Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (interuniversitario: UOC, UAB, URV, UIB)

Evaluación de Impacto relativa a la Protección de Datos

Nombre del estudiante: Eladio Cortizas de Castro

Nombre del Profesor/a colaborador/a: Antonio José Segovia Henares

Nombre del Profesor/a: Carles Garrigues Olivella

Fecha: 5 de junio de 2019

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-SinObraDerivada 3.0 España de Creative Commons

Resumen del trabajo:

Estudio y diseño de una metodología de Evaluaciones de Impacto relativas a la Protección de Datos (EIPD), incluyendo la gestión del riesgo derivada, así como su revisión. Todo ello orientado en los tratamientos de datos personales para su uso en pymes españolas.

Abstract (in English):

Study and design of a methodology of Privacy Impact assessment (PIA), including the management of the derived risk, as well as its revision. All this oriented in the processing of personal data for use in Spanish SMEs.

Índice

1. Introducción. 13
2. Justificación del TFM. 13
3. Alcance. 13
4. Objetivos. 15
   4.1. Objetivo general. 15
   4.2. Objetivos específicos. 15
5. Planificación del Trabajo. 15
6. Introducción a la normativa en materia de protección de datos. 15
   6.1. Tipos de datos personales. 16
      6.1.1. Clasificación de los datos. 17
   6.2. RGPD Introducción. 17
      6.2.1. Principios. 17
         6.2.1.1. Principio de responsabilidad proactiva (accountability). 17
         6.2.1.2. Principio de protección de datos por defecto y desde el diseño. 17
         6.2.1.3. Principio de licitud, lealtad y transparencia. 17
         6.2.1.4. Principio de limitación de la finalidad. 17
         6.2.1.5. Principio de minimización de los datos. 17
         6.2.1.6. Principio de exactitud de los datos. 17
         6.2.1.7. Principio de limitación del plazo de conservación de los datos. 17
         6.2.1.8. Principio de integridad y confidencialidad. 18
      6.2.2. Obligaciones. 18
         6.2.2.1. Delegado de Protección de Datos. 18
         6.2.2.2. Evaluación de Impacto relativa a la Protección de Datos. 19
         6.2.2.3. Ventanilla única. 19
         6.2.2.4. Brechas de seguridad. 19
         6.2.2.5. Datos de categoría especial. 19
         6.2.2.6. Encargado del tratamiento. 19
         6.2.2.7. Transferencias internacionales de datos. 19
         6.2.2.8. Códigos de conducta y certificaciones. 20
         6.2.2.9. Sanciones. 20
      6.2.3. Derechos. 20
         6.2.3.1. Supresión. 20
         6.2.3.2. Oposición y decisiones individuales automatizadas. 20
         6.2.3.3. Portabilidad. 20
         6.2.3.4. Limitación. 20

6.2.3.5. Acceso. 20
6.2.3.6. Rectificación. 20
6.3. LOPDGDD Introducción. 22
6.3.1. Legitimación de las administraciones públicas para el uso y cesión de los datos personales. 22
6.3.2. Delegado de Protección de Datos. 22
6.3.3. Redes sociales. 23
6.3.4. Protección de Datos personas fallecidas. 23
6.3.5. Régimen jurídico de los empleados. 23
6.3.6. Esquema nacional de seguridad. 23
6.3.7. Datos para perfilación por parte de partidos políticos. 24
7. Metodología de Evaluación de Impacto relativa a la Protección de Datos. 25
7.1. Introducción a las EIPD 25
7.2. Evaluación de impacto vs Análisis de riesgos. 26
7.3. Propuesta de metodología de Evaluación de Impacto relativa a la Protección de Datos. 27
7.3.1. Procedimiento de metodología de Evaluación de Impacto relativa a la Protección de Datos 29
7.3.2. Identificación de tratamiento. 30
7.3.2.1. Tratamientos ya iniciados antes del 25 de mayo de 2018. 30
7.3.3. Descripción del tratamiento. 30
7.3.4. Análisis de la necesidad de la EIPD, evaluación objetiva. 31
7.3.4.1. Comprobar si es obligatoria según RGPD. 31
7.3.4.2. Comprobar criterios de “alto riesgo” proporcionados por el CEPD. 31
7.3.4.3. Comprobar criterios de “mayor riesgo” que constan en la LOPDGDD. 32
7.3.4.4. Comprobar si está en el listado de tratamientos identificados por la Agencia Española de Protección de datos. 32
7.3.4.5. Comprobar si está en el listado de tratamientos identificados por las autoridades de control de protección de datos europeas. 32
7.3.5. Descripción sistemática del tratamiento. 33
7.3.5.1. Ciclo de vida de los datos. 33
7.3.6. Analizar la necesidad y proporcionalidad del tratamiento 36
7.3.7. Legitimación del tratamiento. 36
7.3.8. Análisis de Riesgos de los derechos y libertades fundamentales de las personas físicas. 38
7.3.8.1. Introducción 38
7.3.8.2. Tipos de metodologías de análisis de riesgos 38
7.3.8.2.1. Metodología basada en activos. 38
7.3.8.2.2. Metodología basada en riesgos 39
7.3.8.3. Propuesta metodología de Análisis de Riesgos de los derechos y libertades fundamentales de las personas físicas. 40
7.3.8.3.1. Procedimiento. 40

7.3.8.3.2. Identificación de Riesgos. 41
7.3.8.3.3. Valoración de Riesgos 41
7.3.8.3.4. Evaluación de Riesgos 41
7.3.8.3.5. Tratamiento de Riesgos. Plan de acción de mitigación de riesgos. 42
7.3.8.3.6. Riesgo Residual. Aceptación del riesgo. 44
7.3.9. Informe EIPD. 45
7.3.10. Revisión EIPD. 46
7.3.10.1. Requisitos. Alcance 46
7.3.10.2. Generación de la auditoría 46
7.3.10.3. Generación del informe de auditoría 46
7.3.10.4. Seguimiento de la auditoría 46
8. Caso práctico. 47
8.1. Tratamiento recursos humanos. 47
8.1.1. Identificación de tratamiento. 47
8.1.2. Descripción del tratamiento 47
8.1.3. Análisis de la necesidad de la EIPD, evaluación objetiva 47
8.1.4. Ciclo de vida de los datos. 48
8.1.5. Analizar la necesidad y proporcionalidad del tratamiento. 49
8.1.5.1. Necesidad del tratamiento. 49
8.1.5.2. Proporcionalidad del tratamiento. 49
8.1.6. Legitimación del tratamiento. 49
8.1.7. Análisis de Riesgos de los derechos y libertades fundamentales de las personas físicas. 49
8.1.7.1. Identificación de Riesgos. 49
8.1.7.2. Valoración de Riesgos 50
8.1.7.3. Evaluación de Riesgos 51
8.1.7.4. Tratamiento de Riesgos 51
8.1.7.5. Riesgo Residual. Aceptación del riesgo 52
8.1.8. Informe EIPD 52
8.1.9. Revisión EIPD. 52
8.1.9.1. Requisitos. Alcance 52
8.1.9.2. Generación de la auditoría 53
8.1.9.3. Generación del informe de auditoría 53
8.1.9.4. Seguimiento de la auditoría. 53
8.2. Tratamiento gestión de pacientes. 54
8.2.1. Identificación de tratamiento. 54
8.2.2. Descripción del tratamiento 54
8.2.3. Análisis de la necesidad de la EIPD, evaluación objetiva 54
8.2.4. Ciclo de vida de los datos. 55

8.2.5. Analizar la necesidad y proporcionalidad del tratamiento. 56
8.2.5.1. Necesidad del tratamiento. 56
8.2.5.2. Proporcionalidad del tratamiento. 56
8.2.6. Legitimación del tratamiento. 56
8.2.7. Análisis de Riesgos de los derechos y libertades fundamentales de las personas físicas.57
8.2.7.1. Identificación de Riesgos. 57
8.2.7.2. Valoración de Riesgos. 57
8.2.7.3. Evaluación de Riesgos 58
8.2.7.4. Tratamiento de Riesgos. 59
8.2.7.5. Riesgo Residual. Aceptación del riesgo 59
8.2.8. Informe EIPD 59
8.2.9. Revisión EIPD. 60
8.2.9.1. Requisitos. Alcance 60
8.2.9.1. Generación de la auditoría 60
8.2.9.2. Generación del informe de auditoría 60
8.2.9.3. Seguimiento de la auditoría. 61
8.3. Tratamiento formación 62
8.3.1. Identificación de tratamiento. 62
8.3.2. Descripción del tratamiento 62
8.3.3. Análisis de la necesidad de la EIPD, evaluación objetiva 62
8.3.4. Ciclo de vida de los datos. 63
8.3.5. Analizar la necesidad y proporcionalidad del tratamiento. 63
8.3.5.1. Necesidad del tratamiento. 63
8.3.5.2. Proporcionalidad del tratamiento. 63
8.3.6. Legitimación del tratamiento. 63
8.3.7. Análisis de Riesgos de los derechos y libertades fundamentales de las personas físicas.64
8.3.7.1. Identificación de Riesgos. 64
8.3.7.2. Valoración de Riesgos. 64
8.3.7.3. Evaluación de Riesgos 65
8.3.7.4. Tratamiento de Riesgos. 66
8.3.7.5. Riesgo Residual. Aceptación del riesgo 66
8.3.8. Informe EIPD 66
8.3.9. Revisión EIPD. 66
8.3.9.1. Requisitos. Alcance 67
8.3.9.1. Generación de la auditoría 67
8.3.9.2. Generación del informe de auditoría 67
8.3.9.3. Seguimiento de la auditoría. 68
9. Conclusiones 69

10. Términos y definiciones 70
10.1. Definiciones recogidas en el Reglamento general de protección de datos. 70
10.2. Otras definiciones. 72
10.3. Acrónimos. 72
11. Bibliografía y referencias. 74
12. Anexos. 75
12.1. Anexo 1: Listado de datos personales. 75
12.1.1. Datos personales. 75
12.1.1.1. Datos de carácter identificativo. 75
12.1.1.2. Características Personales. 75
12.1.1.3. Circunstancias sociales. 76
12.1.1.4. Académicos y profesionales. 76
12.1.1.5. Detalles de Empleo. 76
12.1.1.6. Información comercial. 76
12.1.1.7. Económicos, financieros y de seguros. 76
12.1.1.8. Transacciones de bienes y servicios. 77
12.1.1.9. Datos de control de presencia. 77
12.1.1.10. Datos relativos a comportamiento o personalidad. 77
12.1.1.11. Otros Datos. 77
12.1.2. Datos personales de categoría especial. 77
12.1.3. Datos personales de condenas e infracciones penales. 77
12.2. Anexo 2: Listado de tratamientos de ejemplo. 78
12.3. Anexo 3: Listado de Operaciones de tratamiento de ejemplo. 80
12.4. Anexo 4: Listado de riesgos. 81
12.5. Anexo 5: Método para identificar nuevos riesgos. 84
12.6. Anexo 6: Valoración de riesgos. 95
12.6.1. Criterios de aplicabilidad de riesgos. 95
12.6.2. Criterios de probabilidad de riesgos. 95
12.6.3. Criterios de Gravedad de riesgos 95
12.7. Anexo 7: Listado de finalidades. 97
12.8. Anexo 8: Tratamientos identificados por las autoridades de control de protección de datos (ACPD) europeas que necesitan EIPD. 99
12.9. Anexo 9: Medidas de mitigación de riesgos. 100
12.9.1. Medidas generales. 100
12.9.2. Medidas específicas de un grupo de riesgos. 100
12.10. Anexo 10: Eficacia niveles de madurez. 103
12.11. Anexo 11: Lista orientativa de tipos de tratamiento que requieren una evaluación de impacto relativa a la protección de datos según artículo 35.4 RGPD, según la AEPD. 104
12.12. Anexo 12 Cuestionario de revisión de EIPD 106

Índice de Figuras

Figura 1: AA RR como parte de EIPD. 26

Figura 2: Proceso EIPD según AEPD Guía práctica para las Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD 27

Figura 3: Proceso EIPD según L'Autoritat Catalana de Protecció de Dades. Guía sobre la evaluación de impacto relativa a la protección de datos en el RGPD. 28

Figura 4: Proceso EIPD según 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. Propuestas por CEPD 29

Figura 5: Proceso EIPD propuesto en este TFM 29

Figura 6: Anexo D ISO/IEC 29134. 33

Figura 7: Proceso AA RR. 40

Figura 8: Informe EIPD. 45

Índice de tablas

Tabla 1: Ciclo de vida de los datos. 34
Tabla 2: Ciclo de vida de los datos. 35
Tabla 3: Ejemplo de matriz de riesgos. 41
Tabla 4: Mapa de calor de riesgos. 42
Tabla 5: Ejemplo de matriz de riesgos con nivel de riesgo muy alto. 42
Tabla 6: Ciclo de vida de los datos. Caso práctico tratamiento recursos humanos. 48
Tabla 7: Ciclo de vida de los datos. Caso práctico tratamiento recursos humanos. 49
Tabla 8: Valoración de riesgos. Caso práctico tratamiento recursos humanos. 51
Tabla 9: Mapa de calor riesgo inherente. Caso práctico tratamiento recursos humanos. 51
Tabla 10: Mapa de calor riesgo residual. Caso práctico tratamiento recursos humanos. 52
Tabla 11: Cuestionario de revisión EIPD. Caso práctico tratamiento recursos humanos. 52
Tabla 12: Aplicabilidad. Caso práctico tratamiento recursos humanos. 53
Tabla 13: No conformidades subsanables. Caso práctico tratamiento recursos humanos. 53
Tabla 14: Ciclo de vida de los datos. Caso práctico tratamiento gestión de pacientes. 56
Tabla 15: Ciclo de vida de los datos. Caso práctico tratamiento gestión de pacientes. 56
Tabla 16: Valoración de riesgos. Caso práctico tratamiento gestión de pacientes. 58
Tabla 17: Mapa de calor riesgo inherente. Caso práctico tratamiento gestión de pacientes. 59
Tabla 18: Mapa de calor riesgo residual. Caso práctico tratamiento gestión de pacientes. 59
Tabla 19: Cuestionario de revisión EIPD. Caso práctico tratamiento gestión de pacientes. 60
Tabla 20: Aplicabilidad. Caso práctico tratamiento gestión de pacientes. 60
Tabla 21: No conformidades subsanables. Caso práctico tratamiento gestión de pacientes. 61
Tabla 22: Ciclo de vida de los datos. Caso práctico tratamiento formación. 63
Tabla 23: Ciclo de vida de los datos. Caso práctico tratamiento formación. 63
Tabla 24: Valoración de riesgos. Caso práctico tratamiento formación. 65
Tabla 25: Mapa de calor riesgo inherente. Caso práctico tratamiento formación. 66
Tabla 26: Mapa de calor riesgo residual. Caso práctico tratamiento formación. 66
Tabla 27: Cuestionario de revisión EIPD. Caso práctico tratamiento formación. 66
Tabla 28: Aplicabilidad. Caso práctico tratamiento formación. 67
Tabla 29: No conformidades subsanables. Caso práctico tratamiento formación. 67
Tabla 30: Listado de tratamientos de ejemplo. 79
Tabla 31: Listado de operaciones de tratamiento de ejemplo. 80
Tabla 32: Listado de riesgos. 83
Tabla 33: Listado de artículos del RGPD susceptibles de obtener riesgos derivados. 94
Tabla 34: Criterios de probabilidad de riesgos. 95
Tabla 35: Criterios de gravedad de riesgos de riesgos. Genérica y física. 95

Tabla 36: Criterios de gravedad de riesgos de riesgos. Material y moral. 96

Tabla 37: Tratamientos identificados por las autoridades de control de protección de datos (ACPD) europeas que necesitan EIPD. 99

Tabla 38: Medidas de mitigación de riesgos generales. 100

Tabla 39: Medidas de mitigación de riesgos grupos de riesgos. 102

Tabla 40: Eficacia niveles de madurez. 103

Tabla 41: Cuestionario de revisión de EIPD. 106

1. Introducción.

Tras la entrada en vigor del Reglamento Europeo de Protección de Datos (UE 2016/679) (RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), el ambiente de novedad regulatoria ha introducido cambios tan importantes como en Accountability o responsabilidad proactiva, lo cual se traduce en la exigencia de una mayor implicación por parte de los responsables. Entre otras muchas medidas se encuentra la realización de Evaluaciones de Impacto relativas a la Protección de Datos (EIPD).

El presente Trabajo de Fin de Máster plantea el estudio de la definición de una metodología de Evaluaciones de Impacto relativas a la Protección de Datos (EIPD).

2. Justificación del TFM.

Actualmente estamos en una etapa de novedades legales en el ámbito de la protección de datos, donde surgen nuevas obligaciones en la materia. Entre ellas las Evaluaciones de Impacto relativas a la Protección de Datos. Estas buscan garantizar los derechos y libertades de las personas.

Vemos la necesidad, para los responsables de privacidad en general, de ampliar conocimientos sobre las Evaluaciones de Impacto relativas a la Protección de Datos. Consideramos que hay poca información disponible al ser un campo nuevo en la legislación española.

3. Alcance.

La finalidad de este TFM es proporcionar a las empresas y organizaciones un método práctico, útil, fiable y robusto con el cual poder llevar a cabo las Evaluaciones de Impacto relativas a la Protección de Datos necesarias y que les permita ser conscientes del nivel de protección a través de un plan de mejora continua aplicando la metodología desarrollada en este TFM con un caso práctico.

Nos centraremos en la identificación de los posibles tratamientos de datos y de la realización de la Evaluación de Impacto relativa a la Protección de Datos de dichos tratamientos. Por tanto, el alcance de este TFM va desde la identificación de los tratamientos de datos llevados a cabo por una empresa u organización hasta la finalización de la Evaluación de Impacto relativa a la Protección de Datos.

En líneas generales cada paso de la metodología va a contener una descripción de las actividades que deben desarrollarse, de qué manera (metodología) y con qué resultado (finalidad).

Dentro de la EIPD destacaremos la metodología para realizar los Análisis de Riesgos de los tratamientos para garantizar **los derechos y libertades de las personas**. Esto incluye tanto aquellos riesgos para garantizar la seguridad, integridad y disponibilidad de los

datos personales como los riesgos de cumplimiento legal asociados a la propia normativa en materia de protección de datos.

El considerando 76 del RGPD dice:

La probabilidad y la gravedad del riesgo para los derechos y libertades del interesado debe determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. El riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto.

Para desarrollar la metodología planteada nos basaremos en un escenario ficticio, aunque para ello tomemos elementos de una empresa real.

Nos basaremos en algunos de los tratamientos que puede desempeñar un centro sanitario multidisciplinar. El ejemplo ficticio será un centro sanitario donde se realizan tratamientos de fisioterapia, psicología e impartición de cursos.

Para llevar a cabo el trabajo introduciremos algunos aspectos básicos de la normativa en materia de protección de datos.

4. Objetivos.

4.1. Objetivo general.

Desarrollar una metodología de Evaluaciones de Impacto relativas a la Protección de Datos (EIPD).

4.2. Objetivos específicos.

- Transmitir la necesidad de realizar las EIPD.
- Proporcionar instrumentos útiles para implementar la EIPD.
- Facilitar documentación para la realización de Análisis de Riesgos.
- Proponer un listado de riesgos o amenazas.
- Desarrollar la metodología de evaluación de riesgos.
- Ofrecer medidas de mitigación de riesgos.
- Presentar un modelo de informe de EIPD.

5. Planificación del Trabajo

La planificación del TFM se regirá por los siguientes hitos:

- **Parte 1:** Definición del alcance, tipos de datos personales, introducción al RGPD.
- **Parte 2:** Desarrollo de la metodología de Evaluación de Impacto relativa a la Protección de Datos que incluye la metodología de Análisis de Riesgos para garantizar los derechos y libertades de las personas.
- **Parte 3:** Realización de una Evaluación de Impacto relativa a la Protección de Datos sobre un escenario ficticio, incluida la parte de Análisis de Riesgos: identificación y valoración.
- **Parte 4:** Evaluación de Impacto relativa a la Protección de Datos, Análisis de Riesgos: Tratamientos de Riesgos (medidas para mitigar el nivel de riesgo). Reducción de riesgo.
- **Parte 5:** Revisión Evaluación de Impacto relativa a la Protección de Datos, breve auditoría.

6. Introducción a la normativa en materia de protección de datos.

Actualmente a fecha de redacción del presente TFM, la normativa de protección de datos se basa en:

- Artículo 18.4 de la Constitución Española: 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.

- Artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea: Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
- Artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea: Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
- Reglamento (UE) 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos RGPD o GDPR por sus siglas en inglés).
- DIRECTIVA (UE) 2016/680 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

6.1. Tipos de datos personales.

De acuerdo con el RGPD y la LOPDGDD, se define dato personal como *cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables*. Cuando la ley habla de datos personales incluye cualquier tipo de información siempre que haga referencia a una persona física identificada (directamente, se sabe quién es por el dato facilitado, ejemplo: DNI) o identificable (indirectamente, no se sabe de quién es por el dato facilitado, pero se podría averiguar, ejemplo: huella dactilar).

Los datos personales se dividen en tres posibles categorías:

- Datos personales.
- Datos personales de categoría especial.
- Datos personales de condenas e infracciones penales.

Estos últimos se podrían considerar una categoría de datos personales parecida a categoría especial. Aunque no podemos incluir los datos relativos a la infracciones y sanciones penales dentro de la categoría especial del artículo 9 del RGPD, encontramos varios preceptos que permiten apreciar una cierta equiparación entre los datos de categoría especial y los relativos a condenas e infracciones penales, como es el caso de los supuestos de designación del delegado de protección de datos, de registro de las actividades de tratamiento o de evaluación de impacto relativa a la protección de datos.

Además, prevé la posibilidad de limitar el alcance de los derechos recogidos en el propio RGPD, entre otros supuestos, cuando sea preciso para salvaguardar la prevención,

investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales. En todo caso, es importante destacar que el propio RGPD remite a la Directiva 2016/680 para determinados tratamientos de este tipo de datos.

Hay que señalar que pasamos de una clasificación de datos personales de categoría básica, media y alta a esta nueva categorización de los datos personales.

6.1.1. Clasificación de los datos.

En el Anexo 1, tenemos un listado con distintos tipos de datos. Hay que recordar que este listado es ampliable, pero sirve de base.

6.2. RGPD Introducción.

6.2.1. Principios.

6.2.1.1. Principio de responsabilidad proactiva (accountability).

Habrá que aplicar medidas oportunas y eficaces para tratar los datos personales como exige la norma. Es una responsabilidad proactiva. No incumplir ya no será suficiente. El responsable del tratamiento debe estar en todo momento en disposición de demostrar que cumple la normativa vigente.

6.2.1.2. Principio de protección de datos por defecto y desde el diseño.

Se deberán adoptar medidas técnicas y organizativas que garanticen el cumplimiento de la norma en las primeras fases del diseño, de forma que se garantice la intimidad y los principios de protección de datos desde el primer momento.

6.2.1.3. Principio de licitud, lealtad y transparencia.

La información debe facilitarse de forma comprensible, simple, inteligible y accesible. Incluso pueden usarse iconos normalizados.

6.2.1.4. Principio de limitación de la finalidad.

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

6.2.1.5. Principio de minimización de los datos.

Los datos personales recogidos deben ser los mínimos necesarios para la finalidad establecida. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad.

6.2.1.6. Principio de exactitud de los datos.

Los datos personales serán exactos y, si fuera necesario, actualizados. Para ello se tomarán todas las medidas técnicas y organizativas necesarias.

6.2.1.7. Principio de limitación del plazo de conservación de los datos.

Los datos personales deben ser mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los mismos. Posteriormente a ese plazo, sólo podrán conservarse para finalidades de

archivo en interés público, fines de investigación científica o histórica o fines estadísticos, siendo en ocasiones preciso, en orden a salvaguardar el principio de minimización, proceder a la seudonimización de los mismos, y sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas para proteger los derechos del interesado.

6.2.1.8. Principio de integridad y confidencialidad.

Los datos personales serán tratados de manera que se garantice una seguridad y confidencialidad adecuadas de los mismos. Esto incluye para impedir el acceso o uso no autorizados de dichos datos.

6.2.2. Obligaciones.

6.2.2.1. Delegado de Protección de Datos.

Designar un Delegado de Protección de Datos (DPD o DPO por sus siglas en inglés), interno o externo, que asista a las organizaciones en el proceso de cumplimiento normativo. Según el artículo 37.1 del RGPD se designará siempre que:

37.1.a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;

37.1.b) las actividades principales del responsable o del encargado consistan 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, o

37.1.c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

La misión principal del DPD es asegurarse que el tratamiento de los datos personales no impacte negativamente sobre los interesados. En diversas situaciones hará funciones de mediador entre los interesados y la propia organización. El DPD no se limita a intervenir una vez que el tratamiento ya ha sido implementado, sino asesorar acerca de las mejores prácticas y como aplicar los principios de privacidad por diseño y privacidad por defecto. El artículo 39 del RGPD dice:

Artículo 39

Funciones del delegado de protección de datos

1. El delegado de protección de datos tendrá como mínimo las siguientes funciones:

a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;

b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;

d) cooperar con la autoridad de control;

e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

2. El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

6.2.2.2. Evaluación de Impacto relativa a la Protección de Datos.

Realización de Evaluación de Impacto relativa a la Protección de Datos (EIPD), que determinen los riesgos específicos que supone tratar ciertos datos personales y prevean medidas para mitigar o eliminar dichos riesgos.

6.2.2.3. Ventanilla única.

Aquellas empresas u organizaciones establecidas en varios Estados de la UE o, las que estando en un solo Estado, traten datos personales de ciudadanos de varios Estados de la UE, tendrán que responder solamente ante la Autoridad de control del Estado miembro en el que se encuentren registradas.

6.2.2.4. Brechas de seguridad.

Una brecha de seguridad según el RGPD se trata de errores, fallos o violaciones intencionales que, producidos en o contra un sistema informático, derivan en la destrucción, pérdida o alteración de datos personales, comunicación o acceso en favor de terceras personas no autorizadas. Las brechas de seguridad deberán ser comunicadas a las autoridades de control y, en casos graves, a los afectados, tan pronto sean conocidas, estableciéndose un plazo máximo de 72 horas.

6.2.2.5. Datos de categoría especial.

Se amplía el listado de datos especialmente protegidos, incluyendo entre otros, ahora los datos genéticos, biométricos y las infracciones y condenas penales.

6.2.2.6. Encargado del tratamiento.

Los encargados de tratamiento, que son los que tratan datos por cuenta de terceros, a partir de la entrada en vigor de RGPD, sus contrataciones se vuelven más restrictivas, ya que tendrán demostrar que cumplen con garantías suficientes de cumplimiento normativo.

6.2.2.7. Transferencias internacionales de datos.

Se exigen garantías adicionales para las transferencias internacionales de datos. Garantías más restrictivas y mecanismos de seguimiento en relación con las transferencias internacionales de datos a países, territorios o sectores específicos que no garantizan un nivel de protección adecuado. Para ello se ha creado una lista de países fuera de la UE que se consideran que si cumplen con las garantías adecuadas. Países como: Andorra, Argentina, Canadá, Guernesey, Isla de Man, Islas Feroe, Israel, Jersey, Nueva Zelanda, Suiza, Uruguay y Estados Unidos (solo si la entidad está adherida a “Privacy Shield”).

6.2.2.8. Códigos de conducta y certificaciones.

Se prevé que se creen sellos y certificaciones de cumplimiento que permiten acreditar la responsabilidad activa o Accountability por parte de las organizaciones. Son mecanismos con carácter voluntario.

6.2.2.9. Sanciones.

Las cuantías suben considerablemente pudiendo llegar a los 20 millones de euros o el 4% de la facturación global anual (la cantidad más alta de las dos).

6.2.3. Derechos.

Pasamos de los derechos ARCO a los derechos ARCO+ o SOPLAR:

6.2.3.1. Supresión.

El interesado tiene derecho a la supresión de los datos personales que le conciernan. El derecho de supresión alcanza una dimensión más amplia a fin de reforzar el "derecho al olvido" en el entorno on-line reconocido jurisprudencialmente.

6.2.3.2. Oposición y decisiones individuales automatizadas.

El derecho de oposición permite al interesado, en los casos previstos en el RGPD, oponerse al tratamiento de sus datos personales y que por tanto dejen de usarse. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

6.2.3.3. Portabilidad.

El interesado tendrá derecho a recibir sus datos personales en un formato estructurado, de uso común y lectura mecánica. Estos datos se podrán transmitir, a su vez, a otra organización o empresa.

6.2.3.4. Limitación.

El derecho a la limitación permite al interesado solicitar que la organización o empresa aplique medidas sobre sus datos personales para evitar su modificación o, en su caso, su borrado o supresión.

6.2.3.5. Acceso.

Toda persona tiene derecho a acceder a los datos recogidos que le conciernan. Si las solicitudes son manifiestamente infundadas o excesivas (carácter repetitivo) el responsable podrá cobrar a la persona que los solicita un canon proporcional a los costes administrativos soportados, sin que pueda generar un beneficio económico.

6.2.3.6. Rectificación.

Es el derecho que tiene el interesado, cuando los datos personales son inexactos o están incompletos, a que se rectifiquen.

A mayores de estos derechos también podemos considerar el **consentimiento** para poder tratar datos personales ha de ser informado, inequívoco, libre y revocable y deberá darse mediante un acto afirmativo claro. No se admite consentimiento tácito.

6.3. LOPDGDD Introducción.

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. (LOPDGDD) añade entre otras las siguientes novedades.

6.3.1. Legitimación de las administraciones públicas para el uso y cesión de los datos personales.

Se establecen bases de legitimación para el tratamiento de los datos personales, de las cuales algunas sirven para la utilización (y en su caso cesión) de los datos personales por parte de las Administraciones Publicas.

6.3.2. Delegado de Protección de Datos.

Se amplían los supuestos en los que es obligatoria la designación de un Delegado de Protección de Datos y para su cualificación se tendrá en cuenta a través de mecanismos voluntarios de certificación. Estos supuestos se recogen en el artículo 34.

Artículo 34. Designación de un delegado de protección de datos.

1. Los responsables y encargados del tratamiento deberán designar un delegado de protección de datos en los supuestos previstos en el artículo 37.1 del Reglamento (UE) 2016/679 y, en todo caso, cuando se trate de las siguientes entidades:

a) Los colegios profesionales y sus consejos generales.

b) 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.

c) Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.

d) Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.

e) Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.

f) Los establecimientos financieros de crédito.

g) Las entidades aseguradoras y reaseguradoras.

h) Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.

i) Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.

j) 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.

k) 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.

l) Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes. Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.

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

n) 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.

o) Las empresas de seguridad privada.

p) Las federaciones deportivas cuando traten datos de menores de edad.

2. Los responsables o encargados del tratamiento no incluidos en el párrafo anterior podrán designar de manera voluntaria un delegado de protección de datos, que quedará sometido al régimen establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

3. Los responsables y encargados del tratamiento comunicarán en el 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 de los delegados de protección de datos tanto en los supuestos en que se encuentren obligadas a su designación como en el caso en que sea voluntaria.

4. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán, en el ámbito de sus respectivas competencias, una lista actualizada de delegados de protección de datos que será accesible por medios electrónicos.

5. En el cumplimiento de las obligaciones de este artículo los responsables y encargados del tratamiento podrán establecer la dedicación completa o a tiempo parcial del delegado, entre otros criterios, en función del volumen de los tratamientos, la categoría especial de los datos tratados o de los riesgos para los derechos o libertades de los interesados.

6.3.3. Redes sociales.

Derecho al olvido en servicios de redes sociales y servicios equivalentes, recogiendo el derecho de toda persona a que sean suprimidos, con su simple solicitud, los datos personales que hubiese facilitado tanto ella como terceros cuando fueran inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieran devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.

6.3.4. Protección de Datos personas fallecidas.

Las personas vinculadas al fallecido por razones familiares o, de hecho, así como sus herederos, podrán solicitar el acceso, rectificación o supresión, con la excepción de que la persona fallecida lo hubiera prohibido expresamente o que así lo establezca una ley.

6.3.5. Régimen jurídico de los empleados.

Se modifican las dos normas básicas que regulan las relaciones laborales: El Texto Refundido de la Ley del Estatuto de los Trabajadores relativo a su derecho a la intimidad en relación con el entorno digital y a la desconexión y la Ley del Estatuto Básico del Empleado Público. Se recoge el derecho a la intimidad en el uso de dispositivos digitales puestos a su disposición y frente al uso de dispositivos de videovigilancia y geolocalización, así como la desconexión digital

6.3.6. Esquema nacional de seguridad.

Se establece el Esquema nacional de seguridad como mecanismo suficiente para garantizar las medidas de seguridad técnicas y organizativas que exige el RGPD en el ámbito del sector público y en las empresas privadas que operan en él.

6.3.7. Datos para perfilación por parte de partidos políticos.

Utilización de medios tecnológicos y datos personales en las actividades electorales. Permite la recopilación de las opiniones políticas de las personas por parte de los partidos políticos en el marco de sus actividades electorales.

7. Metodología de Evaluación de Impacto relativa a la Protección de Datos.

7.1. Introducción a las EIPD

Según la definición de la Agencia Española de Protección de Datos.

Es un proceso ligado a los principios de protección de datos desde el diseño y protección de datos por defecto concebido para describir, de manera anticipada y preventiva, un tratamiento de datos personales, evaluar su necesidad y proporcionalidad y gestionar los potenciales riesgos para los derechos y libertades a los que estarán expuestos los datos personales en función de las actividades de tratamiento que se lleven a cabo con los mismos, determinando las medidas necesarias para reducirlos hasta un nivel de riesgo aceptable.

El Reglamento general de protección de datos, en su considerando 84 dice:

A fin de mejorar el cumplimiento del presente Reglamento en aquellos casos en los que sea probable que las operaciones de tratamiento entrañen un alto riesgo para los derechos y libertades de las personas físicas, debe incumbir al responsable del tratamiento la realización de una evaluación de impacto relativa a la protección de datos, que evalúe, en particular, el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo. El resultado de la evaluación debe tenerse en cuenta cuando se decidan las medidas adecuadas que deban tomarse con el fin de demostrar que el tratamiento de los datos personales es conforme con el presente Reglamento. Si una evaluación de impacto relativa a la protección de datos muestra que las operaciones de tratamiento entrañan un alto riesgo que el responsable no puede mitigar con medidas adecuadas en términos de tecnología disponible y costes de aplicación, debe consultarse a la autoridad de control antes del tratamiento.

Las EIPD deben situarse en el contexto de las medidas o acciones preventivas, es decir, se trata de un proceso de evaluación que, con carácter general, debe realizarse antes de iniciar las operaciones de tratamiento de los datos personales.

Su finalidad está en la línea con el principio de protección de datos por defecto y desde el diseño. como se dice en el considerando 78:

A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto…

También será muy útil para cumplir con el principio de responsabilidad proactiva (accountability) ya que el proceso y posterior documentación permiten demostrar el grado de cumplimiento.

El Comité Europeo de protección de Datos (en adelante CEPD) manifestó que:

Una EIPD es 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. Las EIPD son instrumentos importantes para la rendición de cuentas, ya que ayudan a los responsables no solo a cumplir los requisitos del RGPD, sino también a demostrar que se han tomado medidas adecuadas para garantizar el cumplimiento del Reglamento.

Se trata de un proceso sistemático, objetivo, repetible, comparable y documentado.

7.2. Evaluación de impacto vs Análisis de riesgos.

Para todo tratamiento de datos es obligatorio la realización de un análisis de riesgos de los derechos y libertades fundamentales de las personas físicas.

El artículo 32 del RGPD dice:

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo…

En definitiva, el primer paso para determinar las medidas de seguridad será la evaluación del riesgo, una vez evaluado el riesgo será necesario determinar las medidas de seguridad encaminadas para reducir o eliminar los riesgos para el tratamiento de los datos. Mientras que el Análisis de riesgos es una obligación para todos los tratamientos las evaluaciones de impacto, el artículo 35 del RGPD indica que será necesario llevarlo a cabo si el tratamiento de datos "*entraña un alto riesgo para los derechos y libertades de las personas físicas*". Por tanto, sólo en ciertos casos son obligatorias las Evaluación de impacto frente a la gestión de riesgos que es obligatoria siempre.

Tenemos que entender que el AARR es una parte de la EIPD. En los casos en los que la EIPD no sea obligatoria sólo tendremos la obligación de gestionar los riesgos del tratamiento a través de un AARR.

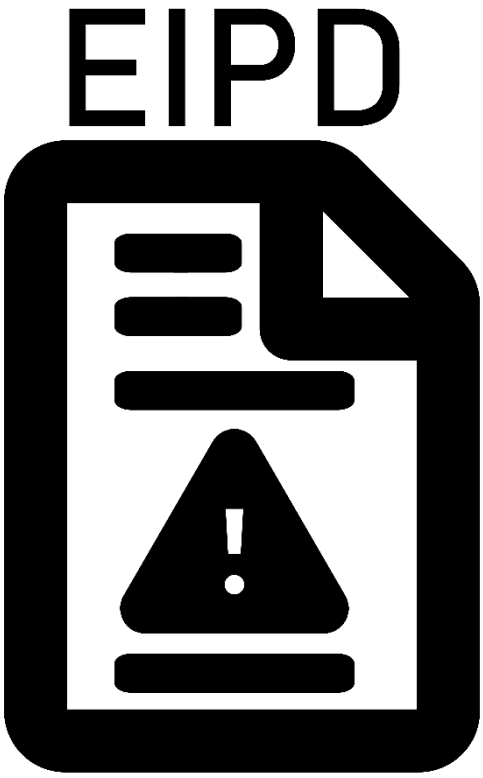

Figura 1: AA RR como parte de EIPD.

7.3. Propuesta de metodología de Evaluación de Impacto relativa a la Protección de Datos.

No existe una metodología concreta de EIPD. El RGPD habla solamente de unos mínimos que debe contener en su artículo 35.7.

a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;

b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y

d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

Por tanto, siempre y cuando nos ciñamos a estos cuatro puntos tenemos una gran libertad a la hora de desarrollar una metodología.

A continuación, mostramos algunas de las propuestas hechas al respecto.

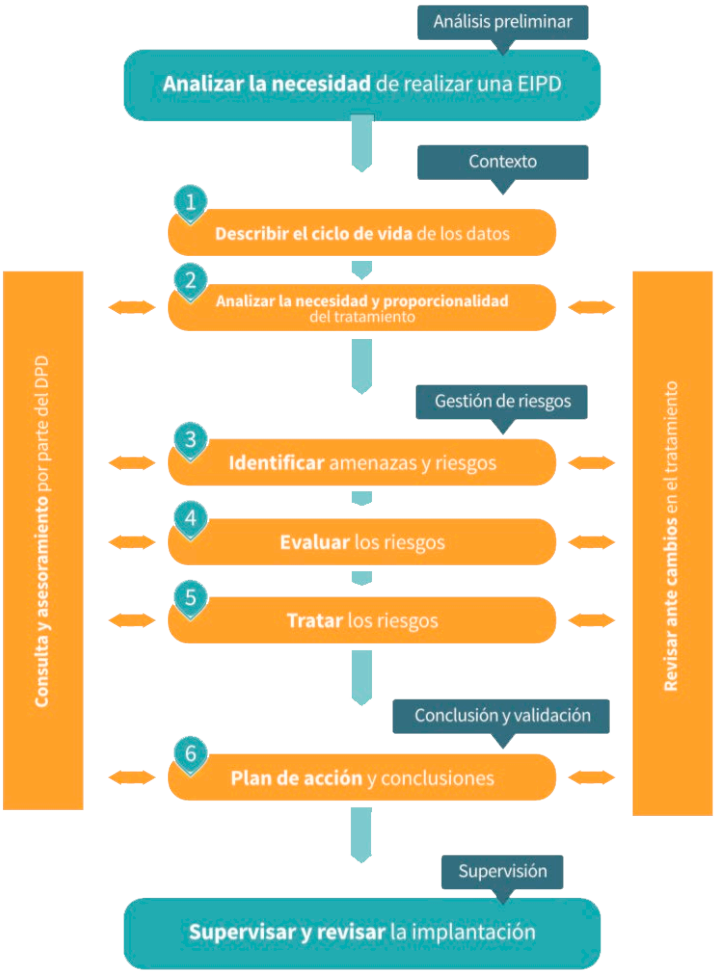

Figura 2: Proceso EIPD según AEPD Guía práctica para las Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD

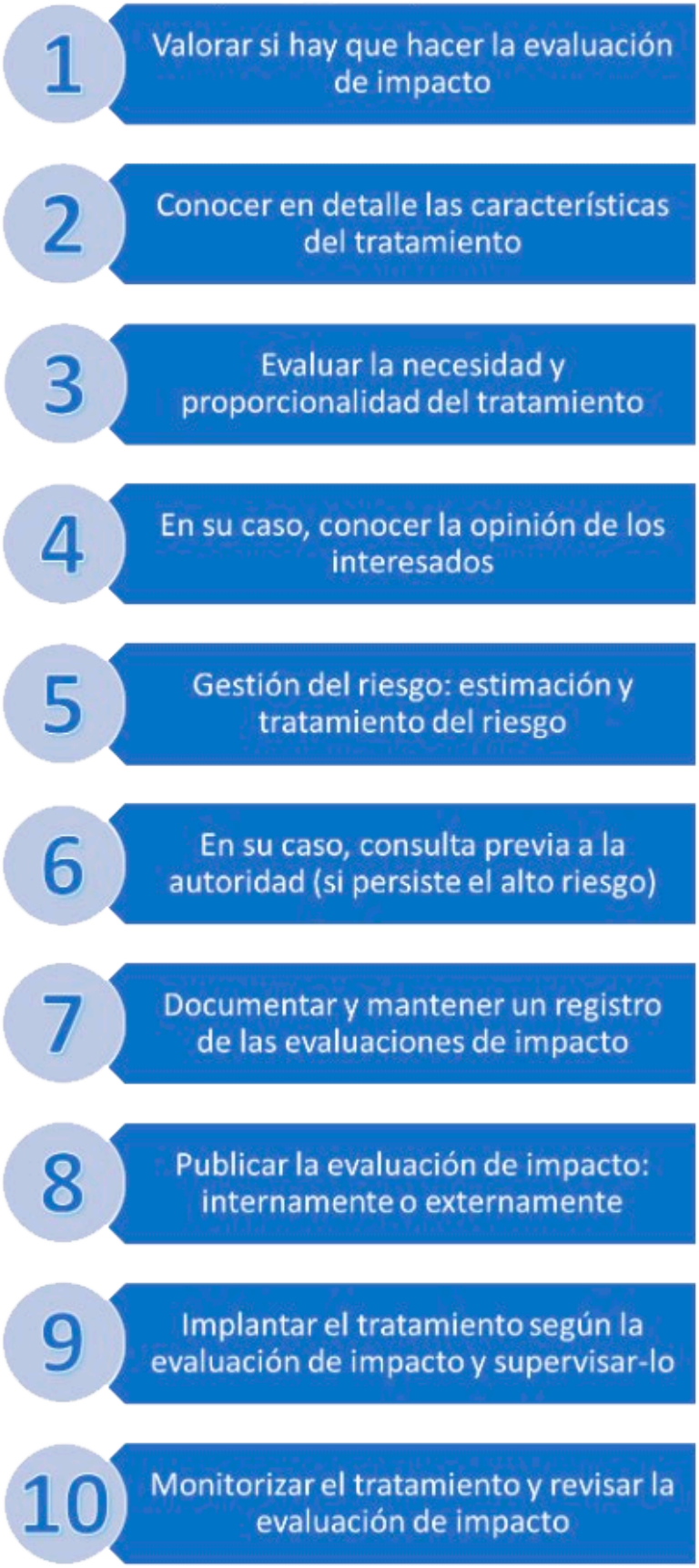

Figura 3: Proceso EIPD según L'Autoritat Catalana de Protecció de Dades. Guía sobre la evaluación de impacto relativa a la protección de datos en el RGPD

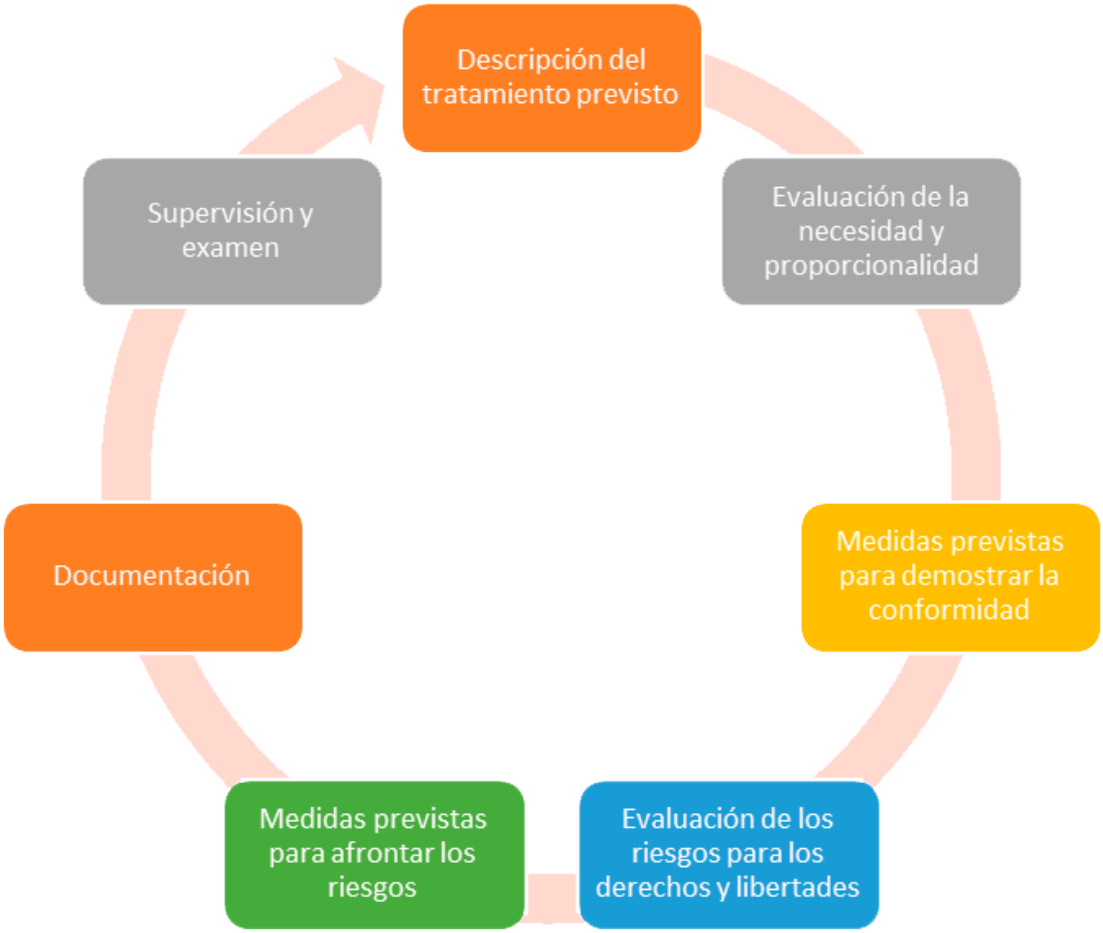

Figura 4: Proceso EIPD según Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679. Propuestas por CEPD

7.3.1. Procedimiento de metodología de Evaluación de Impacto relativa a la Protección de Datos

La metodología propuesta para este TFM girará en torno a los siguientes ítems.

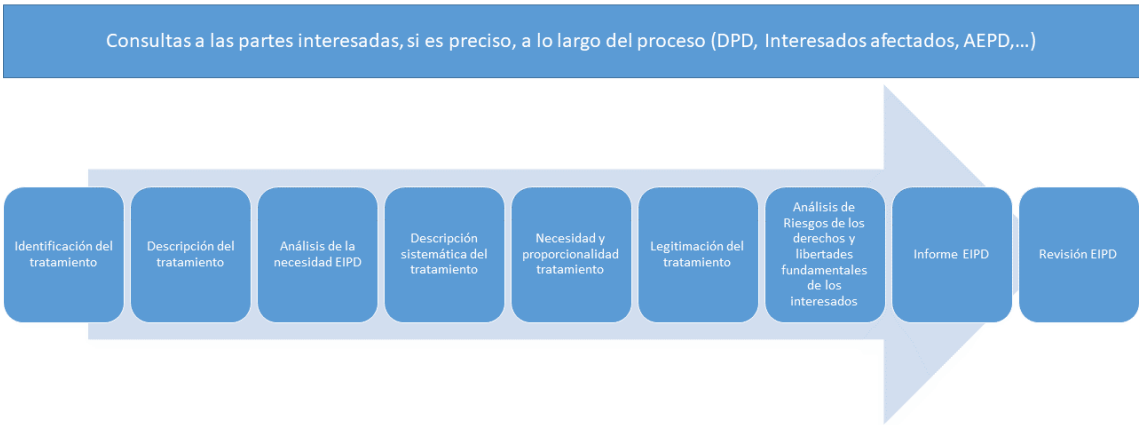

Figura 5: Proceso EIPD propuesto en este TFM

7.3.2. Identificación de tratamiento.

El primer paso que debemos realizar en sin duda la identificación del tratamiento, para ello debemos determinar la denominación del tratamiento (el título) y hacernos una idea general sobre el mismo. Podemos preguntar a los clientes los tipos de procedimientos que realizan con los datos poniendo varios ejemplos.

Es bueno a modo de detección de tratamientos partir de un listado inspirador de tratamientos. Este listado podrá ser todo lo amplio que queramos y nos ayudará a la hora de identificar tratamientos en una empresa. Este listado en concreto está basado en el registro de actividades del tratamiento de la AEPD, tratamientos en los que es obligatoria una EIPD según el CNIL y otros. En el Anexo 2 tenemos un listado de tratamientos a modo de ejemplo.

7.3.2.1. Tratamientos ya iniciados antes del 25 de mayo de 2018.

Aunque estos tratamientos en principio están exentos de la realización de una EIPD, no lo están de la gestión de riesgos y sería recomendable la utilización de esta metodología para la realización de la evaluación de impacto ya que si son tratamientos con un nivel alto o muy alto de precalificación de riesgo tendrán que someterse a una completa gestión de riesgos donde las EIPD sirven como método.

Además, según *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, WP248.*

Podría requerirse una EIPD después de que se produzca un cambio de los riesgos a causa de las operaciones de tratamiento, por ejemplo, debido a la puesta en marcha de una nueva tecnología o a que los datos personales se usan para un fin distinto.

Por lo que el proceso de revisión de EIPDs será de aplicación a tratamientos ya existentes para determinar si es necesario iniciar el proceso de EIPD. En este caso se podría denominar la misma como **Evaluación de Impacto relativa a la Protección de Datos ex post.**

7.3.3. Descripción del tratamiento.

Debemos ser capaces de describir el tratamiento, fijando para ello los objetivos perseguidos con el tratamiento. De esta manera podremos determinar las finalidades del tratamiento.

7.3.4. Análisis de la necesidad de la EIPD, evaluación objetiva.

En este proceso debemos determinar si es necesario y por tanto obligatorio realizar una EIPD. Como los criterios son bastante subjetivos y mientras la AEPD o el CEPD no se manifiesten muy claramente con listados de tratamientos para los cuales es obligatorio hacer una EIPD y para aquellos que no, es muy recomendable hacerla. Como es muy probable querido lector, que si has llegado hasta aquí necesites para alguno de tus tratamientos realizar una EIPD, te recomiendo que lo hagas con todos. Porque, a fin de cuentas, la EIPD no es más que una toma de datos documentada y vitaminada.

Los criterios que vamos a usar para determinar si es necesaria o no, están basados en cuatro análisis:

7.3.4.1. Comprobar si es obligatoria según RGPD.

La EIPD, según el artículo 35.3 del RGPD será obligatoria si:

a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o

c) observación sistemática a gran escala de una zona de acceso público.

7.3.4.2. Comprobar criterios de "alto riesgo" proporcionados por el CEPD.

El motivo por el cual resulta obligatoria la EIPD es el "*alto riesgo*" del tratamiento, por lo tanto, siempre que consideremos que existe un "*alto riesgo*" para los derechos y libertades fundamentales de las personas físicas procederemos a realizar la EIPD.

Criterios para determinar si existe un "*alto riesgo*": tendríamos las *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,* del CEPD que serían:

- Evaluación o puntuación.
- Toma de decisiones automatizadas con efecto jurídico significativo o similar.
- Observación sistemática.
- Datos sensibles o datos muy personales.
- Tratamiento de datos a gran escala.
- Asociación o combinación de conjuntos de datos.
- Datos relativos a interesados vulnerables.
- Uso innovador o aplicación de nuevas soluciones tecnológicas u organizativas.
- Cuando el propio tratamiento impida a los interesados ejercer un derecho o utilizar un servicio o ejecutar un contrato.

Podemos consultar en profundidad las 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. para determinar el nivel de riesgo alto.

7.3.4.3. Comprobar criterios de "mayor riesgo" que constan en la LOPDGDD.

La LOPDGDD en el artículo 28.2 también nos habla de un "*mayor riesgo*" y nos da una serie de pautas para determinarlo. Hay que recordar que el hecho de encajar en alguno de dichos supuestos no implica que necesariamente exista un "*alto riesgo*". Insistimos en la recomendación de hacer EIPD independientemente de tener la certeza de que el tratamiento supone un "*alto riesgo*".

(…) los responsables y encargados del tratamiento del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos:

a) Cuando el tratamiento pudiera generar situaciones 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, moral o social significativo para los afectados.

b) Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.

c) Cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta ley orgánica o de los datos relacionados con la comisión de infracciones administrativas.

d) Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.

e) Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.

f) Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.

g) Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección.

h) Cualesquiera otros que a juicio del responsable o del encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación.

7.3.4.4. Comprobar si está en el listado de tratamientos identificados por la Agencia Española de Protección de datos.

Este listado se encuentra en el Anexo 11.

7.3.4.5. Comprobar si está en el listado de tratamientos identificados por las autoridades de control de protección de datos europeas.

Este listado se encuentra en el Anexo 8.

7.3.5. Descripción sistemática del tratamiento.

7.3.5.1. Ciclo de vida de los datos.

Los datos desde que se recaban por primera vez hasta que se destruyen pasan por un ciclo de vida.

Según el anexo D de la ISO/IEC 29134

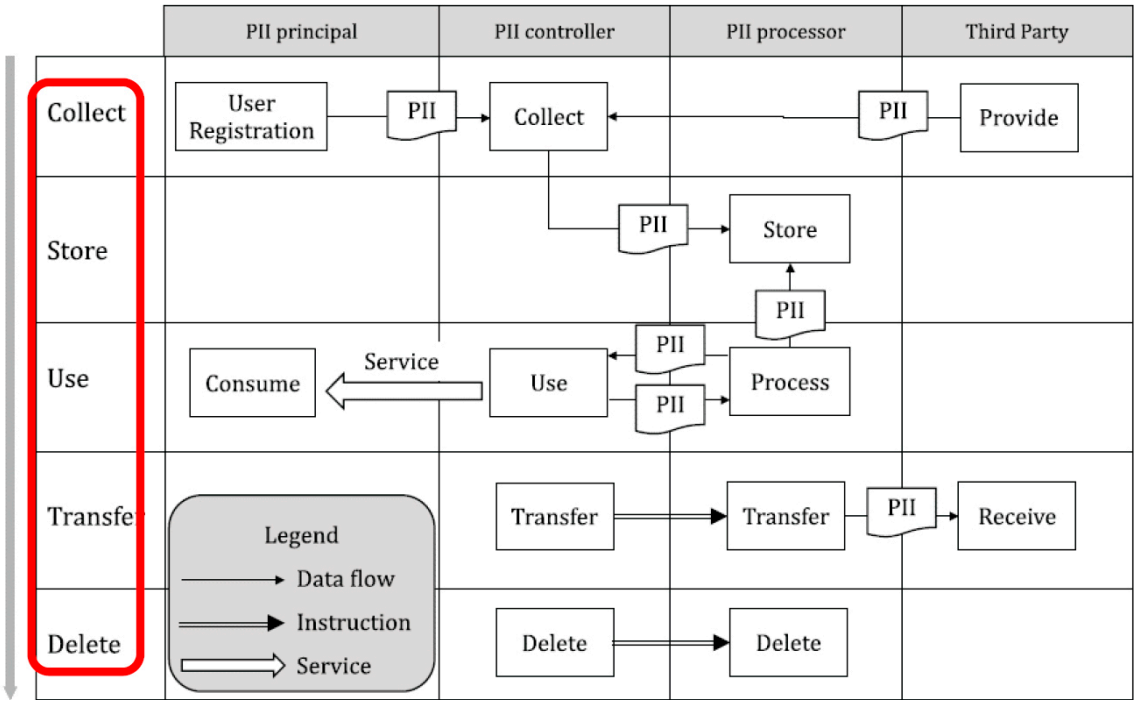

Figura 6: Anexo D ISO/IEC 29134

Este ciclo de los datos es el que debemos analizar de una manera sistémica. El ciclo de vida de los datos es ese momento en una toma de datos dónde estamos formulándole las dudas al cliente sobre todos los procesos que se realizan en la empresa en la que intervienen datos. Simplificando un poco el modelo propuesto en la ISO/IEC 29134 nos limitaremos a establecer sus cinco fases: Recoger, Almacenar, Utilizar, Transferir y Borrar. Para cada una de las fases debemos indicar:

- Las partes que intervienen: interesados, responsables del tratamiento, encargados del tratamiento, trabajadores, y terceras partes.
- Tipos de datos: Los reflejados en el Anexo 1.
- Operaciones de tratamiento. Podemos inspirarnos en las operaciones de tratamiento del Anexo 3.
- Medios tecnológicos indicando si la tecnología es emergente o invasiva. Se debe identificar la tecnología (cloud, BBDD, servidores), aplicaciones, dispositivos y técnicas empleadas en el procesamiento de los datos

Según la Guía práctica para las evaluaciones de impacto en la protección de datos sujetas al RGPD de la AEPD sobre las fases o etapas del ciclo de vida se dice:

- **Recoger - Captura de datos:** Proceso de obtención de datos para su almacenamiento y posterior procesado. Dentro de la captura de datos se pueden encontrar diversas técnicas, como, por ejemplo: formularios web, formularios en papel, la toma de muestras y realización de encuestas, grabaciones de audio y video, fuentes externas o públicas como redes sociales, captación mediante sensores, etc.
- **Almacenar - Clasificación / Almacenamiento:** Establecer categorías y asignarlas a los datos para su clasificación y almacenamiento en los sistemas o archivos.
- **Utilizar - Uso / Tratamiento:** Operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos de los datos automatizados o manuales.
- **Transferir - Cesión de los datos a un tercero para su tratamiento:** Traspaso o comunicación de datos realizada a un tercero (toda persona física o jurídica, pública o privada u órgano administrativo). El concepto de cesión o comunicación es muy amplio, puesto que la revelación recoge tanto la entrega, comunicación, consulta, interconexión, transferencia, difusión o cualquier otra forma que facilite el acceso a los datos.
- **Borrar - Destrucción:** Eliminar los datos que puedan estar contenidos en los sistemas o archivos, de manera que no puedan ser recuperados de los soportes.

Por tanto, tenemos que crear una tabla como la que adjuntamos donde para cada una de las fases descritas, tanto en la ISO/IEC 29134 como por la AEPD, deben ser cubiertas.

	Recoger	Almacenar	Utilizar	Transferir	Borrar
Interesados					
Tipos de datos					
Operaciones de tratamiento					
Tecnologías					

Tabla 1: Ciclo de vida de los datos.

Para facilitarnos esta tarea, una propuesta hecha por la APDCAT para la recogida de datos de cara a analizarlos en el ciclo de vida de los mismos sería:

Recogida de información sobre los datos		
Datos personales facilitados directamente por las personas afectadas		
Categoría especial		
Descripción	**SI**	**NO**
(por ejemplo: DNI)		
Datos personales facilitados por terceros (el origen de los datos son cesiones o comunicaciones)		
Categoría especial		
Descripción	**SI**	**NO**
(por ejemplo: apellidos)		
Datos personales ya disponibles anteriormente (el origen de los datos es el propio responsable del tratamiento, que dispone de estos datos porque los ha tratado previamente)		
Categoría especial		
Descripción	**SI**	**NO**
(Por ejemplo: histórico altas y bajas)		
Datos personales capturados (los datos se han obtenido mediante dispositivos o aplicaciones que, de manera autónoma, sin una acción concreta de la persona afectada, recogen información diversa –información de "cookies", navegador utilizado, información de dispositivos móviles, coordenadas de geoposicionamiento, dirección IP, tiempo de conexión, etc.		
Categoría especial		
Descripción	**SI**	**NO**
(por ejemplo: dirección IP)		
Datos personales calculados (el origen son operaciones de tratamiento que dan como resultado información de carácter personal adicional: coordenadas de geoposicionamiento que es traducen en ubicaciones concretas, preferencias de consumo, nivel de riesgo financiero, etc.)		
Categoría especial		
Descripción	**SI**	**NO**
(por ejemplo: distancia)		
Datos que inicialmente no se considera dato de carácter personal (esta clasificación puede variar posteriormente: direcciones IP, versiones de navegador, datos anonimizados, etc.)		
Categoría especial		
Descripción	**SI**	**NO**
(por ejemplo: código de seudonimización)		

Tabla 2: Ciclo de vida de los datos.

7.3.6. Analizar la necesidad y proporcionalidad del tratamiento

En este caso estamos analizando la necesidad y proporcionalidad del tratamiento. La necesidad de realizar la EIPD ya se trató en un punto anterior.

Necesidad del tratamiento: los datos personales solo deberán ser objeto de tratamiento si su finalidad no puede alcanzarse "razonablemente" por otros medios, es decir, sin tratar datos personales, por tanto, cuando evaluemos la necesidad, en relación a la finalidad, siempre deberemos cuestionarnos si todos los datos que se pretenden recopilar y tratar son necesarios.

Proporcionalidad del tratamiento: la finalidad no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para la intimidad de las personas y para su derecho a la protección de datos personales. El juicio de proporcionalidad viene muy bien explicado en la **STC 66/1995, 8 de mayo de 1995**, dónde con otras palabras dice:

Para comprobar si la medida impeditiva del ejercicio del derecho supera el juicio de proporcionalidad exigible, es necesario constatar si cumple los siguientes tres requisitos o condiciones:

1. *si tal medida era susceptible de conseguir el objetivo propuesto (ejemplo: la garantía del orden público sin peligro para personas y bienes);*
2. *si además era necesaria en el sentido de que no existía otra medida más moderada para la consecución de tal propósito con igual eficacia;*
3. *y, finalmente, si la misma era proporcionada, en sentido estricto, es decir, ponderada o equilibrada por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto.*

7.3.7. Legitimación del tratamiento.

Una vez identificados los distintos tratamientos, analizado el ciclo de vida de los datos y la necesidad y proporcionalidad del tratamiento, debemos identificar la base legitimadora del tratamiento. Es decir, el tratamiento previsto sólo podrá llevarse a cabo si encaja en alguno de los supuestos de licitud o bases legitimadoras del artículo 6.1 del RGPD.

Además, cuando el tratamiento incluya categorías especiales de datos, también será necesario identificar en qué excepción encaja de las previstas en el artículo 9.2 del RGPD.

De no encajar en alguno de estos supuestos y excepciones, no será posible llevar a cabo el tratamiento previsto.

Además, es relevante señalar que, conforme el artículo 6.3 RGPD, cuando la base del tratamiento sea el cumplimiento de una obligación legal o el cumplimiento de una misión de interés público o ejercicio de poderes públicos, esta base deberá venir establecida en:

- Norma de Derecho de la UE (Reglamento legislativo; Directiva legislativa; Decisión legislativa)

- Norma con rango de ley (Ley Orgánica, Ley Común, Decreto-Ley; Decreto Legislativo; Ley Autonómica) que determine la finalidad del tratamiento.

7.3.8. Análisis de Riesgos de los derechos y libertades fundamentales de las personas físicas.

7.3.8.1. Introducción

Cuando hablamos de Análisis de Riesgos de los derechos y libertades fundamentales de las personas físicas, no nos referimos exclusivamente a un análisis de los riesgos vinculados al uso de las tecnologías de la información (por tanto, conectado con la seguridad de la información). En todo caso, la gestión de riesgos de la seguridad de la información será una parte, en tanto la seguridad de los datos resulta esencial para preservar los derechos y libertades fundamentales. El análisis de riesgos que se realizará se centra en los riesgos que para los derechos y libertades de las personas pueden suponer las operaciones de tratamiento de datos personales.

Cuando hablamos de un Análisis de Riesgos de la Seguridad, estamos analizando los riesgos internos o externos que pueden sufrir los datos de nuestra organización. En cambio, cuando hablamos de un Análisis de Riesgos de los derechos y libertades fundamentales de las personas físicas, estamos analizando los riesgos que podemos provocar nosotros a las personas físicas de los que tratamos datos personales.

En esta etapa vamos a identificar qué situaciones de riesgo podrían afectar negativamente a las personas a las que hacen referencia los datos personales objeto de tratamiento.

Esta gestión de riesgos estará orientada exclusivamente al riesgo que puedan generar las operaciones de tratamiento sobre los datos personales, o sobre los derechos y libertades de las personas afectadas por los tratamientos.

7.3.8.2. Tipos de metodologías de análisis de riesgos

Existen varios tipos de metodologías de análisis de riesgos, entre otras:

7.3.8.2.1. Metodología basada en activos.

La mayoría de las metodologías de riesgos tienen aspectos en común, como son: el ciclo de vida de la gestión de riesgos y las opciones de tratamiento de los riesgos. En general muchas de las acciones que varían en estas metodologías, comprenden, la forma de presentar los resultados y de obtener los datos para el análisis. Esto es, en los aspectos de evaluación de riesgos. Por lo demás, los procesos de comunicación, consulta, monitoreo y revisión son obligatorios a realizar para gestionar adecuadamente los hallazgos evidenciados.

Las metodologías basadas en activos parten de la identificación de los activos de información.

Activos de información: corresponden a elementos que la organización requiere para realizar actividades de negocio o llevar a cabo cualquier proceso interno.

Luego se consideran un listado de amenazas (mayoritariamente se dispone de ese listado previo de anteriores análisis u obtenido por fuentes externas de información)

Amenazas: son las situaciones que desencadenan un incidente en la empresa, realizando un daño material o pérdidas inmateriales de sus activos de información.

Una vez teniendo definidos los activos y amenazas procedemos a la caracterización de las amenazas. Se realiza una estimación de vulnerabilidades e impactos que pueden sufrir los activos debido a las amenazas.

La vulnerabilidad de un activo de seguridad es la potencialidad o la posibilidad de que se materialice una amenaza sobre el activo de información. El impacto es el resultado o la consecuencia que se produce cuando una amenaza aprovecha una vulnerabilidad para afectar un activo de información.

Tras la caracterización de las amenazas obtenemos el mapa de riesgos.

7.3.8.2.2.Metodología basada en riesgos

Las metodologías basadas en riesgos parten de la identificación de los posibles riesgos a los que se puede enfrentar una organización. Esta metodología separa la gestión de los activos de la gestión de los riesgos. Se centra en el riesgo en sí mismo. Normas como la ISO 27001:2013 eliminó la necesidad de usar activos en los análisis de riesgos desapareciendo las referencias a la identificación de activos, amenazas y vulnerabilidades. Es mediante la ISO 31010 se determina que para que la descripción del riesgo sea de utilidad, deberá contener algún elemento como las fuentes de riesgo, que son los elementos con el potencial para influir en los resultados esperados, un evento, que sería un conjunto específico de circunstancias o las consecuencias de que el evento se produzca. En cierta forma los riesgos de esta metodología se parecen a las amenazas, salvo que no se centran en un activo en particular. Posteriormente se evalúa la probabilidad y gravead de sufrir ese riesgo y se obtiene igualmente un mapa de riesgos.

Esta metodología de riesgos es muy utilizada en prevención de riesgos laborales, en prevención de riesgos ambientales y en prevención de riesgos legales en que partimos de una legislación de obligado cumplimiento.

En el caso de los Análisis de Riesgos de los derechos y libertades fundamentales de las personas físicas hay una correspondencia entre registro de actividades de tratamiento y activos de la información en que un tratamiento se puede considerar como un activo más de la organización.

Para esto se necesita un estudio completo que responda a preguntas como: ¿qué eventos (riesgos) pueden afectar a la organización?, ¿han ocurrido anteriormente? ¿qué consecuencias tienen tanto económicas como de los derechos y libertades de las personas? Para la evaluación de estos riesgos se considera: la frecuencia con la que ocurren y las consecuencias posibles.

Para el escenario de riesgos debemos realizar una matriz de estimación del riesgo o mapa de riesgos en la que por cada riesgo determinaremos:

Si aplica: hemos identificado que la finalidad del tratamiento en cuestión tiene ese riesgo de la privacidad.

Valorar la probabilidad de que ese riesgo se materialice (según los criterios definidos).

Valorar la gravedad si se materializa ese riesgo (según los criterios definidos). La valoración de la gravedad debe contemplar tanto la gravedad que puede producir en la organización una sanción económica impuesta por la AEPD, así como la gravedad en los derechos y libertades de las personas.

La matriz de estimación de riesgo estaría formada por los campos: Riesgo, Probabilidad, Gravedad y Nivel de Riesgo

Una vez revisadas las diferentes metodologías se ha optado por la metodología basada en riesgos para la elaboración del presente TFM.

7.3.8.3. Propuesta metodología de Análisis de Riesgos de los derechos y libertades fundamentales de las personas físicas.

7.3.8.3.1. Procedimiento.

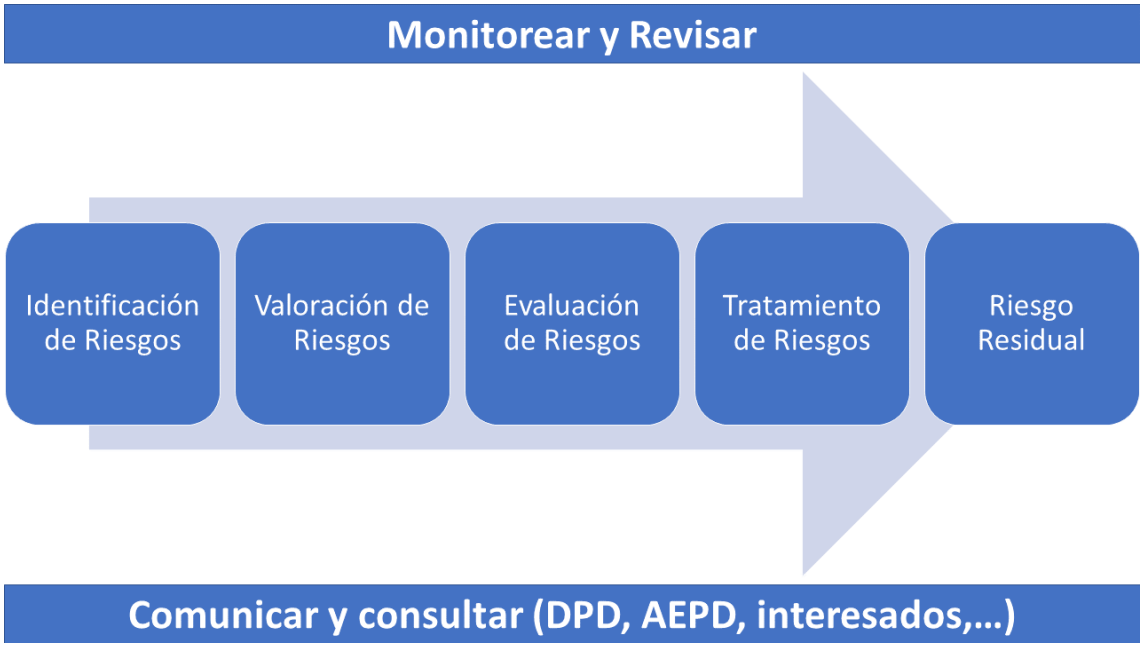

Figura 7: Proceso AA RR.

- **Identificación de Riesgos:** En esta fase se identificarán los riesgos.
- **Valoración de Riesgos:** En esta fase se determinará la aplicabilidad, probabilidad y gravedad.
- **Evaluación de Riesgos:** En esta fase se estimará el nivel de riesgo intrínseco y se priorizarán riesgos.
- **Tratamiento de Riesgos:** En esta fase se aplicarán medidas de mitigación del riesgo.
- **Riesgo Residual:** En esta fase se medirá el nivel de riesgo residual tras el tratamiento de los riesgos.

7.3.8.3.2. Identificación de Riesgos.

En nuestra metodología partiremos de un listado de riesgos que facilitamos en el Anexo 4. También proponemos en el Anexo 5 un método para identificar nuevos riesgos haciendo un barrido por los artículos del RGPD.

7.3.8.3.3. Valoración de Riesgos

Determinaremos la aplicabilidad (si el riesgo en concreto va a afectar al tratamiento analizado o no).

Valoraremos la probabilidad y la gravedad de cada uno de los riesgos sobre el tratamiento objeto de análisis.

En el Anexo 6 se encuentran unas tablas para valorar la probabilidad y gravedad de cada riesgo.

7.3.8.3.4. Evaluación de Riesgos

Estimaremos el nivel de riesgo y priorizaremos unos riesgos sobre otros. Priorizaremos aquellos riesgos que sean más elevados o más fácilmente implantarlos.

Para estimar el nivel de riesgos podemos usar una matriz de riesgos o a través de un mapa de riesgos.

Matriz de riesgos: No es más que una tabla en la que en una columna nombraremos el riesgo o amenaza, en otra la probabilidad de que se materialice, en otra la gravedad y finalmente en la última el nivel de riesgo que no será otra cosa más que la suma de ambas cantidades.

Riesgo	Probabilidad	Gravedad	Nivel de Riesgo
Riesgo ejemplo1	Baja	Bajo	Bajo
Riesgo ejemplo2	Baja	Medio	Bajo
Riesgo ejemplo3	Baja	Alto	Bajo
Riesgo ejemplo4	Baja	Muy Alto	Medio
Riesgo ejemplo5	Media	Medio	Medio
Riesgo ejemplo6	Alta	Medio	Medio
Riesgo ejemplo7	Muy Alta	Alto	Alto
Riesgo ejemplo8	Muy Alta	Muy Alto	Muy Alto

Tabla 3: Ejemplo de matriz de riesgos.

Mapa de riesgos: Para su confección pondremos en un eje las probabilidades y en otro eje la gravedad fijaremos un criterio de calor (más rojo o más verde) y en cada celda pondremos el número de riesgos totales en ese nivel. Es más visual así el nivel de riesgos. A modo de ejemplo quedaría.

Probabilidad

Muy alta	4	8	12	16
Alta	3	6	9	12
Media	2	4	6	8
Baja	1	2	3	4
	Baja	**Media**	**Alta**	**Muy Alta**

Gravedad

en los derechos y libertades de las personas físicas

Tabla 4: Mapa de calor de riesgos.

Es decisión de la dirección de la organización qué riesgos se priorizan, aunque en el caso del RGPD tendrán que reducirse todos aquellos que entrañen un nivel de riesgo alto o muy alto. Es importante destacar en este punto que el nivel de riesgo no se promedia, es decir, si tenemos todos los riesgos en un nivel bajo menos uno; y este último está en un nivel muy alto, el resultado de la valoración de riesgos dará como nivel muy alto. El nivel de riesgo resultante será aquel valor más alto.

Ejemplo con una matriz de riesgos.

Riesgo	Probabilidad	Gravedad	Nivel de Riesgo
Riesgo ejemplo1	Baja	Bajo	Bajo
Riesgo ejemplo2	Baja	Bajo	Bajo
Riesgo ejemplo3	Baja	Bajo	Bajo
Riesgo ejemplo4	Baja	Bajo	Bajo
Riesgo ejemplo5	Baja	Bajo	Bajo
Riesgo ejemplo6	Baja	Bajo	Bajo
Riesgo ejemplo7	Baja	Bajo	Bajo
Riesgo ejemplo8	Muy Alta	Muy Alto	Muy Alto

Nivel de riesgo = Muy Alto

Tabla 5: Ejemplo de matriz de riesgos con nivel de riesgo muy alto.

De ahí la importancia de priorizar los riesgos, ya que, aunque tengamos casi todos en niveles bajos uno o unos pocos determinan nuestro nivel real de riesgos.

Este hecho tiene la ventaja que nos permite separar las labores de identificación y valoración de riesgos entre varios miembros del equipo. Dónde unos se centrarían en riesgos de seguridad y otros en riesgos legales por poner un ejemplo.

7.3.8.3.5.Tratamiento de Riesgos. Plan de acción de mitigación de riesgos.

Los riesgos los podemos:

- **Aceptar:** Cuando el riesgo no se considere alto, como organización lo podemos aceptar.

- **Transferir:** Como por ejemplo cubriendo el riesgo con un seguro. En el caso de riesgos contra los derechos y libertades de los afectados esto no será posible. Sólo se pueden transferir los riesgos asociados a pérdidas económicas.
- **Mitigar:** Aplicar medidas para reducirlo.
- **Eliminar:** No llegar a realizar el tratamiento o las operaciones de tratamiento que provocan ese nivel de riesgo.

Aplicaremos medidas de mitigación de riesgos. Las medidas se pueden clasificar de muchas maneras.

- **Organizativas:** Medidas asociadas a procedimientos, a la organización y gobierno de la entidad. En esta tipología de medidas se pueden incluir los procedimientos para ejercer los derechos de las personas físicas, protocolos para gestionar vulnerabilidades e incidentes, ...
- **Legales:** Medidas asociadas al cumplimiento normativo. Por ejemplo, cláusulas para recogida de consentimientos explícitos, ...
- **Técnicas:** Medidas que permiten velar por la seguridad física y lógica de los activos de información. Por ejemplo, controles de acceso, cifrado, ...

Otra clasificación sería:

- **Seguridad de los datos:** Aquellas relacionadas con la seguridad de la información.
- **Cumplimiento:** Aquellas relacionadas con el cumplimiento del RGPD exceptuando las medidas de seguridad de los datos. Medidas jurídicas y organizativas.

Según la metodología MAGERIT otra clasificación sería:

- **Reducen la probabilidad:** Preventivas, Disuasorias, Eliminatorias.
- **Reducen la gravedad:** Minimizadoras, Correctivas, Recuperativas.
- **Reducen probabilidad y gravedad aplicadas con las anteriores:** Monitorización, Detección, Concienciación, Administrativas.

Para nuestra metodología vamos a aplicar la siguiente categorización de medidas:

- **Generales:** Se implantarán a nivel de toda la organización. Repercutirán sobre todos los riesgos de todos los tratamientos. La diferencia entre unos tratamientos y otros será su nivel de madurez.
- **Grupo de riesgos:** Se implantarán a nivel de toda la organización. Repercutirán sobre el grupo de riesgo correspondiente.

En base a estas dos categorías en el Anexo 9 se encuentran listadas las medidas. En nuestro proceso de gestión del riesgo iremos implantando las medidas recogidas en el Anexo 9 y esto nos reducirá el nivel de riesgo. Cada medida tiene un nivel de madurez que sigue los criterios del Esquema nacional de seguridad que a su vez se basa en Modelo de Madurez de Capacidades o CMM (Capability Maturity Model). Estos niveles son:

- **L0 – Inexistente:** En el nivel L0 de madurez no hay nada.
- **L1 - Inicial / ad hoc:** En el nivel L1 de madurez, las salvaguardas existen, pero no se gestionan. El éxito depende de buena suerte. En este caso, las organizaciones exceden con frecuencia presupuestos y tiempos de respuesta.
- **L2 - Reproducible pero intuitivo:** En el nivel L2 de madurez, la eficacia de las salvaguardas depende de la buena suerte y de la buena voluntad de las personas. Los éxitos son repetibles, pero no hay plan para los incidentes más allá de la reacción heroica.
- **L3 - Proceso definido:** Se despliegan y se gestionan las salvaguardas. Hay normativa establecida y procedimientos para garantizar la reacción profesional ante los incidentes. Se ejerce un mantenimiento regular de las protecciones. Las oportunidades de sobrevivir son altas, aunque siempre queda el factor de lo desconocido (o no planificado).
- **L4 – Gestionado y medible:** Usando medidas de campo, la dirección puede controlar empíricamente la eficacia y la efectividad de las salvaguardas. En particular, la dirección puede fijar metas cuantitativas de la calidad. En el nivel L4 de madurez, el funcionamiento de los procesos está bajo control con técnicas estadísticas y cuantitativas. La confianza es cuantitativa, mientras que en el nivel L3, la confianza era solamente cualitativa.
- **L5 – Optimizado:** El nivel L5 de madurez se centra en la mejora continua de los procesos con mejoras tecnológicas incrementales e innovadoras. Se establecen objetivos cuantitativos de mejora de los procesos. Y se revisan continuamente para reflejar los cambios en los objetivos de negocio, utilizándose como indicadores en la gestión de la mejora de los procesos.

La total implantación de todas las medidas generales en un nivel L5 nos reducirán cada uno de los riesgos en un 50%. La total implantación de todas las medidas de grupo de riesgos en un nivel L5 nos reducirán cada riesgo de su grupo en un 50% sobre el riesgo resultante de las medidas generales. Y en función del nivel de madurez su eficacia resultará de la tabla del Anexo 10.

A través de los archivos con tablas dinámicas en Excel que se adjuntan se calcula la mitigación del nivel de riesgo en función de las medidas implantadas y su grado de madurez.

La totalidad de las medidas que se decidan implantar y los plazos y niveles de madurez de la implantación serán la propuesta del plan de acción de mitigación de riesgos, que no es más que un breve resumen de la manera en la que pensamos implantar las medidas de mitigación de riesgo. En cuanto a plazos de revisión se recomienda un plazo de 1 año para tratamientos con precalificación de riesgo alto y de 3 años para los demás tratamientos. El plan de acción de mitigación de riesgos deberá ser supervisado por el DPD en caso de ser una figura obligatoria en la organización.

7.3.8.3.6. Riesgo Residual. Aceptación del riesgo.

Obtendremos un nivel de riesgo residual. Este nivel, es aquél que resulta después implantar el plan de acción de mitigación de riesgos, por tanto, mientras dura la

implantación del plan de acción este nivel de riesgo se irá poco a poco alcanzando. Como criterio general, siempre y cuando el resultado del Análisis de Riesgos suponga que el riesgo residual del tratamiento es alto o muy alto, el responsable del tratamiento debe realizar una consulta a la AEPD. En función de la resolución a la que llegue la AEPD, se establecerán las condiciones y medidas que se deben aplicar para llevar a cabo el tratamiento o, si fuese de aplicación, se indicaría que en ningún caso se podrá llevar a cabo el tratamiento. Por tanto, el criterio de aceptación de riesgo será para aquellos casos en que el nivel de riesgo residual, resultante del plan de acción, sea bajo o medio.

7.3.9. Informe EIPD.

El informe EIPD simplemente es el contenido total de todo el proceso anterior, desde la identificación del tratamiento, hasta la propuesta del plan de acción. Al ser una metodología sistemática la hemos documentado. A mayores se añadirán plazos de revisión de la EIPD que será el mismo plazo que el propuesto en el plan de acción de mitigación de riesgos. Con el paso de los años, y a medida que se realicen revisiones de la EIPD, estas pasarán a formar parte del informe a modo de anexos. En el caso de cambio sustancial de la EIPD, y ser necesario rehacerla, se podría cambiar la versión de la misma y conservar las versiones antiguas durante un plazo de 10 años (orientativo).

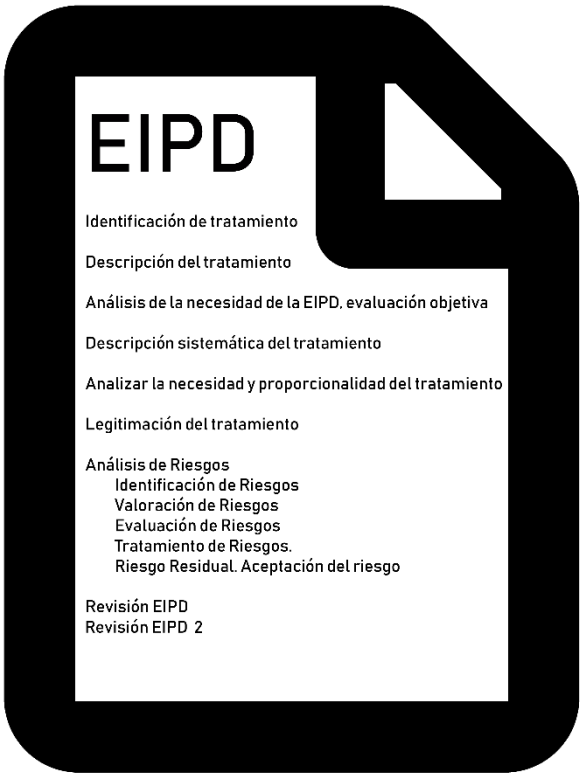

Figura 8: Informe EIPD.

Se puede distinguir entre un informe privado EIPD y un informe público EIPD. La diferencia entre ambos será en que en el primero formará parte todo el contenido de la metodología y en el segundo se hará un resumen con una introducción explicativa sobre lo que es una EIPD y no mencionando en detalle el proceso de Análisis de Riesgos de los

derechos y libertades fundamentales de las personas físicas. Se mencionaría de manera muy resumida para no exponer la seguridad de la organización.

7.3.10. Revisión EIPD.

A través de un cuestionario comprobaremos que la EIPD sigue estando vigente. Este cuestionario de revisión se encuentra en el Anexo 12. Si contestamos alguna de las preguntas del cuestionario como afirmativas tendremos que rehacer la EIPD desde el punto **7.3.5 Descripción sistemática del tratamiento**.

En caso contrario la revisión de la EIPD, a modo de auditoría, constará de las siguientes fases:

7.3.10.1. Requisitos. Alcance

La auditoría se limitará al plan de acción de mitigación de riesgos.

7.3.10.2. Generación de la auditoría

Se realizará una revisión del plan de acción, es decir, si se han implantado todas las medidas propuestas en dicho plan y en qué grado de madurez se encuentran implantadas, y si dicho nivel coincide con el que se ha determinado para la fecha. Es importante destacar que estas medidas se revisarán in situ, no aceptando los niveles de madurez alcanzados que proponga la organización. Si los grados de madurez de las medidas de seguridad implantadas en el plan de acción de mitigación de riesgos están muy por debajo de los necesarios para alcanzar un nivel de riesgo residual aceptable, será necesario hacer un informe de no conformidad. Para ello determinamos como umbral de aplicabilidad el 90% del total de medidas tanto los controles generales como de los específicos de grupo, y al menos un 50% de cada uno de los controles. Si existe no conformidad podrá ser a nivel de todos los controles, por tanto, no subsanable o a nivel de un único control, por tanto, subsanable. Si al final se determina no conformidad para la auditoría, debe informarse al responsable del tratamiento y al DPD de la organización (este último de existir).

7.3.10.3. Generación del informe de auditoría

Nuevamente el informe constará de la documentación por escrito de todo el proceso que hemos realizado en la fase anterior, junto con un apartado sobre el seguimiento de la auditoría en el que propondremos nuevos plazos de revisión de la EIPD en caso de que dicha auditoría sea conforme, en caso contrario propondríamos plazos y medidas de subsanación.

7.3.10.4. Seguimiento de la auditoría

También esta fase incorpora un mantenimiento del informe de EIPD, ya que si se produce una modificación en algunos de los aspectos que han servido de base para la realización del informe, este tendrá que ser actualizado en base a dicha modificación. También habrá que tener en cuenta que este mantenimiento del informe se deberá realizar si el tratamiento sufre alguna modificación sustancial que implique esta necesidad: nuevas operaciones de tratamiento, nuevos datos tratados, nuevos riesgos identificados, posibles cambios en la valoración inicial de los riesgos.

8. Caso práctico.

Nuestro caso práctico es un ejemplo ficticio. Será un centro sanitario donde se realizan tratamientos de fisioterapia, psicología e impartición de cursos. Hay personal contratado y empresas (autónomos) que prestan sus servicios.

No vamos a realizar un ejercicio práctico de implantación de RGPD en dicho ejemplo ficticio. Vamos a seleccionar uno o varios tratamientos y realizar todo el proceso de Evaluación de Impacto relativa a la Protección de Datos. Por tanto, no forma parte de este proceso determinar los mecanismos para identificar todos los posibles tratamientos, ni conocer el contexto del centro del ejemplo ficticio.

8.1. Tratamiento recursos humanos.

8.1.1. Identificación de tratamiento.

Título del tratamiento: Recursos humanos

8.1.2. Descripción del tratamiento

Los objetivos perseguidos por el tratamiento son: la gestión de los aspectos relacionados con el personal.

Finalidades:

- Gestión de personal.
- Control horario.
- Emisión de la nómina del personal.

8.1.3. Análisis de la necesidad de la EIPD, evaluación objetiva

Este tratamiento con casi total seguridad podríamos decir que no necesita una EIPD, pero como el objetivo de este TFM es mostrar mediante ejemplos dicho proceso vamos adelante.

Revisamos que no es obligatoria según los criterios del artículo 35.3 del RGPD.

Revisamos si cumple con alguno de los criterios del CEPD conforme existe un alto riesgo.

Revisamos si existe un “mayor riesgo” según el artículo 28.2 de la LOPDGDD.

Revisamos si se encuentra en el listado de la AEPD.

Revisamos si se encuentra en el listado de las autoridades de control de protección de datos europeas.

De aquí escribiríamos unas conclusiones con la motivación de hacer la EIPD.

8.1.4. Ciclo de vida de los datos

Cubrimos, mediante una tabla los distintos tipos de datos detectados en este tratamiento con el cliente.

Recogida de información sobre los datos						
Datos personales facilitados directamente por las personas afectadas						
Descripción	Categorías Especiales	Ciclo de vida de los datos				
		Recoger	Almacenar	Utilizar	Transferir	Borrar
DNI		X	X	X	X	X
Nombre		X	X	X	X	X
Apellidos		X	X	X	X	X
Dirección postal		X	X	X		X
Teléfono		X	X	X		X
Firma manuscrita		X	X	X		X
Firma electrónica		X	X	X		X
Nº SS / Mutualidad		X	X	X	X	X
Correo electrónico		X	X	X		X
Datos de estado civil		X	X	X	X	X
Datos de familia		X	X	X	X	X
Fecha de nacimiento		X	X	X	X	X
Sexo		X	X	X	X	X
Formación, titulaciones		X	X	X		X
Experiencia profesional		X	X	X		X
Pertenencia a colegios o a asociaciones		X	X	X		X
Profesión		X	X	X		X
Puestos de trabajo		X	X	X		X
Historial del trabajado		X	X	X		X
Datos bancarios		X	X	X	X	X
Datos económicos de nómina		X	X	X	X	X
Datos deducciones impositivas/impuestos		X	X	X	X	X
Motivo de ausencia		X	X	X		X
Datos sobre sanciones		X	X	X		X
Discapacidad	X	X	X	X	X	X
Datos personales calculados						
Fecha/hora entrada		X	X	X		X
Fecha/hora salida		X	X	X		X

Tabla 6: Ciclo de vida de los datos. Caso práctico tratamiento recursos humanos.

	Recoger	Almacenar	Utilizar	Transferir	Borrar
Intervinientes	Interesado; Responsable tratamiento	Responsable tratamiento	Responsable tratamiento	Gestoría	Responsable tratamiento
Operaciones de tratamiento	Alta trabajador Registro de acceso	Almacenamiento	Consulta	Emisión de nómina	Baja trabajador
Tecnologías	Programa fichaje pc; BBDD trabajadores	BBDD trabajadores	Programa fichaje pc; BBDD trabajadores	Pendrive	

Tabla 7: Ciclo de vida de los datos. Caso práctico tratamiento recursos humanos.

8.1.5. Analizar la necesidad y proporcionalidad del tratamiento.

8.1.5.1. Necesidad del tratamiento.

Su finalidad no puede alcanzarse "razonablemente" por otros medios ya que se necesitan los datos personales para el tratamiento. No es posible su gestión sin los datos recabados.

8.1.5.2. Proporcionalidad del tratamiento.

No existe otra forma más moderada o menos invasiva para conseguir los fines del tratamiento. Se recaban los datos mínimos legales para cubrir las nóminas y controlar que el personal realice las tareas asignadas.

8.1.6. Legitimación del tratamiento.

La legitimación de este tratamiento la obtenemos de los supuestos del artículo 6.1.a y en caso de datos de categoría especial, levantaremos la prohibición con las excepciones de los supuestos del artículo 9.2.a.

RGPD: 6.1.b. Tratamiento necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales.

RGPD: 6.1.c. Tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.

RGPD: 9.2.b. el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;

8.1.7. Análisis de Riesgos de los derechos y libertades fundamentales de las personas físicas.

8.1.7.1. Identificación de Riesgos.

Partimos del listado de riesgos del Anexo 4 y por tanto no los necesitamos identificar. Aun así, se recomienda hacer siempre hacer el ejercicio de revisar el Anexo 5 de cara a identificar nuevos riesgos para completar el listado óptimo de cada organización.

8.1.7.2. Valoración de Riesgos

Riesgo	Aplica	Probabilidad	Gravedad	NIVEL
La base que legitima el tratamiento no es adecuada, es ilícita o no se ha formalizado adecuadamente	SI	BAJA	MEDIA	BAJO
No se ha ponderado adecuadamente el interés legítimo en relación con los intereses, derechos y libertades fundamentales del interesado	NO			
Las finalidades del tratamiento no son precisas, son ilegítimas, etc.	SI	BAJA	MEDIA	BAJO
Hay un cambio de finalidad que puede ser incompatible con la finalidad original	SI	BAJA	ALTA	BAJO
No obtener el consentimiento a través de una clara acción afirmativa	NO			
No se permite retirar el consentimiento	NO			
No utilizar medios que permitan demostrar que el interesado prestó su consentimiento	NO			
Se recogen datos inadecuados, no pertinentes, excesivos o innecesarios para la finalidad prevista	SI	BAJA	ALTA	BAJO
Se registran datos inexactos o no se mantienen actualizados	SI	MEDIA	ALTA	MEDIO
Los datos personales se conservan más tiempo del necesario	SI	BAJA	MEDIA	BAJO
Los datos se tratan de manera desleal o poco transparente (no se cumple la expectativa de la persona interesada respecto del tratamiento de sus datos)	SI	BAJA	ALTA	BAJO
Se hacen operaciones de tratamiento desproporcionadas	SI	BAJA	MEDIA	BAJO
En la recogida de datos no se proporciona la información mínima al afectado	SI	BAJA	MEDIA	BAJO
La respuesta al ejercicio del derecho de acceso no se hace en el tiempo y la forma adecuados	SI	BAJA	ALTA	BAJO
La respuesta al ejercicio del derecho de rectificación no se hace en el tiempo y la forma adecuados	SI	MUY ALTA	MUY ALTA	MUY ALTO
La respuesta al ejercicio del derecho de supresión no se hace en el tiempo y la forma adecuados	SI	BAJA	MEDIA	BAJO
La respuesta al ejercicio del derecho a la limitación del tratamiento no se hace en el tiempo y la forma adecuados	SI	BAJA	MEDIA	BAJO
La respuesta al ejercicio del derecho de portabilidad de los datos no se hace en el tiempo y la forma adecuados	SI	BAJA	MEDIA	BAJO
La respuesta al ejercicio del derecho de oposición no se hace en el tiempo y la forma adecuados	SI	BAJA	MEDIA	BAJO
Se toman decisiones que afectan a una persona utilizando exclusivamente medios automatizados	NO			
No hay procedimientos para dar una respuesta adecuada a los derechos	SI	MUY ALTA	ALTA	ALTO
La organización desconoce los procedimientos para responder el ejercicio de derechos	SI	ALTA	ALTA	ALTO
No se verifica adecuadamente la identidad de la persona que ejerce un derecho	NO			
Se incumple la regulación general sobre el derecho a la protección de los datos de carácter personal	SI	BAJA	ALTA	BAJO
Se incumplen otras regulaciones sectoriales que inciden en la protección de los datos de carácter personal	SI	BAJA	MEDIA	BAJO
Se incumplen las cláusulas sobre la protección de datos incorporados a los contratos o condiciones de uso	SI	MEDIA	ALTA	MEDIO
Se incumplen estipulaciones recogidas en un código de conducta (si se está adherido)	NO			
No se puede demostrar el cumplimiento (responsabilidad proactiva)	SI	MEDIA	ALTA	MEDIO
Las limitaciones del tratamiento no se comunican a terceros	NO			
Las certificaciones o sellos de protección de datos no se han renovado o han perdido vigencia	NO			
Hay transferencia internacional de datos no autorizada o desconocida	NO			
Los encargados de tratamiento no se han seleccionado adecuadamente	SI	MEDIA	ALTA	MEDIO

No se ha formalizado adecuadamente la relación con los encargados de tratamientos	SI	MEDIA	ALTA	MEDIO
No se ejerce suficiente control sobre la actividad del encargado de tratamiento (en las operaciones de tratamiento que le han sido encargadas)	SI	ALTA	ALTA	ALTO
Se desconocen las cadenas de subcontratación de los encargados de tratamiento	SI	MUY ALTA	ALTA	ALTO
Hay destrucción o pérdida accidental de datos personales	SI	MEDIA	ALTA	MEDIO
Hay destrucción malintencionada de datos personales	SI	BAJA	ALTA	BAJO
Hay alteración no autorizada de datos personales	SI	BAJA	ALTA	BAJO
Hay comunicación no autorizada de datos personales	SI	MEDIA	ALTA	MEDIO
Hay acceso no autorizado a datos personales	SI	MEDIA	ALTA	MEDIO
Los sistemas de información no están disponibles	SI	BAJA	MEDIA	BAJO
Hay incapacidad para detectar y gestionar incidentes que afectan a la seguridad de los datos	SI	MUY ALTA	ALTA	ALTO
Las violaciones de datos no se notifican en el tiempo y la forma adecuados (data breach)	SI	MUY ALTA	ALTA	ALTO
Las violaciones de datos no se comunican en el tiempo y la forma adecuados (data breach)	SI	MUY ALTA	ALTA	ALTO
No se ha designado delegado de protección de datos (si es obligatorio)	NO			
No se proporcionan medios suficientes al delegado de protección de datos	NO			
No se atiende un requerimiento de la autoridad de supervisión competente	SI	BAJA	ALTA	BAJO
No se ha hecho una consulta previa a la autoridad de supervisión, cuando era necesaria	SI	MUY ALTA	ALTA	ALTO
No se ha tenido en cuenta la protección de datos en el momento de diseñar el tratamiento	SI	MUY ALTA	ALTA	ALTO
No se ha incorporado la protección de datos por defecto en las operaciones de tratamiento	SI	MUY ALTA	ALTA	ALTO

Tabla 8: Valoración de riesgos. Caso práctico tratamiento recursos humanos.

8.1.7.3. Evaluación de Riesgos

Del análisis y posterior valoración de riesgos podemos deducir que el nivel de riesgo del tratamiento es bajo o medio.

El mapa de calor de riesgos quedaría.

Riesgo Inherente				
Muy alta	0	0	0	0
Alta	0	3	0	0
Media	0	0	16	0
Baja	0	12	7	0
	Bajo	**Medio**	**Alto**	**Muy Alto**

Tabla 9: Mapa de calor riesgo inherente. Caso práctico tratamiento recursos humanos.

Al no haber riesgos con nivel alto o muy alto la dirección podría aceptar los riesgos y finalizar el AARR. En caso contrario procederá al tratamiento de los riesgos.

8.1.7.4. Tratamiento de Riesgos

El plan de acción de mitigación de riesgos consistirá en la implementación de todos los controles generales en un nivel de madurez L3 y de todos los controles específicos de

grupo (salvo el grupo DPO) en un nivel de madurez L2. El plazo para alcanzar estos niveles de madurez se establece en un año.

Para este tratamiento en concreto no sería necesario este plan de acción. Para organizaciones pequeñas el plan de acción de mitigación de riesgos será igual para todos los tratamientos. Del proceso de implantación de medidas se acompaña archivo adjunto ***Riesgos Tratamiento Recursos Humanos.xlsx*** para poder gestionar el grado de eficacia del plan de acción. A modo de ejemplo para un instante determinado, el resultado se muestra en la siguiente imagen. Esta sería la foto fija de un momento determinado de la gestión de riesgos.

Riesgo Residual				
	50	0	0	0
	Bajo	Medio	Alto	Muy Alto

Tabla 10: Mapa de calor riesgo residual. Caso práctico tratamiento recursos humanos.

8.1.7.5. Riesgo Residual. Aceptación del riesgo

En el caso de este tratamiento el riesgo residual resultante será bajo por lo que la dirección puede aceptar el nivel de riesgo y por tanto no será necesario realizar consulta a la AEPD.

8.1.8. Informe EIPD

Todo el contenido desde el punto 9.1.1 Identificación de tratamiento y a mayores el plazo de revisión de la EIPD que sería el mismo propuesto en el plan de acción de mitigación de riesgos, en este caso un año.

8.1.9. Revisión EIPD.

Esta revisión se propuso hacerla un año después de la EIPD. Supongamos que ha pasado un año y estamos en el plazo de realización de la revisión.

Primeramente, responderemos al cuestionario de revisión de EIPD.

Pregunta	Si/No
Se produjeron cambios en las leyes y regulaciones relacionadas con la protección de datos	NO
Se produjeron cambios en las políticas y estándares internos relacionados con el tratamiento	NO
Se produjeron cambios en el sistema de información en el que se tratan los datos personales	NO
Se produjeron cambios en las finalidades y los medios para el tratamiento de los datos	NO
Se produjeron nuevos flujos de datos o se modificaron los existentes	NO
Se produjo una expansión del negocio o una nueva adquisición	NO

Tabla 11: Cuestionario de revisión EIPD. Caso práctico tratamiento recursos humanos.

Por tanto, no será necesario rehacer la EIPD.

8.1.9.1. Requisitos. Alcance

La auditoría se limitará al plan de acción de mitigación de riesgos del tratamiento recursos humanos.

8.1.9.2. Generación de la auditoría

Procedemos a revisar las medidas implantadas y su grado de madurez. A modo de ejemplo ficticio de caso práctico vamos a determinar el siguiente resultado.

Tras revisar todos los controles del plan de mitigación de riesgos obtenemos una aplicabilidad general:

Aplicabilidad	
Controles generales	95,77%
Controles de grupo	90,86%

Tabla 12: Aplicabilidad. Caso práctico tratamiento recursos humanos.

Se acompaña archivo adjunto ***Riesgos Tratamiento Recursos Humanos.xlsx*** para consultar la aplicabilidad de cada uno de los controles.

8.1.9.3. Generación del informe de auditoría

Después de las pruebas realizadas, es indicada una serie de recomendaciones a ser aplicadas en la organización y en los sistemas auditados.

Se ha comprobado que el nivel de aplicabilidad tanto para los controles generales como para los específicos es superior al 90% que es el umbral de aplicabilidad solicitado.

También se ha comprobado que el nivel de aplicabilidad para cada uno de los controles es superior al 50% salvo para los siguientes controles.

Control/medida	Nivel Madurez Inicial	Nivel Madurez Actual	Nivel de Madurez Propuesto	Aplicabilidad
Registro de entrada salida	L0	L1	L3	11,11%
Procedimiento de consultas	L0	L1	L2	20,00%
Registro de consultas	L0	L1	L2	20,00%
Procedimiento para establecer medidas de cumplimiento respecto a los nuevos tratamientos de datos desde el inicio de la activad y durante el ciclo de vida	L0	L1	L2	20,00%
Procedimiento de Evaluación Objetiva para precalificar el riesgo	L0	L1	L2	20,00%

Tabla 13: No conformidades subsanables. Caso práctico tratamiento recursos humanos.

Por tanto, se considera la auditoría **no conforme subsanable**. Se propone un plazo de tres meses para la subsanación de los controles de la tabla anterior.

Se acompaña archivo adjunto ***Riesgos Tratamiento Recursos Humanos.xlsx*** con resultado de aplicabilidad para los controles.

8.1.9.4. Seguimiento de la auditoría

Siempre y cuando las no conformidades del informe anterior sean subsanadas en plazo, se fija un plazo ordinario de revisión de auditoría y de EIPD de dos años.

8.2. Tratamiento gestión de pacientes.

8.2.1. Identificación de tratamiento.

Título del tratamiento: Gestión de pacientes.

8.2.2. Descripción del tratamiento

Los objetivos perseguidos por el tratamiento son: la gestión de los aspectos relacionados con el historial del paciente.

Finalidades:

- Gestión de los servicios médicos a los pacientes.

8.2.3. Análisis de la necesidad de la EIPD, evaluación objetiva

Revisamos que no es obligatoria según los criterios del artículo 35.3 del RGPD.

El tratamiento no encaja en ninguno de los tres supuestos.

Revisamos si cumple con alguno de los criterios del CEPD conforme existe un alto riesgo.

- *Datos sensibles o datos muy personales:* El tratamiento puede recabar esta tipología de datos debido a que la clínica presta servicios de psicología y fisioterapia.

Revisamos si existe un "mayor riesgo" según el artículo 28.2 de la LOPDGDD.

Obtenemos dos supuestos del artículo que encajan con mayores riesgos:

a) Cuando el tratamiento pudiera generar situaciones 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, moral o social significativo para los afectados.

Hay un **mayor riesgo** de pérdida de confidencialidad de datos de categoría especial.

h) Cualesquiera otros que a juicio del responsable o del encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación.

Este apartado es de interpretación muy libre y para este caso vamos a considerarlo como que se da.

Revisamos si se encuentra en el listado de la AEPD. No encontramos coincidencias.

Revisamos si está en la lista de Tratamientos identificados por las autoridades de control de protección de datos europeas. No encontramos coincidencias.

Por tanto, concluimos que, aunque no se dan varios supuestos claros que confirmen que estamos ante un riesgo alto, existen dudas razonables que recomiendan llevarlo a cabo debido al tratamiento de datos de categoría especial.

8.2.4. Ciclo de vida de los datos

Cubrimos, mediante una tabla los distintos tipos de datos detectados en este tratamiento con el cliente.

Recogida de información sobre los datos						
Datos personales facilitados directamente por las personas afectadas						
Descripción	Categorías Especiales	Ciclo de vida de los datos				
		Recoger	Almacenar	Utilizar	Transferir	Borrar
DNI		**X**	**X**	**X**		**X**
Nombre		X	X	X		X
Apellidos		X	X	X		X
Dirección postal		X	X	X		X
Teléfono		X	X	X		X
Firma manuscrita		X	X	X		X
Firma electrónica		X	X	X		X
Imagen / voz		X	X	X		X
Correo electrónico		X	X	X		X
Marcas físicas		X	X	X		X
Datos de estado civil		X	X	X		X
Fecha de nacimiento		X	X	X		X
Sexo		X	X	X		X
Datos de familia		X	X	X		X
Lugar de nacimiento		X	X	X		X
Edad		X	X	X		X
Nacionalidad		X	X	X		X
Lengua Materna		X	X	X		X
Características físicas o antropométricas		X	X	X		X
Características de alojamiento, vivienda		X	X	X		X
Situación militar		X	X	X		X
Propiedades, posesiones		X	X	X		X
Aficiones y estilo de vida		X	X	X		X
Pertenencia a clubes, asociaciones		X	X	X		X
Formación, titulaciones.		X	X	X		X
Historial del estudiante.		X	X	X		X
Experiencia profesional		X	X	X		X
Profesión.		X	X	X		X
Ingresos y rentas		X	X	X		X
Subsidios, beneficios		X	X	X		X
Hábitos de consumo		X	X	X		X
Intereses		X	X	X		X
Preferencias		X	X	X		X
Opiniones políticas	**X**	X	X	X		X
Afiliación sindical	**X**	X	X	X		X
Convicciones religiosas	**X**	X	X	X		X
Convicciones filosóficas	**X**	X	X	X		X
Origen racial o étnico	**X**	X	X	X		X
Datos relativos a la salud	**X**	X	X	X		X
Vida sexual	**X**	X	X	X		X

Datos genéticos.	**X**	X	X	X		X
Datos biométricos.	**X**	X	X	X		X
Orientación sexual.	**X**	X	X	X		X
Estado fisiológico.	**X**	X	X	X		X
Necesidades educativas especiales	**X**	X	X	X		X
Discapacidades físicas e intelectuales	**X**	X	X	X		X

Tabla 14: Ciclo de vida de los datos. Caso práctico tratamiento gestión de pacientes.

	Recoger	Almacenar	Utilizar	Transferir	Borrar
Intervinientes	Interesado; Responsable tratamiento; Encargados tratamiento	Responsable tratamiento; Encargados tratamiento	Responsable tratamiento; Encargados tratamiento	Encargados tratamiento	Responsable tratamiento
Operaciones de tratamiento	Formularios que rellenan los pacientes en la consulta; Datos recabados por los especialistas	Información almacenada	Gestión de los servicios médicos a los pacientes	Prestación de servicios médicos	Destrucción de la información
Tecnologías	BB DD	BBDD	BBDD	BBDD	

Tabla 15: Ciclo de vida de los datos. Caso práctico tratamiento gestión de pacientes.

8.2.5. Analizar la necesidad y proporcionalidad del tratamiento.

8.2.5.1. Necesidad del tratamiento.

Su finalidad no puede alcanzarse "razonablemente" por otros medios ya que se necesitan los datos personales para el tratamiento. Los datos de salud recabados son necesarios para la llevanza del historial médico fisioterapéutico y los demás datos son necesarios para realizar la psicoterapia.

8.2.5.2. Proporcionalidad del tratamiento.

No existe otra forma más moderada o menos invasiva para conseguir los fines del tratamiento. Se recaban los datos mínimos para prestar el servicio.

8.2.6. Legitimación del tratamiento.

La legitimación de este tratamiento la obtenemos de los supuestos del artículo 6.1.a y en caso de datos de categoría especial, levantaremos la prohibición con las excepciones de los supuestos del artículo 9.2.a.

RGPD: 6.1.a. el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos.

RGPD: 9.2.a. el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;

8.2.7. Análisis de Riesgos de los derechos y libertades fundamentales de las personas físicas.

8.2.7.1. Identificación de Riesgos.

Partimos otra vez del listado de riesgos del Anexo 4 y por tanto no los necesitamos identificar. Volvemos a recordar que se recomienda hacer siempre el ejercicio de revisar el Anexo 5 de cara a identificar nuevos riesgos para completar el listado óptimo de cada organización.

8.2.7.2. Valoración de Riesgos.

Procedemos a valorar los riesgos y por tanto obtener su nivel de riesgo.

Riesgo	Aplica	Probabilidad	Gravedad	NIVEL
La base que legitima el tratamiento no es adecuada, es ilícita o no se ha formalizado adecuadamente	SI	MEDIA	ALTA	MEDIO
No se ha ponderado adecuadamente el interés legítimo en relación con los intereses, derechos y libertades fundamentales del interesado	NO			
Las finalidades del tratamiento no son precisas, son ilegítimas, etc.	SI	MEDIA	ALTA	MEDIO
Hay un cambio de finalidad que puede ser incompatible con la finalidad original	SI	MEDIA	MUY ALTA	MEDIO
No obtener el consentimiento a través de una clara acción afirmativa	SI	MEDIA	ALTA	MEDIO
No se permite retirar el consentimiento	SI	MEDIA	ALTA	MEDIO
No utilizar medios que permitan demostrar que el interesado prestó su consentimiento	SI	MEDIA	ALTA	MEDIO
Se recogen datos inadecuados, no pertinentes, excesivos o innecesarios para la finalidad prevista	SI	MEDIA	MUY ALTA	MEDIO
Se registran datos inexactos o no se mantienen actualizados	SI	ALTA	MUY ALTA	ALTO
Los datos personales se conservan más tiempo del necesario	SI	ALTA	ALTA	ALTO
Los datos se tratan de manera desleal o poco transparente (no se cumple la expectativa de la persona interesada respecto del tratamiento de sus datos)	SI	MEDIA	MUY ALTA	MEDIO
Se hacen operaciones de tratamiento desproporcionadas	SI	MEDIA	ALTA	MEDIO
En la recogida de datos no se proporciona la información mínima al afectado	SI	MEDIA	ALTA	MEDIO
La respuesta al ejercicio del derecho de acceso no se hace en el tiempo y la forma adecuados	SI	MEDIA	MUY ALTA	MEDIO
La respuesta al ejercicio del derecho de rectificación no se hace en el tiempo y la forma adecuados	SI	MUY ALTA	MUY ALTA	MUY ALTO
La respuesta al ejercicio del derecho de supresión no se hace en el tiempo y la forma adecuados	SI	MEDIA	ALTA	MEDIO
La respuesta al ejercicio del derecho a la limitación del tratamiento no se hace en el tiempo y la forma adecuados	SI	MEDIA	ALTA	MEDIO
La respuesta al ejercicio del derecho de portabilidad de los datos no se hace en el tiempo y la forma adecuados	SI	MEDIA	ALTA	MEDIO
La respuesta al ejercicio del derecho de oposición no se hace en el tiempo y la forma adecuados	SI	MEDIA	ALTA	MEDIO
Se toman decisiones que afectan a una persona utilizando exclusivamente medios automatizados	NO			
No hay procedimientos para dar una respuesta adecuada a los derechos	SI	MUY ALTA	MUY ALTA	MUY ALTO

La organización desconoce los procedimientos para responder el ejercicio de derechos	SI	MUY ALTA	MUY ALTA	MUY ALTO
No se verifica adecuadamente la identidad de la persona que ejerce un derecho	SI	BAJA	MUY ALTA	MEDIO
Se incumple la regulación general sobre el derecho a la protección de los datos de carácter personal	SI	MEDIA	MUY ALTA	MEDIO
Se incumplen otras regulaciones sectoriales que inciden en la protección de los datos de carácter personal	SI	MEDIA	ALTA	MEDIO
Se incumplen las cláusulas sobre la protección de datos incorporados a los contratos o condiciones de uso	SI	ALTA	MUY ALTA	ALTO
Se incumplen estipulaciones recogidas en un código de conducta (si se está adherido)	SI	BAJA	MUY ALTA	MEDIO
No se puede demostrar el cumplimiento (responsabilidad proactiva)	SI	ALTA	MUY ALTA	ALTO
Las limitaciones del tratamiento no se comunican a terceros	NO			
Las certificaciones o sellos de protección de datos no se han renovado o han perdido vigencia	NO			
Hay transferencia internacional de datos no autorizada o desconocida	NO			
Los encargados de tratamiento no se han seleccionado adecuadamente	SI	ALTA	MUY ALTA	ALTO
No se ha formalizado adecuadamente la relación con los encargados de tratamientos	SI	ALTA	MUY ALTA	ALTO
No se ejerce suficiente control sobre la actividad del encargado de tratamiento (en las operaciones de tratamiento que le han sido encargadas)	SI	MUY ALTA	MUY ALTA	MUY ALTO
Se desconocen las cadenas de subcontratación de los encargados de tratamiento	SI	MUY ALTA	MUY ALTA	MUY ALTO
Hay destrucción o pérdida accidental de datos personales	SI	ALTA	MUY ALTA	ALTO
Hay destrucción malintencionada de datos personales	SI	MEDIA	MUY ALTA	MEDIO
Hay alteración no autorizada de datos personales	SI	MEDIA	MUY ALTA	MEDIO
Hay comunicación no autorizada de datos personales	SI	ALTA	MUY ALTA	ALTO
Hay acceso no autorizado a datos personales	SI	ALTA	MUY ALTA	ALTO
Los sistemas de información no están disponibles	SI	MEDIA	ALTA	MEDIO
Hay incapacidad para detectar y gestionar incidentes que afectan a la seguridad de los datos	SI	MUY ALTA	MUY ALTA	MUY ALTO
Las violaciones de datos no se notifican en el tiempo y la forma adecuados (data breach)	SI	MUY ALTA	MUY ALTA	MUY ALTO
Las violaciones de datos no se comunican en el tiempo y la forma adecuados (data breach)	SI	MUY ALTA	MUY ALTA	MUY ALTO
No se ha designado delegado de protección de datos (si es obligatorio)	NO			
No se proporcionan medios suficientes al delegado de protección de datos	NO			
No se atiende un requerimiento de la autoridad de supervisión competente	SI	MEDIA	MUY ALTA	MEDIO
No se ha hecho una consulta previa a la autoridad de supervisión, cuando era necesaria	SI	MUY ALTA	MUY ALTA	MUY ALTO
No se ha tenido en cuenta la protección de datos en el momento de diseñar el tratamiento	SI	MUY ALTA	MUY ALTA	MUY ALTO
No se ha incorporado la protección de datos por defecto en las operaciones de tratamiento	SI	MUY ALTA	MUY ALTA	MUY ALTO

Tabla 16: Valoración de riesgos. Caso práctico tratamiento gestión de pacientes.

8.2.7.3. Evaluación de Riesgos

Del análisis y posterior valoración de riesgos podemos deducir que el nivel de riesgo del tratamiento es alto o muy alto.

El mapa de calor quedaría:

Riesgo Inherente				
Muy alta	0	0	0	11
Alta	0	0	1	8
Media	0	0	13	8
Baja	0	0	0	2
	Bajo	Medio	Alto	Muy Alto

Tabla 17: Mapa de calor riesgo inherente. Caso práctico tratamiento gestión de pacientes.

No se pueden aceptar los riesgos y se procederá al tratamiento de los mismos, priorizando aquellos con un nivel más alto.

8.2.7.4. Tratamiento de Riesgos

El plan de acción de mitigación de riesgos consistirá en la implementación de todos los controles generales en un nivel de madurez L3 y de todos los controles específicos de grupo (salvo el grupo DPO) en un nivel de madurez L2. El plazo para alcanzar estos niveles de madurez se establece en un año.

Para organizaciones pequeñas el plan de acción de mitigación de riesgos será igual para todos los tratamientos. Del proceso de implantación de medidas Se acompaña archivo adjunto ***Riesgos Tratamiento Pacientes.xlsx*** para poder gestionar el grado de eficacia del plan de acción. A modo de ejemplo para un instante determinado, el resultado se muestra en la siguiente imagen. Esta sería la foto fija de un momento determinado de la gestión de riesgos.

Riesgo Residual				
	34	16	0	0
	Bajo	Medio	Alto	Muy Alto

Tabla 18: Mapa de calor riesgo residual. Caso práctico tratamiento gestión de pacientes.

8.2.7.5. Riesgo Residual. Aceptación del riesgo

En el caso de este tratamiento el riesgo residual resultante será bajo o medio por lo que la dirección puede aceptar el nivel de riesgos.

8.2.8. Informe EIPD

Todo el contenido desde el punto 9.2.1 Identificación de tratamiento y a mayores el plazo de revisión de la EIPD que sería el mismo propuesto en el plan de acción de mitigación de riesgos, en este caso un año.

8.2.9. Revisión EIPD.

Esta revisión se propuso hacerla un año después de la EIPD. Supongamos que ha pasado un año y estamos en el plazo de realización de la revisión.

Primeramente, responderemos al cuestionario de revisión de EIPD.

Pregunta	Si/No
Se produjeron cambios en las leyes y regulaciones relacionadas con la protección de datos	NO
Se produjeron cambios en las políticas y estándares internos relacionados con el tratamiento	NO
Se produjeron cambios en el sistema de información en el que se tratan los datos personales	NO
Se produjeron cambios en las finalidades y los medios para el tratamiento de los datos	NO
Se produjeron nuevos flujos de datos o se modificaron los existentes	NO
Se produjo una expansión del negocio o una nueva adquisición	NO

Tabla 19: Cuestionario de revisión EIPD. Caso práctico tratamiento gestión de pacientes.

Por tanto, no será necesario rehacer la EIPD.

8.2.9.1. Requisitos. Alcance

La auditoría se limitará al plan de acción de mitigación de riesgos del tratamiento recursos humanos.

8.2.9.1. Generación de la auditoría

Procedemos a revisar las medidas implantadas y su grado de madurez. A modo de ejemplo ficticio de caso práctico vamos a determinar el siguiente resultado.

Tras revisar todos los controles del plan de mitigación de riesgos obtenemos una aplicabilidad general:

Aplicabilidad	
Controles generales	95,77%
Controles de grupo	90,86%

Tabla 20: Aplicabilidad. Caso práctico tratamiento gestión de pacientes.

Se acompaña archivo adjunto ***Riesgos Tratamiento Gestion de Pacientes.xlsx*** para consultar la aplicabilidad de cada uno de los controles.

8.2.9.2. Generación del informe de auditoría

Después de las pruebas realizadas, es indicada una serie de recomendaciones a ser aplicadas en la organización y en los sistemas auditados.

Se ha comprobado que el nivel de aplicabilidad tanto para los controles generales como para los específicos es superior al 90% que es el umbral de aplicabilidad solicitado.

También se ha comprobado que el nivel de aplicabilidad para cada uno de los controles es superior al 50% salvo para los siguientes controles.

Control/medida	Nivel Madurez Inicial	Nivel Madurez Actual	Nivel de Madurez Propuesto	Aplicabilidad
Registro de entrada salida	L0	L1	L3	11,11%
Procedimiento de consultas	L0	L1	L2	20,00%
Registro de consultas	L0	L1	L2	20,00%
Procedimiento para establecer medidas de cumplimiento respecto a los nuevos tratamientos de datos desde el inicio de la activad y durante el ciclo de vida	L0	L1	L2	20,00%
Procedimiento de Evaluación Objetiva para precalificar el riesgo	L0	L1	L2	20,00%

Tabla 21: No conformidades subsanables. Caso práctico tratamiento gestión de pacientes.

Por tanto, se considera la auditoría **no conforme subsanable**. Se propone un plazo de tres meses para la subsanación de los controles de la tabla anterior.

Se acompaña archivo adjunto ***Riesgos Tratamiento Gestión de Pacientes.xlsx*** con resultado de aplicabilidad para los controles.

8.2.9.3. Seguimiento de la auditoría

Siempre y cuando las no conformidades del informe anterior sean subsanadas en plazo, se fija un plazo ordinario de revisión de auditoría y de EIPD de dos años.

8.3. Tratamiento formación

8.3.1. Identificación de tratamiento.

Título del tratamiento: Formación

8.3.2. Descripción del tratamiento

Los objetivos perseguidos por el tratamiento son: la gestión de los alumnos que asisten a las distintas clases y talleres impartidos en el centro.

Finalidades:

- Gestión datos alumnos.
- Control actividades formativas.

8.3.3. Análisis de la necesidad de la EIPD, evaluación objetiva

Este tratamiento con casi total seguridad podríamos decir que no necesita una EIPD, pero como el objetivo de este TFM es mostrar mediante ejemplos dicho proceso vamos adelante.

Revisamos que no es obligatoria según los criterios del artículo 35.3 del RGPD.

Revisamos si cumple con alguno de los criterios del CEPD conforme existe un alto riesgo.

Revisamos si existe un “mayor riesgo” según el artículo 28.2 de la LOPDGDD.

Revisamos si se encuentra en el listado de la AEPD.

Revisamos si se encuentra en el listado de las ACPD.

De aquí escribiríamos unas conclusiones con la motivación de hacer la EIPD.

8.3.4. Ciclo de vida de los datos

Cubrimos, mediante una tabla los distintos tipos de datos detectados en este tratamiento con el cliente.

Recogida de información sobre los datos						
Datos personales facilitados directamente por las personas afectadas						
Descripción	Categorías Especiales	Ciclo de vida de los datos				
		Recoger	Almacenar	Utilizar	Transferir	Borrar
DNI		X	X	X	X	X
Nombre		X	X	X	X	X
Apellidos		X	X	X	X	X
Dirección postal		X	X	X		X
Teléfono		X	X	X		X
Correo electrónico		X	X	X		X
Datos bancarios		X	X	X	X	X
Tarjetas crédito		X	X	X	X	X

Tabla 22: Ciclo de vida de los datos. Caso práctico tratamiento formación.

	Recoger	Almacenar	Utilizar	Transferir	Borrar
Intervinientes	Interesado; Responsable tratamiento	Responsable tratamiento	Responsable tratamiento	Gestoría	Responsable tratamiento
Operaciones de tratamiento	Alta alumno Registro de asistencia	Almacenamiento	Consulta	Facturas	Baja alumno
Tecnologías	Ficha alumno	BBDD alumnos	BBDD alumnos	Pendrive	

Tabla 23: Ciclo de vida de los datos. Caso práctico tratamiento formación.

8.3.5. Analizar la necesidad y proporcionalidad del tratamiento.

8.3.5.1. Necesidad del tratamiento.

Su finalidad no puede alcanzarse "razonablemente" por otros medios ya que se necesitan los datos personales para el tratamiento. No es posible su gestión sin los datos recabados.

8.3.5.2. Proporcionalidad del tratamiento.

No existe otra forma más moderada o menos invasiva para conseguir los fines del tratamiento. Se recaban los datos mínimos para impartir las formaciones y facturarlas.

8.3.6. Legitimación del tratamiento.

La legitimación de este tratamiento la obtenemos de los supuestos del artículo 6.1.a y en caso de datos de categoría especial, levantaremos la prohibición con las excepciones de los supuestos del artículo 9.2.a.

RGPD: 6.1.a. el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos.

8.3.7. Análisis de Riesgos de los derechos y libertades fundamentales de las personas físicas.

8.3.7.1. Identificación de Riesgos.

Partimos del listado de riesgos del Anexo 4 y por tanto no los necesitamos identificar. Aun así, se recomienda hacer siempre el ejercicio de revisar el Anexo 5 de cara a identificar nuevos riesgos para completar el listado óptimo de cada organización.

8.3.7.2. Valoración de Riesgos.

Procedemos a valorar los riesgos y por tanto obtener su nivel de riesgo.

Riesgo	Aplica	Probabilidad	Gravedad	NIVEL
La base que legitima el tratamiento no es adecuada, es ilícita o no se ha formalizado adecuadamente	SI	BAJA	BAJA	BAJO
No se ha ponderado adecuadamente el interés legítimo en relación con los intereses, derechos y libertades fundamentales del interesado	NO			
Las finalidades del tratamiento no son precisas, son ilegítimas, etc.	SI	BAJA	MEDIA	BAJO
Hay un cambio de finalidad que puede ser incompatible con la finalidad original	SI	BAJA	MEDIA	BAJO
No obtener el consentimiento a través de una clara acción afirmativa	SI	BAJA	MEDIA	BAJO
No se permite retirar el consentimiento	SI	BAJA	MEDIA	BAJO
No utilizar medios que permitan demostrar que el interesado prestó su consentimiento	SI	BAJA	MEDIA	BAJO
Se recogen datos inadecuados, no pertinentes, excesivos o innecesarios para la finalidad prevista	SI	BAJA	MEDIA	BAJO
Se registran datos inexactos o no se mantienen actualizados	SI	MEDIA	MEDIA	MEDIO
Los datos personales se conservan más tiempo del necesario	SI	BAJA	BAJA	BAJO
Los datos se tratan de manera desleal o poco transparente (no se cumple la expectativa de la persona interesada respecto del tratamiento de sus datos)	SI	BAJA	MEDIA	BAJO
Se hacen operaciones de tratamiento desproporcionadas	SI	BAJA	BAJA	BAJO
En la recogida de datos no se proporciona la información mínima al afectado	SI	BAJA	BAJA	BAJO
La respuesta al ejercicio del derecho de acceso no se hace en el tiempo y la forma adecuados	SI	BAJA	MEDIA	BAJO
La respuesta al ejercicio del derecho de rectificación no se hace en el tiempo y la forma adecuados	SI	ALTA	MEDIA	MEDIO
La respuesta al ejercicio del derecho de supresión no se hace en el tiempo y la forma adecuados	SI	BAJA	BAJA	BAJO
La respuesta al ejercicio del derecho a la limitación del tratamiento no se hace en el tiempo y la forma adecuados	SI	BAJA	BAJA	BAJO
La respuesta al ejercicio del derecho de portabilidad de los datos no se hace en el tiempo y la forma adecuados	SI	BAJA	BAJA	BAJO
La respuesta al ejercicio del derecho de oposición no se hace en el tiempo y la forma adecuados	SI	BAJA	BAJA	BAJO
Se toman decisiones que afectan a una persona utilizando exclusivamente medios automatizados	NO			
No hay procedimientos para dar una respuesta adecuada a los derechos	SI	MUY ALTA	MEDIA	MEDIO
La organización desconoce los procedimientos para responder el ejercicio de derechos	SI	ALTA	MEDIA	MEDIO
No se verifica adecuadamente la identidad de la persona que ejerce un derecho	NO			
Se incumple la regulación general sobre el derecho a la protección de los datos de carácter personal	SI	BAJA	MEDIA	BAJO
Se incumplen otras regulaciones sectoriales que inciden en la protección de los datos de carácter personal	SI	BAJA	BAJA	BAJO

Se incumplen las cláusulas sobre la protección de datos incorporados a los contratos o condiciones de uso	SI	MEDIA	MEDIA	MEDIO
Se incumplen estipulaciones recogidas en un código de conducta (si se está adherido)	NO			
No se puede demostrar el cumplimiento (responsabilidad proactiva)	SI	MEDIA	MEDIA	MEDIO
Las limitaciones del tratamiento no se comunican a terceros	NO			
Las certificaciones o sellos de protección de datos no se han renovado o han perdido vigencia	NO			
Hay transferencia internacional de datos no autorizada o desconocida	NO			
Los encargados de tratamiento no se han seleccionado adecuadamente	SI	MEDIA	MEDIA	MEDIO
No se ha formalizado adecuadamente la relación con los encargados de tratamientos	SI	MEDIA	MEDIA	MEDIO
No se ejerce suficiente control sobre la actividad del encargado de tratamiento (en las operaciones de tratamiento que le han sido encargadas)	SI	ALTA	MEDIA	MEDIO
Se desconocen las cadenas de subcontratación de los encargados de tratamiento	SI	MUY ALTA	MEDIA	MEDIO
Hay destrucción o pérdida accidental de datos personales	SI	MEDIA	MEDIA	MEDIO
Hay destrucción malintencionada de datos personales	SI	BAJA	MEDIA	BAJO
Hay alteración no autorizada de datos personales	SI	BAJA	MEDIA	BAJO
Hay comunicación no autorizada de datos personales	SI	MEDIA	MEDIA	MEDIO
Hay acceso no autorizado a datos personales	SI	MEDIA	MEDIA	MEDIO
Los sistemas de información no están disponibles	SI	BAJA	BAJA	BAJO
Hay incapacidad para detectar y gestionar incidentes que afectan a la seguridad de los datos	SI	MUY ALTA	MEDIA	MEDIO
Las violaciones de datos no se notifican en el tiempo y la forma adecuados (data breach)	SI	MUY ALTA	MEDIA	MEDIO
Las violaciones de datos no se comunican en el tiempo y la forma adecuados (data breach)	SI	MUY ALTA	MEDIA	MEDIO
No se ha designado delegado de protección de datos (si es obligatorio)	NO			
No se proporcionan medios suficientes al delegado de protección de datos	NO			
No se atiende un requerimiento de la autoridad de supervisión competente	SI	BAJA	MEDIA	BAJO
No se ha hecho una consulta previa a la autoridad de supervisión, cuando era necesaria	SI	MUY ALTA	MEDIA	MEDIO
No se ha tenido en cuenta la protección de datos en el momento de diseñar el tratamiento	SI	MUY ALTA	MEDIA	MEDIO
No se ha incorporado la protección de datos por defecto en las operaciones de tratamiento	SI	MUY ALTA	MEDIA	MEDIO

Tabla 24: Valoración de riesgos. Caso práctico tratamiento formación.

8.3.7.3. Evaluación de Riesgos

Del análisis y posterior valoración de riesgos podemos deducir que el nivel de riesgo del tratamiento es, medio o bajo.

El mapa de calor quedaría:

Riesgo Inherente				
Muy alta	0	8	0	0
Alta	0	3	0	0
Media	0	8	0	0
Baja	10	12	0	0
	Bajo	**Medio**	**Alto**	**Muy Alto**

Tabla 25: Mapa de calor riesgo inherente. Caso práctico tratamiento formación.

Al no haber riesgos con nivel alto o muy alto la dirección podría aceptar los riesgos y finalizar el AARR. En caso contrario procederá al tratamiento de los riesgos.

8.3.7.4. Tratamiento de Riesgos

El plan de acción de mitigación de riesgos consistirá en la implementación de todos los controles generales en un nivel de madurez L3 y de todos los controles específicos de grupo (salvo el grupo DPO) en un nivel de madurez L2. El plazo para alcanzar estos niveles de madurez se establece en un año.

Para este tratamiento en concreto no sería necesario este plan de acción. Para organizaciones pequeñas el plan de acción de mitigación de riesgos será igual para todos los tratamientos. Del proceso de implantación de medidas se acompaña archivo adjunto ***Riesgos Tratamiento Formacion.xlsx*** para poder gestionar el grado de eficacia del plan de acción. A modo de ejemplo para un instante determinado, el resultado se muestra en la siguiente imagen. Esta sería la foto fija de un momento determinado de la gestión de riesgos.

Riesgo Residual				
	50	0	0	0
	Bajo	Medio	Alto	Muy Alto

Tabla 26: Mapa de calor riesgo residual. Caso práctico tratamiento formación.

8.3.7.5. Riesgo Residual. Aceptación del riesgo

En el caso de este tratamiento el riesgo residual resultante será bajo por lo que la dirección puede aceptar el nivel de riesgo.

8.3.8. Informe EIPD

Todo el contenido desde el punto 9.3.1 Identificación de tratamiento y a mayores el plazo de revisión de la EIPD que sería el mismo propuesto en el plan de acción de mitigación de riesgos, en este caso un año.

8.3.9. Revisión EIPD.

Esta revisión se propuso hacerla un año después de la EIPD. Supongamos que ha pasado un año y estamos en el plazo de realización de la revisión.

Primeramente, responderemos al cuestionario de revisión de EIPD.

Pregunta	Si/No
Se produjeron cambios en las leyes y regulaciones relacionadas con la protección de datos	NO
Se produjeron cambios en las políticas y estándares internos relacionados con el tratamiento	NO
Se produjeron cambios en el sistema de información en el que se tratan los datos personales	NO
Se produjeron cambios en las finalidades y los medios para el tratamiento de los datos	NO
Se produjeron nuevos flujos de datos o se modificaron los existentes	NO
Se produjo una expansión del negocio o una nueva adquisición	NO

Tabla 27: Cuestionario de revisión EIPD. Caso práctico tratamiento formación.

Por tanto, no será necesario rehacer la EIPD.

8.3.9.1. Requisitos. Alcance

La auditoría se limitará al plan de acción de mitigación de riesgos del tratamiento recursos humanos.

8.3.9.1. Generación de la auditoría

Procedemos a revisar las medidas implantadas y su grado de madurez. A modo de ejemplo ficticio de caso práctico vamos a determinar el siguiente resultado.

Tras revisar todos los controles del plan de mitigación de riesgos obtenemos una aplicabilidad general:

Aplicabilidad	
Controles generales	95,77%
Controles de grupo	90,86%

Tabla 28: Aplicabilidad. Caso práctico tratamiento formación.

Se acompaña archivo adjunto ***Riesgos Tratamiento Formacion.xlsx*** para consultar la aplicabilidad de cada uno de los controles.

8.3.9.2. Generación del informe de auditoría

Después de las pruebas realizadas, es indicada una serie de recomendaciones a ser aplicadas en la organización y en los sistemas auditados.

Se ha comprobado que el nivel de aplicabilidad tanto para los controles generales como para los específicos es superior al 90% que es el umbral de aplicabilidad solicitado.

También se ha comprobado que el nivel de aplicabilidad para cada uno de los controles es superior al 50% salvo para los siguientes controles.

Control/medida	Nivel Madurez Inicial	Nivel Madurez Actual	Nivel de Madurez Propuesto	Aplicabilidad
Registro de entrada salida	L0	L1	L3	11,11%
Procedimiento de consultas	L0	L1	L2	20,00%
Registro de consultas	L0	L1	L2	20,00%
Procedimiento para establecer medidas de cumplimiento respecto a los nuevos tratamientos de datos desde el inicio de la activad y durante el ciclo de vida	L0	L1	L2	20,00%
Procedimiento de Evaluación Objetiva para precalificar el riesgo	L0	L1	L2	20,00%

Tabla 29: No conformidades subsanables. Caso práctico tratamiento formación.

Por tanto, se considera la auditoría **no conforme subsanable**. Se propone un plazo de tres meses para la subsanación de los controles de la tabla anterior.

Se acompaña archivo adjunto ***Riesgos Tratamiento Formacion.xlsx*** con resultado de aplicabilidad para los controles.

8.3.9.3. Seguimiento de la auditoría

Siempre y cuando las no conformidades del informe anterior sean subsanadas en plazo, se fija un plazo ordinario de revisión de auditoría y de EIPD de dos años.

9. Conclusiones

Esta metodología de Evaluación de Impacto relativa a la Protección de Datos podrá servir de ejemplo ilustrativo y didáctico para pequeñas y medianas empresas, a modo de guía o recomendación para todo el proceso.

La memoria ha resultado ser un proceso de mejora continua.

El objetivo general que nos propusimos consistió en desarrollar una metodología sencilla de Evaluaciones de Impacto relativas a la Protección de Datos (EIPD). Creemos que lo hemos conseguido.

Existen guías de la Agencia Española de Protección de Datos y de la Autoritat Catalana de Protecció de Dades pero buscábamos un resultado más práctico y este TFM lo ha alcanzado.

Esta memoria junto con archivo adjunto ***Riesgos.xlsx***, permiten realizar un completa EIPD, facilitando enormemente todo el proceso, incluida la gestión del riesgo.

Este TFM es susceptible de ampliaciones para futuros proyectos. El listado de riesgos propuesto, los controles propuestos, así como el cálculo de mitigación de riesgos.

10. Términos y definiciones

10.1. Definiciones recogidas en el Reglamento general de protección de datos.

1) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable 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;

2) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

3) «limitación del tratamiento»: el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro;

4) «elaboración de perfiles»: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física;

5) «seudonimización»: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;

6) «fichero»: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;

7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;

8) «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

9) «destinatario»: la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento;

10) «tercero»: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado;

11) «consentimiento del interesado»: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen;

12) «violación de la seguridad de los datos personales»: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos;

13) «datos genéticos»: 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;

14) «datos biométricos»: 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;

15) «datos relativos a la salud»: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;

16) «establecimiento principal»:

> *a) en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal;*
>
> *b) en lo que se refiere a un encargado del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al presente Reglamento;*

17) «representante»: persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 27, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento;

18) «empresa»: persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica;

19) «grupo empresarial»: grupo constituido por una empresa que ejerce el control y sus empresas controladas;

20) «normas corporativas vinculantes»: las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta;

21) «autoridad de control»: la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51;

22) «autoridad de control interesada»: la autoridad de control a la que afecta el tratamiento de datos personales debido a que:

> *a) el responsable o el encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control;*
>
> *b) los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento, o*
>
> *c) se ha presentado una reclamación ante esa autoridad de control;*

23) «tratamiento transfronterizo»:

> *a) el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o*
>
> *b) el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro;*

24) «objeción pertinente y motivada»: la objeción a una propuesta de decisión sobre la existencia o no de infracción del presente Reglamento, o sobre la conformidad con el presente Reglamento de acciones previstas en relación con el responsable o el encargado del tratamiento, que demuestre claramente la importancia de los riesgos que entraña el proyecto de decisión para los derechos y libertades fundamentales de los interesados y, en su caso, para la libre circulación de datos personales dentro de la Unión;

25) «servicio de la sociedad de la información»: todo servicio conforme a la definición del artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo (19);

26) «organización internacional»: una organización internacional y sus entes subordinados de Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo.

10.2. Otras definiciones.

Comité Europeo de protección de Datos: es un organismo europeo independiente que contribuye a la aplicación coherente de las normas de protección de datos en toda la Unión Europea y promueve la cooperación entre las autoridades de protección de datos de la UE. Sus siglas en español son CEPD y sus siglas en inglés son EDPB.

Alto riesgo: en protección de datos hace referencia a las consecuencias sometidas a una serie de criterios.

Derecho al olvido: consiste en el derecho de un usuario al borrado o desindexación de sus datos personales en el entorno digital.

Gestión de riesgos: las actividades coordinadas para dirigir y controlar una organización respecto al riesgo.

Grupo de riesgos: Conjunto de riesgos agrupados bajo una temática común.

Medidas de seguridad: En la gestión de riesgos, son aquellas que reducen la probabilidad o la gravedad de uno o varios riesgos.

Nivel de madurez: el logro de los objetivos genéricos y específicos que se aplican a cada conjunto predefinido de áreas de un proceso, en el caso de este TFM, el grado de implementación de las medidas de seguridad para mitigación de riesgos.

Nivel de riesgo: valoración cuantitativa o cualitativa asignada a un riesgo o a un conjunto de riesgos.

Observación sistemática: es aquella que se dispone de antemano, tanto el campo a estudiar (lugares e individuos) como de los aspectos concretos o conductas sobre las que se va a centrar la atención.

Riesgo: es un escenario que describe un acontecimiento y sus consecuencias, estimado en términos de gravedad y probabilidad.

Riesgo inherente: el riesgo intrínseco de cada actividad, sin tener en cuenta las medidas de control que mitigan o reducen su nivel de exposición.

Riesgo residual: el riesgo de cada actividad una vez se hayan aplicado las medidas de control para mitigar y/o reducir su nivel de exposición.

Vulnerabilidad: el riesgo que una persona, sistema u objeto puede sufrir frente a peligros inminentes.

10.3. Acrónimos.

ACPD: Autoridades de Control de Protección de Datos.

AEPD: Agencia Española de Protección de datos.

AARR: Análisis de Riesgos.

CEPD: Comité Europeo de Protección de Datos (EDPB en inglés).

CMM: Modelo de Madurez de Capacidades (Capability Maturity Model).

CNIL: Comisión Nacional de la Informática y las Libertades francesa

DPD: Delegado de protección de datos.

DPO: Data Protection Officer.

EIPD: Evaluación de Impacto relativa a la Protección de datos.

LOPDGDD:

RGPD:

11. Bibliografía y referencias

- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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.
- Lista de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos (art 35.4).
- Guía Práctica de Análisis de Riesgos en los Tratamientos de Datos Personales sujetos al RGPD (AEPD).
- Guía Práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD (AEPD).
- Guía Práctica Evaluación de impacto relativa a la protección de datos (APDCAT; Enero, 2018, versión 2.0).
- Handbook on Security of Personal Data Processing (ENISA; December 2017).
- Implementing a Privacy Protection Program: Using COBIT 5 Enablers With the ISACA Privacy Principles.
- Analyse d'impact relative à la protection des données (AIPD Commission Nationale de l'Informatique et des Libertés.
- ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements.
- ISO/IEC 29100:2011 Information technology -- Security techniques -- Privacy framework.
- ISO/IEC 29134:2017 Information technology -- Security techniques -- Guidelines for privacy impact assessment.
- ISO/IEC 29151:2017 Information technology -- Security techniques -- Code of practice for personally identifiable information protection.
- How to do a Privacy Impact Assessment - a step-by-step guide to completing your PIA successfully. The Privacy Commissioner's Office New Zealand.
- 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.
- Privacy Impact Assessment Handbook. Information Commissioner’s Office.
- Guidelines on the protection of personal data in IT governance and IT management of EU institutions. Supervisor Europeo de Protección de Datos (SEPD).

12. Anexos

12.1. Anexo 1: Listado de datos personales.

12.1.1. Datos personales.

12.1.1.1. Datos de carácter identificativo.

- DNI / Pasaporte / NIE.
- Nombre.
- Apellidos.
- Dirección postal.
- Teléfono.
- Firma manuscrita.
- Firma electrónica.
- Nº SS / Mutualidad.
- Tarjeta Sanitaria.
- Imagen / voz.
- Marcas físicas.
- Correo electrónico.
- Número de registro personal.
- Geolocalización.
- Versión Navegador.
- Versión Sistema Operativo.
- Dirección IP.
- Interfaz de Usuario.
- Idioma Navegador.
- Nombre de usuario.
- Contraseña.
- Dirección de MAC.
- Ciudad desde dónde accede a nuestro sitio web.
- Provincia desde dónde accede a nuestro sitio web.
- País desde dónde accede a nuestro sitio web.
- Las páginas visitadas en nuestro sitio web.
- La información o el texto ingresado en nuestro sitio web.
- Las URL visitadas antes y después de usar nuestro sitio web.

12.1.1.2. Características Personales.

- Datos de estado civil.
- Datos de familia.
- Fecha de nacimiento.
- Lugar de nacimiento.
- Edad.
- Sexo.

- Nacionalidad.
- Lengua Materna.
- Características físicas o antropométricas.

12.1.1.3. Circunstancias sociales.

- Características de alojamiento, vivienda.
- Situación militar.
- Propiedades, posesiones.
- Aficiones y estilo de vida.
- Pertenencia a clubes, asociaciones.
- Licencias, permisos, autorizaciones.

12.1.1.4. Académicos y profesionales.

- Formación, titulaciones.
- Historial del estudiante.
- Experiencia profesional.
- Pertenencia a colegios o a asociaciones profesionales.

12.1.1.5. Detalles de Empleo.

- Profesión.
- Puestos de trabajo.
- Datos no económicos de nómina.
- Historial del trabajador.

12.1.1.6. Información comercial.

- Actividades y negocios.
- Licencias comerciales.
- Suscripciones a publicaciones/medios de comunicación.
- Creaciones artísticas, literarios, científicas o técnicas.

12.1.1.7. Económicos, financieros y de seguros.

- Ingresos y rentas.
- Inversiones, bienes patrimoniales.
- Créditos, préstamos, avales.
- Datos bancarios.
- Planes de pensiones, jubilación.
- Datos económicos de nómina.
- Datos deducciones impositivas/impuestos.
- Seguros.
- Hipotecas.
- Subsidios, beneficios.
- Historial créditos.
- Tarjetas crédito.

12.1.1.8. Transacciones de bienes y servicios.

- Bienes y servicios suministrados por el afectado.
- Bienes y servicios recibidos por el afectado.
- Transacciones financieras.
- Compensaciones/Indemnizaciones.

12.1.1.9. Datos de control de presencia.

- Fecha/hora entrada.
- Fecha/hora salida.
- Motivo de ausencia.

12.1.1.10. Datos relativos a comportamiento o personalidad.

- Hábitos de consumo
- Perfilado
- Comportamiento en la red
- Intereses
- Preferencias

12.1.1.11. Otros Datos.

- Datos relativos a la acción social.
- Datos sobre sanciones.
- Puesto en entidad a la que representa.

12.1.2. Datos personales de categoría especial.

- Opiniones políticas.
- Afiliación sindical.
- Convicciones religiosas.
- Convicciones filosóficas.
- Origen racial o étnico.
- Datos relativos a la salud.
- Vida sexual.
- Datos genéticos.
- Datos biométricos.
- Orientación sexual.
- Estado fisiológico.
- Necesidades educativas especiales.
- Discapacidades físicas e intelectuales.

12.1.3. Datos personales de condenas e infracciones penales.

- Condenas o infracciones penales.

12.2. Anexo 2: Listado de tratamientos de ejemplo.

Listado de tratamientos de ejemplo.
Actividad de promoción
Actuaciones de fuerzas y cuerpos de seguridad con fines policiales
Agenda de la empresa
Control de presencia
Comercio electrónico
Compras y Contrataciones
Comunicación y relaciones institucionales
Consultas
Cumplimiento/incumplimiento de obligaciones dinerarias
Denuncias Internas, quejas y reclamaciones
Desarrollo de programas de cultura corporativa
Educación y cultura
Elaboración de perfiles
Encuestas y estudios
Evaluaciones de empleado
Fines de interés público basados en la legislación vigente
Fines estadísticos, históricos o científicos
Formación
Gestión de actividades asociativas, culturales, recreativas, deportivas y sociales
Gestión de asistencia social
Gestión de asistencia social (con historial clínico)
Gestión de asociados o miembros de entidades sin ánimo de lucro, cuya finalidad sea política, religiosa o sindical
Gestión de brechas de seguridad
Gestión de censo promocional
Gestión de clientes, contable, fiscal y administrativa
Gestión de derechos RGPD
Gestión de nóminas
Gestión de nóminas (discapacitados)
Gestión económica y contabilidad
Gestión económica-financiera pública
Gestión general de personal
Gestión sancionadora pública
Gestión y control de la biblioteca
Gestión y control sanitario
Guías/repertorios de servicios de comunicación electrónica
Hacienda pública y gestión de administración tributaria
Historial clínico
Investigación epidemiológica y actividades analógicas
Justicia

Libro recetario
Nóminas y otros pagos al personal
Padrón de habitantes
Prestación de servicios de certificación electrónica
Prestación de servicios de comunicaciones electrónicas
Prestación de servicios de solvencia patrimonial y crédito
Prevención de riesgos laborales
Prevención de riesgos laborales (con historial clínico)
Procedimiento administrativo
Procesos de Calidad, Auditorías y Mejora continua
Procesos de selección
Procesos judiciales, asesoría jurídica interna y cumplimiento normativo.
Proyectos y desarrollo de negocio
Publicaciones
Publicidad y prospección comercial
Recursos humanos
Registro de E/S
Registro de visitas
Relación con Proveedores y Clientes
Relaciones Laborales y actividad Sindical
Retribución flexible
Revisión de Nóminas
Seguridad física
Seguridad lógica y gestión IT
Seguridad privada
Seguridad pública y defensa
Seguridad y control de acceso a edificios
Servicios económicos-financieros y seguros
Trabajo y gestión de empleo
Viajes
Video vigilancia
Vigilancia de Salud

Tabla 30: Listado de tratamientos de ejemplo.

12.3. Anexo 3: Listado de Operaciones de tratamiento de ejemplo.

Operaciones de tratamiento
adaptación
administración de usuarios
almacenamiento
alta de clientes
archivo
baja de usuarios
combinación
comparación
comunicación
consulta
destrucción
difusión
estructuración
extracción
formulario web
gestión de medios de pago
modificación
obtención
organización
recogida
registro
restricción
supresión
utilización

Tabla 31: Listado de operaciones de tratamiento de ejemplo.

12.4. Anexo 4: Listado de riesgos.

Principios
La base que legitima el tratamiento no es adecuada, es ilícita o no se ha formalizado adecuadamente
No se ha ponderado adecuadamente el interés legítimo en relación con los intereses, derechos y libertades fundamentales del interesado
Las finalidades del tratamiento no son precisas, son ilegítimas, etc.
Hay un cambio de finalidad que puede ser incompatible con la finalidad original

Consentimiento
No obtener el consentimiento a través de una clara acción afirmativa
No se permite retirar el consentimiento
No utilizar medios que permitan demostrar que el interesado prestó su consentimiento

Calidad de los datos
Se recogen datos inadecuados, no pertinentes, excesivos o innecesarios para la finalidad prevista
Se registran datos inexactos o no se mantienen actualizados
Los datos personales se conservan más tiempo del necesario
Los datos se tratan de manera desleal o poco transparente (no se cumple la expectativa de la persona interesada respecto del tratamiento de sus datos)
Se hacen operaciones de tratamiento desproporcionadas

Derechos
En la recogida de datos no se proporciona la información mínima al afectado
La respuesta al ejercicio del derecho de acceso no se hace en el tiempo y la forma adecuados
La respuesta al ejercicio del derecho de rectificación no se hace en el tiempo y la forma adecuados
La respuesta al ejercicio del derecho de supresión no se hace en el tiempo y la forma adecuados
La respuesta al ejercicio del derecho a la limitación del tratamiento no se hace en el tiempo y la forma adecuados
La respuesta al ejercicio del derecho de portabilidad de los datos no se hace en el tiempo y la forma adecuados
La respuesta al ejercicio del derecho de oposición no se hace en el tiempo y la forma adecuados
Se toman decisiones que afectan a una persona utilizando exclusivamente medios automatizados
No hay procedimientos para dar una respuesta adecuada a los derechos
La organización desconoce los procedimientos para responder el ejercicio de derechos
No se verifica adecuadamente la identidad de la persona que ejerce un derecho

Obligaciones
Se incumple la regulación general sobre el derecho a la protección de los datos de carácter personal
Se incumplen otras regulaciones sectoriales que inciden en la protección de los datos de carácter personal
Se incumplen las cláusulas sobre la protección de datos incorporados a los contratos o condiciones de uso
Se incumplen estipulaciones recogidas en un código de conducta (si se está adherido)
No se puede demostrar el cumplimiento (responsabilidad proactiva)
Las limitaciones del tratamiento no se comunican a terceros
Las certificaciones o sellos de protección de datos no se han renovado o han perdido vigencia

Transferencias internacionales de datos
Hay transferencia internacional de datos no autorizada o desconocida

Encargado de tratamiento
Los encargados de tratamiento no se han seleccionado adecuadamente
No se ha formalizado adecuadamente la relación con los encargados de tratamientos
No se ejerce suficiente control sobre la actividad del encargado de tratamiento (en las operaciones de tratamiento que le han sido encargadas)
Se desconocen las cadenas de subcontratación de los encargados de tratamiento

Seguridad
Hay destrucción o pérdida accidental de datos personales
Hay destrucción malintencionada de datos personales
Hay alteración no autorizada de datos personales
Hay comunicación no autorizada de datos personales
Hay acceso no autorizado a datos personales
Los sistemas de información no están disponibles

Brechas
Hay incapacidad para detectar y gestionar incidentes que afectan a la seguridad de los datos
Las violaciones de datos no se notifican en el tiempo y la forma adecuados (data breach)
Las violaciones de datos no se comunican en el tiempo y la forma adecuados (data breach)

DPO
No se ha designado delegado de protección de datos (si es obligatorio)
No se proporcionan medios suficientes al delegado de protección de datos

Consultas
No se atiende un requerimiento de la autoridad de supervisión competente
No se ha hecho una consulta previa a la autoridad de supervisión, cuando era necesaria

Protección de datos desde el diseño y por defecto
No se ha tenido en cuenta la protección de datos en el momento de diseñar el tratamiento
No se ha incorporado la protección de datos por defecto en las operaciones de tratamiento

Tabla 32: Listado de riesgos.

12.5. Anexo 5: Método para identificar nuevos riesgos.

Cuando no consideremos suficientes los riesgos del listado del Anexo 4, podemos analizar el RGPD para obtener nuevos riesgos.

Para ello haríamos un barrido por todo el RGPD buscando artículos de los que deduzcamos riesgos derivados. El listado de artículos susceptibles de obtener riesgos derivados sería:

Artículo
[A.5] Artículo 5 - Principios relativos al tratamiento
[A.5.1] Los datos personales serán:
[A.5.1.a] tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»)
[A.5.1.b] recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);
[A.5.1.c] adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);
[A.5.1.d] exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);
[A.5.1.e] mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);
[A.5.1.f] tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).
[A.5.2] El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).
[A.6] Artículo 6 - Licitud del tratamiento
[A.6.1] El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:
[A.6.1.a] el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
[A.6.1.b] el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
[A.6.1.c] el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
[A.6.1.d] el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
[A.6.1.e] el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
[A.6.1.f] el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el 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 un niño.
[A.6.4] Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1, el responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas:
[A.6.4.a] cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;
[A.6.4.b] el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;
[A.6.4.c] la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;
[A.6.4.d] las posibles consecuencias para los interesados del tratamiento ulterior previsto;
[A.6.4.e] la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización.
[A.7] Artículo 7 - Condiciones para el consentimiento

[A.7.1] Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.
[A.7.2] Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.
[A.7.3] El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.
[A.7.4] Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.
[A.8] Artículo 8 - Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información
[A.8.1] Cuando se aplique el artículo 6, apartado 1, letra, 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.
[A.8.2] El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible.
[A.9] Artículo 9 - Tratamiento de categorías especiales de datos personales
[A.9.2] El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:
[A.9.2.a] el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;
[A.9.2.b] el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;
[A.9.2.e] el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;
[A.9.2.f] el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;
[A.9.2.g] el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;
[A.9.2.h] el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;
[A.9.2.i] el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional,
[A.9.2.j] el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.
[A.9.3] Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra , cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.
[A.10] Artículo 10 - Tratamiento de datos personales relativos a condenas e infracciones penales
[A.10.1] El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas sobre la base del artículo 6, apartado 1, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas.
[A.11] Artículo 11 - Tratamiento que no requiere identificación
[A.11.2] Cuando, en los casos a que se refiere el apartado 1 del presente artículo, el responsable sea capaz de demostrar que no está en condiciones de identificar al interesado, le informará en consecuencia, de ser posible. En tales casos no se aplicarán los artículos 15 a 20, excepto cuando el interesado, a efectos del ejercicio de sus derechos en virtud de dichos artículos, facilite información adicional que permita su identificación.
[A.12] Artículo 12 - Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado
[A.12.1] El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida

específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.
[A.12.2] El responsable del tratamiento facilitará al interesado el ejercicio de sus derechos en virtud de los artículos 15 a 2 En los casos a que se refiere el artículo 11, apartado 2, el responsable no se negará a actuar a petición del interesado con el fin de ejercer sus derechos en virtud de los artículos 15 a 22, salvo que pueda demostrar que no está en condiciones de identificar al interesado.
[A.12.3] El responsable del tratamiento facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22, y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. El responsable informará al interesado de cualquiera de dichas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el interesado solicite que se facilite de otro modo.
[A.12.4] Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.
[A.12.5] La información facilitada en virtud de los artículos 13 y 14 así como toda comunicación y cualquier actuación realizada en virtud de los artículos 15 a 22 y 34 serán a título gratuito. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá:
[A.12.6] Sin perjuicio de lo dispuesto en el artículo 11, cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud a que se refieren los artículos 15 a 21, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado.
[A.12.7] La información que deberá facilitarse a los interesados en virtud de los artículos 13 y 14 podrá transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente.
[A.13] Artículo 13 - Información que deberá facilitarse cuando los datos personales se obtengan del interesado
[A.13.1] Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:
[A.13.1.a] la identidad y los datos de contacto del responsable y, en su caso, de su representante;
[A.13.1.b] los datos de contacto del delegado de protección de datos, en su caso;
[A.13.1.c] los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
[A.13.1.d] cuando el tratamiento se base en el artículo 6, apartado 1, letra, los intereses legítimos del responsable o de un tercero;
[A.13.1.e] los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
[A.13.1.f] en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.
[A.13.2] Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:
[A.13.2.a] el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;
[A.13.2.b] la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
[A.13.2.c] cuando el tratamiento esté basado en el artículo 6, apartado 1, letra, o el artículo 9, apartado 2, letra, la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;
[A.13.2.d] el derecho a presentar una reclamación ante una autoridad de control;
[A.13.2.e] si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;
[A.13.2.f] la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.
[A.13.3] Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.
[A.14] Artículo 14 - Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado
[A.14.1] Cuando los datos personales no se hayan obtenidos del interesado, el responsable del tratamiento le facilitará la siguiente información:
[A.14.1.a] la identidad y los datos de contacto del responsable y, en su caso, de su representante;
[A.14.1.b] los datos de contacto del delegado de protección de datos, en su caso;
[A.14.1.c] los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento;

[A.14.1.d] las categorías de datos personales de que se trate;
[A.14.1.e] los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
[A.14.2] Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente respecto del interesado:
[A.14.2.a] el plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo;
[A.14.2.b] cuando el tratamiento se base en el artículo 6, apartado 1, letra, los intereses legítimos del responsable del tratamiento o de un tercero;
[A.14.2.c] la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, y a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
[A.14.2.d] cuando el tratamiento esté basado en el artículo 6, apartado 1, letra, o el artículo 9, apartado 2, letra, la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basada en el consentimiento antes de su retirada;
[A.14.2.e] el derecho a presentar una reclamación ante una autoridad de control;
[A.14.2.f] la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público;
[A.14.2.g] la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.
[A.14.3] El responsable del tratamiento facilitará la información indicada en los apartados 1 y 2:
[A.14.3.a] dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos;
[A.14.3.b] si los datos personales han de utilizarse para comunicación con el interesado, a más tardar en el momento de la primera comunicación a dicho interesado, o
[A.14.3.c] si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.
[A.14.4] Cuando el responsable del tratamiento proyecte el tratamiento ulterior de los datos personales para un fin que no sea aquel para el que se obtuvieron, proporcionará al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y cualquier otra información pertinente indicada en el apartado 2.
[A.14.5] Las disposiciones de los apartados 1 a 4 no serán aplicables cuando y en la medida en que:
[A.14.5.a] el interesado ya disponga de la información;
[A.14.5.b] la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, a reserva de las condiciones y garantías indicadas en el artículo 89, apartado 1, o en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información;
[A.14.5.c] la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado, o
[A.14.5.d] cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza estatutaria.
[A.15] Artículo 15 - Derecho de acceso del interesado
[A.15.1] El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información:
[A.15.1.a] los fines del tratamiento;
[A.15.1.b] las categorías de datos personales de que se trate;
[A.15.1.c] los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales;
[A.15.1.d] de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;
[A.15.1.e] la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;
[A.15.1.f] el derecho a presentar una reclamación ante una autoridad de control;
[A.15.1.g] cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;
[A.15.1.h] la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.
[A.15.2] Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas en virtud del artículo 46 relativas a la transferencia.
[A.15.3] El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos. Cuando el

interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.
[A.15.4] El derecho a obtener copia mencionado en el apartado 3 no afectará negativamente a los derechos y libertades de otros.
[A.16] Artículo 16 - Derecho de rectificación
[A.16.1] El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.
[A.17] Artículo 17 - Derecho de supresión («el derecho al olvido»)
[A.17.1] El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:
[A.17.1.a] los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;
[A.17.1.b] el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra, o el artículo 9, apartado 2, letra, y este no se base en otro fundamento jurídico;
[A.17.1.c] el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;
[A.17.1.d] los datos personales hayan sido tratados ilícitamente;
[A.17.1.e] los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;
[A.17.1.f] los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.
[A.17.2] Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.
[A.18] Artículo 18 - Derecho a la limitación del tratamiento
[A.18.1] El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:
[A.18.1.a] el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;
[A.18.1.b] el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;
[A.18.1.c] el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;
[A.18.1.d] el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.
[A.18.3] Todo interesado que haya obtenido la limitación del tratamiento con arreglo al apartado 1 será informado por el responsable antes del levantamiento de dicha limitación.
[A.19] Artículo 19 - Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento
[A.19.1] El responsable del tratamiento comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo al artículo 16, al artículo 17, apartado 1, y al artículo 18 a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita.
[A.20] Artículo 20 - Derecho a la portabilidad de los datos
[A.20.1] El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:
[A.20.1.a] el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra, o el artículo 9, apartado 2, letra, o en un contrato con arreglo al artículo 6, apartado 1, letra, y
[A.20.1.b] el tratamiento se efectúe por medios automatizados.
[A.20.2] Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.
[A.21] Artículo 21 - Derecho de oposición
[A.21.1] El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras o, incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.
[A.21.2] Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.
[A.21.3] Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines.

[A.21.4] A más tardar en el momento de la primera comunicación con el interesado, el derecho indicado en los apartados 1 y 2 será mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información.
[A.21.5] En el contexto de la utilización de servicios de la sociedad de la información, y no obstante lo dispuesto en la Directiva 2002/58/CE, el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.
[A.21.6] Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.
[A.22] Artículo 22 - Decisiones individuales automatizadas, incluida la elaboración de perfiles
[A.22.1] Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.
[A.22.2] El apartado 1 no se aplicará si la decisión:
[A.22.2.a] es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;
[A.22.2.b] está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o
[A.22.2.c] se basa en el consentimiento explícito del interesado.
[A.22.3] En los casos a que se refiere el apartado 2, letras y, el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.
[A.22.4] Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra o, y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.
[A.24] Artículo 24 - Responsabilidad del responsable del tratamiento
[A.24.1] 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.
[A.24.2] Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.
[A.25] Artículo 25 - Protección de datos desde el diseño y por defecto
[A.25.1] Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.
[A.25.2] El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.
[A.26] Artículo 26 - Corresponsables del tratamiento
[A.26.1] Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el presente Reglamento, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información a que se refieren los artículos 13 y 14, salvo, y en la medida en que, sus responsabilidades respectivas se rijan por el Derecho de la Unión o de los Estados miembros que se les aplique a ellos. Dicho acuerdo podrá designar un punto de contacto para los interesados.
[A.26.2] El acuerdo indicado en el apartado 1 reflejará debidamente las funciones y relaciones respectivas de los corresponsables en relación con los interesados. Se pondrán a disposición del interesado los aspectos esenciales del acuerdo.
[A.28] Artículo 28 - Encargado del tratamiento
[A.28.1] Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado.
[A.28.2] El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En este último caso, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios.
[A.28.3] El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulará, en particular, que el encargado:
[A.28.3.a] tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;

[A.28.3.b] garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;
[A.28.3.c] tomará todas las medidas necesarias de conformidad con el artículo 32;
[A.28.3.d] respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;
[A.28.3.e] asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;
[A.28.3.f] ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;
[A.28.3.g] a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;
[A.28.3.h] pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.
[A.28.4] Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado a que se refiere el apartado 3, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado.
[A.28.9] 9. El contrato u otro acto jurídico a que se refieren los apartados 3 y 4 constará por escrito, inclusive en formato electrónico.
[A.29] Artículo 29 - Tratamiento bajo la autoridad del responsable o del encargado del tratamiento
[A.29.1] El encargado del tratamiento y cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo podrán tratar dichos datos siguiendo instrucciones del responsable, a no ser que estén obligados a ello en virtud del Derecho de la Unión o de los Estados miembros.
[A.30] Artículo 30 - Registro de las actividades de tratamiento
[A.30.1] Cada responsable y, en su caso, su representante llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:
[A.30.1.a] el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;
[A.30.1.b] los fines del tratamiento;
[A.30.1.c] una descripción de las categorías de interesados y de las categorías de datos personales;
[A.30.1.d] las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
[A.30.1.e] en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;
[A.30.1.f] cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
[A.30.1.g] cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.
[A.30.2] Cada encargado y, en su caso, el representante del encargado, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:
[A.30.2.a] el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos;
[A.30.2.b] las categorías de tratamientos efectuados por cuenta de cada responsable;
[A.30.2.c] en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;
[A.30.2.d] cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 30, apartado 1.
[A.31] Artículo 31 - Cooperación con la autoridad de control
[A.31.1] El responsable y el encargado del tratamiento y, en su caso, sus representantes cooperarán con la autoridad de control que lo solicite en el desempeño de sus funciones.
[A.32] Artículo 32 - Seguridad del tratamiento
[A.32.1] Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:
[A.33] Artículo 33 - Notificación de una violación de la seguridad de los datos personales a la autoridad de control

[A.33.1] En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.
[A.33.2] El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.
[A.33.4] Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.
[A.33.5] El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo.
[A.34] Artículo 34 - Comunicación de una violación de la seguridad de los datos personales al interesado
[A.34.1] Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.
[A.34.2] La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras, y.
[A.34.4] Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3.
[A.35] Artículo 35 - Evaluación de impacto relativa a la protección de datos
[A.35.1] Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.
[A.35.2] El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.
[A.35.3] La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:
[A.35.3.a] evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;
[A.35.3.b] tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o
[A.35.3.c] observación sistemática a gran escala de una zona de acceso público.
[A.35.4] La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado La autoridad de control comunicará esas listas al Comité a que se refiere el artículo 68.
[A.35.5] La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. La autoridad de control comunicará esas listas al Comité.
[A.35.7] La evaluación deberá incluir como mínimo:
[A.35.7.a] una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;
[A.35.7.b] una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;
[A.35.7.c] una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y
[A.35.7.d] las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.
[A.35.9] 9. Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.
[A.35.11] 1 En caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento.
[A.36] Artículo 36 - Consulta previa
[A.36.1] El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para para mitigarlo.
[A.36.3] Cuando consulte a la autoridad de control con arreglo al apartado 1, el responsable del tratamiento le facilitará la información siguiente:

[A.36.3.a] en su caso, las responsabilidades respectivas del responsable, los corresponsables y los encargados implicados en el tratamiento, en particular en caso de tratamiento dentro de un grupo empresarial;
[A.36.3.b] los fines y medios del tratamiento previsto;
[A.36.3.c] las medidas y garantías establecidas para proteger los derechos y libertades de los interesados de conformidad con el presente Reglamento;
[A.36.3.d] en su caso, los datos de contacto del delegado de protección de datos;
[A.36.3.e] la evaluación de impacto relativa a la protección de datos establecida en el artículo 35, y
[A.36.3.f] cualquier otra información que solicite la autoridad de control.
[A.37] Artículo 37 - Designación del delegado de protección de datos
[A.37.1] El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:
[A.37.1.a] el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;
[A.37.1.b] las actividades principales del responsable o del encargado consistan 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, o
[A.37.1.c] las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.
[A.37.5] El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39.
[A.37.7] El responsable o el encargado del tratamiento publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control.
[A.38] Artículo 38 - Posición del delegado de protección de datos
[A.38.1] El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.
[A.38.2] El responsable y el encargado del tratamiento respaldarán al delegado de protección de datos en el desempeño de las funciones mencionadas en el artículo 39, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados.
[A.38.3] El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.
[A.38.4] Los interesados podrán ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del presente Reglamento.
[A.38.5] El delegado de protección de datos estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros.
[A.38.6] El delegado de protección de datos podrá desempeñar otras funciones y cometidos. El responsable o encargado del tratamiento garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses.
[A.39] Artículo 39 - Funciones del delegado de protección de datos
[A.39.1] El delegado de protección de datos tendrá como mínimo las siguientes funciones:
[A.39.1.a] informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;
[A.39.1.b] supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;
[A.39.1.c] ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;
[A.39.1.d] cooperar con la autoridad de control;
[A.39.2] El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.
[A.45] Artículo 45 - Transferencias basadas en una decisión de adecuación
[A.45.1] Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica.
[A.45.5] Cuando la información disponible, en particular tras la revisión a que se refiere el apartado 3 del presente artículo, muestre que un tercer país, un territorio o un sector específico de ese tercer país, o una organización internacional ya no garantiza un nivel de protección adecuado a tenor del apartado 2 del presente artículo, la Comisión, mediante actos de ejecución, derogará, modificará o suspenderá, en la medida necesaria y sin efecto retroactivo, la decisión a que se refiere el apartado 3 del presente artículo. Dichos actos de ejecución se adoptarán de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2.
[A.46] Artículo 46 - Transferencias mediante garantías adecuadas

[A.46.1] A falta de decisión con arreglo al artículo 45, apartado 3, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.
[A.46.2] Las garantías adecuadas con arreglo al apartado 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control, por:
[A.46.2.a] un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos;
[A.46.2.b] normas corporativas vinculantes de conformidad con el artículo 47;
[A.46.2.c] cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2;
[A.46.2.d] cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere en el artículo 93, apartado 2;
[A.46.2.e] un código de conducta aprobado con arreglo al artículo 40, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados, o
[A.46.2.f] un mecanismo de certificación aprobado con arreglo al artículo 42, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados.
[A.46.3] Siempre que exista autorización de la autoridad de control competente, las garantías adecuadas contempladas en el apartado 1 podrán igualmente ser aportadas, en particular, mediante:
[A.46.3.a] cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o
[A.46.3.b] disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados.
[A.47] Artículo 47 - Normas corporativas vinculantes
[A.47.1] La autoridad de control competente aprobará normas corporativas vinculantes de conformidad con el mecanismo de coherencia establecido en el artículo 63, siempre que estas:
[A.47.1.a] sean jurídicamente vinculantes y se apliquen y sean cumplidas por todos los miembros correspondientes del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, incluidos sus empleados;
[A.47.1.b] confieran expresamente a los interesados derechos exigibles en relación con el tratamiento de sus datos personales, y cumplan los requisitos establecidos en el apartado 2.
[A.47.3] La Comisión podrá especificar el formato y los procedimientos para el intercambio de información entre los responsables, los encargados y las autoridades de control en relación con las normas corporativas vinculantes a tenor de lo dispuesto en el presente artículo. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.
[A.48] Artículo 48 - Transferencias o comunicaciones no autorizadas por el Derecho de la Unión
[A.48.1] Cualquier sentencia de un órgano jurisdiccional o decisión de una autoridad administrativa de un tercer país que exijan que un responsable o encargado del tratamiento transfiera o comunique datos personales únicamente será reconocida o ejecutable en cualquier modo si se basa en un acuerdo internacional, como un tratado de asistencia jurídica mutua, vigente entre el país tercero requirente y la Unión o un Estado miembro, sin perjuicio de otros motivos para la transferencia al amparo del presente capítulo.
[A.49] Artículo 49 - Excepciones para situaciones específicas
[A.49.1] En ausencia de una decisión de adecuación de conformidad con el artículo 45, apartado 3, o de garantías adecuadas de conformidad con el artículo 46, incluidas las normas corporativas vinculantes, una transferencia o un conjunto de transferencias de datos personales a un tercer país u organización internacional únicamente se realizará si se cumple alguna de las condiciones siguientes:
[A.49.1.a] el interesado haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas;
[A.49.1.b] la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado;
[A.49.1.c] la transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica;
[A.49.1.d] la transferencia sea necesaria por razones importantes de interés público;
[A.49.1.e] la transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones;
[A.49.1.f] la transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento;
[A.49.1.g] 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.
[A.49.2] Una transferencia efectuada de conformidad con el apartado 1, párrafo primero, letra, no abarcará la totalidad de los datos personales ni categorías enteras de datos personales contenidos en el registro. Si la finalidad del registro es la consulta por parte de personas que tengan un interés legítimo, la transferencia solo se efectuará a solicitud de dichas personas o si estas han de ser las destinatarias.
[A.49.3] En el apartado 1, el párrafo primero, letras, y, y el párrafo segundo no serán aplicables a las actividades llevadas a cabo por las autoridades públicas en el ejercicio de sus poderes públicos.

[A.49.4] El interés público contemplado en el apartado 1, párrafo primero, letra, será reconocido por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento.
[A.49.6] El responsable o el encargado del tratamiento documentarán en los registros indicados en el artículo 30 la evaluación y las garantías apropiadas a que se refiere el apartado 1, párrafo segundo, del presente artículo.

Tabla 33: Listado de artículos del RGPD susceptibles de obtener riesgos derivados.

12.6. Anexo 6: Valoración de riesgos.

12.6.1. Criterios de aplicabilidad de riesgos

Los criterios de aplicabilidad serán específicos de cada tratamiento. Por ejemplo: Si la base jurídica no se basa en el consentimiento no aplicarán los riesgos basados en consentimiento.

12.6.2. Criterios de probabilidad de riesgos

VALOR	EJEMPLOS
BAJA (Despreciable)	**La posibilidad de ocurrencia es muy remota** Un evento que puede pasar de forma fortuita. Puede ocurrir menos de una vez al año.
MEDIA (Limitada)	**La posibilidad de ocurrencia es ocasional.** Un evento que puede pasar de forma ocasional. Puede ocurrir anualmente.
ALTA (Significativa)	**La posibilidad de ocurrencia es elevada.** Un evento que puede pasar con bastante frecuencia. Puede ocurrir mensualmente.
MUY ALTA (Máxima)	**La posibilidad de ocurrencia es muy elevada. Ocurrirá casi con total seguridad** Ocurrirá casi con total seguridad y con mucha frecuencia. Puede ocurrir semanalmente

Tabla 34: Criterios de probabilidad de riesgos.

12.6.3. Criterios de Gravedad de riesgos

	Descripción genérica de la gravedad (directa e indirecta)	Ejemplos de gravedad física
BAJA (Despreciable)	Los afectados no se verán afectados o pueden encontrar algunos inconvenientes, que se superarán sin ningún problema	Falta de atención adecuada para una persona dependiente (menor de edad, persona bajo tutela); Dolores de cabeza transitorios
MEDIA (Limitada)	Los afectados pueden encontrar inconvenientes significativos, que podrán superar a pesar de algunas dificultades	Afecciones físicas menores (por ejemplo, enfermedades menores debidas a no tener en cuenta las contraindicaciones); Falta de atención que conduce a un daño menor pero real (por ejemplo, discapacidad); Difamación que resulta en represalias físicas o psicológicas
ALTA (Significativa)	Los afectados pueden encontrar consecuencias significativas, que deberían poder superar, aunque con dificultades reales y serias.	Enfermedades físicas graves que causan daños a largo plazo (por ejemplo, empeoramiento de la salud debido a una atención inadecuada o el desconocimiento de contraindicaciones); Alteración de la integridad física, por ejemplo, después de una agresión, un accidente en el hogar, el trabajo, etc.
MUY ALTA (Máxima)	Los afectados pueden encontrar consecuencias significativas, o incluso irreversibles, que no pueden superar	Enfermedades físicas a largo plazo o permanentes (por ejemplo, por desconocimiento de contraindicaciones); Muerte (por ejemplo, asesinato, suicidio, accidente mortal); Deterioro permanente de la integridad física

Tabla 35: Criterios de gravedad de riesgos de riesgos. Genérica y física.

	Ejemplos de gravedad material	Ejemplos de gravedad moral
BAJA (Despreciable)	Pérdida de tiempo en la repetición de trámites o en espera de que se cumplan; Recepción de correo no solicitado (por ejemplo, spam). Reutilización de datos publicados en sitios web con fines de publicidad dirigida (información a redes sociales, reutilización para correo en papel); Publicidad dirigida. para productos comunes de consumo	Mera molestia causada por la información recibida o solicitada; Miedo a perder el control sobre los datos personales; Sensación de invasión de la privacidad sin daños reales u objetivos (por ejemplo, intrusión comercial); Pérdida de tiempo en la configuración de los datos personales; Falta de respeto por la libertad en línea movimiento debido a la denegación de acceso a un sitio comercial (por ejemplo, alcohol debido a la edad incorrecta)
MEDIA (Limitada)	Pagos no anticipados (p. Ej. Multas impuestas erróneamente), costos adicionales (p. Ej., Cargos bancarios, honorarios legales), impagos de pagos. Denegación del acceso a servicios administrativos o comerciales. Pérdidas de comodidad (es decir, cancelación de tiempo libre, compras, vacaciones, terminación de una cuenta en línea) - Promoción de carrera perdida; Cuenta de servicios en línea bloqueados (por ejemplo, juegos, administración); Recepción de correos dirigidos no solicitados que puedan dañar la reputación de las personas físicas; Aumento de costos (por ejemplo, aumento en los precios de los seguros); Datos no actualizados (por ejemplo, posición celebrado previamente); Procesamiento de datos incorrectos, por ejemplo, mal funcionamiento de las cuentas (banco, clientes, con organizaciones sociales, etc.); Publicidad en línea dirigida a un aspecto privado que la persona quería mantener confidencial (por ejemplo, publicidad sobre el embarazo, tratamiento de drogas); perfiles inexactos o inadecuados	Negativa a continuar utilizando sistemas de información (denuncias, redes sociales); Enfermedades psicológicas menores pero objetivas (difamación, reputación); Problemas de relación con conocidos personales o profesionales (por ejemplo, imagen, reputación empañada, pérdida de reconocimiento); Sentimiento de invasión de privacidad sin Daño irreversible; Intimidación en las redes sociales.
ALTA (Significativa)	Malversación de dinero no compensado; Dificultades financieras no temporales (por ejemplo, obligación de tomar un préstamo); Periódico, único y no recurrente, oportunidades perdidas (por ejemplo, préstamo hipotecario, rechazo de estudios, pasantías o empleo, prohibición de examen); Prohibición de la tenencia de cuentas bancarias; Daño a la propiedad; Pérdida de vivienda; Pérdida de empleo; Separación o divorcio; Pérdida financiera como resultado de un fraude (por ejemplo, después de un intento de phishing); Bloqueado en el extranjero; Pérdida de datos de clientes	Enfermedades psicológicas graves (por ejemplo, depresión, desarrollo de una fobia); Sentimiento de invasión de la privacidad con daños irreversibles; Sentimiento de vulnerabilidad después de una citación ante el tribunal; Sentimiento de violación de derechos fundamentales (por ejemplo, discriminación, libertad de expresión); Víctima de chantaje; Ciberacoso y hostigamiento.
MUY ALTA (Máxima)	Riesgo financiero; Deudas sustanciales; Incapacidad para trabajar; Incapacidad para reubicarse; Pérdida de evidencia en el contexto de un litigio; Pérdida de acceso a infraestructura vital (agua, electricidad)	Enfermedades psicológicas a largo plazo o permanentes; Pena penal; Sustracción; Pérdida de vínculos familiares; Incapacidad para demandar; Cambio de estatus administrativo y / o pérdida de autonomía legal (tutela)

1. Fuente "Privacy Impact Assessment Methodology" CNIL

Tabla 36: Criterios de gravedad de riesgos de riesgos. Material y moral.

12.7. Anexo 7: Listado de finalidades

- GESTIÓN DE CLIENTES, CONTABLE, FISCAL Y ADMINISTRATIVA
    - Gestión económica y contable
    - Gestión fiscal
    - Gestión administrativa
    - Gestión de facturación
    - Gestión de clientes
    - Gestión de proveedores
    - Gestión de cobros y pagos
    - Administración de fincas
    - Consultorías, auditorías, asesorías y servicios relacionados
    - Históricos de relaciones comerciales.
- RECURSOS HUMANOS
    - Gestión de personal
    - Formación de personal
    - Prestaciones sociales
    - Selección de personal
    - Gestión de trabajo temporal
    - Promoción y gestión de empleo
    - Control horario.
- GESTIÓN DE NÓMINAS
- PREVENCIÓN DE RIESGOS LABORALES
- PRESTACIÓN DE SERVICIOS DE SOLVENCIA PATRIMONIAL Y CRÉDITO
- CUMPLIMIENTO/INCUMPLIMIENTO DE OBLIGACIONES DINERARIAS
- SERVICIOS ECONÓMICOS-FINANCIEROS Y SEGUROS
    - Cuenta de crédito
    - Cuenta de depósito
    - Gestión de patrimonios
    - Gestión de fondos de pensiones y similares
    - Gestión de tarjetas de crédito y similares
    - Registro de acciones y obligaciones
    - Otros servicios financieros
    - Seguros de vida y salud
    - Otros tipos de seguros.
- ANÁLISIS DE PERFILES
- PUBLICIDAD Y PROSPECCIÓN COMERCIAL
    - Publicidad
    - Venta a distancia
    - Encuestas de opinión
    - Prospección comercial
    - Segmentación de mercados
    - Sistema de ayuda a la toma de decisiones
    - Recopilación de direcciones.
- PRESTACIÓN DE SERVICIOS DE COMUNICACIONES ELECTRÓNICAS
- GUIAS/REPERTORIOS DE SERVICIOS DE COMUNICACIONES ELECTRÓNICAS
- COMERCIO ELECTRÓNICO
- PRESTACIÓN DE SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA

- GESTIÓN DE ASOCIADOS O MIEMBROS DE PARTIDOS POLÍTICOS, SINDICATOS, IGLESIAS, CONFESIONES O COMUNIDADES RELIGIOSAS Y ASOCIACIONES, FUNDACIONES Y OTRAS ENTIDADES SIN ÁNIMO DE LUCRO, CUYA FINALIDAD SEA POLÍTICA, FILOSÓFICA, RELIGIOSA O SINDICAL
- GESTIÓN DE ACTIVIDADES ASOCIATIVAS, CULTURALES, RECREATIVAS, DEPORTIVAS Y SOCIALES
    - Gestión de actividades culturales
    - Gestión de clubes o asociaciones deportivas, culturales, profesionales y similares
    - Actividades asociativas diversas
    - Gestión de medios de comunicación social.
- GESTIÓN DE ASISTENCIA SOCIAL
- EDUCACIÓN
    - Enseñanza infantil y primaria
    - Enseñanza secundaria
    - Enseñanza universitaria
    - Educación especial
    - Otras enseñanzas.
- INVESTIGACIÓN EPIDEMIOLÓGICA Y ACTIVIDADES ANÁLOGAS
- GESTIÓN Y CONTROL SANITARIO
- HISTORIAL CLÍNICO
- SEGURIDAD PRIVADA
    - Investigaciones privadas a personas
    - Otras actividades de seguridad.
- SEGURIDAD Y CONTROL DE ACCESO A EDIFICIOS
- VIDEOVIGILANCIA
- FINES ESTADÍSTICOS, HISTÓRICOS O CIENTÍFICOS
- LIBRO RECETARIO
- GESTIÓN ESCOLAR
- GESTIÓN COMUNIDAD PROPIETARIOS
- COMERCIO ELECTRONICO

12.8. Anexo 8: Tratamientos identificados por las autoridades de control de protección de datos (ACPD) europeas que necesitan EIPD.

Características de los tratamientos	Número de ACPD
Datos biométricos	22
Datos genéticos	22
Monitorización de empleados	18
Uso de nuevas tecnologías	16
Geoposicionamiento / localización	12
Cuando se apliquen excepciones del art. 14.5 RGPD	8
Tratamientos que impliquen compartir datos con terceros (art. 19 RGPD)	7
Llevar a cabo tratamientos adicionales a los previstos inicialmente	6
Tratamiento con fines científicos o históricos sin consentimiento	6
Datos biométricos y genéticos (conjuntamente)	3
Tratamientos basados en implantes	3
Tratamientos a gran escala	3
Tratamiento con más de un responsable	2
El uso de la ley como base de legitimación del tratamiento	2
Transferencias internacionales	2
Recogida de datos mediante dispositivos electrónicos (sin autorización)	2
Tratamiento realizado con medios en diversos territorios	1
Migración de datos a otros sistemas de información	1

Tabla 37: Tratamientos identificados por las autoridades de control de protección de datos (ACPD) europeas que necesitan EIPD.

12.9. Anexo 9: Medidas de mitigación de riesgos.

12.9.1. Medidas generales.

Control/medida
Cláusulas confidencialidad
Control de acceso físico
Cuestionario de autoevaluación, evalúa los principales aspectos del tratamiento de cara a garantizar el cumplimiento de la normativa
Documento de política de seguridad
Inventario de soportes en papel
Manual buenas prácticas Protección de datos
Plan de formación y comunicación interna
Política de mesas limpias
Política de traslado de documentación
Procedimiento de archivo
Procedimiento de expurgo
Procedimiento de gestión de personal (altas y bajas)
Procedimiento para garantizar mecanismos de anonimización segura e irreversible
Protección contra fuentes de riesgo (SAI, antiincendios)
Registro de acceso físico
Registro de entrada salida
Registro de equipos informáticos
Registro de proveedores sin acceso a datos
Registro de usuarios con acceso
Segregación de tareas por perfiles
Seudonimización

Tabla 38: Medidas de mitigación de riesgos generales.

12.9.2. Medidas específicas de un grupo de riesgos.

Principios
Licitud del tratamiento: Revisión de las bases, por un tercero que puedan legitimar el tratamiento
Revisión por un tercero de las Cláusulas de Información, consentimientos recabados y registro de Actividad del Tratamiento

Consentimiento
Establecer canales para obtención y retirada con la misma usabilidad. Tanto online como presencial
Trazabilidad del consentimiento
Verificación de edad
Protocolo de revisión de consentimientos

Calidad de los datos
Procedimiento de Minimización de datos personales
Sistema de gestión documental

Derechos
Protocolo de actuación para la gestión y resolución de los ejercicios de derechos
Cláusulas informativas
Establecer procedimientos de información online y presencial

Obligaciones
Registro de actividades de tratamiento
Procedimiento de revisión de cláusulas específicas y certificaciones

Transferencias internacionales de datos
Política de control del importador de datos
Análisis de países seguros
Procedimiento de TID

Encargado de tratamiento
Contrato Encargado tratamiento
Solicitud de evidencias de cumplimiento normativo
Protocolo de comunicación de brechas de seguridad de Encargados de Tratamiento
Registro de Encargados de tratamiento

Seguridad
Copias de seguridad
Control de acceso lógico
Cifrado de datos
Antivirus
Pruebas de pentesting
Registro de accesos
Seguridad de redes
Procedimiento recuperación de datos
Protocolo de gestión de incidencias no cibernéticas
Inventario de incidencias

Brechas
Protocolo de comunicación de brechas de seguridad

DPO
DPO independiente (externo o interno sin funciones ejecutivas de seguridad)
Datos de contacto DPO accesibles
DPO certificado

Consultas
Procedimiento de consultas
Registro de consultas

Protección de datos desde el diseño y por defecto
Procedimiento para establecer medidas de cumplimiento respecto a los nuevos tratamientos de datos desde el inicio de la activad y durante el ciclo de vida
Procedimiento de Evaluación Objetiva para precalificar el riesgo

Tabla 39: Medidas de mitigación de riesgos grupos de riesgos.

12.10. Anexo 10: Eficacia niveles de madurez.

Eficacia	Nivel	Significado
0%	**L0**	inexistente
10%	**L1**	inicial / ad hoc
50%	**L2**	reproducible, pero intuitivo
90%	**L3**	proceso definido
95%	**L4**	gestionado y medible
100%	**L5**	optimizado

Tabla 40: Eficacia niveles de madurez.

12.11. Anexo 11: Lista orientativa de tipos de tratamiento que requieren una evaluación de impacto relativa a la protección de datos según artículo 35.4 RGPD, según la AEPD.

En el momento de analizar tratamientos de datos será necesario realizar una EIPD en la mayoría de los casos en los que dicho tratamiento cumpla con dos o más criterios de la lista expuesta a continuación, salvo que el tratamiento se encuentre en la lista de tratamientos que no requieren EIPD a la que se refiere en artículo 35.5 del RGPD. Cuantos más criterios reúna el tratamiento en cuestión, mayor será el riesgo que entrañe dicho tratamiento y mayor será la certeza de la necesidad de realizar una EIPD. Esta lista se basa en los criterios establecidas por el Grupo de Trabajo del Artículo 29 en la guía WP248 "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 RGPD", los complementa y debe entenderse como una lista no exhaustiva:

- Tratamientos que impliquen perfilado o valoración de sujetos, incluida la recogida de datos del sujeto en múltiples ámbitos de su vida (desempeño en el trabajo, personalidad y comportamiento), que cubran varios aspectos de su personalidad o sobre sobre sus hábitos.
- Tratamientos que impliquen la toma de decisiones automatizadas o que contribuyan en gran medida a la toma de tales decisiones, incluyendo cualquier tipo de decisión que impida a un interesado el ejercicio de un derecho o el acceso a un bien o un servicio o formar parte de un contrato.
- Tratamientos que impliquen la observación, monitorización, supervisión, geolocalización o control del interesado de forma sistemática y exhaustiva, incluida la recogida de datos y metadatos a través de redes, aplicaciones o en zonas de acceso público, así como el procesamiento de identificadores únicos que permitan la identificación de usuarios de servicios de la sociedad de la información como pueden ser los servicios web, TV interactiva, aplicaciones móviles, etc.
- Tratamientos que impliquen el uso de categorías especiales de datos a las que se refiere el artículo 9.1 del RGPD, datos relativos a condenas o infracciones penales a los que se refiere el artículo 10 del RGPD o datos que permitan determinar la situación financiera o de solvencia patrimonial o deducir información sobre las personas relacionada con categorías especiales de datos.
- Tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física.
- Tratamientos que impliquen el uso de datos genéticos para cualquier fin.
- Tratamientos que impliquen el uso de datos a gran escala. Para determinar si un tratamiento se puede considerar a gran escala se considerarán los criterios

establecidos en la guía WP243 “Directrices sobre los delegados de protección de datos (DPD)” del Grupo de Trabajo del Artículo 29.

- Tratamientos que impliquen la asociación, combinación o enlace de registros de bases de datos de dos o más tratamientos con finalidades diferentes o por responsables distintos.
- Tratamientos de datos de sujetos vulnerables o en riesgo de exclusión social, incluyendo datos de menores de 14 años, mayores con algún grado de discapacidad, discapacitados, personas que acceden a servicios sociales y víctimas de violencia de género, así como sus descendientes y personas que estén bajo su guardia y custodia.
- Tratamientos que impliquen la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas, incluyendo la utilización de tecnologías a una nueva escala, con un nuevo objetivo o combinadas con otras, de forma que suponga nuevas formas de recogida y utilización de datos con riesgo para los derechos y libertades de las personas.
- Tratamientos de datos que impidan a los interesados ejercer sus derechos, utilizar un servicio o ejecutar un contrato, como por ejemplo tratamientos en los que los datos han sido recopilados por un responsable distinto al que los va a tratar y aplica alguna de las excepciones sobre la información que debe proporcionarse a los interesados según el artículo 14.5 (b,c,d) del RGPD.

12.12. Anexo 12 Cuestionario de revisión de EIPD

Pregunta	Si/No
Se produjeron cambios en las leyes y regulaciones relacionadas con la protección de datos	
Se produjeron cambios en las políticas y estándares internos relacionados con el tratamiento	
Se produjeron cambios en el sistema de información en el que se tratan los datos personales	
Se produjeron cambios en las finalidades y los medios para el tratamiento de los datos	
Se produjeron nuevos flujos de datos o se modificaron los existentes	
Se produjo una expansión del negocio o una nueva adquisición	

Tabla 41: Cuestionario de revisión de EIPD.