GUÍA BÁSICA DE PROTECCIÓN DE DATOS PERSONALES PARA ENTIDADES DE ACCIÓN SOCIAL

Plataforma de ONG de Acción Social

Guía básica de protección de datos personales para entidades de acción social

Edita
Plataforma de ONG de Acción Social
Tribulete 18, 1ª Planta. 28012 Madrid.
91 535 10 26
info@plataformaong.org

Deposito legal
M-35683-2023

Coordinación
Plataforma de ONG de Acción Social
Oscar D. Perea Arias
Mónica Luque Rodríguez

Autora
Mercedes Gutiérrez Duque

Financiado por
Ministerio de Derechos Sociales y Agenda 2030
Secretaría de Estado de Derechos Sociales
Dirección General de Diversidad Familiar y Servicios Sociales
Plataforma de ONG de Acción Social

Diseño y maquetación
Materia Gris S.L.

Edición española disponible en
www.plataformaong.org

Índice

Prólogo

La Plataforma de ONG de Acción Social presenta la Guía Básica de Protección de Datos Personales para entidades de Acción Social. Con ella, pretendemos aumentar el conocimiento de la normativa fundamental que cada organización, independientemente de su tamaño, tiene que incorporar para el logro de una gestión eficaz en materia de protección de datos, así como conocer los principios relativos al tratamiento de los datos, incluyéndose los derechos de las personas interesadas.

La sociedad es cada vez más exigente con las organizaciones sociales, y esto incluye un funcionamiento eficaz del sistema de protección de datos que garantice la protección de los derechos fundamentales de las partes interesadas con la organización. Además, es importante que las organizaciones conozcan el ámbito de aplicación de las normativas que rigen el Reglamento General de Protección de Datos.

Tras las publicaciones anteriores en materia de Cumplimiento Normativo, con el *Manual de elaboración de planes de cumplimiento Normativo para entidades del Tercer Sector de Acción Social,* publicado en 2020, y el *Manual para la implementación de los elementos básicos del Modelo de Cumplimiento Normativo*, publicado en 2021; En el año 2022 se publicaron dos guías: *la Guía básica de Transparencia para entidades de Acción Social y la Guía básica de buen gobierno para entidades de Acción Social.* Por ello, y siguiendo a sus publicaciones predecesoras, ahora presentamos *la Guía básica de Protección de Datos para entidades de Acción Social,* se presenta para dar una herramienta más, que facilite a las entidades sociales el manejo de los datos de las personas con las que trabajan y contactan en su día a día.

La Guía Básica de Protección de datos personales para entidades de Acción Social, está orientada a ser un referente para el Sector y, además, servir de apoyo para que las entidades del Tercer Sector de Acción Social obtengan mecanismos útiles

que les ayuden a gestionar y a hacer un correcto análisis de los datos que tratan, ver con qué finalidad lo hacen y cuál es el tipo de tratamiento que llevan a cabo. Todo ello basándose en el marco legislativo de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y el Reglamento Europeo de Protección de Datos, que describen los principios relativos al tratamiento.

Esta guía es fruto del esfuerzo y del trabajo que viene desarrollando la Comisión de Transparencia, Buen Gobierno e Innovación de la Plataforma de ONG de Acción Social desde el año 2017. La principal motivación de la puesta en marcha de los proyectos de dicha Comisión es ofrecer herramientas accesibles a las organizaciones, independientemente de su tamaño y ubicación, que actúen como semillas para extender y fortalecer un compromiso común por el Cumplimiento Normativo y por una cultura de Transparencia y Buen Gobierno en todo el Tercer Sector de Acción Social.

El día a día de las organizaciones de Acción Social constituye un sistema de gestión, actividades y operaciones (proyectos o servicios) que muchas veces generan amenazas y riesgos, en lo que respecta al tratamiento de sus datos personales, incluyendo las personas con las que se trabaja, por lo que se considera fundamental disponer de una descripción, detallada del mismo tratamiento de datos, de su contexto así como de los elementos más relevantes que intervienen en dicho tratamiento para poder gestionar los riesgos, con el fin de minimizarlos al máximo.

El proceso de gestión de datos personales implica conocer los principios relativos a su tratamiento, así como conocer desde el ámbito normativo los derechos de la persona interesada, la transparencia de la información, el ámbito de aplicación y el principio de responsabilidad que está dirigida al responsable del tratamiento, que en su caso ha de aplicar medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con la Ley Orgánica y el Régimen General de Protección de Datos.

La Guía básica de Protección de Datos está orientada y diseñada para que las entidades del Tercer Sector de Acción Social obtengan directrices que les ayuden a cumplir la normativa existente en materia de protección de datos en sus organizaciones, de esta manera, desde la Plataforma de ONG, seguimos impulsando una cultura de transparencia, buen gobierno y cumplimiento normativo en el Tercer Sector.

Contar con materiales adaptados a las demandas y necesidades de nuestras entidades, ha llevado a crear esta publicación, que deseo cumpla con las necesidades surgidas en las entidades sociales, así como que sirva de referente en la construcción de un Tercer Sector de Acción Social más solvente, transparente y ético.

Yolanda Besteiro de la Fuente
Presidenta
Plataforma de ONG de Acción Social

01

INTRODUCCIÓN

La Plataforma de ONG de Acción Social es una organización de ámbito estatal, privada, aconfesional y sin ánimo de lucro que trabaja para promover el pleno desarrollo de los derechos sociales y civiles de los colectivos más vulnerables y desprotegidos de nuestro país, ayudando a fortalecer el Tercer Sector de Acción Social.

Una de las áreas de trabajo de la Plataforma se centra en la Gestión de la Calidad, la Transparencia, el Buen Gobierno y el Cumplimiento Normativo. En relación con esta línea de trabajo se han llevado a cabo distintos proyectos y actuaciones tales como el acompañamientos a entidades sociales para la gestión de la calidad, el desarrollo de una **Aplicación de Autoevaluación en la Herramienta de transparencia y buen gobierno,** la publicación del Manual de elaboración de Planes de Cumplimiento Normativo para entidades del Tercer Sector de Acción Social1 y del Manual para la implementación de los elementos básicos del modelo de cumplimiento normativo2, la publicación de una Guía básica de Transparencia para entidades de Acción Social3 y la publicación de una Guía básica de Buen Gobierno para entidades de Acción Social4, formaciones en materia de Cumplimiento Normativo, el fomento del Compromiso por la calidad en el Tercer Sector de Acción Social o el consenso de unas Recomendaciones Éticas del Tercer Sector de Acción Social.

Desde la creación de la Comisión de Transparencia, Buen Gobierno e Innovación de la Plataforma de ONG en el año 2017, se ha creado una línea de trabajo enfocada a la promoción de herramientas para ayudar a las entidades sociales en la implementación de una cultura de transparencia y buen gobierno. Desde la Comisión también se ha trabajado en dar respuesta a los principales aspectos que afectan al Tercer Sector de Acción Social en materia de cumplimiento normativo.

Para un correcto desarrollo de estas actuaciones, la Plataforma de ONG ha establecido alianzas con otras organizaciones del Tercer Sector como la Coordinadora de

1. *Plataforma de ONG de Acción Social (2020). Manual de elaboración de Planes de Cumplimiento normativo para entidades del Tercer Sector de Acción Social.*

2. *Plataforma de ONG de Acción Social (2021). Manual para la implementación de los elementos básicos del Cumplimiento normativo para entidades del Tercer Sector de Acción Social.*

3. *Plataforma de ONG de Acción Social (2022). Guía básica de Transparencia para entidades de Acción Social*

4. *Plataforma de ONG de Acción Social (2022). Guía básica de Buen Gobierno para entidades de Acción Social*

ONG para el Desarrollo España o el Instituto para la Calidad de las ONG (ICONG), y tiene convenios suscritos con diferentes organismos de las administraciones públicas, entre los que se encuentra el Consejo de Transparencia y Buen Gobierno de España.

Fruto del trabajo de esta Comisión de Transparencia, Buen Gobierno e Innovación, desde el año 2020, se está ejecutando un programa de transparencia, buen gobierno y cumplimiento normativo. Durante el año 2023 este programa ha desarrollado varias actuaciones que dan continuidad a los procesos de implementación del marco de cumplimiento normativo en entidades sociales: la elaboración de dos guías, una sobre Protección de Datos en entidades de Acción Social y una Guía básica de gestión y desarrollo organizacional en entidades de Acción Social, la continuidad de la formación en ámbito de Gestión y Elaboración de Planes de Cumplimiento Normativo, y una formación online en relación a los Elementos básicos del Modelo de Cumplimiento Normativo en las entidades del Tercer Sector de Acción Social; así como dos nuevos cursos formativos sobre Transparencia y Buen gobierno en entidades de Acción Social, y la difusión de la herramienta de autoevaluación sobre transparencia y buen gobierno, para las entidades de Acción Social.

El objetivo de la ***Guía Básica de Protección de Datos*** es orientar a las organizaciones del Tercer Sector de Acción Social a la hora de incorporar las directrices que marcan por un lado la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos, y por otro lado el Reglamento Europeo de Protección de Datos. La guía está orientada para que las entidades del Tercer Sector de Acción Social obtengan directrices que les ayuden a cumplir la normativa existente en materia de protección de datos en sus organizaciones. De esta manera, seguimos impulsando una cultura de transparencia, buen gobierno y cumplimiento normativo en el Tercer Sector.

La guía, por tanto, proporciona herramientas y ofrece recomendaciones para que las organizaciones, independientemente de su tamaño y ubicación, dispongan de sistemas de gestión que incorporen los elementos en cuanto a protección de datos se refiere. Esta guía, por tanto, pretende ayudar a las entidades del Tercer Sector de Acción Social, en especial a aquellas que disponen de recursos limitados, a cumplir con los requisitos básicos de la legislación estatal que les es de aplicación y a mejorar su gestión, reduciendo sus riesgos, mejorando su eficiencia, y contribuyendo de este modo a implantar una cultura de cumplimiento normativo en el Tercer Sector.

La elaboración de dos guías una sobre Protección de Datos en entidades de Acción Social y una Guía básica de gestión y desarrollo organizacional en entidades de Acción Social.

02

LEGISLACIÓN EN MATERIA DE PROTECCIÓN DE DATOS

La Protección de Datos de Carácter Personal es un derecho fundamental que tienen todas las personas físicas para garantizar su privacidad e implica el control y poder disponer de su información pública y privada.

No obstante, no es un derecho absoluto, sino que debe estar en equilibrio con otros derechos fundamentales. Este equilibrio se puede conseguir mediante el principio de proporcionalidad. La protección de los datos personales está regulada a nivel europeo, estatal y autonómico.

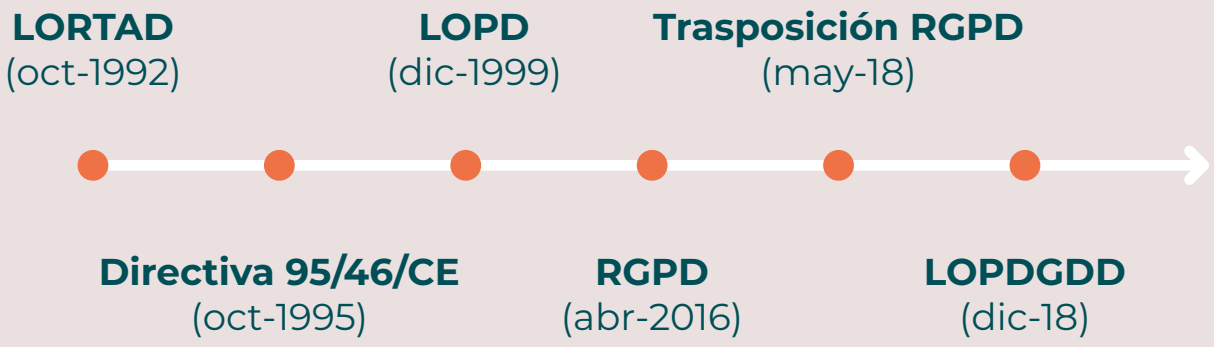


Ilustración 1 Legislación en materia de protección de datos

2.1. LEGISLACIÓN EUROPEA

En la legislación europea el derecho a la protección de datos viene recogido desde los orígenes en la Carta de los Derechos Fundamentales de la Unión Europea[5] y en el Tratado de Funcionamiento de la Unión Europea[6], que establecen que "Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan".

No obstante, la primera normativa específica sobre protección de datos es la Direc-

5. Artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea.

6. Artículo 16.1 del Tratado de Funcionamiento de la Unión Europea.

tiva 95/46/CE, cuyo objetivo era que garantizar el derecho a la protección de datos personales no supusiese un impedimento a la libre circulación de los datos dentro de la Unión Europea, asegurando que, en caso de transferencia internacional de datos, el tratamiento de dichos datos estuviera protegido en el país de destino.

La Directiva 95/46/CE fue derogada por 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. Este Reglamento, vigente actualmente, es de aplicación directa en España y, además de proteger los derechos de la titularidad de los datos personales, establece un nuevo enfoque proactivo a la hora de tratar los datos personales.

2.1.1. REGLAMENTO (UE) 2016/679, DEL PARLAMENTO EUROPEO Y DEL CONSEJO, DE 27 DE ABRIL DE 2016 (RGPD)

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 (RGPD) entró en vigor el 24 de mayo de 2016 y fue de aplicación obligatoria para todos los Estados miembros desde el 25 de mayo de 2018.

Este Reglamento regula el reconocimiento del derecho a la privacidad de toda la ciudadanía de la Unión Europea (UE), independientemente de la nacionalidad o del lugar de residencia, y logra la unificación de la normativa reguladora del libre flujo de información personal.

Los principales aspectos que introduce el RGPD son:

1. Ámbito de aplicación	**2. Responsabilidad proactiva y enfoque de riesgo**	**3. Categorías especiales de datos**	**4. Consentimiento y consentimiento de menores**
5. Derecho de información y otros derechos de las personas interesadas	**6. Registro de actividades de tratamiento**	**7. Evaluación de impacto de protección de datos**	**8. Protección desde el diseño y por defecto**
9. Códigos de conducta y mecanismos de certificación	**10. Delegado de protección de datos**	**11. Medidas de seguridad**	**12. Notificación de brechas de seguridad**

Ilustración 2 Aspectos a destacar del RGPD

1. **Ámbito de aplicación:** En toda la UE y a todas las personas que llevan a cabo tratamientos de datos cuando las actividades de tratamientos están relacionadas con la oferta de bienes, servicios o con el control del comportamiento de las personas que se encuentran en la UE.

2. **Conceptos de responsabilidad proactiva y enfoque de riesgo:** La responsabilidad proactiva requiere que las organizaciones analicen qué datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo. A partir de los resultados del análisis deben determinar qué medidas aplicarán y cómo, dejando documentado todo el proceso para poder demostrarlo ante las personas interesadas y ante las autoridades de supervisión. El enfoque de riesgo implica que las medidas que se van a aplicar estarán ponderadas en función del nivel y tipo de riesgo que los tratamientos presenten.

3. **Nuevas categorías especiales de datos:** Además de los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias, origen racial o étnico, o vida sexual, se incluyen como categorías especiales de datos los datos genéticos[7] y los biométricos[8].

4. **Consentimiento:** Es necesario que la persona interesada preste el consentimiento mediante una declaración inequívoca o una acción afirmativa clara. No son consentimientos válidos las casillas ya marcadas, el consentimiento tácito o la inacción. El consentimiento de las personas menores de edad sólo es válido si tienen más de dieciséis años. Sin embargo, el RGPD permite que los estados miembros de la UE rebajen la edad hasta los trece años.

5. **Derecho de información:** La información es un derecho de las personas afectadas, a las que hay que informar sobre aspectos tales como la base jurídica del tratamiento, el plazo durante el cual se conservarán los datos, el derecho a solicitar la portabilidad o la limitación del tratamiento, el derecho a retirar en cualquier momento el consentimiento que se haya prestado, si la comunicación de datos es un requisito legal o contractual o un requisito necesario para suscribir un contrato, el derecho a presentar una reclamación ante una autoridad de control, entre otros. La información debe ser concisa, transparente, inteligible y de fácil acceso y con un lenguaje claro y sencillo. Además, las personas interesadas tienen derecho de acceso, rectificación, oposición, supresión (conocido como "derecho al olvido"), limitación del tratamiento, portabilidad y de no ser objeto de decisiones individualizadas.

6. **Documentación de las operaciones de tratamiento:** registro de actividades de tratamiento: El RGPD exige que las organizaciones, cuando se den ciertas circunstancias, dispongan de un registro de actividades de tratamiento de datos que llevan a cabo, cuyo contenido mínimo está fijado en el RGPD, y que se tiene que entregar a las Autoridades de Control si lo solicitaran.

7. A De acuerdo al RGPD los datos genéticos son: "datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona".

8. De acuerdo al RGPD los datos biométricos son: "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos".

7. Evaluaciones de impacto relativas a **la protección de datos:** Se debe hacer una Evaluación del Impacto en la Protección de Datos (EIPD) cuando un tratamiento, por su naturaleza, alcance, contexto o fines suponga un alto riesgo para los derechos y libertades de las personas físicas, especialmente cuando se utilicen nuevas tecnologías.

8. **Protección de datos desde el diseño y por defecto:** Implica que se incluyan los principios de protección de datos dentro de las organizaciones a lo largo de toda la vida de los tratamientos de datos que se realicen y que sólo se lleven a cabo los tratamientos de datos realmente necesarios para la consecución de los fines del tratamiento.

9. **Códigos de conducta y mecanismos de certificación:** El RGPD también regula los códigos de conducta que pueden promover las asociaciones y otros organismos para la correcta aplicación del Reglamento. El Reglamento también promueve los mecanismos de certificación, como certificados, sellos o marcas.

10. **Delegado de protección de datos (DPD):** La persona Delegada de Protección de Datos, que puede formar parte de la plantilla de la organización o actuar bajo un contrato de servicios, tendrá funciones en materia de coordinación y control del cumplimiento de la normativa en materia de protección de datos. Sólo será necesario designar un DPD en determinadas circunstancias.

11. **Medidas de seguridad:** El RGPD no establece un listado de las medidas de seguridad que son de aplicación, sino que establece que organización aplicará medidas técnicas y organizativas adecuadas al riesgo que conlleva el tratamiento. Esto implica tener que hacer una evaluación de los riesgos asociados a cada tratamiento, para determinar las medidas de seguridad a implementar.

12. **Notificación de brechas de seguridad:** La organización deberá notificar a la autoridad competente cualquier brecha de seguridad que se haya producido en el plazo de 72 horas desde que ocurra. Además, si la brecha implica un riesgo para las personas interesadas, también se les deberá notificar a ellas. Se considera que existe constancia de una violación de seguridad cuando hay una certeza que se ha producido y se tiene un conocimiento suficiente de la naturaleza y el alcance.

13. **Ventanilla única:** Permite que la ciudadanía y las personas que lleven a cabo tratamientos en el ámbito de aplicación del RGPD tengan una única autoridad de protección de datos como interlocutora.

2.2. LEGISLACIÓN ESTATAL

La Constitución Española fue pionera en el reconocimiento del derecho fundamental a la protección de datos personales ya que en el artículo 18.4 establece que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"[9].

Este derecho fundamental a la protección de datos se plasmó en la Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos personales, conocida como LORTAD, que fue reemplazada por la Ley Orgánica 15/1999, de 5 de diciembre, de protección de datos personales (LOPD). Con fecha 25 de mayo de 2018 se comenzó a aplicar en España 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 (RGPD). Y, finalmente, el 6 de diciembre de 2018 entró en vigor la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales u garantía de derechos digitales (LOPDGDD).

2.2.1. LEY ORGÁNICA 5/1992, DE 29 DE OCTUBRE, REGULADORA DEL TRATAMIENTO AUTOMATIZADO DE DATOS PERSONALES (LORTAD)

La Ley Orgánica 5/1992, de 29 de octubre, Reguladora del Tratamiento Automatizado de Datos Personales (LORTAD) tiene por finalidad hacer frente a los riesgos que para los derechos de la persona puede suponer la recogida y el tratamiento de datos por medios informáticos.

Una de las razones para su aprobación fue la firma en 1990 del Acuerdo de Schengen y del Convenio para la Aplicación del Convenio de Schengen, que exigía que todos los países que quisieran formar parte tenían que implantar un sistema de protección de datos personales.

Los aspectos más significativos de la LORTAD son:

- Es de aplicación sólo a los datos personales que figuran en ficheros automatizados y a ficheros de datos de carácter personal registrados en soporte físico susceptible de tratamiento automatizado.
- Los datos sólo podrán ser recogidos y tratados cuando sean adecuados, pertinentes y no excesivos en relación con su ámbito y su finalidad, así como ser exactos y estar actualizados.
- Los datos solo pueden ser usados cuando lo justifique la finalidad para que fueron obtenidos.
- Se exige el consentimiento consciente e informado de la persona afectada para que la obtención de los datos sea lícita.
- Trata por primera vez el concepto de "datos sensibles".
- Regula las cesiones de datos personales.
- Reconoce los derechos de acceso, rectificación y cancelación, información y el derecho de impugnación de valoraciones basadas exclusivamente en datos automatizados.
- Deber de informar a las personas a las que se soliciten datos personales de la existencia de un fichero de datos, de la identidad y dirección de la persona Responsable, de las consecuencias de la obtención de sus datos, de los dere-

9. *Artículo 18.4 de la Constitución Española.*

chos que tienen y del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

- Prohíbe de forma general la transferencia de datos personales a países que no proporcionen un nivel de protección equiparable al establecido en la LORTAD.

- Crea la Agencia de Protección de Datos, a quien encomienda el control de la aplicación de la LORTAD.

- Establece la obligatoriedad de notificar previamente la creación de dichos ficheros al Registro General de Protección de Datos dependiente de la Agencia de Protección de Datos.

2.2.2. LEY ORGÁNICA 15/1999, DE 5 DE DICIEMBRE, DE PROTECCIÓN DE DATOS PERSONALES (LOPD)

La Ley Orgánica 15/1999, de 5 de diciembre, de protección de datos personales (LOPD) es la trasposición de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, que establecía un plazo máximo de tres meses para la trasposición. Deroga a la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.

La LOPD está desarrollada por el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RLOPD).

De la LOPD se puede destacar como novedoso:

- Es de aplicación a todos los datos personales que figuran en ficheros, no sólo a los automatizados. No obstante, no será de aplicación si los datos no están en soporte físico y/o no son susceptibles de tratamiento.

- Son datos de carácter personal "cualquier información concerniente a personas físicas identificadas o identificables".

- El consentimiento debe ser inequívoco.

- Se añade el derecho de oposición, estableciendo los conocidos como derechos ARCO.

- Las organizaciones tienen que adoptar las medidas técnicas y organizativas que sean necesarias para garantizar la seguridad de los datos de carácter personal.

Estas medidas están desarrolladas en el **Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados** que contengan datos de carácter personal, donde se establecen distintos niveles en función de los tipos de datos obtenidos y tratados:

  - Nivel básico: deberán ser adoptadas por cualquier fichero.
  - Nivel medio: deberán ser adoptadas para ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y solvencia patrimonial y crediticia.
  - Nivel alto: aplicables a ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual, así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas.

- Se agrega la figura del Encargado del fichero.

2.2.3. TRANSPOSICIÓN DEL REGLAMENTO (UE) 2016/679, DEL PARLAMENTO EUROPEO Y DEL CONSEJO, DE 27 DE ABRIL DE 2016 (RGPD)

El Reglamento General de Protección de Datos (RGPD), que entró en vigor en mayo de 2016 y que es de aplicación a todas las organizaciones, establecidas o no en la Unión Europea, que tratan datos personales de personas residentes en Europa en la Unión Europea, se comenzó a aplicar en España desde el 25 de mayo de 2018 derogando de la anterior legislación todo lo que contradiga a lo establecido en dicho RGPD.

Adicionalmente, el Real Decreto-Ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos, se aprobó con el objetivo de adecuar algunos aspectos recogidos en el RGPD cuya adaptación requería cierta urgencia.

2.2.4. LEY ORGÁNICA 3/2018, DE 5 DE DICIEMBRE, DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES (LOPDGDD)

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales u garantía de derechos digitales (LOPDGDD) es la adaptación del 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 (RGPD).

La LOPDGDD tiene mucho contenido en común con el RGPD, de hecho, en un gran parte de su articulado remite a dicho RGPD. No obstante, hay algunas diferencias y unos temas que la LOPDGDD trata de forma específica:

- Establece la edad mínima de consentimiento de las personas menores de edad en 14 años.
- Tratamientos concretos de datos de:
  - Contacto sobre empresarios/as individuales y profesionales liberales.
  - Sistemas de información sobre créditos.
  - Videovigilancia.
  - Para la protección de las personas que informen sobre infracciones normativas.
- En relación con la persona Delegada de Protección de Datos:
  - Requiere de una certificación para poder ejercer sus funciones.
  - Establece cuándo debe ser obligatorio su nombramiento en una organización.
- Garantizar los derechos digitales:
  - En el ámbito laboral se reconoce el derecho a la desconexión digital y a la intimidad y uso de dispositivos digitales.
  - Derecho al olvido en internet y en redes sociales.
  - Derecho a la educación digital y protección de menores.
  - Derecho de acceso a Internet.

2.3. LEGISLACIÓN AUTONÓMICA

A nivel autonómico no se ha aprobado ninguna normativa que regule específicamente la protección de datos, aunque sí se han emitido algunas leyes para la creación y regulación de agencias autonómicas de protección de datos.

A lo largo de esta guía se va a desarrollar el contenido del RGPD junto a la normativa nacional vigente de aplicación, que es la LOPDGDD.

03

CONCEPTOS BÁSICOS

3.1. DEFINICIONES

En una guía sobre protección de datos y, para ayudar a entender con mayor facilidad los conceptos y particularidades de la normativa europea y española aplicados a las entidades de Acción Social, es imprescindible conocer las definiciones básicas sobre protección de datos personales.

En primer lugar, y como punto de partida, se define qué es un dato personal y, posteriormente se proporciona una definición de otros conceptos que van a ser mencionados continuamente, tanto en esta guía como cada vez que proporcionemos nuestros datos personales.

3.1.1. DATO PERSONAL

De acuerdo a la web de la Comisión Europea "los datos personales son cualquier información relativa a una persona física viva identificada o identificable. Las distintas informaciones, que recopiladas pueden llevar a la identificación de una determinada persona, también constituyen datos de carácter personal[10]."

Como persona identificable se considera "toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona[11]."

Así, un dato de carácter personal o dato personal, como habitualmente se denomina, es **cualquier información que se puede utilizar para identificar directa o indirectamente a una persona. Esta información puede ser numérica, gráfica, fotográfica, acústica o de cualquier otro tipo, y que afecte a personas físicas perfectamente identificadas o identificables.**

10. https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_es

11. Artículo 4 del RGPD.

Ejemplos de datos personales:

» *Nombres y apellidos.*
» *Número de tarjeta de crédito.*
» *Dirección postal.*
» *Número de seguridad social.*
» *Fotografías.*
» *Número de DNI, pasaporte o de identificación personal.*
» *Número de teléfono.*
» *Número de placa de matrícula del vehículo.*
» *Dirección de correo electrónico personal.*
» *Dirección IP.*
» *Dirección de correo profesional nominativo.*
» *ID de cookie.*
» *Datos de localización.*
» *Contraseña.*
» *Número de cuenta bancaria.*
» *ID / enlaces de perfil de redes sociales.*

En contraposición, no son datos personales aquellos con los que no se pueda identificar directa o indirectamente a una persona física.

Ejemplos de datos no personales:

» *Direcciones de correo electrónico no nominativas como info@plataformaong.org.*
» *Número de registro mercantil.*

Además, existen las categorías especiales de datos, que son aquellas cuyo tratamiento podría entrañar importantes riesgos de vulneración de derechos y libertades fundamentales. Las categorías especiales de datos son[12]:

1. El origen étnico o racial.
2. Las opiniones políticas.
3. Las convicciones religiosas o filosóficas.
4. La afiliación sindical.
5. El tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física.
6. Los datos relativos a la salud.
7. Los datos relativos a la vida sexual.
8. Los datos relativos a la orientación sexual.

3.1.2. OTRAS DEFINICIONES

Adicionalmente a conocer qué es un dato personal, otros conceptos que merecen atención son:

- **Tratamiento de datos:** Es cualquier actividad que se lleve a cabo con un dato personal, ya sea de forma automatizada o manual. Por lo tanto, son tratamiento la recogida, registro, organización, conservación, almacenamiento, manipulación, modificación, utilización, comunicación, interconexión, transferencia, cesión, limitación, supresión o destrucción de datos.

- **Sistema de tratamiento:** Es el modo en que se organiza o utiliza un tratamiento, que podrá ser automatizados, no automatizados o parcialmente automatizados.

- **Responsable del tratamiento:** Es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine la finalidad y medios del tratamiento.

- **Encargado del tratamiento:** Es la persona física o jurídica, autoridad pública, servicio u otro organismo que trate los datos personales autorizada por la persona responsable del Tratamiento.

12. *Artículo 9 del RGPD y artículo 9 de la LOPDGDD.*

- **Seudonimización:** Es el tratamiento de datos personales de manera tal que ya no puedan usarse para identificar a la persona física sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas de seguridad.

- **Anonimización:** Es el tratamiento de datos personales de manera tal que ya no puedan usarse para identificar a la persona física. Los datos anonimizados quedan fuera del ámbito de aplicación de la normativa de Protección de Datos "en la medida que es posible demostrar objetivamente que no existe capacidad material para asociar los datos anonimizados a una persona física determinada, directa o indirectamente"[13]. Para que los datos se consideren verdaderamente anónimos, la anonimización debe ser irreversible.

- **Riesgo:** Es la posibilidad de que se produzca una amenaza a la protección de datos carácter personal.

- **Amenaza:** Cualquier riesgo con potencial para provocar un daño o perjuicio en relación con los datos de carácter personal que están siendo tratados.

- **Consentimiento:** Es una 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*[14]. Es decir, la persona física debe autorizar libremente y de forma expresa que sus datos personales sean tratados.

- **Fichero de datos personales:** Es un conjunto organizado de datos personales conforme a un determinado criterio, independientemente de su forma de tratamiento, que puede ser automatizado o manual.

La normativa actual se centra en los tratamientos y no en cómo están organizados los datos personales en la entidad.

- **Autoridades de control:** Son las autoridades públicas independientes encargadas de supervisar la aplicación de la legislación sobre protección de datos y de velar por el derecho a la protección de datos personales. Se las denomina también Autoridades de protección de datos. Existe una autoridad de control en cada Estado miembro de la Unión Europea. En España la autoridad de control es la Agencia Española de Protección de Datos (AEPD) y sus homólogas autonómicas, que a día de hoy sólo son la Autoridad Catalana de Protección de Datos, la Agencia Vasca de Protección de Datos y el Consejo de Transparencia y Protección de Datos de Andalucía.

- **Persona interesada o afectada:** Es la persona a quien se refieren los datos personales, que debe ser una persona física, identificada o identificable

3.2. PRINCIPIOS DE PROTECCIÓN DE DATOS

La normativa de protección de datos señala un conjunto de principios que se deben observar al tratar datos personales. Los principios de protección de datos personales son la base sobre la que se asienta la normativa de protección de datos y establecen las premisas básicas a la hora de obtener, acceder o tratar los datos personales de las personas interesadas.

13. *Anonimización y seudonimización (6 de octubre de 2021). Agencia Española de Protección de Datos.*

14. *Artículo 4.11) del RGPD.*

Los principios figuran en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD), y, posteriormente son adaptados en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

En este capítulo nos vamos a basar en la clasificación de los principios que figura en la normativa europea[15]:

A. Principio de licitud, lealtad y transparencia del tratamiento:

El tratamiento de datos deberá tener unas bases legítimas y hacerse de forma leal y transparente respecto de la persona titular de los datos o interesada. En otras palabras, no se pueden recoger datos de forma fraudulenta o ilícita y, por otro lado, se debe informar a la persona titular de los datos de su tratamiento. A continuación, se va a explicar en qué consiste la licitud, la lealtad y la transparencia en más detalle:

- **Licitud:** Los datos personales deben ser tratados con el consentimiento explícito de la persona interesada o apoyarse en una base legal que lo legitime (contrato, obligación legal, intereses públicos, intereses vitales e interés legítimo).

El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones[16]:

a. La persona interesada dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos.

> ***Ejemplo:*** *cuando se acepta recibir el boletín de noticias de una entidad o se proporcionan datos personales para participar en una jornada aceptando la cláusula de protección de datos.*

b. El tratamiento es necesario para la ejecución de un contrato o actuaciones precontractuales en el que la persona interesada es parte.

> ***Ejemplo:*** *cuando se firma un contrato con una empresa proveedora y figuran algunos datos personales de su representante legal.*

c. El tratamiento es necesario para el cumplimiento de una obligación legal aplicable a la persona Responsable del tratamiento.

> ***Ejemplo:*** *cuando se firma un contrato laboral los datos de la persona contratada van a ser tratados para cumplir la normativa laboral, la de la Seguridad Social y la de la Agencia Tributaria.*

d. El tratamiento es necesario para proteger intereses vitales de la persona interesada o de otra persona física.

> ***Ejemplo:*** *cuando el tratamiento es necesario para fines humanitarios como el control de una epidemia y en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano contratada van a ser tratados*

15. *Artículo 5 del RGPD.*

16. *Artículo 6 del RGPD.*

e. El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos a la persona Responsable del tratamiento.

> ***Ejemplo:*** *cuando para participar en programas o proyectos dirigidos a menores de edad se exige un certificado negativo del Registro Central de delincuentes*

f. El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por la persona Responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea una persona menor de edad.

> ***Ejemplo:*** *cuando sea estrictamente necesario para la prevención del fraude.*

Normalmente, y como regla general, un tratamiento será lícito cuando cuente con el consentimiento de la persona interesada. Este consentimiento debe ser:

- **Libre:** la persona interesada no puede verse obligada a otorgarlo y no debe existir un desequilibrio evidente entre la persona interesada y la persona Responsable del tratamiento.

- **Inequívoco:** lo que supone que se preste mediante una manifestación expresa. Elimina la posibilidad del consentimiento tácito, es decir, que las personas interesadas deberán decir expresamente que consienten el tratamiento.

> ***Ejemplo de consentimiento inequívoco (expreso):*** *cuando en un cuestionario online la persona que lo completa tiene que marcar una casilla donde se acepta el tratamiento de los datos aportados para los fines que se indican, siendo necesario para poder completar la encuesta y enviarla.*
>
> ***Ejemplo de consentimiento tácito:*** *cuando en un cuestionario se informa del tratamiento de los datos aportados y de los fines de dicho tratamiento, pero no es necesario que la persona interesada lo acepte.*

- **Específico:** debe ser obtenido para cada uno de los fines para los que los datos personales son recogidos.
- **Informado:** la persona interesada debe conocer, como mínimo, la identidad de la persona Responsable del tratamiento, los fines del tratamiento a los cuales están destinados los datos personales, sus derechos y cómo ejercerlos. Para informar tiene que usarse un lenguaje claro y sencillo.
- **Revocable:** puede anularse en cualquier momento a través de medios sencillos y gratuitos. Cuando el consentimiento sea prestado por una persona menor de edad, se requerirá siempre el consentimiento de quien ostente la patria potestad o tutela, excepto si es mayor de 14 años, donde el consentimiento de la persona menor será el único necesario para tratar sus datos personales.

En relación con los datos sensibles o "categorías especiales de datos[17]" , el

17. *Artículo 9 del RGPD.*

consentimiento explícito de la persona titular no será suficiente para su tratamiento, con el fin de evitar situaciones discriminatorias y se deberá contar con otra de las bases de legitimación previstas.

- **Lealtad:** No pueden recabarse datos personales por medios fraudulentos y/o utilizando medios o métodos engañosos, que den lugar a una discriminación injusta o arbitraria contra los titulares o que sean ilegales, o estén fuera o al margen de la Ley.

- **Transparencia:** Exige que toda información y comunicación relativa al tratamiento de datos personales sea fácilmente accesible y fácil de entender, y se utilice un lenguaje sencillo y claro.

B. Principio de limitación de la finalidad:

Los datos personales deben ser recogidos con una finalidad determinada, explícita y legítima y no serán tratados posteriormente para otros fines.

> ***Ejemplo:*** *se obtuvo el consentimiento expreso para la obtención de datos personales para el envío del boletín de noticias de la organización y, posteriormente, esos datos quieren usarse para realizar una encuesta de percepción social.*

Cuando se van a tratar los datos para otro fin diferente de aquel para el que se recogieron, antes de hacerlo, se deberá tener en cuenta:

1. La relación existente entre el tratamiento para el que se recogieron los datos y el que se desea realizar.

> ***Ejemplo:*** *se recogen los datos para la realización de una formación y se les quiere enviar noticias de la entidad sin que haya habido consentimiento expreso.*
>
> ***Ejemplo:*** *se recogen los datos para la realización de una formación y se quiere utilizar esos datos para la justificación de una subvención que financia esa formación.*

2. El contexto en el que se hayan recogido los datos y, en particular, la relación entre la persona responsable del tratamiento y las personas interesadas.
3. La naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales[18] o datos personales relativos a condenas e infracciones penales[19].
4. Las posibles consecuencias para las personas interesadas del tratamiento ulterior previsto.
5. La existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización.

C. Principio de minimización:

Los datos que se obtengan deben ser adecuados, pertinentes y no excesivos en relación con la finalidad para la que son tratados. Sólo se deben recoger aquellos datos que sean necesarios para el fin para el que se realiza el tratamiento.

D. Principio de exactitud:

Los datos deben ser exactos y, en caso de contener errores, deben ser corregidos y actualizados. Así, se deberán adoptar las medidas correctoras necesarias y razonables y modificar los datos inexactos o

18. *Artículo 9 del RGPD.*

19. *Artículo 10 del RGPD.*

incompletos, para así poder garantizar la veracidad y seguridad de la información objeto de tratamiento.

E. Principio de conservación de los datos:

Los datos personales deben ser eliminados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la que fueron recogidos o, lo que es lo mismo, la conservación de los datos debe limitarse en el tiempo al logro de los fines que persigue el tratamiento. Una vez que los fines del tratamiento se han alcanzado, los datos deben ser borrados, bloqueados o, en su defecto, anonimizados, lo que implica eliminar todo elemento que permita identificar a las personas interesadas.

Se podrán conservar por más tiempo, con las correspondientes medidas de seguridad (bloqueados o anonimizados), si se prevé conservar exclusivamente para fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. Así, se deberán establecer plazos para la eliminación de los datos, así como de la revisión periódica de dichos plazos y de los datos conservados. En todo caso, los plazos de conservación deben ser proporcionales y respetar los límites legales establecidos para que las personas interesadas puedan ejercer acciones legales.

En una organización del TSAS los plazos necesarios para el tratamiento de los datos podrían ser:

Ilustración 3 Plazos de conservación de los datos personales en una organización del TSAS

Además del plazo de conservación de los datos personales recabados por la organización, otro plazo a tener en cuenta es el plazo de conservación para la defensa de reclamaciones por parte de quien sea responsable (plazo de prescripción de las acciones ante reclamaciones por el tratamiento de datos realizado).

F. Principio de integridad y confidencialidad:

Los tratamientos de datos deben garantizar su seguridad evitando un tratamiento no autorizado o ilícito aplicando las medidas técnicas u organizativas adecuadas. Y, además, toda persona que trate datos personales se encuentra sometida a un deber de confidencialidad de la información tratada.

- **Integridad:** Los datos deben ser tratados de tal manera que se garantice una seguridad adecuada mediante la aplicación de medidas de control apropiadas. Se debe impedir el acceso o uso no autorizado a los datos personales.

- **Confidencialidad:** La información no se pone a disposición o se revela a personas, entidades o procesos no autorizados. Además, cualquier persona que intervenga en cualquiera de las fases del tratamiento de datos personales está sujeta a guardar la confidencialidad de los datos con carácter indefinido.

G. Principio de responsabilidad proactiva:

Quien sea responsable del tratamiento deberá cumplir con todos los principios del tratamiento de datos personales y, lo que es más importante, debe ser "capaz de demostrarlo".

Este principio obliga a mantener diligencia debida de manera permanente para proteger y garantizar los derechos y libertades

3.3. TRANSPARENCIA E INFORMACIÓN

La transparencia es uno de los principios en los que se basa el RGPD y, por consiguiente, la LOPDGDD. Este principio de transparencia exige, por un lado, que se informe a las personas interesadas sobre los tratamientos que van a tener sus datos personales y sobre los derechos que tienen y, por otro, cómo debe ser la información proporcionada.

Respecto a la información a proporcionar a las personas interesadas, hay que distinguir entre si los datos se obtienen directamente de la persona interesada o si no se han obtenido de ella.

Cuando los datos personales se obtienen directamente de la persona interesada, la organización debe informarle acerca de:

1. La identidad y los datos de contacto (dirección, teléfono, correo electrónico, etc.) de la persona Responsable del tratamiento.
2. Los datos de contacto de la persona Delegada de protección de datos, si la hubiera.
3. La finalidad del tratamiento: para qué se van a usar los datos personales.
4. La base jurídica del tratamiento o su licitud, por ejemplo, si los datos se proporcionan con el consentimiento explícito de la persona interesada, si son necesarios para la celebración de un contrato o para el cumplimiento de una obligación legal aplicable.
5. Los intereses legítimos si el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por la persona Responsable del tratamiento o por una tercera persona.
6. Las personas destinatarias o las categorías de destinatarias de los datos personales, si las hubiera.
7. Información acerca de la transferencia internacional de los datos, si fuera el caso.
8. El plazo de conservación de los datos personales o, cuando no sea posible indicar el plazo exacto, los criterios utilizados para determinar ese plazo.
9. Los derechos que tiene la persona interesada y cómo los puede ejercer.

10. El derecho a retirar el consentimiento en caso de que la persona interesada lo hubiera dado.
11. El derecho a presentar una reclamación ante la autoridad de control correspondiente.
12. Si los datos personales se comunican para suscribir un contrato o son un requisito legal, las consecuencias de no facilitar esos datos.
13. Si va a haber decisiones automatizadas, incluida la elaboración de perfiles e información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para la persona interesada.

La información se tiene que proporcionar con anterioridad a la obtención de los datos personales, debiéndose obtener el consentimiento expreso de la persona interesada antes de recabarlos.

En caso de que los datos se vayan a tratar para una finalidad distinta a aquella para los que fueron recogidos, se proporcionará a la persona interesada, siempre con anterioridad a la realización del nuevo tratamiento, como mínimo, la información que figura en los puntos 8 a 13 anteriores.

Ejemplo: *la persona interesada proporciona sus datos personales para la participación en una jornada:*
Responsable del tratamiento: *Plataforma de ONG de Acción Social. NIF: G-82747668. C/Tribulete 18, 1ª planta, 28012 Madrid. info@plataformaong.org*
Delegado de Protección de Datos: *dpd@plataformaong.org*
Finalidad del tratamiento: *gestionar la inscripción y participación en la jornada "La protección de datos en las entidades de Acción Social".*
Se informa a las personas usuarias de la necesidad de facilitar todos los datos de carácter obligatorio para poder cumplir con las finalidades anteriormente indicadas. Estos campos constan identificados mediante un asterisco (*).

En caso de que no nos facilite dichos datos, ello podrá dar lugar a la imposibilidad por parte de la Plataforma de cumplir con tales finalidades.

Base jurídica: *libre consentimiento mostrado acudiendo a la jornada organizada.*
Personas destinatarias: *sus datos personales podrán ser comunicados al Ministerio de Derechos Sociales y Agenda 2030, así como a otras autoridades competentes, en caso de que los mismos fuesen requeridos, con la finalidad de acreditar y justificar la recepción de subvenciones. Dicha comunicación se legitima en el cumplimiento de una obligación legal. No están previstas transferencias internacionales de datos.*
Plazo de conservación: *sus datos se conservarán para la realización de los tratamientos mencionados, sin perjuicio de la conservación que resultase necesaria para la formulación, el ejercicio o la defensa de potenciales reclamaciones y/o siempre que lo permitiese la legislación aplicable.*
Derechos de la persona interesada: tendrá la posibilidad de ejercer los derechos de acceso, rectificación, oposición, supresión, portabilidad y limitación del tratamiento, así como a rechazar el tratamiento automatizado de los datos personales, y retirar su consentimiento en cualquier momento. Podrá ejercer estos derechos a través de la dirección de correo electrónico dpd@plataformaong.org, indicando qué derecho desea ejercitar y aportando su DNI o documento acre-

ditativo de su identidad similar.

Podrá presentar una reclamación ante la Agencia Española de Protección de Datos, a través de su página web.

***Ejemplo:** la persona interesada envía su curriculum vitae:*
***Responsable del tratamiento:** Plataforma de ONG de Acción Social. NIF: G-82747668. C/Tribulete 18, 1ª planta, 28012 Madrid. info@plataformaong.org Delegado de Protección de Datos: dpd@plataformaong.org*
***Finalidad del tratamiento:** atender las solicitudes de trabajo y gestionar su participación en los procesos de selección. Base jurídica: consentimiento mostrado mediante la libre remisión de su currículum vitae.*

No se realizarán cesiones de datos ni transferencias internacionales de datos.
***Plazo de conservación:** máximo de seis meses desde que se finaliza el proceso de selección*
***Derechos de la persona interesada:** tendrá la posibilidad de ejercer los derechos de acceso, rectificación, oposición, supresión, portabilidad y limitación del tratamiento, así como a rechazar el tratamiento automatizado de los datos personales, y retirar su consentimiento en cualquier momento. Podrá ejercer estos derechos a través de la dirección de correo electrónico dpd@plataformaong.org, indicando qué derecho desea ejercitar y aportando su DNI o documento acreditativo de su identidad similar. Por último, podrá presentar una reclamación ante la Agencia Española de Protección de Datos, a través de su página web.*

Cuando los datos personales no se obtienen directamente de la persona interesada, la organización debe informar acerca de:

1. La identidad y los datos de contacto de la persona Responsable del tratamiento.
2. Los datos de contacto de la persona Delegada de protección de datos, si la hubiera.
3. La finalidad del tratamiento: para qué se van a usar los datos personales.
4. La base jurídica del tratamiento o su licitud.
5. Las categorías de datos personales obtenidos.
6. Las personas destinatarias o las categorías de destinatarias de los datos personales, si las hubiera.
7. Información acerca de la transferencia internacional de los datos, si fuera el caso.
8. El plazo de conservación de los datos personales o, cuando no sea posible indicar el plazo exacto, los criterios utilizados para determinar ese plazo.
9. Los intereses legítimos si el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por la persona Responsable del tratamiento o por una tercera persona.
10. Los derechos que tiene la persona interesada y cómo los puede ejercer.
11. El derecho a retirar el consentimiento en caso de que la persona interesada lo hubiera dado.
12. El derecho a presentar una reclamación ante la autoridad de control correspondiente.
13. La fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público: de dónde se han obtenido los datos personales.
14. Si va a haber decisiones automatizadas, incluida la elaboración de perfiles e información significativa sobre

la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para la persona interesada.

La información se tiene que proporcionar a la persona interesada:

- En un plazo razonable máximo de un mes una vez obtenidos los datos personales.
- En caso de que los datos sean necesarios para comunicarse con la persona interesada, en el momento de la primera comunicación.

En caso de que los datos vayan a ser comunicados a otra persona destinataria, con anterioridad a la primera comunicación.

En algunos casos no será necesario informar a la persona interesada como, por ejemplo, cuando se tenga certeza de que la persona interesada disponga ya de la información o la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado. Pero habrá que tener plena certeza de que se encuentra en los supuestos contemplados por normativa y, en caso de duda, lo más conveniente sería informar.

En caso de que los datos se vayan a tratar para una finalidad distinta a aquella para los que fueron recogidos, se proporcionará a la persona interesada, siempre con anterioridad a la realización del nuevo tratamiento, como mínimo, la información que figura en los puntos 8 a 14 anteriores.

Respecto a cómo debe ser la información proporcionada, el RGPD especifica en su Considerando 58 que “El principio de transparencia exige que toda información dirigida al público o al interesado sea concisa, fácilmente accesible y fácil de entender, y que se utilice un lenguaje claro y sencillo, y, además, en su caso, se visualice”. Así, la información que se proporciones:

- Será concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.
- Deberá evitarse las fórmulas enrevesadas y/o que remitan a textos legales.
- Deberá proporcionarse por escrito y usarse medios electrónicos cuando sea posible.

3.4. DERECHOS DE LAS PERSONAS RELATIVOS A LA PROTECCIÓN DE DATOS

Las personas físicas deben conocer los derechos relativos al tratamiento de datos personales, así como el modo de ejercitarlos.

La normativa de protección de datos permite que las personas físicas puedan ejercer sus derechos relativos al tratamiento de datos personales ante la persona Responsable del tratamiento. Estos derechos son de acceso, rectificación, oposición, supresión (conocido como “derecho al olvido”), limitación del tratamiento, portabilidad y de no ser objeto de decisiones individualizadas.

Ver gráfico en la página siguiente

Ilustración 4 Derechos de las personas en materia de protección de datos[20]

Estos derechos se caracterizan por lo siguiente :

1. Su ejercicio es gratuito, aunque puede haber excepciones tal y como se menciona en el punto 5.

2. Los derechos relativos al tratamiento de datos personales se pueden ejercer directamente por la persona afectada o por medio de representante legal o voluntario.

3. La persona Responsable del tratamiento debe informar a la persona cuyos datos vayan a ser tratados de:

   - Los derechos que puede ejercitar.
   - Los medios disponibles para ejercer esos derechos.

4. Estos medios deben ser fácilmente accesibles y nunca se podrá denegar que se ejerzan los derechos si se utilizara otro medio. Los medios más comúnmente puestos a disposición de las personas afectadas o interesadas son el correo electrónico y/o formularios en la página web, aunque las personas afectadas pueden hacer uso de cualquier otro medio de contacto con la persona Responsable.

5. Si la solicitud se presenta por medios electrónicos, la información se facilitará por estos medios cuando sea posible, salvo que la persona interesada solicite que sea de otro modo[21].

6. Las solicitudes deben responderse en el plazo de un mes, aunque el plazo podrá prorrogarse dos meses más en caso necesario, en base a la complejidad y número de solicitudes[22].

7. Si la persona Responsable no da curso a la solicitud, deberá informar a la persona afectada, en el plazo máximo de un mes, de las razones de su no actuación, de la posibilidad de reclamar ante una Autoridad de Control y de ejercitar acciones judiciales[23].

8. La persona Encargada del tratamiento podrá atender la solicitud de las personas afectadas en lugar de que lo haga la persona Responsable si así se establece en un contrato o en un acto jurídico que les vincule.

9. Si las solicitudes son claramente infundadas o excesivas, la persona Respon-

20. *Artículo 12 de la LOPDGDD.*
21. *Artículo 15.3 del RGPD.*
22. *Artículo 12.3 del RGPD.*
23. *Artículo 12.4 del RGPD.*
24. *Artículo 12.5 del RGPD.*

sable del tratamiento podrá[24]:

- Cobrar un canon proporcional a los costes administrativos soportados.
- Negarse a actuar

Una solicitud será excesiva cuando sea repetitiva, es decir, cuando se ejerza el derecho de acceso por la misma persona en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima para ello[25].

Cuando la persona afectada elija un medio distinto al que se le ofrece que suponga un coste desproporcionado, la solicitud será considerada excesiva, por lo que dicha persona asumirá el exceso de costes que su elección comporte. En este caso, solo será exigible a la persona Responsable del tratamiento que atienda la solicitud sin dilaciones indebidas[26].

En el caso de que la persona afectada solicite que se le proporcionen los datos personales objeto del tratamiento (derecho de acceso) en más de una ocasión, la persona Responsable podrá solicitar un canon basado en los costes administrativos que supongan las entregas adicionales [27].

10. La persona Responsable del tratamiento será quien tenga que demostrar que se ha respondido a las solicitudes de las personas afectadas en relación con el ejercicio de sus derechos. Es decir, que la prueba del cumplimiento del deber de responder a la solicitud de ejercicio de sus derechos recaerá sobre la persona Responsable.

11. En el caso de personas menores de catorce años, las personas que ejerzan su patria potestad serán quienes puedan ejercitar sus derechos.

3.4.1. DERECHO DE ACCESO

Es el derecho a obtener información de la persona Responsable del tratamiento sobre si sus datos están siendo objeto de tratamiento, la finalidad del mismo, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos.

La información que la persona interesada puede obtener es la siguiente[28]:

- Si se están tratando o no sus datos personales.
- Una copia de los datos personales que son objeto del tratamiento.
- Los fines del tratamiento.
- Las categorías de datos personales que se tratan.
- Los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados esos datos personales y, en particular, los destinatarios en terceros países u organizaciones internacionales.
- El plazo previsto de conservación de esos datos personales o, al menos, los criterios utilizados para determinar ese plazo.
- La existencia del derecho de la persona interesada a solicitar la rectificación o supresión de sus datos personales, la limitación del tratamiento de sus datos personales u oponerse a ese tratamiento.
- El derecho a presentar una reclama-

25. *Artículo 13.3 de la LOPDGDD.*

26. *Artículo 13.4 de la LOPDGDD.*

27. *Artículo 15.3 del RGPD.*

28. *Artículo 15 del RGPD.*

ción ante una Autoridad de Control.

- Cuando los datos personales no se hayan obtenido directamente de la persona interesada, cualquier información disponible sobre su origen.

- La existencia de decisiones automatizadas, incluida la elaboración de perfiles, y al menos en tales casos, información significativa sobre la lógica aplicada, la importancia y las consecuencias previstas de ese tratamiento para la persona interesada.

Cuando se traten una gran cantidad de datos relativos a la persona afectada y ésta ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, la persona Responsable del tratamiento podrá solicitarle, antes de facilitar la información, que la persona afectada especifique los datos o actividades de tratamiento a los que se refiere la solicitud[29].

El derecho de acceso se entenderá otorgado si la persona Responsable del tratamiento facilitara a la persona afectada un sistema de acceso remoto, directo y seguro a sus datos personales que garantice, de modo permanente, el acceso a su totalidad. A tales efectos, la comunicación por la persona Responsable a la afectada del modo en que ésta podrá acceder a dicho sistema bastará para tener por atendida la solicitud de ejercicio del derecho[30].

Ejemplo: *cuando se da acceso a una persona al área de alumnado en un curso de formación y en esa área existe un apartado donde figuren los datos personales recabados de la persona y necesarios para la realización de su formación y, si fuera necesario, para la posterior justificación al organismo financiador.*

La Agencia Española de Protección de Datos dispone de un formulario para el ejercicio del derecho de acceso que las personas interesadas pueden implementarlo y presentarlo ante cualquier persona Responsable del tratamiento de sus datos personales:

- **Formulario para el ejercicio del derecho de acceso. https://www.aepd.es/es/documento/formulario-derecho-de-acceso.pdf**

3.4.2. DERECHO DE RECTIFICACIÓN

Es el derecho que tiene la persona interesada a obtener la rectificación de sus datos personales inexactos por parte de la persona Responsable[31]. Teniendo en cuenta los fines del tratamiento, la persona interesada tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

La persona interesada deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Deberá acompañar a la solicitud, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento[32].

Ejemplo: *cuando una persona receptora del boletín de noticias de la organización modifica su correo electrónico o desea que*

29. *Artículo 13 de la LOPDGDD.*
30. *Artículo 13 de la LOPDGDD.*
31. *Artículo 16 del RGPD.*
32. *Artículo 14 de la LOPDGDD.*

se le envíen las comunicaciones a otra dirección, puede ejercer su derecho de rectificación para modificar su correo electrónico.

La Agencia Española de Protección de Datos dispone de un formulario para el ejercicio del derecho de rectificación que las personas interesadas pueden implementarlo y presentarlo ante cualquier persona Responsable del tratamiento de sus datos personales:

- **Formulario para el ejercicio del derecho de rectificación. https://www.aepd.es/es/documento/formulario-derecho-de-rectificacion.pdf**

3.4.3. DERECHO DE OPOSICIÓN

Este derecho implica que la persona afectada se puede oponer a que la persona Responsable lleve a cabo un tratamiento de sus datos personales.

Se puede ejercer en los siguientes casos:

- Cuando los datos personales se traten basándose en una misión de interés público o en el interés legítimo, incluido la elaboración de perfiles[33]: la persona Responsable del tratamiento dejará de tratar los datos salvo que acredite motivos imperiosos que prevalezcan sobre los intereses, derechos y libertades de la persona interesada, o para la formulación, el ejercicio o la defensa de reclamaciones.

- Cuando el tratamiento tenga como finalidad la mercadotecnia directa, incluida también la elaboración de perfiles anteriormente citada: la persona Responsable del tratamiento dejará de tratar los datos para dichos fines. En este caso, tal y como se menciona en el apartado del derecho de supresión, si los datos sólo son tratados para esta finalidad, la persona Responsable estará obligada a suprimir los datos personales de la persona afectada.

***Ejemplo:** la persona afectada proporcionó sus datos para participar en un estudio elaborado por la organización sobre los derechos laborales de las personas empleadas en el Tercer Sector de Acción Social. Posteriormente, descubre que en la política de privacidad figura que los datos proporcionados pueden ser utilizados para la elaboración de estudios de campañas de mercadotecnia para, por ejemplo, la emisión de anuncios en redes sociales. Como la persona afectada no dio su consentimiento expreso para el uso de sus datos personales para ese tratamiento, decide ejercer su derecho de oposición a que sus datos sean usados para la elaboración de campañas de mercadotecnia.*

Aunque pueda parecer lo mismo, el derecho de oposición no es lo mismo que el derecho que tienen las personas afectadas para revocar el consentimiento expreso. Ejercer este derecho implica que los datos personales dejen de ser tratados, pero no que necesariamente deban ser eliminados.

La Agencia Española de Protección de

***33.** El artículo 4 del RGPD define la elaboración de perfiles como "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".*

Datos dispone de formularios para el ejercicio del derecho de oposición que las personas interesadas pueden implementarlos y presentarlos ante cualquier persona Responsable del tratamiento de sus datos personales:

- **Formularios para el ejercicio del derecho de oposición. https://www.aepd.es/es/documento/formulario-derecho-de-oposicion.pdf**

3.4.4. DERECHO DE SUPRESIÓN

Es el derecho que tiene la persona interesada a obtener de la persona Responsable del tratamiento la supresión de los datos personales.

La persona Responsable del tratamiento estará obligada a suprimir los datos personales de la persona afectada en las siguientes circunstancias[34]:

- Si los datos personales ya no son necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo.

Ejemplo: *cuando se proporcionan los datos personales para participar en una comisión de trabajo de la organización y, cuando se deja de participar en dicha comisión, esos datos personales ya no son necesarios.*

- Si el tratamiento de los datos personales se ha basado en el consentimiento que se prestó a la persona Responsable y se retira, siempre que dicho tratamiento no se base en otra causa que lo legitime.

Ejemplo: *cuando una persona consiente que se le envié el boletín de noticias periódico de la organización y posteriormente se retira ese consentimiento y sus datos personales no son usados para otro tratamiento necesario, como puede ser la justificación de subvenciones, la liquidación de impuestos u otra obligación legal.*

- Tal y como se ha mencionado anteriormente, si la persona afectada se ha opuesto al tratamiento de los datos personales al ejercitar su derecho de oposición en las siguientes circunstancias:

  - El tratamiento se fundamentaba en el interés legítimo o en el cumplimiento de una misión de interés público y no han prevalecido otros motivos para legitimar el tratamiento de los datos.

  - Que los datos personales sean objeto de mercadotecnia directa, incluyendo la elaboración de perfiles relacionada con la citada mercadotecnia.

Ejemplo: *cuando la persona afectada ha proporcionado sus datos personales para la elaboración de estudios de campañas de mercadotecnia y ejerció su derecho de oposición a dicho tratamiento. Como esos datos personales sólo tenían ese tratamiento, la persona Responsable tendrá que suprimir los datos personales.*

- Si los datos personales han sido tratados ilícitamente.

34. *Artículo 17 del RGPD.*

- 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 a la persona Responsable del tratamiento.

- Si los datos personales se han obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1 (condiciones aplicables al tratamiento de datos de los menores en relación con los servicios de la sociedad de la información)[35].

Además, la persona Responsable del tratamiento que haya hecho públicos los datos personales estará obligada a indicar a las demás personas responsables que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos.

No obstante, se puede no proceder a la supresión de los datos personales cuando el tratamiento sea necesario:

- Para el ejercicio de la libertad de expresión e información.

- Para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos a la persona Responsable.

- Por razones de interés público, en el ámbito de la salud pública, con fines de archivo de interés público, fines de investigación científica o histórica o fines estadísticos.

- Para la formulación, el ejercicio o la defensa de reclamaciones.

La Agencia Española de Protección de Datos dispone de formularios para el ejercicio del derecho de supresión que las personas interesadas pueden implementarlos y presentarlos ante cualquier persona Responsable del tratamiento de sus datos personales:

- **Formularios para el ejercicio del derecho de supresión. https://www.aepd.es/es/documento/formulario-derecho-de-supresion.pdf**

3.4.5. DERECHO A LA LIMITACIÓN DEL TRATAMIENTO

Este derecho consiste en que, a petición de la persona interesada, sus datos personales se dejan de tratar.

La limitación se puede solicitar cuando:

- Mientras la persona Responsable determina si tiene que atender la solicitud realizada por la persona interesada cuando ejercita sus derechos de rectificación o de oposición.

- El tratamiento es ilícito, hecho que determinaría el borrado de los datos, pero el interesado se opone a la supresión.

- Los datos ya no son necesarios para el tratamiento, hecho que determinaría el borrado de los datos, pero la persona interesada se opone a la supresión porque los necesita para formular, ejercer o defender reclamaciones.

Mientras dura la limitación, la persona Responsable sólo podrá tratar los datos afectados, además de conservarlos, y siempre con el consentimiento de la per-

35. *Artículo 8 del RGPD: "Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó".*

sona afectada, en los casos siguientes:

- Para formular, ejercer o defender reclamaciones.
- Para proteger los derechos de otra persona física o jurídica.
- Por razones de interés público importantes, de la Unión o del estado miembro correspondiente.

La persona Responsable deberá informar a la persona interesada que haya obtenido la limitación del tratamiento antes del levantamiento de dicha limitación.

> ***Ejemplo:*** *cuando una persona interesada participa como voluntaria en un programa de la organización financiado con una subvención concedida por el Ministerio de Derechos Sociales y Agenda 2030 y, una vez finalizada su participación, le solicita a la organización que elimine todos sus datos personales. Sin embargo, la organización está obligada a la guardia y custodia de la documentación justificativa del programa durante al menos cuatro años. En este caso, la persona interesada puede solicitar una limitación del tratamiento para asegurarse de que sus datos personales no se utilizan para otros fines.*

3.4.6. DERECHO A LA PORTABILIDAD

Este derecho consiste en que la persona interesada puede recibir los datos personales que haya facilitado a la persona Responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otra persona Responsable del tratamiento sin que lo impida la persona Responsable que se los hubiera facilitado.

Se podrán ejercer cuando se den estas dos condiciones al mismo tiempo:

1. La persona dio su consentimiento expreso para el uso de sus datos personales para uno o varios fines específicos[36] o cuando el tratamiento es necesario para la ejecución de un contrato en el que la persona interesada es parte o para la aplicación a petición de esta de medidas precontractuales.
2. El tratamiento se efectúe por medios automatizados.

Al ejercer su derecho a la portabilidad de los datos, la persona interesada tendrá derecho a que los datos personales se transmitan directamente de persona Responsable a persona Responsable cuando sea técnicamente posible.

No obstante, este derecho, por su propia naturaleza, no se puede aplicar cuando el tratamiento sea necesario para el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos conferidos a la persona Responsable.

El ejercicio de este derecho se entenderá sin perjuicio derecho de supresión.

La Agencia Española de Protección de Datos dispone de formularios para el ejercicio del derecho a la portabilidad que las personas interesadas pueden implementarlos y presentarlos ante cualquier persona Responsable del tratamiento de sus datos personales:

- **Formularios para el ejercicio del derecho a la portabilidad. https://www.aepd.es/es/documento/formulario-derecho-de-portabilidad.**

36. *Artículo 6, apartado 1, letra a) y artículo 9, apartado 2, letra a) del RGPD.*

pdf

3.4.7. DERECHO DE NO SER OBJETO DE DECISIONES INDIVIDUALES AUTOMATIZADAS

Este derecho consiste en que la persona afectada pueda oponerse al uso de sus datos personales para la toma de decisiones basadas en un proceso automático, que pueda afectar a sus derechos y libertades.

Las decisiones automatizadas son aquéllas que se realizan a través de medios tecnológicos sin necesidad de intervención del ser humano

> ***Ejemplo**: cuando una organización selecciona a las personas beneficiadas de un programa basándose exclusivamente en un algoritmo sin ningún tipo de intervención humana.*

Este derecho pretende garantizar que la persona afectada no sea objeto de una decisión basada únicamente en el tratamiento de tus datos, incluida la elaboración de perfiles, que produzca efectos jurídicos sobre ti o te afecte significativamente de forma similar.

Aunque este derecho está muy relacionado con el derecho de oposición, no son lo mismo, ya que el derecho de oposición al tratamiento de datos personales no se limita a las decisiones automatizadas.

El derecho a no ser objeto de decisiones individuales automatizadas no será aplicable cuando:

- Sea necesario para la celebración o ejecución de un contrato entre la persona interesada y la persona Responsable, siempre y cuando la persona Responsable garantice el derecho a obtener la intervención humana, que la persona afectada pueda expresar su punto de vista e impugnar la decisión si así lo estimase oportuno.

- El tratamiento de los datos personales se fundamente en el consentimiento expreso, siempre y cuando la persona Responsable garantice el derecho a obtener la intervención humana, que la persona afectada pueda expresar su punto de vista e impugnar la decisión si así lo estimase oportuno.

- Esté autorizado por el Derecho de la Unión o de los Estados miembros y se establezcan medidas adecuadas para salvaguardar los derechos y libertades e intereses legítimos de la persona interesada.

Estas excepciones no se aplicarán sobre las categorías especiales de datos salvo que la persona afectada haya dado su consentimiento de forma explícita o el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros y se hayan tomado las medidas adecuadas para salvaguardar los derechos y libertades e intereses legítimos de la persona afectada.

La Agencia Española de Protección de Datos dispone de formularios para el ejercicio del derecho a no ser objeto de decisiones individuales automatizadas que las personas interesadas pueden implementarlos y presentarlos ante cualquier persona Responsable del tratamiento de sus datos personales:

- **Formularios para el ejercicio del derecho a no ser objeto de decisiones individualizadas. https://www.aepd.es/es/documento/formulario-derecho-de-oposicion-decisiones-automatizadas.pdf**

3.5. TRATAMIENTOS CONCRETOS

En la LOPDGDD figuran una serie de tratamientos que por su particularidad se les da una especial relevancia. Son los siguientes:

- Tratamiento de datos de contacto, de empresarios individuales y de profesionales liberales.
- Sistemas de información crediticia.
- Tratamientos relacionados con la realización de determinadas operaciones mercantiles.
- Tratamientos con fines de videovigilancia.
- Sistemas de exclusión publicitaria.
- Tratamiento de datos para la protección de las personas que informen sobre infracciones normativas.
- Tratamiento de datos en el ámbito de la función estadística pública.
- Tratamiento de datos con fines de archivo en interés público por parte de las Administraciones Públicas.
- Tratamiento de datos relativos a infracciones y sanciones administrativas.

A continuación, se explican los tratamientos que es más probable que se lleven a cabo en una organización del TSAS debido a su actividad:

Tratamiento de datos de empresarios individuales y profesionales individuales.

Las organizaciones podrán tratar los datos personales de autónomos/as y de profesionales individuales basándose en el interés legítimo de la organización[37] (licitud del tratamiento), siempre que los datos se utilicen exclusivamente para que puedan prestar su servicio.

Tratamientos con fines de videovigilancia. Lo más significativo respecto a este tratamiento es:

- Las organizaciones podrán llevar a cabo tratamiento de imágenes a través de cámaras o videocámaras para preservar la seguridad en sus instalaciones.
- No podrán captarse imágenes de la vía pública a no ser que sean imprescindibles para preservar la seguridad.
- Sólo se pueden conservar los datos obtenidos durante un mes, excepto cuando sirvan de prueba para acreditar un acto contra la integridad de personas, bienes o instalaciones. En este caso, las imágenes deben entregarse a la autoridad competente en un plazo de 72 horas desde que se tenga constancia del acto grabado.
- Para informar del tratamiento basta con colocar un cartel informativo visible que incluya:

  • La existencia del tratamiento.

  • La identidad de la persona responsable.

  • La posibilidad de ejercitar los derechos

  • Un código de conexión o dirección de internet donde figure la información anterior si se estima oportuno.

- El tratamiento de los datos personales de las personas empleadas se analiza en el apartado 3.8. Garantía de los derechos digitales.

Tratamiento de datos para la protección de las personas que informen sobre infracciones normativas. Este tratamiento lo llevarán a cabo las organizaciones que dispongan de un Canal de denuncias y tengan que implantar procedimientos en los que se debe proteger a las personas informantes y a terceras personas afectadas.

37. *Artículo 6.1.f) del RGPD.*

38. *Plataforma de ONG de Acción Social. (2021). Manual para la Implementación de los Elementos Básicos de Cumplimiento Normativo.*

La protección de datos de los canales de denuncias se trata en detalle en el Manual para la Implementación de los Elementos Básicos de Cumplimiento Normativo[38], por lo que se remite a dicha publicación.

3.6. TRANSFERENCIAS INTERNACIONALES DE DATOS

Una transferencia internacional de datos se produce cuando los datos personales que son tratados por una organización son enviados a una persona destinataria situada fuera del Espacio Económico Europeo[39].

Dado que normalmente no se suelen hacer transferencias internacionales de datos desde organizaciones del TSAS no se va a profundizar en el tema, aunque se van a mencionar las ideas principales por si fuera necesario.

Hay tres supuestos principales relativos a las transferencias internacionales de datos:

1. La Comisión Europea ha decidido que el país u organización internacional garantiza un nivel de protección adecuado: se pueden realizar transferencias internaciones y no se requerirá ninguna autorización previa[40]. En la Agencia Española de Protección de Datos se puede consultar el listado donde figuran los países que figuran como adecuados.

2. No se ha decidido que el país u organización internacional garantiza un nivel de protección adecuado, pero se establecen las garantías adecuadas y se asegura que se respetan los derechos de las personas afectadas y que éstas puedan ejercer las acciones legales efectivas: se pueden realizar transferencias internacionales y no se requerirá autorización previa de una autoridad de control siempre y cuando las garantías de que se dispone de un nivel de protección adecuado se hayan presentado ante la autoridad de control.

3. No se ha decidido que el país u organización internacional garantiza un nivel de protección adecuado, ni se establecen las garantías adecuadas ni se asegura que se respetan los derechos de las personas afectadas y que éstas puedan ejercer las acciones legales efectivas: se podrá efectuar cuando se cumplan alguna de las siguientes condiciones[41]:

- La persona interesada ha dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informada de los posibles riesgos de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas.
- La transferencia sea necesaria para la ejecución de un contrato entre la persona interesada y la organización o para la ejecución de medidas precontractuales adoptadas a solicitud de la persona interesada.
- La transferencia sea necesaria para la celebración o ejecución de un contrato, en interés de la persona interesada, entre la organización y otra persona física o jurídica;
- La transferencia sea necesaria por razones importantes de interés público;
- La transferencia sea necesaria para la

39. *Países de la Unión Europea, Islandia, Liechtenstein y Noruega*

40. *Artículo 45 del RGPD.*

41. *Artículo 49 del RGPD.*

formulación, el ejercicio o la defensa de reclamaciones;

- La transferencia sea necesaria para proteger los intereses vitales de la persona interesada o de otras personas, cuando la persona interesada esté física o jurídicamente incapacitada para dar su consentimiento;

- La transferencia se realice desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero sólo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta. En este supuesto se requiere la autorización previa de una autoridad de control, concretamente de la Agencia Española de Protección de Datos.

En todo caso, con anterioridad a la realización de una transferencia internacional de datos se recomienda que se consulte previamente a la Agencia Española de Protección de Datos para asegurar que se respetan en todo momento los derechos de las personas afectadas y que no se incumple ningún principio de protección de datos.

3.7. AUTORIDADES DE PROTECCIÓN DE DATOS

Las Autoridades de Protección de Datos son organismos independientes encargados de velar y supervisar el cumplimiento del RGPD en cada Estado miembro de la UE mediante los poderes de investigación y correctivos. Existe una en cada Estado miembro de la UE. En España la autoridad estatal es la Agencia Española de Protección de Datos (AEPD).

3.7.1. LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD)

La Agencia Española de Protección de Datos (AEPD) es la autoridad estatal de control independiente encargada de velar por el cumplimiento de la normativa sobre protección de datos y controlar su aplicación. Fue creada en 1992 mediante la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD) y comenzó a funcionar en 1994.

Funciones de las autoridades de control

Las funciones de la AEPD son las mismas que las del resto de autoridades de control de protección de datos de los estados integrantes de la UE[42] y son las siguientes:

- Controlar la aplicación del RGPD y hacerlo aplicar.

- Promover la sensibilización de todos los aspectos de la protección de datos a la ciudadanía y a responsables y encargados de tratamientos.

- Asesorar a los gobiernos y otras instituciones y organismos públicos en materia de protección de datos sobre las medidas legislativas y administrativas.

- Informar a las personas interesadas en relación con el ejercicio de sus derechos.

- Recibir, tramitar, archivar o resolver las reclamaciones presentadas por personas afectadas.

- Cooperar con otras autoridades de control y contribuir a las actividades del Comité Europeo de Protección de

42. *Artículo 57 del RGPD.*

Datos.

- Evaluar los cambios tecnológicos que puedan tener incidencia e impacto en la protección de datos.

- Adoptar cláusulas contractuales tipo y autorizar las cláusulas no tipo.

- Elaborar y actualizar la lista de entidades obligadas a realizar evaluaciones de impacto de protección de datos y responder las consultas previas al respecto.

- Fomentar y gestionar la creación de códigos de conducta y mecanismos de certificación en protección de datos.

- Aprobar las normas corporativas vinculantes.

- Registrar infracciones y medidas adoptadas.

Poderes de las autoridades de control de protección de datos

Los poderes[43] atribuidos a cada autoridad de control de protección de datos son de investigación, correctivos y de autorización y consultivos:

- **Poderes de investigación:**

  - Ordenar a las personas responsables y encargadas del tratamiento que faciliten cualquier información que requieran para el desempeño de sus funciones.
  - Realizar investigaciones en forma de auditorías de protección de datos.
  - Revisar las certificaciones expedidas.
  - Notificar a las personas responsables y encargadas las presuntas infracciones cometidas.
  - Obtener de responsables y encargados el acceso a todos los datos personales y a toda la información necesaria para ejercer sus funciones.
  - Obtener el acceso a todos los locales de responsable y encargado del tratamiento, incluidos los equipos y medios de tratamiento de datos, de acuerdo con el Derecho procesal de la UE o de los Estados miembros.

- **Poderes correctivos:**

  - Sancionar a responsables y encargados del tratamiento con una advertencia cuando las actividades de tratamiento puedan suponer una infracción del RGPD.
  - Sancionar a responsables y encargados del tratamiento con apercibimiento cuando las actividades de tratamiento hayan infringido el RGPD.
  - Ordenar a responsables o encargados del tratamiento que atiendan las solicitudes de ejercicio de los derechos de las personas interesadas.
  - Ordenar a responsables o encargados del tratamiento que las actividades de tratamiento se ajusten a las disposiciones del RGPD, cuando proceda, de una determinada manera y dentro de un plazo específico.
  - Ordenar a responsables del tratamiento que comuniquen a las personas interesadas las brechas de seguridad.
  - Imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición.
  - Ordenar la rectificación o supresión de datos personales o la limitación del tratamiento, y notificar dichas medidas a los interesados.
  - Imponer multas administrativas.
  - Ordenar la suspensión de los flujos de datos hacia una persona destinataria situada en un tercer país o hacia una organización internacional.

43. *Artículo 58 del RGPD*

- **Poderes de autorización y consultivos:**
  - Asesorar al responsable del tratamiento conforme al procedimiento de consulta previa.
  - Emitir, por iniciativa propia o solicitud previa, dictámenes destinados al Parlamento nacional, al Gobierno del Estado miembro o a otras instituciones y organismos, así como al público, sobre cualquier asunto relacionado con la protección de datos personales.
  - Autorizar el tratamiento realizado por un responsable en el ejercicio de una misión realizada en interés público, en concreto, el tratamiento en relación con la protección social y la salud pública.
  - Emitir dictamen y aprobar proyectos de códigos de conducta.
  - Acreditar los organismos de certificación.
  - Expedir certificaciones y aprobar criterios de certificación.
  - Adoptar cláusulas tipo de protección de datos.
  - Autorizar las cláusulas contractuales en relación con transferencias internacionales.
  - Autorizar los acuerdos administrativos en relación con transferencias internacionales.
  - Aprobar normas corporativas vinculantes.

3.7.2. AUTORIDADES DE PROTECCIÓN DE DATOS AUTONÓMICAS

Se crearon cuatro agencias de protección de datos autonómicas, aunque a fecha actual sólo perduran tres:

- Agencia de Protección de datos de Madrid, creada en 2001 y suprimida en 2013.
- Autoridad Catalana de Protección de Datos, creada en 2003. **Inicio. Autoridad Catalana de Protección de Datos (gencat.cat)**
- Agencia Vasca de Protección de Datos, creada en 2004. **Agencia Vasca de Protección de Datos (euskadi.eus)**
- Consejo de Transparencia y Protección de Datos de Andalucía, creada en 2014. **Inicio | CTPD Andalucía (ctpdandalucia.es)**

Las autoridades de control de protección de datos autonómicas pueden ejercer las funciones y potestades de las autoridades de control cuando se refieran a:

- Tratamientos de los que sean responsables entidades del sector público de la Comunidad Autónoma o de las Entidades Locales incluidas en su ámbito territorial.
- Tratamientos realizados por personas físicas o jurídicas para el ejercicio de funciones públicas en materias que sean competencia de la correspondiente Administración Autonómica o Local.
- Tratamientos que estén expresamente previstos en los respectivos Estatutos de Autonomía.

3.8. GARANTÍA DE LOS DERECHOS DIGITALES

En la LOPDGDD se introduce, como novedad, el reconocimiento de una serie de derechos digitales de la ciudadanía de acuerdo a lo establecido en la Constitución Española. Se divide entre derechos digitales de carácter personal y los que afectan a las personas en el ámbito laboral:

- **Derechos digitales de carácter personal:**

1. Derecho a la neutralidad de internet: los proveedores de los servicios de internet no pueden condicionar el tráfico de datos según el perfil de cada persona. Es decir, que no pueden usar filtros o bloquear a personas usuarias, denegar servicios o eliminar resultados de búsquedas.

2. Derecho al acceso universal a internet: todas las personas tienen derecho a acceder a internet sin importar su condición, personal, social, económica o geográfica. Garantiza el acceso

universal, asequible, de calidad y no discriminatorio.

3. Derecho a la seguridad digital: los proveedores de servicios de internet deben informar a las personas que usan sus servicios de sus derechos.

4. Derechos a la educación digital: el sistema educativo debe garantizar la formación en competencias digitales del personal docente y del alumnado.

5. Derecho a la protección de menores en internet implica que:

- Las personas responsables de menores procurarán que éstos últimos hagan un uso responsable de dispositivos digitales y de internet para garantizar el desarrollo adecuado de su personalidad y preservar su dignidad y derechos fundamentales.
- Intervención del Ministerio Fiscal cuando la utilización o difusión de imágenes o información personal de menores en las redes sociales y servicios de la sociedad de la información equivalentes puedan implicar una intromisión ilegítima en sus derechos fundamentales.

Implica tener especial cuidado con las imágenes de menores que se suben a internet ya que pueden afectar a su intimidad e incluso perjudicar su reputación online.

El principal riesgo que existe cuando se publica la imagen de menores en internet es que las imágenes puedan ser capturadas y recopiladas por depredadores sexuales virtuales y que las compartan con otros.

Tal y como se ha mencionado anteriormente, el tratamiento de datos personales de menores requiere del consentimiento expreso de quien ostente su patria potestad o tutela o del menor cuando es mayor de 14 años, no obstante, se recomienda no publicar imágenes de menores que sean identificables a no ser que sea estrictamente necesario.

6. Derecho a la rectificación en internet: obligación de adoptar protocolos para que, en caso de que se difundan contenidos que atenten contra el derecho al honor, la intimidad personal y familiar en Internet y el derecho a comunicar o recibir libremente información veraz, las personas usuarias puedan solicitar su rectificación.

7. Derecho a la actualización de informaciones en medios de comunicación digitales: todas las personas tienen derecho a solicitar a los medios de comunicación digitales, cuando les esté causando un perjuicio y no se refleje su situación actual, la inclusión de un aviso de actualización visible.

8. Derecho al olvido en búsqueda en internet y en redes sociales: todas las personas tienen derecho a que en los motores de búsqueda en internet se eliminen los enlaces que figuren tras una búsqueda con su nombre. Estos enlaces tienen que contener información inadecuada, inexacta, no pertinente, no actualizada o excesiva. Este derecho no implica que el enlace se suprimirá, si no que dejará de ser visible en la búsqueda, y se mostrará cuando se busque otro término, palabra o nombre.

Igualmente, las personas tienen derecho a que se supriman sus datos personales facilitados de las redes sociales. Y, en caso de que sus datos personales hayan sido facilitados por terceros, cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos, siempre y cuando los datos no hubiesen sido facilitados por personas físicas en el ejercicio de actividades personales o domésticas.

9. Derecho a la portabilidad en redes sociales y servicios equivalentes: las personas usuarias tendrán derecho

a recibir y transmitir la información y contenidos que hubieran proporcionado a servicios de redes sociales y servicios de la sociedad de la información, así como a que los prestadores los transmitan a otros prestadores.

10. Derecho al testamento digital: los derechos digitales de acceso, modificación o eliminación de datos personales de las personas fallecidas pueden ser ejercidos por familiares o sus herederos, siempre que no hubieran determinado expresamente lo contrario antes de su muerte. En el caso de que se trate de menores también podrán ejercitar sus derechos representantes legales o el Ministerio Fiscal.

- **Derechos digitales de ámbito laboral:**

1. Derecho a la intimidad y uso de dispositivos digitales: la organización debe garantizar que las personas contratadas cuando usen dispositivos digitales:
  - La organización sólo podrá acceder al contenido de los dispositivos digitales de las personas trabajadoras (ordenadores, móviles, tablets, etc.) para revisar el cumplimiento de las obligaciones laborales y tener constancia de que los dispositivos se están usando adecuadamente.
  - La organización debe establecer directrices para el uso de los dispositivos que respete y proteja la intimidad de las personas trabajadoras (protocolo de uso de dispositivos cedido).
  - Si la organización autoriza el uso de los dispositivos de trabajo para su uso personal y privado, la entidad deberá establecer por escrito las directrices para su uso.

Este derecho está relacionado con lo establecido en el artículo 20.b del Estatuto de los Trabajadores[44].

2. Derecho a la desconexión digital: las personas empleadas tienen derecho a disponer de tiempo de descanso, permisos y vacaciones, así como a su intimidad personal y familiar con desconexión digital. Para que se pueda ejercer, la organización:
  - Deberá elaborar una política interna de personal en la que se regulará el ejercicio del derecho a la desconexión, incluyendo cuando se realiza total o parcialmente el trabajo a distancia mediante el uso de herramientas tecnológicas.
  - Deberá implantar acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática.

3. Intimidad frente al uso de dispositivos de vigilancia y de grabación de sonidos en el espacio de trabajo: implica que la instalación y uso de aparatos de videovigilancia y grabación de sonidos:
  - Sólo estará permitido para las funciones de control de las personas trabajadoras contempladas en la legislación.
  - Sólo podrá permitirse si se ha informado previamente a las personas trabajadoras de forma clara, concisa y expresa. En caso de que con el uso de dispositivos de videovigilancia y de grabación de sonidos se captase un hecho ilícito llevado a cabo por una persona trabajadora, se admiti-

44. *Artículo 20 bis del Estatuto de los Trabajadores: "Derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión. Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales".*

rá que se ha cumplido con el deber de informar si existe, al menos, un cartel informativo de zona vigilada.
- No podrá permitirse en zonas destinadas al descanso o esparcimiento, como vestuarios, aseos y comedores.

4. Intimidad frente al uso de localizadores geográficos: implica que el uso de localizadores geográficos:
- Sólo estará permitido para las funciones de control de las personas trabajadoras contempladas en la legislación.
- Sólo podrá permitirse si se ha informado de su uso previamente a las personas trabajadoras de forma clara, concisa y expresa. También se les debe informar acerca de sus derechos de acceso, rectificación, limitación del tratamiento y supresión.

No todos estos derechos digitales afectan a las organizaciones del TSAS ya que la mayoría hacen referencia a proveedores de servicios de internet, redes sociales y de servicios equivalentes. Los derechos digitales que las entidades sociales tienen que tener en cuenta en su Modelo de protección de datos son el derecho a la protección de menores en internet y todos los de ámbito laboral.

Cuando en la LOPDGDD se tratan los derechos digitales se incluyen algunas medidas que las organizaciones deben implantar para que se puedan ejercer con garantías. Estas medidas, como puede ser un protocolo de uso de dispositivos cedidos o la política de personal que contemple la desconexión digital, tal y como se tratará más adelante en esta guía, son medidas mitigadoras.

04

LA PROTECCIÓN DE DATOS EN LAS ORGANIZA-CIONES DE ACCIÓN SOCIAL

4.1.MEDIDAS DE RESPONSABILIDAD ACTIVA

La responsabilidad activa (de acuerdo a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales) o responsabilidad proactiva (según el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016) es la obligación que tienen las organizaciones no solo de cumplir la normativa, sino de demostrar que la cumplen.

Cada organización tiene que aplicar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento cumple con la normativa de protección de datos y que se tratan los datos personales de un modo lícito y seguro[45].

Tal y como veremos en el apartado 4.2. Roles en la organización, normalmente será la persona Responsable del tratamiento la encargada de llevar a cabo casi todas las tareas y desempeñar las funciones relativas a la protección de datos en la entidad, no obstante, para simplificar, se va a hacer referencia a la organización en lugar de a la persona Responsable del tratamiento.

La responsabilidad activa en materia de protección de datos se basa en el compromiso, la proactividad y la responsabilidad:

a. **Compromiso:** La responsabilidad activa debe ser adoptada por todas las personas integrantes de la organización, incluyendo los órganos directivos, todo el personal contratado y las personas voluntarias.
b. **Proactividad:** La responsabilidad activa en protección de datos quiere decir que todas las organizaciones han de desarrollar e implementar las medidas técnicas y organizativas necesarias para garantizar el cumplimiento nor-

45. *Artículo 24.1 del RGPD.*

mativo. Está relacionado con la protección de datos desde el diseño y por defecto.

c. Responsabilidad: La organización debe garantizar que todas las personas integrantes cumplan con las responsabilidades que se les asignan en materia de protección de datos.

Conforme al principio de responsabilidad activa, no es suficiente con señalar que la organización no incumple con la normativa exigida, sino que se tiene que demostrar que se cumple y cómo.

Entre las medidas técnicas y organizativas que las organizaciones deben cumplimentar para garantizar que los tratamientos que se realizan sean conformes con la legislación y estén en condiciones de demostrarlo se encuentran:

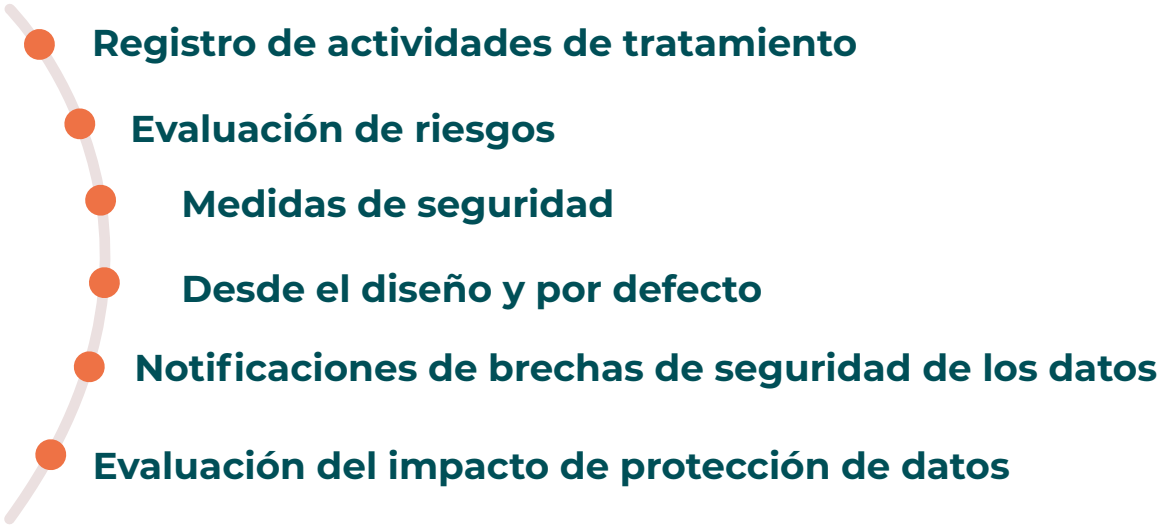


Ilustración 5 Medidas de responsabilidad activa

Otras medidas que las organizaciones están obligadas a instaurar en determinadas condiciones, que se tratarán más adelante en el punto 4.2. Roles en la entidad, son la definición clara de las funciones de la persona Responsable del tratamiento o el nombramiento de una persona Delegada de protección de datos, si fuera el caso.

Las medidas de responsabilidad activa suponen la implantación de un sistema interno de cumplimiento en materia de protección de datos, que estará integrado por la política de protección de datos de la organización y una serie de políticas, procedimientos, controles, medidas y evaluaciones que deberán ser actualizados y revisados periódicamente.

En esta línea, es importante resaltar que para poder demostrar que se ha implantado un sistema de cumplimiento eficiente hay que dejar constancia documental de todas las acciones que se han llevado a cabo, así como de las medidas técnicas y organizativas desarrolladas.

A continuación, se describen cada una de las principales medidas de responsabilidad activa:

4.1.1. REGISTRO DE ACTIVIDADES DE TRATAMIENTO

Es un documento que constará por escrito, preferiblemente en formato electrónico, que recoge las categorías de datos personales que la organización trata, la legitimidad para dicho tratamiento, la finalidad del tratamiento, el período de conservación de los datos y otra información pertinente, incluida la identificación de la

persona Responsable del tratamiento.

La legislación exige un contenido mínimo[46]:

- El nombre y los datos de contacto de la persona Responsable y de la persona Delegada de protección de datos (si la hubiera).
- Los fines del tratamiento.
- La descripción de las categorías de personas interesadas.
- La descripción de las categorías de datos personales.
- Las categorías de las personas destinatarias a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales.
- Si las hubiera, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, si fuera el caso, la documentación de garantías adecuadas.
- Los plazos previstos para la supresión de las diferentes categorías de datos o los criterios para establecerlos.
- La descripción general de las medidas técnicas y organizativas de seguridad implantadas por la organización.

Este contenido será el mínimo que debe tener un registro de actividades de tratamiento. Cada organización puede decidir si añadir otra información que pudiera serle útil, ya sea para el cumplimiento de la normativa de protección de datos como para la mejora de los procesos organizativos.

Al tener que estar el registro disponible si la autoridad de control lo solicitase, debe evitarse que se pudiera ver información que pudiera ser perjudicial para la organización, para los tratamientos de datos personales y que comprometiese la propia seguridad de los datos.

El registro de actividades no es obligatorio para todas las organizaciones. Sólo es obligatorio para una entidad cuando:

- Tenga más de 250 personas empleadas.
- Un tratamiento, que sea habitual, pueda conllevar un riesgo para los derechos y libertades de las personas interesadas.
- Se trate categorías especiales de datos.
- Se trate datos a gran escala o de manera sistemática.
- Se trate datos relativos a condenas o delitos penales.

REGISTRO DE ACTIVIDADES DE TRATAMIENTO
Documento escrito, preferiblemente en formato electrónico
Debe tener un contenido mínimo
No es obligatorio a no ser que se den ciertas condiciones

Tabla 1 Registro de Actividades de tratamiento

46. *Artículo 30 del RGPD y artículo 31 de la LOPDGDD*

4.1.2. EVALUACIÓN DE RIESGOS

Una de las medidas de responsabilidad activa a cumplimentar por las organizaciones es la evaluación de riesgos. En este sentido, es importante señalar que todo el proceso de evaluación de riesgos que se lleve a cabo debe estar documentado, para así poder demostrar que se ha efectuado.

La evaluación o gestión de los riesgos consiste en identificar el riesgo y su origen, llevar a cabo su análisis y la posterior gestión de las medidas que pudieran ser necesarias para mitigar dicho riesgo y evitar las posibles consecuencias negativas que el tratamiento pudiera implicar para las personas interesadas.

El enfoque basado en el riesgo es un factor clave en la normativa de protección de datos, ya que las organizaciones deberán analizar el nivel de riesgo en el que se encuentra respecto de los tratamientos de datos antes de llevarlos a cabo, durante y después.

En primer lugar, se debe entender qué se considera como riesgo. En el RGPD se menciona en todo momento **el riesgo para los derechos y libertades**[47] de las personas afectadas, que es la posibilidad de que se vulneren no sólo los derechos o libertades de las personas cuyos datos personales se tratan, sino también los de todas las personas afectadas por el tratamiento[48]. No se debe confundir con el riesgo de cumplimiento normativ o, que se puede definir como la posibilidad de que se produzca un incumplimiento de la normativa de protección de datos en la entidad.

Así, los conceptos de gestión de riesgos para los derechos y libertades y gestión de riesgos de cumplimiento normativo no son lo mismo:

a. La gestión del riesgo para los derechos y libertades analiza el impacto y la probabilidad de causar daño a las personas al tratar sus datos personales.

b. La gestión de riesgo de cumplimiento normativo analiza el grado de cumplimiento de las obligaciones legales que tiene la entidad en relación con los tratamientos de datos personales que realiza.

47. *El Considerando 75 del RGPD establece que: "Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados".*

48. *Ver el documento Gestión del riesgo y evaluación de impacto en tratamientos de datos personales de la Agencia de Protección de datos*

No obstante, ambos están muy relacionados ya que el cumplimiento normativo es un requisito para gestionar los riesgos para los derechos y libertades. La evaluación de riesgos de la organización debe ir enfocada a los riesgos para los derechos y libertades, es decir, que no basta con prevenir que la organización incumpla la legislación protegiéndola de los posibles incumplimientos, sino que tiene que evitar que se perjudique a cualquier persona como consecuencia de los tratamientos de datos personales que se lleven a cabo. Las organizaciones del Tercer Sector de Acción Social en mayor medida, dado su carácter social, deben velar para que no se perjudique a ninguna persona como consecuencia de los datos que traten.

Como ya se ha mencionado, la evaluación de los riesgos es un proceso cuyas fases son:

Ilustración 6 Proceso de gestión y evaluación de los riesgos

I. DESCRIPCIÓN DE LOS TRATAMIENTOS:

No se podrán identificar ni evaluar los riesgos si no se conocen previamente los tratamientos que lleva a cabo la organización ni la descripción de los mismos.

Para describir los tratamientos es necesario analizar el ciclo de vida de los datos y determinar la naturaleza, el contexto y el alcance y la finalidad de cada tratamiento.

Saber acerca del ciclo de vida de los datos permitirá identificar los tratamientos diferentes que se llevan a cabo de los datos personales. El ciclo de vida de los datos se puede dividir en las siguientes etapas:

Ilustración 7 Etapas del ciclo de vida de los datos

1. **Captura o recogida:** los datos son obtenidos.
2. **Almacenamiento:** se establecen categorías y se asignan para que sean guardados en los archivos digitales y/o físicos.
3. **Uso:** se realiza una operación o varias sobre los datos de forma automatizada o manual.
4. **Cesión o transferencia a una tercera persona:** si fuera el caso, los datos se traspasan o se comunican a una tercera persona.
5. **Eliminación:** los datos son destruidos de manera que no podrán ser recuperados en el futuro.

Es fundamental determinar la naturaleza, el alcance o ámbito, el contexto y la finalidad de cada tratamiento de datos identificado que pueden influir en todas las etapas del ciclo de vida de los datos:

a. Naturaleza del tratamiento: cómo se traten los datos influirá en las medidas a tomar por parte de la organización. Implica identificar, entre otros:

- Las diferentes actividades de los procesos en las que se implementa.
- El flujo de datos personales.
- Si los datos se tratan en formato físico o digitalmente y si es de forma manual o automatizada.
- Los elementos sobre los que se implementa el tratamiento (aplicaciones, programas informáticos).
- Las personas de la organización que acceden a los datos.
- Las características tecnologías relevantes en el tratamiento.
- La participación de la figura del Encargado del tratamiento en distintas operaciones (gestorías, proveedores de correo electrónico, hosting, mantenimiento de la página web, servicio de almacenaje, etc.)
- Posibles incidentes de seguridad sobre los datos personales que pueden dar lugar a brechas de seguridad.

b. Ámbito / alcance: se tiene que determinar, entre otros:

- Tipo de datos recogidos, procesados o inferidos en el tratamiento.
- Categoría de personas interesadas: menores de 14 años, víctimas de violencia de género, personas con discapacidad, personas mayores, personas que acceden a servicios sociales, personas en riesgo de exclusión social, personas vulnerables, personas contratadas por la organización, etc.
- Número de personas afectadas.
- Diversidad de los datos tratados.
- Duración en el tiempo del tratamiento y de la conservación de los datos.
- El volumen de los datos.
- La extensión geográfica de los datos.
- La frecuencia de la recogida de los datos.

c. Contexto: los riesgos serán diferentes dependiendo de la organización, de qué se desprende de su análisis interno y externo. Hay que considerar, entre otros factores:

- El sector de la entidad y el colectivo al que se dirigen sus actuaciones.
- El entorno social en el que se desenvuelve.
- La legislación externa e interna que le es de aplicación.
- La interacción con otros tratamientos de la entidad, como pueden ser la prevención del blanqueo de capitales, gestión de los elementos básicos del Modelo de Cumplimiento Normativo, planes de igualdad, gestión de personas, etc.
- Las cesiones de datos que son necesarias.
- Las transferencias internacionales que se produzcan.
- Las brechas de seguridad o incidentes que se producen en tratamientos relacionados.
- Los efectos colaterales en la sociedad, es decir, los perjuicios pueden suceder accidentalmente o de for-

ma no intencional como consecuencia del tratamiento. Se trata de una consecuencia en lugar de un factor.

d. Finalidad del tratamiento: dependiendo de para qué se vayan a usar los datos personales las medidas a adoptar serán diferentes. Es diferente que se trate los datos para el envío del boletín de noticias, para la gestión del personal o en la gestión y ejecución de programas destinados a personas vulnerables.

Los fines del tratamiento y su legitimación han de estar fijados con anterioridad al inicio de la gestión del riesgo.
Se recomienda la identificación de los fines últimos y de otros fines vinculados a los principales o últimos.

II. IDENTIFICACIÓN DEL RIESGO Y SU ORIGEN (AMENAZAS):

Los riesgos para los derechos y libertades de las personas afectadas son variables y dependen de las amenazas a las que esté expuesta cada actividad de tratamiento. Todas las actividades de tratamiento de datos personales implican un riesgo para las personas cuyos datos son tratados y, concretamente, para sus derechos y libertades.

Cada organización debe identificar sus propios riesgos basándose en la descripción de los tratamientos que se llevan a cabo. Es importante analizar los riesgos que existen para establecer las medidas técnicas destinadas a mitigarlos.

Desde la perspectiva de protección de datos personales, los riesgos se pueden clasificar en dos grandes grupos:

1. Riesgos asociados a la protección de los datos (información): afectan a la confidencialidad, disponibilidad e integridad de los datos.

Ejemplos de riesgos asociados a la protección de los datos:

» *Acceso ilegítimo a datos personales recabados por la organización*

Confidencialidad

» *Eliminación de datos personales necesarios para una finalidad*

Disponibilidad

» *Cesión no autorizada e ilegítima de los datos a una tercera persona*

Confidencialidad

» *Modificación no autorizada de los datos*

Integridad

2. Riesgos asociados a la defensa de los derechos y libertades de las personas interesadas: relacionados con garantizar el ejercicio de los derechos de las personas interesadas y con garantizar los principios relativos a la protección de datos:

Ejemplos de riesgos asociados a la defensa de los derechos y libertades de las personas interesadas y sus posibles consecuencias:

» *No hay un procedimiento diseñado para que las personas interesadas ejerzan sus derechos*

» *Tratamiento de datos personales sensibles sin consentimiento explícito*

» *Robo de datos personales de las personas interesadas del servidor de la organización*

La Agencia Española de Protección de Datos (AEPD) tiene publicada una herramienta de evaluación del nivel de riesgo de un tratamiento denominada **EVALÚA_RIESGO RGPD (https://www.aepd.es/guias-y-herramientas/herramientas/evalua-riesgo-rgpd)**, que permite realizar una primera toma de contacto a la identificación y evaluación del riesgo de un tratamiento en base a una serie de categorías de factores de riesgo. En esta guía se ha optado por usar las categorías que propone la AEPD, pero adaptándolas al análisis realizado en el apartado "Descripción de los tratamientos". El uso de las mismas categorías permite que las organizaciones puedan usar las herramientas disponibles y gratuitas de la AEPD como complemento al análisis propuesto en esta guía.

Las actividades de tratamiento se pueden agrupar por tipologías, englobando en un mismo grupo todas las actividades similares que estén expuestas a riesgos similares. Esto facilita el análisis y el establecimiento de medidas mitigadoras de riesgos.

A continuación, se muestran los factores de riesgo para cada categoría de factores de riesgo relacionados con la naturaleza, ámbito, contexto y finalidad del tratamiento:

DESCRIPCIÓN DEL TRATAMIENTO	CATEGORÍAS DE FACTORES DE RIESGO	FACTORES DE RIESGO
NATURALEZA	Recogida y generación de datos	Factores de riesgo derivados de recogida o generación de datos de forma específica
	Factores técnicos del tratamiento	Factores de riesgo derivados de implementarse con determinadas características técnicas o tecnologías
	Brechas de seguridad	Factores de riesgo que se derivan de la posible materialización de brechas de seguridad sobre los datos personales
ÁMBITO / ALCANCE	Tipos de datos utilizados	Factores de riesgo derivados de los datos recogidos, procesados o inferidos en el tratamiento
	Categorías de personas interesadas	Factores de riesgo relativos a la categoría de personas interesadas como menores de 14 años, víctimas de violencia de género, personas con discapacidad, personas mayores, personas que acceden a servicios sociales, personas en riesgo de exclusión social, personas vulnerables, personas contratadas por la organización, etc.
	Extensión y alcance del tratamiento	Factores de riesgo relativos al número de personas afectadas, a la diversidad de los datos tratados, a la duración en el tiempo del tratamiento y de la conservación de los datos, el volumen de los datos, la extensión geográfica de los datos, la frecuencia de la recogida de los datos, etc.

CONTEXTO	Categoría de las personas Responsable / Encargada del tratamiento	Factores de riesgo derivados del sector de la entidad y el colectivo al que se dirigen sus actuaciones
	Comunicaciones de datos	Factores de riesgo derivadas de las comunicaciones de datos a terceros en el marco del tratamiento
	Efectos colaterales del tratamiento	Factores de riesgo que se derivan de consecuencias no contempladas en los propósitos originales previstos del tratamiento
FINALIDAD	Operaciones relacionadas con los fines del tratamiento	Factores de riesgo que se derivan del fin declarado del tratamiento y otros fines vinculados al propósito principal

Tabla 2 Categorías y factores de riesgo

Para la identificación de los riesgos también nos vamos a basar en el enfoque que figura en el **Manual de Elaboración de Planes de Cumplimiento Normativo,** donde se diferencia entre riesgo genérico y riesgo específico:

1. Riesgo genérico es una posible conducta o actividad que se produce en la organización y que puede afectar a la protección de los datos y/o defensa de los derechos y libertades de las personas interesadas.
2. Riesgo específico es un riesgo genérico pero adaptado a la especificidad de la organización que esté realizando el análisis.

Mientras los riesgos genéricos serán comunes a todas las organizaciones del TSAS, los riesgos específicos serán diferentes en cada organización y, concretamente, dependerán de las conclusiones obtenidas en la descripción de los tratamientos.

Así, para la identificación de los riesgos, se parte de la naturaleza, el contexto y el alcance y la finalidad de cada tratamiento analizados (descripción de los tratamientos), y de cada categoría de los factores de riesgo, se identifican los riesgos genéricos para una entidad que, a su vez, se dividen entre riesgos asociados a la protección de los datos y riesgos asociados a la defensa de los derechos y libertades de las personas interesadas.

A continuación, se muestran algunos ejemplos de riesgos genéricos a los que pueden enfrentarse las organizaciones del TSAC:

Ver tabla en la página siguiente

DESCRIPCIÓN DEL TRATAMIENTO	CATEGORÍAS DE FACTORES DE RIESGO	FACTORES DE RIESGO	EJEMPLOS DE RIESGOS GENÉRICOS
NATURALEZA	Recogida y generación de datos	Factores de riesgo derivados de recogida o generación de datos de forma específica	Riesgos asociados a la protección de los datos: - Que la confidencialidad de los datos esté comprometida - Que los datos recogidos no sean precisos, completos, consistentes y confiables Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando se recojan los datos mediante: - Acceso a base de datos sobre blanqueo de capitales o financiación del terrorismo - Obtenidos en zonas de acceso público - Aplicaciones - Procedentes de dos o más tratamientos con finalidades diferentes - Falta de transparencia del momento preciso de la recogida de datos
	Factores técnicos del tratamiento	Factores de riesgo derivados de implementarse con determinadas características técnicas o tecnologías	Riesgos asociados a la protección de los datos: - Que la confidencialidad de los datos esté comprometida - Que los datos no estén disponibles - Que se pierda la integridad de los datos Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando se traten datos usando: - Aplicaciones móviles - Internet de las cosas (IoT) - Inteligencia Artificial - Uso innovador o nuevas soluciones organizativas - Uso innovador de tecnologías consolidadas - Tratamientos automatizados - Videovigilancia
	Brechas de seguridad	Factores de riesgo que se derivan de la posible materialización de brechas de seguridad sobre los datos personales	Riesgos asociados a la protección de los datos: - Un incidente de seguridad puede afectar a la confidencialidad, integridad y disponibilidad de los datos personales Incidentes de seguridad que supongan una brecha de seguridad

ÁMBITO / ALCANCE	Tipos de datos utilizados	Factores de riesgo derivados de los datos recogidos, procesados o inferidos en el tratamiento	Riesgos asociados a la protección de los datos: Los riesgos que afecten a la confidencialidad, disponibilidad e integridad de los datos serán más o menos elevados en función del tipo de datos tratados Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando los datos tratados sean: Documentación personal: correspondencia por correo electrónico, documentos privados, etc. - Información de aplicaciones de registro de actividades vitales - Preferencias de consumo, hábitos, gustos, necesidades, etc. que no permitan inferir informaciones relacionadas con categorías especiales de datos - Rendimiento laboral: Control de acceso al lugar de trabajo, grabación de imágenes del puesto de trabajo, monitorización de los equipos de las personas empleadas, Inferencia del rendimiento a través de indicadores (productividad y calidad del trabajo, eficiencia, formación adquirida, objetivos conseguidos), etc. - Situación económica: renta, ingresos mensuales, situación laboral, etc. - Datos de medios de pago: números de tarjeta, números de cuenta bancaria - Datos sanitarios - Datos biométricos - Categorías especiales de datos o que permitan inferirlos: origen étnico, origen racial, opiniones políticas, afiliación sindical, datos relativos a la orientación sexual, etc. - Categorías especiales de datos seudonimizados - Datos personales relativos a condenas e infracciones penales - Datos de navegación web: registro de páginas visitadas (historial de navegación, logs de servidores web, etc.), registro del tiempo que se está en cada página, registro del momento de la visita a la página, registro del número de conexiones, etc.
	Categorías de personas interesadas	Factores de riesgo relativos a la categoría de personas interesadas como menores de 14 años, víctimas de violencia de género, personas con discapacidad, personas mayores, personas que acceden a servicios sociales, personas en riesgo de exclusión social, personas vulnerables, personas contratadas por la organización, etc.	Riesgos asociados a la protección de los datos: Los riesgos que afecten a la confidencialidad, disponibilidad e integridad de los datos serán más o menos elevados en función de las categorías de las personas interesadas Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando las personas afectadas cuyos datos se vayan a tratar o se traten sean de: - Menores de 14 años - Víctimas de violencia de género - Personas con discapacidad - Personas mayores - Personas que acceden a servicios sociales - Personas en riesgo de exclusión social - Personas vulnerables - Personas contratadas por la organización
	Extensión y alcance del tratamiento	Factores de riesgo relativos al número de personas afectadas, a la diversidad de los datos tratados, a la duración en el tiempo del tratamiento y de la conservación de los datos, el volumen de los datos, la extensión geográfica de los datos, la frecuencia de la recogida de los datos, etc.	Riesgos asociados a la protección de los datos: - La confidencialidad de los datos puede comprometerse - La disponibilidad de los datos puede disminuir - La integridad puede verse afectada Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando el tratamiento: - Involucra a gran número de sujetos - La duración sea elevada - Tenga un gran alcance geográfico - Se recopilen excesivos datos con relación al fin del tratamiento

CONTEXTO	Categoría de las personas Responsable / Encargada del tratamiento	Factores de riesgo derivados del sector de la entidad y el colectivo al que se dirigen sus actuaciones	Riesgos asociados a la protección de los datos: Los riesgos que afecten a la confidencialidad, disponibilidad e integridad de los datos serán más o menos elevados en función del colectivo Riesgo cuando la organización sea: - Organización con personas usuarias de colectivos vulnerables - Organización con personal contratado - Organización con personal voluntario
	Comunicaciones de datos	Factores de riesgo derivadas de las comunicaciones de datos a terceros en el marco del tratamiento	Riesgos asociados a la protección de los datos: - La confidencialidad de los datos puede comprometerse - Que los datos no estén disponibles o la disponibilidad sea menor - Que la integridad esté afectada Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando: - Falta de trasparencia de medios usados en el tratamiento: redes sociales, Inteligencia Artificial - Transferencias internacionales
	Efectos colaterales del tratamiento	Factores de riesgo que se derivan de consecuencias no contempladas en los propósitos originales previstos del tratamiento	- Excede las expectativas de las personas interesadas - Posible reversión no autorizada de la seudonimización - Posible pérdida de control de los datos tratados por la persona Encargada del tratamiento - Puede provocar exclusión - Puede provocar discriminación - Posible usurpación de identidad - Posible daño reputacional - Posible perjuicio económico significativo - Posible perjuicio moral significativo - Posible pérdida de confidencialidad de datos - Podría impedir el ejercicio de un derecho
FINALIDAD	Operaciones relacionadas con los fines del tratamiento	Factores de riesgo que se derivan del fin declarado del tratamiento y otros fines vinculados al propósito principal	Riesgos asociados a la protección de los datos: - La confidencialidad de los datos puede comprometerse cuando los datos son usados para otros fines vinculados - Que los datos no estén disponibles o parte de ellos para los otros fines - Que se pierda la integridad de los datos Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando los fines del tratamiento sean: - Creación, uso y otros tratamientos con perfiles - Control de las personas contratadas: evaluación, grabación de audios y/o imágenes, control del tiempo invertido en realizar tareas, control del uso de internet y del teléfono, geolocalización, monitorización y control del correo electrónico, etc. - Control de acceso a internet - Videovigilancia - Decisiones automatizadas sin intervención humana - Tratamiento automatizado para soporte a la toma de decisiones - Decidir sobre o impedir el ejercicio de derechos fundamentales: derechos de igualdad, no discriminación, intimidad personal y familiar, a la libertad sindical, etc. - Decidir sobre el control del interesado de sus datos personales: derecho de acceso, rectificación, oposición, supresión, limitación del tratamiento, etc. - Decidir sobre el acceso a un servicio - Conservación de los datos

Tabla 3 Ejemplos de riesgos genéricos asociados a cada categoría de factores de riesgo

La normativa de protección de datos[49] proporciona una lista de lo que debe de ser considerado como riesgo para los derechos y libertades de las personas interesadas. Esta lista no es excluyente, sino que proporciona una idea aproximada de lo que puede ser considerado riesgo:

- Tratamientos que pueden dar lugar problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo.

- Tratamientos que pueden privar a las personas interesadas de sus derechos y libertades o impedirles ejercer el control sobre sus datos personales.

- Tratamientos de datos personales sensibles que revelen origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas.

- Tratamientos en la elaboración de perfiles, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales.

- Tratamientos de datos personales de personas físicas vulnerables, en particular de menores de edad y personas con discapacidad.

- Tratamientos que impliquen una gran cantidad de datos personales y que afecten a un gran número de personas interesadas.

- Tratamientos que impliquen habitualmente transferencia de datos a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección.

III. ANÁLISIS DEL RIESGO:

Una vez identificados los riesgos[50], el siguiente paso es analizarlos.

El análisis del riesgo consiste en determinar, para cada riesgo, la probabilidad de que se produzca y el impacto de sus consecuencias sobre los derechos y libertades de las personas afectadas. La combinación de la probabilidad y del impacto determinará el nivel de riesgo, así, cuanto más probable sea y mayor impacto tenga el tratamiento, el nivel de riesgo será mayor y más medidas de protección de datos serán necesarias implantar para mitigarlo. El nivel de riesgo se puede representar mediante un mapa de calor:

49. *Considerando 75 del RGPD y artículo 28 de la LOPDGDD.*

50. *Basado en los establecido en el Manual de Elaboración de Planes de Cumplimiento Normativo*

PROBABILIDAD						
	CASI CIERTO	MEDIO	ALTO	ALTO	MUY ALTO	MUY ALTO
	PROBABLE	BAJO	MEDIO	ALTO	ALTO	MUY ALTO
	POSIBLE	BAJO	MEDIO	MEDIO	ALTO	ALTO
	IMPROBABLE	MUY BAJO	BAJO	MEDIO	MEDIO	ALTO
	RARO	MUY BAJO	MUY BAJO	BAJO	BAJO	MEDIO
		NO APRECIABLE	LIMITADO	MEDIO	GRAVE	MUY GRAVE
		IMPACTO				

Tabla 4 Mapa de calor del nivel de riesgo

La probabilidad mide las posibilidades de que un factor de riesgo afecte a la protección de los datos y/o defensa de los derechos y libertades de las personas interesadas. Se puede clasificar la probabilidad en cinco niveles en función de :

- Si se ha materializado previamente: cuando el factor de riesgo se ha producido anteriormente es más probable que se vuelva a producir.

- Existencia de medidas mitigadoras: si la organización tiene implantadas medidas que dificultan que la amenaza se produzca, el nivel de riesgo será menor.

- Periodicidad del tratamiento: cuanto mayor sea la frecuencia en que se lleva a cabo el tratamiento, la probabilidad de que se materialice el riesgo será mayor.

Así, la descripción de cada uno de los niveles de probabilidad sería:

a. **Raro:** la probabilidad de que se produzca es rara. No se ha materializado previamente, existen medidas implantadas y evaluadas y es un tratamiento puntual o con una periodicidad superior a la anual.
b. **Improbable:** la probabilidad de que suceda es improbable cuando no se ha materializado previamente, existen medidas implantadas y evaluadas asociadas a un tratamiento que se desarrolla con una frecuencia anual.
c. **Posible:** la probabilidad de que afecte a la protección de los datos y/o defensa de los derechos y libertades de las personas interesadas es posible cuando se ha materializado previamente, aun existiendo medidas implantadas y evaluadas referentes a un tratamiento que se desarrolla con una frecuencia diaria o semanal.
d. **Probable:** la probabilidad de que suceda es probable cuando se ha materializado previamente y las medidas implantadas a un tratamiento que se desarrolla con una frecuencia diaria o semanal no han sido evaluadas.
e. **Casi cierto:** la probabilidad de que afecte a la protección de los datos y/o defensa de los derechos y libertades de las personas interesadas es casi cierta cuando se ha producido anteriormente en repetidas ocasiones y no hay medidas asociadas a un tratamiento que se desarrolla con una frecuencia diaria o semanal.

MEDICIÓN DE LA PROBABILIDAD *INDICADORES*	RARO	IMPROBABLE	POSIBLE	PROBABLE	CASI CIERTO
Se ha materializado previamente	No se ha producido previamente	No se ha producido previamente	Se ha producido previamente	Se ha producido previamente	Se ha producido previamente en repetidas ocasiones
Medidas preventivas implantadas	Medidas de control implantadas y evaluadas	Medidas de control implantadas y evaluadas	Medidas de control implantadas y evaluadas	Medidas de control implantadas no evaluadas	No hay medidas de control implantadas
Periodicidad del tratamiento	No se suele realizar	Periodicidad anual	Tratamiento frecuente (diario /semanal)	Tratamiento frecuente (diario /semanal)	Tratamiento frecuente (diario /semanal)

Tabla 5 Indicadores para la medición de la probabilidad del riesgo

El impacto es la consecuencia de que un factor de riesgo afecte a la protección de los datos y/o defensa de los derechos y libertades de las personas interesadas. Se puede clasificar el impacto en cinco niveles en función de las consecuencias que generaría como, por ejemplo:

- Pérdida de control de algún dato personal: derivados de riesgos asociados a la protección de los datos que afectan a la confidencialidad, disponibilidad e integridad de los datos.
- El número de personas afectadas: cuanto mayor número de personas afectadas el impacto será mayor.
- La naturaleza de los datos: los datos pueden ser de carácter general, de categorías especiales y/o de naturaleza penal. El impacto será menor cuando sólo se traten datos de carácter general y, dentro de éstos, los datos identificativos como el nombre y apellidos suponen un menor riesgo que los datos bancarios, por ejemplo.
- Pérdida económica derivada de sanciones y/o de pérdida de financiación para la organización.
- Perjuicio social para las personas afectadas o para determinados colectivos.
- Pérdida reputacional de la organización.
- Consecuencias que afectan al ejercicio de los derechos de las personas interesadas y/o garantizar los principios relativos a la protección de datos.

Cabe mencionar que el impacto mide las consecuencias tanto para la organización como para las personas afectadas.

Así, la descripción de cada uno de los niveles de impacto sería:

a. **No apreciable:** cuando las consecuencias son fácilmente subsanables, como puede ser una pérdida reversible muy limitada del control de algún dato personal, que afecte a personas puntuales, y sea de datos de carácter general; y/o una pérdida económica insignificante.
b. **Limitado:** cuando las consecuencias no tienen una gran repercusión, como pueden ser una pérdida irreversible muy limitada del control de algún dato personal, que afecte a personas

puntuales, y sea de datos de carácter general; y/o una pérdida financiera no significativa.

c. **Medio:** cuando las consecuencias tienen una repercusión media, como pueden ser una pérdida irreversible del control de datos personales, que afecte a un grupo de personas, y sea de datos de carácter general; y/o una pérdida económica y/o reputacional significativa.

d. **Grave:** cuando las consecuencias tienen una repercusión alta, como puede ser una pérdida reversible de control de los datos personales que se tratan, que afecte a un número de personas elevado, y sea de categorías especiales de datos o relativas a infracciones penales; y/o una pérdida económica significativa para la organización; y/o pérdidas económicas significativas y/o reputacionales; y/o supone un perjuicio social para las personas afectadas o determinados colectivos.

e. **Muy grave:** cuando las consecuencias tienen una repercusión muy alta que afecta al ejercicio de derechos fundamentales y libertades públicas de las personas afectadas; y/o las consecuencias están relacionadas con categorías especiales de datos o relativas a infracciones penales; y/o causa un daño social significativo, como la discriminación; y/o afecta a personas en situación de especial vulnerabilidad; y/o las pérdidas económicas y/o reputacionales que conllevan la paralización de la actividad de la organización o el cierre de la misma.

MEDICIÓN DEL IMPACTO INDICADORES	NO APRECIABLE	LIMITADO	MEDIO	GRAVE	MUY GRAVE
Pérdida de control de algún dato personal	Pérdida reversible muy limitada	Pérdida irreversible muy limitada	Pérdida reversible	Pérdida irreversible	Pérdida irreversible
Número de personas afectadas	Personas puntuales	Personas puntuales	Grupo de personas	Número elevado	Número elevado
Naturaleza de los datos	Datos generales	Datos generales	Datos generales	Categorías especiales, penales y generales	Categorías especiales, penales y generales
Pérdida económica	Insignificante	No significativa	Significativa	Muy significativa	Puede suponer el cierre de la organización
Perjuicio social para las personas afectadas	No	No	No	Sí	Sí
Pérdida reputacional	Insignificante	No significativa	Significativa	Muy significativa	Puede suponer el cierre de la organización
Afecta al ejercicio de derechos y principios de protección de datos	No	No	No	Si	Sí

Tabla 6 Indicadores para la medición del impacto del riesgo

Para determinar el nivel de impacto cabe hacer algunas aclaraciones:

- La naturaleza de los datos tiene prioridad ante el resto de indicadores.
- No tienen que cumplirse todos los indicadores de cada uno de los niveles.

A continuación, se muestran algunos ejemplos de la determinación del nivel de riesgo:

Ejemplo de análisis y determinación del nivel de riesgo Medio:		
Riesgo: Eliminación no voluntaria de los datos recogidos de las personas voluntarias que participan en una actividad		
Se ha materializado el riesgo previamente	Se ha producido previamente	
Medidas preventivas implantadas	Medidas de control implantadas y evaluadas	
Periodicidad del tratamiento concreto	Tratamiento frecuente	
Pérdida de control de algún dato personal	Pérdida irreversible muy limitada o reversible (se hacen copias de seguridad periódicas)	**Impacto: medio**
Número de personas afectadas	Grupo de personas	**Probabilidad: posible**
Naturaleza de los datos	Datos de carácter general (nombre y apellidos, DNI y datos de contacto)	
Pérdida económica	No	**Nivel de riesgo: Medio**
Perjuicio social para las personas afectadas	No	
Pérdida reputacional	No	
Afecta al ejercicio de derechos y principios de protección de datos	No	

Tabla 7 Ejemplo de análisis y determinación del nivel de riesgo Medio

PROBABILIDAD						
	CASI CIERTO	MEDIO	ALTO	ALTO	MUY ALTO	MUY ALTO
	PROBABLE	BAJO	MEDIO	ALTO	ALTO	MUY ALTO
	POSIBLE	BAJO	MEDIO	**MEDIO**	ALTO	ALTO
	IMPROBABLE	MUY BAJO	BAJO	MEDIO	MEDIO	ALTO
	RARO	MUY BAJO	MUY BAJO	BAJO	BAJO	MEDIO
		NO APRECIABLE	**LIMITADO**	**MEDIO**	**GRAVE**	**MUY GRAVE**
		IMPACTO				

Tabla 8 Mapa de calor del nivel de riesgo del ejemplo de análisis y determinación del nivel de riesgo Medio

Ejemplo de análisis y determinación del nivel de riesgo Alto:		
Riesgo: Acceso ilegítimo a los datos de personas usuarias que sean menores de edad		
Se ha materializado el riesgo previamente	No se ha producido previamente	**Probabilidad: posible** **Impacto: muy grave** **Nivel de riesgo: Alto**
Medidas preventivas implantadas	Medidas de control implantadas y no evaluadas	
Periodicidad del tratamiento concreto	Periodicidad anual	
Pérdida de control de algún dato personal	Pérdida irreversible (no se puede revertir el hecho de que se haya accedido a los datos)	
Número de personas afectadas	Grupo de personas	
Naturaleza de los datos	Datos generales de menores de edad	
Pérdida económica	No	
Perjuicio social para las personas afectadas	Si	
Pérdida reputacional	Significativa / Muy significativa	
Afecta al ejercicio de derechos y principios de protección de datos	Si. Al tratarse de personas vulnerables, el impacto es muy alto	

Tabla 9 Ejemplo de análisis y determinación del nivel de riesgo Alto

PROBABILIDAD						
	CASI CIERTO	MEDIO	ALTO	ALTO	MUY ALTO	MUY ALTO
	PROBABLE	BAJO	MEDIO	ALTO	ALTO	MUY ALTO
	POSIBLE	BAJO	MEDIO	MEDIO	ALTO	ALTO
	IMPROBABLE	MUY BAJO	BAJO	MEDIO	MEDIO	ALTO
	RARO	MUY BAJO	MUY BAJO	BAJO	BAJO	MEDIO
		NO APRECIABLE	**LIMITADO**	**MEDIO**	**GRAVE**	**MUY GRAVE**
		IMPACTO				

Tabla 10 Mapa de calor del nivel de riesgo

IV. GESTIÓN DE LAS MEDIDAS MITIGADORAS:

El artículo 24.1 del RGPD establece que: "Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario".

Estas medidas técnicas y organizativas son políticas, procedimientos, controles, medidas y evaluaciones de protección de datos a implantar serán las que mitiguen los riesgos detectados y analizados.

Las medidas mitigadoras no serán aplicables por igual, si no que se adoptarán en función de los resultados del análisis del riesgo en el tratamiento de datos para los derechos y libertades de las personas afectadas. Así, el enfoque basado en el riesgo influirá en la implantación de las medidas mitigadoras de dos formas:

- Se aplicarán determinadas medidas en función de si se produce un alto riesgo para los derechos y libertades de las personas interesadas.

- El propio riesgo funcionará como un factor de ponderación en la cada medida a implantar.

Cabe señalar que, aunque se apliquen medidas técnicas y organizativas para mitigar los riesgos, seguirá existiendo un riesgo residual o inherente.

Riesgo residual

Es aquel riesgo que permanece tras aplicar las medidas mitigadoras.

Una vez que se apliquen las medidas de control puede que el nivel riesgo se reduzca pasando, por ejemplo, de un nivel alto a un nivel medio o bajo.

Para determinar el nivel de riesgo residual habrá que volver a calcular el nivel de riesgo según su impacto y probabilidad.

En el siguiente apartado, cuando se traten las medidas de seguridad, se analizarán las medidas mitigadoras en mayor profundidad.

EVALUACIÓN DE RIESGOS
- Proceso que debe quedar documentado
- Enfoque basado en el riesgo
- Gestión del riesgo para los derechos y libertades vs gestión del riesgo de cumplimiento normativo
- Etapas del proceso: descripción de los tratamientos, identificación de riesgos, análisis de riesgos y gestión de medidas
- Descripción de los tratamientos: determinar la naturaleza, el contexto, el alcance y los fines de cada tratamiento
- Identificación de los riesgos y su origen: factores de riesgo y riesgos genéricos
- Análisis del riesgo: probabilidad e impacto
- Riesgo residual
- Gestión de medidas mitigadoras: gestión de políticas, procedimientos, controles, medidas y evaluaciones de protección de datos a implantar en base al análisis del riesgo

Tabla 11 Evaluación de riesgos

4.1.3. MEDIDAS DE SEGURIDAD

Tal y como se ha mencionado en el punto anterior, las medidas de seguridad son políticas, procedimientos, controles, medidas y evaluaciones que se deben implantar en la organización para mitigar los riesgos identificados y analizados.

Las medidas de seguridad se deberán implantar en función del nivel de riesgo que se haya establecido, pero, además, de acuerdo al RGPD, se deberá tener en cuenta[52]:

- El estado de la técnica.
- El coste de aplicación.
- La naturaleza del tratamiento.
- El ámbito de aplicación o alcance.
- El contexto.
- Las finalidades del tratamiento.
- Los riesgos de diversa probabilidad y gravedad (no sólo riesgo alto) que entrañe para los derechos y libertades de los interesados.

El RGPD no establece un listado de medidas de seguridad que deben de ser aplicables a los tratamientos de datos, pero sí que se establece como ejemplos de medidas a implementar[53]:

- La seudonimización y el cifrado de datos personales;

- La capacidad permanente de garantizar la confidencialidad, integridad, disponibilidad y resiliencia o adaptación al cambio de los sistemas de información y servicios de tratamiento;

- La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

- La verificación, evaluación y valoración regular de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Las medidas a implementar se pueden clasificar en:

- Dependiendo de cuándo se implantan, si antes de que se materialice o después:

  - Medidas correctivas: son las que implanta la organización una vez se ha detectado algún incidente de seguridad o dificultad y/o impedimento para que las personas interesadas ejerzan sus derechos y libertades, con la finalidad de evitar o, al menos, reducir la probabilidad de que vuelva a suceder.
  - Medidas preventivas: son las que implanta la organización para garantizar que, con anterioridad a que se produzca algún incidente, la probabilidad de que ocurra sea la menor posible.

- Dependiendo de la naturaleza de las medidas:

  - Organizativas: son las políticas y procedimientos aprobados que están relacionados con la protección de los datos que se tratan en la entidad.

Ejemplos: *política de protección de datos, procedimiento de gestión de brechas de seguridad, política de teletrabajo, procedimiento de borrado y destrucción de documentación, registro de actividades de tratamiento, designación de una persona Delegada de protección de datos, etc.*

52. *Ver artículo 32 del RGPD.*

53. *Ver artículo 32 del RGPD.*

- Técnicas: son las que se aplican directamente en las actividades de tratamiento de los datos personales.

> ***Ejemplos:*** *realizar copias de seguridad, tener controles de acceso y contraseñas, llevar a cabo seudonimización, realizar cifrado de datos, instalar antivirus, proteger el correo electrónico, tener cerrados con llave los armarios y archivos que contengan documentación con datos personales en papel, etc.*

Cada organización deberá realizar su propio análisis de riesgos y evaluar qué medidas de seguridad considera que se deben aplicar para garantizar los derechos y libertades de las personas interesadas en cuanto al tratamiento de sus datos personales. Las medidas a implantar no figuran en un listado preestablecido, sino que pueden ser muy diversas, por lo que su supervisión, verificación, evaluación y valoración de su eficacia consistirá en la revisión del análisis de riesgos llevado a cabo.

Partiendo del análisis para determinar el nivel de riesgo de los factores de riesgos identificados, se ha confeccionado una lista de ejemplos de medidas mitigadoras del riesgo:

Ver tabla en la página siguiente

DESCRIPCIÓN DEL TRATAMIENTO	CATEGORÍAS DE FACTORES DE RIESGO	FACTORES DE RIESGO	EJEMPLOS DE RIESGOS GENÉRICOS	EJEMPLOS DE MEDIDAS MITIGADORAS
NATURALEZA		Factores de riesgo derivados de recogida o generación de datos de forma específica	Riesgos asociados a la protección de los datos: - Que la confidencialidad de los datos esté comprometida - Que los datos recogidos no sean precisos, completos, consistentes y confiables Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando se recojan los datos mediante: - Acceso a base de datos sobre blanqueo de capitales o financiación del terrorismo - Obtenidos en zonas de acceso público - Aplicaciones - Procedentes de dos o más tratamientos con finalidades diferentes - Falta de transparencia del momento preciso de la recogida de datos	- Política de protección de datos o política de privacidad - Política de cookies y aviso de cookies en la página web - Informar a las personas interesadas sobre Responsable tratamiento, finalidad de tratamiento, licitud y/o interés legítimo, plazo de conservación, terceras personas destinatarias, etc. - Informar a las personas interesadas acerca de sus derechos y cómo pueden ejercerlos - Política de uso de dispositivos corporativos - Política de uso de dispositivos externos (o personales)
	Factores técnicos del tratamiento	Factores de riesgo derivados de implementarse con determinadas características técnicas o tecnologías	Riesgos asociados a la protección de los datos: - Que la confidencialidad de los datos esté comprometida - Que los datos no estén disponibles - Que se pierda la integridad de los datos Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando se traten datos usando: - Aplicaciones móviles - Internet de las cosas (IoT) - Inteligencia Artificial - Uso innovador o nuevas soluciones organizativas - Uso innovador de tecnologías consolidadas - Tratamientos automatizados - Videovigilancia	- Política de protección de datos o política de privacidad - Política de cookies y aviso de cookies en la página web - Política de personal (derecho a desconexión) - Política de uso de dispositivos corporativos - Política de uso de dispositivos externos (o personales) - Política de ciberseguridad - Política de uso de nuevas tecnologías - Instalar carteles informando de la existencia de cámaras
	Brechas de seguridad	Factores de riesgo que se derivan de la posible materialización de brechas de seguridad sobre los datos personales	Riesgos asociados a la protección de los datos: - Un incidente de seguridad puede afectar a la confidencialidad, integridad y disponibilidad de los datos personales Incidentes de seguridad que supongan una brecha de seguridad	- Procedimiento de gestión de brechas de seguridad - Política de ciberseguridad - Formar al personal para que haga un uso apropiado de la información y de los medios - Anonimizar o seudonimizar los datos - Bloqueo de los datos - Instalar medidas de seguridad en el servidor, equipos informáticos y correo electrónico - Aplicar contraseñas, accesos restringidos y usuarios - Procedimiento de copias de seguridad - Protocolo de archivo de documentación física que contenga datos personales - Protocolo de destrucción de documentación física y de eliminación de documentos digitales que contengan datos personales

ÁMBITO / ALCANCE	Tipos de datos utilizados	Factores de riesgo derivados de los datos recogidos, procesados o inferidos en el tratamiento	- Riesgos asociados a la protección de los datos: - Los riesgos que afecten a la confidencialidad, disponibilidad e integridad de los datos serán más o menos elevados en función del tipo de datos tratados - Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando los datos tratados sean: • Documentación personal: correspondencia por correo electrónico, documentos privados, etc. • Información de aplicaciones de registro de actividades vitales • Preferencias de consumo, hábitos, gustos, necesidades, etc. que no permitan inferir informaciones relacionadas con categorías especiales de datos • Rendimiento laboral: Control de acceso al lugar de trabajo, grabación de imágenes del puesto de trabajo, monitorización de los equipos de las personas empleadas, Inferencia del rendimiento a través de indicadores (productividad y calidad del trabajo, eficiencia, formación adquirida, objetivos conseguidos), etc. • Situación económica: renta, ingresos mensuales, situación laboral, etc. • Datos de medios de pago: números de tarjeta, números de cuenta bancaria • Datos sanitarios • Datos biométricos • Categorías especiales de datos o que permitan inferirlos: origen étnico, origen racial, opiniones políticas, afiliación sindical, datos relativos a la orientación sexual, etc. • Categorías especiales de datos seudonimizados • Datos personales relativos a condenas e infracciones penales • Datos de navegación web: registro de páginas visitadas (historial de navegación, logs de servidores web, etc.), registro del tiempo que se está en cada página, registro del momento de la visita a la página, registro del número de conexiones, etc...	- Política de protección de datos o política de privacidad - Política de cookies y aviso de cookies en la página web - Evitar la recogida de ciertos tipos de datos - Formar al personal para que haga un uso apropiado de la información - Política de uso de dispositivos externos (o personales) - Contrato o acuerdo con cada persona trabajadora de confidencialidad, cesión de datos y obligaciones. Puede incluir información acerca de videovigilancia y otras cuestiones - Registro de actividades de tratamiento - Realizar un análisis de riesgos - Realizar Evaluación de Impacto de Protección de Datos

Continua en la página siguiente

ÁMBITO / ALCANCE	Categorías de personas interesadas	Factores de riesgo relativos a la categoría de personas interesadas como menores de 14 años, víctimas de violencia de género, personas con discapacidad, personas mayores, personas que acceden a servicios sociales, personas en riesgo de exclusión social, personas vulnerables, personas contratadas por la organización, etc.	Riesgos asociados a la protección de los datos: Los riesgos que afecten a la confidencialidad, disponibilidad e integridad de los datos serán más o menos elevados en función de las categorías de las personas interesadas Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando las personas afectadas cuyos datos se vayan a tratar o se traten sean de: - Menores de 14 años - Víctimas de violencia de género - Personas con discapacidad - Personas mayores - Personas que acceden a servicios sociales - Personas en riesgo de exclusión social - Personas vulnerables - Personas contratadas por la organización	- Política de protección de datos o de privacidad - Evitar la recogida de ciertos tipos de datos - Aislar y segregar fases del tratamiento entre sí para que traten datos de una forma más limitada (anonimizando los datos o seudonimizando, por ejemplo) - Formar al personal para que haga un uso apropiado de la información y de los medios - Contrato o acuerdo con cada persona trabajadora de confidencialidad, cesión de datos y obligaciones. Puede incluir información acerca de videovigilancia y otras cuestiones - Acuerdo de trabajo a distancia - Protocolo de desconexión digital
	Extensión y alcance del tratamiento	Factores de riesgo relativos al número de personas afectadas, a la diversidad de los datos tratados, a la duración en el tiempo del tratamiento y de la conservación de los datos, el volumen de los datos, la extensión geográfica de los datos, la frecuencia de la recogida de los datos, etc.	Riesgos asociados a la protección de los datos: - La confidencialidad de los datos puede comprometerse - La disponibilidad de los datos puede disminuir - La integridad puede verse afectada Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando el tratamiento: - Involucra a gran número de sujetos - La duración sea elevada - Tenga un gran alcance geográfico - Se recopilen excesivos datos con relación al fin del tratamiento	- Reducir el alcance del tratamiento - No solicitar datos que no sean estrictamente necesarios para el tratamiento

DESCRIPCIÓN DEL TRATAMIENTO	CATEGORÍAS DE FACTORES DE RIESGO	FACTORES DE RIESGO	EJEMPLOS DE RIESGOS GENÉRICOS	EJEMPLOS DE MEDIDAS MITIGADORAS
CONTEXTO	Categoría de las personas Responsable / Encargada del tratamiento	Factores de riesgo derivados del sector de la entidad y el colectivo al que se dirigen sus actuaciones	Riesgos asociados a la protección de los datos: Los riesgos que afecten a la confidencialidad, disponibilidad e integridad de los datos serán más o menos elevados en función del colectivo Riesgo cuando la organización sea: - Organización con personas usuarias de colectivos vulnerables - Organización con personal contratado - Organización con personal voluntario	- Política de protección de datos o de privacidad - Evitar la recogida de ciertos tipos de datos
	Comunicaciones de datos	Factores de riesgo derivadas de las comunicaciones de datos a terceros en el marco del tratamiento	Riesgos asociados a la protección de los datos: - La confidencialidad de los datos puede comprometerse - Que los datos no estén disponibles o la disponibilidad sea menor - Que la integridad esté afectada Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando: - Falta de trasparencia de medios usados en el tratamiento: redes sociales, Inteligencia Artificial - Transferencias internacionales	- Política de protección de datos o de privacidad - Política de comunicaciones de datos a terceros - Contrato con cada Encargado de tratamiento - Procedimiento de comunicación de datos - Procedimiento de transferencias internacionales
	Efectos colaterales del tratamiento	Factores de riesgo que se derivan de consecuencias no contempladas en los propósitos originales previstos del tratamiento	- Excede las expectativas de las personas interesadas - Posible reversión no autorizada de la seudonimización - Posible pérdida de control de los datos tratados por la persona Encargada del tratamiento - Puede provocar exclusión - Puede provocar discriminación - Posible usurpación de identidad - Posible daño reputacional - Posible perjuicio económico significativo - Posible perjuicio moral significativo - Posible pérdida de confidencialidad de datos - Podría impedir el ejercicio de un derecho	- Política de protección de datos o de privacidad - Contrato con cada Encargado del tratamiento - Análisis periódico de la necesidad y proporcionalidad del tratamiento - Registro de actividades de tratamiento - Realizar un análisis de riesgos - Realizar Evaluación de Impacto de Protección de Datos

FINALIDAD	Operaciones relacionadas con los fines del tratamiento	Factores de riesgo que se derivan del fin declarado del tratamiento y otros fines vinculados al propósito principal	Riesgos asociados a la protección de los datos: - La confidencialidad de los datos puede comprometerse cuando los datos son usados para otros fines vinculados - Que los datos no estén disponibles o parte de ellos para los otros fines - Que se pierda la integridad de los datos Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando los fines del tratamiento sean: - Creación, uso y otros tratamientos con perfiles - Control de las personas contratadas: evaluación, grabación de audios y/o imágenes, control del tiempo invertido en realizar tareas, control del uso de internet y del teléfono, geolocalización, monitorización y control del correo electrónico, etc. - Control de acceso a internet - Videovigilancia - Decisiones automatizadas sin intervención humana - Tratamiento automatizado para soporte a la toma de decisiones - Decidir sobre o impedir el ejercicio de derechos fundamentales: derechos de igualdad, no discriminación, intimidad personal y familiar, a la libertad sindical, etc. - Decidir sobre el control del interesado de sus datos personales: derecho de acceso, rectificación, oposición, supresión, limitación del tratamiento, etc. - Decidir sobre el acceso a un servicio - Conservación de los datos	- Política de protección de datos o de privacidad - Registro de Actividades de Tratamiento - Análisis periódico de las necesidades y proporcionalidades de los tratamientos - Contrato o acuerdo con cada persona trabajadora de confidencialidad, cesión de datos y obligaciones. Puede incluir información acerca de videovigilancia y otras cuestiones - Bloqueo de los datos - Formar e informar al personal sobre protección de datos - Procedimiento de copias de seguridad - Protocolo de archivo de documentación física que contenga datos personales - Protocolo de destrucción de documentación física y de eliminación de documentos digitales que contengan datos personales

Tabla 12 Ejemplos de medidas mitigadoras

4.1.4. DESDE EL DISEÑO Y POR DEFECTO

La protección de datos desde el diseño implica que se aplicarán medidas técnicas y organizativas adecuadas para aplicar los principios de protección de datos en todos los tratamientos desde que se diseñan, se ponen en práctica y hasta que finalizan o se suprimen. Las medidas a aplicar, en función del riesgo y del nivel de riesgo son las que se han desarrollado en el apartado anterior 4.1.3. Medidas de seguridad.

La protección de datos por defecto determina que deben de aplicarse medidas técnicas y organizativas apropiadas para que solamente se realicen los tratamientos de datos necesarios para los fines del tratamiento. Es decir, que sólo se recogerán los datos necesarios, que no tendrán

acceso a los datos más personas que las estrictamente necesarias, que el plazo de conservación no se extenderá innecesariamente, etc.

4.1.5. NOTIFICACIÓN DE BRECHAS DE SEGURIDAD DE LOS DATOS

El RGPD define las violaciones o brechas de seguridad de los datos personales como "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"[54].

> ***Ejemplos:*** *el acceso no autorizado a las bases de datos de una organización, el borrado accidental o no de registros de la entidad o la pérdida de un ordenador portátil o de un teléfono móvil con acceso a datos personales de la organización.*

Una de las obligaciones que tienen las organizaciones como sujetos obligados por la normativa de protección de datos es la **notificación de las brechas de seguridad** que se produzcan en la organización cuando tenga consecuencias sobre los derechos y libertades de las personas afectadas, tanto a la autoridad de control como a las personas y a las entidades afectadas.

En caso de que se produjese una brecha de seguridad de los datos personales, las consecuencias para la organización podrían ser materiales e inmateriales, como la usurpación de identidad, la exposición pública de datos confidenciales, pérdidas económicas, etc.

¿Cómo puede la organización gestionar los incidentes de seguridad?

La organización debe estar preparada por si se produjera un incidente de seguridad, y tal y como se ha mencionado 4.1.3. Medidas de seguridad, tiene que haber implantado medidas para prevenir que sucedan y medidas correctivas para que, en caso de que se produjera, tener establecido quién y qué acciones se llevaran a cabo. Además, es más que recomendable el disponer de mecanismos que permitan detectar las brechas de seguridad en cuanto se produzcan.

Es recomendable que la organización disponga de un procedimiento para la gestión de incidencias. Como sugerencia, a continuación, se muestra un ejemplo de cómo podría ser un procedimiento de gestión de incidencias:

Ver gráfico en la página siguiente

54. *Artículo 4 del RGPD.*

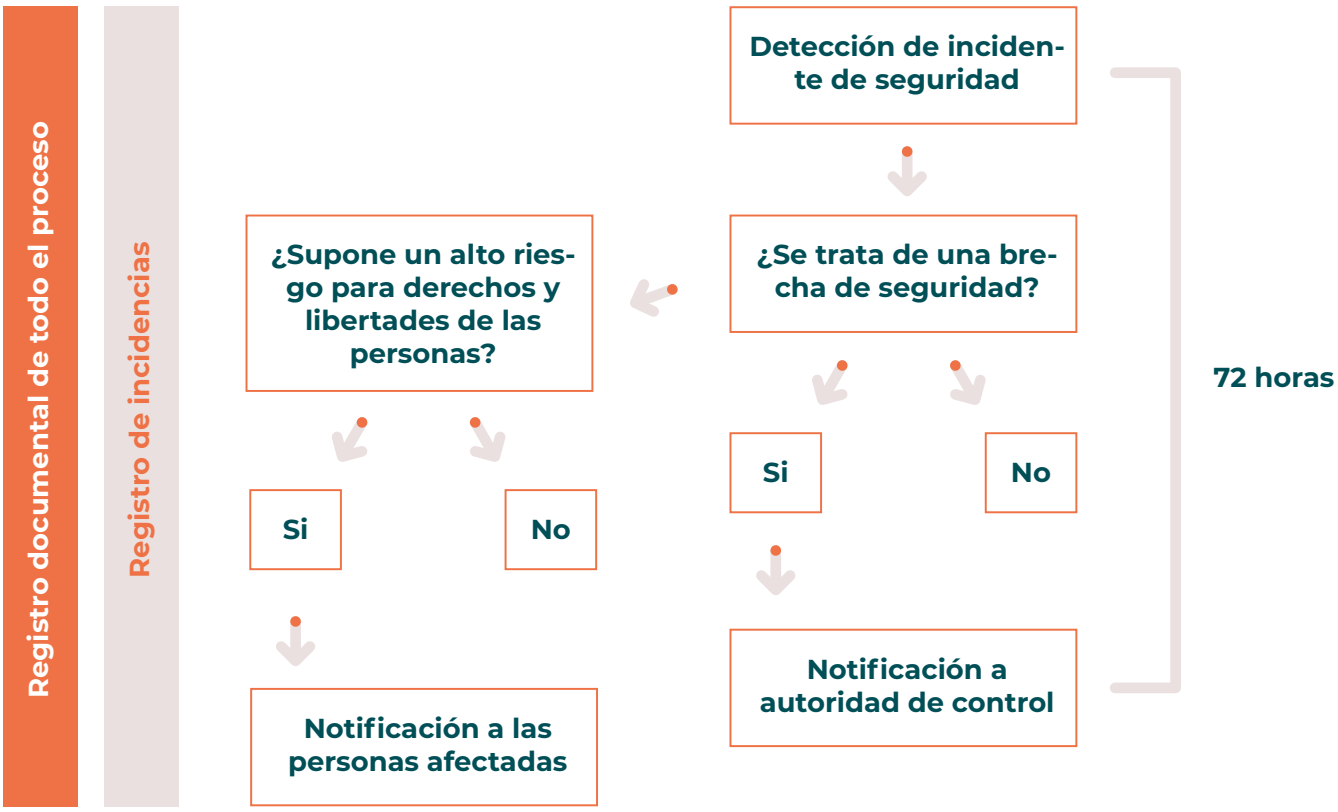


Ilustración 8 Modelo de procedimiento de gestión de incidencias

Si se produce un incidente de seguridad en la organización en primer lugar, se debe investigar y obtener información para decidir si se trata de una brecha de seguridad de los datos personales y qué medidas adoptar:

- Hecho que ha generado el incidente, por ejemplo, se han publicado datos personales por error o se han enviado a un destinatario equivocado, se ha perdido un portátil o un pendrive con datos personales, se ha producido una intrusión no autorizada en la red de la organización, etc.
- Si el origen del incidente ha sido interno o externo.
- Si se ha debido a un hecho intencionado o no.
- Qué datos personales se han visto afectados: si son datos generales, datos correspondientes a categorías especiales o penales.
- Cuál es el volumen de los datos afectados.
- Qué tipo de personas son las afectados, si se trata de personas vulnerables.
- Cuando se produjo el incidente, cuándo se ha detectado y cuándo se prevé se solucionará.

Tras el conocimiento de esta información ya se puede saber si se trata de una brecha de seguridad, su origen y alcance y estimar qué consecuencias podría tener sobre las personas afectadas.

Será una brecha de seguridad cuando el incidente afecte a datos personales que esté tratando la organización, o lo que es lo mismo, cuando pueda producir consecuencias sobre los derechos y libertades de las personas afectadas.

Ejemplos de incidentes que no constituyen brechas de seguridad: la recepción de correos

electrónicos sospechosos de malware sin que se ejecute o recibir un intento de ciberataque sin que se llegue a producir.

No obstante, aunque no se tratase de una brecha de seguridad, la organización deberá gestionar el incidente con la finalidad de determinar si es necesario la implantación de medidas eficaces que mitiguen el riesgo de que vuelva a suceder. Asimismo, el incidente deberá incluirse en el Registro de incidentes de seguridad.

Cuando se trate de una brecha de seguridad de los datos personales, la organización tiene que:

a. **Notificarlo a la autoridad de control en un plazo de 72 horas desde que se tenga constancia de ella[55].** Si la notificación a la autoridad de control no tiene lugar en ese plazo, se deberán explicar los motivos de la tardanza. En caso de que sea necesario, se admite que se proporcione la información de manera gradual. La organización debe definir, como mínimo:

   - Cuál es la autoridad de control a la que se debe notificar.
   - Qué persona debe realizar la notificación.
   - Qué medios técnicos o de cualquier índole son necesarios para notificar.

La Agencia Española de Protección de Datos dispone de un formulario para la notificación de brechas de seguridad. **https://www.aepd.es/documento/formulario-brechas.pdf** En el caso de que la notificación hubiera que realizarla a otra autoridad de control, habrá que consultar si disponen de formularios modelo.

Se considera que se tiene constancia de una brecha de seguridad cuando se sabe que se ha producido y se tiene un conocimiento suficiente de su origen, a qué datos ha afectado y sus posibles consecuencias.

Ejemplos:

» *Una persona de otra entidad informa a la organización de que ha recibido accidentalmente los datos personales de las personas asistentes a una jornada y proporciona pruebas de la comunicación no autorizada. Dado que se han presentado pruebas claras de la existencia de una brecha de seguridad que afecta a la confidencialidad, no cabe duda de que se tiene constancia de ella.*

» *En caso de pérdida de un pendrive que contenía datos personales no cifrados, no es posible determinar si personas no autorizadas han tenido acceso a dichos datos. No obstante, aunque no se pueda determinar si se ha producido una brecha de seguridad, se debe notificar, ya que, aunque no se sabe si ha afectado a la confidencialidad, sí que lo ha hecho a la disponibilidad. El momento en el que se considera que se tiene constancia de la brecha es cuando se conoce que el pendrive se ha perdido.*

» *La organización detecta que ha habido una posible intrusión en su red. Se comprueban los sistemas para determinar si los datos personales que están siendo tratados se han visto comprometidos y, aunque no se tiene certeza, la probabilidad es elevada. En este caso*

55. *Ver artículo 33 del RGPD.*

se recomienda notificarlo a la autoridad de control.

» *Una persona contratada de la organización informa de que ha recibido un mensaje de correo electrónico de alguien que se hace pasar por la dirección de la organización y que contiene datos personales relativos a su uso del servicio, lo cual indica que la seguridad de la organización se ha visto comprometida. Tras llevar a cabo una breve investigación se detecta la intrusión en la red de la entidad y pruebas del acceso no autorizado a los datos personales que contiene. Al conseguir las pruebas se tiene constancia de la brecha de seguridad y se debe informar a la autoridad de control.*

b. Documentar el proceso con toda la información que se vaya recopilando para adjuntarla al registro de incidentes que debe tener la organización.

Contenido de la notificación a la autoridad de control:

La notificación deberá contener como mínimo la siguiente información:

- Descripción de la brecha de seguridad de los datos personales: explicación del hecho que la ha provocado, su origen interno o externo, si ha sido intencionada o no, la categoría y extensión de los datos personales afectados y la tipología y el número aproximado de personas afectadas.

- Descripción de las posibles consecuencias de la brecha.

- Descripción de las medidas adoptadas o propuestas por la organización para poner solventar la brecha de seguridad, así como las consecuencias del incidente.

- Nombre y los datos de contacto de quien sea Delegado de Protección de Datos, si lo hubiera, o de otra persona de contacto en la organización.

Notificación a las personas afectadas[56]

Además de la comunicación a la autoridad de control correspondiente, en caso de que la brecha de seguridad suponga un alto riesgo para los derechos y libertades de las personas físicas, la organización deberá comunicárselo a las personas interesadas. La comunicación deberá realizarse lo antes posible.

La comunicación no será necesaria si se cumple alguna de las siguientes condiciones:

- La organización tiene implantadas, con anterioridad a la brecha de seguridad, medidas técnicas y organizativas adecuadas para la protección de los datos personales que fueron afectados por la brecha. Estas medidas impedirán que terceras personas ajenas puedan usarlos.

- La organización ha implantado medidas para evitar que se vuelva a repetir el incidente de seguridad en el futuro.

- Cuando la comunicación suponga un esfuerzo desproporcionado. Si fuera el caso, se optará por una comunicación pública u otro medio para que las personas afectadas se enteren.

En el procedimiento de gestión de las brechas de seguridad se deberán incluir aspectos relativos a la comunicación a las personas afectadas como quién realizará

56. *Ver artículo 34 del RGPD.*

la comunicación, cómo se comunicará y qué canales y/o medios se emplearán.

Contenido de la notificación a las personas afectadas:

La comunicación, que debe estar redactada con un lenguaje sencillo y claro, describirá cómo se ha producido la brecha de seguridad y contendrá, como mínimo, la siguiente información:

- Nombre y los datos de contacto de quien sea Delegado de Protección de Datos, si lo hubiera, o de otra persona de contacto en la organización.
- Descripción de las posibles consecuencias de la brecha de seguridad.
- Descripción de las medidas adoptadas o propuestas por la organización para poner solventar la brecha de seguridad, así como las consecuencias del incidente.

Registro de incidentes de seguridad

El registro de incidentes de seguridad es un documento que tienen que tener todas las organizaciones y debe usarse para dejar constancia y documentar el análisis realizado desde que se ha detectado el incidente de seguridad hasta que se haya resuelto.

Debería contener:

- Los incidentes de seguridad que se produzcan especificando:
  - Breve descripción del incidente.
  - Origen, indicando si es externo o interno.
  - Si ha sido intencionado o no.
  - Categoría y extensión de los datos personales afectados.
  - Tipología y número aproximado de personas afectadas.
  - Indicar si se trata de una brecha de seguridad.
  - Las notificaciones realizadas a la autoridad competente de dichas brechas.
  - La información relativa a las respuestas, requerimientos y resto de comunicaciones a y desde la autoridad competente.
  - La comunicación a las personas afectadas, si fuera necesario hacerlo, incluida una copia de la comunicación efectuada.

4.1.6. EVALUACIÓN DEL IMPACTO SOBRE LA PROTECCIÓN DE DATOS

Una Evaluación de Impacto sobre la Protección de Datos (en adelante, EIPD) es, de acuerdo al WP 248[57] *"un proceso concebido para describir el tratamiento, evaluar su necesidad y proporcionalidad y ayudar a gestionar los riesgos para los derechos y libertades de las personas físicas derivados del tratamiento de datos personales evaluándolos y determinando las medidas para abordarlos"*. Es decir, es un proceso que se ayuda a las organizaciones a cumplir con la legislación en materia de protección de datos y a demostrar que se han tomado las medidas adecuadas para garantizar su cumplimiento.

La EIPD deberá realizarse cuando sea probable que las operaciones de tratamiento entrañen un alto riesgo para los derechos y libertades de las personas físicas y evaluará el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo. Se deberá llevar a cabo siempre con anterioridad a llevar a cabo el tratamiento.

a. ¿Cuándo es obligatorio realizar una Evaluación de Impacto?

57. *WP 248. 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. Grupo "Protección de Datos" del artículo 29.*

La EIPD deberá realizarse cuando sea probable que un tipo de tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas[58].

De acuerdo al RGPD la Evaluación de Impacto deberá realizarse al menos en tres supuestos:

- En la evaluación sistemática y exhaustiva de aspectos personales de una persona, incluida la elaboración de perfiles.
- En el tratamiento a gran escala de datos sensibles.
- En la observación sistemática a gran escala de una zona pública.

La Agencia Española de Protección de Datos (AEPD) dispone de dos documentos denominados **Listas de tipos de tratamientos de datos que requieren Evaluación de Impacto relativa a Protección de Datos** https://www.aepd.es/documento/listas-dpia-es-35-4.pdf y Lista orientativa de tipos de tratamientos que no requieren una Evaluación de Impacto relativa a la Protección de Datos según el artículo 35.5 RGPD **https://www.aepd.es/documento/listasdpia-35.5l.pdf,** donde se puede verificar si la organización está realizando tratamientos que requieran de una EIPD.

Ejemplo de tratamientos que requieren de una EIPD: *entidad que observa sistemáticamente las actividades de las personas empleadas, incluida la observación de los puestos de trabajo o la actividad en internet (cámaras de vigilancia dentro de las oficinas y/o monitorización de los ordenadores).*

Ejemplo de tratamientos que no requieren de una EIPD: *envío del boletín mensual de la organización usando la base de datos las personas que dieron su consentimiento.*

b. ¿En qué consiste una Evaluación de Impacto de Protección de Datos?

Una EIPD analiza cuáles son los potenciales riesgos a los que están expuestos los datos personales en función de las actividades de tratamiento que se llevan a cabo con los mismos. Concretamente, evalúa el origen, la naturaleza, la particularidad y la gravedad de dichos riesgos.

Para realizar una EIPD se requiere de una metodología, así como de un procedimiento. La metodología debe incluir, como mínimo:

- Una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento.
- Cuando proceda, revisión del interés legítimo del tratamiento.
- Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad.
- Una evaluación de los riesgos para los derechos y libertades de las personas interesadas.
- Las medidas previstas por la organización para mitigar los riesgos.
- En caso de que la organización disponga de Delegado de protección de datos, debe asesorar en todo el proceso.
- En algunos casos también se debe consultar a las personas interesadas.

58. *Ver artículo 35 del RGPD.*

59. *Ver artículo 35.7 del RGPD.*

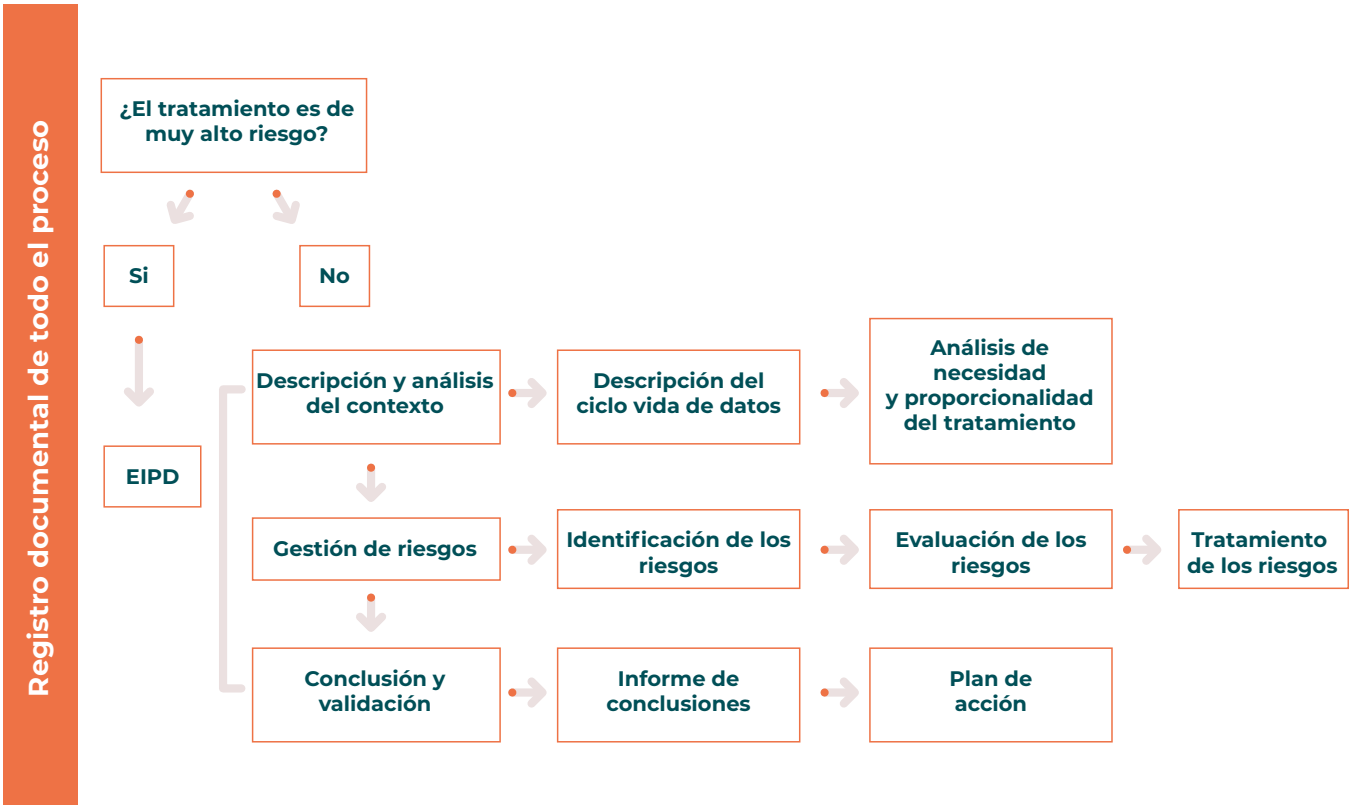


Ilustración 9 Procedimiento de una Evaluación de Impacto de Protección de Datos

El procedimiento para llevar a cabo una EIPD sería:

1. Descripción y análisis del contexto:

1.1. Describir el ciclo de vida de los datos: Consiste en la descripción detallada del ciclo de vida y del flujo de datos en el tratamiento, que también conlleva la identificación de los datos tratados, personas que intervienen, terceras personas que participan, los sistemas implicados y cualquier elemento relevante que participe en la actividad de tratamiento.

Es fundamental determinar la naturaleza, el contexto y el alcance y la finalidad de cada tratamiento de datos identificado que pueden influir en todas las etapas del ciclo de vida de los datos

1.2. Analizar la necesidad y proporcionalidad del tratamiento: Supone el análisis de la base de legitimación y la necesidad y proporcionalidad del tratamiento que se pretenden llevar a cabo en relación con su finalidad.

2. Realizar una gestión de riesgos:

2.1. Identificar los riesgos: Se trata de identificar los riesgos potenciales a los que están expuestos las actividades de tratamiento, tal y como se ha explicado en el apartado 4.1.2. Evaluación de riesgos.

2.2. Evaluar los riesgos: Consiste en determinar el nivel del riesgo que, tal y como se ha analizado anteriormente, es la combinación de la probabilidad y del impacto de que se materialicen los riesgos a los que está expuesta tanto la organización como los derechos y libertades de las personas interesadas.

2.3. Tratar los riesgos: Es la respuesta ante los riesgos identificados para minimizar la probabilidad y el impacto de que estos se materialicen.

3. Conclusión y validación:

Consiste en la elaboración del informe de conclusiones y del plan de acción:

- El informe de conclusiones de la EIPD es el documento donde figure el resultado obtenido del proceso de EIPD.
- El plan de acción es el documento donde figuran las medidas mitigadoras a implantar.

Se recomienda que se supervise y revise la implantación o puesta en marcha del nuevo tratamiento con el objetivo de garantizar la eficacia de las medidas mitigadoras que figuran en el Plan de acción.

La EIPD debe revisarse siempre que se modifiquen o actualicen las actividades de tratamiento, a no ser que los cambios sobre el tratamiento no sean significativos, y no generen por tanto nuevas amenazas y riesgos sobre los derechos y libertades de las personas interesadas. En cualquier caso, se deben valorar los cambios habidos y documentar las decisiones tomadas. Si las modificaciones o actualizaciones afectan a la descripción del tratamiento o se tenga constancia de nuevos riesgos, se deberá realizar una nueva EIPD llevando a cabo todo el procedimiento asociado.

Si al llevar a cabo una EIPD el resultado muestra que las operaciones de tratamiento suponen un nivel de riesgo muy alto que no puede ser mitigado con las medidas implantadas o a implantar, antes de realizar el tratamiento se debe consultar a la autoridad de control correspondiente.

4.2. ROLES EN UNA ENTIDAD

En una organización del TSAS en relación con la protección de datos personales son tres las figuras que hay que tener en cuenta: Responsable del tratamiento, Encargado del tratamiento y Delegado de protección de datos.

En este apartado se explica qué papel juega cada uno de estas figuras en la protección de datos de las entidades, en especial en cuanto a las medidas de responsabilidad activa.

No obstante, no hay que olvidar que la normativa de protección de datos personales debe respetarse en todas las actividades de la organización en las que se traten datos personales, por lo que todo el personal de la entidad contratado y voluntario debe tener formación y estar informado al respecto.

4.2.1. RESPONSABLE DEL TRATAMIENTO

Tal y como se menciona en el punto 3.1.2., la persona **Responsable del tratamiento de datos personales es aquella persona física, jurídica o autoridad pública que decide sobre el tratamiento de datos personales de las personas interesadas, determinando tanto para qué son usados esos datos (fines) como la forma en que son usados (medios).**

Es cada organización del TSAS quien ostentaría el rol de Responsable del tratamiento de datos personales.

Funciones y obligaciones

Las funciones y obligaciones de la persona Responsable son, entre otras:

- **Garantizar el cumplimiento de los principios de protección de datos, incluido el establecimiento de la legitimidad del tratamiento y la obtención d e un consentimiento válido.**
- **Asegurar la transparencia en la recogida de los datos personales y en su tratamiento cuando los datos no hubieran sido facilitados por la persona interesada.**
- **Garantizar los derechos de las personas interesadas.**

- **Determinar las medidas técnicas y organizativas** que la organización tiene que aplicar a fin de garantizar y poder demostrar que el tratamiento cumple con la normativa de protección de datos y que se tratan los datos personales de un modo lícito y seguro.

- **Elaborar un Registro de Actividades de Tratamiento, en caso de que la organización estuviera obligada o quiera tenerlo.**

- **Aplicar las medidas desde el diseño y por defecto.**

- **Notificar las incidencias de seguridad.**

- **Realizar la evaluación de impacto relativa** a la protección de datos con anterioridad al tratamiento si éste entrañe un alto riesgo.

- Consultar a la autoridad de control con anterioridad al tratamiento cuando el resultado de una **evaluación de impacto** relativa a la protección de datos muestre que dicho tratamiento entraña un alto riesgo y no se toman medidas.

- Seleccionar y supervisar a la persona Encargada del tratamiento, si fuera el caso. La persona Responsable elegirá únicamente a la Encargada que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas.

- **Designar a la persona Delegada de protección de datos en caso de que fuera obligatorio o que se designe de forma voluntaria.**

En el siguiente cuadro se puede ver en qué apartado de esta guía se trata cada una de las funciones mencionadas de la persona Responsable del tratamiento:

Funciones Responsable	Análisis en la guía
Garantizar principios de protección de datos	Apartado 3.2.
Asegurar la transparencia	Apartado 3.3.
Garantizar los derechos de las personas interesadas	Apartado 3.4.
Determinar las medidas técnicas y organizativas a implementar	Apartado 4.1.
Elaborar un Registro de Actividades de Tratamiento	Apartado 4.1.1.
Aplicar las medidas desde el diseño y por defecto	Apartado 4.1.4.
Notificar incidencias de seguridad	Apartado 4.1.5.
Realizar la evaluación de impacto relativa a la protección de datos	Apartado 4.1.6.
Consulta previa a la autoridad de control	Apartado 4.1.6.
Seleccionar a la persona Encargada del tratamiento	Apartado 4.2.2.
Designar a la persona Delegada de protección de datos	Apartado 4.2.3.

Tabla 13 Funciones de la persona Responsable del tratamiento

4.2.2. ENCARGADO DEL TRATAMIENTO

La persona que ostenta el rol de Encargado del tratamiento de datos personales es aquella persona física o jurídica o autoridad pública que, para desarrollar su actividad o prestar sus servicios, tiene que acceder y tratar datos personales que son responsabilidad de la persona Responsable del tratamiento.

La persona Encargada del tratamiento tratará los datos personales a los que pueda tener acceso sólo por encargo de la persona Responsable del tratamiento y debe cumplir con sus instrucciones, por lo que suele ser una tercera persona externa a la organización.

Cabe destacar que la persona Responsable continúa siendo responsable del adecuado tratamiento de los datos personales y de garantizar los derechos y libertades de las personas afectadas.

> ***Ejemplo:*** *la gestoría que realiza los trámites administrativos de personal o liquida los impuestos de la organización es la Encargada del tratamiento de los datos personales necesarios para prestar sus servicios (datos necesarios para la redacción de los contratos laborales, para dar de alta en la Seguridad Social, para la gestión y pago de las nóminas, etc.)*

Funciones y obligaciones

Las funciones y obligaciones de la persona Encargada de protección de datos son, entre otras:

- **Elaborar un Registro de Actividades de Tratamiento,** en caso de que estuviera obligada o quiera tenerlo.
- **Aplicar las medidas técnicas y organizativas necesarias** para garantizar un nivel de seguridad adecuado al riesgo asociado al tratamiento[60], **con el objetivo de cumplir con la normativa de protección de datos y asegurar que se traten los datos personales de un modo lícito y seguro.** Las medidas no podrán variar las finalidades y los usos de los datos, ni éstos podrán ser usados para sus propias finalidades. Las decisiones que adopte deben respetar en todo caso las instrucciones dadas por la persona Responsable del tratamiento.
- **Designar a la persona Delegada de protección de datos en caso de que fuera obligatorio o que se designe de forma voluntaria.**
- **Garantizar el cumplimiento de los principios de protección de datos, en concreto:**
  - **Asegurar la transparencia en el tratamiento de los datos personales.**
  - Garantizar la confidencialidad de las personas interesadas. Esta obligación abarca a todas las personas autorizadas que vayan a tratar los datos personales.
- **Asistir a la persona Responsable en la atención al ejercicio de derechos de las personas interesadas, siempre que sea posible.**
- **Colaborar** con la persona Responsable en el cumplimiento de sus obligaciones, como son la seguridad del tratamiento, notificarle las brechas de seguridad en el momento de detectarlas, evaluación de impacto relativa a la protección de datos y consulta previa.
- Colaborar con la persona Responsable para demostrar el cumplimiento:

60. *De conformidad con lo establecido en el artículo 32 del RGPD.*

- Poniendo a disposición de la persona Responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones de la persona Encargada.
- Permitiendo y contribuyendo a la realización de auditorías e inspecciones.

Estas funciones sólo son de aplicación respecto al tratamiento de los datos cuya responsabilidad corresponde a la persona Responsable del tratamiento.

Contrato entre Responsable y Encargado de protección de datos

La relación entre la persona Responsable y la persona Encargada deben formalizarse en un contrato o en un acto jurídico que les vincule, que debe figurar por escrito y firmarse con anterioridad a que se inicie la relación.

El **contenido mínimo del contrato** es:

- El objeto, duración, naturaleza y finalidad del tratamiento.
- El tipo de datos personales y las categorías de las personas interesadas.
- La obligación de la persona Encargada de tratar los datos personales únicamente siguiendo instrucciones de la persona Responsable:
  - Estas instrucciones deben figurar de forma precisa.
  - Se debe especificar las comunicaciones a terceros encomendadas, incluyendo las transferencias internacionales.
- La obligación de la persona Encargada de garantizar la confidencialidad de las personas interesadas, incluyendo a todas las personas autorizadas a tratar los datos personales.
- El compromiso de la persona Encargada para aplicar todas las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo asociado al tratamiento.
- El régimen de subcontratación, que implica la autorización previa para que la persona Encargada pueda recurrir a otra persona encargada (subcontratación) para desarrollar el servicio encomendado, cuando conlleve el tratamiento de los datos personales por parte de una tercera persona[61].

Ejemplo: *la empresa que presta servicios informáticos como el almacenamiento en la nube o el hosting. Esa empresa, como Encargada del tratamiento, sólo podrá subcontratar parte de ese servicio a otro Encargado si ha recibido autorización previa de la organización (Responsable del tratamiento).*

- La asistencia a la persona Responsable en la atención al ejercicio de derechos de las personas interesadas, siempre que sea posible.
- La colaboración con la persona Responsable en el cumplimiento de sus obligaciones, como son la seguridad del tratamiento, notificación de las brechas de seguridad, evaluación de impacto relativa a la protección de datos y consulta previa.
- El destino de los datos al finalizar la presentación del servicio:
  - Indicar si cuando finalice el plazo de

61. *Apartados 2 y 4 del Artículo 28 del RGPD.*

ejecución del contrato la persona Encargada debe suprimir los datos tratados o devolverlos a la persona Responsable o a otra tercera persona designada por la Responsable.
- Establecer la forma y plazo en que debe cumplirse.

- La voluntad de colaborar con la persona Responsable para demostrar el cumplimiento poniendo a disposición de la responsable toda la información necesaria y permitiendo y contribuyendo a la realización de auditorías e inspecciones.

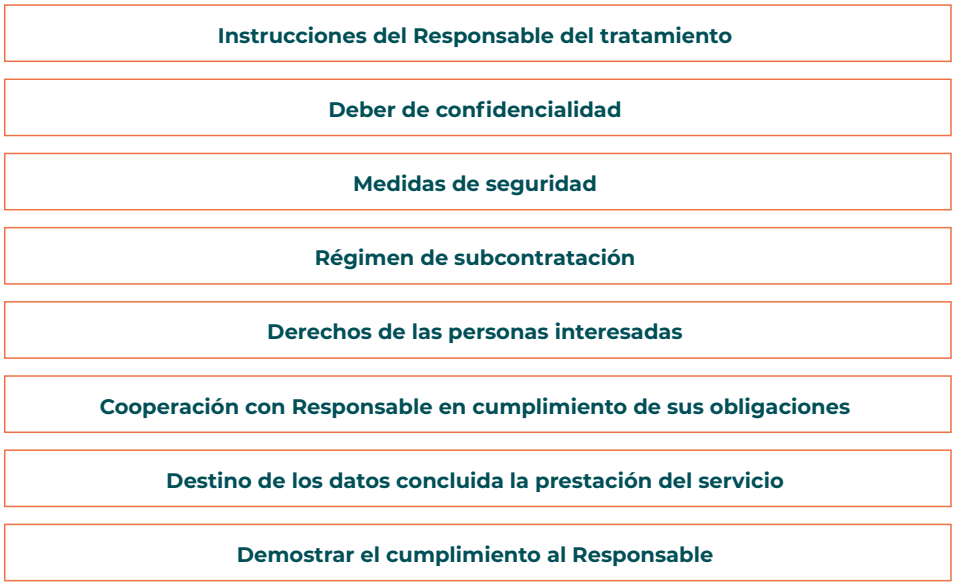


Ilustración 10 Contenido mínimo del contrato de Encargado del tratamiento

En caso de que la organización tuviera contratos antiguos firmados con personas Encargadas del tratamiento de datos, deben modificarse para que incluyan como mínimo este contenido. Se puede firmar un anexo al contrato incluyendo toda esta información.

4.2.3. DELEGADO DE PROTECCIÓN DE DATOS

La persona **Delegada de Protección de Datos (DPD) es una persona física o jurídica que será la garante del cumplimiento de la normativa de protección de datos en la organización.** Puede ser una persona contratada por la persona Responsable del tratamiento, por la persona Encargada del tratamiento o puede contratarse con un servicio externo como, por ejemplo, con una consultora especializada en protección de datos.

No todas las organizaciones tienen que contar con la figura de Delegado de Protección de Datos, la normativa indica en qué situaciones se tiene la obligación de hacerlo, aunque cualquier entidad puede hacerlo de forma voluntaria.

Quien ostente el rol de Delegado de Protección de Datos ha de ser nombrado por la persona Responsable, por la persona Encargada del tratamiento, o por ambos,

en función de quién esté obligada a su nombramiento o quiera hacerlo.

En todo caso, si se nombra a una persona Delegada de Protección de Datos de forma voluntaria, se aplicarán a su designación, su puesto y sus tareas los mismos requisitos que si el nombramiento hubiera sido obligatorio.

Se deberá comunicar en un plazo de diez días a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos, las designaciones, nombramientos y ceses del Delegado de Protección de Datos tanto cuando su designación sea obligatoria como voluntaria.

Requisitos de la persona a nombrar como Delegado de Protección de Datos

La persona que ostente el rol de Delegada de Protección de Datos debe contar con conocimientos especializados en Derecho y tener experiencia en la aplicación de la normativa de protección de datos. No es requisito que disponga de una titulación específica, pero dado que entre sus funciones se incluye el asesoramiento a la persona Responsable y/o a la Encargada en relación con la normativa de protección de datos, será necesario que disponga de conocimientos jurídicos y del uso de herramientas tecnológicas aplicadas al tratamiento de datos y que tenga un amplio conocimiento interno y externo de la organización.

Requisitos de la figura de Delegado de Protección de Datos

La figura del Delegado de Protección de Datos en la organización tiene que cumplir unos requisitos:

- Debe ser independiente, por lo que no debe recibir ninguna instrucción en el desempeño de sus funciones. En este sentido y para proteger esa autonomía, cuando se trate de una persona física con contrato laboral, no podrá ser despedida, sancionada, ni removida de su cargo por desempeñar sus funciones, salvo que incurriera en dolo o negligencia grave en su ejercicio.

- Debe tener total autonomía en el ejercicio de sus funciones.

- Debe disponer de todos los recursos necesarios para desarrollar su actividad de manera eficiente, que serán proporcionados por la persona Responsable del tratamiento y/o por la Encargada.

- Debe mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones.

- Es necesario que se relacione con la Dirección y/o con niveles superiores de toma de decisiones de la organización.

- En el ejercicio de sus funciones tendrá acceso a todos los datos personales y a los procesos de tratamiento de la organización.

- Podrá desempeñar otras funciones y actividades siempre y cuando no den lugar a un conflicto de intereses.

¿Cuándo puede ser obligatorio para una entidad de acción social disponer de una persona Delegada de Protección de Datos?

Tanto el RGPD[62] como la LOPDGDD[63] enumeran los supuestos en los que es obligatorio la designación de una persona Delegada de Protección de datos. Se va a mencionar sólo aquellos supuestos que podrían ser de aplicación a las organizaciones de acción social:

62. *Ver artículo 37 del RGPD.*

63. *Ver artículo 34 de la LOPDGDD.*

- Cuando las actividades principales consisten en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala:

  - Las actividades principales[64] son aquellas fundamentales para la organización. El tratamiento de los datos personales de las personas trabajadoras no se consideraría actividad principal sino de apoyo o auxiliar.

Ejemplo de actividad principal: *en una organización cuyas personas usuarias son personas con TEA y sus familias una de las actividades principales puede ser el apoyo psicosocial a sus personas usuarias, por lo que el tratamiento de los datos obtenidos para poder llevar a cabo ese apoyo se considera actividad principal.*

  - Con observación habitual y sistemática[65] se hace referencia a que se hace seguimiento de forma continuada, periódica o recurrente, que está sujeto a un sistema preestablecido y organizado.

Ejemplos de actividad que requiera de una observación habitual y sistémica: *actividades de mercadotécnica basadas en datos (anuncios en redes sociales dirigidos en función de ciertos datos personales); elaborar perfiles para evaluar riesgos en prevención del blanqueo de capitales; seguimiento de los datos de bienestar, estado físico y salud; sistemas de vigilancia mediante televisión de circuito cerrado; dispositivos conectados mediante domótica, etc.*

Las entidades de pequeña dimensión no suelen llevar a cabo actividades que requieran una observación habitual y sistémica directamente pero sí que pueden subcontratar dichas actividades en el marco de proyectos o programas.

- Cuando las actividades principales consisten en el tratamiento a gran escala[66] de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales.

  - Con actividad de tratamiento a gran escala se hace referencia a un tratamiento que afecta a gran cantidad de datos personales, provenientes de un elevado número de personas, que provengan de una extensa diversidad geográfica y que pueden entrañar un riesgo para las personas interesadas.

Ejemplo de actividad con tratamiento a gran escala de categorías especiales de datos personales: *recopilación y conservación de listados con datos personales de personas refugiadas o de personas pertenecientes al colectivo LGTBI+ a nivel nacional.*

64. *La Agencia Española de Protección de Datos en su página web en el apartado de "Preguntas frecuentes" da una interpretación de qué se puede considerar como actividades principales.*
65. *La Agencia Española de Protección de Datos en su página web en el apartado de "Preguntas frecuentes" da una interpretación de qué se puede considerar como observación habitual y sistemática.*
66 *La Agencia Española de Protección de Datos en su página web en el apartado de "Preguntas frecuentes" da una interpretación de qué se puede considerar como observación habitual y sistemática.*

En todo caso, se deberá designar cuando se trate de las siguientes organizaciones:

- Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.

- Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.

- Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.

- Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.

- 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.

Funciones y obligaciones

Las funciones y obligaciones de una persona Delegada de Protección de Datos son:

- Informar y asesorar de las obligaciones derivadas de la normativa aplicable en protección de datos.

- Supervisar el cumplimiento de la normativa aplicable en protección de datos tanto externa como interna de la organización, incluidas las políticas aprobadas, la asignación de responsabilidades, los planes de comunicación y formación del personal que participa en operaciones de tratamiento y las auditorías correspondientes.

- Documentar y comunicar las vulneraciones habidas en materia de protección de datos.

- Ofrecer el asesoramiento que se solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.

- Cooperar con la autoridad de control: llevar a cabo la interlocución con la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa cuando el resultado de la evaluación de impacto desprende que el riesgo del tratamiento es alto, y realizar consultas, en su caso, sobre cualquier otro asunto.

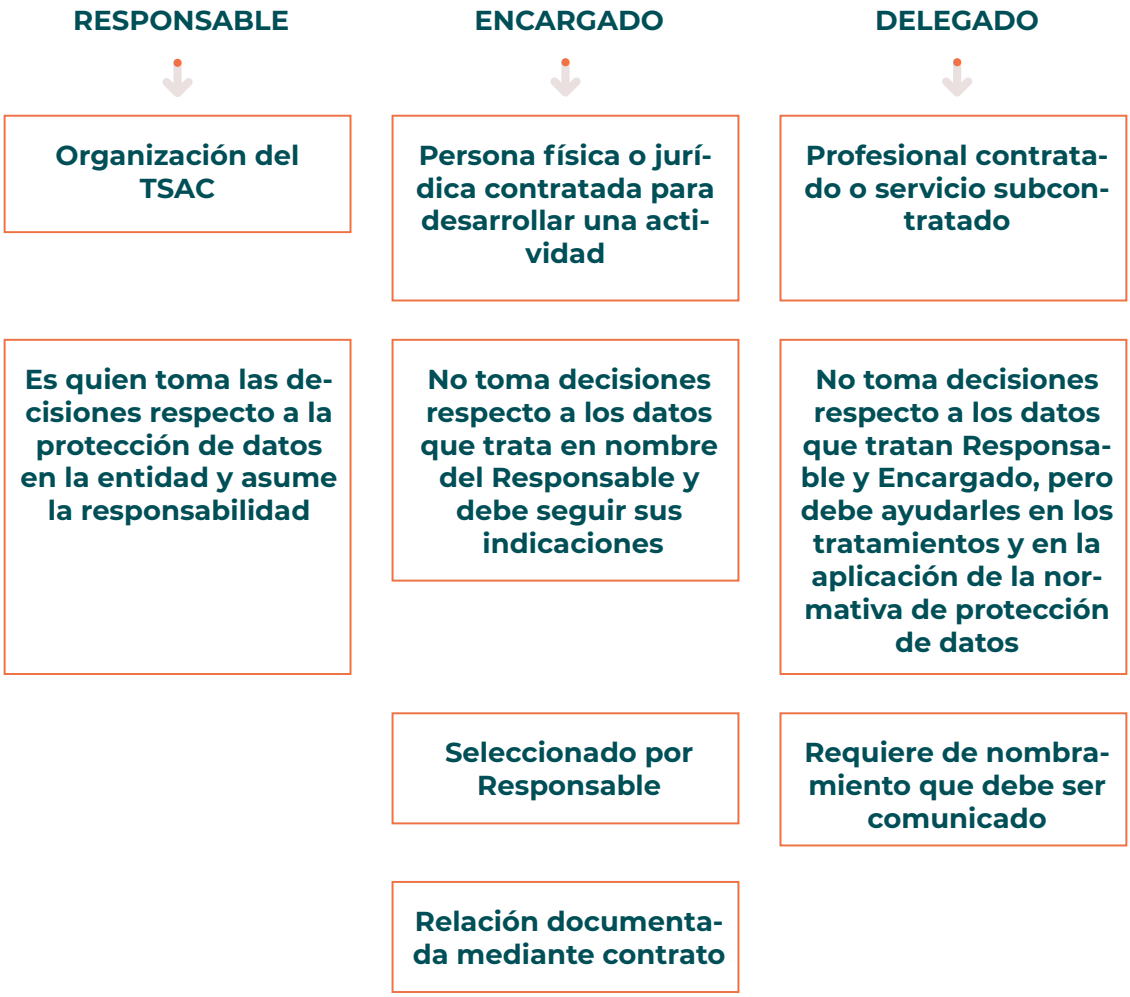


Ilustración 11 Comparativa de los roles en protección de datos personales

4.3. VULNERACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS

¿Qué es una vulneración de la normativa de protección de datos?

Una vulneración de la normativa de protección de datos puede ser, por un lado, un incidente de seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de los datos personales tratados o la comunicación o acceso no autorizado a dichos datos o, por otro lado, una acción que pueda suponer un trato o exposición ilícita de datos personales, así como cualquier transgresión de la propia normativa en cuanto a los derechos de las personas interesadas respecto a sus datos personales[67].

Hay que tener en cuenta que será una vulneración tanto si se produce de forma deliberada o por negligencia.

Ejemplos:

» *Organización que envía publicidad a personas sin haber obtenido su consentimiento.*

67. *Artículos 72, 73 y 74 de la LOPDGDD.*

» *Entidad que no informa de los derechos que pueden ejercitar las personas interesadas cuando recoge los datos a través de la inscripción en una jornada.*

» *Filtración de los datos de personas solicitantes de asilo de una organización.*

» *Una persona interesada se pone en contacto con la organización para que no le vuelvan a enviar correos con información y su solicitud no es atendida.*

» *Entidad que cede datos personales a una empresa para la prestación de un servicio sin el consentimiento ni conocimiento de las personas interesadas.*

Procedimiento de denuncia

Cuando se produce una vulneración de la normativa de protección de datos la casuística del procedimiento dependerá de la causa y de si se trata de un hecho deliberado o negligente. Aunque en la normativa se contempla la posibilidad de que la vulneración se produzca en el caso de que el tratamiento sea transfronterizo, en esta guía se va a describir sólo en caso de que sea a nivel nacional debido a que es lo más frecuente.

El procedimiento depende de si la persona afectada reclama porque la organización no ha atendido una solicitud de ejercicio de sus derechos o porque se considera que ha habido una posible infracción de la normativa de protección de datos:

A. Vulneración de los derechos de las personas afectadas por **falta de atención de una solicitud de ejercicio de los derechos[68]:**

En este caso, cuando la persona quiere ejercer sus derechos se debe poner en contacto previamente con la organización (Responsable del tratamiento) por un medio que permita acreditarlo. Si la organización no ha respondido en el plazo establecido o la persona afectada considera que la respuesta no es adecuada, podrá poner una reclamación ante la Agencia Española de Protección de Datos (AEPD).

Ejemplo: *la entidad no ha atendido una solicitud de darse de baja de recibir el boletín (derecho de supresión).*

El procedimiento que se llevará a cabo por la AEPD es el siguiente:

Ver gráfico en la página siguiente

68. *Artículos 63, 64 y 65 de la LOPDGDD.*

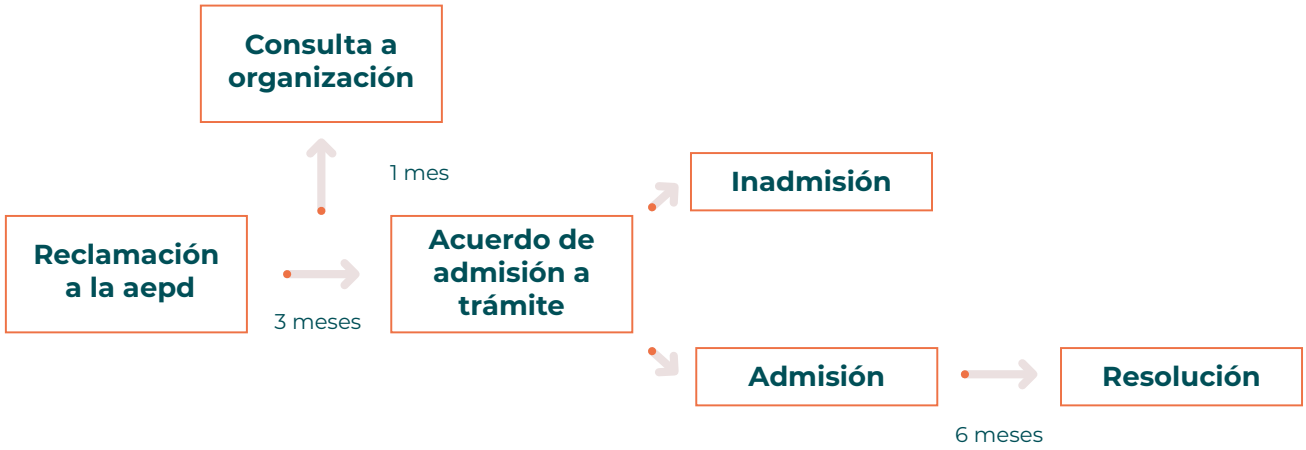


Ilustración 12 Procedimiento reclamación por falta de atención de una solicitud de ejercicio de los derechos

- Se iniciará por **acuerdo de admisión a trámite.**

- Cuando se presenta a la AEPD una reclamación, esta deberá evaluar su admisibilidad a trámite:

  - La AEPD puede remitir la reclamación a la organización, ya sea al Responsable del tratamiento o al Encargado del tratamiento, en el caso de que no hubiera Delegado de protección de datos. La organización deberá dar respuesta en el plazo de un mes.
  - **La decisión sobre la admisión o inadmisión a trámite deberá notificarse al reclamante en el plazo de tres meses** desde que se dio entrada a la reclamación. Si transcurrido este plazo no se produjera dicha notificación, se entenderá que prosigue la tramitación de la reclamación, sin perjuicio de la facultad de la AEPD de archivar posteriormente y de forma expresa la reclamación:

    - **Inadmisión:** la AEPD inadmitirá las reclamaciones cuando:

      - No traten sobre cuestiones de protección de datos personales.

      - Carezcan manifiestamente de fundamento.

      - Sean abusivas.

      - No aporten indicios racionales de la existencia de una infracción.

      - La organización ha adoptado las medidas correctivas adecuadas y concurre alguna de las siguientes circunstancias:

        a. Que no se haya causado perjuicio a la persona afectada en el caso de infracciones consideradas leves.
        b. Que el derecho de la persona afectada queda plenamente garantizado mediante la aplicación de las medidas.

    - **Admisión:** la AEPD continuará con la tramitación de la reclamación, aunque si la entidad demuestra haber adoptado las me-

didas correctivas adecuadas se podría resolver la reclamación y proceder a su archivo.

- El plazo para resolver el procedimiento es de seis meses a contar desde la fecha en que hubiera sido notificado a la persona reclamante el acuerdo de admisión a trámite. Transcurrido ese plazo, la persona interesada podrá considerar estimada su reclamación.

B. Determinación de la existencia de una posible infracción:

En este caso, ha habido un tratamiento ilícito o un incidente de seguridad en la organización, ya sea por negligencia o deberse a un hecho deliberado:

a. Tratamiento ilícito llevado a cabo por negligencia: el tratamiento debe finalizar y, si los datos no son necesarios para otro tratamiento lícito, deberán ser eliminados.

Que la organización haya tomado las medidas necesarias y adecuadas para solventar el incidente no implica que pueda ser denunciada por las personas afectadas y recibir una sanción con posterioridad. Las personas afectadas podrían denunciar en la AEPD o en un juzgado.

b. Incidente de seguridad por negligencia o deliberado:

- Si el incidente afecta al Responsable del tratamiento: se deberá aplicar el procedimiento establecido por la organización relativo a los incidentes de seguridad, por lo que remitimos al apartado 4.1.5. Notificación de brechas de seguridad de los datos de esta guía.
- Si el incidente afecta al Encargado del tratamiento: lo deberá notificar al Responsable del tratamiento lo antes posible, quien iniciará procedimiento establecido por la organización relativo a los incidentes de seguridad.

Tanto en el supuesto de que una persona afectada por el tratamiento ilícito o por un incidente de seguridad de la organización decida reclamar ante la AEPD o, sea la propia AEPD quien actúe por iniciativa propia, el procedimiento será como sigue[69]:

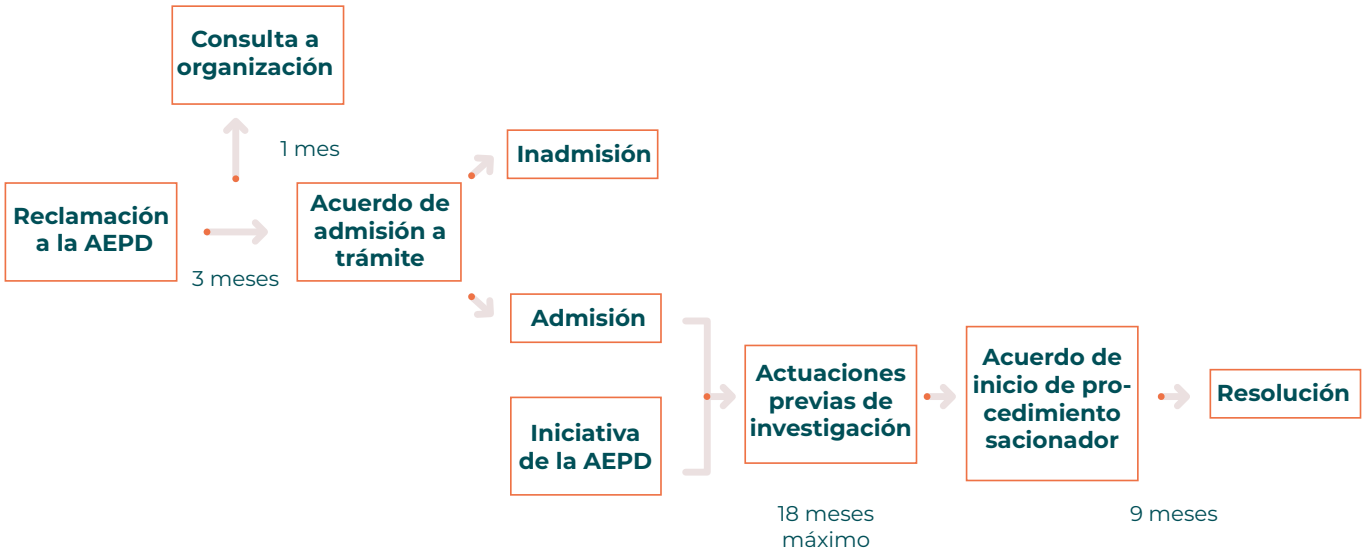


Ilustración 13 Procedimiento reclamación para determinación de posible infracción

69. *Artículos 63, 64, 65 ,66, 67 y 68 de la LOPDGDD.*

- Cuando el procedimiento se inicie porque la persona afectada ha interpuesto una reclamación en la AEPD, las actuaciones serán las mismas que cuando se ha producido una vulneración de los derechos de las personas afectadas por falta de atención de una solicitud de ejercicio de los derechos, hasta el momento de resolver la admisión a trámite.

- En el caso de que se haya admitido la reclamación o cuando la AEPD actúe por iniciativa propia, la AEPD puede establecer una fase de **actuaciones previas de investigación** para analizar los hechos y las circunstancias de la posible vulneración. Estas Actuaciones no podrán tener una duración superior a dieciocho meses desde la fecha del acuerdo de admisión a trámite o desde la fecha del acuerdo por el que se decida su iniciación cuando la AEPD actúe por propia iniciativa.

- Una vez concluyan las Actuaciones previas de investigación y se concluya que ha habido una infracción, la Presidencia de la AEPD podrá dictar el acuerdo de inicio del procedimiento sancionador, donde se especificarán los hechos, la identificación de la persona y/u organización contra la que dirigir el procedimiento, la infracción que haya podido cometer y la posible sanción.

- El procedimiento sancionador tendrá una duración máxima de 9 meses a contar desde el acuerdo de inicio.

- Durante las actuaciones previas de investigación o una vez iniciado el procedimiento sancionador (tras el acuerdo de inicio), la AEPD podrá acordar motivadamente las medidas provisionales necesarias y proporcionadas para salvaguardar el derecho fundamental a la protección de datos. y, en especial:

a. El bloqueo cautelar de los datos: ordenar el bloqueo y cesación del tratamiento o proceder a la inmovilización de los datos.
b. La obligación inmediata de atender un derecho solicitado, para los casos de reclamaciones sobre el ejercicio de derechos.

4.3.1. RÉGIMEN SANCIONADOR

Están sujetos al régimen sancionador las personas Responsables y Encargadas del tratamiento, pero no las personas Delegadas de protección de datos.

A. Infracciones. Las infracciones se clasifican entre muy graves, graves y leves:

- **Infracciones muy graves.** Son las que conllevan un incumplimiento substancial del procesamiento de datos personales y estén relacionadas principalmente con los siguientes supuestos[70]:

  - Incumplimiento de los principios de protección de datos, incluida la licitud del tratamiento (consentimiento y la limitación de la finalidad).
  - No permitir que las personas interesadas ejerzan sus derechos de protección de datos, incluida la exigencia del pago de un canon para poder ejercerlos o el incumplimiento de la obligación del bloqueo de los datos cuando sea exigible.
  - La transferencia internacional de información sin garantías.
  - No facilitar el acceso a los datos y la resistencia u obstrucción de la función inspectora de la autoridad de protección de datos.

  Prescriben a los tres años.

70. *Ver artículo 72 de la LOPDGDD y artículo 83.5 del RGDP.*

- **Infracciones graves:** Son las que suponen una vulneración substancial del tratamiento, por ejemplo[71]:

  - Tratamiento de datos de una persona menor de edad sin consentimiento.
  - La no adopción de medidas técnicas y organizativas necesarias para la protección de datos efectiva.
  - La falta del registro de actividades de tratamiento (cuando sea obligatorio).
  - El tratamiento de los datos sin haber realizado la evaluación de impacto previa cuando sea obligatorio.
  - El incumplimiento de la obligación de notificar las brechas de seguridad a la autoridad de control.
  - Contratar a un Encargado de tratamiento que no ofrezca las garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas.
  - Incumplimientos por parte de una persona Encargada del tratamiento, como el de notificar las brechas de seguridad o contratar a otros encargados sin la autorización previa del Responsable del tratamiento.
  - El incumplimiento de la obligación de nombrar a una persona Delegada de Protección de Datos (cuando sea obligatorio).

  Prescriben a los dos años.

- **Infracciones leves:** Son las que suponen un incumplimiento no incluido en los anteriores apartados, por ejemplo[72]:

  - Falta de transparencia en la información dada a las personas afectadas.
  - No incorporar toda la información necesaria en el registro de actividades de tratamiento.
  - En relación con las brechas de seguridad, el incumplimiento del deber de informar a las personas afectadas, informar tarde, de forma incompleta o defectuosa a la autoridad de control o el incumplimiento de la obligación de documentarlas.
  - No publicar los datos de contacto de la persona Delegada de Protección de Datos o no comunicarlos a la autoridad de control cuando el nombramiento sea obligatorio.

  Prescriben al año.

B. Sanciones. Las sanciones dependerán del tipo de infracción[73]:

- Para las infracciones muy graves: serán por un importe superior a 300.000 euros.
- Para las infracciones graves serán por un importe comprendido entre 40.001 y 300.000 euros[74].
- Para las infracciones leves serán de importe igual o inferior a 40.000 euros[75].

71. *Ver artículo 73 de la LOPDGDD y artículo 83.4 del RGDP.*

72. *Ver artículo 74 de la LOPDGDD*

73. *Artículo 78 de la LOPDGDD.*

74. *El RGPD prevé multas de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior para las infracciones graves, para el incumplimiento de: Las obligaciones del Responsable y del Encargado (artículos 8, 11, 25 a 39, 42 y 43); Las obligaciones de los organismos de certificación (artículos 42 y 43); Las obligaciones de la autoridad (artículo 41, apartado 4)*

75. *El RGPD prevé multas de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, para el incumplimiento, entre otros, de: Los principios básicos para el tratamiento (artículos 5, 6, 7 y 9); Los derechos de las personas interesadas (artículos 12 a 22); Las transferencias de datos personales a terceros países no permitidas (artículos 44 a 49)*

Las sanciones se impondrán teniendo en cuenta diversos criterios[76]:

- La naturaleza, gravedad y duración de la infracción, el alcance o propósito del tratamiento y el número de personas afectadas y el nivel de los daños y perjuicios sufridos.
- Si ha habido intencionalidad o negligencia en la infracción.
- Cualquier medida tomada por la entidad para paliar los daños y perjuicios sufridos por las personas afectadas.
- El grado de responsabilidad de la entidad, en función de las medidas técnicas u organizativas que se hayan aplicado.
- La reincidencia, es decir, si la entidad ha cometido infracciones anteriormente.
- El grado de cooperación con la autoridad de control para poner remedio a la infracción y mitigar los posibles efectos adversos.
- Las categorías de datos afectadas por la infracción.
- La forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si la entidad notificó la infracción y, en ese caso, en qué medida.
- Cuando la entidad cumpla las siguientes medidas ordenadas por la AEPD: atender una advertencia, un requerimiento, atender el ejercicio de derechos, respetar una limitación temporal o definitiva del tratamiento, retirada de una certificación o suspender una transferencia internacional de datos.
- El carácter continuado de la infracción.
- La vinculación de la actividad de la entidad con la realización de tratamientos de datos personales.
- Los beneficios obtenidos como consecuencia de la comisión de la infracción.
- La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.
- La afectación a los derechos de personas menores de edad.
- Disponer, cuando no fuere obligatorio, de un Delegado de protección de datos.
- Cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

C. Indemnizaciones. Las personas afectadas también podrán solicitar una indemnización de la organización cuando hayan sufrido daños y perjuicios por una infracción de la normativa de protección de datos.

Para reclamar la indemnización la persona afectada deberá presentar una denuncia ante los tribunales.

4.4. IMPLEMENTACIÓN DE UN MODELO DE PROTECCIÓN DE DATOS EN LA ENTIDAD

Todas las organizaciones del Tercer Sector de Acción Social están obligadas a implementar medidas para el cumplimiento de la normativa de protección da datos porque tratan datos personales, ya sean datos de las personas contratadas, del personal voluntario, de las personas integrantes de

76. *Artículo 83.2 del RGPD y artículo 76 de la LOPDGDD.*

la Asamblea o del Patronato o de personas usuarias.

Las medidas implementadas forman parte de un modelo de protección de datos que se puede incluir dentro del Modelo de Cumplimiento Normativo de la entidad.

En esta guía se va a proponer un modelo de protección de datos basado en la metodología expuesta en el **Manual de elaboración de planes de cumplimiento normativo para entidades del Tercer Sector de Acción Social**[77] siendo la normativa de protección de datos uno de los dieciséis ámbitos normativos que pueden afectar a una organización.

A modo de recordatorio, a continuación, se muestra el Modelo de Cumplimiento que se planteaba en el manual anteriormente mencionado:

Ver gráfico en la página siguiente

77. *Plataforma de ONG de Acción Social. (2020). Manual de elaboración de planes de cumplimiento normativo para entidades del Tercer Sector de Acción Social*

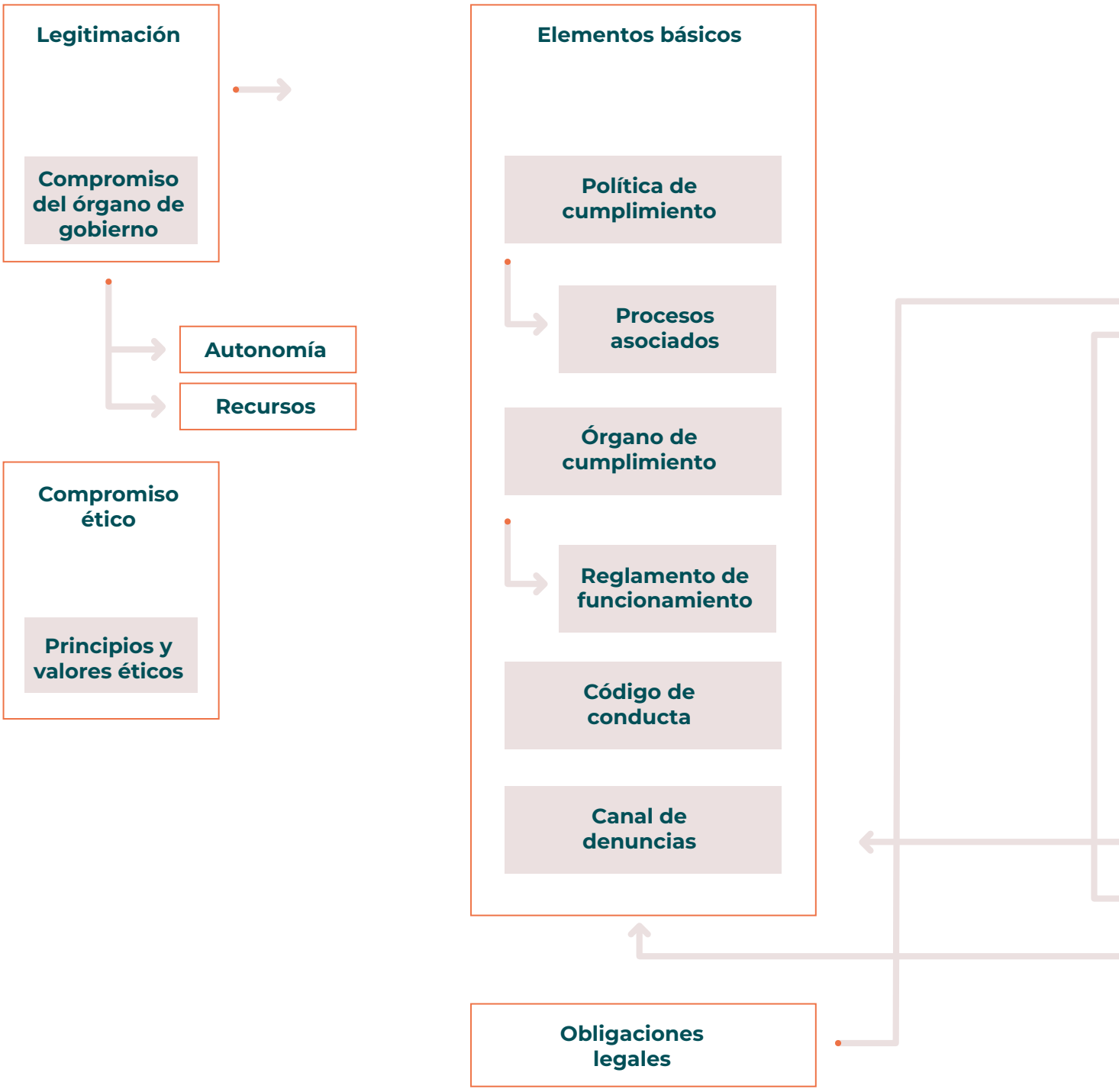
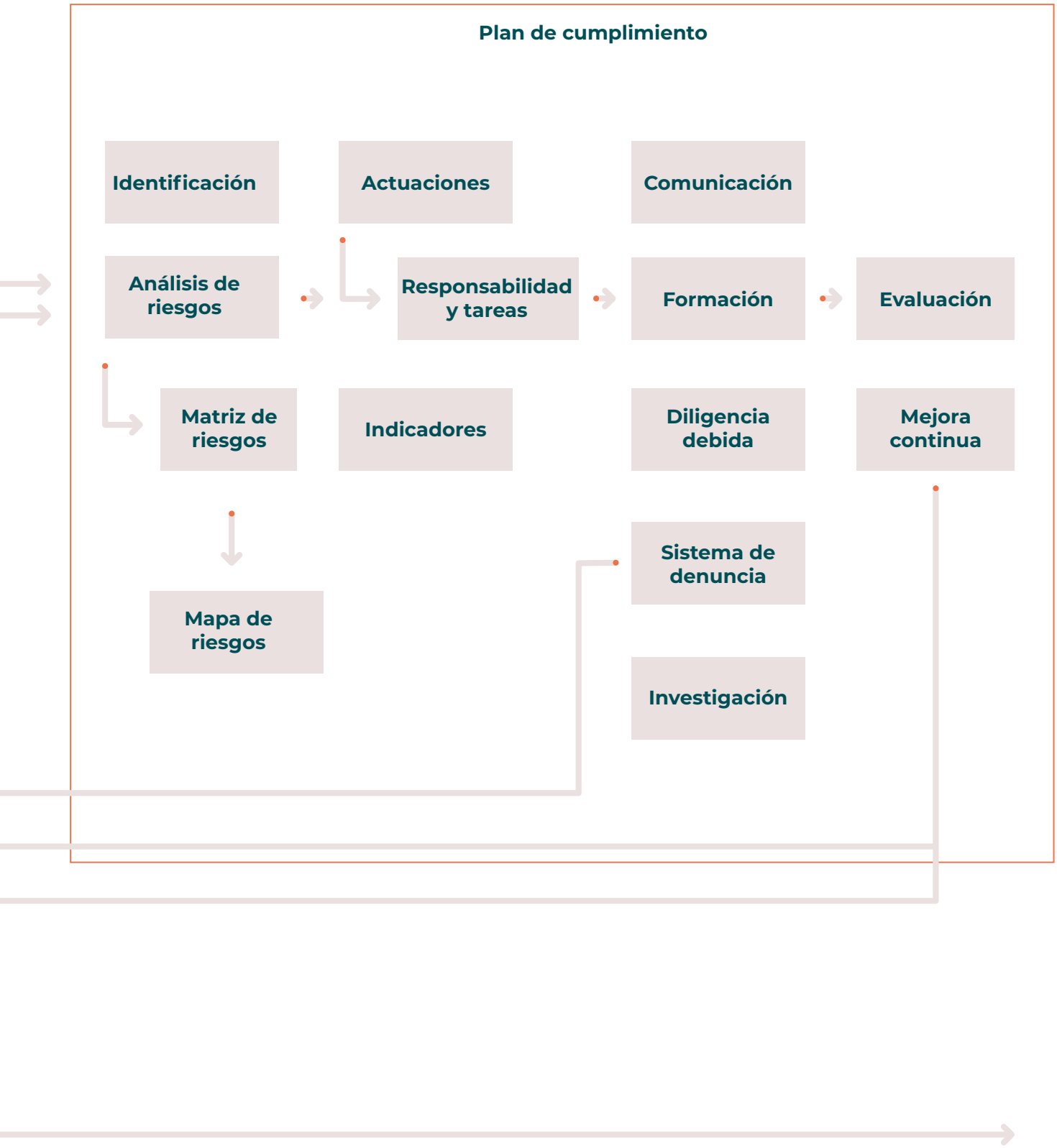


Ilustración 14 Ejemplo de Modelo de Cumplimiento Normativo


Plan de cumplimiento
Identificación
Actuaciones
Comunicación
Análisis de riesgos
Responsabilidad y tareas
Formación
Evaluación
Matriz de riesgos
Indicadores
Diligencia debida
Mejora continua
Mapa de riesgos
Sistema de denuncia
Investigación

La normativa sobre protección de datos se englobaría dentro de las obligaciones legales a las que una entidad tiene que hacer frente y el modelo de protección de datos estaría integrado en el Plan de Cumplimiento y formaría parte de todas sus etapas.

En los siguientes apartados se va a relacionar lo tratado en los anteriores capítulos de esta guía con el Plan de Cumplimiento Normativo desde un punto de vista práctico.

4.4.1. MODELO DE PROTECCIÓN DE DATOS

En esta guía se va a denominar Modelo de protección de datos al proceso que comprende entre la identificación de los tratamientos que lleva a cabo la organización hasta la evaluación de las medidas técnicas y organizativas implantadas por la entidad en materia de protección de datos.

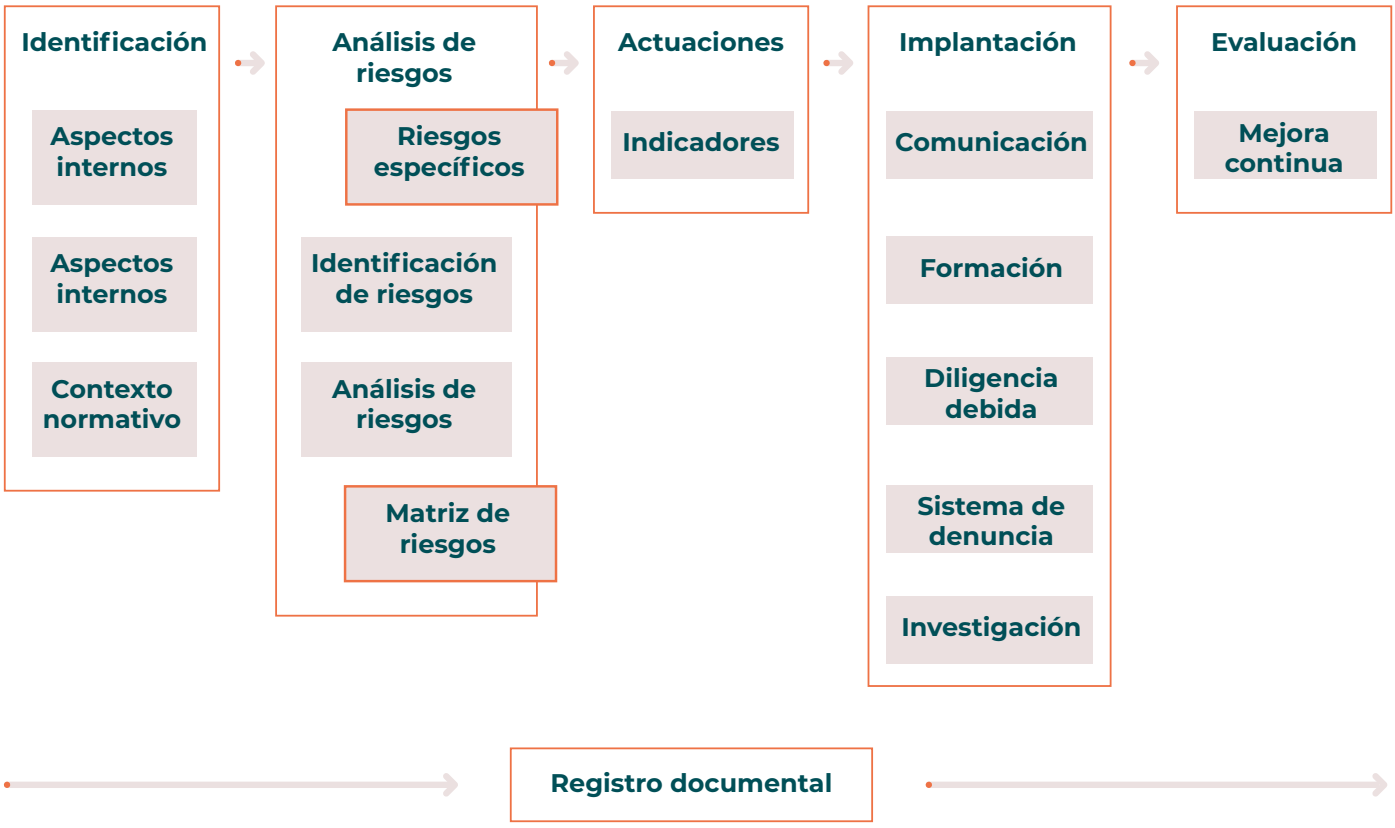


Ilustración 15 Ejemplo de Modelo de Protección de Datos

En esta guía nos vamos a centrar en las etapas de Identificación, Análisis de riesgos y Actuaciones que son específicas para la protección de datos. Para el resto de las etapas, al ser comunes para todo el ámbito de aplicación del Plan de Cumplimiento Normativo, se remite al Manual de elaboración de planes de cumplimiento normativo para entidades del Tercer Sector de Acción Social mencionado anteriormente, donde son explicadas y analizas en profundidad.

4.4.1.1. IDENTIFICACIÓN

Consiste en enumerar y describir brevemente los aspectos internos, los aspectos externos y el contexto normativo que pueden condicionar las medidas técnicas y organizativas a implementar en la entidad en materia de protección de datos.

Si la organización ya dispone de un Plan de Cumplimiento Normativo, esta etapa

no hace falta volver a hacerla y se puede recurrir al trabajo ya realizado y documentado. Se recomienda hacer una sencilla enumeración de:

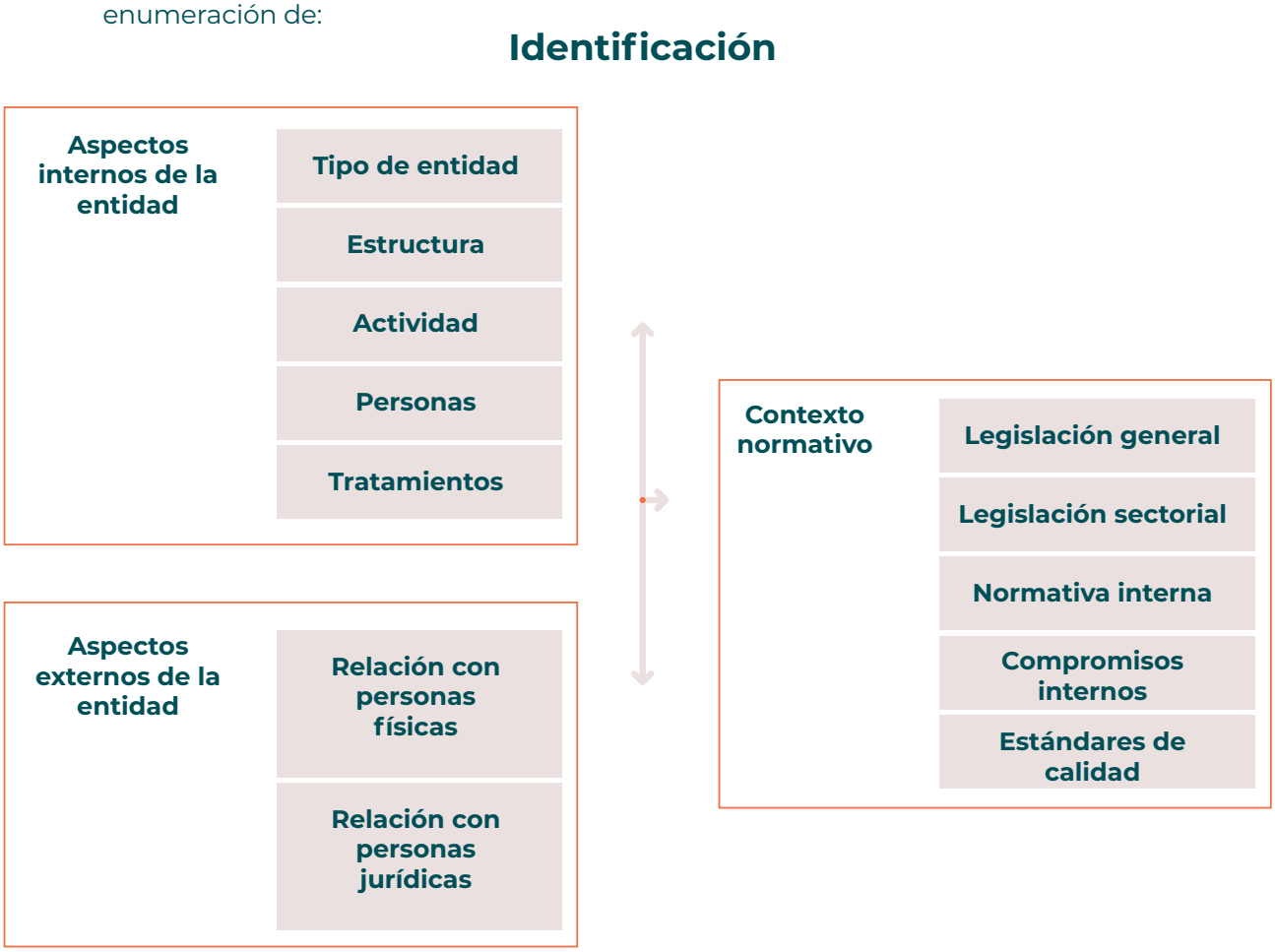


Ilustración 16 Etapa de identificación

• En relación con los aspectos internos de la entidad:

Para poder identificar los aspectos internos de la organización es necesario conocer: la tipología, la identidad, la estructura, la actividad, las personas que colaboran en la organización, los procesos organizacionales y los posibles riesgos en materia de protección de datos a los que se enfrenta.

- Tipo de entidad: indicar la razón social completa, la forma jurídica (asociación o fundación), el nivel, tamaño, si es de utilidad pública, ámbito territorial, sedes sociales, tipología de socios (personas o entidades) en caso de que se trate de una asociación, órganos de gobierno y su composición.

Para facilitar la recopilación de esta información, a modo de ejemplo, se puede utilizar la siguiente tabla obtenida de otra similar que figura en el **Manual de elaboración de planes de cumplimiento normativo para entidades del Tercer Sector de Acción Social**[78]

78. *Plataforma de ONG de Acción Social. (2020). Manual de elaboración de planes de cumplimiento normativo para entidades del Tercer Sector de Acción Social*

CUESTIONARIO DE IDENTIFICACIÓN DEL TIPO DE ENTIDAD	
Razón social completa (Denominación de la entidad)	
Forma jurídica	*Asociación / Fundación*
Nivel	*Primer nivel / Segundo nivel / Tercer nivel*
Tamaño	*(Indicar volumen de ingresos y número de personas contratadas)*
Utilidad pública	*Sí / No*
Ámbito territorial	*Local / Provincial / Autonómico / Nacional / Internacional*
Sedes sociales	
Tipología de socios	*Personas jurídicas / Personas físicas*
Órganos de gobierno	*Asamblea / Patronato / Junta Directiva / Comisión Permanente*
Composición de los órganos de gobierno	Persona designada / Organización que representa (si aplica)

Tabla 14 Cuestionario de identificación del tipo de entidad

- Estructura de la organización: se podría identificar de manera gráfica la estructura de la organización a través de un organigrama en el que se muestren los diferentes departamentos o unidades, las relaciones entre departamentos o unidades y la función de cada una de ellos, así como de las personas que trabajan en los mismos.

- Actividad de la organización: cuáles son sus actividades principales, a qué colectivos dirigen esas actuaciones, si es de atención directa, si comercializa productos y/o servicios, tipos de ingresos y su origen, así como la tipología de gastos.

Para facilitar la recopilación de esta información, a modo de ejemplo, se puede utilizar la siguiente tabla obtenida de otra similar que figura en el **Manual de elaboración de planes de cumplimiento normativo para entidades del Tercer Sector de Acción Social**[79]

79. *Plataforma de ONG de Acción Social. (2020). Manual de elaboración de planes de cumplimiento normativo para entidades del Tercer Sector de Acción Social*

CUESTIONARIO DE ACTIVIDAD DE LA ENTIDAD	
¿Cómo clasificarías la organización según su campo de actuación?	
¿Qué principales servicios provee la organización?	
¿Qué actividades principales relacionadas con otras funciones sociales, distintas a la provisión de servicios, realizan desde la organización?	
¿Qué grupos de personas son destinatarias de la actividad de la entidad?	
¿Cuál es el número de personas beneficiarias directas y el número aproximado de beneficiarias indirectas de servicios/ actividades de la organización?	
¿Cuál es la financiación pública obtenida atendiendo a su origen (quién la concede)?	
¿Cuál es la financiación pública obtenida atendiendo a su naturaleza (para qué se va destinar)?	
¿Cuál es la financiación privada obtenida atendiendo a su origen (quién la concede)?	
¿Cuál es la financiación pública obtenida atendiendo a su naturaleza (para qué se va destinar)?	
¿Qué servicios presta la organización?	
¿Quiénes prestan estos servicios en la organización?	
¿Qué productos vende la entidad?	
¿Qué canales de distribución o puntos de venta son utilizados para la venta de los productos?	

Tabla 15 Cuestionario de actividad de la entidad

- Personas: se refiere a las personas que intervienen en la actividad de la organización:
  - Personas contratadas: si hay personas contratadas, su número y las tareas que realiza cada una. Identificar a las personas y sus tareas ayudará a conocer quiénes tienen contacto con los datos personales.
  - Personas voluntarias: si hay personas voluntarias que colaboren con la organización, su número y las tareas que realiza cada una. Igual que con las personas contratadas, identificar a las personas voluntarias y las tareas que desempeñan ayuda a descubrir si tratan datos personales de la entidad.
- Tratamientos: tal y como se mencionó en el apartado 4.1.3. Evaluación de riesgos, para describir los tratamientos es necesario analizar el ciclo de vida de los datos y determinar la naturaleza, el alcance o ámbito, el contexto y la finalidad de cada tratamiento.

Al describir los tratamientos se identifican aspectos internos y externos de la organización y el contexto normativo, por lo que se recomienda que, si se analiza algún aspecto en este apartado, no se lleve a cabo en otros apartados.

El siguiente cuestionario puede servir de ayuda para determinar la naturaleza, el alcance o ámbito, el contexto y la finalidad de cada tratamiento:

CUESTIONARIO DE TRATAMIENTOS	
Naturaleza:	
¿En qué actividades de la entidad se recogen, usan o almacenan datos personales?	
¿Qué flujos de datos hay en la organización? Identificación de los movimientos de datos dentro de la entidad	
¿Los datos se tratan física o digitalmente?	
Si se tratan digitalmente, ¿se hace de forma manual o automatizada?	
¿Qué dispositivos, programas informáticos o aplicaciones se utilizan para tratar los datos?	
Personal de la organización con acceso a los datos personales (contratado, voluntario, externo)	
Tecnología que interviene en el tratamiento	
Actividades externalizadas en las que se tratan datos de la organización (gestoría, mantenimiento informático, mantenimiento del correo electrónica, almacén, etc.)	
¿Ha habido algún incidente de seguridad?	
Si ha habido un incidente, ¿se ha tratado de una brecha de seguridad o no ha dado lugar?	
Ámbito / alcance:	
Tipos de datos recogidos (Datos de identificación, datos de localización, datos bancarios, datos sensibles, etc.)	
¿Qué categorías tienen las personas cuyos datos son tratados? (Trabajadoras, voluntarias, personas vulnerables, menores de edad, etc.)	
¿Cuál es el número de personas cuyos datos son tratados?	
Diversidad de los datos tratados, ¿son similares o hay muchas diferencias entre las tipologías?	
¿Cuál es la duración del tratamiento? (Desde que se recogen los datos hasta que se eliminan?	
¿Cuáles son los plazos necesarios para la conservación de los datos?	
¿Cuál es el volumen de los datos? (Número de datos)	
¿Cuál es la extensión geográfica de la recogida de los datos? (Local, provincial, autonómica, nacional o internacional)	
¿Cada cuánto tiempo se recogen los datos?	

Contexto:	
¿A qué colectivos dirige la atención la organización?	
¿Cuál es el entorno social en el que se sitúa la entidad?	
¿Qué legislación o normativa externa es de aplicación? (Normativa de protección de datos, normativa de subvenciones y cualquier otra normativa que tenga que aplicar la organización)	
¿Qué normativa interna es de aplicación? (Estatutos, Código de conducta, canal de denuncia, plan de igualdad, protocolo antiacoso, estándares de calidad y cualquier otra normativa que se tenga que aplicar)	
¿Qué cesiones de datos a terceras personas lleva a cabo la organización?	
¿Se realizan transferencias internacionales?	
¿Se han producido brechas de seguridad en organizaciones del sector?	
¿Qué posibles consecuencias podría producir en la ciudadanía un incidente de seguridad en la organización?	
Finalidad:	
¿Para qué se usan los datos que recoge la organización? (Finalidad principal)	
Además de la finalidad principal, ¿para qué son necesarios los datos recogidos?	

Tabla 16 Cuestionario de tratamientos

- **En relación con los aspectos externos de la entidad:**

  La organización se relaciona con personas físicas y jurídicas:

  - Personas físicas: englobaría a las personas usuarias, a las socias y a las personas que ejercer su profesión en régimen de autónomos.
  - Personas jurídicas: comprendería a proveedores de bienes y servicios, administraciones públicas, universidades, otras organizaciones sin ánimo de lucro y otros.

- **Respecto al contexto normativo:**

El contexto normativo condiciona la actividad de la organización y, en particular, la normativa de protección de datos determina cómo la entidad tiene que tratar los datos personales.

Pero no solamente hay que tener en cuenta la normativa de protección de datos, el resto de normativa también puede afectar al tratamiento de datos en la entidad porque para su cumplimiento sea necesario solicitar otro tipo de datos personales o haya que aumentar los plazos de conservación de estos, sin olvidar que darían lugar a otros fines.

Hay que tener en cuenta la normativa externa que le sea de aplicación a la entidad, así como la interna.

4.4.1.2. ANÁLISIS DE RIESGOS

Una vez se haya realizado la fase de identificación de los aspectos internos, externos y el contexto normativo que condicionan la protección de datos, el siguiente paso es la identificación de los riesgos y su análisis. Los riesgos a identificar y analizar serán los asociados a la protección de datos (información) y los asociados a la defensa de los derechos y libertades de las personas interesadas.

En el apartado 4.1.2. Evaluación de riesgos de esta guía se trató cómo identificar los riesgos genéricos que puede tener una organización del TSAS, por lo que remitimos a dicho apartado.

Para la determinación del nivel del riesgo (análisis) el procedimiento que se propone es el que figura en el apartado 4.1.2. Evaluación de riesgos de esta guía, donde el nivel de cada riesgo es la combinación entre su probabilidad y su posible impacto, representándose en un mapa de calor. Cabe mencionar que las organizaciones que no están obligadas a realizar una EIPD no tienen que hacer un análisis de riesgos, pero sería recomendable que lo hicieran, aunque sea uno sencillo.

Tal y como se ha mencionado, cada organización tiene sus riesgos específicos, sin embargo, hay una serie de riesgos que serían comunes a la mayoría de las organizaciones:

- **Cuando la entidad tiene PERSONAL CONTRATADO:**

Las personas interesadas serán aquellas cuyos datos se tratan, ya sea en los procesos de selección, como en la contratación, relación laboral y finalización del contrato.

Los riesgos específicos del tratamiento de los datos de las personas interesadas podrían ser:

DESCRIPCIÓN DEL TRATAMIENTO	CATEGORÍAS DE FACTORES DE RIESGO	FACTORES DE RIESGO	EJEMPLOS DE RIESGOS ESPECÍFICOS
NATURALEZA	Recogida y generación de datos	Factores de riesgo derivados de recogida o generación de datos de forma específica	Riesgos asociados a la protección de los datos: - Que los datos personales de las personas que envían los curriculum vitae o de las personas contratadas por la organización estén comprometidos (no confidencialidad) - Que se recojan datos no necesarios Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando se recojan los datos mediante: - Curriculum vitae recibidos directamente de otras organizaciones - Externalización del proceso de selección de personal - Curriculum vitae recibidos mediante correo electrónico por iniciativa propia de la persona interesada - Recogida de datos de redes sociales de la persona interesada - Falta de transparencia del momento preciso de la recogida de datos de las personas contratadas - Información procedente del canal de denuncias
	Factores técnicos del tratamiento	Factores de riesgo derivados de implementarse con determinadas características técnicas o tecnologías	Riesgos asociados a la protección de los datos: Que la confidencialidad de los datos esté comprometida, que los datos no estén disponibles y/o que se pierda la integridad de los datos Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando se traten datos usando: - Aplicaciones móviles para geolocalización, registro de la jornada - Uso innovador o nuevas soluciones organizativas - Videovigilancia
	Brechas de seguridad	Factores de riesgo que se derivan de la posible materialización de brechas de seguridad sobre los datos personales	Riesgos asociados a la protección de los datos: Un incidente de seguridad puede afectar a la confidencialidad, integridad y disponibilidad de los datos personales - Incidentes de seguridad que supongan una brecha de seguridad

ÁMBITO / ALCANCE	Tipos de datos utilizados	Factores de riesgo derivados de los datos recogidos, procesados o inferidos en el tratamiento	Riesgos asociados a la protección de los datos: Que la confidencialidad de los datos esté comprometida, que los datos no estén disponibles y/o que se pierda la integridad de los datos Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando los datos tratados sean: - Datos que midan el rendimiento laboral: control de acceso al lugar de trabajo, grabación de imágenes del puesto de trabajo, monitorización de los equipos de las personas empleadas, Inferencia del rendimiento a través de indicadores (productividad y calidad del trabajo, eficiencia, formación adquirida, objetivos conseguidos), etc. - Datos de medios de pago: números de cuenta bancaria - Datos sanitarios (bajas laborales, justificantes de visitas médicas e información de reconocimientos médicos) - Datos personales relativos a condenas e infracciones penales (certificado de delitos de naturaleza sexual)
	Categorías de personas interesadas	Factores de riesgo relativos a la categoría de personas interesadas	Riesgos asociados a la protección de los datos: Los riesgos que afecten a la confidencialidad, disponibilidad e integridad de los datos son elevados Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando las personas afectadas cuyos datos se vayan a tratar o se traten sean de: - Personas contratadas por la organización que, a su vez, pueden ser víctimas de violencia de género, personas con discapacidad, personas en riesgo de exclusión social y/o personas vulnerables
	Extensión y alcance del tratamiento	Factores de riesgo relativos al número de personas afectadas, a la diversidad de los datos tratados, a la duración en el tiempo del tratamiento y de la conservación de los datos, el volumen de los datos, la extensión geográfica de los datos, la frecuencia de la recogida de los datos	Riesgos asociados a la protección de los datos: La confidencialidad de los datos puede comprometerse, la disponibilidad de los datos puede disminuir y la integridad puede verse afectada Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando el tratamiento: - Se recopilen excesivos datos con relación al fin del tratamiento - El riesgo es más elevado porque se trata de tratamientos continuados en el tiempo (mientras dure la relación laboral y el período de conservación)

DESCRIPCIÓN DEL TRATAMIENTO	CATEGORÍAS DE FACTORES DE RIESGO	FACTORES DE RIESGO	EJEMPLOS DE RIESGOS ESPECÍFICOS
CONTEXTO	Categoría de las personas Responsable / Encargada del tratamiento	Factores de riesgo derivados del sector de la entidad y el colectivo al que se dirigen sus actuaciones	Riesgo derivado de que la organización dispone de personal contratado
	Comunicaciones de datos	Factores de riesgo derivadas de las comunicaciones de datos a terceros en el marco del tratamiento	Riesgos asociados a la protección de los datos: La confidencialidad de los datos puede comprometerse, que los datos no estén disponibles o la disponibilidad sea menor y que la integridad esté afectada Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando: - Externalización de actividades (gestión de nóminas, seguros sociales e impuestos; prevención de riesgos laborales) - Revisión de las cuentas justificativas de subvenciones y auditoría de las cuentas anuales por auditor de cuentas - Justificación de subvenciones al organismo financiador
	Efectos colaterales del tratamiento	Factores de riesgo que se derivan de consecuencias no contempladas en los propósitos originales previstos del tratamiento	- Posible pérdida de control de los datos tratados por la persona Encargada del tratamiento - Puede provocar exclusión - Puede provocar discriminación - Posible daño reputacional - Posible perjuicio económico significativo - Posible perjuicio moral significativo - Posible pérdida de confidencialidad de datos - Podría impedir el ejercicio de un derecho a las personas contratadas
FINALIDAD	Operaciones relacionadas con los fines del tratamiento	Factores de riesgo que se derivan del fin declarado del tratamiento y otros fines vinculados al propósito principal	Riesgos asociados a la protección de los datos: La confidencialidad de los datos puede comprometerse cuando los datos son usados para otros fines vinculados, que los datos no estén disponibles o parte de ellos para los otros fines y que se pierda la integridad de los datos Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando los fines del tratamiento sean: - Control de las personas contratadas: evaluación, grabación de audios y/o imágenes, control del tiempo invertido en realizar tareas, control del uso de internet y del teléfono, geolocalización, monitorización y control del correo electrónico, etc. - Videovigilancia - Decidir sobre o impedir el ejercicio de derechos fundamentales: derechos de igualdad, no discriminación, intimidad personal y familiar, a la libertad sindical, etc. - Decidir sobre el control de los datos de la persona interesada - Uso de imágenes del personal en redes sociales y/o en la página web - Conservación de los datos

Tabla 17 Riesgos derivados de tener personal contratado

- **Cuando la organización dispone de PÁGINA WEB:**

Las personas interesadas serán aquellas que consulten los contenidos de la página web, a las que soliciten información y envíen datos a través de formularios de la web, a quienes usen el canal de denuncias para informar de posibles incumplimientos normativos y cualquiera que acceda a la página web de la organización.

Los riesgos específicos del tratamiento de los datos de las personas interesadas podrían ser:

DESCRIPCIÓN DEL TRATAMIENTO	CATEGORÍAS DE FACTORES DE RIESGO	FACTORES DE RIESGO	EJEMPLOS DE RIESGOS ESPECÍFICOS
NATURALEZA	Recogida y generación de datos	Factores de riesgo derivados de recogida o generación de datos de forma específica	Riesgos asociados a la protección de los datos: Que la confidencialidad de los datos esté comprometida Que los datos recogidos no sean precisos, completos, consistentes y confiables Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando se recojan los datos mediante: - Falta de transparencia del momento preciso de la recogida de datos (cookies de la página, formularios, canal de denuncias, recepción de donaciones)
	Factores técnicos del tratamiento	Factores de riesgo derivados de implementarse con determinadas características técnicas o tecnologías	Riesgos asociados a la protección de los datos: Que la confidencialidad de los datos esté comprometida, que los datos no estén disponibles y/o que se pierda la integridad de los datos Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando se traten datos usando: - Uso de cookies propias o de terceros - Uso innovador o nuevas soluciones organizativas - Tratamientos automatizados
	Brechas de seguridad	Factores de riesgo que se derivan de la posible materialización de brechas de seguridad sobre los datos personales	Riesgos asociados a la protección de los datos: - Un incidente de seguridad puede afectar a la confidencialidad, integridad y disponibilidad de los datos personales Incidentes de seguridad que supongan una brecha de seguridad

DESCRIPCIÓN DEL TRATAMIENTO	CATEGORÍAS DE FACTORES DE RIESGO	FACTORES DE RIESGO	EJEMPLOS DE RIESGOS ESPECÍFICOS
ÁMBITO / ALCANCE	Tipos de datos utilizados	Factores de riesgo derivados de los datos recogidos, procesados o inferidos en el tratamiento	Riesgos asociados a la protección de los datos: Los riesgos que afecten a la confidencialidad, disponibilidad e integridad de los datos serán más o menos elevados en función del tipo de datos tratados Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando los datos tratados sean: - Datos de medios de pago: números de tarjeta, números de cuenta bancaria - Datos de navegación web: registro de páginas visitadas (historial de navegación, logs de servidores web, etc.), registro del tiempo que se está en cada página, registro del momento de la visita a la página, registro del número de conexiones, etc.
	Extensión y alcance del tratamiento	Factores de riesgo relativos al número de personas afectadas, a la diversidad de los datos tratados, a la duración en el tiempo del tratamiento y de la conservación de los datos, el volumen de los datos, la extensión geográfica de los datos, la frecuencia de la recogida de los datos	Riesgos asociados a la protección de los datos: La confidencialidad de los datos puede comprometerse, la disponibilidad de los datos puede disminuir y la integridad puede verse afectada Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando el tratamiento: Se recopilen excesivos datos con relación al fin del tratamiento
	Comunicaciones de datos	Factores de riesgo derivadas de las comunicaciones de datos a terceros en el marco del tratamiento	Riesgos asociados a la protección de los datos: La confidencialidad de los datos puede comprometerse, que los datos no estén disponibles o la disponibilidad sea menor y que la integridad esté afectada Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando: - Cookies de terceros en la página web - Transferencias internacionales
	Efectos colaterales del tratamiento	Factores de riesgo que se derivan de consecuencias no contempladas en los propósitos originales previstos del tratamiento	- Puede provocar exclusión - Puede provocar discriminación - Posible usurpación de identidad - Posible daño reputacional - Posible perjuicio económico significativo - Posible perjuicio moral significativo - Posible pérdida de confidencialidad de datos - Podría impedir el ejercicio de un derecho

DESCRIPCIÓN DEL TRATAMIENTO	CATEGORÍAS DE FACTORES DE RIESGO	FACTORES DE RIESGO	EJEMPLOS DE RIESGOS ESPECÍFICOS
FINALIDAD	Operaciones relacionadas con los fines del tratamiento	Factores de riesgo que se derivan del fin declarado del tratamiento y otros fines vinculados al propósito principal	Riesgos asociados a la protección de los datos: La confidencialidad de los datos puede comprometerse cuando los datos son usados para otros fines vinculados, que los datos no estén disponibles o parte de ellos para los otros fines y que se pierda la integridad de los datos Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando los fines del tratamiento sean: - Decisiones automatizadas sin intervención humana - Decidir sobre o impedir el ejercicio de derechos fundamentales: derechos de las personas que acceden a la página o interactúan, derechos de las personas informantes a través del Canal de denuncias - Decidir sobre el control de la persona interesada de sus datos personales - Decidir sobre el acceso a un servicio - Conservación de los datos

Tabla 18 Riesgos derivados de la página web

- Cuando en la organización se usa **EQUIPAMIENTO INFORMÁTICO y CORREO ELECTRÓNICO:**

Las personas interesadas serán aquellas cuyos datos sean tratados en la organización.

Los riesgos específicos del tratamiento de los datos de las personas interesadas podrían ser:

DESCRIPCIÓN DEL TRATAMIENTO	CATEGORÍAS DE FACTORES DE RIESGO	FACTORES DE RIESGO	EJEMPLOS DE RIESGOS ESPECÍFICOS
NATURALEZA	Recogida y generación de datos	Factores de riesgo derivados de recogida o generación de datos de forma específica	Riesgos asociados a la protección de los datos: Que la confidencialidad de los datos esté comprometida Que los datos recogidos no son precisos, completos, consistentes y confiables Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando se recojan los datos mediante: - Procedentes de dos o más tratamientos con finalidades diferentes - Falta de transparencia del momento preciso de la recogida de datos
	Factores técnicos del tratamiento	Factores de riesgo derivados de implementarse con determinadas características técnicas o tecnologías	Riesgos asociados a la protección de los datos: Que la confidencialidad de los datos esté comprometida, que los datos no estén disponibles y que se pierda la integridad de los datos Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando se traten datos usando: - Internet de las cosas (IoT) - Inteligencia Artificial - Uso innovador o nuevas soluciones organizativas - Uso innovador de tecnologías consolidadas - Tratamientos automatizados
	Brechas de seguridad	Factores de riesgo que se derivan de la posible materialización de brechas de seguridad sobre los datos personales	Riesgos asociados a la protección de los datos: Un incidente de seguridad puede afectar a la confidencialidad, integridad y disponibilidad de los datos personales Incidentes de seguridad que supongan una brecha de seguridad, ya sea por un error o intencionados
ÁMBITO / ALCANCE	Tipos de datos utilizados	Factores de riesgo derivados de los datos recogidos, procesados o inferidos en el tratamiento	No aplica (los riesgos derivan de los datos no de la forma de tratarlos)
	Categorías de personas interesadas	Factores de riesgo relativos a la categoría de personas interesadas	No aplica (los riesgos derivan de las personas interesadas no de la forma de tratarlos)
	Extensión y alcance del tratamiento	Factores de riesgo relativos al número de personas afectadas, a la diversidad de los datos tratados, a la duración en el tiempo del tratamiento y de la conservación de los datos, el volumen de los datos, la extensión geográfica de los datos, la frecuencia de la recogida de los datos	No aplica (los riesgos derivan de la extensión y alcance del tratamiento no de la forma de tratarlos)

DESCRIPCIÓN DEL TRATAMIENTO	CATEGORÍAS DE FACTORES DE RIESGO	FACTORES DE RIESGO	EJEMPLOS DE RIESGOS ESPECÍFICOS
CONTEXTO	Categoría de las personas Responsable / Encargada del tratamiento	Factores de riesgo derivados del sector de la entidad y el colectivo al que se dirigen sus actuaciones	No aplica (los riesgos derivan del Responsable y/o del Encargado del tratamiento no de la forma de tratarlos)
	Comunicaciones de datos	Factores de riesgo derivadas de las comunicaciones de datos a terceros en el marco del tratamiento	Riesgos asociados a la protección de los datos: La confidencialidad de los datos puede comprometerse, que los datos no estén disponibles o la disponibilidad sea menor y que la integridad esté afectada Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando: - Falta de trasparencia de medios usados en el tratamiento: redes sociales, Inteligencia Artificial
	Efectos colaterales del tratamiento	Factores de riesgo que se derivan de consecuencias no contempladas en los propósitos originales previstos del tratamiento	- Posible reversión no autorizada de la seudonimización - Puede provocar exclusión - Puede provocar discriminación - Posible usurpación de identidad - Posible daño reputacional - Posible perjuicio económico significativo - Posible perjuicio moral significativo - Posible pérdida de confidencialidad de datos - Podría impedir el ejercicio de un derecho
FINALIDAD	Operaciones relacionadas con los fines del tratamiento	Factores de riesgo que se derivan del fin declarado del tratamiento y otros fines vinculados al propósito principal	Riesgos asociados a la protección de los datos: - La confidencialidad de los datos puede comprometerse cuando los datos son usados para otros fines vinculados - Que los datos no estén disponibles o parte de ellos para los otros fines - Que se pierda la integridad de los datos Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando los fines del tratamiento sean: - Creación, uso y otros tratamientos con perfiles - Control de acceso a internet - Decisiones automatizadas sin intervención humana - Tratamiento automatizado para soporte a la toma de decisiones - Decidir sobre o impedir el ejercicio de derechos fundamentales - Decidir sobre el control de la persona interesada de sus datos personales - Decidir sobre el acceso a un servicio - Conservación de los datos

Tabla 19 Riesgos derivados del uso de equipamiento informático y del correo electrónico

- Cuando se recogen datos a través de **FORMULARIOS** para la inscripción en jornadas, eventos, formación:

Las personas interesadas serán aquellas que rellenen con sus datos personales los formularios.

Los riesgos específicos del tratamiento de los datos de las personas interesadas podrían ser:

DESCRIPCIÓN DEL TRATAMIENTO	CATEGORÍAS DE FACTORES DE RIESGO	FACTORES DE RIESGO	EJEMPLOS DE RIESGOS ESPECÍFICOS
NATURALEZA	Recogida y generación de datos	Factores de riesgo derivados de recogida o generación de datos de forma específica	Riesgos asociados a la protección de los datos: - Que la confidencialidad de los datos esté comprometida - Que los datos recogidos no son precisos, completos, consistentes y confiables Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando se recojan los datos mediante: - Falta de transparencia del momento preciso de la recogida de datos
	Factores técnicos del tratamiento	Factores de riesgo derivados de implementarse con determinadas características técnicas o tecnologías	Riesgos asociados a la protección de los datos: Que la confidencialidad de los datos esté comprometida, que los datos no estén disponibles y que se pierda la integridad de los datos Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando se traten datos usando: - Uso innovador o nuevas soluciones organizativas - Uso innovador de tecnologías consolidadas - Tratamientos automatizados
	Brechas de seguridad	Factores de riesgo que se derivan de la posible materialización de brechas de seguridad sobre los datos personales	Riesgos asociados a la protección de los datos: Un incidente de seguridad puede afectar a la confidencialidad, integridad y disponibilidad de los datos personales Incidentes de seguridad que supongan una brecha de seguridad
ÁMBITO / ALCANCE	Tipos de datos utilizados	Factores de riesgo derivados de los datos recogidos, procesados o inferidos en el tratamiento	No aplica (los riesgos derivan de los datos no de la forma de tratarlos)
	Categorías de personas interesadas	Factores de riesgo relativos a la categoría de personas interesadas	No aplica (los riesgos derivan de las personas interesadas no de la forma de tratarlos)
	Extensión y alcance del tratamiento	Factores de riesgo relativos al número de personas afectadas, a la diversidad de los datos tratados, a la duración en el tiempo del tratamiento y de la conservación de los datos, el volumen de los datos, la extensión geográfica de los datos, la frecuencia de la recogida de los datos, etc.	No aplica (los riesgos derivan de la extensión y alcance del tratamiento no de la forma de tratarlos)

DESCRIPCIÓN DEL TRATAMIENTO	CATEGORÍAS DE FACTORES DE RIESGO	FACTORES DE RIESGO	EJEMPLOS DE RIESGOS ESPECÍFICOS
CONTEXTO	Categoría de las personas Responsable / Encargada del tratamiento	Factores de riesgo derivados del sector de la entidad y el colectivo al que se dirigen sus actuaciones	No aplica (los riesgos derivan del Responsable y/o del Encargado del tratamiento no de la forma de tratarlos)
	Comunicaciones de datos	Factores de riesgo derivadas de las comunicaciones de datos a terceros en el marco del tratamiento	Riesgos asociados a la protección de los datos: La confidencialidad de los datos puede comprometerse, que los datos no estén disponibles o la disponibilidad sea menor y que la integridad esté afectada Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando: - Falta de trasparencia de medios usados en el tratamiento
	Efectos colaterales del tratamiento	Factores de riesgo que se derivan de consecuencias no contempladas en los propósitos originales previstos del tratamiento	Excede las expectativas de las personas interesadas Posible reversión no autorizada de la seudonimización Posible pérdida de control de los datos tratados por la persona Encargada del tratamiento - Puede provocar exclusión - Puede provocar discriminación - Posible usurpación de identidad - Posible daño reputacional - Posible perjuicio económico significativo - Posible perjuicio moral significativo - Posible pérdida de confidencialidad de datos - Podría impedir el ejercicio de un derecho
FINALIDAD	Operaciones relacionadas con los fines del tratamiento	Factores de riesgo que se derivan del fin declarado del tratamiento y otros fines vinculados al propósito principal	Riesgos asociados a la protección de los datos: La confidencialidad de los datos puede comprometerse cuando los datos son usados para otros fines vinculados, que los datos no estén disponibles o parte de ellos para los otros fines y que se pierda la integridad de los datos Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando los fines del tratamiento sean: - Videovigilancia - Decisiones automatizadas sin intervención humana - Tratamiento automatizado para soporte a la toma de decisiones - Decidir sobre o impedir el ejercicio de derechos fundamentales: derechos de igualdad, no discriminación, intimidad personal y familiar - Decidir sobre el control del interesado de sus datos personales: derecho de acceso, rectificación, oposición, supresión, limitación del tratamiento, etc. - Uso de imágenes para difusión de actividades - Decidir sobre el acceso a un servicio - Conservación de los datos

Tabla 20 Riesgos derivados del uso de formularios

- En caso de **CONTRATACIÓN DE SERVICIOS A TERCERAS PERSONAS EXTERNAS:**

Las personas interesadas serán aquellas cuyos datos estén vinculados a las actividades que se vayan a externalizar.

Los riesgos específicos del tratamiento de los datos de las personas interesadas podrían ser:

DESCRIPCIÓN DEL TRATAMIENTO	CATEGORÍAS DE FACTORES DE RIESGO	FACTORES DE RIESGO	EJEMPLOS DE RIESGOS ESPECÍFICOS
NATURALEZA	Recogida y generación de datos	Factores de riesgo derivados de recogida o generación de datos de forma específica	Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando se recojan los datos mediante: - Falta de transparencia del momento preciso de la recogida de datos (no se informe de la persona Encargada del tratamiento)
	Factores técnicos del tratamiento	Factores de riesgo derivados de implementarse con determinadas características técnicas o tecnologías	Riesgos asociados a la protección de los datos: Que la confidencialidad de los datos esté comprometida, que los datos no estén disponibles y que se pierda la integridad de los datos Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando se traten datos usando: - Aplicaciones móviles - Internet de las cosas (IoT) - Inteligencia Artificial - Uso innovador o nuevas soluciones organizativas - Uso innovador de tecnologías consolidadas - Tratamientos automatizados - Videovigilancia
	Brechas de seguridad	Factores de riesgo que se derivan de la posible materialización de brechas de seguridad sobre los datos personales	Riesgos asociados a la protección de los datos: - Un incidente de seguridad en el Encargado puede afectar a la confidencialidad, integridad y disponibilidad de los datos personales Incidentes de seguridad en el Encargado del tratamiento que supongan una brecha de seguridad

DESCRIPCIÓN DEL TRATAMIENTO	CATEGORÍAS DE FACTORES DE RIESGO	FACTORES DE RIESGO	EJEMPLOS DE RIESGOS ESPECÍFICOS
ÁMBITO / ALCANCE	Tipos de datos utilizados	Factores de riesgo derivados de los datos recogidos, procesados o inferidos en el tratamiento	No aplica (los riesgos derivan de que exista un Encargado no de la forma de tratarlos)
	Categorías de personas interesadas	Factores de riesgo relativos a la categoría de personas interesadas	No aplica (los riesgos derivan de que exista un Encargado no de la forma de tratarlos)
	Extensión y alcance del tratamiento	Factores de riesgo relativos al número de personas afectadas, a la diversidad de los datos tratados, a la duración en el tiempo del tratamiento y de la conservación de los datos, el volumen de los datos, la extensión geográfica de los datos, la frecuencia de la recogida de los datos, etc.	No aplica (los riesgos derivan de que exista un Encargado no de la forma de tratarlos)
CONTEXTO	Categoría de las personas Responsable / Encargada del tratamiento	Factores de riesgo derivados del sector de la entidad y el colectivo al que se dirigen sus actuaciones	El riesgo puede ser mayor dependiendo de la actividad de la persona Encargada del tratamiento
	Comunicaciones de datos	Factores de riesgo derivadas de las comunicaciones de datos a terceros en el marco del tratamiento	Riesgos asociados a la protección de los datos: La confidencialidad de los datos puede comprometerse, que los datos no estén disponibles o la disponibilidad sea menor y que la integridad esté afectada - Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando: - Que se cedan los datos a otras terceras personas sin el consentimiento de la organización
	Efectos colaterales del tratamiento	Factores de riesgo que se derivan de consecuencias no contempladas en los propósitos originales previstos del tratamiento	Excede las expectativas de las personas interesadas - Posible reversión no autorizada de la seudonimización - Posible pérdida de control de los datos tratados por la persona Encargada del tratamiento - Puede provocar exclusión - Puede provocar discriminación - Posible usurpación de identidad - Posible daño reputacional - Posible perjuicio económico significativo - Posible perjuicio moral significativo - Posible pérdida de confidencialidad de datos - Podría impedir el ejercicio de un derecho

DESCRIP-CIÓN DEL TRATA-MIENTO	CATEGORÍAS DE FAC-TORES DE RIESGO	FACTORES DE RIESGO	EJEMPLOS DE RIESGOS ESPECÍFICOS
FINALIDAD	Operaciones relacionadas con los fines del tratamiento	Factores de riesgo que se derivan del fin declarado del tratamiento y otros fines vincu-lados al propósi-to principal	Riesgos asociados a la protección de los datos: La confidencialidad de los datos puede comprometerse cuando los datos son usados para otros fines vinculados, que los datos no estén disponibles o parte de ellos para los otros fines y que se pierda la integridad de los datos Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando la persona Encargada pueda usar los datos para otros fines.

Tabla 21 Riesgos derivados de la subcontratación de servicios a terceras personas

4.4.1.3. ACTUACIONES

Las actuaciones son las medidas técnicas y organizativas implantadas o que deben ser implantadas en la entidad para mitigar los riesgos identificados.

No obstante, la existencia de una medida de prevención no implica que sea efectiva, puede ser ineficaz o que su implantación no sea suficiente para mitigar el riesgo y sean necesarias otras medidas.

> *Ejemplo: disponer de claves de acceso en todos los ordenadores de la entidad es una medida de prevención para que una perso-na ajena acceda a la información de los equipos, pero si esas claves están anotadas en un lugar visi-ble, no sería una medida eficaz, ya que no mitigaría ese riesgo.*

Estas medidas dependerán de los riesgos específicos identificados. Así, para los ries-gos específicos mencionados en el apar-tado anterior, las medidas a implantar para mitigarlos serían:

Ver tabla en la página siguiente

- Cuando la entidad tiene **PERSONAL CONTRATADO:**

DESCRIPCIÓN DEL TRATAMIENTO	CATEGORÍAS DE FACTORES DE RIESGO	FACTORES DE RIESGO	EJEMPLOS DE RIESGOS GENÉRICOS	EJEMPLOS DE MEDIDAS MITIGADORAS
NATURALEZA	Recogida y generación de datos	Factores de riesgo derivados de recogida o generación de datos de forma específica	Riesgos asociados a la protección de los datos: Que los datos personales de las personas que envían los curriculum vitae o de las personas contratadas por la organización estén comprometidos (no confidencialidad) Que se recojan datos no necesarios Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando se recojan los datos mediante: Curriculum vitae recibidos directamente de otras organizaciones Externalización del proceso de selección de personal Curriculum vitae recibidos mediante correo electrónico por iniciativa propia de la persona interesada Recogida de datos de redes sociales de la persona interesada Falta de transparencia del momento preciso de la recogida de datos de las personas contratadas Información procedente del canal de denuncias	- Establecer un procedimiento de selección de personal donde se establezcan medidas de protección de la información de los CV (personas autorizadas, anonimización de CV, eliminación tras plazo de conservación estipulado, etc.) - Uso de una ficha estándar para la presentación de CV (asegurar la recogida de los datos estrictamente necesarios) - Contratos o acuerdos firmados con otras organizaciones o con empresas externas (relaciones entre Responsables) - Automatización de una respuesta informando a las personas que envíen el CV por correo electrónico - No recoger datos personales de redes sociales a no ser que sea información profesional y se informe a la persona interesada - Contrato o acuerdo con cada persona trabajadora de confidencialidad, cesión de datos y obligaciones. Puede incluir información acerca de videovigilancia y otras cuestiones - Información sobre el canal de denuncias, procedimiento y derechos - Protección a las personas denunciantes y a terceras interesadas
	Factores técnicos del tratamiento	Factores de riesgo derivados de implementarse con determinadas características técnicas o tecnologías	Riesgos asociados a la protección de los datos: Que la confidencialidad de los datos esté comprometida, que los datos no estén disponibles y/o que se pierda la integridad de los datos Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando se traten datos usando: Aplicaciones móviles para geolocalización, registro de la jornada Uso innovador o nuevas soluciones organizativas Videovigilancia	- Política de personal (derecho a desconexión) - Política de uso de dispositivos corporativos - Política de uso de dispositivos externos (o personales) - Política de ciberseguridad - Política de uso de nuevas tecnologías - Protocolo de desconexión digital - Instalar carteles informando de la existencia de cámaras de videovigilancia
	Brechas de seguridad	Factores de riesgo que se derivan de la posible materialización de brechas de seguridad sobre los datos personales	Riesgos asociados a la protección de los datos: Un incidente de seguridad puede afectar a la confidencialidad, integridad y disponibilidad de los datos personales Incidentes de seguridad que supongan una brecha de seguridad	- Procedimiento de gestión de brechas de seguridad - Política de ciberseguridad - Formar al personal para que haga un uso apropiado de la información y de los medios - Anonimizar o seudonimizar los datos - Bloqueo de los datos - Instalar medidas de seguridad en el servidor, equipos informáticos y correo electrónico - Aplicar contraseñas, accesos restringidos y usuarios - Procedimiento de copias de seguridad - Protocolo de archivo de documentación física que contenga datos personales - Protocolo de destrucción de documentación física y de eliminación de documentos digitales que contengan datos personales - Cambio de contraseñas y usuarios cuando las personas finalicen la relación laboral

DESCRIPCIÓN DEL TRATAMIENTO	CATEGORÍAS DE FACTORES DE RIESGO	FACTORES DE RIESGO	EJEMPLOS DE RIESGOS GENÉRICOS	EJEMPLOS DE MEDIDAS MITIGADORAS
ÁMBITO / ALCANCE	Tipos de datos utilizados	Factores de riesgo derivados de los datos recogidos, procesados o inferidos en el tratamiento	Riesgos asociados a la protección de los datos: Que la confidencialidad de los datos esté comprometida, que los datos no estén disponibles y/o que se pierda la integridad de los datos Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando los datos tratados sean: - Datos que midan el rendimiento laboral: control de acceso al lugar de trabajo, grabación de imágenes del puesto de trabajo, monitorización de los equipos de las personas empleadas, Inferencia del rendimiento a través de indicadores (productividad y calidad del trabajo, eficiencia, formación adquirida, objetivos conseguidos), etc. - Datos de medios de pago: números de cuenta bancaria - Datos sanitarios (bajas laborales, justificantes de visitas médicas e información de reconocimientos médicos) - Datos personales relativos a condenas e infracciones penales (certificado de delitos de naturaleza sexual)	- Evitar la recogida de ciertos tipos de datos - Recoger solo los datos estrictamente necesarios - Formar al personal para que haga un uso apropiado de la información - Política de uso de dispositivos externos (o personales) - Contrato o acuerdo con cada persona trabajadora de confidencialidad, cesión de datos y obligaciones. Puede incluir información acerca de videovigilancia y otras cuestiones (Cláusula de información) - Eliminación de los datos al finalizar el plazo de conservación establecido
	Categorías de personas interesadas	Factores de riesgo relativos a la categoría de personas interesadas	Riesgos asociados a la protección de los datos: Los riesgos que afecten a la confidencialidad, disponibilidad e integridad de los datos son elevados Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando las personas afectadas cuyos datos se vayan a tratar o se traten sean de: - Personas contratadas por la organización que, a su vez, pueden ser víctimas de violencia de género, personas con discapacidad, personas en riesgo de exclusión social y/o personas vulnerables	- Evitar la recogida de ciertos tipos de datos - Aislar y segregar fases del tratamiento entre sí para que traten datos de una forma más limitada (anonimizando los datos o seudonimizando, por ejemplo) - Formar al personal para que haga un uso apropiado de la información y de los medios - Contrato o acuerdo con cada persona trabajadora de confidencialidad, cesión de datos y obligaciones. Puede incluir información acerca de videovigilancia y otras cuestiones - Acuerdo de trabajo a distancia (teletrabajo) - Protocolo de desconexión digital
	Extensión y alcance del tratamiento	Factores de riesgo relativos al número de personas afectadas, a la diversidad de los datos tratados, a la duración en el tiempo del tratamiento y de la conservación de los datos, el volumen de los datos, la extensión geográfica de los datos, la frecuencia de la recogida de	Riesgos asociados a la protección de los datos: - La confidencialidad de los datos puede comprometerse, la disponibilidad de los datos puede disminuir y la integridad puede verse afectada Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando el tratamiento: - Se recopilen excesivos datos con relación al fin del tratamiento - El riesgo es más elevado porque se trata de tratamientos continuados en el tiempo (mientras dure la relación laboral y el período de conservación)	- No solicitar datos que no sean estrictamente necesarios para el tratamiento - Establecimiento de procedimientos y medidas de seguridad en todo el tratamiento

DESCRIPCIÓN DEL TRATAMIENTO	CATEGORÍAS DE FACTORES DE RIESGO	FACTORES DE RIESGO	EJEMPLOS DE RIESGOS GENÉRICOS	EJEMPLOS DE MEDIDAS MITIGADORAS
CONTEXTO	Categoría de las personas Responsable / Encargada del tratamiento	Factores de riesgo derivados del sector de la entidad y el colectivo al que se dirigen sus actuaciones	Riesgo derivado de que la organización dispone de personal contratado	- Evitar la recogida de ciertos tipos de datos - Establecimiento de procedimientos y medidas de seguridad en todo el tratamiento
	Comunicaciones de datos	Factores de riesgo derivadas de las comunicaciones de datos a terceros en el marco del tratamiento	Riesgos asociados a la protección de los datos: La confidencialidad de los datos puede comprometerse y que los datos no estén disponibles o la disponibilidad sea menor y que la integridad esté afectada Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando: Externalización de actividades (gestión de nóminas, seguros sociales e impuestos; prevención de riesgos laborales) Revisión de las cuentas justificativas de subvenciones y auditoría de las cuentas anuales por auditor de cuentas Justificación de subvenciones al organismo financiador	- Contrato con cada Encargado del tratamiento - Acuerdo de confidencialidad - Envío de información por canales seguros - Establecimiento de medidas de seguridad para la documentación física
	Efectos colaterales del tratamiento	Factores de riesgo que se derivan de consecuencias no contempladas en los propósitos originales previstos del tratamiento	Posible pérdida de control de los datos tratados por la persona Encargada del tratamiento Puede provocar exclusión Puede provocar discriminación Posible daño reputacional Posible perjuicio económico significativo Posible perjuicio moral significativo Posible pérdida de confidencialidad de datos Podría impedir el ejercicio de un derecho a las personas contratadas	- Contrato con cada Encargado del tratamiento - Análisis periódico de la necesidad y proporcionalidad del tratamiento

DESCRIPCIÓN DEL TRATAMIENTO	CATEGORÍAS DE FACTORES DE RIESGO	FACTORES DE RIESGO	EJEMPLOS DE RIESGOS GENÉRICOS	EJEMPLOS DE MEDIDAS MITIGADORAS
FINALIDAD	Operaciones relacionadas con los fines del tratamiento	Factores de riesgo que se derivan del fin declarado del tratamiento y otros fines vinculados al propósito principal	Riesgos asociados a la protección de los datos: La confidencialidad de los datos puede comprometerse cuando los datos son usados para otros fines vinculados, que los datos no estén disponibles o parte de ellos para los otros fines y que se pierda la integridad de los datos Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando los fines del tratamiento sean: Control de las personas contratadas: evaluación, grabación de audios y/o imágenes, control del tiempo invertido en realizar tareas, control del uso de internet y del teléfono, geolocalización, monitorización y control del correo electrónico, etc. Videovigilancia Decidir sobre o impedir el ejercicio de derechos fundamentales: derechos de igualdad, no discriminación, intimidad personal y familiar, a la libertad sindical, etc. Decidir sobre el control de los datos de la persona interesada Uso de imágenes del personal en redes sociales y/o en la página web Conservación de los datos	- Análisis periódico de las necesidades y proporcionalidades de los tratamientos - Contrato o acuerdo con cada persona trabajadora de confidencialidad, cesión de datos y obligaciones. Puede incluir información acerca de videovigilancia y otras cuestiones como autorización para grabar imágenes para su publicación en redes sociales y/o en la web - Bloqueo de los datos personales una vez finalizada la relación laboral - Formar e informar al personal sobre protección de datos - Procedimiento de copias de seguridad - Fijación de períodos de conservación de los datos - Protocolo de archivo de documentación física que contenga datos personales - Protocolo de destrucción de documentación física y de eliminación de documentos digitales que contengan datos personales

Tabla 22 Medidas mitigadoras de los riesgos derivados de tener personal contratado

A continuación, de los ejemplos de medidas de la tabla, se van a explicar los que se consideran más útiles para una organización:

Medidas a implementar en el tratamiento de Curriculum Vitae (CV):

- Si se recibe un CV a través del correo electrónico, una buena práctica sería la de responder al correo con un texto estándar previamente redactado por la organización donde se informe acerca del tratamiento, de sus derechos como persona afectada y donde se le solicite que conteste consintiendo expresamente que sus datos sean tratados por la organización.

- Si en la página web hay habilitado un apartado para el envío de CV, se debería configurar para que no se pueda enviar un CV si no se ha leído previamente la política de privacidad y se ha aceptado el tratamiento de los datos.

Medidas a implementar cuando hay personal contratado:

- Aunque con la firma del contrato la persona trabajadora está autorizando a la organización a tratar sus datos en

el ámbito laboral, si se van utilizar los datos para otras finalidades o se van a recoger y tratar otros datos para otras finalidades como, por ejemplo, usar su imagen en la página web de la entidad o para publicaciones en redes sociales, será necesario su consentimiento expreso e inequívoco.

- Se debe informar a las personas contratadas del tratamiento que se va a llevar a cabo con sus datos personales. Para ello, la organización puede redactar una Circular que todo el personal contratado debe recibir en el momento de su contratación, que contenga:
  - El nombre del Responsable del tratamiento. es el responsable y encargado del tratamiento,
  - Qué tipo de datos se van a tratar.
  - Si los datos se van a ceder a terceras personas.
  - El nombre de la persona Encargada del tratamiento (si la hubiera).
  - El plazo de conservación de los datos.
  - Los derechos de tienen en relación con la protección de datos y cómo pueden ejercerlos.

No es necesario que se firme la circular, sólo hay que garantizar que el personal la tenga a su disposición y pueda leerla.

- Las personas contratadas deben firmar un acuerdo de confidencialidad en el que se comprometan a no divulgar los datos personales a los que tengan acceso durante el desempeño de sus funciones, incluso cuando finalice la relación laboral.

Para facilitar la implantación de las medidas anteriores, se pueden aglutinar en un solo documento que firme cada persona contratada.

- Cuando finalice la relación laboral de una persona contratada se deben cambiar sus contraseñas de acceso a las aplicaciones y servicios que las requieran, así como eliminar su usuario para evitar que pueda acceder a la información con posterioridad.

- Cuando la organización dispone de **PÁGINA WEB:**

DESCRIPCIÓN DEL TRATAMIENTO	CATEGORÍAS DE FACTORES DE RIESGO	FACTORES DE RIESGO	EJEMPLOS DE RIESGOS ESPECÍFICOS	EJEMPLOS DE MEDIDAS MITIGADORAS
NATURALEZA	Recogida y generación de datos	Factores de riesgo derivados de recogida o generación de datos de forma específica	Riesgos asociados a la protección de los datos: - Que la confidencialidad de los datos esté comprometida - Que los datos recogidos no sean precisos, completos, consistentes y confiables Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando se recojan los datos mediante: - Falta de transparencia del momento preciso de la recogida de datos (cookies de la página, formularios, canal de denuncias, recepción de donaciones)	- Política de protección de datos o política de privacidad - Política de cookies - Aviso sobre las cookies - Política de privacidad del Canal de denuncias
	Factores técnicos del tratamiento	Factores de riesgo derivados de implementarse con determinadas características técnicas o tecnologías	Riesgos asociados a la protección de los datos: - Que la confidencialidad de los datos esté comprometida, que los datos no estén disponibles y/o que se pierda la integridad de los datos Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando se traten datos usando: - Uso de cookies propias o de terceros - Uso innovador o nuevas soluciones organizativas - Tratamientos automatizados	- Política de protección de datos o política de privacidad - Política de cookies - Aviso sobre las cookies - Política de privacidad del Canal de denuncias - Política de ciberseguridad - Política de uso de nuevas tecnologías
	Brechas de seguridad	Factores de riesgo que se derivan de la posible materialización de brechas de seguridad sobre los datos personales	Riesgos asociados a la protección de los datos: - Un incidente de seguridad puede afectar a la confidencialidad, integridad y disponibilidad de los datos personales Incidentes de seguridad que supongan una brecha de seguridad	- Procedimiento de gestión de brechas de seguridad - Política de ciberseguridad - Instalar medidas de seguridad - Formar al personal para que haga un uso apropiado de la información y de los medios

DESCRIPCIÓN DEL TRATAMIENTO	CATEGORÍAS DE FACTORES DE RIESGO	FACTORES DE RIESGO	EJEMPLOS DE RIESGOS ESPECÍFICOS	EJEMPLOS DE MEDIDAS MITIGADORAS
ÁMBITO / ALCANCE	Tipos de datos utilizados	Factores de riesgo derivados de los datos recogidos, procesados o inferidos en el tratamiento	Riesgos asociados a la protección de los datos: Los riesgos que afecten a la confidencialidad, disponibilidad e integridad de los datos serán más o menos elevados en función del tipo de datos tratados Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando los datos tratados sean: - Datos de medios de pago: números de tarjeta, números de cuenta bancaria - Datos de navegación web: registro de páginas visitadas (historial de navegación, logs de servidores web, etc.), registro del tiempo que se está en cada página, registro del momento de la visita a la página, registro del número de conexiones, etc.	- Política de protección de datos o política de privacidad - Política de cookies - Aviso sobre las cookies - Instalar medidas de seguridad - Política de privacidad del Canal de denuncias
	Extensión y alcance del tratamiento	Factores de riesgo relativos al número de personas afectadas, a la diversidad de los datos tratados, a la duración en el tiempo del tratamiento y de la conservación de los datos, el volumen de los datos, la extensión geográfica de los datos, la frecuencia de la recogida de los datos	Riesgos asociados a la protección de los datos: La confidencialidad de los datos puede comprometerse, la disponibilidad de los datos puede disminuir y la integridad puede verse afectada Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando el tratamiento: - Se recopilen excesivos datos con relación al fin del tratamiento	- Política de protección de datos o política de privacidad - Política de cookies - Aviso sobre las cookies - Instalar medidas de seguridad - No solicitar datos que no sean estrictamente necesarios para el tratamiento
	Comunicaciones de datos	Factores de riesgo derivadas de las comunicaciones de datos a terceros en el marco del tratamiento	Riesgos asociados a la protección de los datos: La confidencialidad de los datos puede comprometerse, que los datos no estén disponibles o la disponibilidad sea menor y que la integridad esté afectada Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando: - Cookies de terceros en la página web - Transferencias internacionales	- Política de protección de datos o política de privacidad - Política de cookies - Aviso sobre las cookies - Contrato con cada Encargado de tratamiento
	Efectos colaterales del tratamiento	Factores de riesgo que se derivan de consecuencias no contempladas en los propósitos originales previstos del tratamiento	- Puede provocar exclusión - Puede provocar discriminación - Posible usurpación de identidad - Posible daño reputacional - Posible perjuicio económico significativo - Posible perjuicio moral significativo - Posible pérdida de confidencialidad de datos - Podría impedir el ejercicio de un derecho	- Política de protección de datos o política de privacidad - Política de cookies - Aviso sobre las cookies - Contrato con cada Encargado de tratamiento - Análisis periódico de la necesidad y proporcionalidad del tratamiento - Registro de actividades de tratamiento - Realizar un análisis de riesgos

DESCRIPCIÓN DEL TRATAMIENTO	CATEGORÍAS DE FACTORES DE RIESGO	FACTORES DE RIESGO	EJEMPLOS DE RIESGOS ESPECÍFICOS	EJEMPLOS DE MEDIDAS MITIGADORAS
FINALIDAD	Operaciones relacionadas con los fines del tratamiento	Factores de riesgo que se derivan del fin declarado del tratamiento y otros fines vinculados al propósito principal	Riesgos asociados a la protección de los datos: - La confidencialidad de los datos puede comprometerse cuando los datos son usados para otros fines vinculados - Que los datos no estén disponibles o parte de ellos para los otros fines - Que se pierda la integridad de los datos Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando los fines del tratamiento sean: - Decisiones automatizadas sin intervención humana - Decidir sobre o impedir el ejercicio de derechos fundamentales: derechos de las personas que acceden a la página o interactúan, derechos de las personas informantes a través del Canal de denuncias - Decidir sobre el control de la persona interesada de sus datos personales - Decidir sobre el acceso a un servicio - Conservación de los datos	- Política de protección de datos o política de privacidad - Política de cookies - Aviso sobre las cookies - Contrato con cada Encargado de tratamiento - Análisis periódico de la necesidad y proporcionalidad del tratamiento - Registro de actividades de tratamiento - Realizar un análisis de riesgos

Tabla 23 Medidas mitigadoras de los riesgos derivados de la página web

A continuación, de los ejemplos de medidas de la tabla se van a explicar los que se considera pueden ser de más utilidad para una organización:

Medidas a implementar cuando se dispone de página web:

- **Política de privacidad:** Cuando la organización dispone de página web es obligatorio disponer de una Política de privacidad cuando se recojan datos personales, lo que prácticamente en todas, ya que se suelen alojar cookies que recogen direcciones de IP o tienen formularios de contacto. La política de privacidad es un documento que explica cómo se van a tratar los datos personales de las personas que acceden a la página web. El lenguaje debe ser sencillo, conciso y comprensible y ser transparente. La política de privacidad debe ser accesible, por lo que se debería crear en una página independiente y separada. La fórmula más utilizada es incluir un enlace a la política de privacidad en la página principal de la web que deberá visualizarse correctamente desde cualquier navegador y dispositivo. Debe contener, como mínimo, la siguiente información:
  - Identificación de la persona Responsable del tratamiento y sus datos de contacto.
  - Finalidad del tratamiento de los datos.
  - El plazo de conservación de los datos.
  - Base de legitimación para el tratamiento de los datos.
  - Indicar las personas destinatarias de los datos.
  - Los derechos de las personas interesadas y cómo ejercerlos.
  - El derecho de la persona interesada a retirar el consentimiento.
  - La posibilidad de reclamar ante la autoridad de control (AEPD).
  - Seguridad y confidencialidad de los datos, refiriéndose a las medidas implantadas para proteger los datos de las personas usuarias de la web.

- Identificación de la persona Delegada de protección de datos, si la hubiera.
- Transferencias internacionales de datos.

- **Política de cookies:** Es un documento que tiene que redactar y publicar en la web toda organización que tenga cookies en su página web, que informa a las personas usuarias de la web acerca las cookies, de su titular, finalidad, duración y utilidad. Las personas usuarias tienen que consentir o no la instalación de las cookies. El lenguaje de la política de cookies debe ser sencilla y clara. La política de cookies debe contener, al menos:
  - Información de que la página web utiliza cookies, tanto de las propias de la entidad como de las de terceros.
  - Explicación breve sobre qué son las cookies y los tipos de cookies que se pueden encontrar.
  - Explicación de cómo rechazar el uso de cookies.
  - Detalle de las cookies que se utilizan en la página web, tanto las propias como las de terceros. De cada cookie se debería indicar el nombre, a quién pertenece (proveedor), el tipo de cookie del que se trata, la finalidad que tiene y la duración.

- **Aviso de cookies (banner de cookies):** se trata de un aviso informativo acerca del uso de las cookies en la página web de la organización y que debe permitir a la persona interesada aceptar o rechazar las cookies de la página, además de tener un enlace a la política de cookies. Para que sea válida, debe cumplir con los siguientes requisitos:
  - Informar de que se utilizan cookies en la página web.
  - Contener un enlace a la política de cookies.
  - Contener un botón para aceptar cookies o configurar las cookies que se quiera aceptar o rechazar.

No se puede condicionar el uso o acceso a los servicios ofrecidos en la página web a la aceptación de las cookies.

Ilustración 17 Ejemplo de página web con aviso de cookies

- Cuando en la organización se usa **EQUIPAMIENTO INFORMÁTICO y CORREO ELECTRÓNICO:**

DESCRIPCIÓN DEL TRATAMIENTO	CATEGORÍAS DE FACTORES DE RIESGO	FACTORES DE RIESGO	EJEMPLOS DE RIESGOS ESPECÍFICOS	EJEMPLOS DE MEDIDAS MITIGADORAS
NATURALEZA	Recogida y generación de datos	Factores de riesgo derivados de recogida o generación de datos de forma específica	Riesgos asociados a la protección de los datos: - Que la confidencialidad de los datos esté comprometida - Que los datos recogidos no son precisos, completos, consistentes y confiables Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando se recojan los datos mediante: - Procedentes de dos o más tratamientos con finalidades diferentes - Falta de transparencia del momento preciso de la recogida de datos	- Política de protección de datos o política de privacidad - Informar a las personas interesadas sobre Responsable tratamiento, finalidad de tratamiento, licitud y/o interés legítimo, plazo de conservación, terceras personas destinatarias, etc. - Informar a las personas interesadas acerca de sus derechos y cómo pueden ejercerlos - Política de uso de dispositivos corporativos - Política de uso de dispositivos externos (o personales)
	Factores técnicos del tratamiento	Factores de riesgo derivados de implementarse con determinadas características técnicas o tecnologías	Riesgos asociados a la protección de los datos: Que la confidencialidad de los datos esté comprometida, que los datos no estén disponibles y que se pierda la integridad de los datos Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando se traten datos usando: - Internet de las cosas (IoT) - Inteligencia Artificial - Uso innovador o nuevas soluciones organizativas - Uso innovador de tecnologías consolidadas - Tratamientos automatizados	- Política de uso de dispositivos corporativos - Política de uso de dispositivos externos (o personales) - Política de ciberseguridad - Política de uso de nuevas tecnologías
	Brechas de seguridad	Factores de riesgo que se derivan de la posible materialización de brechas de seguridad sobre los datos personales	Riesgos asociados a la protección de los datos: - Un incidente de seguridad puede afectar a la confidencialidad, integridad y disponibi - lidad de los datos personales Incidentes de seguridad que supongan una brecha de seguridad, ya sea por un error o intencionados	- Procedimiento de gestión de brechas de seguridad - Política de ciberseguridad - Formar al personal para que haga un uso apropiado de la información y de los medios - Anonimizar o seudonimizar los datos - Bloqueo de los datos - Instalar medidas de seguridad en el servidor, equipos informáticos y correo electrónico - Aplicar contraseñas, accesos restringidos y usuarios - Cambio de contraseñas y usuarios cuando las personas finalicen la relación laboral - Procedimiento de copias de seguridad - Protocolo de eliminación de documentos digitales que contengan datos personales - Mensaje sobre protección de datos en el correo electrónico

DESCRIPCIÓN DEL TRATAMIENTO	CATEGORÍAS DE FACTORES DE RIESGO	FACTORES DE RIESGO	EJEMPLOS DE RIESGOS ESPECÍFICOS	EJEMPLOS DE MEDIDAS MITIGADORAS
ÁMBITO / ALCANCE	Tipos de datos utilizados	Factores de riesgo derivados de los datos recogidos, procesados o inferidos en el tratamiento	No aplica (los riesgos derivan de los datos no de la forma de tratarlos)	No aplica (los riesgos derivan de los datos no de la forma de tratarlos)
	Categorías de personas interesadas	Factores de riesgo relativos a la categoría de personas interesadas	No aplica (los riesgos derivan de las personas interesadas no de la forma de tratarlos)	No aplica (los riesgos derivan de las personas interesadas no de la forma de tratarlos)
	Extensión y alcance del tratamiento	Factores de riesgo relativos al número de personas afectadas, a la diversidad de los datos tratados, a la duración en el tiempo del tratamiento y de la conservación de los datos, el volumen de los datos, la extensión geográfica de los datos, la frecuencia de la recogida de los datos	No aplica (los riesgos derivan de la extensión y alcance del tratamiento no de la forma de tratarlos)	No aplica (los riesgos derivan de la extensión y alcance del tratamiento no de la forma de tratarlos)

DESCRIPCIÓN DEL TRATAMIENTO	CATEGORÍAS DE FACTORES DE RIESGO	FACTORES DE RIESGO	EJEMPLOS DE RIESGOS ESPECÍFICOS	EJEMPLOS DE MEDIDAS MITIGADORAS
CONTEXTO	Categoría de las personas Responsable / Encargada del tratamiento	Factores de riesgo derivados del sector de la entidad y el colectivo al que se dirigen sus actuaciones	No aplica (los riesgos derivan del Responsable y/o del Encargado del tratamiento no de la forma de tratarlos)	No aplica (los riesgos derivan del Responsable y/o del Encargado del tratamiento no de la forma de tratarlos)
	Comunicaciones de datos	Factores de riesgo derivadas de las comunicaciones de datos a terceros en el marco del tratamiento	Riesgos asociados a la protección de los datos: - La confidencialidad de los datos puede comprometerse - Que los datos no estén disponibles o la disponibilidad sea menor - Que la integridad esté afectada Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando: - Falta de trasparencia de medios usados en el tratamiento: redes sociales, Inteligencia Artificial	- Informar a las personas interesadas sobre la protección de datos - Informar a las personas interesadas acerca de sus derechos y cómo pueden ejercerlos - Política de comunicaciones de datos a terceros - Contrato con cada Encargado de tratamiento - Procedimiento de comunicación de datos - Procedimiento de transferencias internacionales - Mensaje sobre protección de datos en el correo electrónico
	Efectos colaterales del tratamiento	Factores de riesgo que se derivan de consecuencias no contempladas en los propósitos originales previstos del tratamiento	- Posible reversión no autorizada de la seudonimización - Puede provocar exclusión - Puede provocar discriminación - Posible usurpación de identidad - Posible daño reputacional - Posible perjuicio económico significativo - Posible perjuicio moral significativo - Posible pérdida de confidencialidad de datos - Podría impedir el ejercicio de un derecho	- Análisis periódico de la necesidad y proporcionalidad del tratamiento - Registro de actividades de tratamiento - Realizar un análisis de riesgos - Realizar Evaluación de Impacto de Protección de Datos - Política de ciberseguridad
FINALIDAD	Operaciones relacionadas con los fines del tratamiento	Factores de riesgo que se derivan del fin declarado del tratamiento y otros fines vinculados al propósito principal	Riesgos asociados a la protección de los datos: La confidencialidad de los datos puede comprometerse cuando los datos son usados para otros fines vinculados, que los datos no estén disponibles o parte de ellos para los otros fines y que se pierda la integridad de los datos Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando los fines del tratamiento sean: - Control de acceso a internet - Decisiones automatizadas sin intervención humana - Tratamiento automatizado para soporte a la toma de decisiones - Decidir sobre o impedir el ejercicio de derechos fundamentales - Decidir sobre el control de la persona interesada de sus datos personales - Decidir sobre el acceso a un servicio - Conservación de los datos	- Registro de Actividades de Tratamiento - Análisis periódico de las necesidades y proporcionalidades de los tratamientos - Bloqueo de los datos - Formar e informar al personal sobre protección de datos - Procedimiento de copias de seguridad - Protocolo de eliminación de documentos digitales que contengan datos personales

Tabla 24 Medidas mitigadoras de los riesgos derivados del uso de equipamiento informático y del correo electrónico

A continuación, de los ejemplos de medidas de la tabla se van a explicar los que se considera pueden ser de más utilidad para una organización:

Medidas a implementar cuando se usa equipamiento informático y correo electrónico:

- Se debe informar a todo el personal de la organización de los riesgos asociados a la ciberseguridad y de las medidas que ha implantado la entidad para protegerse y que deben cumplir, así como del procedimiento a seguir en caso de que se detecte una incidencia de seguridad.

- Proteger las contraseñas de acceso a los sistemas informáticos, así como a los ficheros protegidos que contengan datos personales. Las contraseñas se deben modificar de forma periódica, así como cuando una persona deja de formar parte de la organización.

- Cuando se envíe un correo electrónico a más de una persona destinataria ajena a la organización, se deberían colocar las direcciones en CCO (copia oculta) para evitar que se tenga acceso al resto de direcciones a las que se ha enviado el correo, así se preserva la confidencialidad de las personas destinatarias.

- Mensaje en el correo electrónico: el correo electrónico es el medio a través del cual se suele enviar información que contiene datos personales, e incluso el propio correo electrónico puede ser un dato personal. Por estos motivos, es necesario integrar un texto en la firma del correo electrónico con la siguiente información:

  - Cláusula de confidencialidad y deber de secreto sobre la información contenida en el correo.
  - Aviso acerca de cómo proceder en caso de que se envíe el correo a un destinatario erróneo.
  - Información sobre el tratamiento.
  - Enlace a la Política de privacidad.

La política de privacidad incluirá toda la información acerca de los tratamientos de datos de la organización, tal y como se ha explicado anteriormente al tratar las medidas mitigadoras de los riesgos asociados a la página web de la organización.
Esta forma de presentar la información, donde se enlaza a la política de privacidad, se denomina “información por capas”. Consiste en que en una primera capa informativa sobre el tratamiento de datos se informa de quién es la persona Responsable del tratamiento y se incluye un enlace a la política de privacidad, que será la segunda capa y en donde ya se proporcione toda la información detallada sobre el tratamiento de los datos personales.

***Ejemplo*:**

Este mensaje y sus adjuntos contienen información confidencial y reservada, dirigida exclusivamente a su destinatario. Si ha recibido este mensaje por error, se ruega lo notifique inmediatamente por esta misma vía y borre el mensaje de su sistema.

Le informamos que los datos que figuran en esta comunicación serán tratados por la PLATAFORMA DE ONG DE ACCIÓN SOCIAL con el fin de gestionar las comunicaciones y/o relación establecida entre usted (o la entidad que usted representa) y la PLATAFORMA DE ONG DE ACCIÓN SOCIAL. La base legal de este tratamiento es el mantenimiento de la relación contractual establecida, el interés legítimo en mantener el contacto profesional o bien el consentimiento otorgado. Usted puede obtener información adicional, consultando nuestra ***Política de Privacidad.***

- Cuando se recogen datos a través de **FORMULARIOS** para la inscripción en jornadas, eventos, formación:

DESCRIPCIÓN DEL TRATAMIENTO	CATEGORÍAS DE FACTORES DE RIESGO	FACTORES DE RIESGO	EJEMPLOS DE RIESGOS ESPECÍFICOS	EJEMPLOS DE MEDIDAS MITIGADORAS
NATURALEZA	Recogida y generación de datos	Factores de riesgo derivados de recogida o generación de datos de forma específica	Riesgos asociados a la protección de los datos: - Que la confidencialidad de los datos esté comprometida - Que los datos recogidos no son precisos, completos, consistentes y confiables Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando se recojan los datos mediante: - Falta de transparencia del momento preciso de la recogida de datos	- Informar a las personas interesadas sobre Responsable tratamiento, finalidad de tratamiento, licitud y/o interés legítimo, plazo de conservación, terceras personas destinatarias, etc. - Informar a las personas interesadas acerca de sus derechos y cómo pueden ejercerlos - Obtener el consentimiento expreso para el tratamiento de los datos
	Factores técnicos del tratamiento	Factores de riesgo derivados de implementarse con determinadas características técnicas o tecnologías	Riesgos asociados a la protección de los datos: - Que la confidencialidad de los datos esté comprometida, que los datos no estén disponibles y que se pierda la integridad de los datos Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando se traten datos usando: - Uso innovador o nuevas soluciones organizativas - Uso innovador de tecnologías consolidadas - Tratamientos automatizados	- Política de uso de nuevas tecnologías
	Brechas de seguridad	Factores de riesgo que se derivan de la posible materialización de brechas de seguridad sobre los datos personales	Riesgos asociados a la protección de los datos: - Un incidente de seguridad puede afectar a la confidencialidad, integridad y disponibilidad de los datos personales. Incidentes de seguridad que supongan una brecha de seguridad	- Procedimiento de gestión de brechas de seguridad - Política de ciberseguridad - Formar al personal para que haga un uso apropiado de la información y de los medios - Anonimizar o seudonimizar los datos - Bloqueo de los datos - Instalar medidas de seguridad en el servidor, equipos informáticos y correo electrónico - Aplicar contraseñas, accesos restringidos y usuarios

DESCRIPCIÓN DEL TRATAMIENTO	CATEGORÍAS DE FACTORES DE RIESGO	FACTORES DE RIESGO	EJEMPLOS DE RIESGOS ESPECÍFICOS	EJEMPLOS DE MEDIDAS MITIGADORAS
ÁMBITO / ALCANCE	Tipos de datos utilizados	Factores de riesgo derivados de los datos recogidos, procesados o inferidos en el tratamiento	No aplica (los riesgos derivan de los datos no de la forma de tratarlos)	No aplica (los riesgos derivan de los datos no de la forma de tratarlos)
	Categorías de personas interesadas	Factores de riesgo relativos a la categoría de personas interesadas	No aplica (los riesgos derivan de las personas interesadas no de la forma de tratarlos)	No aplica (los riesgos derivan de las personas interesadas no de la forma de tratarlos)
	Extensión y alcance del tratamiento	Factores de riesgo relativos al número de personas afectadas, a la diversidad de los datos tratados, a la duración en el tiempo del tratamiento y de la conservación de los datos, el volumen de los datos, la extensión geográfica de los datos, la frecuencia de la recogida de los datos, etc.	No aplica (los riesgos derivan de la extensión y alcance del tratamiento no de la forma de tratarlos)	No aplica (los riesgos derivan de la extensión y alcance del tratamiento no de la forma de tratarlos)

DESCRIPCIÓN DEL TRATAMIENTO	CATEGORÍAS DE FACTORES DE RIESGO	FACTORES DE RIESGO	EJEMPLOS DE RIESGOS ESPECÍFICOS	EJEMPLOS DE MEDIDAS MITIGADORAS
CONTEXTO	Categoría de las personas Responsable / Encargada del tratamiento	Factores de riesgo derivados del sector de la entidad y el colectivo al que se dirigen sus actuaciones	No aplica (los riesgos derivan del Responsable y/o del Encargado del tratamiento no de la forma de tratarlos)	No aplica (los riesgos derivan del Responsable y/o del Encargado del tratamiento no de la forma de tratarlos)
	Comunicaciones de datos	Factores de riesgo derivadas de las comunicaciones de datos a terceros en el marco del tratamiento	Riesgos asociados a la protección de los datos: La confidencialidad de los datos puede comprometerse, que los datos no estén disponibles o la disponibilidad sea menor y que la integridad esté afectada Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando: Falta de trasparencia de medios usados en el tratamiento	- Política de comunicaciones de datos a terceros - Contrato con cada Encargado de tratamiento - Procedimiento de comunicación de datos
	Efectos colaterales del tratamiento	Factores de riesgo que se derivan de consecuencias no contempladas en los propósitos originales previstos del tratamiento	- Excede las expectativas de las personas interesadas - Posible reversión no autorizada de la seudonimización - Posible pérdida de control de los datos tratados por la persona Encargada del tratamiento - Puede provocar exclusión - Puede provocar discriminación - Posible usurpación de identidad - Posible daño reputacional - Posible perjuicio económico significativo - Posible perjuicio moral significativo - Posible pérdida de confidencialidad de datos - Podría impedir el ejercicio de un derecho	- Contrato con cada Encargado del tratamiento - Análisis periódico de la necesidad y proporcionalidad del tratamiento - Registro de actividades de tratamiento - Realizar un análisis de riesgos - Realizar Evaluación de Impacto de Protección de Datos

DESCRIPCIÓN DEL TRATAMIENTO	CATEGORÍAS DE FACTORES DE RIESGO	FACTORES DE RIESGO	EJEMPLOS DE RIESGOS ESPECÍFICOS	EJEMPLOS DE MEDIDAS MITIGADORAS
FINALIDAD	Operaciones relacionadas con los fines del tratamiento	Factores de riesgo que se derivan del fin declarado del tratamiento y otros fines vinculados al propósito principal	Riesgos asociados a la protección de los datos: - La confidencialidad de los datos puede comprometerse cuando los datos son usados para otros fines vinculados - Que los datos no estén disponibles o parte de ellos para los otros fines - Que se pierda la integridad de los datos Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando los fines del tratamiento sean: - Videovigilancia - Decisiones automatizadas sin intervención humana - Tratamiento automatizado para soporte a la toma de decisiones - Decidir sobre o impedir el ejercicio de derechos fundamentales: derechos de igualdad, no discriminación, intimidad personal y familiar, etc. - Decidir sobre el control del interesado de sus datos personales: derecho de acceso, rectificación, oposición, supresión, limitación del tratamiento, etc. - Uso de imágenes para difusión actividades - Decidir sobre el acceso a un servicio - Conservación de los datos	- Registro de Actividades de Tratamiento - Análisis periódico de las necesidades y proporcionalidades de los tratamientos - Bloqueo de los datos - Formar e informar al personal sobre protección de datos - Protocolo de eliminación de documentos digitales que contengan datos personales

Tabla 25 Medidas mitigadoras de los riesgos derivados del uso de formularios

A continuación, de los ejemplos de medidas de la tabla se van a explicar los que se considera pueden ser de más utilidad para una organización:

Medidas a implementar cuando se usan formularios:

- Recoger sólo los datos que sean estrictamente necesarios para la finalidad.

- Cláusula en el formulario: en el formulario se van a recoger los datos necesarios para asistir a una jornada, evento o para participar en una formación. Como se recogen datos personales es necesario que las personas afectadas den el consentimiento expreso con anterioridad al tratamiento de los datos, de tal manera que la aceptación sea un requisito imprescindible para poder completar y enviar el formulario. La cláusula que incluye el consentimiento debe contener la siguiente información:

- Información sobre la persona Responsable del tratamiento.
- Finalidad del tratamiento.
- Derechos de las personas interesadas y cómo ejercerlos.
- Enlace a la Política de privacidad.

La política de privacidad incluirá toda la información acerca de los tratamientos de datos de la organización, tal y como se ha explicado anteriormente al tratar las medidas mitigadoras de los riesgos asociados a la página web de la organización.

Ejemplo:

Concedo el consentimiento para el tratamiento de mis datos de acuerdo a:

La PLATAFORMA DE ONG DE ACCIÓN SOCIAL, como Responsable del tratamiento, le informa que sus datos son recabados con la finalidad de: Recoger los datos de carácter personal para la organización y gestión de la jornada Presentación de la Guía de protección de datos para organizaciones de Acción Social. La base jurídica para el tratamiento es la base legal para el tratamiento de sus datos es el consentimiento del interesado al contactar con nuestra organización. Sus datos no se cederán a terceros salvo obligación legal. Cualquier persona tiene derecho a solicitar el acceso, rectificación, supresión, limitación del tratamiento, oposición o derecho a la portabilidad de sus datos personales, enviando un correo electrónico a pd@plataformaong.org, indicando el derecho que desea ejercer. Puede obtener información adicional consultando nuestra Política de Privacidad.

- Si se pretende tratar los datos para otras finalidades diferentes como puede ser el envío del boletín de la organización o se van a obtener otro tipo de datos como fotografías o vídeos de las personas afectadas, será necesario obtener un consentimiento expreso adicional.

- En caso de **CONTRATACIÓN DE SERVICIOS A TERCERAS PERSONAS EXTERNAS:**

Ver tabla en la página siguiente

DESCRIPCIÓN DEL TRATAMIENTO	CATEGORÍAS DE FACTORES DE RIESGO	FACTORES DE RIESGO	EJEMPLOS DE RIESGOS ESPECÍFICOS	EJEMPLOS DE MEDIDAS MITIGADORAS
NATURALEZA	Recogida y generación de datos	Factores de riesgo derivados de recogida o generación de datos de forma específica	Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando se recojan los datos mediante: - Falta de transparencia del momento preciso de la recogida de datos (no se informe de la persona Encargada del tratamiento)	- Política de protección de datos o política de privacidad - Política de cookies y aviso de cookies en la página web - Informar a las personas interesadas sobre Encargado del tratamiento, terceras personas destinatarias, etc. - Informar a las personas interesadas acerca de sus derechos y cómo pueden ejercerlos
	Factores técnicos del tratamiento	Factores de riesgo derivados de implementarse con determinadas características técnicas o tecnologías	Riesgos asociados a la protección de los datos: - Que la confidencialidad de los datos esté comprometida - Que los datos no estén disponibles - Que se pierda la integridad de los datos Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando se traten datos usando: - Aplicaciones móviles - Internet de las cosas (IoT) - Inteligencia Artificial - Uso innovador o nuevas soluciones organizativas - Uso innovador de tecnologías consolidadas - Tratamientos automatizados - Videovigilancia	- Política de protección de datos o política de privacidad - Política de cookies y aviso de cookies en la página web Contrato con cada persona Encargada del tratamiento
	Brechas de seguridad	Factores de riesgo que se derivan de la posible materialización de brechas de seguridad sobre los datos personales	Riesgos asociados a la protección de los datos: - Un incidente de seguridad en el Encargado puede afectar a la confidencialidad, integridad y disponibilidad de los datos personales Incidentes de seguridad en el Encargado del tratamiento que supongan una brecha de seguridad	- Procedimiento de gestión de brechas de seguridad - Asegurase de que Encargado del tratamiento avise a la organización en cuanto detecte un incidente de seguridad - Asegurarse de contratar los servicios de Encargados del tratamiento que tengan medidas técnicas y organizativas para garantizar la protección de datos - Contrato con cada persona Encargada del tratamiento

DESCRIPCIÓN DEL TRATAMIENTO	CATEGORÍAS DE FACTORES DE RIESGO	FACTORES DE RIESGO	EJEMPLOS DE RIESGOS ESPECÍFICOS	EJEMPLOS DE MEDIDAS MITIGADORAS
ÁMBITO / ALCANCE	Tipos de datos utilizados	Factores de riesgo derivados de los datos recogidos, procesados o inferidos en el tratamiento	No aplica (los riesgos derivan de que exista un Encargado no de la forma de tratarlos)	No aplica (los riesgos derivan de que exista un Encargado no de la forma de tratarlos)
	Categorías de personas interesadas	Factores de riesgo relativos a la categoría de personas interesadas	No aplica (los riesgos derivan de que exista un Encargado no de la forma de tratarlos)	No aplica (los riesgos derivan de que exista un Encargado no de la forma de tratarlos)
	Extensión y alcance del tratamiento	Factores de riesgo relativos al número de personas afectadas, a la diversidad de los datos tratados, a la duración en el tiempo del tratamiento y de la conservación de los datos, el volumen de los datos, la extensión geográfica de los datos, la frecuencia de la recogida de los datos, etc.	No aplica (los riesgos derivan de que exista un Encargado no de la forma de tratarlos)	No aplica (los riesgos derivan de que exista un Encargado no de la forma de tratarlos)
CONTEXTO	Categoría de las personas Responsable / Encargada del tratamiento	Factores de riesgo derivados del sector de la entidad y el colectivo al que se dirigen sus actuaciones	El riesgo puede ser mayor dependiendo de la actividad de la persona Encargada del tratamiento	- Asegurarse de contratar los servicios de Encargados del tratamiento que tengan medidas técnicas y organizativas para garantizar la protección de datos - Contrato con cada persona Encargada del tratamiento
	Comunicaciones de datos	Factores de riesgo derivadas de las comunicaciones de datos a terceros en el marco del tratamiento	Riesgos asociados a la protección de los datos: - La confidencialidad de los datos puede comprometerse - Que los datos no estén disponibles o la disponibilidad sea menor - Que la integridad esté afectada Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando: - Que se cedan los datos a otras terceras personas sin el consentimiento de la organización	- Contrato con cada persona Encargada del tratamiento
	Efectos colaterales del tratamiento	Factores de riesgo que se derivan de consecuencias no contempladas en los propósitos originales previstos del tratamiento	- Excede las expectativas de las personas interesadas - Posible reversión no autorizada de la seudonimización - Posible pérdida de control de los datos tratados por la persona Encargada del tratamiento - Puede provocar exclusión - Puede provocar discriminación - Posible usurpación de identidad - Posible daño reputacional - Posible perjuicio económico significativo - Posible perjuicio moral significativo - Posible pérdida de confidencialidad de datos - Podría impedir el ejercicio de un derecho	- Asegurarse de contratar los servicios de Encargados del tratamiento que tengan medidas técnicas y organizativas para garantizar la protección de datos - Contrato con cada persona Encargada del tratamiento

DESCRIPCIÓN DEL TRATAMIENTO	CATEGORÍAS DE FACTORES DE RIESGO	FACTORES DE RIESGO	EJEMPLOS DE RIESGOS ESPECÍFICOS	EJEMPLOS DE MEDIDAS MITIGADORAS
FINALIDAD	Operaciones relacionadas con los fines del tratamiento	Factores de riesgo que se derivan del fin declarado del tratamiento y otros fines vinculados al propósito principal	Riesgos asociados a la protección de los datos: La confidencialidad de los datos puede comprometerse cuando los datos son usados para otros fines vinculados, que los datos no estén disponibles o parte de ellos para los otros fines y que se pierda la integridad de los datos Riesgo de que las libertades y derechos de las personas afectadas y los principios de protección de datos se vean afectados cuando la persona Encargada pueda usar los datos para otros fines.	- Asegurarse de contratar los servicios de Encargados del tratamiento que tengan medidas técnicas y organizativas para garantizar la protección de datos - Contrato con cada persona Encargada del tratamiento

Tabla 26 Medidas mitigadoras de los riesgos derivados de la subcontratación de servicios a terceras personas

El rol de la persona Encargada del tratamiento y las medidas a implementar se describieron en el apartado 4.2.2. Encargado del tratamiento, por lo que remitimos a lo mencionado en dicho apartado.

Estas serían las medidas básicas, pero cada organización debe analizar los tratamientos y establecer medidas para prevenir incumplimientos con el objetivo de proteger los derechos de las personas interesadas y los principios de protección de datos.

Cada organización debe analizar los tratamientos y establecer medidas para prevenir incumplimientos con el objetivo de proteger los derechos de las personas interesadas y los principios de protección de datos.

05

BIBLIOGRAFÍA

- Plataforma de ONG de Acción Social (2020). **Manual de elaboración de Planes de Cumplimiento normativo para entidades del Tercer Sector de Acción Social.**
- Plataforma de ONG de Acción Social (2021). **Manual para la implementación de los elementos básicos del Cumplimiento normativo para entidades del Tercer Sector de Acción Social.**
- Plataforma de ONG de Acción Social (2022). **Guía básica de Transparencia para entidades de Acción Social**
- Plataforma de ONG de Acción Social (2022). **Guía básica de Buen Gobierno para entidades de Acción Social**
- **Carta de los Derechos Fundamentales de la Unión Europea.**
- **Tratado de Funcionamiento de la Unión Europea.**
- **Reglamento UE 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD)**
- **Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos personales (LORTAD).**
- **Ley Orgánica 15/1999, de 5 de diciembre, de protección de datos personales (LOPD)**
- **Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RLOPD).**
- **Agencia Española de Protección de Datos. Anonimización y seudonimización (6 de octubre de 2021).**
- **Transposición del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD)**
- **Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos Digitales (LOPDGDD)**

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

Plataforma de ONG
de Acción Social

PLATAFORMA DE ONG
DE ACCIÓN SOCIAL

Tribulete 18, 1ª Planta.
28012 Madrid
915 351 026

Info@plataforma.org

GOBIERNO DE ESPAÑA
MINISTERIO DE DERECHOS SOCIALES, CONSUMO Y AGENDA 2030
POR SOLIDARIDAD
OTROS FINES DE INTERÉS SOCIAL