implantación, por el Responsable de la Seguridad.

Nivel: alto

- Prevención de fallos.

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

Nivel: bajo, medio, alto

- Hay que disponer de mecanismos de prevención y reacción contra código malicioso.
- Es necesario instalar un Software de protección en todos los equipos, sitios de usuarios, servidores y elementos perimetrales.
- Hay que analizar los archivos de fuentes externas antes de trabajar.
- Es necesario mantener las bases de datos de detección de malware permanentemente actualizadas.
- En los sitios de usuario debe existir una configuración adecuada del software de detección de malware.

Nivel: medio, alto

- Escaneo periódico.
- Revisión preventiva del sistema.

Nivel: alto

- Solo aplicaciones autorizadas (lista blanca).
- Capacidad de respuesta en caso de incidente.

6.5.21 Gestión de incidencias [op.exp.7] (sistema)

Nivel: bajo, medio, alto

- Se dispondrá de un proceso integral para hacer frente a los incidentes de seguridad.
- La gestión de incidentes que afecten a datos personales tendrá en cuenta lo dispuesto en el Reglamento General de Protección de Datos.

Nivel: medio, alto

- Procedimiento de notificación.
- Detección y respuesta (implantación de medidas urgentes, asignación de recursos, comunicación del incidente, medidas para prevenir la repetición).

Nivel: alto

- Reconfiguración dinámica (cambios reglas routers, listas de control de acceso, ...).

6.5.22 Registro de la actividad de les persones usuarias [op.exp.8] (sistema[11])

Nivel: bajo, medio, alto

Hay que registrar todas las actividades de las personas usuarias del sistema, de manera que:

- Indique quién hace una actividad, cuándo la hace y sobre qué datos.
- Incluya la actividad de les persones usuarias, de operadores y administradores.
- En ella consten las actividades realizadas y los intentos fallidos.
- Se activen los registros de actividad en los servidores.

Nivel: medio, alto

- Revisión de los registros.
- Sincronización de los relojes del sistema.
- Retención de los registros.
- Control de acceso.

Nivel: alto

- Revisión automática y correlación de eventos.

6.5.23 Registro de la gestión de incidencias [op.exp.9] (sistema)

Nivel: bajo, medio, alto

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

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

[11] En el ENS la propiedad es T.

6.5.24 Protección de les claves criptográficas [op.exp.10] (sistema)

Nivel: bajo, medio, alto

- Las claves criptográficas deben protegerse durante todo su ciclo de vida: generación, transporte al punto de explotación, custodia durante la explotación, archivo y destrucción.
- Los medios de generación deben estar aislados de los de explotación.
- Las claves archivadas deben estar en soportes aislados de los de explotación.

Nivel: medio, alto

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

6.5.25 Contratación y acuerdos de nivel de servicios [op.ext.1] (sistema)

Nivel: medio, alto

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

6.5.26 Gestión diaria [op.ext.2] (sistema)

Nivel: medio, alto

Para la gestión diaria del sistema, es necesario:

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

6.5.27 Protección de la cadena de suministro [op.ext.3] (sistema)

Nivel: alto

- Análisis de impacto si hay incidente en la cadena de suministro.
- Estimación del riesgo sobre el sistema a causa del impacto en el punto anterior.
- Medidas de contención de los impactos estimados.

6.5.28 Interconexión de sistemas [op.ext.4] (sistema)

Nivel: medio, alto

- Intercambio de información y prestación de servicios con autorización previa.
- Para cada interconexión se documentará específicamente: características de la interfaz, requisitos de seguridad y protección de datos, y la naturaleza de la información intercambiada.

Nivel: alto

- Coordinación de actividades.

6.5.29 Protección de servicios en la nube [op.nub.1] (sistema)

Nivel: bajo, medio, alto

- Cumplimiento de las medidas establecidas en función del tipo de servicio por el CCN a los proveedores que den servicio al sector público.
- Los sistemas de información de servicios en la nube de terceros deberán cumplir el ENS:
  - Auditoría de test de intrusión
  - Transparencia
  - Cifrado y gestión de claves
  - Jurisdicción de los datos

Nivel: medio, alto

- Servicios certificados.

Nivel: alto

- Guía de configuración de seguridad específicos.

6.5.30 Análisis de impacto [op.cont.1] (D)

Nivel: medio, alto

Hay que hacer un análisis de lo siguiente:

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

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

Nivel: alto

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

- Se deben acreditar 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 recibirán formación específica.
- El plan de continuidad debe integrarse con otros planes de continuidad en materias ajenas a la seguridad.

6.5.32 Pruebas periódicas [op.cont.3] (D)

Nivel: alto

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

6.5.33 Medios alternativos [op.cont.4] (D)

Nivel: alto

- Disponibilidad de medios alternativos para poder seguir prestando servicios cuando los medios habituales no estén disponibles. Se cubrirán los siguientes elementos:
  - a) servicios contratados a terceros.
  - b) Instalaciones alternativas.
  - c) Personal alternativo.
  - d) Equipamiento informático alternativo.
  - e) Medios de comunicación alternativos.
- Tiempo máximo para que entren en funcionamiento los medios alternativos.
- Mismas garantías de seguridad que los medios habituales. Se deben acreditar funciones, responsabilidades y actividades a realizar.

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

Nivel: bajo, medio, alto

- Hay que disponer de herramientas de detección y prevención de intrusiones.

Nivel: medio, alto

- Detección basada en reglas.

Nivel: alto

- Procedimientos de respuesta.

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

Nivel: bajo, medio, 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.

Nivel: medio, alto

- Efectividad del sistema de gestión de incidentes.
- Eficiencia de las medidas de seguridad.

6.5.36 Vigilancia [op.mon.3] (sistema)

Nivel: bajo, medio, alto

- Se dispondrá de un sistema automático de recolección de eventos de seguridad.

Nivel: medio, alto

- Correlación de eventos (sistema automático)
- Soluciones de vigilancia que permitan determinar la superficie de exposición en relación con vulnerabilidades y deficiencias de configuración.

Nivel: alto

- Ciberamenazas avanzadas
- Observatorios digitales
- Minería de datos
- Inspecciones de seguridad

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

Nivel: bajo, medio, alto

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

6.5.38 Identificación de les personas [mp.if.2] (sistema)

Nivel: 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.

6.5.39 Acondicionamiento de los locales [mp.if.3] (sistema)

Nivel: bajo, medio, alto

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

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

6.5.40 Energía eléctrica [mp.if.4] (D)

Nivel: bajo, medio, alto

Los locales donde se ubiquen 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.

Nivel: medio, alto

- En caso de fallo del suministro general, hay que garantizar el suministro eléctrico de los sistemas, con el tiempo suficiente para hacer un apagón ordenado y salvaguardando la información.

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

Nivel: bajo, medio, alto

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

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

Nivel: medio, alto

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

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

Nivel: 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.

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

Nivel: medio, alto

- Hay que definir las responsabilidades relacionadas con la seguridad en cada puesto de trabajo.
- Hay que definir las condiciones que deben satisfacer las personas que ocupan cada puesto de trabajo (en particular, respecto de la confidencialidad).
- Se tendrán en cuenta las condiciones anteriores en la selección del personal, incluida la verificación de su vida laboral, formación y otros datos.

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

Nivel: bajo, medio, alto

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

- Las medidas disciplinarias.
- Las obligaciones tanto el período de desarrollo del trabajo como en el caso de finalización o traslado.
- El deber de confidencialidad respecto de los datos a que tiene acceso. Para el personal contratado a través de un tercer, es necesario establecer:
- Los deberes y las obligaciones del personal.
- Los deberes y las obligaciones de cada parte.
- El procedimiento para resolver incidentes relacionados con el incumplimiento de las obligaciones.

Nivel: medio, alto

- Confirmación expresa.

6.5.46 Concienciación [mp.per.3] (sistema)

Nivel: bajo, medio, alto

Hay que hacer las acciones necesarias para concienciar regularmente al personal respecto 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 a reportar.
- El procedimiento para informar de incidencias de seguridad.

6.5.47 Formación [mp.per.4] (sistema)

Nivel: bajo, medio, alto

Se formará 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: almacenaje, transferencia, copia, distribución y destrucción.

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

Nivel: bajo, medio, alto

Se debe exigir 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.

Nivel: medio, alto

El material se debe guardar en un lugar cerrado.

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

Nivel: medio, alto

El puesto de trabajo debe bloquearse al cabo de un tiempo de inactividad y hay que requerir la autenticación de la persona usuaria para continuar la actividad.

Nivel: alto

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

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

Nivel: bajo, medio, alto

Los equipos que abandonan las instalaciones deben protegerse adecuadamente:

- Hay que hacer un inventario de los equipos portátiles, con la identificación de la persona responsable y control regular de que los equipos están bajo su control.
- Hay que establecer un canal para informar de pérdidas o sustracciones.
- 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.

Nivel: alto

- La información de nivel alto que tiene almacenada debe cifrarse.
- Entornos protegidos.

6.5.51 Otros dispositivos conectados a la red [mp.eq.4] (C)

Nivel: bajo, medio, alto

- Los dispositivos conectados a la red deben tener configuración de seguridad adecuada.
- Si disponen de almacenamiento incluirán la funcionalidad para eliminar información. Es necesario 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.
- Es necesario establecer un tiempo máximo para que los equipos alternativos entren en funcionamiento.

Nivel: medio, alto

- Se utilizarán productos certificados.

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

Nivel: bajo, medio, alto

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

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

Nivel: bajo, medio, alto

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

Nivel: medio, alto

- Hay que utilizar algoritmos acreditados por el CCN.

Nivel: alto

- Hay que utilizar dispositivos de hardware para establecer y utilizar la VPN.
- Hay que utilizar productos certificados.

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

Nivel: 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 detecten. Se consideran ataques activos: la alteración de la información en tráfico, la introducción de información espuria y el secuestro de la sesión por una tercera parte.

Nivel: 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.

Nivel: alto

- Se debe valorar positivamente el uso de dispositivos de hardware a la hora de establecer la VPN.
- Hay que utilizar productos certificados.

6.5.55 Segregación de flujos de información [mp.com.4] (sistema)

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

Nivel: medio, alto

- El tráfico de la red se segregará para que cada equipo sólo tenga acceso a la información que necesita.

- Si se utilizan comunicaciones inalámbricas será en un segmento separado.
- La red debe segmentarse, al menos de una de las siguientes formas:
  - Segmentación lógica básica.
  - Segmentación lógica avanzada.
  - Segmentación física.

Nivel: alto

- No se acepta la segmentación lógica básica.
- Puntos de interconexión particularmente asegurados.

6.5.57 Etiquetado [mp.si.1] (C)

Nivel: medio, alto

- Los soportes de información deben etiquetarse de manera que, sin revelar su contenido, se indique el nivel de seguridad de la información contenida.

6.5.58 Criptografía [mp.si.2] (IC)

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

Nivel: medio, alto

- Hay que aplicar mecanismos criptográficos que garanticen la integridad y la confidencialidad de la información contenida.
- Hay que utilizar algoritmos acreditados por el CCN.

Nivel: alto

- Hay que utilizar, productos certificados.
- Copias de seguridad.

6.5.59 Custodia [mp.si.3] (sistema)

Nivel: 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 aplicar la diligencia y el control adecuados para el soporte 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.

6.5.60 Transporte [mp.si.4] (sistema)

Nivel: bajo, medio, alto

La persona responsable de sistemas debe garantizar que, mientras se desplazan, los dispositivos están bajo control y que se cumplen los requisitos de seguridad. Es necesario:

- Disponer de un registro de salida que identifique a la persona transportista que recibe el apoyo.
- Disponer de un registro de entrada que identifique a la persona 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].

6.5.61 Borrado y destrucción [mp.si.5] (C)

Nivel: medio, alto

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

- Los apoyos a 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.

Nivel: medio, alto

- Productos certificados.

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

Nivel: medio, alto

- El desarrollo de acopios debe hacerse sobre un sistema diferente y separado del de producción. No debe haber herramientas o datos de desarrollo en torno a producción.
- Mínimo privilegio.
- 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 siguientes elementos 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 deben realizarse con datos reales, salvo que se asegure el nivel de seguridad correspondiente.

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

Nivel: 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.

Nivel: medio, alto

Antes de la puesta en funcionamiento, hay que hacer las inspecciones siguientes:

- Las pruebas deben realizarse en un entorno aislado (preproducción).

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

Nivel: bajo, medio, alto

- Para calificar la información, hay que tener en cuenta su naturaleza.
- La política de seguridad debe establecer la persona responsable de cada información.
- La política de seguridad debe contener los criterios que determinan el nivel de seguridad requerido.
- Con los criterios anteriores, la persona 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.

6.5.65 Firma electrónica [mp.info.3] (IA)

La firma electrónica garantiza la autenticidad de la persona firmante y la integridad del contenido.

También es un mecanismo de prevención del repudio.

Nivel: bajo, medio, alto

- Se puede utilizar cualquier medio de firma electrónica.

Nivel: medio, alto

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

- Cuando se empleen sistemas de firma electrónica avanzada basados en certificados, estos serán cualificados.
- Se utilizarán algoritmos acreditados por el CCN.

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 verificación 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.

Nivel: alto

- Se usará firma electrónica avanzada basada en certificados cualificados complementada por un segundo factor del tipo “algo que se sabe” o “algo que se es”

6.5.66 Sellos temporales [mp.info.4] (T)

Nivel: alto

Los sellos temporales evitan la posibilidad de repudio posterior:

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

6.5.67 Limpieza de documentos [mp.info.5] (C)

Nivel: 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 si esta información es pertinente a la persona receptora.

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

6.5.68 Copias de seguridad [mp.info.6] (D)

Nivel: bajo, medio, alto

- Se deben realizar copias de seguridad que permitan recuperar datos perdidos accidental o intencionadamente.
- Los procedimientos de las copias deben contener:
    - Frecuencia de copia, requisitos de almacenamiento en el mismo sitio, requisito de almacenamiento en otro sitio, control de acceso autorizado. Las copias deben tener la misma seguridad que los datos iniciales. En particular, debe considerarse la necesidad de que estén cifradas.

Nivel: medio, alto

- Pruebas de recuperación.

Nivel: alto

- Protección de las copias de seguridad.

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

Nivel: bajo, medio, alto

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

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

Nivel: 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, es necesario:

- Evitar que el servidor ofrezca acceso a los documentos por vías alternativas.
- Prevenir ataques de manipulación de galletas.
- Prevenir ataques de inyección de código.
- Prevenir los intentos de escalada de privilegios.
- Prevenir los ataques de XSS.
- Y uno de los siguientes refuerzos:
    - Auditoría de seguridad.
    - Auditoría de seguridad avanzada.

Nivel: alto

- Auditoría de seguridad avanzada
- Protección de las cachés.

6.5.71 Protección de la navegación web [mp.s.3] (sistema)

Nivel: bajo, medio, alto

El acceso de los usuarios internos a la navegación por internet debe protegerse contra las amenazas que le son propias. En particular, es necesario:

- Normativa de utilización.
- Concienciación sobre higiene de navegación web.
- Formación al personal encargado de la monitorización.
- Protección de la información de resolución de direcciones web.
- Protección frente a problemas que se materializan vía web.
- Protección contra software malicioso.
- Establecimiento de política de control de cookies.

Nivel: alto

- Monitorización.

6.5.72 Protección contra la denegación de servicio [mp.s.4] (D) (impacto, probabilidad)

Nivel: medio, alto

Se deben 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.

Nivel: alto

- Hay que establecer un sistema de detección de los ataques de denegación de servicio.
- Hay que establecer procedimientos de reacción a los ataques, incluida la comunicación con el proveedor de comunicaciones.

6.6 Cálculo del riesgo residual

Una vez establecidos los controles de seguridad, se determinarán cómo afectan al riesgo. En general, los controles de seguridad se clasifican según el objetivo que tienen: preventivo, detective, 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 debe 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 residual y la probabilidad residual, 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 hay que consultar a la autoridad de protección de datos competente sobre su idoneidad.