UNIVERSIDAD DE EXTREMADURA

Escuela Politécnica

Máster Universitario en Dirección TIC

Trabajo Fin de Máster

El nuevo Reglamento General de Protección de Datos: un enfoque práctico

Begoña Ordiales Rosado

Julio, 2019

UNIVERSIDAD DE EXTREMADURA

Escuela Politécnica

Máster Universitario en Dirección TIC

Trabajo Fin de Máster

El nuevo Reglamento General de Protección de Datos: un enfoque práctico

Autora: Begoña Ordiales Rosado

Tutor: Andrés Caro Lindo

Tribunal calificador

Presidente: Pablo García Rodríguez

Secretaria: Mar Ávila Vegas

Vocal: Francisco Javier Rodríguez Pérez

Índice de contenidos

RESUMEN 9
PALABRAS CLAVE 9
ABSTRACT 10
KEYWORDS 10
1 INTRODUCCIÓN 11
2 OBJETIVOS 14
3 ESTADO DEL ARTE 15
4 GUÍA DE REFERENCIA E IMPLEMENTACIÓN 18
4.1 DEFINICIONES 22
4.2 ÁMBITO DE APLICACIÓN 26
4.3 DATOS DE CARÁCTER PERSONAL 29
4.4 PRINCIPIOS DE PROTECCIÓN DE DATOS 33
4.5 DERECHOS DE LAS PERSONAS 35
4.6 RESPONSABLE DEL TRATAMIENTO 50
4.7 ENCARGADO DEL TRATAMIENTO 54
4.8 DELEGADO DE PROTECCIÓN DE DATOS 55
4.9 TRANSFERENCIAS INTERNACIONALES DE DATOS 60
4.10 REGISTRO DE ACTIVIDADES DE TRATAMIENTO 62
4.11 PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO 65
4.12 ANÁLISIS DE RIESGOS 66
4.13 EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS 82
4.14 MEDIDAS DE SEGURIDAD 92
4.15 GESTIÓN Y NOTIFICACIÓN DE VIOLACIONES DE SEGURIDAD 97
4.16 RÉGIMEN SANCIONADOR 108
5 DISCUSIÓN 114
6 CONCLUSIONES 115
REFERENCIAS BIBLIOGRÁFICAS 116
ANEXO HERRAMIENTAS PARA LA IMPLEMENTACIÓN DE LAS MEDIDAS DE SEGURIDAD 119

Índice de tablas

Tabla 1 Clasificación de la amenazas *66*

Tabla 2 Medidas y tareas durante el Proceso de respuesta a violaciones de seguridad..... *106*

Índice de figuras

Figura 1 Esquema relación LOPDGDD - RGPD *13*
Figura 2 Empresas de Extremadura por número de asalariados (Fuente: Instituto Nacional de Estadística) *14*
Figura 3 Evolución de la legislación de la UE en materia de protección de datos *17*
Figura 4 Categorías de datos de carácter personal *31*
Figura 5 Principio de transparencia en el tratamiento de datos personales *39*
Figura 6 Información básica cuando los datos son obtenidos del interesado *40*
Figura 7 Información adicional cuando los datos son obtenidos del interesado *41*
Figura 8 Información adicional cuando los datos no son obtenidos del interesado *43*
Figura 9 Derechos de las personas *50*
Figura 10 De los niveles de seguridad al principio de responsabilidad proactiva *51*
Figura 11 Obligaciones de las figuras del tratamiento *60*
Figura 12 Supuestos transferencias internacionales de datos personales *61*
Figura 13 Registro de Actividades de Tratamiento para el responsable *64*
Figura 14 Registro de Actividades de Tratamiento del encargado *65*
Figura 15 Flujo de trabajo para el análisis de riesgos (Fuente: Guía Práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD de la AEPD) *67*
Figura 16 Ciclo de vida de los datos personales *72*
Figura 17 La tecnología en el ciclo de vida de las actividades de tratamiento *73*
Figura 18 Metodología para realización EIPD (Fuente: AEPD - Guía práctica para las EIPD sujetas al RGPD) *83*
Figura 19 Resumen medidas seguridad LOPD *94*
Figura 20 Proceso de gestión de incidentes (Fuente: Guía para la gestión y notificación de brechas de seguridad de la AEPD) *100*
Figura 21 Fuentes detección físicas de violaciones de seguridad *101*
Figura 22 Fuentes de detección de violaciones de ciberseguridad *101*
Figura 23 Fases del Proceso de respuesta a violaciones de seguridad *106*

RESUMEN

Este trabajo de fin de máster, “El nuevo Reglamento General de Protección de Datos: un enfoque práctico”, pretende ser una guía de referencia para la implantación de la protección de datos personales en una PYME.

Se trata de un trabajo de revisión teórica, en el que se ha tratado de recopilar la información publicada hasta el momento sobre la nueva legislación de protección de datos aplicable en la Unión Europea, dándole un enfoque práctico para que sea de utilidad a cualquier PYME.

El trabajo se sustenta en el Reglamento General de Protección de Datos – RGPD (Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos) y en la Ley orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales - LOPDGDD, relacionando los aspectos más relevantes de la normativa con actividades de tratamiento de datos personales habituales en una PYME como pueden ser la contratación de personal y la confección y pago de nóminas.

La estructura seguida en el trabajo es la marcada por la legislación española, de forma que cada apartado se corresponde con un título de la Ley de Protección de Datos Personales (LOPDGDD) en el que se desarrolla el título con referencias a ejemplos e información que ayudan a entender mejor su significado, seguido, cuando sea procedente, de la implantación en el ejemplo de referencia.

PALABRAS CLAVE

Protección de datos, Reglamento General de Protección de Datos, RGPD, Ley española de protección de datos

ABSTRACT

This paper, "The new General Data Protection Regulation: a practical approach" aims to be a reference guide for the implementation of personal data protection in an SME.

This is a theoretical review work, in which it has tried to collect the published information on the new data protection legislation applicable in the European Union, giving it a practical approach to be useful to any SME.

The work is based on the General Data Protection Regulation - GDRP (Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data) and Organic Law 3/2018 of December 5 on the Protection of Personal Data and the Guarantee of Digital Rights, relating the most relevant aspects of the regulation with personal data processing activities common in an SME such as hiring staff and the preparation and payment of payroll.

The structure of this work is marked by Spanish legislation, so that each section corresponds to a title of the Personal Data Protection Act in which the title is developed with references to examples and information that help to better understand its meaning, followed, where appropriate, by the implementation in the reference example.

KEYWORDS

Protection personal data, General Data Protection Regulation, GDRP, Spanish organic law protection personal data

1 INTRODUCCIÓN

A diario facilitamos nuestros datos personales en infinidad de ocasiones, tanto en el mundo real como en el virtual: al registrarnos en una aplicación, al acudir a un centro de salud, en el banco, al hacer una reserva en un hotel, al realizar una compra online…Con la rápida evolución de la tecnología difundimos cada vez mayor información personal y a cualquier parte del mundo. Todo esto hace que las empresas y autoridades públicas utilicen gran cantidad de datos personales en el desarrollo de sus actividades.

Aunque cada vez somos (o intentamos ser) más precavidos en la información que facilitamos, a quién se la facilitamos y para qué la facilitamos todavía, en muchas ocasiones, desconocemos qué se hace realmente con estos datos y empezamos a recibir llamadas y correos electrónicos de empresas sin saber cómo han conseguido nuestros datos.

El objetivo general que persigue el Reglamento de Protección de Datos es garantizar un nivel equivalente de protección de los derechos y libertades de las personas físicas en todo el Espacio Económico Europeo, que permita la libre circulación de datos personales en la Unión Europea.

El RGPD refuerza los derechos de los interesados, dándoles el control total sobre sus datos personales, y obliga a los responsables del tratamiento a ser totalmente transparentes con el uso que hacen de los mismos, además de tener que garantizar la seguridad antes, durante y después del tratamiento.

En la actualidad, el tratamiento de la información en general, y de los datos personales en particular, se apoya en las tecnologías a lo largo de todo su ciclo de vida desde la recogida o captura de datos hasta la destrucción de los mismos pasando por el almacenamiento, el uso o tratamiento y la cesión o transferencia. Por este motivo, los profesionales de las tecnologías de la información y la comunicación desempeñamos un papel de gran importancia en la protección de datos personales.

La elaboración de este proyecto se fundamenta en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016,

relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos (Reglamento General de protección de datos – RGPD) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) la cual adapta el ordenamiento jurídico español al RGPD.

Este proyecto desarrolla los aspectos más relevantes de la LOPDGDD en la implantación de la protección de datos de una PYME, ampliándola y ofreciendo ejemplos con información obtenida de otras fuentes como son la Agencia Española de Protección de Datos (www.aepd.es) y el Comité Europeo de Protección de Datos (https://ec.europa.eu).

En el siguiente gráfico se relacionan los diferentes títulos de la LOPDGDD con los capítulos del RGPD.

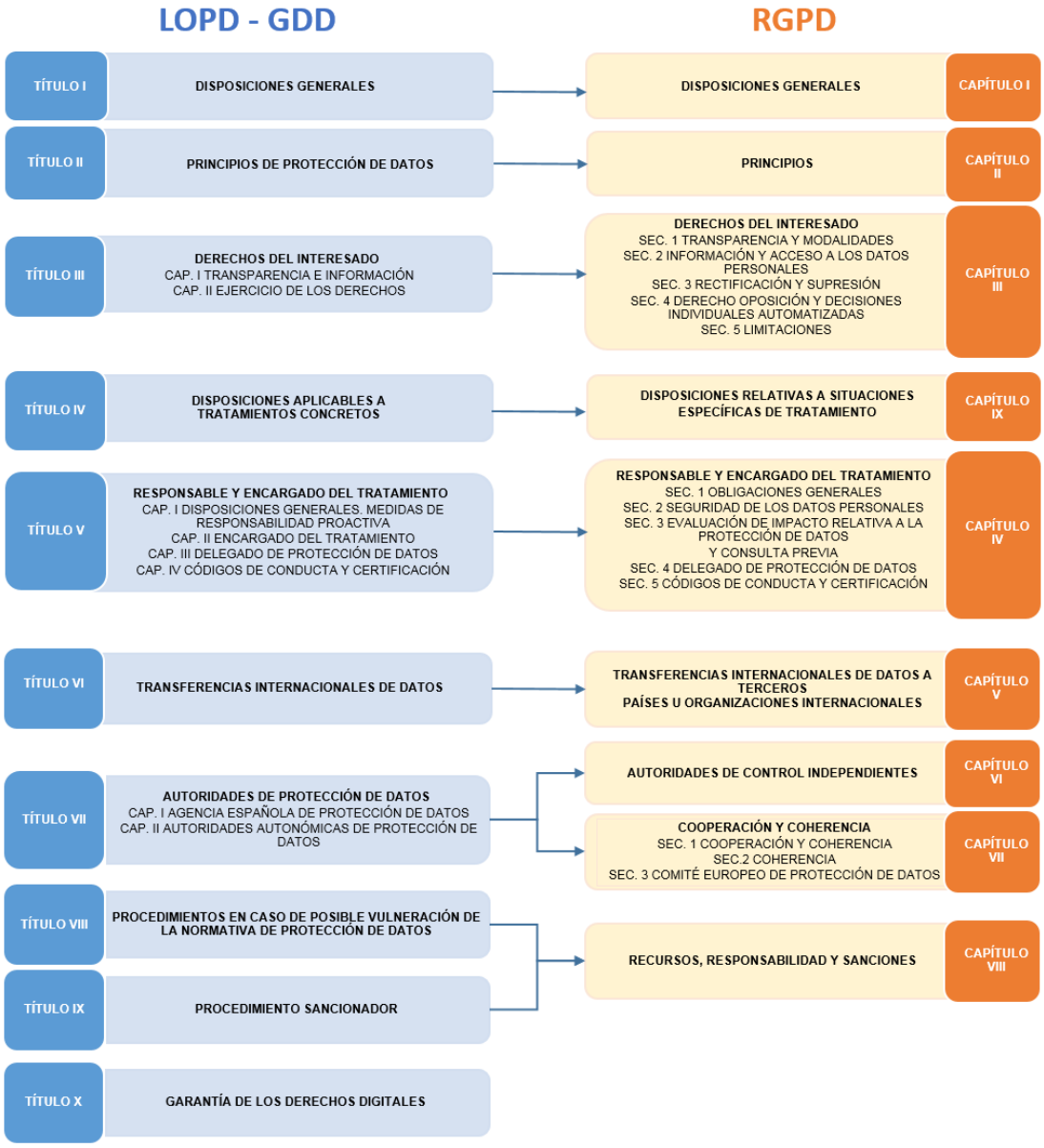


Figura 1 Esquema relación LOPDGDD - RGPD

2 OBJETIVOS

El objetivo general de este proyecto es ofrecer una guía práctica de referencia para la implantación de la protección de datos personales en una PYME. Para conseguir este objetivo, se ha realizado un compendio de lo publicado respecto a la protección de datos personales por organismos e instituciones, de forma que cualquier PYME tenga un punto de referencia único.

La metodología usada para la consecución del objetivo marcado, es el desarrollo de los artículos de la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales y del Reglamento General de Protección de Datos. El apartado de la implantación práctica de la protección de datos se desarrolla a partir de actividades generales, que conllevan el tratamiento de datos personales, llevadas a cabo de forma habitual en una PYME, tales como la gestión de recursos humanos y las relaciones con clientes y proveedores.

En base a los datos publicados por el Instituto Nacional de Estadística, que reflejan que la mayoría de las empresas de Extremadura tienen un número de empleados menor de 50, la implantación práctica se llevará a cabo tomando como referencia la organización de una empresa de menos de 50 asalariados.

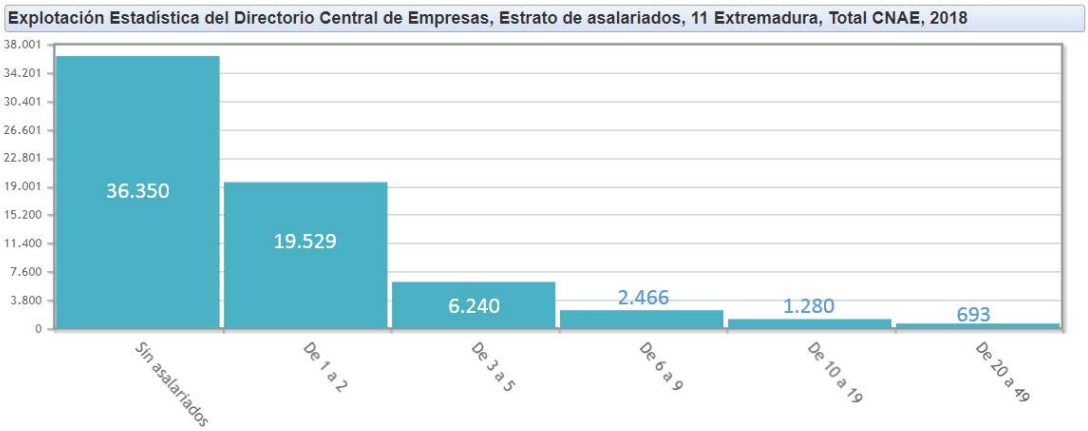


Figura 2 Empresas de Extremadura por número de asalariados (Fuente: Instituto Nacional de Estadística)

3 ESTADO DEL ARTE

El 25 de mayo de 2016, se aprobó el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD), que es de aplicación desde el 25 de mayo de 2018. El RGPD deroga la directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos.

La Directiva de 1995 se desarrolló con un doble objetivo, la protección de los derechos y libertades fundamentales de las personas, en particular, el derecho a la protección de datos, y la realización del mercado interior, es decir, la libre circulación de datos personales en la Unión Europea. A pesar de que estos objetivos siguen vigentes, la rápida evolución tecnológica y la globalización han planteado nuevos retos en la protección de datos personales.

Ante este nuevo contexto, la Comisión Europea se embarcó en un examen exhaustivo de la legislación de la Unión Europea en materia de protección de datos con el objetivo de saber si era suficiente para hacer frente a estos nuevos retos. El resultado determinó que era necesario modernizar el régimen jurídico de la UE en materia de protección de datos teniendo en cuenta los retos derivados de la globalización y de las nuevas tecnologías.

En noviembre de 2010, la Comisión Europea publicó una comunicación con los resultados obtenidos y los objetivos esenciales que debía alcanzar la nueva legislación[1].

Los resultados obtenidos concluyeron que era necesario:

- Clarificar y precisar la aplicación de los principios de protección de datos a las nuevas tecnologías, con el fin de garantizar una protección

[1] http://ec.europa.eu/transparency/regdoc/rep/1/2010/ES/1-2010-609-ES-F1-1.Pdf

real y efectiva de los datos personales independientemente de la tecnología utilizada para tratarlos.

- Homogeneizar la aplicación de la legislación en todos los Estados miembros.
- Mejorar las transferencias internacionales de datos, definiendo cuál es la aplicación aplicable y la atribución de responsabilidad cuando el tratamiento se realiza fuera de la UE.

Los objetivos esenciales que debía abarcar la nueva legislación eran:

- Reforzar los derechos de las personas.
- Garantizar la libre circulación de datos personales entre los Estados miembros en el mercado interior, evitando divergencias entre las legislaciones nacionales que transponen la normativa.
- Clarificar y simplificar las normas aplicables a las transferencias internacionales de datos.
- Reforzar la cooperación entre las autoridades de protección de datos de los diferentes Estados miembros.

El Reglamento General de Protección de Datos es el resultado de la adaptación del régimen jurídico de la UE al nuevo entorno de constante evolución tecnológica y la forma en la que nuestros datos personales se utilizan y comparten.

La transposición de este Reglamento a la legislación española se materializó con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), que entró en vigor el 6 de diciembre de 2018 y que adapta y completa el ordenamiento jurídico español al dicho Reglamento.

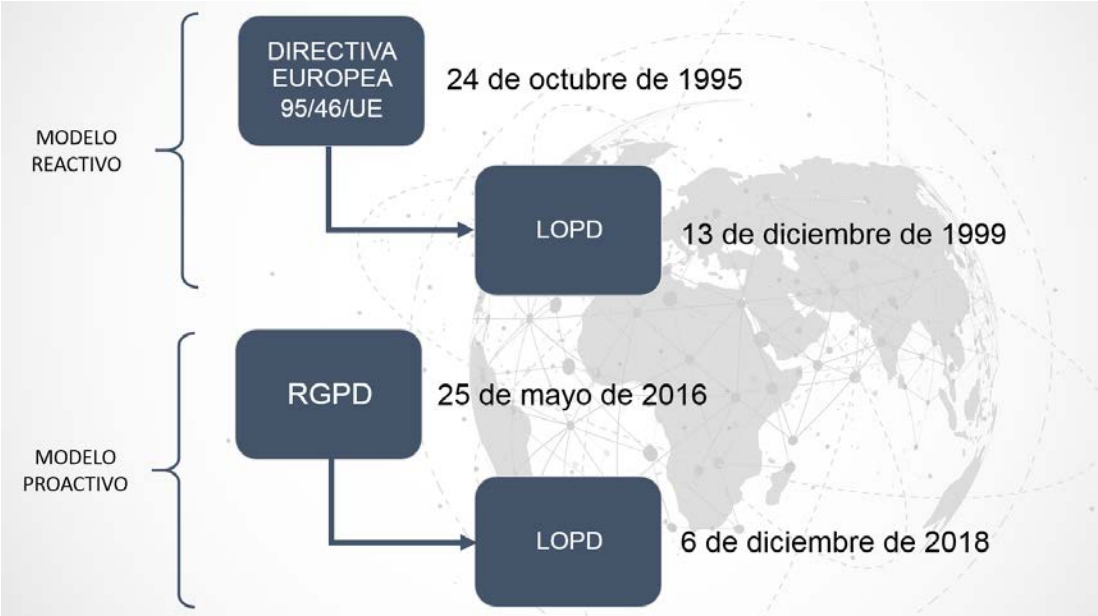


Figura 3 Evolución de la legislación de la UE en materia de protección de datos

4 GUÍA DE REFERENCIA E IMPLEMENTACIÓN

Este apartado combina el desarrollo de la legislación vigente actualmente en materia de protección datos, poniendo especial interés en aquellos aspectos que tienen mayor repercusión en la parte tecnológica del tratamiento de datos, con el desarrollo de un ejemplo práctico basado en actividades de tratamiento llevadas a cabo en un modelo de pequeña empresa.

El contenido del apartado sigue la estructura de la Ley Orgánica de Protección de datos y garantía de derechos digitales (LOPDGDD), completándolo con los artículos del Reglamento General de Protección de Datos (RGPD) a los que referencia. A lo largo de todo el trabajo, se intenta completar la teoría con ejemplos e información adicional que ayudan a entender el significado del artículo desarrollado.

EJEMPLO PRÁCTICO – CONTEXTO

La protección de datos personales se aplica a tres ámbitos diferentes dentro de la organización: legal, organizativo y de seguridad.

En este documento, serán objeto de desarrollo aquellas obligaciones incluidas en el ámbito de la seguridad, ya que las tareas que deben realizarse para cumplir con ellas llevan asociado un alto componente tecnológico.

- Análisis de riesgos
- Medidas de seguridad
- Evaluación de impacto
- Notificación de violaciones de seguridad (gestión de incidentes de seguridad)

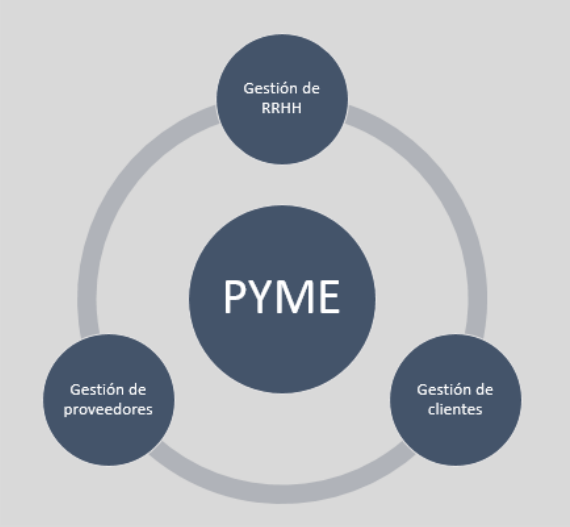
Sin embargo, no hay que pasar por alto que, otras de las obligaciones del responsable del tratamiento, pueden encontrar en la tecnología un importante apoyo para facilitar su cumplimiento y demostrarlo. Por ejemplo, obtener el consentimiento del interesado o soportar los procedimientos para el ejercicio de los derechos de los interesados.

La tecnología puede ayudar a garantizar la seguridad de los tratamientos con herramientas que permitan:

- Monitorizar el uso de los datos, conocer quién accede, cuándo se borran y cifrarlos cuando sea necesario.
- Evitar accesos no autorizados mediante sistemas de gestión de identidad y autenticación.
- Realizar copias de seguridad.
- La protección contra el malware.
- Proteger las comunicaciones.

Para el desarrollo de la aplicación práctica de la protección de datos se tomará como base la organización de una pequeña empresa de menos de 10 empleados cuya actividad principal no sea el tratamiento de datos personales.

Las principales actividades que conllevan tratamiento de datos personales en el desarrollo de la actividad del responsable son: la gestión de recursos humanos, la gestión de clientes y la gestión de proveedores.



La primera pregunta que nos planteamos al abordar el tema de la protección de datos es **¿debo aplicar la protección de datos en mi empresa?** Para responder a esta pregunta debemos formularnos otra **¿trata mi empresa datos personales de personas físicas, ya sea de clientes, proveedores o empleados?** Si la respuesta es afirmativa, entonces **SÍ** debo aplicar la protección de datos en mi empresa.

En el apartado 4.3 puede consultarse qué son datos de carácter personal.

El enfoque práctico de este TFM se centrará en el área tecnológica del tratamiento de datos personales en la gestión de recursos humanos. Se toma como base esta actividad por ser una de las más complejas que conllevan tratamiento de datos personales, sin entrar a valorar la actividad principal de la organización.

Normalmente, las PYMES tienen subcontratada esta actividad en una gestoría. Por este motivo la infraestructura de servidores de aplicaciones que pudieran dar el servicio al software específico, queda fuera de este ejemplo de implementación de protección de datos,

4.1 DEFINICIONES

El artículo 4 del Reglamento (UE) 2016/679 define una serie de conceptos claves para la comprensión del mismo.

Algunas de estas definiciones son:

- **Datos personales**: Toda información sobre una persona física identificada o identificable ("el interesado"). (Ver apdo. 4.3 *Datos de carácter personal*)
- **Tratamiento**: Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimiento automatizados o no.

  El tratamiento abarca una amplia gama de operaciones realizadas sobre los datos personales: recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

EJEMPLOS DE TRATAMIENTO

- Gestión de personal y administración de nóminas
- Acceso o consulta a base de datos de contactos que contengan datos personales
- Envío de correo electrónicos promocionales
- Triturado de documentos que contengan datos personales
- Publicación de una foto de una persona en un sitio web
- Almacenamiento de direcciones IP o MAC
- Grabación de vídeo

*Comisión Europea. ¿Qué constituye tratamiento de datos? (**https://ec.europa.eu**)*

- **Seudonimización**: Es el tratamiento de datos personales de manera que no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté protegida de manera que garantice que los datos personales no se atribuyan a una persona física identificada o identificable. La seudonimización reduce la vinculabilidad de un conjunto de datos con la identidad del interesado; se trata, por tanto, de una medida de seguridad útil, pero no es un método de anonimización.

TÉCNICAS DE SEUDONIMIZACIÓN*

- Cifrado con clave secreta. El poseedor de la clave podrá descifrar el conjunto de datos.
- Función hash: Se trata de una función que devuelve un resultado de tamaño fijo a partir de un valor de entrada de cualquier tamaño. Esta función no es reversible, sin embargo, si se conoce el rango de valores de la función hash (por ejemplo, el DNI) se pueden pasar estos valores por la función a fin de obtener el valor real de un registro determinado. Las funciones hash están sujetas a ataques de fuerza bruta (probar todas las posibles entradas para crear tablas de equivalencia).
- Función con clave almacenada: Se trata de un tipo de función hash que hace uso de una clave secreta a modo de valor de entrada suplementario. El responsable del tratamiento puede reproducir la ejecución de la función con el atributo y la clave secreta. Sin embargo, los atacantes, que no conocen la clave, lo tendrían mucho más difícil ya que el número de combinaciones que habría que probar sería demasiado grande.
- Cifrado determinista o función hash con clave con borrado de clave: Esta técnica equivale a generar un número aleatorio a modo de

◆ Descomposición en tokens: Esta técnica se usa típicamente en el sector financiero (aunque no exclusivamente en él) para reemplazar los números de identificación de tarjetas por valores que son de poca utilidad para los atacantes. Se basa en la aplicación de mecanismos de cifrado unidireccionales o en la asignación, mediante función de índice, de un número de secuencia o un número generado aleatoriamente que no derive matemáticamente de los datos originales.

GT29. Dictamen 05/2014 sobre técnicas de anonimización.

- **Fichero**: Todo conjunto de datos estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.
- **Responsable del tratamiento**: persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento. (Ver apdo. 4.6 *Responsable del tratamiento*).
- **Encargado del tratamiento**: persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable. (Ver apdo. 4.7 *Encargado del tratamiento*).

Un encargado del tratamiento puede ser la gestoría a la que el responsable del tratamiento le encarga la elaboración de las nóminas de sus empleados, o la empresa de informática a la que le contrata el servicio de correo electrónico.

- **Destinatario**: persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros.

En la confección de contratos laborales, el Servicio Público de Empleo Estatal (SEPE) es un destinatario de los datos personales.

- **Tercero**: persona física o jurídica, autoridad pública, servicio u otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar datos personales bajo la autoridad directa del responsable o del encargado.

Si cedemos los datos personales de nuestros clientes a otra empresa para que haga publicidad de sus productos, esta empresa será un tercero. Debemos tener el consentimiento del interesado a esta cesión de datos personales.

- **Consentimiento del interesado**: Es toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

CONDICIONES PARA CONSENTIMIENTO VÁLIDO

- Debe obtenerse antes de que el responsable comience a tratar datos personales para los que requiere el consentimiento.
- Cuando el servicio conlleve múltiples operaciones de tratamiento de datos para más de un fin, el proceso o procedimiento para obtener el consentimiento debe permitir a los interesados autorizar por separado las distintas operaciones.
- Ha de ser informado, es decir, el responsable del tratamiento debe facilitar información a los interesados antes de obtener su consentimiento para que puedan tomar decisiones informadas, comprender qué es lo que están autorizando y poder ejercer sus derechos.

◆ Al solicitar el consentimiento, los responsables del tratamiento deben utilizar un lenguaje claro y sencillo, comprensible por el ciudadano medio y valorando el tipo de público que proporciona datos a su organización.

- **Violación de la seguridad de los datos personales**: Toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.
  Es decir, todo incidente que dé lugar a la violación de la confidencialidad, disponibilidad o integridad de los datos
- **Elaboración de perfiles**: Toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

4.2 ÁMBITO DE APLICACIÓN

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales se aplica:

- A cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.
  Según el considerando 15 del RGPD, la protección de datos personales debe ser independiente de la tecnología utilizada para su tratamiento, y se aplica tanto al tratamiento automatizado como manual, siempre que los datos se organicen con arreglo a criterios predeterminados.

TIPOS DE FICHEROS:

◆ No automatizados. Son conjuntos de datos personales organizados de forma no automática y estructurados conforme a criterios específicos (como orden alfabético) relativos a personas físicas.

Por ejemplo: listado en papel de clientes, formularios de datos…

◆ Automatizados. Son conjuntos de datos personales organizados de forma automática y gestionados mediante programas, soportes y equipos informáticos.

Por ejemplo: Base de datos de empleados, clientes, directorio corporativo publicado en la intranet…

- A toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados se consideran información sobre una persona física identificable.
- Al tratamiento de datos personales en el contexto de las actividades llevadas a cabo por un responsable o encargado del tratamiento de la Unión Europea, independientemente de que el tratamiento tenga lugar en la Unión o no.
- Al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades estén relacionadas con:
    - ❖ la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se quiere su pago.
    - ❖ el control de su comportamiento, en la medida en que este tenga lugar en la Unión.

No es de aplicación:

- Al tratamiento de datos personales relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de persona jurídica y sus datos de contacto.

No es de aplicación al tratamiento de datos de empresas u organismos públicos, como la Seguridad Social, las Universidades… Ni a los datos de empresas privadas, asociaciones…

- Al tratamiento de datos personales en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión, actividades relativas a la seguridad nacional.
- Al tratamiento de datos de carácter personal por una persona física en el ejercicio de actividades exclusivamente personales o domésticas.

Una agenda con teléfonos, mail, direcciones… de nuestros familiares y amigos utilizados para actividades personales o domésticas. Si los datos fueran utilizados para, por ejemplo, publicitar su negocio debería cumplir la normativa en protección de datos.

- A los datos personales de personas fallecidas. En este caso, la LOPDGDD establece que las personas vinculadas a la persona fallecida podrán solicitar el acceso a los datos personales de ésta y, en su caso, su rectificación o supresión.

4.3 DATOS DE CARÁCTER PERSONAL

Según el artículo 4.1 del RGPD son datos personales “toda información sobre una persona física identificada o identificable”.

EJEMPLOS DE DATOS PERSONALES:

- Nombre y apellidos
- Dirección
- Dirección de correo electrónico del tipo *nombre.apellido@empresa.com*
- Número de documento nacional de identidad
- Datos de localización

EJEMPLOS DE DATOS NO CONSIDERADOS PERSONALES:

- Número de registro mercantil
- Dirección de correo electrónico del tipo info@empresa.com
- Datos anonimizados

Comisión Europea. https://ec.europa.eu/info/law/law-topic/data-protection/reform

La identificación de una persona, a efectos de protección de datos, se realiza cuando puede determinarse la identidad directa o indirectamente a través de uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona o mediante un identificador, como un nombre, un número de identificación, datos de localización, un identificador en línea.

La normativa contempla dos categorías de datos, por una parte, tenemos los datos sensibles y por otros los no sensibles. Todos los datos que no son considerados datos sensibles o “categorías especiales de datos”, se consideran como datos no sensibles.

Dentro de la categoría de datos no sensibles tenemos, entre otros:

- Datos identificativos: nombre, apellidos, número de documentos nacional de identidad

- Datos referidos a la situación laboral
- Datos relativos a la situación financiera

En las categorías especiales de datos el RGPD incluye los siguientes datos:

- Datos personales relativos a la salud, datos que dan información relativa al estado de salud física o mental pasado, presente o futuro del interesado. Se incluye:
  - ❖ Información recogida al inscribirse a efectos de asistencia sanitaria o con la prestación de tal asistencia.
  - ❖ Todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios.
  - ❖ La información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal y cualquier información relativa a una enfermedad, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente.
- Datos que revelen el origen racial o étnico, opiniones políticas, convicciones religiosas o fisiológicas, o afiliación sindical.
- Datos genéticos, estos son los datos personales relacionados con características genéticas, heredadas o adquiridas, provenientes del análisis de una muestra biológica (examen cromosómico, análisis de ADN o ARN).
- Datos biométricos, datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales que permiten la identificación única de una persona (imágenes faciales, datos dactiloscópicos…)
- Datos relativos a la vida sexual u orientación sexual.

Como regla general los datos de las categorías especiales no pueden ser tratados, salvo cuando concurra una la de las siguientes circunstancias (Art. 9 LOPDGDD y Art.9 RGPD):

1. El interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más fines específicos.

2. El tratamiento es necesario para proteger intereses vitales del interesado, cuando no esté capacitado, física o jurídicamente, para dar su consentimiento.
3. El tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social.
4. El tratamiento lo realiza, legítimamente y con las debidas garantías, una fundación, asociación u otro organismo sin ánimo de lucro con finalidad política, religiosa, filosófica o sindical y únicamente se refiera a los miembros actuales o antiguos de dichas organizaciones.
5. El tratamiento se refiere a datos que el interesado ha hecho públicos.
6. El tratamiento es realizado por un profesional sujeto a la obligación del secreto profesional.
7. El tratamiento es necesario para procedimientos judiciales.
8. El tratamiento es necesario por razones de interés público en el ámbito de la salud pública o la asistencia sanitaria.
9. El tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia sanitaria o social.
10. El tratamiento es necesario para fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.

DATOS NO SENSIBLES

- Datos identificativos
- Datos de situación laboral
- Datos de situación financiera

CATEGORÍAS ESPECIALES DE DATOS

- Relativos a la salud o la vida sexual y/o la orientación sexual
- Origen racial o étnico
- Opiniones políticas
- Convicciones religiosas o fisiológicas
- Afiliación sindical
- Datos genéticos
- Datos biométricos

Figura 4 Categorías de datos de carácter personal

EJEMPLO PRÁCTICO – DATOS DE CARÁCTER PERSONAL

El primer paso es identificar los datos personales que son objeto de tratamiento en la organización y distinguir cuáles pertenecen a la categoría de datos sensibles.

Para ello identificaremos los colectivos de los que tratamos datos y analizaremos los datos de cada uno de ellos:

- EMPLEADOS:
    - Nombre y apellidos
    - NASS
    - DNI
    - Dirección
    - Correo electrónico
    - Teléfono de contacto
    - Nivel de estudios
- CLIENTES
    - Nombre y apellidos
- PROVEEDORES
    - Nombre y apellidos
    - Nº cuenta bancaria para el pago

En el caso de los colectivos de clientes y proveedores, debemos tener en cuenta que no se consideran datos personales los datos referidos a personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de persona jurídica y sus datos de contacto.

4.4 PRINCIPIOS DE PROTECCIÓN DE DATOS

Los tratamientos de datos de carácter personal están sujetos a unos principios que determinan cómo recoger y tratar los datos (Art 5 RGPD).

4.4.1 LICITUD, LEALTAD Y TRANSPARENCIA

Los datos personales serán tratados de forma lícita, leal y transparente.

El tratamiento de los datos debe estar amparado en alguna de las siguientes bases jurídicas:

1. Consentimiento del interesado.
2. Relación contractual.
3. Intereses vitales del interesado o de otras personas.
4. Obligación legal para el responsable.
5. Interés público o ejercicio de poderes públicos.
6. Intereses legítimos prevalentes del responsable o de terceros a los que se comunican los datos

El responsable debe informar, previamente al tratamiento de los datos, sobre el objeto y fines del tratamiento, sus consecuencias y posibles riesgos (Ver apdo. 4.5.1 *Transparencia*).

4.4.2 LIMITACIÓN DE LA FINALIDAD

Los datos personales serán recogidos para unos fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines.

4.4.3 PRINCIPIO DE MINIMIZACIÓN DE DATOS

Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

4.4.4 PRINCIPIO DE EXACTITUD

Los datos personales serán exactos y si fuera necesario actualizados, adoptándose medidas razonables para que se supriman o rectifiquen sin delación los datos personales que sean inexactos a los fines para los que se tratan.

4.4.5 PRINCIPIO DEL PLAZO DE CONSERVACIÓN

Los datos personales serán mantenidos de forma que se permita la identificación de los interesados por un plazo de tiempo no superior al necesario para cumplir con los fines del tratamiento.

4.4.6 PRINCIPIO DE INTEGRIDAD Y CONFIDENCIALIDAD

Los datos personales serán tratados de manera que se garantice su adecuada seguridad, incluyendo la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, aplicando las medidas técnicas y de organización apropiadas.

4.4.7 PRINCIPIO DE RESPONSABILIDAD PROACTIVA

Los responsables y encargados de tratamiento deben cumplir los principios mencionados anteriormente y ser capaces de demostrar dicho cumplimiento. El RGPD establece un catálogo de medidas que deben aplicar, tanto los responsables como los encargados, para garantizar que los tratamientos de datos personales se realizar conforme a la normativa.

- Análisis de riesgos (Ver apdo. 4.12)
- Registro de actividades de tratamiento (Ver apdo. 4.10)
- Protección de datos desde el diseño y por defecto (Ver apdo. 4.11)
- Medidas de seguridad (Ver apdo. 4.14)
- Notificación de violaciones de seguridad (Ver apdo. 4.15)
- Evaluación de impacto (Ver apdo. 4.13)
- Delegado de protección de datos (Ver apdo. 4.8)

4.5 DERECHOS DE LAS PERSONAS[2]

El Título III de la LOPDGDD regula el derecho de los usuarios a ser informados acerca del tratamiento de sus datos personales, así como los derechos de acceso, rectificación, supresión, oposición, derecho a la limitación del tratamiento y derecho a la portabilidad.

4.5.1 TRANSPARENCIA

El RGPD y, por extensión, la LOPDGDD obliga a los responsables y encargados del tratamiento a informar a los interesados en todo momento qué datos se están tratando, con qué finalidad, cómo reclamar al responsable y/o encargado, así como dar a los interesado un control total sobre sus datos.

Esta transparencia debe aplicarse a tres ámbitos:

1. al suministro de información a los interesados
2. cómo los responsables del tratamiento se comunican con los interesados
3. cómo los responsables del tratamiento facilitan que los interesados ejerzan sus derechos.

La transparencia debe aplicarse en todos los tratamientos de datos personales, independientemente de la base jurídica y a lo largo de todo el ciclo de vida del mismo:

- antes de comenzar el tratamiento o al inicio del mismo.
- a lo largo del todo el periodo del tratamiento
- en momentos específicos mientras el tratamiento está en curso (por ejemplo, cuando se produzcan violaciones de seguridad)

La información o comunicación debe cumplir las siguientes normas (Art. 12.1 RGPD):

- debe ser concisa, transparente, inteligible y de fácil acceso.

[2] Grupo de trabajo del artículo 29. Directrices sobre la transparencia

EJEMPLOS DE COMUNICACIÓN DE FÁCIL ACCESO

- Cuando el responsable mantenga un sitio web
  - Declaraciones/Avisos de privacidad. Visible y accesible fácilmente desde todas las páginas del sitio web (Enlace directo bajo un término de uso común “Privacidad”, “Política de privacidad”…).
- En las aplicaciones
  - La información debe estar disponible en la tienda en línea y debe seguir siendo fácilmente accesible desde dentro de la aplicación. Por ejemplo, una manera de cumplir con este requisito es que no haga falta más de “dos toques” para acceder.

- debe utilizarse un lenguaje claro y sencillo, en particular cuando va dirigida a niños.

RECOMENDACIONES USO DEL LENGUAJE

- Debe evitarse el uso de calificativos del tipo “puede”, “podría”, “algunos”, “frecuentemente” y “posible” que pueden dar lugar a distintas interpretaciones.
- Los párrafos y las oraciones deben estar bien estructurados, utilizando viñetas y guiones.
- Debe utilizarse la voz activa
- No debe contener lenguaje o terminología excesivamente legal, técnica o especializada.
- Cuando los bienes/servicios son utilizados particularmente por niños, el responsable debe asegurar que el vocabulario, el tono y el estilo es apropiado para los niños.

EJEMPLO DE PRÁCTICA DEFICIENTE

“Podremos utilizar sus datos para desarrollar nuevos servicios”

No especifica qué servicios ni cómo ayudarán los datos a desarrollarlos

EJEMPLO DE BUENAS PRÁCTICAS

“Conservaremos su historial de compra y utilizaremos detalles de los productos que ha comprado anteriormente para sugerirles otros productos que creemos que podrían interesarle”

En este ejemplo, está claro qué datos se utilizarán y con qué finalidad

- debe facilitarse por escrito o por otros medios, incluso por medios electrónicos. A la hora de elegir el medio para facilitar la información debe tenerse en cuenta cómo interactúan el responsable y el interesado.

MEDIOS PARA FACILITAR LA INFORMACIÓN

- Medios electrónicos escritos:
  - Declaraciones/avisos de privacidad en un sitio web.
  - Avisos contextuales emergentes
  - Avisos mediante 3D Touch
  - Avisos al posar el cursor
  - Paneles de privacidad
- Medios electrónicos no escritos
  - Vídeos
  - Alertas de voz para teléfonos inteligentes o dispositivos del IoT.
- Otros medios (no necesariamente electrónicos)
  - Dibujos animados, cómics, pictogramas (especialmente si va dirigido a niños)
  - Infografías
  - Diagramas de flujo
  - Impresos en manuales de instrucciones

- podrá facilitarse verbalmente cuando lo solicite el interesado, siempre que se demuestre la identidad del interesado por otros medios.
- La condición de verificar la identidad del interesado no se aplica al suministro de información general sobre privacidad (datos del responsable y del delegado, fines del tratamiento…) ya que ésta debe ponerse a disposición de futuros usuarios/clientes. Sí es necesario verificar la identidad previamente al ejercicio de sus derechos por parte de un interesado específico.
- El responsable del tratamiento debe disponer del registro de la solicitud de información por medios verbales, el método utilizado para verificar la identidad del interesado y el hecho de que se facilitó la información al interesado.

Además de presencialmente o por teléfono, es posible facilitar la información verbalmente de manera automatizada. Por ejemplo, podemos dar la opción de audio de la información de un aviso de privacidad para personas con alguna discapacidad visual o en el contexto de dispositivos inteligentes sin pantalla.

El GT29 recomienda que, el responsable del tratamiento debe permitir que el interesado pueda volver a escuchar los mensajes pregrabados, esto es imprescindible cuando la solicitud de obtener la información verbalmente provenga de interesados con dificultades para acceder o entender la información en formato escrito.

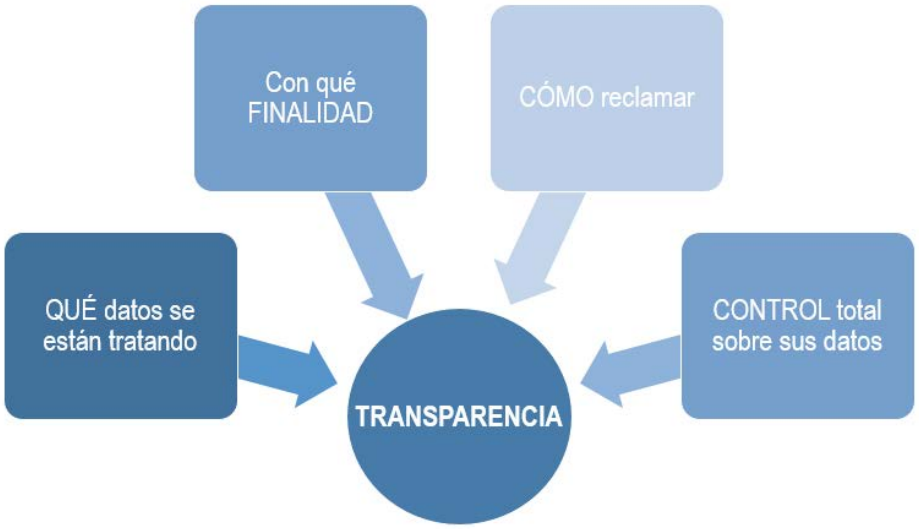


Figura 5 Principio de transparencia en el tratamiento de datos personales

4.5.2 INFORMACIÓN CUANDO LOS DATOS SEAN OBTENIDOS DEL INTERESADO

Se consideran datos personales obtenidos directamente del interesado aquellos que[3]:

- un interesado ha facilitado directamente a un responsable del tratamiento (por ejemplo, al rellenar un formulario en línea).
- un responsable del tratamiento obtiene de un interesado mediante observación (por ejemplo, utilizando dispositivos automáticos o programas informáticos de captura de datos, como cámaras, equipos de red, localización por wifi, RFID u otros tipos de sensores.

En este caso, se debe informar a los interesados sobre las circunstancias relativas al tratamiento de sus datos en el momento en que se le soliciten.

Si posteriormente se quieren utilizar los datos para un fin diferente a aquel para el que se recogieron, debe informarse al interesado de la nueva finalidad antes de su tratamiento.

[3] Directrices sobre transparencia. GT29 apdo. 26

Según el Art. 11.2 de la LOPD-GDD y el art. 13 del RGPD, cuando los datos personales sean obtenidos del interesado, el responsable del tratamiento deberá facilitarle la siguiente información:

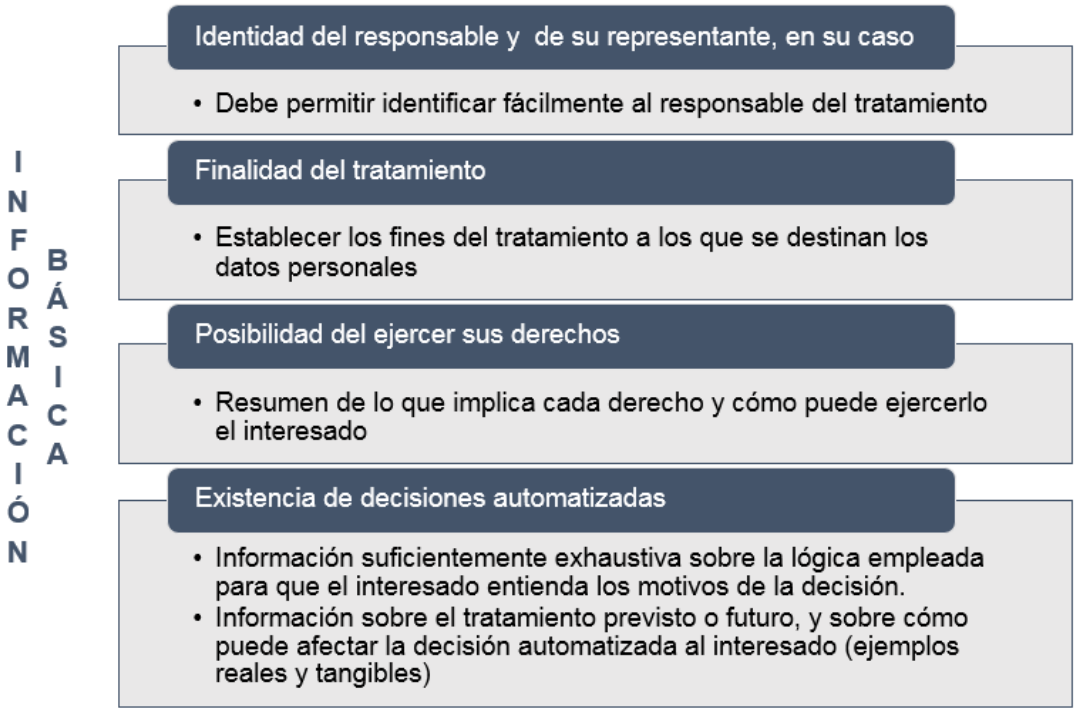


Figura 6 Información básica cuando los datos son obtenidos del interesado

Al suministrar la información básica, el responsable deberá facilitar una dirección de correo electrónico u otro medio que permita acceder al resto de información. El resto de información debe ser accesible de forma sencilla e inmediata.

Figura 7 Información adicional cuando los datos son obtenidos del interesado

4.5.3 INFORMACIÓN CUANDO LOS DATOS NO SEAN OBTENIDOS DEL INTERESADO

Los datos personales no han sido obtenidos del interesado cuando el responsable los ha obtenido de fuentes como:[4]

- responsables de tratamiento terceros
- fuentes de acceso público
- intermediarios de datos
- otros interesados

[4] Directrices sobre transparencia. GT29 apdo. 26

La información relativa al tratamiento de sus datos debe ponerse a disposición de los interesados dentro de un plazo razonable y, a más tardar, dentro de un mes desde el momento en el que se obtuvieron.

Es posible que deba informarse con anterioridad por alguna de las siguientes causas:

- si los datos han de utilizarse para comunicarse con el interesado, se debe informar antes o en la primera comunicación con el interesado.
- si está previsto comunicarlos a otro destinatario, se debe comunicar antes o en la primera comunicación con el interesado.

Al igual que en el caso de que los datos personales hayan sido obtenidos directamente del interesado, si posteriormente se quieren utilizar los datos para un fin diferente a aquel para el que se recogieron, debe informarse al interesado de la nueva finalidad antes de su tratamiento.

Según el Art. 11.3 de la LOPDGDD y el art. 13 del RGPD, cuando los datos personales sean obtenidos del interesado, el responsable del tratamiento deberá facilitarle la siguiente información:

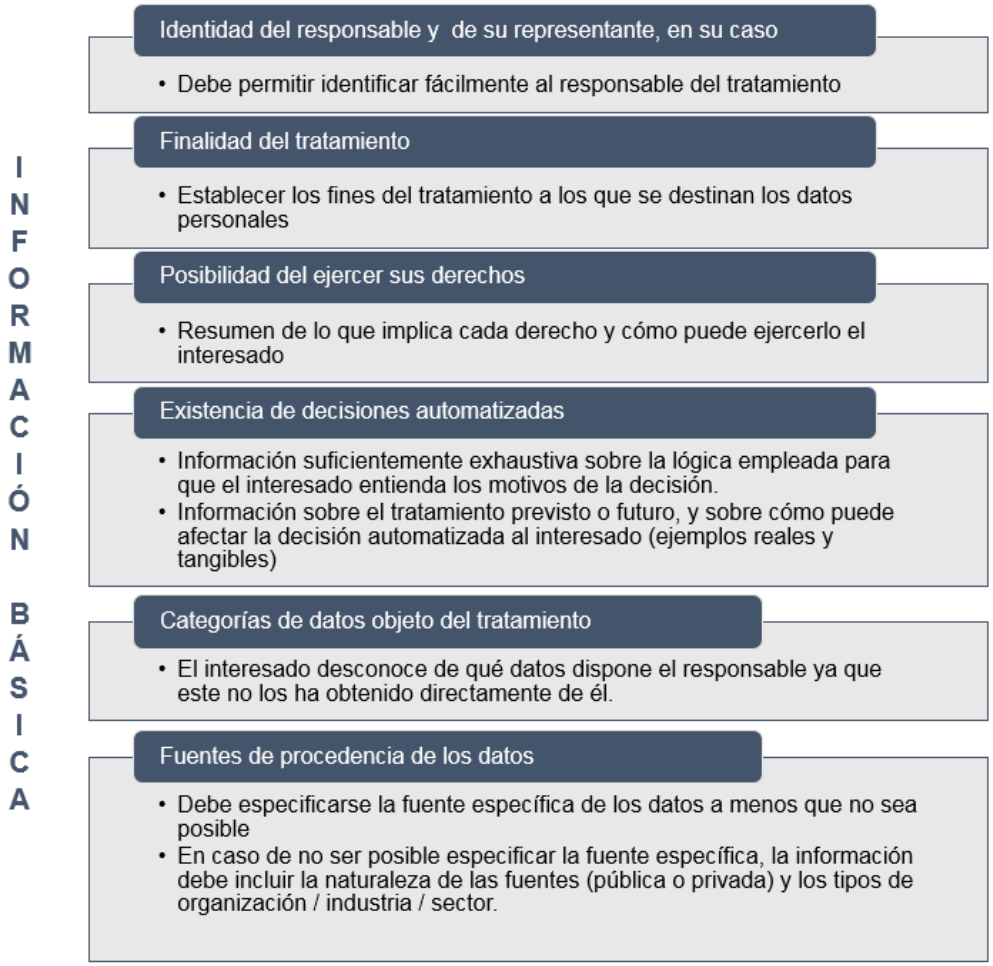


Figura 8 Información adicional cuando los datos no son obtenidos del interesado

La información adicional que debe facilitar el responsable en este caso es la misma que cuando ha obtenido los datos directamente del interesado (Ver. *Figura 7. Información adicional cuando los datos son obtenidos del interesado*).

4.5.4 EJERCICIO DE LOS DERECHOS[5]

La normativa de protección de datos permite que los interesados puedan ejercitar ante el responsable del tratamiento sus derechos de acceso, rectificación, oposición, supresión ("derecho al olvido"), limitación del tratamiento, portabilidad y no ser objeto de decisiones individualizadas.

Estos derechos se caracterizan por (Art. 12 LOPDGDD):

[5] Protección de datos: Guía para el ciudadano de la AEPD.

1. El ejercicio de los derechos es gratuito.
2. El responsable deberá responder a la solicitud en el plazo de un mes a partir de la recepción de la solicitud. (Art. 12.3 RGPD).
3. El plazo de respuesta se podrá prorrogar otros dos meses, teniendo en cuenta la complejidad y el número de solicitudes. El responsable deberá informar al interesado de la prorroga en el plazo de un mes desde la recepción de la solicitud, indicando los motivos (Art. 12.3 RGPD).
4. Si las solicitudes son manifiestamente infundadas o excesivas (carácter repetitivo) el responsable podrá:
   - Cobrar un canon proporcional a los costes administrativos soportados
   - Negarse a actuar

Podrá considerarse repetitivo el derecho de acceso en más de una ocasión en el plazo de seis meses, a menos que exista causa legítima para ello (Art. 13.3 LOPDGDD).

Cuando el afectado elija un medio distinto al que se le ofrece que suponga un coste desproporcionado, la solicitud será considerada excesiva (Art 13.4 LOPDGDD).

5. Pueden ejercerse directamente o por medio de representante legal o voluntario.
6. El responsable del tratamiento está obligado a informar al interesado sobre los medios que están a su disposición para ejercitar sus derechos. Estos medios deben ser accesibles y no se puede denegar el ejercicio del derecho por el único motivo de que el interesado opte por otro medio.
7. El encargado del tratamiento, por cuenta del responsable, podrá atender las solicitudes siempre que así se haya establecido en el contrato o acto jurídico que les vincula.
8. El responsable debe poder probar que ha respondido a la solicitud de ejercicio de los derechos formulado por el afectado.
9. Los titulares de la patria potestad podrán ejercitar los derechos en nombre y representación de los menores de catorce años.

Métodos para facilitar al interesado el ejercicio de sus derechos:

1. Escrito a una dirección postal.
2. Escrito a una dirección de correo electrónico.
3. Envío de formulario electrónico en un sitio web.
4. Funcionalidad que permita la modificación de los datos personales, borrado de todos los datos (eliminación cuenta) en una aplicación .

Para el ejercicio de los derechos el responsable debe verificar la identidad del usuario:

1. Solicitando fotocopia del documento de identidad adjunta en el correo electrónico.
2. Autenticación mediante usuario y contraseña para acceder a un sistema informático.
3. Autenticación mediante PIN.
4. Validación de datos asociados a una operación (por ej. Nombre completo, DNI y teléfono asociado a un contrato)
5. Autenticación mediante rasgos físicos (huellas dactilares, reconocimiento facial…).
6. Autenticación por SMS (envío de SMS con un código al móvil).

4.5.5 DERECHO DE ACCESO

Este derecho permite al interesado dirigirse al responsable del tratamiento para conocer si se están tratando o no sus datos personales y, en el caso de que se estén realizando el tratamiento (Art. 12 LOPDGDD y Art. 15 RGPD):

- Obtener copia de los datos personales que se están tratando. Cuando el responsable trate una gran cantidad de datos relativos al afectado, el responsable podrá solicitar al afectado, antes de facilitar la información, que especifique los datos o actividades de tratamiento a los que se refiere la solicitud.
- Los fines del tratamiento

- Las categorías de datos personales de que se trate.
- Los destinatarios o categorías de destinatarios a los que se comunicaron o comunicarán los datos personales, en particular destinatarios en terceros países u organizaciones internacionales.
- De ser posible, el plazo previsto de conservación de los datos personales o, si no es posible, los criterios utilizados para determinar este plazo.
- La existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado u oponerse a dicho tratamiento.
- El derecho a presentar una reclamación ante una autoridad de control.
- Cuando los datos no se hayan obtenido del interesado, cualquier información disponible sobre su origen.
- La existencia de decisiones automatizadas, incluidas la elaboración de perfiles, y al menos, en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.
- Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas relativa a la transferencia realizada.

Los responsables podrán atender a este derecho facilitando el acceso remoto a un sistema seguro que ofrezca al interesado un acceso directo a sus datos personales. En estos casos, la comunicación por el responsable al afectado del modo en que puede acceder a dicho sistema bastará para dar por atendida la solicitud.

El interesado podrá solicitar el resto de información relativa al tratamiento de sus datos personales que no se incluya en el sistema remoto.

4.5.6 DERECHO DE RECTIFICACIÓN

Derecho del afectado a que se modifiquen los datos, sin dilación indebida del responsable del tratamiento, que resulten ser inexactos o incompletos (Art. 14 LOPDGDD y Art. 16 RGPD).

En la solicitud el interesado deberá indicar los datos a los que se refiere y la corrección que haya que realizar, debiendo adjuntar, cuando sea necesario, la documentación justificativa de la inexactitud o carácter incompleto de los datos.

4.5.7 DERECHO DE SUPRESIÓN

Derecho del afectado a que se supriman los datos personales que le conciernan (de aquí surge el llamado “derecho al olvido“). El responsable está obligado a suprimir los datos sin dilación indebida cuando se de alguna de las siguientes circunstancias (Art. 15 LOPDGDD y Art.17 RGPD):

- Si los datos personales ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo.
- Si el tratamiento de los datos está basado en el consentimiento y se retira, siempre que el tratamiento no se base en otro fundamento jurídico.
- Si el usuario se ha opuesto al tratamiento de sus datos en las siguientes circunstancias:
    - El tratamiento se basaba en un interés legítimo o en el cumplimiento de una misión de interés público y no han prevalecido otros motivos para legitimar el tratamiento.
    - El tratamiento tenía por objeto la mercadotecnia directa. En este caso el responsable podrá conservar los datos identificativos del interesado necesarios con el fin de impedir tratamientos futuros para fines de mercadotecnia directa.
- Si los datos personales han sido tratados ilícitamente.
- Si los datos personales deben suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento.
- Si los datos personales se han obtenido en relación con la oferta directa de servicios de la sociedad de la información a niños

4.5.8 DERECHO A LA LIMITACIÓN DEL TRATAMIENTO

Limitar el tratamiento supone que, si el interesado quiere borrar sus datos personales pero algún motivo legal lo impide, éste puede solicitar la limitación

del tratamiento de sus datos al responsable. De esta forma, los datos pueden ser conservados, pero no utilizado para otros fines.

Este derecho podrá ejercerse cuando se de alguna de las siguientes circunstancias (Art. 16 LOPDGDD y Art. 18 RGPD):

- Cuando el interesado impugne la exactitud de los datos, durante un plazo que permita al responsable verificar la exactitud de los datos.
- Cuando el tratamiento es ilícito pero el interesado se oponga a la supresión.
- Cuando el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones.
- Cuando el interesado se haya opuesto al tratamiento de sus datos personales que el responsable realiza en base a un interés legítimo o misión de interés público, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

Ejemplo:

El interesado decide cambiar de banco y solicita al “antiguo” banco que cierre todas sus cuentas y borre todos los datos personales. Sin embargo, el “antiguo” banco está sujeto a una ley que obliga a conservar todos los datos de sus clientes durante diez años. En este caso, el interesado puede solicitar una limitación del tratamiento para asegurarse que sus datos se utilicen para fines no deseados.

https://ec.europa.eu. Derecho de los ciudadanos.

4.5.9 DERECHO A LA PORTABILIDAD

El interesado tendrá derecho a que el Responsable transmita sus datos a otro responsable del tratamiento o al mismo interesado, mediante un formato estructurado de uso habitual y lectura mecánica (por ejemplo, fichero Excel o csv. No está permitido el formato PDF o imágenes que no pueden ser

tratadas), cuando el tratamiento se efectúe por medios automatizados y se base en:

- El consentimiento del interesado para fines específicos.
- La ejecución de un contrato o precontrato con el interesado.

El derecho a la portabilidad de datos no se aplicará cuando:

- Sea técnicamente imposible la transmisión, por ejemplo, cuando el tratamiento no se efectúe por medios automatizados.
- Pueda afectar negativamente a los derechos y libertades de terceros.
- El tratamiento tenga una misión de interés público fundamentado en la legislación vigente.

4.5.10 DERECHO DE OPOSICIÓN

Derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los supuestos en que:

- Sean objeto de tratamiento basado en una misión de interés público o en el interés legítimo, incluido la elaboración de perfiles. El responsable dejará de tratar los datos salvo que acredite motivos imperiosos que prevalezcan sobre los intereses, derechos y libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.
- Cuando el tratamiento tenga por finalidad la mercadotecnia, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.
- Cuando el interesado se oponga al tratamiento de fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines.

Figura 9 Derechos de las personas

4.6 RESPONSABLE DEL TRATAMIENTO

El responsable del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios de tratamiento.

Una de las principales novedades que presenta el RGPD respecto a la anterior normativa, son las medidas de seguridad que deben aplicarse para garantizar que el tratamiento de los datos se realizará de manera que garantice la protección de la persona física.

Si la anterior legislación establecía tres niveles de seguridad (básico, medio y alto) atendiendo al tipo de datos tratados, el RGPD introduce dos principios generales que recaen sobre los responsables del tratamiento:

- **El principio de responsabilidad proactiva**. El RGPD define este principio como la necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento.
- **El enfoque de riesgo**. El RGPD señala que las medidas dirigidas a garantizar su cumplimiento deben tener en cuenta la naturaleza, el

contexto, el ámbito y los fines del tratamiento, así como los riesgos para los derechos y libertades de las personas.

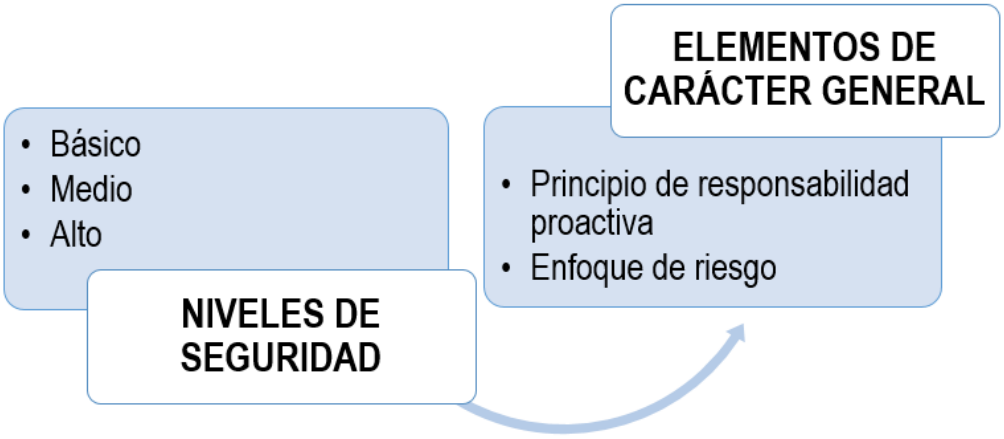


Figura 10 De los niveles de seguridad al principio de responsabilidad proactiva

Las obligaciones del responsable del tratamiento son:

1. Establecer las bases de legitimización para el tratamiento de los datos.
   - Documentar e identificar claramente la base legal sobre la que se desarrollan los tratamientos.

El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones (Art. 6 del RGPD):

1. Consentimiento del interesado
2. Ejecución de un contrato
3. Para proteger intereses vitales del interesado o de otra persona física
4. Cumplimiento de una obligación legal para el responsable
5. Interés público o ejercicio de poderes públicos
6. Intereses legítimos del responsable o de terceros, siempre que no prevalezcan los intereses o los derechos y libertades fundamentales del interesado.

   - Obtener el consentimiento del interesado de formar inequívoca y explícita.

Algunas formas de obtener el consentimiento explícito:

- En una declaración escrita.
- En el contexto digital o en línea, rellenando un impreso electrónico, enviando un correo electrónico, cargando un documento escaneado con su firma o utilizando una firma electrónica.
- Mediante una conversación telefónica, siempre que la información sea justa inteligible y clara y pida una confirmación específica del interesado (por ej. Pulsando un botón o proporcionando una confirmación verbal).

Para obtener el consentimiento el RGPD no permite las casillas previamente marcadas o mecanismos de exclusión voluntaria que requieran la intervención del usuario para evitar el acuerdo.

Por ejemplo: ☐ No consiento el tratamiento…

Según el art. 28 de la LOPDGDD el responsable debe acreditar que el tratamiento es conforme con el RGPD que en su art. 7.1 indica que el responsable deberá ser capaz de demostrar que el interesado consintió el tratamiento de sus datos personales.

Por ejemplo, debe mantener un registro con las declaraciones del consentimiento recibidas, de manera que pueda demostrar cómo y cuándo se obtuvo y qué información se facilitó al interesado. En un contexto en línea, el responsable podría conservar información sobre la sesión en la se expresó el consentimiento, junto con información sobre el flujo de trabajo del consentimiento cuando dicha sesión tuvo lugar y una copia de la información que se presentó en ese momento al interesado. (Grupo de trabajo de art. 29. Directrices sobre el consentimiento, Apdo. 5.1)

2. Informar a los interesados (Ver apdo. 4.5.2 y 4.5.3 de este documento).

- La información deberá proporcionarse de forma concisa, transparente, inteligible y de fácil acceso con un lenguaje claro y sencillo.
- Deberá facilitarse por escrito, incluidos los medios electrónicos cuando sea apropiado.

3. Atender a los interesados en el ejercicio de sus derechos (Ver apdo. 4.5 *Derechos de las personas*).
   - Los responsables deben facilitar a los interesados el ejercicio de sus derechos, y los procedimientos y las formas para ello deben ser visibles, accesibles y sencillos.
   - Debe ser posible la presentación de solicitudes por medios electrónicos, especialmente cuando el tratamiento se realiza por estos medios.
   - Los responsables deben tomar medidas para verificar la identidad de quienes soliciten acceso, rectificación, cancelación u oposición (derechos ARCO) a los datos.
4. Adoptar medidas de responsabilidad activa.
   - Registro de actividades de tratamiento (Art. 30.1). El responsable debe describir los datos de contacto del responsable y del delegado, qué datos de carácter personal recoge, la finalidad del tratamiento, a quién se los comunicará, la trasferencia de datos a terceros países, los plazos previstos para suprimirlos y las medidas técnicas y organizativas de seguridad.
   - Medidas de protección de datos desde el diseño y por defecto. El responsable debe adoptar, con anterioridad al inicio del tratamiento y durante su desarrollo, medidas que garanticen que solo se traten los datos necesarios en lo relativo a la cantidad de datos tratados, la extensión del tratamiento, los periodos de conservación y la accesibilidad a los datos.
   - Análisis de riesgos y adopción de medidas de seguridad. Todos los responsables deberán realizar una valoración del riesgo de los tratamientos que realicen, con el fin de establecer qué medidas aplicar y cómo hacerlo. El análisis variará en función de los tipos de

tratamiento, la naturaleza de los datos, el número de interesados afectados y la cantidad y variedad de tratamientos que se lleven a cabo.

- Notificación de violaciones de seguridad (Art. 33 RGPD). En caso de violación de seguridad de los datos personales, el responsable deberá notificarla a la autoridad de control competente sin dilación y a más tardar 72 horas después de que haya tenido constancia de ella.
- Evaluaciones de impacto sobre la protección de datos. Esta evaluación debe realizarse antes del tratamiento de los datos personales y permite identificar cuáles son los principales riesgos a los que están expuestos los datos personales y establecer las medidas oportunas para minimizarlos.

5. En caso de recurrir a un encargado de tratamiento, debe asegurarse que el encargado elegido ofrece las garantías suficientes para aplicar medidas técnicas y organizativas apropiadas para que el tratamiento sea conforme con el RGPD y la LOPDGDD.
6. Designar un delegado de protección de datos (Art. 34.1 LOPDGDD) (Ver apdo. 4.8 de este documento).

4.7 ENCARGADO DEL TRATAMIENTO

El encargado del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento (Art. 2.8 RGPD).

Las relaciones entre el responsable y el encargado deben formalizarse en un contrato o en un acto jurídico que vincule al encargado respecto al responsable.

El contenido mínimo del contrato debe prever los siguientes aspectos:

- Objeto, duración, naturaliza y finalidad del tratamiento.
- Tipo de datos personales y categorías de interesados.
- Obligaciones y derechos del responsable.
- Obligación del encargado de:

  - Tratar los datos personales únicamente siguiendo instrucciones documentadas del responsable.
  - Garantizar que las personas autorizadas para tratar los datos personales se hayan comprometido a respetar la confidencialidad.
  - Tomar las medidas necesarias para garantizar un nivel de seguridad adecuado al riesgo.
  - No recurrir a otro encargado sin la autorización previa por escrito, específica o general, del responsable.
  - Asistir al responsable en el ejercicio de los derechos de los interesados.
  - Garantizar el cumplimiento de las obligaciones de notificación de violaciones de la seguridad de los datos personales a la autoridad de control y al interesado y de la realización de una evaluación de impacto de las actividades de tratamiento y consulta previa a la autoridad de control, cuando proceda.
- suprimir o devolver, a elección del responsable, todos los datos personales una vez que finalice la prestación de servicios de tratamiento.

Al margen del contrato que le vincule con el responsable, el encargado tiene obligaciones propias:

1. Mantener un registro de actividades de tratamiento.
2. Determinar las medidas de seguridad aplicables a los tratamientos que realizan para garantizar un nivel de seguridad adecuado al riesgo.
3. Designar un Delegado de Protección de Datos, cuando sea necesario. (ver apdo. 4.8 *Delegado de Protección de Datos*).

4.8 DELEGADO DE PROTECCIÓN DE DATOS

El Delegado de Protección de Datos (DPD o DPO) es la persona, física o jurídica, especialista en protección de datos. Será designado por el responsable y el encargado del tratamiento atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos (Art. 37.5 RGPD).

Tanto los responsables como lo encargados del tratamiento tienen la obligación de designar a un DPD cuando se trate de una de las siguientes entidades (LOPDGDD Art. 34):

1. Los colegios profesionales y sus consejos generales.
2. Los centros docentes de todos los niveles, así como las Universidades públicas y privadas.
3. Las entidades que exploten redes y presten servicios de comunicaciones electrónicas, cuando traten habitual y sistemáticamente datos personales a gran escala.
4. Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.
5. Entidades de crédito: los bancos, las cajas de ahorros, las cooperativas de crédito y el Instituto de Crédito Oficial (Art. 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito)
6. Los establecimientos financieros de crédito.
7. Las entidades aseguradoras y reaseguradoras.
8. Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.
9. Los distribuidores y comercializadores de energía eléctrica y gas natural.
10. Las entidades responsables de ficheros para la evaluación de solvencia patrimonial y crédito (“ficheros de morosos”) o de los ficheros para la gestión y prevención del fraude (Art.2 Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo).
11. Las entidades que desarrollen actividades de publicidad y prospección comercial, cuando lleven a cabo tratamiento basados en las preferencias de los afectados o realicen actividades de elaboración de perfiles.
12. Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes. Se exceptúan los profesionales de la salud que ejerzan su actividad a título individual.
13. Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.

14. Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.
15. Las empresas de seguridad privada.
16. Las federaciones deportivas cuando traten datos de menores de edad.

Además de los supuestos previstos en el Art. 37.1 del RGPD:

a) El tratamiento lo lleve a cabo una autoridad u organismo público.
b) cuando las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance o fines, requieran una observación habitual y sistemática de interesados a gran escala
c) cuando las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales o de datos relativos a condenas e infracciones penales.

Es posible que, en algunos casos, solo el responsable o el encargado del tratamiento deban designar un DPD, y en otros casos tanto el responsable como el encargado deban designar respectivos DPD que deberán cooperar entre sí[6].

Los responsables y encargados del tratamiento pueden designar un DPD de manera voluntaria, en este caso se aplicarán a su designación, puesto y tareas los mismos requisitos que si la designación hubiera sido obligatoria.

Es recomendable que los responsables y encargados del tratamiento documenten el análisis interno realizado para determinar si debe nombrarse o no un DPD[7], esto dejará constancia que se aplican las medidas técnicas y organizativas apropiadas para garantizar y demostrar que el tratamiento se realiza conforme a la legislación.

---

[6] GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. Apartado 2.2. (https://www.aepd.es/media/criterios/wp243rev01-es.pdf)
[7] GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. Directrices sobre los delegados de protección de datos. (https://www.aepd.es/media/criterios/wp243rev01-es.pdf)

4.8.1 PUBLICACIÓN, COMUNICACIÓN Y CONSULTA

El responsable y encargado del tratamiento publicarán los datos de contacto del delegado de protección de datos (Art 37.7 RGPD).

La finalidad de este requisito es garantizar que los interesados, tanto internos como externos a la organización, y las autoridades de control puedan contactar de forma fácil y directa con el DPD.

El DPD está obligado a mantener el secreto o confidencialidad en lo que respecta al desempeño de sus funciones.

Los datos de contacto del DPD deben incluir información que permita a los interesados y a las autoridades de control comunicarse con este de forma sencilla:

- Dirección postal
- Número de teléfono específico
- Dirección de correo electrónico específica
- Formulario de contacto específico dirigido al DPD en el sitio web de la organización

Como buena práctica el Grupo de Trabajo del artículo 29 recomienda que las organizaciones informen a sus empleados del nombre y datos de contacto del DPD. Por ejemplo, puede publicarse en la intranet de la organización o en el directorio telefónico corporativo.

Los responsables y encargados del tratamiento deberán comunicar en el plazo de diez días a la Agencia Española de Protección de Datos, o a las autoridades autonómicas de protección de datos cuando corresponda, las designaciones, nombramientos y ceses de los delegados de protección de datos (Art. 34.3 LOPDGDD).

La AEPD ha elaborado la “Guía rápida de comunicación del Delegado de Protección de Datos” que indica los pasos a seguir para la comunicación del DPD a través de su sede electrónica.

https://www.aepd.es/media/guias/guia-rapida-dpd.pdf

La Agencia Española de Protección de datos y las autoridades autonómicas de protección de datos deben mantener una lista de los delegados de protección de datos que será accesible por medios electrónicos.

Desde la dirección https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/consultaDPD.jsf se puede acceder a la lista de DPD registrados en la AEPD.

4.8.2 FUNCIONES DEL DELEGADO DE PROTECCIÓN DE DATOS

Según el artículo 39 del RGPD, el delegado de protección de datos, tendrá como mínimo las siguientes funciones:

1. Supervisar el cumplimiento de la normativa
   - Recabar información para determinar las actividades de tratamiento.
   - Analizar y comprobar la conformidad con la normativa de las actividades de tratamiento.
   - Informar, asesorar y emitir recomendaciones al responsable o encargado del tratamiento.
2. Asesorar al responsable en la realización de las evaluaciones de impacto.
   - Si debe llevarse a cabo o no.
   - Qué metodología seguir para llevarla a cabo.
   - Si debe hacerse en la propia organización o subcontratarse.
   - Qué medidas, técnicas y organizativas, deben aplicarse para minimizar los riesgos.
   - Si las conclusiones de la evaluación de impacto son conformes al RGPD.

3. Cooperar con la autoridad de control y actuar como punto de contacto de la misma.

Figura 11 Obligaciones de las figuras del tratamiento

4.9 TRANSFERENCIAS INTERNACIONALES DE DATOS

Las transferencias internacionales de datos suponen un flujo de datos personales desde el territorio español a destinatarios establecidos fuera del Espacio Económico Europeo (los países de la Unión Europea más Liechtenstein, Islandia y Noruega). La transmisión de datos entre países del Espacio Económico Europeo no se considera transferencias internacionales.

Los responsables y encargados de tratamiento podrán realizar transferencias internacionales de datos sin necesidad de una autorización de la AEPD en los siguientes supuestos (Capítulo V del RGPD y Título VI de la LOPDGDD).

Países declarados con nivel adecuado por la Comisión Europea

- Suiza, Canadá, Argentina, Guernsey, Isla de Man, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda, Japón, EEUU (sólo entidades certificadas en el Marco del Escudo de Privacidad. www.privacyshield.gov/list)

Países que ofrezca las siguientes garantías

- Un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos
- Normas corporativas vinculantes
- Un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos
- Cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión
- Códigos de conducta, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas las relativas a los derechos de los interesados
- Mecanismos de certificación, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas las relativas a los derechos de los interesados.

Excepciones para situaciones específicas

- El interesado haya dado explícitamente su consentimiento
- La transferencia sea necesaria para la ejecución de un contrato o de medias precontractuales entre el interesado y el responsable
- La transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica
- La transferencia sea necesaria por razones importantes de interés público
- La transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones
- La transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento
- La transferencia se realice desde un registro público que tenga por objeto facilitar información al público

Otras transferencias (autorización AEPD)

- Cuando no se cumpla nada de lo anterior, sólo podrá llevarse a cabo la transferencia si:
  - No es repetitiva
  - afecta solo a un número limitado de interesados
  - es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado
  - el responsable del tratamiento evalúe las circunstancias del tratamiento y ofrezca las garantías apropiadas.

Figura 12 Supuestos transferencias internacionales de datos personales

4.9.1 CLOUD COMPUTING (COMPUTACIÓN EN LA NUBE)

El cloud computing es una nueva tecnología que ofrece servicios a través de internet: soluciones de base de datos, correo electrónico, almacenamiento, aplicaciones informáticas…

El proveedor de estos servicios puede encontrarse, prácticamente, en cualquier lugar del mundo. Por lo que, si los datos están localizados en países que no pertenecen al Espacio Económico Europeo habría una transferencia internacional de datos.

El cliente del cloud computing actúa como responsable del tratamiento, mientras que el proveedor del servicio lo hace como encargado del tratamiento.

Antes de la contratación de los servicios debe verificarse las condiciones en las que se prestan los mismos con el fin de determinar si ofrecen un nivel adecuado de cumplimiento: ubicación del tratamiento, información proporcionada, políticas de seguridad, derechos del usuario, obligaciones legales…

Guía para clientes que contraten servicios de cloud computing

https://www.aepd.es/media/guias/guia-cloud-clientes.pdf

4.10 REGISTRO DE ACTIVIDADES DE TRATAMIENTO

Hasta la entrada en vigor del RGPD la normativa, en cuanto al tratamiento de datos de personales, de aplicación en España, recogía como primera obligación del responsable inscribir los ficheros de datos personales empleados en su actividad ante el Registro General de Protección de Datos de la AEPD. El responsable debía describir qué datos recogía el fichero, con qué fin, de quién se recogen, qué medidas de seguridad se tomaban, si el fichero era automatizado, manual o mixto y si los datos iban a cederse a terceros o si iban a transferirse fuera del Espacio Económico Europeo.

A partir de la entrada en vigor de la nueva normativa, el responsable y el encargado del tratamiento, deberán llevar un registro de todas las actividades que la organización realiza sobre los datos de carácter personal. El registro de actividades de tratamiento deberá tener en cuenta todos los colectivos, tanto de los empleados como de personas implicadas en las actividades de la organización (clientes, proveedores, pacientes…).

Según el Art. 30 de RGPD el registro de actividades de tratamiento no será obligatorio para las empresas u organizaciones que empleen a menos de 250 personas, a menos que el tratamiento que realizan:

- Pueda suponer un riesgo para los derechos y libertades de los interesados.
- No sea ocasional.
- Incluya categorías especiales de datos o datos relativos a condenas e infracciones penales.

La aplicación del RGPD estipula que cada responsable llevará un registro de las actividades de tratamiento sobre datos de carácter personal efectuadas bajo su responsabilidad. Corresponde a cada organización decidir el nivel de agregación o segregación para elaborar el registro de actividades de tratamiento teniendo en cuenta sus finalidades, las bases jurídicas y los grupos de interesados.

Según el art. 30.1 del RGPD y del art. 31 de la LOPDGDD, el contenido del registro de actividades para el responsable debe ser:

Figura 13 Registro de Actividades de Tratamiento para el responsable

Según el art. 30.2 del RGPD cada encargado llevará un registro de todas las categorías de actividades efectuadas por cuenta de un responsable. El contenido de este registro de actividades debe contener:

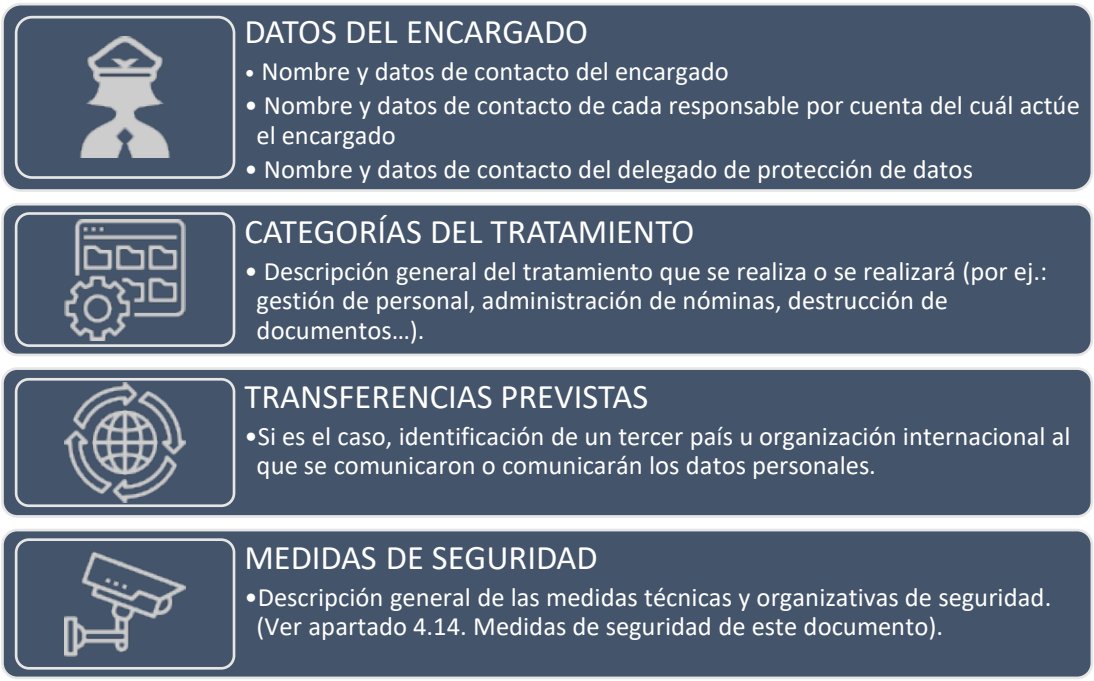


Figura 14 Registro de Actividades de Tratamiento del encargado

Los registros de actividades de tratamiento, tanto del responsable como del encargado, deberán constar por escrito, incluso en formato electrónico.

4.11 PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO[8]

La protección de datos desde el diseño hace referencia a las medidas técnicas y organizativas (ver apdo. 4.14 *Medidas de seguridad*) que el responsable del tratamiento debe aplicar en las primeras fases del diseño de las operaciones de tratamiento con el fin de asegurar la integridad y confidencialidad de los datos personales.

El uso de la seudonimización y de cifrado de datos son ejemplos de medidas técnicas que se deben tener en cuenta durante la fase de diseño de las operaciones de tratamiento.

Por otro lado, los responsables del tratamiento aplicarán las medidas técnicas y organizativas con el fin de garantizar que, por defecto, los datos personales objeto de tratamiento se rijan por los principios de protección de datos (ver

[8] Artículo 25 RGPD

apdo. 4.4 *Principios de protección de datos*). Es decir, por defecto sólo serán tratados los datos necesarios para cada uno de los fines específicos (minimización de datos y limitación de la finalidad), mantenidos de forma que se permita la identificación de los interesados solo durante el tiempo necesario (plazo de conservación) y accesibles únicamente por las personas autorizadas (confidencialidad). Por defecto debe garantizarse que los datos personales no sean accesibles a un número indefinido de personas físicas.

Un ejemplo sería que la configuración de privacidad por defecto de las redes sociales no permitiese el acceso al perfil a un número indefinido de personas.

4.12 ANÁLISIS DE RIESGOS

Una de las actividades incluidas en el principio de responsabilidad proactiva que los responsables y encargados del tratamiento deben tener en cuenta al tratar datos personales, es el análisis de riesgos de los tratamientos que quieran llevar a cabo.

La gestión de riesgos es un conjunto de actividades que permite controlar la incertidumbre relativa a una amenaza. Estas actividades incluyen la identificación y evaluación del riesgo y las medidas para evitarlo o reducir su impacto negativo.

En el contexto de la protección de datos, las amenazas se pueden clasificar en tres tipos atendiendo a la tipología del daño que pueden producir en los datos:

Tabla 1 Clasificación de la amenazas

Confidencialidad	**Acceso ilegítimo a los datos**	**¿Qué daño causaría que los conociera quien no debe?**
Integridad	Modificación no autorizada de los datos	¿Qué perjuicio causaría que estuviera dañado o corrupto?

Disponibilidad	Eliminación de los datos	¿Qué perjuicio causaría no tener un dato o no poder utilizarlo?

Anexo V: Catálogo de amenazas Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD

https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf

El análisis de riesgo debe realizarlo el responsable del tratamiento, antes de comenzar con el mismo, con el fin de definir las medidas de control y seguridad que garanticen los derechos y libertades de las personas.

La Agencia Española de Protección Datos define un posible flujo de trabajo para realizar el análisis de riesgos adecuado al tipo de tratamiento.

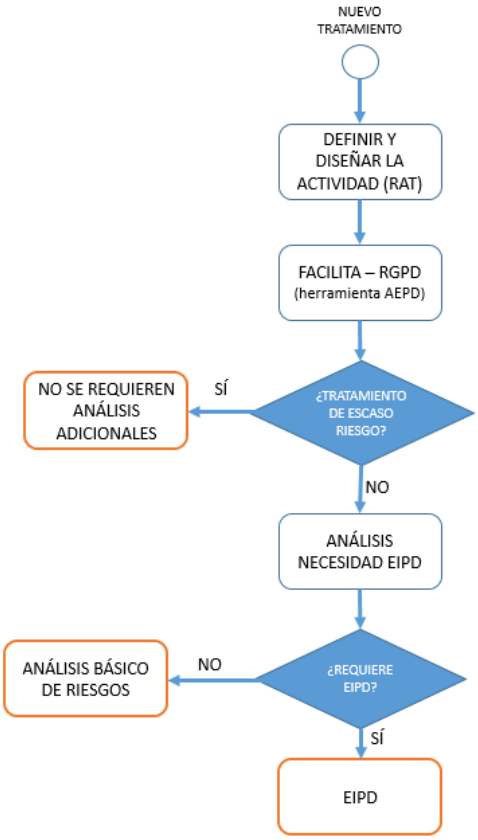


Figura 15 Flujo de trabajo para el análisis de riesgos
(Fuente: Guía Práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD de la AEPD)

4.12.1 DEFINIR Y DISEÑAR LA ACTIVIDAD

Ver apdo. 4.10 *Registro de actividades de tratamiento*.

4.12.2 FACILITA – RGPD

Es una herramienta gratuita de la Agencia Española de Protección de Datos (disponible en el apartado Guías y herramientas de la página web de la Agencia) destinada a empresas que tratan datos de escaso riesgo, como tratamientos de datos de contacto y facturación de clientes o proveedores o el tratamiento de los datos de sus empleados.

La herramienta realiza una serie de preguntas que permiten analizar si el tratamiento se adapta a los requisitos exigidos o si se debe realizar un análisis de riesgo.

La herramienta genera diversos documentos adaptados a la empresa concreta, cláusulas informativas que debe incluir en sus formularios de recogida de datos personales, cláusulas contractuales para anexar a los contratos de encargado de tratamiento, el registro de actividades de tratamiento, y un anexo con medidas de seguridad orientativas consideradas mínimas.

4.12.3 ANÁLISIS DE NECESIDAD DE REALIZAR EVALUACIÓN DE IMPACTO

Si el resultado de la herramienta FACILITA indica que con los datos facilitados el programa no se ajusta a las necesidades de la organización, será necesario realizar un análisis previo para determinar el nivel de riesgo al que está expuesto el tratamiento.

El resultado de este análisis determinará si es necesario o no realizar una Evaluación de Impacto sobre la Protección de Datos (EIPD).

Podemos establecer dos fases en este análisis previo:

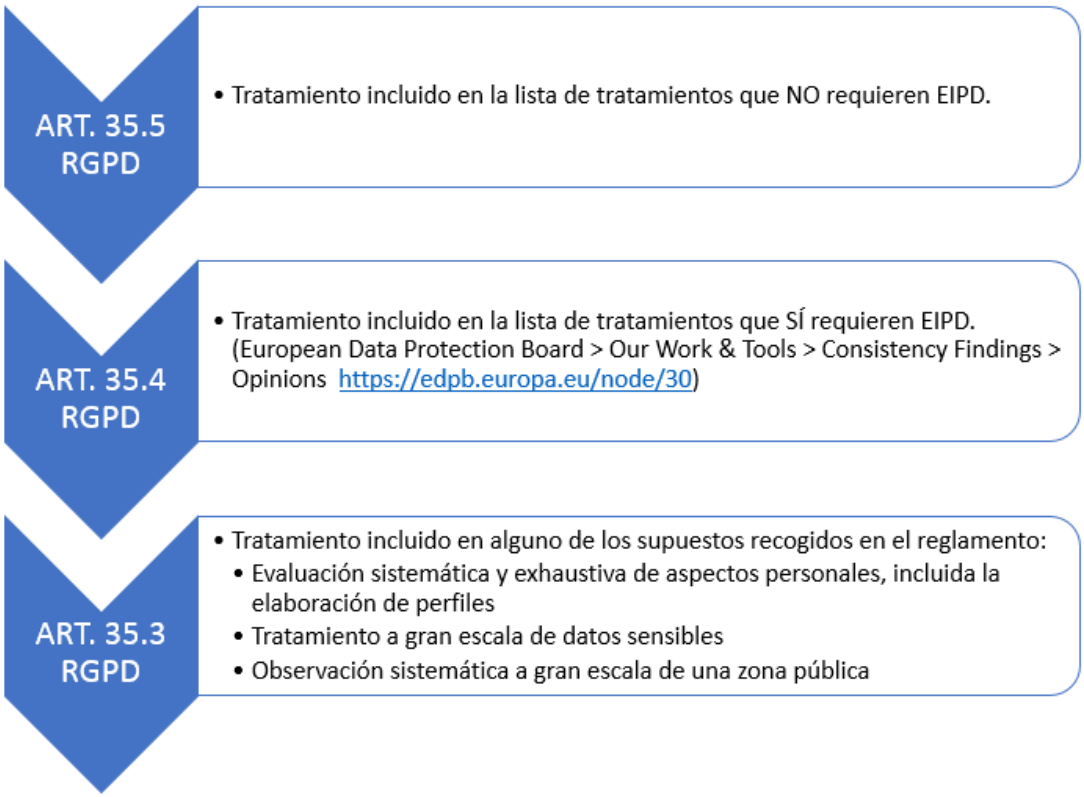
- **Fase I**: Análisis de las listas de tratamientos previstos en los artículos 35.3, 35.4 y 35.5 del RGPD.
  La regulación establece supuestos en los cuales es obligatorio realizar la EIPD sin necesidad de realizar un análisis de riesgos.

Listado de tratamientos de datos personales en los que es obligatoria la realización de una EIPD de la AEPD

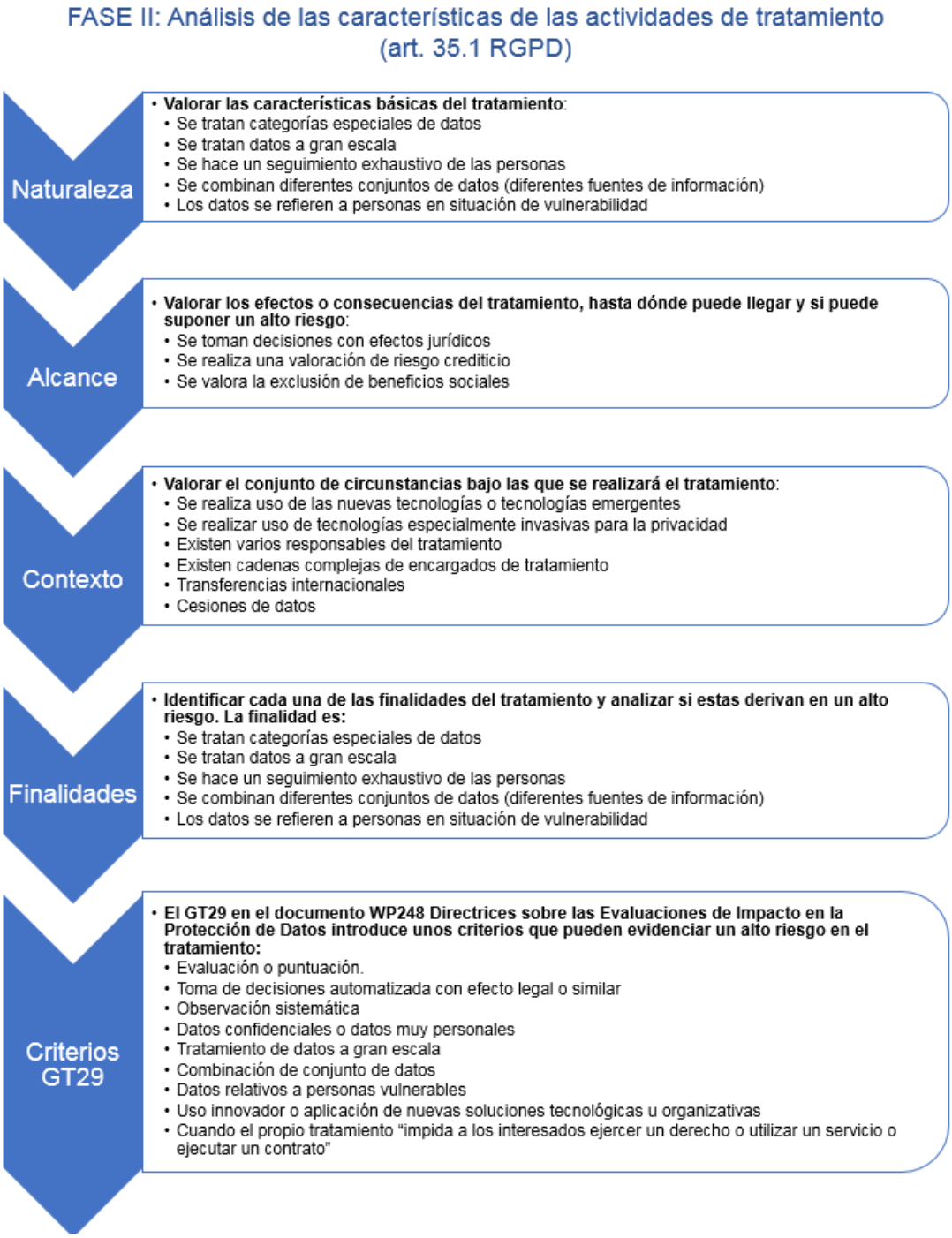
https://www.aepd.es/media/criterios/listas-dpia-es-35-4.pdf

https://edpb.europa.eu/node/30

FASE I: Análisis de las listas de tratamientos previstos en la regulación



- **Fase II**: Análisis de las características de las actividades de tratamiento según los aspectos previstos en el artículo 35.1 del RGPD (naturaleza, alcance, contexto y fines del tratamiento).



El GT29 considera que cuantos más de los criterios cumpla un tratamiento más probable es que suponga un alto riesgo para los derechos y libertades de los interesados.

EIPD obligatoria:

- Un banco que analiza a sus clientes utilizando una base de datos de referencia de crédito.
- Un hospital antes de poner en funcionamiento una nueva base de datos de información sanitaria con los datos de salud de los pacientes.
- Un operador de autobuses antes de instalar cámaras en sus autobuses para controlar el comportamiento de los conductores y pasajeros.

EIPD no obligatoria:

- Un médico de familia que trata datos personales de sus pacientes. No es necesario ya que el tratamiento no se realiza a gran escala.

Fuente: Comisión Europea de Protección de Datos.

Anexo I: Plantilla de análisis de la necesidad de realización de una EIPD

https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf

4.12.4 ANÁLISIS BÁSICO DE RIESGOS

Si el análisis de necesidad de realizar una EIPD determina que las actividades de tratamiento no requieren una EIPD, es posible realizar un análisis básico de riesgos.

El análisis básico de riesgos es un análisis de mínimos que permite determinar las medidas técnicas y organizativas que garanticen los derechos y libertades de los interesados, simplificando el proceso de análisis de riesgos en aquellas actividades de tratamiento con baja exposición al riesgo.

DESCRIPCIÓN DE LAS ACTIVIDADES DE TRATAMIENTO

La descripción de las actividades de tratamiento permite obtener un conocimiento de ciclo de vida de los datos, de las actividades realizadas y de cualquier elemento que intervenga en las mismas.

Las etapas del ciclo de vida de los datos y los elementos que intervienen en cada una de ellas son:

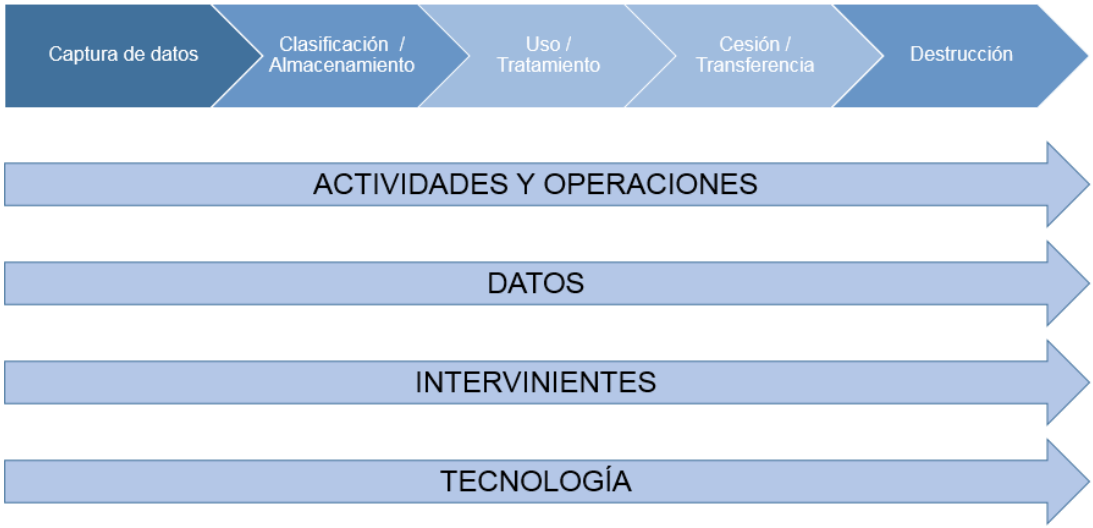


Figura 16 Ciclo de vida de los datos personales

Actividades u operaciones: En el análisis básico de riesgos, las actividades de tratamiento se agrupan por procesos comunes expuestos a riesgos similares. Esta agrupación simplifica el análisis y permite establecer medidas de seguridad por defecto.

Podemos establecer diferentes criterios de agrupación, por ejemplo:

- Procesos que con soporte en la misma tecnología.
- Actividades de tratamiento con finalidades similares sobre grupos de individuos diferentes.

Datos: Se deben identificar los datos de carácter personal tratados o manipulados durante el tratamiento Para cada tipología de datos (identificativos, profesionales, financieros…) debe establecerse su categoría (datos especiales) y su grado de importancia dentro de las actividades de

tratamiento, estableciendo si es imprescindible o no (principio de minimización de datos).

Intervinientes: Son las personas físicas o jurídicas que, de manera individual o colectiva, están implicadas en las actividades del tratamiento y cuyas funciones y responsabilidades están definidas y delimitadas claramente. Por ejemplo: responsable del tratamiento, áreas o empleados de las organizaciones que participen en el procesado de los datos, encargados del tratamiento…

Tecnología: Se debe identificar los elementos tecnológicos, tanto hardware como software, implicados en las actividades de tratamiento a un alto nivel. Por ejemplo: distintas tecnologías (cloud, bases de datos, servidores), aplicaciones, dispositivos y/o técnicas empleadas de procesamiento de datos.

Anexo II: Plantilla de descripción de las actividades de tratamiento

https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf

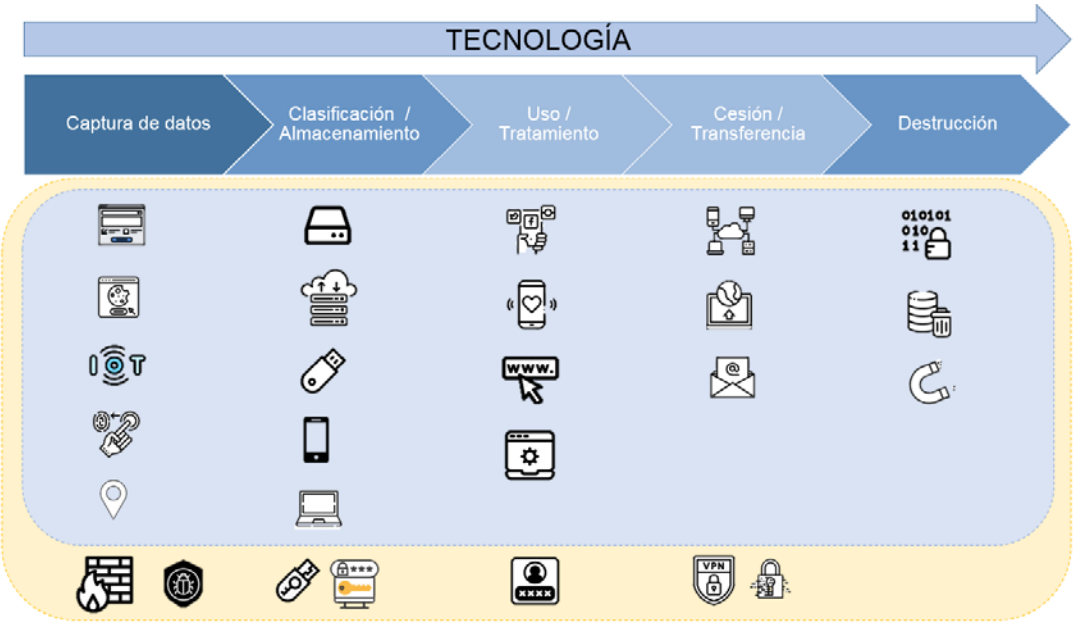


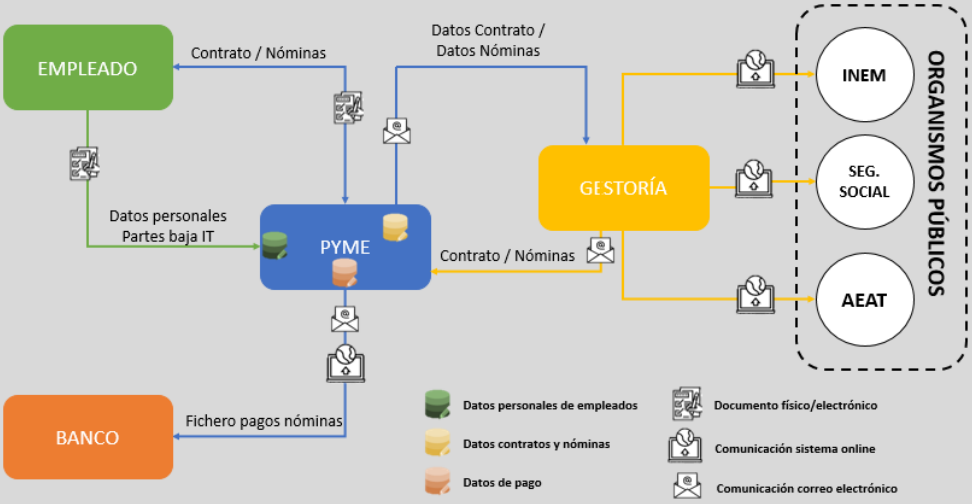
Figura 17 La tecnología en el ciclo de vida de las actividades de tratamiento

EJEMPLO PRÁCTICO – DESCRIPCIÓN ACTIVIDADES DEL TRATAMIENTO

El primer paso es identificar los flujos de datos personales y los sistemas que se utilizan para su almacenamiento y procesamiento.

Si todavía no existen los sistemas, atendiendo al principio de protección de datos desde el diseño y por defecto, estos se deben definir teniendo en cuenta medidas que garanticen la minimización de los datos dependiendo de cada uno de los tratamientos y la seudonimización.

En el proceso de gestión de Recursos Humanos distinguimos cinco entidades que se comunican entre sí con la finalidad de llevar a cabo la elaboración de contratos y nóminas.



En el diagrama se pueden observar los flujos de datos personales que existen entre las diferentes entidades y la tecnología utilizada en la transmisión o comunicación de la información.

Dentro de la gestión de RRHH, distinguiremos dos actividades principales:

- Elaboración de contratos laborales
- Elaboración de nóminas

La descripción de las actividades de tratamiento, nos ayudarán a tener un conocimiento detallado del proceso.

La finalidad de la descripción de las actividades de tratamiento es identificar todas las operaciones de tratamiento y detallar todos los elementos que intervienen a lo largo de todo el ciclo de vida de los datos. Este detalle nos permitirá:

- delimitar cuáles son los datos necesarios para el objetivo de la actividad
- los intervinientes y sus funciones en cada una de las etapas
- las tecnologías utilizadas

Realizaremos un único análisis de riesgo que agrupe las actividades de elaboración de contratos y nóminas, ya que a simple vista puede entenderse que trata datos similares expuestos a los mismos riesgos y para cuyo tratamiento se utilizan las mismas tecnologías.

CICLO DE VIDA DE LOS DATOS

Para la documentar el ciclo de vida de los datos asociados a las actividades de tratamiento, utilizamos la plantilla que se puede encontrar en el ANEXO II de la Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD.

IDENTIFICACIÓN DEL PROCESO: ELABORAR CONTRATOS LABORALES

		CICLO DE VIDA DE LOS DATOS				
		CAPTURA DATOS	CLASIFICACIÓN / ALMACENAMIENTO	USO / TRATAMIENTO	CESIÓN / TRANSFERENCIA	DESTRUCCIÓN
ELEMENTOS QUE INTERVIENEN EN LAS OPERACIONES	ACTIVIDADES	• Rellenar formulario electrónico • Recoger datos	• Almacenar datos • Almacenar contrato • Almacenar reporte	• Procesar datos • Comunicar datos organismos públicos	• Transferir datos a encargado	• Borrar datos
	DATOS	• Identificativos • Domicilio	• Identificativos • Domicilio • Contrato • Comunicaciones organismos públicos	• Identificativos • Domicilio • Contrato	• Identificativos • Domicilio • Contrato	• Identificativos • Domicilio • Contrato
	INTERVINIENTES	• Interesado •Responsable	• Responsable • Encargado	• Encargado • Organismos públicos	• Responsable • Encargado • Organismos públicos	• Responsable • Encargado
	TECNOLOGÍAS	• Formulario electrónico	• Nube • Ordenador personal • Software gestión del encargado	•Software gestión del encargado • Sistemas propios organismos públicos	• Nube • Correo electrónico • Sistemas propios organismos públicos	

ACTIVIDADES

Las actividades identificadas en la descripción de la actividad de tratamiento de datos para elaborar los contratos laborales son las siguientes:

- **Rellenar formulario electrónico:** El empleado (interesado) rellenará un formulario electrónico (formato PDF o en cualquier formato de procesador de texto) con los datos necesarios para la elaboración del contrato.
- **Recoger datos:** El empresario (responsable del tratamiento) o en quien delegue, recogerá los datos facilitados por el empleado.
- **Almacenar datos:** Los datos facilitados por el empleado serán almacenados para su posterior tratamiento y uso.
- **Almacenar contrato:** Los contratos elaborados también se almacenarán.
- **Almacenar reporte:** Los reportes generados por los organismos públicos en el proceso de comunicación del contrato serán almacenados, tanto por el encargado como por el responsable.
- **Procesar datos:** Esta actividad corresponde al tratamiento que debe hacerse de los datos facilitados por el empleado con el fin de elaborar el contrato.
- **Comunicar datos organismos:** La gestoría (encargado del tratamiento) atenderá a la obligación legal de comunicar los datos de los contratos formalizados a los organismos públicos correspondientes.
- **Transferir datos a encargado:** Esta actividad corresponde con el envío de los datos facilitados por el empleado (interesado) por el empresario (responsable del tratamiento) a la gestoría (encargado del tratamiento) con el fin de que ésta procese los datos para conseguir la finalidad perseguida.
- **Borrar datos:** Una vez finalizado el plazo de conservación establecido por la legislación correspondiente, los datos de los contratos deben ser borrados o disociados.

DATOS

Identificamos los datos personales involucrados en cada una de las actividades identificadas en la descripción del proceso.

Distinguimos tres categorías en los datos facilitados por el empleado, necesarios para la elaboración del contrato laboral: datos identificativos, datos de contacto y datos académicos.

IDENTIFICACIÓN DEL PROCESO: ELABORAR CONTRATOS LABORALES

CATEGORÍA DE DATOS: DATOS IDENTIFICATIVOS

DATOS	DESCRIPCIÓN	ESPECIAL	PRESCINDIBLE
Nombre y apellidos	Nombre y apellidos del empleado	☐	☐
NASS	Nº afiliación Seguridad Social	☐	☐
DNI	Nª de documento identificativo	☐	☐

CATEGORÍA DE DATOS: DATOS DE CONTACTO

DATOS	DESCRIPCIÓN	ESPECIAL	PRESCINDIBLE
Domicilio	Datos del domicilio del empleado	☐	☐
Teléfono/s de contacto	Nª de teléfono de contacto	☐	☒

CATEGORÍA DE DATOS: DATOS ACADÉMICOS

DATOS	DESCRIPCIÓN	ESPECIAL	PRESCINDIBLE
Nivel de estudios	Nivel máximo de estudios del empleado	☐	☐

INTERVINIENTES

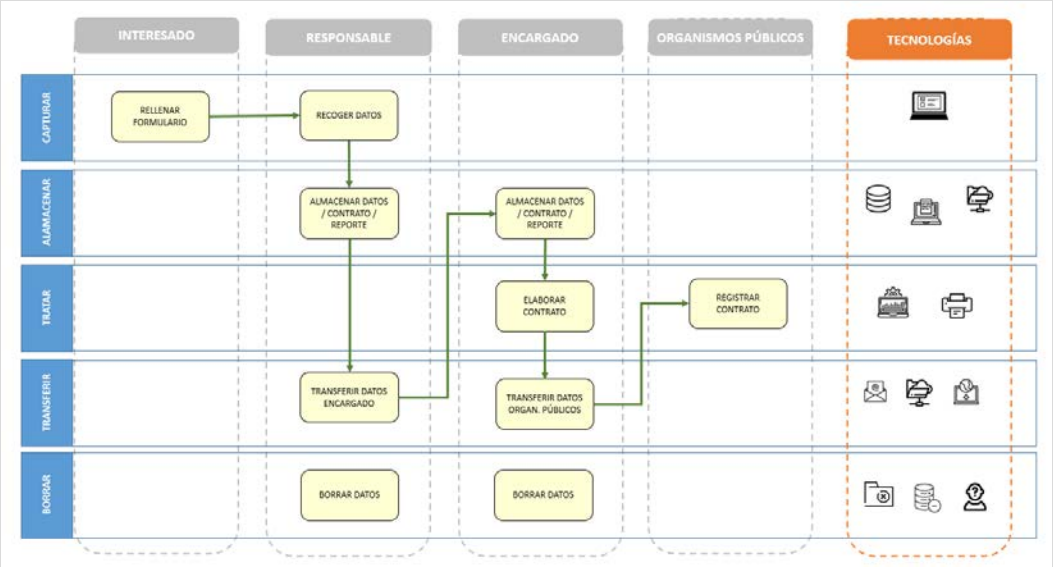
- Interesado: Empleado
- Responsable del tratamiento: Empresario / PYME
- Encargado del tratamiento: Gestoría
- Tercero: Gestoría, organismos públicos

TECNOLOGÍAS

TECNOLOGÍA	ICONO	DESCRIPCIÓN	EJEMPLOS
Formulario electrónico		Formulario online o en cualquier formato electrónico	PDF, Excel, Word...
Almacenamiento en base de datos		Almacenamiento en base de datos estructurada	Access, SQL Server...
Almacenamiento en PC		Almacenamiento de ficheros en ordenador personal o cualquier otro dispositivo móvil	Ordenador personal, memoria USB, DC, DVD...
Almacenamiento en la nube		Almacenamiento o envío de datos utilizando un servicio de almacenamiento en la nube	Google Drive, DropBox, Microsoft OneDrive, Amazon Cloud Drive, Dataprius...
Software específico		Procesamiento de datos con software específico	Para gestión laboral: Navision, Grupo Castilla, A3...
Impresión		Impresión de datos	
Correo electrónico		Envío o transferencia de datos por correo electrónico	Servicios de correo electrónico como Gmail, Outlook...
Aplicación web		Envío o transferencia de datos mediante una aplicación web específica	Contrat@ (comunicaciones al SEPE)
Anonimización		Tratamiento de anonimización de los datos	solución CRM GDPR Compliance de SAGE

DIAGRAMA DE FLUJO DE LOS DATOS PERSONALES

En el siguiente diagrama se representan cada una de las operaciones que tienen lugar durante el desarrollo del proceso de elaboración de contratos durante todo el ciclo de vida de los datos e identificando los intervinientes y las tecnologías utilizadas en cada una de las fases del mismo.



GESTIÓN DE RIESGOS POR DEFECTO

En este caso, en el que las actividades de tratamiento están expuestas a un nivel de riesgo medio o bajo, el proceso de gestión de riesgos se puede simplificar centrándonos en aquellos riesgos más relevantes que pueden afectar a las actividades de tratamiento.

Los principales riesgos para los derechos y libertades de las personas físicas se pueden agrupar en dos dimensiones:

- **Riesgos asociados a la protección de la información.** Integridad, disponibilidad y confidencialidad de los datos personales.
- **Riesgos asociados al cumplimiento de los requisitos regulatorios** relacionados con los derechos y libertades de los interesados. Garantizar el ejercicio de los derechos de los interesados y los principios relativos al tratamiento.

Para cada actividad de tratamiento, se deben identificar los riesgos situados dentro de las dimensiones de protección de datos. A continuación, para cada uno de los riesgos identificados, se deben establecer medidas de seguridad y control que reduzcan su exposición al riesgo.

Listado de cumplimiento normativo elaborado por la AEPD que identifica los aspectos a tener en cuenta en los procesos de análisis de riesgos y de EIPD

https://www.aepd.es/media/guias/guia-listado-de-cumplimiento-del-rgpd.pdf

Ejemplo:

Tipología del riesgo	Riesgo	Medidas de control
Integridad	Modificación o alteración de datos personales no intencionada.	◆ Perfiles de acceso diferenciados. ◆ Monitorización de amenazas en red.
Disponibilidad	Pérdida o borrado no intencionado de los datos personales.	◆ Copias de seguridad ◆ Almacenamiento en diferentes ubicaciones
Confidencialidad	Acceso no autorizado a los datos personales	◆ Mecanismos de control de acceso. ◆ Segmentación de la red.
Ejercicio de los derechos	Ausencia de procedimientos para el ejercicio de los derechos.	◆ Procedimientos y canales para el ejercicio de los derechos.
Principios relativos al tratamiento	Tratamiento ilícito de los datos personales.	◆ Monitorización de uso de los datos personales.

Los riesgos identificados y las medidas de control establecidas deben documentarse, con el objetivo de justificar la evaluación de riesgos realizada.

Una adecuada gestión de riesgos requiere la monitorización continua de los riesgos y la evaluación periódica de la efectividad de las medidas de control definidas.

Es recomendable revisar el análisis de riesgos ante cualquier cambio significativo en las actividades de tratamiento.

Anexo III: Plantilla para documentar el análisis básico de riesgos.

https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf

EJEMPLO PRÁCTICO – IDENTIFICACIÓN DE RIESGOS Y AMENAZAS

La AEPD ha elabora un listado de cumplimiento normativo que facilita la identificación de los aspectos que se deben tener en cuenta a la hora del proceso de análisis de riesgos. (https://www.aepd.es/media/guias/guia-listado-de-cumplimiento-del-rgpd.pdf).

En este apartado, nos centraremos en la identificación de los riesgos y amenazas asociados a la protección de la información, integridad disponibilidad y confidencialidad; dejando al margen los riesgos asociados al cumplimiento de los requisitos regulatorios, garantizar el ejercicio de los derechos de los interesados y el cumplimiento de los principios relativos al tratamiento.

A continuación, detallamos algunos de los riesgos identificados asociados a la protección de la información en las actividades de elaboración de contratos y nóminas:

TIPOLOGÍA DEL RIESGO	DESCRIPCIÓN DEL RIESGOS IDENTIFICADO	MEDIDAS DE CONTROL
Integridad de los datos personales	Modificación o alteración de los datos personales no intencionada	Definir perfiles de acceso a la información
Disponibilidad de los datos personales	Pérdida o borrado no intencionado de datos personales	Realizar copias de seguridad
Confidencialidad de los datos personales	Acceso no autorizado a datos personales	Segmentar de la red

Para la identificación de las amenazas debemos tener en cuenta las operaciones llevadas a cabo en cada una de las etapas del ciclo de vida de los datos. Identificar una amenaza consiste en identificar la fuente del escenario que puede producir un perjuicio para los derechos y libertades de los interesados.

Pasamos a detallar las posibles amenazas y riesgos que pueden identificarse en los procesos de Elaboración de contratos y nóminas:

TIPOLOGÍA	ETAPA	AMENAZA IDENTIFICADA	RIESGO
Confidencialidad	Almacenamiento	Pérdida de dispositivo con datos personales	Acceso no autorizado a los datos personales
Confidencialidad	Almacenamiento	Ataque cibernético que permita acceso a información almacenada en la nube	Acceso no autorizado a los datos personales
Confidencialidad	Transmisión	Envío de correo electrónico con datos personales a destinario incorrecto	Acceso no autorizado a los datos personales
Confidencialidad, Integridad y disponibilidad	Almacenamiento	Acceso no autorizado a ordenador personal con datos personales	Modificación o borrado de datos personales. Acceso no autorizado a los datos personales

4.13 EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS

El artículo 35 del RGPD establece que "*cuando sea probable que un tipo de tratamiento […] entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación de impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen riesgos similares*."

Si el análisis de necesidad de realizar una EIPD realizado en el análisis de riesgos (apdo. 4.12.3 *Análisis de necesidad de realizar evaluación de impacto*) ha dado como resultado que sí es necesario realizar la EIPD, deberá realizarse y documentarse.

La EIPD es una herramienta con carácter preventivo que permite identificar, evaluar y gestionar los riesgos a los que están expuestas las actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas físicas. El EIPD permite determinar el nivel de riesgo que conlleva un tratamiento y establecer medidas de control adecuadas para reducirlo hasta un nivel aceptable.

4.13.1 QUÉ DEBE INCLUIR UNA EIPD

El artículo 35.7 del RGPD establece que la EIPD debe incluir como mínimo:

- Una **descripción sistemática** de las operaciones de tratamiento previstas y de los fines del tratamiento.
- Una **evaluación de la necesidad** y proporcionalidad del tratamiento respecto a su finalidad.
- Una **evaluación de los riesgos** para los derechos y libertades de los interesados.
- Las **medidas previstas para afrontar los riesgos**, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales.

4.13.2 METODOLOGÍA

La EIPD debe ser objetiva. Es fundamental disponer de un proceso sistemático a través de una metodología o procedimiento estandarizado de trabajo que permita establecer criterios comunes para garantizar la homogeneidad, repetitividad y comparabilidad en la ejecución de una EIPD.

La AEPD propone la siguiente metodología para la realización de una EIPD:

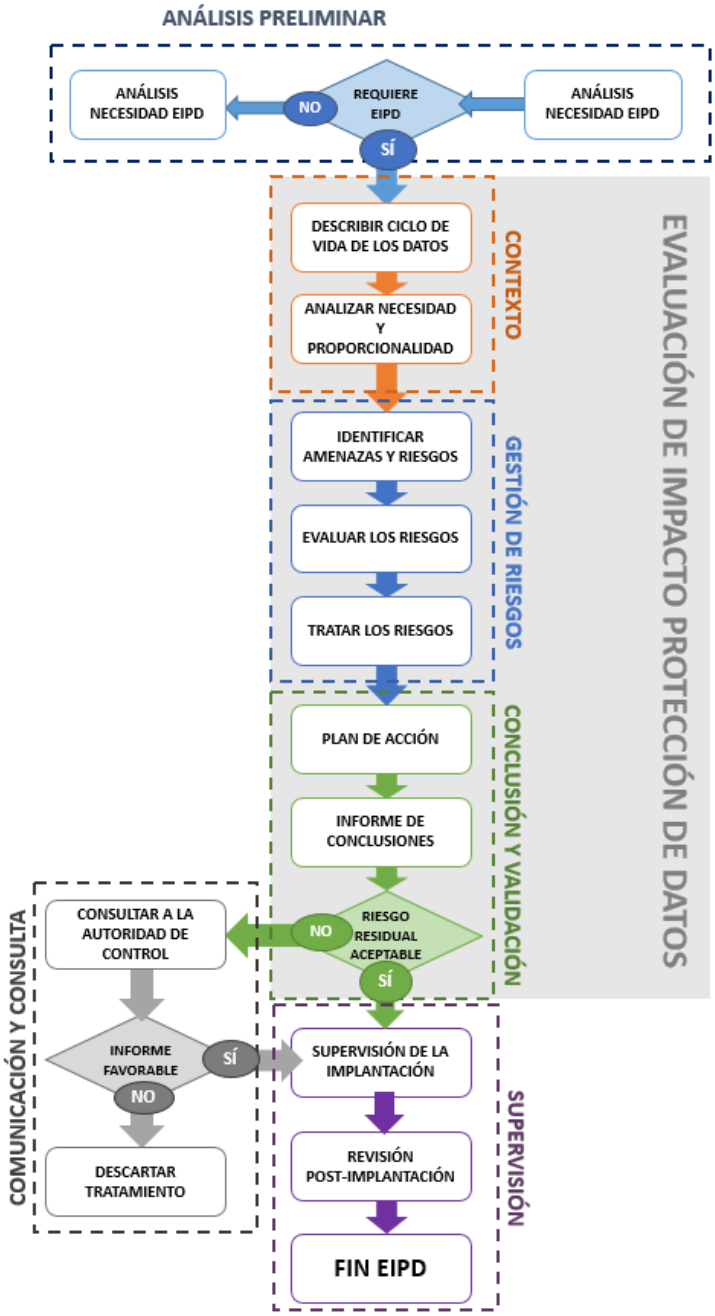


Figura 18 Metodología para realización EIPD
(Fuente: AEPD - Guía práctica para las EIPD sujetas al RGPD)

En la metodología propuesta a las diferentes fases que componen una EIPD, se ha incluido dos fases adicionales. Una fase de comunicación y consulta que será de aplicación únicamente en aquellos casos en los que el resultado de la EIPD conlleve un riesgo elevado para los derechos y libertades de los interesados (Art. 36 del RGPD) y una segunda fase de supervisión que incluye las tareas de la implantación de las medidas de control definidas durante la EIPD.

A continuación, se detalla el contenido de cada una de las fases de esta metodología y sus tareas.

4.13.3 CONTEXTO

Una vez que se ha determinado que es obligatoria la realización de la EIDP, es imprescindible conocer en detalle qué datos concretos se tratarán, qué operaciones de tratamiento se pretenden hacer y en qué circunstancias de forma que se pueda afrontar la gestión de riesgos que pueda conllevar los tratamientos.

El resultado de esta etapa es un documento con el siguiente contenido:

1) Descripción en detalle las operaciones de tratamiento
2) Algunos aspectos generales del tratamiento: la base de legitimación, la finalidad y la necesidad y proporcionalidad de las operaciones de tratamiento.

DESCRIBIR CICLO DE VIDA DE LOS DATOS

Esta tarea de la EIPD es similar a la descrita en el apdo. 4.12.4 *Análisis básico de riesgos / Descripción de las actividades de tratamiento*. La única diferencia significativa es que, al contrario que en el análisis básico de riesgos en el que se podían agrupar las actividades expuestas a riesgos comunes, en el caso de la EIPD debe realizarse la descripción de cada una de las actividades de tratamiento.

También pueden utilizarse diagramas para la identificación los elementos que intervienen en el ciclo de vida de los datos, así como para representar los flujos de datos entre sistemas y roles, el acceso a los datos en cada etapa…

Anexo I: Plantilla de análisis de documentación del ciclo de vida de los datos asociados a las actividades de tratamiento.

https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf

ANALIZAR LA NECESIDAD Y PROPORCIONALIDAD

Para analizar la necesidad y proporcionalidad del tratamiento deben tenerse claramente definidos:

- Qué datos personales se van a tratar. Nombre, apellidos, dirección, datos de salud…
- Con qué finalidad. Identificar las diferentes finalidades para las que se quieren tratar los datos.
- Cómo se van a tratar. Qué se prevé realizar con los datos y los medios con los que se realizará el tratamiento.
- Si son necesarios todos.
- De quién son los datos a tratar (clientes, empleados, potenciales clientes…) y el origen o la fuente de los mismos.
- Cuál es la base legitimadora en la que se basa el tratamiento (ver apdo. 5.1 Licitud, lealtad y transparencia).

Para determinar la necesidad y proporcionalidad de las operaciones de tratamiento previstas, se deben tener en cuenta algunos de los principios de protección de datos (apdo. 4.4 Principios de protección de datos):

1) Limitación de la finalidad: los datos recogidos no se pueden utilizar de manera incompatible con la finalidad para la cual se recogieron.
2) Minimización de datos: los datos que se han previsto tratar deben ser adecuados, pertinentes y limitados a lo que es necesario en relación con las finalidades (no excesivos).
3) Plazo de conservación: los datos no se tienen que mantener más tiempo del necesario para las finalidades del tratamiento.

Para determinar la necesidad y proporcionalidad de las operaciones de tratamiento es fundamental tener clara la finalidad de cada operación de

tratamiento, junto con la finalidad del conjunto del tratamiento y los objetivos que se persiguen.

Anexo II: Plantilla de análisis de la necesidad y proporcionalidad del tratamiento.

https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf

4.13.4 GESTIÓN DE RIESGOS

En el contexto de la protección de datos personales, la gestión de riesgos se concreta en la evaluación de los riesgos que vulneren los derechos y libertades de las personas, como consecuencia del tratamiento de sus datos personales. Es decir, el RGPD establece que la gestión de riesgos va más allá de evaluar la exposición al riesgo de los sistemas de información o de los datos, o de los riesgos para la organización.

IDENTIFICAR AMENAZAS Y RIESGOS

Una amenaza es cualquier factor de riesgo con potencial para provocar un daño o perjuicio a los interesados sobre cuyos datos de carácter personal se realiza un tratamiento.

Para identificar una amenaza debe tenerse en cuenta todo el ciclo de vida de los datos. Identificar una amenaza consiste en identificar la fuente de los escenarios en los que se puede producir un año o una violación de los derechos y libertades de los interesados.

Desde el punto de vista de la protección de datos, las amenazas se pueden clasificar en tres tipos atendiendo a la tipología de daño que pueden producir en los datos:

- Acceso ilegítimo a los datos → **confidencialidad**
- Modificación no autorizada de los datos → **integridad**
- Eliminación de los datos → **disponibilidad**

Un riesgo es la posibilidad que se materialice una amenaza y las consecuencias negativas que conllevaría dicha materialización.

Las amenazas y riesgos están directamente relacionados. Para identificar y evaluar un riesgo se debe considerar siempre la amenaza que lo puede originar.

Anexo V: Catálogo de amenazas.

https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf

EVALUAR LOS RIESGOS

A la hora de evaluar los riesgos que un tratamiento puede tener sobre los derechos y libertades de los interesados, se debe tener en cuenta:

- La **probabilidad** de que se produzca la situación que pone en riesgo derechos y libertades como consecuencia del tratamiento de datos personales.
- La **gravedad** (impacto) de las consecuencias si sucede la situación que pone en riesgo derechos y libertades.

Teniendo en cuenta que todo tratamiento conlleva un cierto nivel de riesgo (riesgo inherente), la evaluación de riesgos permite identificar si el tratamiento supone un alto riesgo haciendo una estimación, lo más objetiva posible, del nivel de riesgo en que se sitúan las operaciones de tratamiento o el tratamiento en su conjunto.

Riesgo inherente es el riesgo intrínseco de cada actividad, sin tener en cuenta las medidas de control que lo minimicen o reduzcan su nivel de exposición.

Riesgo Inherente = Probabilidad X Impacto

La AEPD propone una metodología en cuatro niveles para valorar la probabilidad y el impacto.

VALORACIÓN DE LA PROBABILIDAD

La probabilidad se determina en base a las posibilidades que existen de que la amenaza se materialice.

① **Probabilidad despreciable**. La posibilidad de ocurrencia es muy baja, la materialización de la amenaza puede pasar de forma fortuita.

② **Probabilidad limitada**. La posibilidad de ocurrencia es baja, la materialización de la amenaza puede pasar de forma ocasional.

③ **Probabilidad significativa**. La posibilidad de ocurrencia es alta, la materialización de la amenaza puede pasar con bastante frecuencia.

④ **Probabilidad máxima**. La posibilidad de ocurrencia es muy alta, la materialización de la amenaza puede pasar con mucha frecuencia.

VALORACIÓN DEL IMPACTO

El impacto se determina en base a los posibles daños que se puedan producir si la amenaza se materializa. Los daños ocasionados pueden ser de diferente naturaleza: daño físico (daño en la integridad física del interesado), daño material (pérdidas económicas, de patrimonio, de empleo…) y daño moral (depresión, acoso…).

① **Impacto despreciable**. Los interesados no se verán prácticamente afectados o encontrarán alguna pequeña inconveniencia.

② **Impacto limitado.** Los interesados podrán encontrar inconveniencias no significativas.

③ **Impacto significativo**. Los interesados encontrarán consecuencias significativas, que deberían poder superar sin dificultades serias

④ **Impacto máximo**. Los interesados encontrarán consecuencias significativas o incluso graves, que podrán no llegar a superarse.

Para determinar el riesgo inherente asociado a una actividad de tratamiento, es necesario asignar valores a cada uno de los niveles. De esta forma, enfrentando la probabilidad y el impacto, se forma una matriz de riesgo.

Una matriz de riesgo es una representación gráfica del nivel de riesgo en que se sitúa inicialmente la actividad de tratamiento.

PROBABILIDAD					
Máxima	④	4	8	12	16
Significativa	③	3	6	9	12
Limitada	②	2	4	6	8
Despreciable	①	1	2	3	4
		①	②	③	④
		Depreciable	Limitado	Significativo	Máximo
		IMPACTO			

Según la escala de valores definida, se obtiene una posición en la matriz que se corresponde con el riesgo inherente resultado de aplicar la fórmula de estimación del riesgo.

- Riesgo inherente **bajo**
- Riesgo inherente **medio**
- Riesgo inherente **alto**
- Riesgo inherente **muy alto**

TRATAR LOS RIESGOS

Si el resultado de la evaluación de riesgos es un riesgo inaceptable (riesgo alto) se deben definir y establecer medidas de control para disminuir la probabilidad y/o el impacto asociados al riesgo inherente para situar las operaciones de tratamiento en una zona de riesgo aceptable.

Para definir las medidas de control se debe tratar cada riesgo identificado de forma individual y establecer tantas medidas de control como sean necesarias para lograr un nivel de riesgo aceptable.

Las medidas de control pueden ser de diferentes tipos:

- **Organizativas**: medidas asociadas a procedimientos, a la organización y gobierno de la organización.
- **Legales**: medidas asociadas al cumplimiento normativo.
- **Técnicas**: medidas que permiten velar por la seguridad física y lógicas de la información.

Una vez que se hayan aplicado las medidas de control se debe evaluar nuevamente los riesgos asociados a la actividad de tratamiento.

El **riesgo residual** es el riesgo al que está expuesto una actividad, considerando las medidas de control definidas para reducirlo.

Riesgo residual = Probabilidad X Impacto

Anexo III: Plantilla de gestión de riesgos.

https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf

4.13.5 CONCLUSIÓN Y VALIDACIÓN

PLAN DE ACCIÓN

El plan de acción es el conjunto de iniciativas que se deben llevar a cabo para implantar los controles que ayuden a reducir el riesgo de una actividad de tratamiento hasta un nivel considerado aceptable.

El plan de acción debe incluir al menos la siguiente información:

- Control
- Descripción del control
- Responsable de implantación
- Plazo de implantación

Si la EIPD se ha realizado sobre un tratamiento nuevo, el plan de acción se debe tener en cuenta durante la fase de definición de requerimientos de la actividad (privacidad desde el diseño).

Si la EIPD se ha realizado sobre un tratamiento ya existente, el responsable del tratamiento debe establecer un plazo máximo en el cual se deben implantar las medidas de control incluidas en el plan de acción. Superado el plazo establecido, si no se han implantado dichas medidas de control, el responsable del tratamiento puede interrumpir el tratamiento hasta su implantación.

Anexo IV: Plantilla de plan de acción y conclusión.

https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf

INFORME DE CONCLUSIONES

El informe final de la EIPD debe integrar todas las actividades realizadas para evaluar el impacto de las operaciones de tratamiento, las recomendaciones para minimizar los riesgos inherentes al tratamiento y las conclusiones.

La conclusión de la EIPD debe realizarse basándose en el nivel de riesgo residual obtenido en la fase de gestión de riesgos, valorando si este es aceptable o si es elevado.

Si la conclusión de la EIPD concluye que la actividad de tratamiento implica un alto riesgo, **no es favorable**, se debe activar el procedimiento de consulta previa a la autoridad de control (Art. 36 del RGPD).

Si la conclusión de la EIPD **es favorable**, la actividad de tratamiento se puede llevar a cabo, siempre y cuando, se implanten las medidas de control del plan de acción.

4.13.6 CONSULTAR A LA AUTORIDAD DE CONTROL

El procedimiento de consulta previa, regulado en el artículo 36 del Reglamento General de Protección de Datos, obliga al responsable del tratamiento a consultar a la autoridad de control (Agencia Española de Protección de Datos) antes de proceder al tratamiento cuando la EIPD muestre que el tratamiento sigue teniendo un alto riesgo para los derechos y libertades de los interesados aún tras aplicar medidas para mitigarlo.

El responsable puede realizar la consulta previa a través de la sede electrónica de la AEPD (Procedimientos electrónicos / Consulta previa al inicio de tratamientos de alto riesgo).

4.13.7 SUPERVISIÓN

Una vez finalizada la EIPD, es fundamental que se realice una adecuada supervisión y una posterior revisión de la implantación de las medidas de control definidas en la misma.

Es recomendable que una figura delegada supervise y garantice que las medidas de control definidas durante la EIPD se implanten adecuadamente antes de llevar a cabo las actividades de tratamiento. También es imprescindible monitorizar las actividades, una vez el tratamiento se está realizando, con el fin de revisar que las estimaciones de impacto son válidas.

4.14 MEDIDAS DE SEGURIDAD[9]

El RGPD (Art. 32 RGPD) obliga a todos los responsables y encargados del tratamiento a aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo. Es decir, las medidas de seguridad a implementar vendrán determinadas por los riesgos asociados a cada tratamiento.

Todo el personal que intervenga en el tratamiento está involucrado en la seguridad de los datos y en garantizar los derechos y libertades de los dueños de los mismos.

Además de proporcionar las garantías sobre los datos, las organizaciones deben poder demostrar que lo hacen correctamente.

Entre las medidas organizativas que deben adoptar las organizaciones están:

- Registros de actividad (ver apdo. 4.10).
- Contratos entre responsable y encargado.
- Nombramiento de un delegado de protección de datos (ver apdo. 4.8).
- Todas las obligaciones que debe cumplir el responsable (ver apdo. 4.6).

Para garantizar la seguridad de los datos en cuanto a su confidencialidad, integridad y disponibilidad deberán aplicarse medidas técnicas que permitan:

[9] Guía “Ganar en competitividad cumpliendo el RGPD” (Instituto Nacional de Ciberseguridad)

- Evitar accesos no autorizados y restringir el acceso a los datos mediante Sistemas de gestión de identidad y autenticación.
- Hacer copias de seguridad.
- Seudonimizar y cifrar los datos mediante herramientas de cifrado.
- Controlar el almacenamiento, los soportes y el acceso a datos para ellos se pueden utilizar soluciones de almacenamiento de datos, gestores documentales e incluso soluciones de BI (Business Intelligence).
- Controlar los dispositivos y soportes con herramientas que permitan hacer inventario de los mismos y del software instalado verificando que este sea legítimo y esté actualizado.
- Utilizar herramientas antifraude y antimalware para proteger los datos en los dispositivos, en el puesto de trabajo, en el correo electrónico y en las comunicaciones.
- Utilizar mecanismos adecuados, como cortafuegos, para la protección de las comunicaciones tanto por cable como inalámbricas.
- Definir un procedimiento de gestión de violaciones de seguridad que permita dar una respuesta rápida y eficaz minimizando las consecuencias.

Las medidas de seguridad a aplicar vendrán determinadas por los resultados del análisis de riesgos que deberá realizarse antes del tratamiento de los datos. En algunos casos se podrán el resultado del análisis de riesgo puede concluir que pueden seguir aplicándose las mismas medias que establecía la LOPD 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal.

Figura 19 Resumen medidas seguridad LOPD

Checklist publicados por el Instituto Nacional de Ciberseguridad de España para ayudar a la PYME a mejorar s ciberseguridad.

https://www.incibe.es/protege-tu-empresa/herramientas/politicas

EJEMPLO PRÁCTICO – MEDIDAS DE SEGURIDAD

Partiendo de la base que el riesgo de los tratamientos llevados a cabo en la actividad de elaboración de contratos y nóminas es escaso, sobre todo teniendo en cuenta que la mayor parte del tratamiento es realizado por el encargado del tratamiento, en este apartado se ofrecen unas medidas de seguridad generales que pueden ser tenidas en cuenta en cualquier actividad de tratamiento de datos personales.

1. **Mantener el software actualizado.** Tanto de los ordenadores como de los dispositivos móviles, de esta forma se mejora su funcionalidad y su seguridad.
2. **Seguridad antimalware.** Debemos mantener protegidos los datos en los dispositivos, en el puesto de trabajo, en el correo electrónico (antipishing y antispam) y en las comunicaciones con la implantación de un sistema antimalware que detecte todo tipo de amenazas, también en tiempo real, y que se actualice automáticamente con las nuevas firmas de malware.
3. **Seguridad de la red.** Internet es una fuente inagotable de amenazas para la seguridad de las redes corporativas, es fundamental mantenerla protegida frente a posibles ataques e intrusiones. Algunas medidas que podemos adoptar son:
   - Restringir los accesos
   - Instalación de hardware que permita aumentar la seguridad, tales como firewall, IPS e IDS.
   - Asegurarnos que todos los equipos conectados a la red están correctamente configurados y con el software antimalware actualizado.
   - Controlar y gestionar el uso de dispositivos móviles, que además de ser una potencial entrada de malware a red son una de las principales amenazas de fuga de información. Posibilidad de bloquear los puertos USB y eliminar las unidades lectoras/grabadoras de los equipos de usuarios.
   - Limitar la navegación.
   - Eliminar cuentas y contraseñas por defecto.

4. **Seguridad de la red wifi.** Puede ser una puerta de acceso a nuestra red corporativa de personas ajenas. Algunas medidas que podemos adoptar son:
    - Cambiar regularmente la contraseña de acceso.
    - Ocultar el nombre de la red (SSID) a dispositivos ajenos a la empresa.
    - Activar el cifrado WPA/WPA2.
    - Evitar el acceso a sistemas y recursos internos de la empresa desde redes wifi públicas abiertas.

5. **Seguridad en movilidad.** Los dispositivos móviles son susceptibles de ser robados o extraviados y con ellos toda la información que contienen o a la que tienen acceso. Para proteger la información contenida en ellos debemos aplicar unas medidas básicas.
    - Proteger el desbloqueo con contraseña segura.
    - Evitar utilizar wifi ajenas, especialmente las públicas.
    - Hacer copias de seguridad de la información periódicamente.
    - Almacenar la información en los dispositivos cifrada.
    - Habilitar el bloqueo del dispositivo de manera remota, la geolocalización del dispositivo y el borrado remoto.
    - Habilitar clave de bios e impedir arranque desde USB o CD en PCs y portátiles.
    - Uso de VPN (redes privadas virtuales) en las comunicaciones.

6. **Seguridad en las comunicaciones por correo electrónico.**
    - Cifrado de correo o comprimir y cifrar los documentos adjuntos.
    - Desactivar HTML de las cuentas críticas o que se encuentran a disposición del público para contactar con nuestra empresa.
    - Utilizar la copia oculta cuando se envíen correos a múltiples destinatarios.

7. **Seguridad en el almacenamiento de la información**
    - En la nube. La solución más segura es cifrar la información y después subirla a la plataforma cloud.
    - En la red corporativa. Establecer controles de acceso a discos y directorios, cifrar la información sensible, copias de seguridad…
    - En el puesto de trabajo. Bloqueo programado de sesión, sistema operativo actualizado, deshabilitar puertos USB…

8. **Desechado o reutilización de soportes y equipos**
    - Los comandos de borrado del sistema operativo o el formateo del dispositivo no son suficiente, ya que realizan el borrado de la "lista de archivos" pero el contenido del archivo no se elimina.
    - Desmagnetización: exponer el dispositivo a un potente campo magnético, esto elimina los datos almacenado él. Se puede aplicar a discos duros, disquetes, cintas magnéticas de backup…
    - Destrucción física: inutilizar el dispositivo. Trituración, desintegración, incineración…
    - Sobre-escritura: consiste en formatear un dispositivo de almacenamiento sobrescribiendo la información con datos vacíos, de manera que la información anterior sea irreconocible.

GESTIÓN Y NOTIFICACIÓN DE VIOLACIONES DE SEGURIDAD[10]

En el marco de la responsabilidad proactiva que establece el RGPD como obligación para los responsables y encargados del tratamiento, se encuentra la notificación de las violaciones de seguridad que puedan suponer un riesgo para los derechos y libertades de las personas físicas a la autoridad de control competente, en el caso de España es la Agencia Española de Protección de Datos.

Según el art. 5.12 del RGPD una violación de la seguridad de datos personales es todo incidente de seguridad que ocasione la destrucción, pérdida, alteración accidental o ilícita de datos personales transmitidos, conservados o tratado de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Entendiendo como:

- *Destrucción*: cuando los datos ya no existen, o ya no existen en una forma que sea de utilidad para el responsable del tratamiento.
- *Daño*: Los datos personales han sido alterados, corrompidos o dejan de estar completos.
- *Pérdida*: los datos pueden seguir existiendo, pero el responsable del tratamiento ha perdido el control o el acceso a ellos, o ya no obran en su poder.
- *El tratamiento no autorizado o ilícito*: puede incluir la divulgación de datos personales a destinatarios no autorizados a recibirlos, el acceso a datos personales por parte de destinatarios no autorizados a acceder a los mismos, o cualquier otra forma de tratamiento que infrinja el RGPD.

[10] Directrices sobre la notificación de las violaciones de la seguridad de los datos personales (GT29)
Guía para la gestión y notificación de brechas de seguridad (AEPD)

Algunos ejemplos de violaciones de seguridad:

- Pérdida o robo de un dispositivo con una copia de la base de datos de clientes de un responsable del tratamiento.
- Cifrado de información utilizando una clave de la que ya no dispones el responsable del tratamiento.
- Envío de un correo con datos personales a un destinatario incorrecto.
- Envío de un correo masivo con las direcciones de los destinatarios visibles.
- Dejarle la contraseña personal a un compañero para acceder a información restringida.
- Acceso a la base de datos personales de hacker.
- Encriptación de discos duros con virus informático.

La notificación de incidencias es tan sólo una de las actividades dentro del proceso de gestión de violaciones de seguridad que, toda empresa u organización, debe definir para poder dar una respuesta rápida y eficaz a un incidente de seguridad minimizando sus consecuencias.

La gestión de las violaciones de seguridad implica directamente a los responsables de seguridad ya que, durante todo el proceso, existe un componente de naturaleza tecnológica enfocado a establecer controles y medidas de seguridad.

La gestión de incidentes o violaciones de seguridad puede dividirse en varias fases y procesos secuenciales en el tiempo.

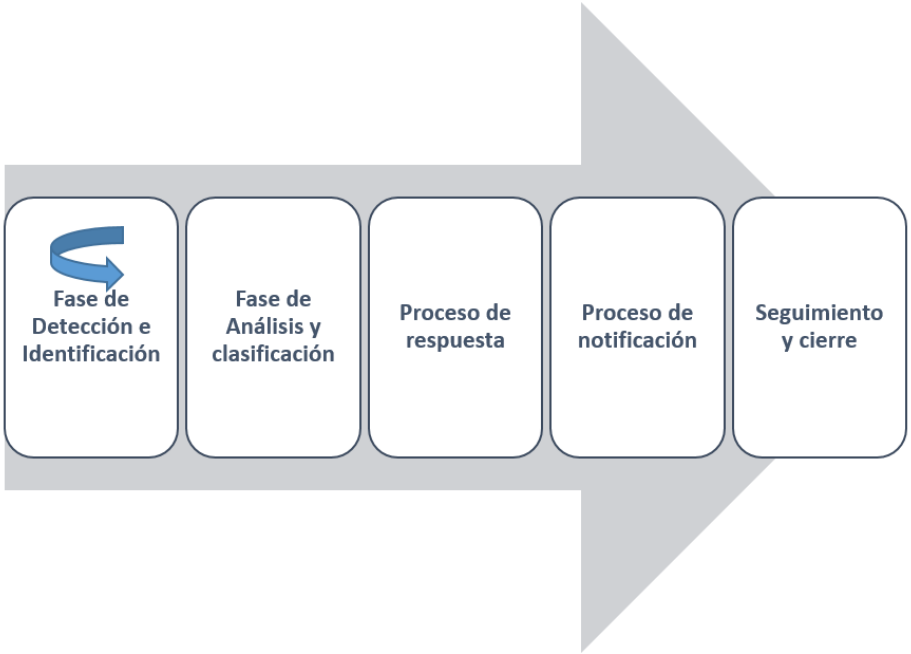


Figura 20 Proceso de gestión de incidentes
(Fuente: Guía para la gestión y notificación de brechas de seguridad de la AEPD)

4.14.1 PROCESO DE DETECCIÓN E IDENTIFICACIÓN

Este proceso consiste en detectar los incidentes de seguridad, debe funcionar de manera continua dentro de las organizaciones.

Durante esta fase se deben definir las situaciones que se consideran violaciones de seguridad de datos personales y las herramientas, mecanismos de detección o sistemas de alerta que permitirán a la organización identificar una brecha de seguridad.

La identificación de un incidente de seguridad puede producirse a través de fuentes internas a la organización o fuentes externas.

SEGURIDAD FÍSICA

FUENTES INTERNAS

- Incumplimiento de medidas de seguridad adoptadas:
  - Políticas de mesas limpias, bloqueos de pantallas, accesos con usuario y contraseña.
  - Detección de intrusos, videovigilancia, control y registro de acceso a zonas restringidas…

Figura 21 Fuentes detección físicas de violaciones de seguridad

CIBERSEGURIDAD

FUENTES INTERNAS

- Notificaciones de usuarios (recepción de correos electrónicos con archivos adjuntos sospechosos, comportamiento extraño de dispositivos, pérdida o robo de dispositivos de almacenamiento...)
- Alertas de software antivirus
- Consumos excesivos y repentinos de memoria o disco en servidores y equipos.
- Picos de tráfico de red en horas inusuales
- Alertas de sistemas de detección/prevención de intrusión (IDS/IPS)
- Análisis de registro de servidores y aplicaciones con intentos de acceso no autorizados

FUENTES EXTERNAS

- Comunicación de un tercero (proveedores de servicios informáticos, proveedores de servicios de internet...)
- Comunicación de un cliente
- Comunicación o notificación de los distintos organismos públicos como el Instituto Nacional de Ciberseguridad (INCIBE), el Centro Criptlógico Nacional (CCN), Fuerzas y Cuerpos de Seguridad del Estado o información publicada en medios de comunicación.

Figura 22 Fuentes de detección de violaciones de ciberseguridad

4.14.2 PROCESO DE ANÁLISIS Y CLASIFICACIÓN

Una vez identificada una violación de seguridad y determinado que afecta a datos personales se debe realizar una clasificación de la misma que posteriormente no permita determinar su peligrosidad y prioridad de actuación. Los factores que deben tenerse en cuenta a la hora de establecer los criterios de clasificación, entre otros:

- Tipo de amenaza: código dañino, intrusiones, fraude…

Clasificación y taxonomía de los ciberincidentes (pág. 12 – 16)

http://www.interior.gob.es/documents/10180/9814700/Gu%C3%ADa+Nacional+de+notificaci%C3%B3n+y+gesti%C3%B3n+de+ciberincidentes.pdf/f01d9ed6-2e14-4fb0-b585-9b0df20f2906

- Origen de la amenaza: interna o externa.
- Categoría de seguridad de los sistemas y datos afectados.

Para establecer la categoría de seguridad de un sistema (BAJA, MEDIA o ALTA) se debe valorar el impacto que tendría un incidente que afecte a la seguridad de la información y de los sistemas, con repercusión en la capacidad organizativa para: alcanzar sus objetivos, proteger los activos a su cargo, cumplir sus obligaciones diarias de servicio, respectar la legalidad vigente, respectar los derechos de las personas.

Para determinar ese impacto hay que tener en cuenta las dimensiones de la seguridad: Disponibilidad, Integridad, Confidencialidad, Autenticidad, y Trazabilidad.

(Según Esquema Nacional de Seguridad – ENS)

- Perfil de los usuarios afectados.
- Número y tipología de los sistemas afectados.
- Impacto que el incidente puede tener en la organización y en los derechos y libertades de los afectados.

- Requerimientos legales y regulatorios.
- “Vector de ataque”, ruta o camino utilizado por el atacante para realizar la violación.

En el contexto de la protección de datos personales, una violación de seguridad puede clasificarse en una o varias de las siguientes categorías:

- *Violación de la confidencialidad*: cuando se produce un acceso no autorizado a los datos personales o estos son revelados de forma no autorizada o accidental. La gravedad depende del número y tipo de partes que han accedido a la información.
- *Violación de la integridad*: se produce una alteración no autorizada o accidental de los datos personales y la alteración puede ser perjudicial para el interesado.
- *Violación de la disponibilidad*: no es posible el acceso a los datos personales. Puede ser temporal cuando los datos son recuperables, pero tardará un periodo de tiempo, o permanente cuando los datos no pueden recuperarse.

Hay pérdida de disponibilidad cuando se produce una interrupción del servicio normal de una organización, por ejemplo, cuando se produce un fallo en el suministro eléctrico.

No constituye una violación de seguridad cuando los datos personales no están disponibles debido a la realización de un mantenimiento planificado del sistema.

Por último, en esta fase de análisis y clasificación, se debe determinar la peligrosidad potencial del incidente y evaluar el nivel de perjuicio que puede causar el incidente a los derechos y libertades de los afectados.

La peligrosidad dependerá de los siguientes factores:

- **Nivel de criticidad** respecto a los sistemas afectados:
  - Crítico. Afecta a datos valiosos, gran volumen y en poco tiempo.
  - Muy alto. Capacidad para afectar a información valiosa en cantidad apreciable.
  - Alto. Capacidad para afectar a información valiosa.
  - Medio. Capacidad para afectar a un volumen apreciable de información.
  - Bajo. Capacidad escasa o nula para afectar a un volumen apreciable de información.
- **Naturaleza, sensibilidad y categorías de los datos personales afectados**:
  - Datos de escaso riesgo. Datos de contacto, de educación, familiares, profesionales, biográficos.
  - Datos de comportamiento. Localización, tráfico, hábitos y preferencias.
  - Datos financieros. Transacciones, posiciones, ingresos, cuentas, facturas.
  - Datos sensibles. De salud, biométricos…
- **Datos legibles/ilegibles**. Datos protegidos mediantes algún sistema de seudonimización o cifrado.
- **Volumen de datos personales**, expresados en cantidad (número de registros, ficheros o documentos) y/o períodos de tiempo.
- **Facilidad de identificación de individuos**.
- **Severidad de las consecuencias para los individuos**. Los daños ocasionados pueden ser de diferente naturaleza: daño físico (daño en la integridad física del interesado), daño material (pérdidas económicas, de patrimonio, de empleo…) y daño moral (depresión, acoso…).
  - Baja. Los interesados no se verán prácticamente afectados (tiempo de reingreso de información, molestias, irritaciones...).

  - Media**.** Los interesados podrán encontrar inconveniencias importantes, que podrán superar sin dificultades (costos adicionales, denegación de acceso a servicios comerciales, miedo, estrés…).
  - Alta. Los interesados encontrarán consecuencias importantes, que deberían poder superar con serias dificultades (listas negras de los bancos, daños a la propiedad, pérdida de empleo, empeoramiento de la salud…).
  - Muy alta. Los interesados encontrarán consecuencias significativas o incluso irreversibles, que podrán no llegar a superarse (exclusión o marginación social, incapacidad para trabajar, dolencias psicológicas o físicas a largo plazo...).
- **Características especiales de los individuos**.
- **Número de individuos afectados**.
- **Características especiales del responsable del tratamiento**, en base a la actividad de la entidad.
- **Perfil de los usuarios afectados**, sus privilegios de acceso a información sensible o confidencial.
- **Impacto** que la brecha puede tener en la organización, desde el punto de vista de la protección de la información, la prestación de los servicios, la conformidad legal y/o la imagen pública.
  - Bajo. Perjuicio limitado
  - Medio. Perjuicio grave.
  - Alto. Perjuicio muy grave.
- **Requerimientos legales y regulatorios**.

4.14.3 PROCESO DE RESPUESTA

La mayoría de las acciones que se lleven a cabo en este proceso serán realizadas por el servicio de informática, que puede formar parte la empresa u organización o estar externalizado.

Las primeras acciones llevadas a cabo en este proceso deben estar encaminadas a mitigar el impacto del incidente (fase de contención), para después proceder a su eliminación en los sistemas afectados (fase de

solución/erradicación) y, finalmente, tratar de restaurar los sistemas a su funcionamiento normal (fase de recuperación).

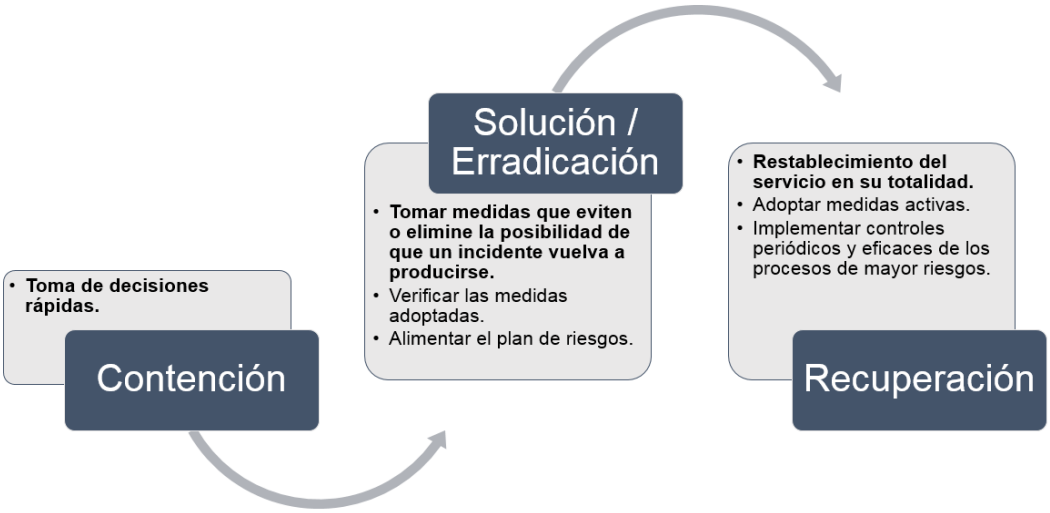


Figura 23 Fases del Proceso de respuesta a violaciones de seguridad

A continuación se detallan algunas medidas o tareas que pueden aplicarse en cada una de las fases:

Tabla 2 Medidas y tareas durante el Proceso de respuesta a violaciones de seguridad

Fases	Medidas / tareas
Contención	• Cambiar las contraseñas de los usuarios con acceso a información privilegiada o confidencial. • Hacer copia del sistema (clonado). • Aislar el sistema utilizado. • Deshabilitar ciertas funciones. • Vigilar la difusión de documentos/datos filtrados en diferentes sitios web y redes sociales.

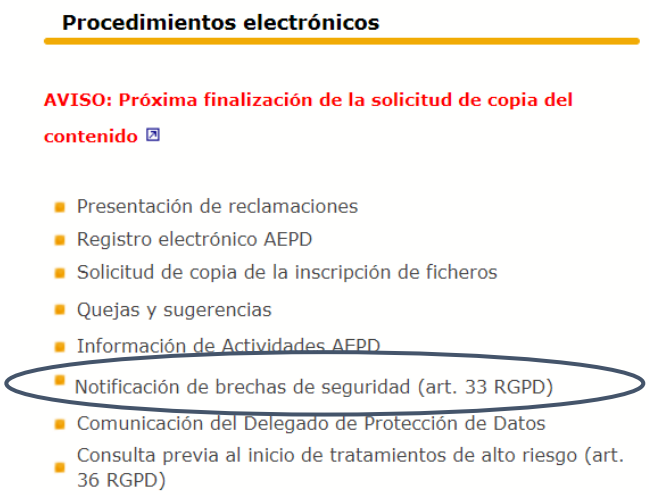
Erradicación	• Definir el proceso de desinfección, basado en firmas, herramientas, nuevas versiones/revisiones de software… y probarlo. • Comprobar la integridad de todos los datos almacenados en el sistema. • Revisar la correcta planificación y actualización de los motores y firmas de antivirus. • Restaurar conexiones y privilegios paulatinamente.
Recuperación	• Garantizar el restablecimiento del sistema a la situación previa al incidente. • Revisar el análisis de riesgos. Si ya estaba incluida la amenaza se deben reevaluar las medidas de salvaguarda.

Todo el proceso de respuesta debe quedar documentado. Esta documentación servirá tanto a la comunicación a las partes interesadas como a la elaboración de un informe de respuesta que permita extraer conclusiones.

4.14.4 PROCESO DE NOTIFICACIÓN

El artículo 33 del RGPD establece la obligación por parte del responsable del tratamiento de notificar a la autoridad de control competente (AEPD) cualquier brecha de seguridad, sin dilaciones indebidas y en todo caso en un plazo máximo de 72 horas, a menos que sea improbable que la brecha constituya un riesgo para los derechos y libertades de las personas físicas.

La comunicación puede realizarse a través de la sede electrónica de la AEPD (https://sedeagpd.gob.es/sede-electronica-web/)



O con el modelo que la AEPD ha publicado en su "Guía para la gestión y notificación de brechas de seguridad". (https://www.aepd.es/media/guias/guia-brechas-seguridad.pdf).

El RGPD establece que cuando sea probable que la violación de seguridad entrañe un alto riesgo para los derechos y libertades de las personas físicas, esta debe ser también comunicada al afectado.

4.14.5 SEGUIMIENTO Y CIERRE

El responsable del tratamiento o en quien tenga delegadas las funciones correspondientes, normalmente el DPD, debe comprobar:

- Que las medidas correctoras adoptadas son adecuadas para la resolución de la violación de seguridad y para la minimización del riesgo en caso de que se produzca otras de características similares.
- Que ha concluido el proceso de comunicación a la Autoridad de control y, en su caso, a los posibles afectados.

El cierre de la violación de seguridad requiere la realización de un informe final que detalle la trazabilidad del suceso, análisis valorativo y el impacto final.

4.15 RÉGIMEN SANCIONADOR

El régimen sancionador actual en materia de protección de datos se basa en el Título X de la LOPDGDD y en Artículo 83 del RGPD.

El régimen sancionador establecido por la LOPDGDD (art. 70) se aplica a:

- Los responsables de los tratamientos.
- Los encargados de los tratamientos.
- Los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la UE.
- Las entidades de certificación.
- Las entidades acreditadas de supervisión de los códigos de conducta.

No será de aplicación a los delegados de protección de datos.

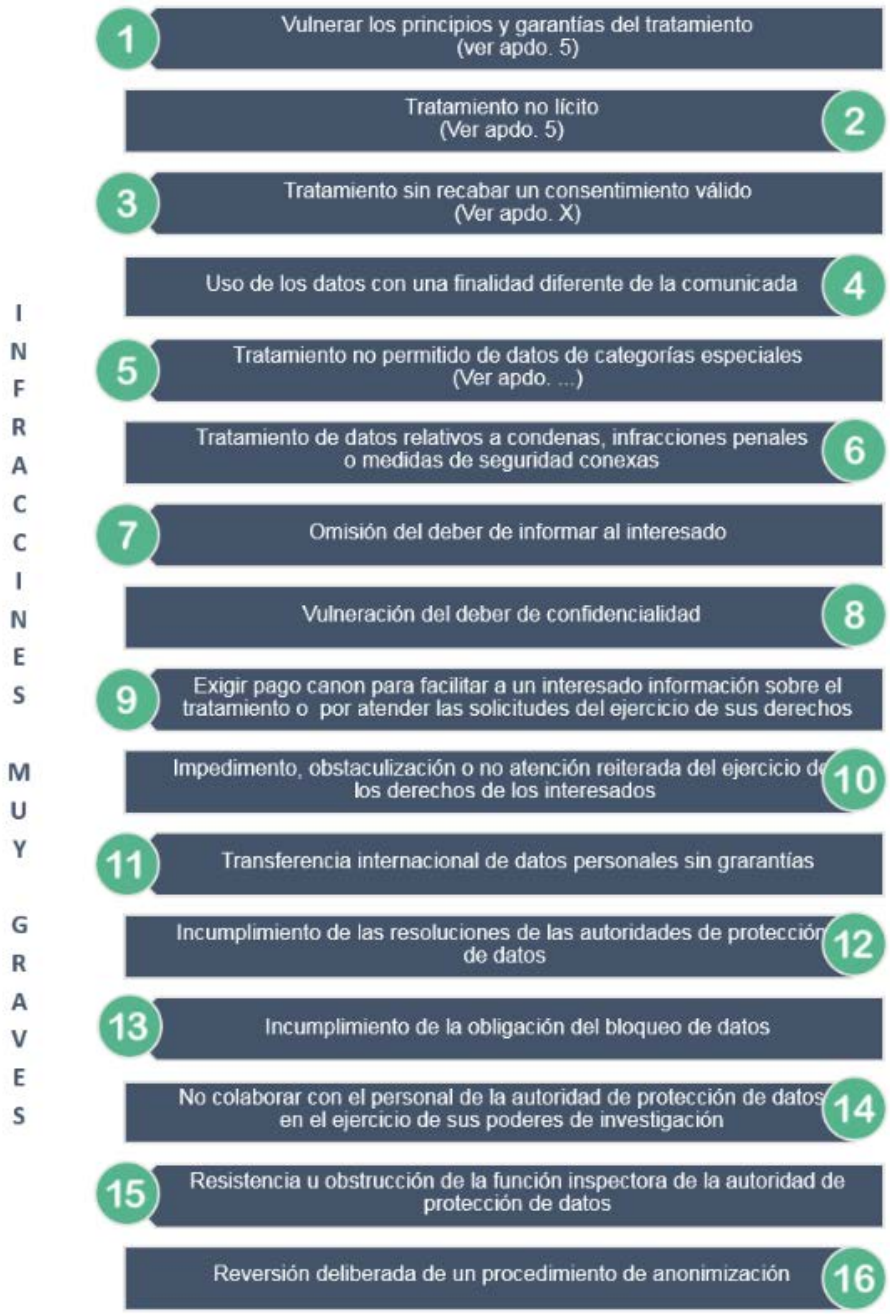
4.15.1 INFRACCIONES MUY GRAVES

(Art. 72 LOPDGDD y Art. 83.5 RGPD)

Se consideran infracciones muy graves y prescribirán a los tres años las que supongan una vulneración sustancial de:

- Los principios básicos del tratamiento, incluidas las condiciones para el consentimiento.
- Los derechos de los interesados.
- Las transferencias de datos personales a un destinatario de un tercer país o una organización internacional.
- El incumplimiento de una resolución o de una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de la autoridad de control.

Estas infracciones se sancionarán con multas administrativas de 20.000.000 € como máximo o de una cuantía equivalente al 4% como máximo de volumen de negocio total anual global del ejercicio anterior, optándose por la de mayor cuantía.



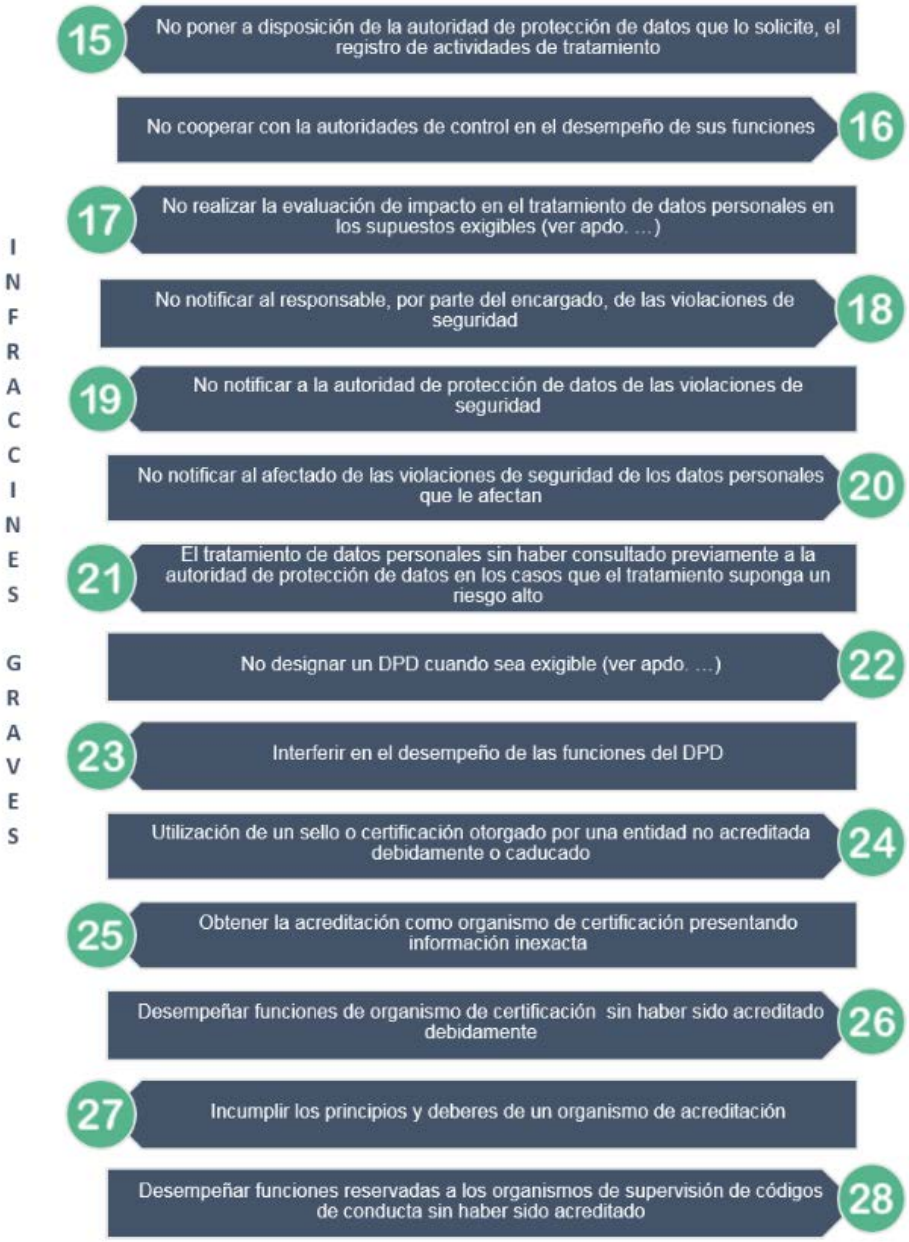
4.15.2 INFRACCIONES GRAVES

(Art. 73 LOPDGDD y Art. 83.4 RGPD)

Se consideran infracciones graves y prescribirán a los dos años las que supongan una vulneración de las siguientes disposiciones:

- Las obligaciones del responsable y del encargado.
- Las obligaciones de los organismos de certificación.
- Las obligaciones de la autoridad de control.

Estas infracciones se sancionarán con multas administrativas de 10.000.000 € como máximo o de una cuantía equivalente al 2% como máximo de volumen de negocio total anual global del ejercicio anterior, optándose por la de mayor cuantía.


INFRACCIONES GRAVES
15
No poner a disposición de la autoridad de protección de datos que lo solicite, el registro de actividades de tratamiento
16
No cooperar con la autoridades de control en el desempeño de sus funciones
17
No realizar la evaluación de impacto en el tratamiento de datos personales en los supuestos exigibles (ver apdo. ...)
18
No notificar al responsable, por parte del encargado, de las violaciones de seguridad
19
No notificar a la autoridad de protección de datos de las violaciones de seguridad
20
No notificar al afectado de las violaciones de seguridad de los datos personales que le afectan
21
El tratamiento de datos personales sin haber consultado previamente a la autoridad de protección de datos en los casos que el tratamiento suponga un riesgo alto
22
No designar un DPD cuando sea exigible (ver apdo. ...)
23
Interferir en el desempeño de las funciones del DPD
24
Utilización de un sello o certificación otorgado por una entidad no acreditada debidamente o caducado
25
Obtener la acreditación como organismo de certificación presentando información inexacta
26
Desempeñar funciones de organismo de certificación sin haber sido acreditado debidamente
27
Incumplir los principios y deberes de un organismo de acreditación
28
Desempeñar funciones reservadas a los organismos de supervisión de códigos de conducta sin haber sido acreditado

4.15.3 INFRACCIONES LEVES

(Art. 74 LOPDGDD y Art.83.4 y 83.5 RGPD)

Se consideran leves y prescribirán al año las infracciones de carácter meramente de las disposiciones descritas en los apartados de infracciones muy graves y graves.

5 DISCUSIÓN

Teniendo en cuenta que uno de los principales desencadenantes que han hecho necesario un nuevo desarrollo de la legislación de protección de datos, no debemos dejar pasar por alto que los profesionales de las tecnologías de la información somos parte esencial en la aplicación de la protección de datos.

A lo largo de todo el RGPD y, por tanto, de la ley española que lo transpone, se hace referencia a que se deben adoptar las medidas organizativas y técnicas con el fin de garantizar que el tratamiento se realiza conforme al Reglamento. Esto da a entender que la parte técnica del tratamiento tiene tanta importancia como la parte legislativa y de organización.

Con el RGPD se ha pasado de un modelo reactivo, como era la Directiva 95/46/CE que se deroga con la entrada en vigor del RGPD, a un modelo proactivo que encuentra su principal base en el enfoque de riesgos.

En este punto, en el enfoque de riesgos, es donde nosotros, los profesionales de las TIC tenemos mucho que aportar ya que llevamos años trabajando esta área en diferentes campos de actuación como son la arquitectura de las redes de comunicaciones, la ciberseguridad, el desarrollo de aplicaciones que tratan o acceden a datos…

Tenemos ante nosotros un escenario que nos plantea oportunidades de desarrollo que hasta ahora nos había mantenido en un segundo plano.

6 CONCLUSIONES

El resultado del trabajo ha sido la elaboración de una guía de referencia en el que se han abordado aspectos de los tres ámbitos de aplicación de la protección de datos personales.

Por un lado, se han desarrollado y explicado, las obligaciones a las que obliga la nueva legislación en el ámbito legal a los responsables del tratamiento:

- Cuáles son las bases de legitimización válidas para el tratamiento de datos personales.
- Los principios de protección de datos.
- Cómo debe ser la comunicación con los interesados.

También se han desarrollado las obligaciones del ámbito organizativo:

- El Delegado de Protección de datos.
- El registro de actividades.
- Notificación de violaciones de seguridad.

Y, por último, se han abordado los aspectos técnicos que están enfocados a garantizar un tratamiento de datos seguro desde antes de su inicio:

- Descripción de las actividades de tratamiento.
- Descripción del ciclo de vida de los datos personales.
- Y, se han desarrollado en detalle, los procesos de análisis de riesgos y evaluación de impacto relativa a la protección de datos y las medidas de seguridad.

Los procesos de análisis de riesgos y las medidas de seguridad a aplicar en los tratamientos, se han desarrollado en mayor profundidad y detalle por tratarse uno de los principales pilares de la nueva legislación, el enfoque de riesgos, y ser los que más componente técnico llevan asociados.

En todos los apartados se ha intentado dar ejemplos prácticos y enlaces a fuentes oficiales (Agencia Española de Protección de Datos, Comisión Europea de Protección de Datos, Instituto Nacional de Ciberseguridad) donde se puede ampliar la información ofrecida, con el fin de clarificar la teoría.

REFERENCIAS BIBLIOGRÁFICAS

Legislación

- Europa. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). *Diario Oficial de la Unión Europea,* 4 de mayo de 2016, núm. L119, P.1
- España. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Boletín Oficial del Estado*, 6 de diciembre de 2018, núm. 294, P. 119788.

Páginas web

- Agencia Española de Protección de Datos. *www.aepd.es*.
- Instituto Nacional de Ciberseguridad. *www.incibe.es*.
- Autoridad Catalana de Protección de Datos. *www.apdcat.cat*.
- Comité Europeo de Protección de Datos. *www.edp.europa.eu*.

Otros

- Grupo de Trabajo sobre protección de datos del artículo 29. Directrices sobre la aplicación y la fijación de multas administrativas a efectos del Reglamento 2016/679. 3 de octubre de 2017.
- Grupo de Trabajo sobre protección de datos del artículo 29. Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679. 3 de octubre de 2017.
- Grupo de Trabajo sobre protección de datos del artículo 29. Directrices sobre el derecho a la portabilidad de los datos. 13 de diciembre de 2016.
- Grupo de Trabajo sobre protección de datos del artículo 29. Directrices para determinar la autoridad de control principal de un responsable o encargado del tratamiento. 13 de diciembre de 2016.

- Grupo de Trabajo sobre protección de datos del artículo 29. Directrices sobre los delegados de protección de datos (DPD). 13 de diciembre de 2016.
- Grupo de Trabajo sobre protección de datos del artículo 29. Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679. 3 de octubre de 2017.
- Grupo de Trabajo sobre protección de datos del artículo 29. Dictamen sobre técnicas de anonimización. 10 de abril de 2014.
- Grupo de Trabajo sobre protección de datos del artículo 29. Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679. 28 de noviembre de 2017.
- Grupo de Trabajo sobre protección de datos del artículo 29. Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento “entraña probablemente un alto riesgo” a efectos del Reglamento (UE) 2016/679. 4 de abril de 2017.
- Grupo de Trabajo sobre protección de datos del artículo 29. Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679. 29 de noviembre de 2017.
- Agencia Española de Protección de Datos. Guía Práctica de Análisis de riesgos en los tratamientos de datos personales sujetos al RGPD.
- Agencia Española de Protección de Datos. Guía para clientes que contraten servicios de Cloud Computing. 2018.
- Agencia Española de Protección de Datos. Guía para el ciudadano.
- Agencia Española de Protección de Datos, Autoridad Catalana de Protección de Datos, Agencia Vasca de Protección de Datos. Guía para el cumplimiento del deber de informar.
- Agencia Española de Protección de Datos. Guía práctica para las evaluaciones de impacto en la protección de datos sujetas al RGPD.
- Agencia Española de Protección de Datos. Guía para la gestión y notificación de brechas de seguridad.

- Agencia Española de Protección de Datos, Autoridad Catalana de Protección de Datos, Agencia Vasca de Protección de Datos. Guía para responsables de tratamiento.
- Agencia Española de Protección de Datos. Orientaciones y garantías en los procedimientos de anonimización de datos personales.
- Instituto Nacional de Ciberseguridad. Copias de seguridad: una guía de aproximación para el empresario.
- Instituto Nacional de Ciberseguridad. Ganar en competitividad cumpliendo el RGPD: una guía de aproximación para el empresario.
- Instituto Nacional de Ciberseguridad. Guía de almacenamiento seguro de la información: una aproximación para el empresario.
- Instituto Nacional de Ciberseguridad. Cloud Computing: una guía de aproximación para el empresario.
- Consejo Nacional de Ciberseguridad, Gobierno de España. Guía Nacional de notificación y gestión de ciberincidentes.

ANEXO

HERRAMIENTAS PARA LA IMPLEMENTACIÓN DE LAS MEDIDAS DE SEGURIDAD

GESTORES DE CONTRASEÑAS	
KeePass	https://portableapps.com/apps/utilities/keepass_portable
LastPass	https://www.lastpass.com/

CIFRADO DE DATOS	
AxCrypt	https://www.axcrypt.net/es/
AES Crypt	https://www.aescrypt.com/download/
BitLocker	Herramienta totalmente gratuita incorporada desde el sistema operativo Windows Vista para sistemas operativos de escritorio y desde Windows Server 2008 para las versiones de servidor.
VeraCrypt	https://www.veracrypt.fr/en/Downloads.html

ANTI-MALWARE	
Malwarebytes	https://es.malwarebytes.com/
kaspersky	https://www.kaspersky.es/small-business-security
avast	https://www.avast.com/en-us/business/solutions/endpoint-protection
AVG	https://www.avg.com/en-gb/business-security#comparison
Bitdefender	https://www.bitdefender.co.uk/

La página web del Instituto Nacional de Ciberseguridad (incibe) dispone de un buscador de soluciones que puede ayudarnos a buscar herramientas para la implementación de las medidas de seguridad que debemos implantar en nuestra empresa:

https://www.incibe.es/protege-tu-empresa/catalogo-de-ciberseguridad/buscador-soluciones