UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería Informática

Responsabilidades de un encargado de tratamiento de datos en relación a las normas relativas a ciberseguridad.

Trabajo Fin de Grado

Grado en Ingeniería Informática

AUTOR/A: Giménez Pérez, Vanesa

Tutor/a: Oltra Gutiérrez, Juan Vicente

CURSO ACADÉMICO: 2022/2023

Resumen

Con la intención de acotar lo máximo posible el alcance de este trabajo Fin de Grado, se pretende dar una visión general de los principales aspectos relacionados con la ciberseguridad y la salvaguarda de la información. Se contextualiza la situación actual en el ámbito digital, tanto a nivel nacional, como europeo.

Se detalla la normativa de aplicación en el ámbito de este trabajo y las implicaciones que dimanan de la misma, sirviéndonos de apoyo en los organismos nacionales que contribuyen a fomentar la seguridad de la información.

El propósito de esta obra es explicar al lector la importancia de identificar los riesgos y peligros desde diversos ángulos, entre ellos el jurídico, el técnico y el de gestión. Se quiere poner en contexto socio-legal la situación actual legislativa y analizar las implicaciones que tiene el uso de las nuevas tecnologías en la protección de datos y la ciberseguridad.

El trabajo tiene como objetivo la puesta en marcha de una guía para ayudar a un Encargado de la Protección de Datos de tal forma que le sirva como apoyo para su trabajo diario. Por último, se dejan abiertas varias líneas de trabajo para futuros desarrollos.

Palabras clave: LOPDGDD, tratamiento, datos, RGPD, protección, riesgo, responsable, encargado, privacidad, ciberseguridad, ciberataque.

Abstract

With the intentio to limit as much as possible the purpose of this Thesis, the aim is to give an overview of the main aspects related to cybersecurity and the safeguarding of information. The current situation in the digital environment is contextualized, both at national and European level.

It details the regulations applicable in the scope of this work and the implications arising therefrom, serving as support in the national bodies that help to promote information security.

The purpose of this work is to explain to the reader the importance of identifying risks and hazards from various angles, including legal, technical and managerial. The aim is to put the current legislative situation in a socio-legal context and to analyze the implications of the use of new technologies on data protection and cybersecurity.

The work aims at setting up a guide to help a Data Protection Processor to serve as a support for his daily work. Finally, several lines of work are left open for future developments.

Keywords : LOPDGDD, processing, data, RGPD, protection, risk, controllers, Processor, privacy, cybersecurity, cyberattack.

Índice de contenidos

Índice de Ilustraciones

1. Introducción

El artículo 18 de nuestra Carta Magna[1], reconoce el derecho fundamental «*al honor, a la intimidad personal y familiar y a la propia imagen*» y dispone, para su garantía, que «l*a ley limita el uso de las tecnologías de la información*» para garantizar estos derechos.

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD-GDD) [2]es una Ley Orgánica aprobada por las Cortes Generales de España, y tiene como objetivo alinear el derecho interno español con el Reglamento General de Protección de Datos (RGPD o GDPR por sus siglas en inglés), una ley que se aplica en toda la Unión Europea y que fue aprobada en 2016, entrando en vigor el 25 de mayo de 2018.

Esta normativa regula la protección de los datos de las personas físicas. De hecho, se tramitó y aprobó en 2016, por lo que se podía utilizar desde entonces. Sin embargo, se dio un largo periodo de adaptación para no entorpecer las operaciones comerciales.

Esta Ley nos ha traído diversas novedades respecto a la conocida Ley de Protección de datos que databa de 1999: [3] reconoce el derecho de acceso, así como el derecho de rectificación o supresión, en su caso, a quienes fueran parientes de personas fallecidas por vínculos familiar o análogos, así como a sus herederos. Cuando el fallecido lo hubiera prohibido expresamente, la misma medida restringe la práctica.

Esta ley también establece la edad a partir de la cual se puede dar permiso de forma autónoma y el derecho a solicitar la supresión de los datos que un menor o un tercero haya aportado a redes sociales u otros servicios de la sociedad de la información mientras era menor de edad. Ambos derechos se establecen a partir de los 14 años en nuestro ordenamiento jurídico.

Entre las novedades destaca la regulación de los sistemas de información crediticia (comúnmente conocidos como «*ficheros de morosos*»), y se reduce de 6 a 5 años la duración máxima de inclusión de las deudas y exige un importe mínimo de 50 euros para dichos sistemas.

Por último, en nuestra legislación, nos encontramos también con la Ley Orgánica 7/2021[4], de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, publicada en el Boletín Oficial del Estado de 27 de mayo de 2021, y que es la transposición de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

Con esta ley se forma el segundo Pilar Normativo de España en el ámbito de la protección de datos, complementando a la L.O. 3/2018 de Protección de Datos Personales y Garantía de los

1 Constitución Española. Boletín Oficial del Estado, 29 de diciembre de 1978, núm. 311. https://www.boe.es/eli/es/c/1978/12/27/(1)/con
2 Ley Orgánica 3/2018, de 5 de diciembre, de *Protección de Datos Personales y Garantía de los Derechos Digitales*. https://www.boe.es/eli/es/lo/2018/12/05/3/con
3 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. https://www.boe.es/eli/es/lo/1999/12/13/15/con.
4 Ley Orgánica 7/2021. de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. https://www.boe.es/eli/es/lo/2021/05/26/7

Derechos Digitales. Sin embargo, el ámbito de aplicación es infinitamente menor, razón por la cual esta ley sólo es utilizada por los organismos públicos autorizados para ello.

Veremos principalmente tres figuras a lo largo de este trabajo:

En primer lugar, el Delegado de Protección de Datos (DPD) o Data Protection Officer (DPO) en inglés, es un cargo importante en la protección de datos, especialmente en organizaciones que gestionan grandes cantidades de datos personales, restringidos o sensibles. Su principal función es asegurar que la empresa cumple con las obligaciones legales establecidas en el RGPD, la Directiva, la LO 3/2018 o la LO 7/2021.

La figura del Responsable del Tratamiento será la que establezca los fines y medios de dicho tratamiento, otorgándole la potestad de precisar por qué y cómo se van a tratar dichos datos personales, siendo el responsable último de los mismos.

Por último, este trabajo se centra en la figura del Encargado de Protección de Datos (en adelante, EPD), el cual puede ser una persona física o jurídica, servicio, autoridad pública u organismo, que se encargará de procesar dichos datos en nombre de un Responsable del tratamiento y dentro de los términos de un acuerdo legal. Aunque esta descripción puede parecer clara, en muchas ocasiones vamos a tener problemas para diferenciar cuándo hablamos de un responsable del tratamiento y cuándo estamos ante un encargado. Esto es en parte porque muchas funciones deben o pueden ser llevadas por ambos, pero en resumen, mientras que el responsable del tratamiento determina la finalidad y los usos de la información que tratará el encargado del tratamiento, éste debe seguir las instrucciones del responsable en relación con el tratamiento adecuado de los datos personales a los que pueda tener acceso como consecuencia de la prestación del servicio encomendado.

1.1 Limitaciones encontradas

Se quiere dejar reflejado y que se tenga en cuenta que éste es un trabajo en el que se citan constantemente nombre de leyes, normas y figuras con nomenclaturas muy similares. Esto ocasiona que aparezcan múltiples coincidencias en multitud de páginas web o trabajos anteriores.

Todo trabajo utilizado como apoyo en este TFG ha sido citado tanto a pie de página como al final del documento.

Si se revisa el informe de Turnitín, se puede observar que en primer lugar de coincidencia aparece www.boe.es, claro ejemplo de la multitud de normativa que se cita en las líneas que siguen.

1.2 Motivación

Como personas no somos conscientes de las ventajas ni de los riesgos asociados al tratamiento de nuestros datos personales, como profesionales puede que percibamos la protección de datos como una pesada carga. Y sin embargo cada segundo de cada día alguien está tratando nuestros datos. Hoy en día vivimos en un mundo cada vez más globalizado, en el que el uso de la informática y las telecomunicaciones está presente en toda actividad y aspecto de nuestra vida. Hay aplicaciones que predicen qué vamos a escribir, qué nos gusta o cómo nos sentimos.

Las compañías comerciales, conocedoras de tal extremo, se nutren de muchos de los datos que el ciudadano introduce en estos sistemas informáticos y telemáticos, con el objetivo de detectar los gustos e inquietudes de la gente y puede ofrecer sus productos o crear necesidades los cuales tratarán de satisfacer con el ofrecimiento de sus servicios. Todo esto depende de que alguna entidad trate los datos, y nosotros, como usuario final esperamos que se haga bien.

Por otro lado, las entidades públicas no viven ajenas a esta problemática. También generan infinidad de registros y ficheros que contienen datos personales necesarios para la gestión de sus actividades. Por lo que nos podemos encontrar desde archivos muy restringidos como puede ser los de la Tesorería General de la Seguridad Social, la Agencia Tributaria o ficheros generados en el marco de una cooperación policial y judicial en materia penal, hasta otros ficheros de acceso público como los concebidos para los Registros de la Propiedad o Mercantil.

La elección de este Trabajo de Fin de Grado sobre otros ofertados, se ha visto influenciada por una perspectiva ante todo personal. Este trabajo pretende ser por una parte un punto y aparte a mi carrera profesional en la empresa privada, donde durante años estuve operando con datos personales. Era labor diaria tanto la recogida, como el registro, el procesamiento y la organización de dichos datos. Por otro lado, lo considero un punto de partida en mi carrera profesional como funcionaria de carrera donde es preciso el conocimiento de la legislación de protección de datos, así como el estado de la ciberseguridad actual. Soy yo la que trato con datos personales de otras personas. En mi mano está en parte, que no circulen o se filtren, preservar su privacidad. Resulta necesario conocer el procedimiento a seguir para la confección o tratamiento de un fichero que contenga datos de carácter personal, con el objeto de no caer en errores que terminen dejando a dicho fichero, y al propio profesional que lo gestiona, al margen de la Ley.

1.3 Objeto y objetivos

El fin de este TFG es la obtención del título de Graduada en Ingeniería Informática, a través del curso específico de adaptación a grado, expedido por la Universidad Politécnica de Valencia. Este Trabajo Final de Grado pretende profundizar en las responsabilidades que tiene un encargado de tratamiento de datos en relación a las normas de ciberseguridad. En este sentido, se analizaría la normativa y la jurisprudencia en relación a la protección de datos personales y su relación con la ciberseguridad.

Como objetivos que van a abordarse en el Trabajo Final de Grado son los siguientes:

- Analizar las normas y regulaciones nacionales e internacionales en materia de ciberseguridad y protección de datos personales.
- Identificar las responsabilidades de un encargado de tratamiento de datos en relación a las normas de ciberseguridad.
- Analizar las implicaciones prácticas de la aplicación de las normas de ciberseguridad en el ámbito del tratamiento de datos personales.
- Investigar la jurisprudencia relacionada con la protección de datos personales y su interacción con la ciberseguridad.
- Formular recomendaciones orientadas al cumplimiento de las normativas de ciberseguridad en el contexto del tratamiento de datos personales.
- Evaluar la eficacia de las medidas de seguridad y prevención de riesgos.
- Analizar las implicaciones que las nuevas tecnologías tienen en la seguridad de datos personales y en la ciberseguridad.

En definitiva, el objetivo principal del Trabajo Final de Grado es profundizar en el conocimiento de las responsabilidades que recaen en un Encargado de Tratamiento de Datos en relación a las normas de ciberseguridad, con el propósito de proponer medidas eficaces para garantizar la protección de la información personal.

2. Estado del Arte

Para la elaboración de este trabajo se han explorado numerosas fuentes referentes al cumplimiento normativo para la protección de datos y de la ciberseguridad, entre todas ellas se quiere destacar los trabajos de fin de grado de MONTESINOS RODRIGO, L. (2022)[5], y de MULLOR BERENGUER, M. (2022)[6], las cuales han desarrollado sendas guías de buenas prácticas para el cumplimiento de las normas relativas privacidad de los datos personales, si bien es cierto que se centran en ciertos aspectos o en particularidades específicas, resultan de gran interés para este trabajo.

Por otro lado, también son dos las referencias bibliográficas en las que se basa este trabajo:

- GÓMEZ HERVÁS, N. del C., 2021. *Normativa de ciberseguridad*. Madrid: Ra-Ma. ISBN 978-84-18971-23-5.

- SEVILLANO JAÉN, F. y BELTRÁN PARDO, M., 2020. *Dirección de seguridad y gestión del ciberriesgo*. Madrid: Ra-Ma. ISBN 978-84-9964-934-4.

Ambas obras se utilizan como hilo conductor para relacionar por un lado el cumplimiento normativo de la ciberseguridad y de la protección de datos, siempre con la misión de identificar, intentar evitar en la mayor medida posible, y dado el caso, atenuar los riesgos que acechan a bienes tan importantes como son la seguridad y la privacidad.

Adicionalmente, se ha consultado fuentes como la Agencia Española de Protección de Datos[7] (en adelante AEPD), pieza clave de este trabajo, ya que proporciona la orientación sobre la seguridad de los datos personales y las sanciones por incumplimiento. De esta página se han consultado las diferentes herramientas que ofrece (FACILITA, GESTIONA…) así como diversa documentación para realizar las diferentes plantillas para ayudar al encargado del tratamiento de datos personales. La AEPD es la entidad encargada de supervisar y hacer cumplir las leyes de protección de datos en España.

El Instituto Nacional de Ciberseguridad[8] (en adelante INCIBE) es una entidad en España dedicada a la promoción de la ciberseguridad. Hemos encontrado recursos valiosos, como guías, informes y capacitaciones relacionadas con la ciberseguridad en este sitio web, que ha ayudado a comprender las amenazas cibernéticas actuales y las medidas de seguridad recomendadas para proteger los datos personales.

[5] MONTESINOS RODRIGO, L., 2022. Guía para la realización del Privacy Impact Assestment (PIA, Evaluación de Impacto en la Protección de Datos Personales) para encargados y responsables de tratamiento de datos. S.l.: Universitat Politècnica de València.
[6] MULLOR BERENGUER, M., 2022. Guía sobre protección de datos e implantación de la LOPDGDD en centros sanitarios. S.l.: Universitat Politècnica de València.
[7] *Agencia Española de Protección de Datos | AEPD*. [en línea]. [consultado el 5 de mayo de 2023]. Disponible en: https://www.aepd.es/es
[8] *INCIBE* [en línea] https://www.incibe.es/

De la Autoridad Catalana de Protección de Datos[9] (en adelante APDCat) se ha consultado su aplicación para gestionar el registro de las actividades de tratamiento (RAT) y diversa documentación que facilita.

También se ha consultado la Autoridad de Protección de Datos del Reino Unido[10] (en adelante I*CO, Informaticon Commissioner's Office*) ya que tiene una de las mejores plantillas que me he encontrado para evaluar el impacto relativo a la protección de datos.

La consulta al CCN-CERT del Centro Criptológico Nacional [11]se ha enfocado en la respuesta a incidentes cibernéticos y la gestión de la ciberseguridad en España. Se ha podido obtener asesoramiento específico sobre cómo prepararse y responder a la ocurrencia de un incidente de seguridad, así como información sobre las mejores prácticas de ciberseguridad. Esto es esencial para un encargado de tratamiento de datos en caso de una violación de seguridad.

El Instituto Nacional de Normas y Tecnología [12] (NIST, por sus siglas en inglés) también proporciona directrices y estándares para la ciberseguridad, que son ampliamente reconocidos y utilizados en todo el mundo.

En resumen, todas estas entidades ofrecen recursos, orientación y estándares esenciales para comprender y abordar las responsabilidades de un encargado de tratamiento de datos en relación con la ciberseguridad en España. Utilizar estos recursos ha ayudado a establecer un marco sólido para la protección de datos personales y el cumplimiento de las regulaciones de ciberseguridad más relevantes.

[9] *APDCAT. Autoritat Catalana de Protecció de Dades* [en línea] [consultado el 8 de mayo de 2023]. https://apdcat.gencat.cat/ca/inici
[10] *ICO Informaticon Commissioner's Office* [en línea] https://ico.org.uk/
[11] *CCN-CERT. CCN-CERT* [en línea] https://www.ccn-cert.cni.es/
[12]*National Institute of Standards and Technology. NIST* [en línea] [consultado el 9 de junio de 2023]. https://www.nist.gov/

2.1 Crítica al Estado del arte.

En el primer trabajo mencionado, denominado "*Guía para la realización del Privacy Impact Assessment (PIA), para a encargados y responsables del tratamiento de datos*", elaborado por Laura Montesinos Rodrigo en 2022 para la Universidad Politécnica de Valencia, tiene como objetivo crear una guía para ayudar a los responsables y encargados del tratamiento de datos personales a elaborar una Evaluación de Impacto respetando el cumplimiento normativo. La AEPD nos dice que el PIA, sirve para identificar los riesgos derivados de un tratamiento de datos, especialmente cuando nos referimos a nuevas tecnologías, con el fin de adoptar medidas de supresión o paliación de problemas de seguridad que podrían impactar en la privacidad de dichos datos.

En el segundo trabajo, titulado "*Guía sobre protección de datos e implementación de la LOPDGDD en centros sanitarios*.", realizado por Marta Mullor Berenguer en 2022 para la Universidad Politécnica de Valencia, se presenta una guía simplificada destinada a respaldar el trabajo de técnicos e informáticos en lo que respecta a la protección de datos relacionados con el ámbito sanitario, datos considerados de especial sensibilidad.

En el texto de Gómez Hervás (2021) titulado "*Normativa de ciberseguridad*" se crea un manual que recopila conceptos y normas fundamentales para cumplir con la protección de datos y la ciberseguridad. Este texto expande los conceptos teóricos mencionados en los dos trabajos anteriores y establece vínculos con la ciberseguridad, además de incorporar la figura del encargado del tratamiento de datos.

Asimismo, en el recurso presentado por Sevillano Jaén y Beltrán Pardo (2020) titulado "*Dirección de seguridad y gestión del ciberriesgo*" se aborda el tema de la relación entre la privacidad de los datos y la ciberseguridad. Se destaca la importancia del encargado del tratamiento de datos, quien lleva a cabo el procesamiento de datos personales en nombre del responsable del tratamiento.

Tanto el Encargado del tratamiento como el Responsable del tratamiento deben colaborar estrechamente con los Equipos de Ciberseguridad para garantizar la implementación adecuada de medidas de seguridad de la información y la gestión efectiva de los riesgos de seguridad de los datos. A pesar de los avances en ciberseguridad, todavía queda mucho que hacer para asegurar la seguridad de los datos en la era digital. Se necesita un enfoque más sólido y un mayor compromiso de las organizaciones para garantizar la seguridad de los datos. También se requiere una mayor estandarización y transparencia en la industria de la ciberseguridad para garantizar la interoperabilidad y la protección de los datos personales, dado que las diferentes soluciones de seguridad utilizan enfoques y tecnologías diversas, lo que dificulta la interoperabilidad y aumenta el riesgo de brechas de seguridad.

En el Balance de ciberseguridad 2022 realizado por el Instituto Nacional de Ciberseguridad (INCIBE)[13], aumentaron en un 8,8% los incidentes que fueron gestionados respecto al año 2021.

[13] *INCIBE* [en línea] https://www.incibe.es/sites/default/files/paginas/que-hacemos/balance_ciberseguridad_2022_incibe.pdf

El 52 % de los ataques realizados fueron a Empresas, donde 9 de cada 10 fueron incidentes relacionados con sistemas vulnerables. Además, hay que recalcar que 1 de cada 3 incidentes, fueron por filtración de datos. Datos sensibles, protegidos o confidenciales que han sido copiados, transmitidos, vistos, robados o utilizados por personas no autorizadas. Destacamos también del estudio que 2 de cada 5 fueron incidentes por vulnerabilidades en los sistemas tecnológicos, por fallos o debilidades que pusieron en riesgo la seguridad del mismo. En resumen, podemos acreditar con datos, que no es un tema que deba pasarse por encima, si no que requiere de un estudio y un trabajo para mejorar ya que los incidentes en ciberseguridad tienen una tendencia a aumentar con los años.

2.2 Propuesta

Para garantizar la privacidad y seguridad de la información de los individuos y obtener la confianza en las organizaciones que manejan estos datos es fundamental la protección de los datos con los que se trabaja. Ya no se espera de nuestros ciudadanos y de las organizaciones que estos datos sean protegidos, si no que se da por hecho que ya se hace y que tenemos claro las medidas que debemos aplicar.

Tradicionalmente los datos siempre han sido uno de los activos más importantes para cualquier empresa u organización. Sobre todo los datos personales, ya que nuestra propia legislación se encarga de hacerlos más blindados. Un robo de datos acarreará muchos problemas a la organización, como puede ser la pérdida de reputación o sanciones económicas muy importantes.

Hoy en día, es necesario que tanto los responsables del tratamiento como los encargados del tratamiento evalúen los riesgos y establezcan las salvaguardias pertinentes. En otras palabras, la atención de encargados y los responsables debe dirigirse a la identificación, gestión, mitigación y autorresponsabilidad de los riesgos.

Las limitaciones de no tener todo esto en cuenta, dentro de un enfoque clásico, sería que no se está orientando al cumplimiento de la legislación desde el principio y que son gestionados de manera independiente los riesgos técnicos (considerándolos como riesgos de seguridad) de los de cumplimiento. Por otro lado, tampoco se tiene en cuenta el factor humano de manera específica, cuando por todos es sabido que el usuario es el eslabón más débil y que suele tener impacto directo en él (trabajadores, clientes, usuarios, etc.), sin contar el impacto económico o técnico adicional de la organización.

Tampoco se tiene en cuenta los flujos de datos, los tratamientos, ni las actividades que se realizan con todos los datos en cada fase o etapa del proyecto, por lo que muchos riesgos quedan ocultos y por lo tanto no se pueden cuantificar ni gestionar. Los datos no son los mismos a lo largo de toda esta cadena, si no que evolucionan con el tiempo, son un activo vivo y, por lo tanto, los riesgos tampoco lo son y también varían con el tiempo.

Debido a lo mencionado anteriormente, no es viable establecer un conjunto fijo de medidas y riesgos para todos los casos. En cambio, es necesario analizar cada posible situación y realizar una evaluación de riesgos para cada etapa de la cadena. El Reglamento General de Protección de Datos (en adelante RGPD) instaura la responsabilidad proactiva, de la cual hablaremos en profundidad, lo que traslada al encargado del tratamiento la obligación de analizar qué ha de hacer, o no, en cada momento.

2.3 Normas que regulan la ciberseguridad

Convenio sobre la ciberdelincuencia, 23 de noviembre de 2001, Budapest[14]**.** Es considerada la norma internacional más completa para combatir el ciberdelito y la evidencia electrónica. El convenio establece medidas para prevenir y sancionar delitos informáticos, incluyendo el acceso ilícito, la interferencia en sistemas informáticos, el sabotaje informático, el fraude informático, la pornografía infantil y la violación de derechos de autor. Además, el convenio aborda la cooperación internacional en la lucha contra la ciberdelincuencia y la protección de los derechos fundamentales en el contexto digital

UNION EUROPEA, 2013. DIRECTIVA (UE) 2013/40 del Parlamento Europeo y del Consejo, de 12 de agosto de 2013[15], relativa a los ataques contra los sistemas de información**.** En ella se establecen medidas para la prevención y sanción de los ataques contra sistemas de información en la Unión Europea. La directiva define los delitos informáticos y establece sanciones mínimas y máximas para cada uno de ellos. La directiva también establece la cooperación entre los Estados miembros para la prevención y la lucha contra los ataques informáticos, incluyendo la creación de puntos de contacto nacionales y una red de puntos de contacto europeos. Además, la directiva establece la obligación de los Estados miembros de recopilar estadísticas sobre los delitos informáticos y de informar a la Comisión Europea sobre las medidas adoptadas para implementar la directiva. En resumen, la Directiva 2013/40/UE tiene como objetivo mejorar la ciberseguridad en la Unión Europea y la protección de los sistemas de información contra los ataques informáticos.

ESPAÑA, 2015. Ley Órgánica 1/2015 por la que se modifica la ley orgánica 10/1995 del código penal[16]**.** En ella, se incluye diversas modificaciones relacionadas con la ciberseguridad. Entre ellas, se establecen penas más severas para los delitos informáticos, como el acceso ilícito, la interceptación de comunicaciones, el sabotaje informático o la difusión de virus informáticos. Además, se introduce el concepto de «*ciberterrorismo*» y se establecen penas para quienes cometan delitos informáticos con el objetivo de causar un perjuicio grave a la seguridad pública. Asimismo, se establece la responsabilidad penal de las personas jurídicas por los delitos informáticos cometidos en su nombre o en su beneficio. En resumen, la LO 1/2015 busca actualizar el Código Penal para adaptarse a la realidad actual de la ciberdelincuencia y mejorar la protección de la sociedad en el entorno digital.

[14] ESPAÑA. Jefatura del Estado. Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. Acuerdo Internacional de 23 de noviembre de 2001. Boletín Oficial del Estado [en línea]. 17 de septiembre de 2010, (226) https://www.boe.es/buscar/act.php?id=BOE-A-2010-14221

[15] UNION EUROPEA, 2013. DIRECTIVA (UE) 2013/40 del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo. , (218) [en línea] https://boe.es/doue/2013/218/L00008-00014.pdf

[16] ESPAÑA. Jefatura del Estado. Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Ley Orgánica n.º 1/2015 de 30 de marzo de 2015. Boletín Oficial del Estado [en línea]. 31 de marzo de 2015, (77) https://www.boe.es/buscar/act.php?id=BOE-A-2015-3439

UNION EUROPEA, 2016. DIRECTIVA (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a medidas para mantener un elevado nivel común de seguridad de las redes y sistemas de información en la Unión[17], también denominada Directiva NIS, es un acto legislativo adoptado por la Unión Europea en 2016. Crea un marco de ciberseguridad para los proveedores de servicios digitales y los operadores de infraestructuras críticas, que deben tomar medidas para reducir los riesgos de seguridad en sus sistemas de información, que los miembros de la UE notifiquen los sucesos importantes en materia de ciberseguridad a las autoridades competentes y que los Estados miembros compartan información sobre dichos sucesos.

UNION EUROPEA, 2019. REGLAMENTO (UE) 2019/881 del Parlamento Europeo y del Consejo[18], de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la ciberseguridad) y a la certificación de la ciberseguridad de las Tecnologías de la información y las comunicaciones (TIC). Exige el desarrollo de un marco de certificación de la ciberseguridad de las TIC, que permitirá a los proveedores de servicios y fabricantes de productos demostrar que sus productos y servicios se adhieren a las normas de ciberseguridad. La organización ENISA de la Unión Europea se encarga de ayudar a la certificación de la ciberseguridad y de ofrecer orientación técnica y científica en asuntos relacionados con la ciberseguridad**.**

ESPAÑA. REAL DECRETO 1150/2021, de 28 de diciembre, [19]por el que se aprueba la Estrategia de Seguridad Nacional 2021. La estrategia establece la necesidad de reforzar la ciberseguridad de las infraestructuras críticas, aumentar la capacidad de detección y respuesta a incidentes de seguridad cibernética y fomentar la colaboración público-privada en materia de ciberseguridad. Además, la estrategia reconoce la importancia de la ciberseguridad en el ámbito internacional y establece la necesidad de mejorar la cooperación internacional en materia de ciberseguridad. La estrategia también establece la necesidad de mejorar la formación y capacitación en ciberseguridad, tanto en el ámbito público como privado.

17 UNION EUROPEA, 2016. Directiva (Ue) 2016/1148 Del Parlamento Europeo Y Del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión [En Línea] https://www.boe.es/doue/2016/194/L00001-00030.pdf

18 UNION EUROPEA, 2019. Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación. [en línea]. https://www.boe.es/doue/2019/151/L00015-00069.pdf

19 ESPAÑA. Presidencia del Gobierno. Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021. Real Decreto n.º 1150/2021 de 28 de diciembre de 2021. Boletín Oficial del Estado [en línea]. 31 de diciembre de 2021, (314). https://www.boe.es/buscar/act.php?id=BOE-A-2021-21884

ESPAÑA. REAL DRECRETO 311/2022[20], de 3 mayo, por el que se regula el Esquema Nacional de Seguridad. Este nuevo Esquema aplica a empresas certificadas en el ENS según el RD 3/2010. El objetivo principal del ENS es establecer las bases y requisitos para garantizar la seguridad de la información en las administraciones públicas españolas, así como en otras entidades y organismos que interactúen electrónicamente con ellas. El ENS se enfoca en asegurar la disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad de la información digital. Actualiza y adapta el ENS a los cambios tecnológicos y amenazas actuales, con el fin de fortalecer la protección de la información ante posibles ciberataques y garantizar la confianza digital. Es de gran relevancia para la seguridad digital en España, ya que establece las pautas y directrices necesarias para salvaguardar la información tanto de las administraciones públicas como de otras entidades que interactúen con ellas.

[20] ESPAÑA. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Boletín Oficial del Estado [en línea]. 4 de mayo de 2022, (106). https://www.boe.es/buscar/act.php?id=BOE-A-2022-7191

Ilustración 1. Cronograma Leyes sobre Ciberseguridad. Fuente: Elaboración propia

2.4 Normativa referente al tratamiento de datos personales

Declaración Universal de los Derechos Humanos, adoptada el 10 de diciembre de 1948[21]. Toda persona tiene derecho a la intimidad y a la protección de su vida privada, domicilio, correspondencia y reputación, según el artículo 12 de la DUDH. . Nadie debe ser objeto de intromisión injustificada o ataques a su honra y si lo es, tienen derecho a buscar protección legal para remediar la situación.

Toda persona tiene derecho a la protección de su vida privada y familiar, de su domicilio y de su correspondencia, según el artículo 8 del **Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales[22],** el cual fue adoptado el 4 de noviembre de 1950. Los poderes públicos sólo pueden atentar contra este derecho en las condiciones previstas por la ley y cuando ello sea necesario en una sociedad democrática para proteger la seguridad nacional, la seguridad pública, la economía, la salud o la moralidad de la nación, o para proteger los derechos y libertades de las personas.

Constitución española de 1978[23]. La Carta Magna en su artículo 18.4 reconoce el derecho fundamental «*al honor, a la intimidad personal y familiar y a la propia imagen*» y dispone, para su garantía, que «*la ley limite el uso de la informática*», significando el derecho de la persona a controlar sus datos, que incluye la capacidad de decidir sobre su uso o destino para evitar el tráfico ilícito de los mismos o que atenten contra la dignidad y los derechos fundamentales.

Con el fin de garantizar que toda persona que se encuentre en territorio la Unión Europea, con independencia de su nacionalidad o lugar de residencia, sea tratada con respeto a sus derechos y libertades fundamentales, y en particular a su derecho a la intimidad en lo que respecta al tratamiento automatizado de los datos de carácter personal, el Consejo de Europa adoptó el **Convenio nº 108** el 28 de enero de 1981**.[24]**

[21] NACIONES UNIDAS, 1948. La Declaración Universal de los Derechos Humanos [en línea]. https://cnrha.sanidad.gob.es/documentacion/bioetica/pdf/Universal_Derechos_Humanos.pdf
[22] ESPAÑA. Declaración formulada por España relativa al artículo 25 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950. Nota Diplomática de 11 de junio de 1981. Boletín Oficial del Estado [en línea]. 30 de junio de 1981, (155) https://www.boe.es/buscar/act.php?id=BOE-A-1981-14565
[23] ESPAÑA. Cortes Generales. Constitución Española. Constitución de 27 de diciembre de 1978. Boletín Oficial del Estado [en línea]. 29 de diciembre de 1978, (311) https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229
[24] ESPAÑA. Jefatura del Estado. Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981. Acuerdo Internacional de 28 de enero de 1981. Boletín Oficial del Estado [en línea]. 15 de noviembre de 1985, (274) https://www.boe.es/buscar/act.php?id=BOE-A-1985-23447

La **Ley Orgánica 1/1982**[25]**,** promulgada el 5 de mayo de 1982, protege los derechos civiles al honor, a la intimidad familiar y a la propia imagen. La ley estipula que el tratamiento de datos personales debe realizarse de acuerdo con los principios de calidad, proporcionalidad y seguridad, y que los datos personales deben ser tratados de forma confidencial. Además, la ley establece que el tratamiento de datos personales debe respetar los derechos fundamentales de las personas y que los titulares de los datos tienen derecho a conocer la finalidad del tratamiento y a ejercer sus derechos de acceso, rectificación, cancelación y oposición.

El 29 de octubre de 1992 se aprobó la **Ley Orgánica 5/1992**[26], que regula el tratamiento automatizado de los datos de carácter personal. Esta ley establece medidas de seguridad y requisitos para quienes tratan dichos datos con el fin de regular el tratamiento automatizado de datos de carácter personal y proteger los derechos y la intimidad de las personas**.** También establece los derechos de los titulares de los datos y las sanciones en caso de incumplimiento. Esta ley se limita al tratamiento automatizado de datos derivados del uso de tecnologías de la información, y la regulación se centró en proteger los daños que pudieran derivarse del uso de datos para el resto de derechos fundamentales del art. 18.

En 1999, España traspuso la Directiva 95/46/CE de la Unión Europea, que permitía intercambiar datos entre los países pertenecientes a la UE, dando lugar a la conocida **LOPD**, **Ley Orgánica 15/1999**[27], del 13 de diciembre, de Protección de datos de Carácter Personal, y derogando la LORTAD.

Reglamento **2016/679/UE** del Parlamento Europeo y del Consejo [28]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. La cual establece normas claras y estrictas sobre la recopilación, el uso y la protección de datos personales dentro de la Unión. Pretende garantizar la libre circulación de estos datos en el mercado único europeo y salvaguardar la intimidad y los derechos fundamentales de las personas en relación con el tratamiento de sus datos. También establece sanciones severas para las empresas que no cumplan con las regulaciones.

[25] ESPAÑA. Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. 14 de mayo de 1982, (115) https://www.boe.es/buscar/act.php?id=BOE-A-1982-11196

26ESPAÑA. Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. Boletín Oficial del Estado [en línea]. 31 de octubre de 1992, (262). https://www.boe.es/buscar/act.php?id=BOE-A-1992-24189

27 ESPAÑA. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Boletín Oficial del Estado [en línea]. 14 de diciembre de 1999, (298) [consultado el 5 de junio de 2023]. https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750

28 UNION EUROPEA. 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) [en línea] https://www.boe.es/doue/2016/119/L00001-00088.pdf

Ley Orgánica 3/2018 [29]de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD). Establece una serie de medidas para garantizar la protección de los datos personales, tales como la obligatoriedad de obtener el consentimiento expreso y documentado del titular de los datos para su tratamiento, la implementación de medidas de seguridad adecuadas para proteger los datos personales o el derecho de los titulares de los datos a acceder, rectificar y suprimir sus datos personales. Además, la ley reconoce el derecho al olvido en internet y establece medidas para garantizar la privacidad en las comunicaciones electrónicas, como la obligación de obtener el consentimiento previo y explícito antes de utilizar cookies o tecnologías similares en los dispositivos de los usuarios.

Directiva 2016/680/UE[30] del Parlamento Europeo y del Consejo 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. Su objetivo es establecer normas y garantías específicas para la protección de datos personales cuando son procesados por las autoridades competentes en el ámbito de la prevención, investigación, detección, enjuiciamiento de infracciones penales o la ejecución de sanciones penales. En otras palabras, la directiva se centra en garantizar que la protección de datos se realice de manera justa, transparente y respetando los derechos fundamentales de las personas afectadas, y asegurar la libre circulación de dichos datos dentro de la Unión Europea.

Ley Orgánica 7/2021 [31]de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales**.** Su objetivo es garantizar la protección de los derechos fundamentales de las personas y establecer las condiciones de tratamiento de los datos personales para garantizar la prevención y persecución de los delitos.

29 ESPAÑA. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. Boletín Oficial del Estado, 6 de diciembre de 2018, (294) https://www.boe.es/eli/es/lo/2018/12/05/3/con

30 UNION EUROPEA, 2016. 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 y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo [en línea]. https://www.boe.es/doue/2016/119/L00089-00131.pdf

31 ESPAÑA. Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. [en línea]. 27 de mayo de 2021, (126) [consultado el 5 de junio de 2023] https://www.boe.es/buscar/act.php?id=BOE-A-2021-8806

Real Decreto 389/2021 [32]por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos (AEPD), establece su organización y funcionamiento. La AEPD es una autoridad administrativa independiente encargada de velar por el cumplimiento de la normativa de protección de datos en España. Este Estatuto establece las funciones, competencias y estructura organizativa de la AEPD, así como los procedimientos para la toma de decisiones y la gestión de recursos. Su objetivo es garantizar la protección de los derechos fundamentales de las personas en relación al tratamiento de sus datos personales.

Además, existen otras normativas que complementan la protección de los datos personales en sectores específicos, como la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSICE) o la Ley de Propiedad Intelectual (LPI).

[32] ESPAÑA, 2021. Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos. [en línea]. https://www.boe.es/eli/es/rd/2021/06/01/389

.

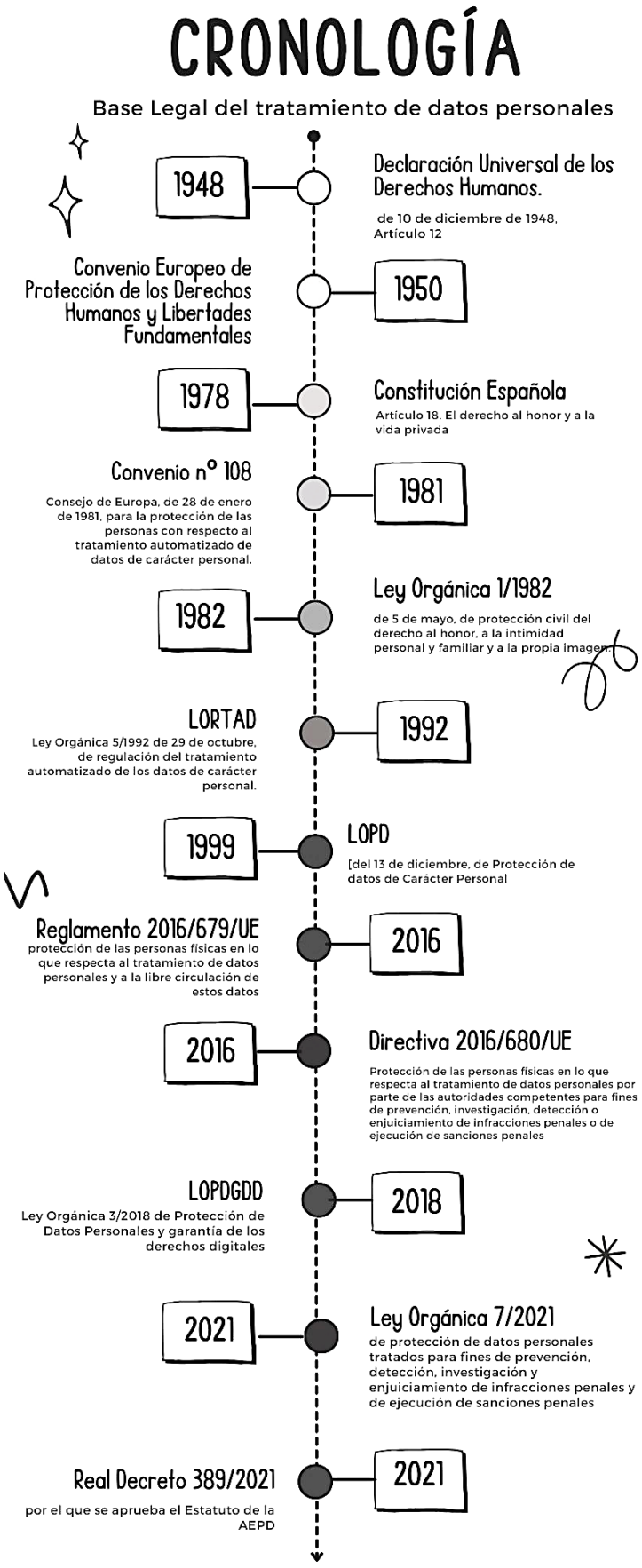

Ilustración 2. Cronograma Leyes sobre Protección de Datos Personales. Fuente: Elaboración propia

3. Análisis del problema

3.1 Relación entre ciberseguridad y Privacidad

La ciberseguridad y la privacidad deben formar un binomio inseparable, porque sin la una no es posible la otra y viceversa. Nuevas tecnologías aparecen cada vez a mayor velocidad, y muchas veces sin las suficientes pruebas, ya que impera la ley del mercado, lo que acarre riesgos en la privacidad.

Cada vez más los gobiernos y empresas obligan a la salvaguarda de la seguridad de los datos. Quizás porque están concienciados con que uno de los principales activos es la información y los datos personales, o quizás porque si no estás vigilando cómo son tus nuevos productos o servicios, te enfrentas a graves sanciones. En cualquier caso, la protección y actuación frente a las amenazas y el fomento de la seguridad es imprescindible para garantizar la confianza y el desarrollo de cualquier organización.

Podemos definir la Ciberseguridad como la protección de activos frente a las amenazas, siempre y cuando estos activos sean digitales y/o que las amenazas provengan del espacio digital. Los activos son cualquier cosa que tenga valor para la organización, y que le permita operar normalmente, pero que pueda ser atacada de manera intencional o accidental. Las amenazas pueden ser cualquier evento, acción o circunstancia que pueda tener un efecto negativo en los activos, ya sea en su confidencialidad, disponibilidad o integridad.

Por lo tanto la Ciberseguridad se ocupa de prevenir, detectar y responder a incidentes con el objetivo de hacer organizaciones ciber resilientes. PREVENIR, ya que todos podemos ser objeto de ataque simplemente por el hecho de estar conectados a Internet. DETECTAR, porque hay dos tipos de organizaciones: «*las que han sido atacadas, y lo saben, y las que han sido atacadas y aún no lo saben*» y CIBER RESILIENCIA o capacidad de resistir y reponerse a un incidente de seguridad, para salir fortalecido del mismo.

Hay que tener en cuenta y considerar que conforme avanzan las TIC y que el usuario de la calle tiene más a su alcance los avances tecnológicos, la privacidad se va difuminando ya que «*vamos regalando nuestros datos personales* sin ser conscientes de ello. Como hemos comentado, esta tecnología aparece de forma muy rápida, y muchas veces sin probar demasiado, lo que acarrea problemas mayores de privacidad, ya que en ocasiones no se realizan las evaluaciones de impacto bien hechas porque, desgraciadamente, lo que impera es el mercado, es decir, que las cosas salgan a la venta cuanto antes.

Y aunque la regulación es cada vez más dura, y nos obligan a tener la salvaguarda de los datos porque si no te arriesgas a una sanción realmente muy importante, que la concienciación también ha cambiado, y aunque vayamos mejorando en la privacidad… La realidad es que nuestros datos están más difundidos, y que no están tan protegidos como el usuario final cree que están. También es cierto, que todavía a fecha de hoy se da más importancia, o pesa más, la facilidad de uso, la gratuidad, o el beneficio que nos reporta frente a los problemas o riesgos por exponer nuestros .datos.

Esta captura de datos se ha convertido en la base de muchos modelos de negocios y es un mundo muy rentable. El nuevo petróleo se llama dato, creando negocios alrededor de estos datos que hace unos años eran inimaginables y que hoy en día se conoce como economía de la vigilancia.

Es por todo esto que la relación entre ciberseguridad y privacidad es fundamental en el ámbito digital, ya que la protección de la información personal y sensible de los usuarios depende en gran medida de medidas de seguridad sólidas. En España, al igual que en muchos otros países, existen leyes y regulaciones que abordan tanto la ciberseguridad como la privacidad para garantizar un entorno en línea seguro y protegido.

En la Declaración Universal de los Derechos Humanos (DUDH), de 10 de diciembre de 1948, en su artículo 12 ya ponía de manifiesto que todas las personas tienen derecho a la privacidad y protección de su vida privada, la de su hogar, su correspondencia y su reputación. Nadie debe ser objeto de intromisión injustificada o ataques a su honra y si lo es, tienen derecho a buscar protección legal.

Hoy en día, la Ley Orgánica 3/2018, de 5 de diciembre, LOPDGDD es la principal normativa española que regula la privacidad y la protección de datos personales en el entorno digital. Esta ley establece los principios y requisitos que las organizaciones deben cumplir al recopilar, procesar y almacenar datos personales, asegurando que se obtenga el consentimiento adecuado de los usuarios y que se implementen medidas de seguridad adecuadas para proteger dichos datos.

En cuanto a la ciberseguridad, España adopta directrices de la Unión Europea (UE) y se basa en el Reglamento (UE) 2016/679 (RGPD), que establece estándares de seguridad para el procesamiento de datos personales. Además, España también sigue la Directiva (UE) 2016/1148 sobre la seguridad de las redes y la información (conocida como Directiva NIS), que exige a todos los Estados miembros y a los proveedores de servicios digitales implementar medidas de ciberseguridad para garantizar la protección de las redes y sistemas de información en sectores esenciales, como energía, transporte, salud y servicios financieros. Si bien su enfoque es la ciberseguridad de infraestructuras críticas, también puede tener implicaciones para la protección de la privacidad, ya que la seguridad de los sistemas de información puede afectar la integridad y confidencialidad de los datos.

Esquema Nacional de Seguridad (ENS) es un marco normativo en España que establece pautas y requisitos para garantizar la seguridad de la información en las entidades y organismos del sector público. Aunque su enfoque principal es la seguridad de la información, también reconoce la importancia de proteger la privacidad de los datos personales. Esto significa que las medidas de seguridad definidas en el ENS deben estar en línea con las regulaciones de privacidad, como la LOPDGDD y el RGPD.

Por lo tanto, el ENS y la Directiva NIS son marcos normativos que se ocupan de la seguridad de la información y la ciberseguridad, pero también reconocen la importancia de proteger la privacidad de los datos personales. La colaboración y el cumplimiento adecuado de estos elementos son esenciales para garantizar la seguridad y la privacidad en el entorno digital.

En resumen, la relación entre ciberseguridad y privacidad en España está estrechamente vinculada a través de la LOPDGDD y el RGPD. Estas dos normativas son fundamentales para garantizar la

privacidad de los datos personales en el marco del Esquema Nacional de Seguridad (ENS) y en el contexto más amplio de la protección de datos en la Unión Europea. Las organizaciones deben asegurarse de implementar medidas sólidas de ciberseguridad para la protección integral de la privacidad y la información en el entorno digital, tanto en el ámbito público como privado.

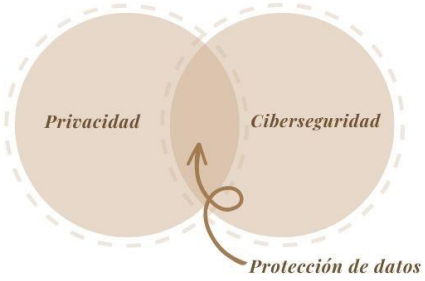

Ilustración 3. Gráfico-Diagrama Relación Seguridad y Privacidad. Fuente: Elaboración propia

3.2 Datos Personales.

Antes de entrar en mayor profundidad en este trabajo, es buen momento para hablar sobre el concepto de dato de carácter personal. ¿Qué entiende la normativa actual por datos de carácter personal y por fichero?; pues bien, siguiendo lo dispuesto en la LOPDGDD y su Reglamento, se puede decir que los datos de carácter personal hacen referencia a «*cualquier información concerniente a personas físicas identificadas e identificables*». Como podemos observar, quedan excluidas las personas jurídicas de este tratamiento y expresamente excluye en la normativa actual la protección a las personas fallecidas. Los datos personales se refieren a cualquier información que pueda identificar directa o indirectamente a una persona. Esta información puede incluir nombres, direcciones, números de teléfono, direcciones de correo electrónico, números de identificación, datos biométricos, preferencias personales y más. En resumen, cualquier dato que pueda utilizarse para identificar a alguien se considera dato personal.

Por otro lado, nos limita el ámbito a «*tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.»* Introduciendo así el concepto de fichero, definido como *«todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica»*.

En el artículo cuarto del Reglamento, enumera un conjunto de definiciones, y en su primer apartado puntualiza dato personal como «*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;* ».

Una de las características clave de los datos personales es su sensibilidad. Algunos datos personales son más sensibles que otros, como aquellos relacionados con la religión, la salud, la orientación sexual o la afiliación política. Estos datos se conocen como categorías especiales de datos personales y están sujetos a un mayor nivel de protección bajo el RGPD.

Existen una serie de principios sobre la protección de datos que vienen enunciados tanto en la Ley como en su Reglamento y que tratan de imponer ciertas restricciones en la recogida de los datos para la creación de los ficheros. Entre estos principios, destaca que los datos recogidos deben respetar las finalidades para las que fueron determinadas, que sean exactos y actualizados y se conculca cualquier recogida de datos por medios fraudulentos o ilegales. Deben ser procesados de manera justa, transparente y lícita. Esto significa que las organizaciones deben informar a las personas sobre cómo se recopilan, utilizan y protegen sus datos personales. También deben obtener el consentimiento explícito de las personas antes de procesar sus datos, a menos que exista una base legal para hacerlo sin su consentimiento.

Es importante que toda la información fluya de la organización hacia abajo, que se sepa con un lenguaje sencillo y comprensible y a través de unos canales de comunicación conocidos, qué hacemos con los datos, cómo se manipulan, cómo se protegen etc.

Por último nos queda un término por cubrir que es la llamada desvinculación, y es que los datos personales capturados para un tratamiento no puedan asociarse con facilidad a los datos personales capturados para otro tratamiento diferente. Esto es necesario para dificultar la creación de perfiles y ayudar a limitar la finalidad de la que somos conscientes.

El RGPD establece que las organizaciones deben implementar medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos personales y prevenir su acceso no autorizado, divulgación, alteración o destrucción. Además, las personas tienen el derecho de acceder a sus datos personales, corregirlos si son inexactos y solicitar su eliminación cuando ya no sean necesarios.

También se establece el principio de responsabilidad proactiva. Esto significa que las organizaciones deben tomar medidas activas para garantizar el cumplimiento del RGPD, como la designación de un responsable de protección de datos, la realización de evaluaciones de impacto en la protección de datos y la implementación de políticas y procedimientos para proteger los mismos. Al almacenar y trabajar todos estos tipos de datos personales, los encargados y los responsables de su tratamiento, deben cumplir con las obligaciones, principios y medidas de seguridad que marca el RGPD, la LOPDGDD y demás normativa.

3.3 El ciberdelito

En la obra de BARRIO ANDRÉS, M., 2017. *Ciberdelitos*: *Amenazas criminales del ciberespacio*. Madrid: REUS editorial. ISBN: 978-84-290-1972-8, se examina el fenómeno según el cual en prácticamente todos los aspectos de la vida contemporánea, existe una profunda dependencia de las Tecnologías de la Información y la Comunicación (TIC). A medida que las redes de comunicación convergen y ofrecen una variedad más amplia de servicios, su susceptibilidad también se incrementa de manera proporcional. De este modo, la interconexión y vulnerabilidad han aumentado de manera constante desde la década de los 90.

Como indican JEWKES, Y. y YAR, M., 2013. *Manual de Delitos en Internet*. Nueva York: Routledge p.105, el término «*CIBERDELITO*» hace referencia a toda actividad ilegal llevada a cabo a través de sistemas informáticos, redes digitales, Internet y otras TIC, tanto de forma directa como asistida. Es decir, a cualquier actividad ilegal llevada a cabo a través de sistemas informáticos y redes digitales. Esto incluye tanto las actividades que se llevan a cabo directamente mediante la tecnología como aquellas que se llevan a cabo con la ayuda de la tecnología.

Todos los peligros derivados de Internet pueden categorizarse en dos grupos principales. En primer lugar, están las amenazas que impactan en los valores legales tradicionales, entre las que se encuentran la preservación de la privacidad, los riesgos asociados al uso de herramientas de espionaje «*sniffers*», la vigilancia digital «*cookies* o *spyware*»; en el ámbito patrimonial se incluiría la considerada técnica del «*phising*», el robo de identidad, los casos de pornografía infantil o la salvaguarda de los derechos de propiedad intelectual. Y en segundo lugar, están los riesgos que recaen sobre las propias infraestructuras, cuando son objeto de ataques con la intención de alterar su operatividad normal, acceder sin autorización o ejecutar ataques deliberados de denegación de servicios «*DoS*».

Todas estas infracciones, que pueden impactar simultáneamente y en diversas ubicaciones, a valores jurídicos tan esenciales como el patrimonio, la privacidad, la libertad y la integridad sexual, han presentado retos y dilemas legales significativos. En respuesta a esta coyuntura, se han promulgado reglamentaciones tanto a nivel estatal como comunitario e internacional. Dada la naturaleza transfronteriza y global de Internet, resulta fundamental fortalecer la cooperación internacional y garantizar la coherencia y cohesión de los marcos normativos nacionales.

Las organizaciones continúan siendo objeto de victimización debido a su amplio uso de las TIC y a los recursos financieros que las hacen objetivos atractivos para los infractores. Además, cualquier individuo que interactúe en línea, participe en foros, intercambie mensajes o comparta contenido, se expone a la posibilidad de sufrir un ataque cibernético que afecte su reputación, privacidad, libertad sexual u otros valores legales similares.

La ciberdelincuencia, y por ende, el ciberdelito, adoptan múltiples manifestaciones y evolucionan constantemente, lo que la convierte en una forma de delincuencia amplia y dinámica. Su naturaleza innovadora y en constante cambio plantea una problemática específica que será explorada.

3.4 La ciberseguridad

El National Institute of Standards and Technology (NIST), el cual fue uno de los organismos pioneros en definir la ciberseguridad, lo hace como el proceso de protección de la información mediante la prevención, detección y respuesta a los ataques.

La ciberseguridad puede definirse más sencillamente como un conjunto de recursos humanos y técnicos y de prácticas destinadas a garantizar un nivel adecuado de seguridad para los activos digitales de una organización.

Puesto que el objeto de este documento es la ciberseguridad, es necesario profundizar en este concepto entendiendo la regulación al respecto que establece Esquema Nacional de Seguridad (E.N.S)[33] y que la define como «*la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos*».

3.4.1 El Esquema Nacional de Seguridad.

El objetivo del Esquema Nacional de Seguridad (ENS) es definir la política de seguridad que se aplicará en el ámbito de los medios electrónicos. Esto se logra estableciendo principios y requisitos que aseguren la protección efectiva de la información. Para ello, se toman en cuenta tanto las normativas europeas relevantes como las directrices específicas propias.

El propósito fundamental del ENS radica en crear un entorno de confianza en el uso de los medios electrónicos. Esto se traduce en la implementación de medidas dirigidas a:

- Garantizar la seguridad de los servicios, comunicaciones, datos y sistemas electrónicos.
- Aumentar la confianza en la capacidad de los sistemas de información para funcionar según lo previsto, libres de interferencias, modificaciones o alteraciones ilícitas e impidiendo el acceso no autorizado a los datos.

La interconexión de los sistemas de información de las administraciones públicas entre sí, así como con los del sector privado, incluidos los de empresas y particulares, plantea problemas de seguridad adicionales. Esto significa que la seguridad va más allá de la protección individual de sistemas específicos. Cada sistema debe definir claramente su alcance, y los responsables de la seguridad deben coordinarse de manera efectiva para evitar áreas sin control y posibles brechas que puedan poner en riesgo la información o los servicios proporcionados.

[33] ESPAÑA. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Boletín Oficial del Estado, 4 de mayo de 2022, (106) https://www.boe.es/eli/es/rd/2022/05/03/311/con

Aunque en muchas ocasiones se utilice de manera indistinta el concepto de «seguridad de la información» y de «ciberseguridad», no son exactamente lo mismo, ya que el primero contiene al segundo. Es decir, la seguridad de la información pretende proteger la información en todos sus estados, en cambio, la ciberseguridad se centra en el ámbito digital.

En las decisiones que se tomen en materia de ciberseguridad deberán tenerse en cuenta los principios fundamentales que marca el ENS:

- Seguridad Integral: Se trata de un procedimiento que abarca todos los recursos tecnológicos, humanos, materiales y organizativos relacionados con el sistema. Concienciar a los individuos (el eslabón más débil) de lo importante que es la seguridad es muy prioritario.
- Gestión de Riesgos: La gestión de la seguridad basada en riesgos es esencial y debe mantenerse actualizada constantemente. Esto asegura un entorno controlado en el que se minimizan los riesgos aceptables.
- Prevención, Detección, Respuesta y Conservación: Deben considerarse estas fases para garantizar que las amenazas no se conviertan en incidentes. Las medidas implementadas tienen como objetivo evitar o reducir tanto las amenazas como los posibles daños al sistema.
- Líneas de Defensa: Es crucial que el sistema tenga una estrategia de defensa ante posibles amenazas o ataques.
- Vigilancia continua y Reevaluación Periódica. Las medidas de seguridad se actualizan y revisan constante a lo largo del tiempo.
- Seguridad como función diferenciada: Los sistemas de información deben distinguir entre roles y diferenciar el responsable de la información del responsable del servicio - responsable de seguridad.

La propia ENS identifica cinco elementos que constituyen la seguridad de la información, definiéndolos de la siguiente manera, para ayudar a comprender el alcance de la idea de ciberseguridad:

Ilustración 4. Seguridad de la Información. Fuente: Elaboración propia

- Disponibilidad: Propiedad o característica de los activos que se refiere al hecho de que son accesibles a las partes o procesos autorizados cuando así lo necesiten.
  Es decir, se trata de que un recurso esté plenamente operativo y preste su servicio con normalidad cuando así se solicite. Esta dimensión puede entrar en conflicto con la confidencialidad ya que el empleo de estrictas medidas de confidencialidad puede ocasionar que la información no esté accesible, aunque sí esté disponible.
- Autenticidad: Cualidad o característica que confirma que una fuente de información es legítima o que una entidad es quien dice ser. Facilita la localización de la fuente de información.
- Integridad: La cualidad o característica de que el activo de información no ha sufrido modificaciones ilegales. Cuando se intercambia información, es importante asegurarse de que un documento llega al destinatario exactamente como fue creado por el remitente, sin modificaciones que comprometan su autenticidad o contenido.
- Confidencialidad: Cualidad o característica que impide que la información se comparta o revele con personas, organizaciones o sistemas no autorizados. Su objetivo es impedir que la información se divulgue sin autorización, de modo que sólo puedan acceder a ella por completo quienes dispongan de la debida autorización.
- Trazabilidad: Cualidad o característica que permite identificar únicamente las acciones de una entidad. Permite gestionar los puntos por los que ha pasado una determinada información de principio a fin, así como observar la evolución y el rastro de esa información.

Un ataque a cualquiera de las mismas podría suponer un incidente de ciberseguridad en la institución. El *Chief Information Security Officer* (CISO), también conocido como director de seguridad de la información, es la figura clave encargada, entre otras cosas, de coordinar la estrategia, informar a la alta dirección y tomar decisiones para satisfacer los requisitos de seguridad de la información.

3.4.2 El ENS y la Protección de datos

A pesar de tener la misma clasificación de riesgos para los datos y la información en el ENS y en el RGPD–clasificados como baja, media o alta-, no tienen el mismo significado para estas normativas.

La clasificación para el ENS se basa en el impacto potencial que un incidente de seguridad puede tener en una organización para lograr sus objetivos, proteger sus activos, cumplir con sus obligaciones de servicio y respetar la ley y los derechos de los ciudadanos. Los niveles de seguridad se determinan para el RGPD en función de la categoría específica a la que pertenezca un dato.

Por lo tanto, la Administración Pública debe adherirse a las leyes de protección de datos, especialmente cuando se trata de información personal de los ciudadanos, aunque cumpla las normas establecidas en el ENS.

3.5 Derechos de los interesados para proteger sus datos personales.

Según las directrices marcadas por el RGPD, la LOPDGDD establece el marco y los requisitos generales para el ejercicio de los derechos de los interesados.

Dispone que el responsable del tratamiento deberá facilitar al interesado la información solicitada de forma clara y concisa cuando así lo solicite el interesado -que podrá ser cualquier persona con capacidad jurídica para obrar actuando por sí misma o a través de representante en los términos previstos-.

En el plazo de un mes desde la recepción de su solicitud, el responsable del fichero está obligado a responder por escrito sobre su situación. Sin perjuicio del derecho del interesado a interponer los recursos y reclamaciones que procedan, la falta de respuesta en el plazo indicado se entenderá como denegación de la solicitud. Si la solicitud se considera excesiva o injustificada, corresponderá al responsable del fichero la carga de la prueba en esta situación, y la decisión será motivada.

El interesado debe recibir la información especificada en la legislación general sobre protección de datos, incluida la identidad y los datos de contacto del responsable del tratamiento, la identidad y los datos de contacto del DPD, si existiera, los fines del tratamiento, el derecho a presentar una reclamación ante la AEPD y el derecho de acceso, rectificación, supresión o limitación del tratamiento. Además de lo anterior, se debe proporcionar la base jurídica del tratamiento, la duración de la conservación de los datos, los tipos de destinatarios de los datos, en particular si son naciones no pertenecientes a la Unión Europea u otras organizaciones internacionales, así como cualquier otro detalle pertinente, en particular si los datos se recogieron sin el conocimiento del interesado.

Cualquier ciudadano que se considere afectado por los datos puede ejercer los siguientes derechos contra el responsable del tratamiento:

• Derecho a la transparencia de la información: Antes de cualquier tratamiento, el interesado debe recibir información clara en el mismo momento en que se recaban los datos. Esta información debe incluir el nombre del responsable del tratamiento, una explicación de cómo se tratarán sus datos, si pueden transferirse a otros países y todos los derechos que el usuario puede ejercer sobre los datos almacenados.

• Derecho de acceso: El interesado tiene derecho a pedir al responsable del tratamiento que confirme si se está tratando o no información personal sobre él. Si se confirma dicho tratamiento, la persona tiene derecho a acceder a los datos y obtener información sobre su origen, su uso previsto, su justificación legal, las categorías de datos implicadas, los posibles destinatarios de dichos datos, durante cuánto tiempo se almacenarán los datos y si es posible ejercer el derecho de rectificación, supresión o limitación del tratamiento de los datos. Además, tendrá derecho a saber de dónde procede la información, pero sólo mientras se mantenga en secreto la identidad de las personas físicas, especialmente si la información procede de fuentes secretas.

Si se proporciona al interesado un sistema directo y seguro a distancia para acceder a sus datos, se considerará concedido el derecho. Puede entregarse de otras formas, siempre que el coste no

se considere excesivo; en ese caso, el interesado sería responsable de sufragar el gasto adicional. Las formas de acceder a los datos serían las propuestas por el responsable del tratamiento si no se aceptara el pago del coste adicional.

• Derecho de rectificación, supresión y limitación del tratamiento: El interesado tiene derecho a que se rectifiquen sin demora los datos erróneos, así como a que se completen los datos incompletos o inexactos. Para ello, deberá enumerar los datos que deben actualizarse junto con los documentos justificativos.

Si el tratamiento de estos datos vulnera los principios sobre la licitud del tratamiento o sobre el tratamiento de categorías especiales de datos, o si así lo exige la ley, los datos deberán suprimirse sin dilación indebida, por iniciativa propia o a petición del interesado, en el plazo máximo de un mes.

Por otra parte, cuando el interesado cuestione la exactitud de los datos y no haya forma de comprobar su veracidad; cuando los datos deban conservarse a efectos probatorios; o cuando el interesado se oponga al tratamiento, el responsable del tratamiento limitará el tratamiento, lo que implica la suspensión del tratamiento o la conservación de los datos para acciones legales.

• Derecho de oposición: Usando este derecho podemos oponernos al tratamiento de nuestros datos personales si, por ejemplo, se utilizan para otra finalidad sin nuestra autorización expresa, u otros motivos particulares acreditados oportunamente.

• Derecho a la portabilidad de los datos: Este derecho da al interesado más control sobre cómo se transfiere su información personal a un tercer responsable del tratamiento de datos. Tenemos derecho a solicitar una copia de la información personal que ha sido tratada por un responsable del tratamiento (el responsable de la transferencia) y a que se envíe inmediatamente a otro responsable del tratamiento (el responsable de la recepción).

• El derecho a quedar exento de decisiones de tratamiento automatizado, incluida la elaboración de perfiles, está protegido por el RGPD, que garantiza que nuestros datos no puedan utilizarse simplemente con fines que tengan repercusiones legales para nosotros. Este derecho no es aplicable si hemos autorizado expresamente al responsable del tratamiento a utilizar los datos para este fin como parte de un contrato entre el interesado y el responsable del tratamiento.

3.6 Deberes de las organizaciones

3.6.1 El responsable del tratamiento de datos.

Esta figura, que se menciona tanto en el artículo 24 como en el 28 del RGPD, desempeña un papel crucial a la hora de determinar las medidas que deben adoptarse para tratar los datos personales de los interesados teniendo siempre presente la integridad y la seguridad de dichos datos. Cuando numerosos responsables del tratamiento trabajan juntos en un mismo proyecto, puede utilizarse el término corresponsable. En esta situación es crucial dejar el acuerdo por escrito.

El responsable del tratamiento es quien toma las decisiones acerca de los propósitos, los objetivos y los métodos de procesamiento, independientemente de si es la persona que lleva a cabo físicamente el proceso de manejo de la información. El papel de responsable del tratamiento puede ser asumido tanto por una persona física como por una entidad legal o una organización. En otras palabras, es una entidad o persona que decide los fines y medios del procesamiento de datos y determina cómo y por qué se recopilan, almacenan, utilizan y comparten los datos personales. Cada responsable del tratamiento debe llevar un registro de todas las actividades del tratamiento. En cualquier organización, los empleados que tratan estos datos lo hacen siguiendo las instrucciones que han sido dadas por el responsable del tratamiento.

En el contexto de la administración pública, por lo general, el responsable del tratamiento es el organismo administrativo que tiene la competencia relacionada con el asunto en cuestión, para el cual se requiere el tratamiento de datos personales. Esto es válido siempre que dicho organismo tenga la autoridad para tomar decisiones acerca del propósito y los métodos de este tratamiento.

El responsable del tratamiento debe actuar de forma íntegra y responsable, asegurándose de que la información personal se utiliza legalmente y que se respetan los derechos de privacidad de las personas.

Las empresas y personas que actúan como responsables del tratamiento de datos deben cumplir estrictamente sus obligaciones legales y éticas para proteger los datos personales y mantener el cumplimiento de las normas vigentes. En caso de no hacerlo, veremos más adelante las consecuencias que puede acarrear.

3.6.2 El encargado del tratamiento.

La figura del encargado del tratamiento de datos[34] es fundamental en este Trabajo Final de Grado, ya que gira en torno a él. El encargado puede ser una persona física o jurídica, autoridad pública, servicio u organismo que brinda un servicio al responsable y realiza el tratamiento de datos personales en su nombre.

Existen diferentes tipos de encargados del tratamiento y diversas formas en las que se regula la relación con el responsable, dependiendo del tipo de servicio que se preste y el acceso a los datos personales que ello conlleve. Es importante tener en cuenta que el responsable es quien decide sobre la finalidad y uso de la información, mientras que el encargado del tratamiento debe cumplir con las instrucciones del responsable en relación al tratamiento de los datos personales a los que tenga acceso.

El encargado del tratamiento puede llevar a cabo todos los procesos, automatizados o no, que el responsable le haya encomendado formalmente, desde la recopilación hasta la supresión de los datos. El acuerdo entre las partes debe estar claramente delimitado. El encargado del tratamiento puede tomar decisiones organizativas y operativas necesarias para la prestación del servicio contratado, pero no puede cambiar las finalidades ni utilizar los datos para sus propios fines. Sus decisiones deben siempre estar en línea con las instrucciones del responsable.

Es importante elegir un encargado del tratamiento que garantice la implementación y mantenimiento de medidas técnicas y organizativas adecuadas para proteger los derechos de las personas afectadas. Esto puede demostrarse a través de la adhesión a códigos de conducta o la posesión de un certificado de protección de datos. La relación entre el responsable y el encargado del tratamiento debe establecerse mediante un acto jurídico (contrato), que debe constar por escrito, incluso en formato electrónico.

En el ámbito del sector público, las competencias de encargado del tratamiento pueden ser atribuidas a un órgano administrativo o a organismos autónomos mediante una norma reguladora que cumpla con los requisitos establecidos en el artículo 28.3 del RGPD.

[34] UNION EUROPEA, 2016. 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) [en línea] https://www.boe.es/doue/2016/119/L00001-00088.pdf

3.6.3 El delegado del tratamiento de datos (DPD)

Su designación vendrá acordada por los responsables y encargados del tratamiento que será obligatoria en los casos del art. 37.1 del Reglamento (UE) 2016/679 y, en todo caso:

- Los consejos generales y colegios profesionales.
- Las instituciones académicas, incluidas las universidades públicas y privadas.
- Organizaciones que gestionan redes y servicios de comunicaciones electrónicas que manejan muchos datos personales.
- Prestadores de servicios de la sociedad de la información que elaboren ampliamente perfiles de usuarios.
- Entidades enumeradas en el artículo 1 de la Ley 10/2014, aprobada el 26 de junio y que regula la supervisión, regulación y solvencia de las entidades financieras.
- Empresas que concedan créditos financieros.
- Empresas que ofrecen seguros y reaseguradoras.
- Prestadores de servicios de inversión sujetos a la normativa del Mercado de Valores.
- Comercializadoras y distribuidoras de electricidad y gas natural.
- Entidades de archivo común para la evaluación de la solvencia patrimonial y crédito, o para la prevención del fraude.
- Organizaciones publicitarias implicadas en tratamientos basados en las preferencias de las personas afectadas o en la elaboración de perfiles.
- Los centros sanitarios que están obligados a conservar los historiales médicos de los pacientes. Se excluyen los profesionales sanitarios que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, practiquen su actividad a título individual.
- Organizaciones que publican informes comerciales que pueden incluir a personas concretas.
- Personas que dirigen operaciones de juego a través de medios interactivos, telemáticos, informáticos y electrónicos.
- Servicios de seguridad para particulares.
- Federaciones deportivas que manejen datos de menores.

Los responsables o encargados del tratamiento que no se encuentren en las situaciones anteriores podrán elegir voluntariamente un DPD. En dicho caso, deberán informar a la AEPD o a la autoridad autonómica de EP de la designación, nombramiento o cese de estos DPD en el plazo de 10 días. La AEPD y las autoridades de DP autonómicas dispondrán en línea de una lista actualizada de los mismos.

Dependiendo del volumen de tratamiento, del tipo de datos tratados o de los peligros para los derechos o la libertad del interesado, los responsables y encargados del tratamiento podrán decidir dedicar al DPD a tiempo completo o parcial.

A la hora de elegir un DPD se tendrá en cuenta la obtención de un título universitario que acredite conocimientos especializados en legislación y práctica de la protección de datos. La posición del DPD es importante, ya que:

- Representará los intereses del responsable o encargado del tratamiento ante la AEPD y las autoridades locales de protección de datos.

- No podrá ser despedido ni sancionado por el desempeño de sus responsabilidades, salvo que haya mediado dolo o negligencia grave.
- No deben existir conflictos de intereses y debe garantizarse la independencia del DPD dentro de la organización.
- Tiene derecho a ver los datos de carácter personal y los procedimientos de tratamiento (no debe haber resistencia por existir un deber de confidencialidad o secreto).
- Cuando exista una violación de seguridad pertinente de protección de datos, tomará nota de ella, documentará e informará a los equipos de administración y gestión del responsable del tratamiento o al encargado del tratamiento.

Además, a continuación se indica cómo debe intervenir el DPD en los casos de reclamaciones presentadas ante las autoridades de protección de datos:

1. Antes de presentar una reclamación contra el responsable o el encargado del tratamiento ante la AEPD o, en su caso, ante las autoridades autonómicas de protección de datos, el interesado podrá dirigirse al DPD cuando se haya designado uno. En este caso, el DPD deberá notificar la decisión tomada al interesado en el plazo máximo de dos meses desde la recepción de la reclamación.

2. El DPD dispondrá de un mes para reaccionar si el interesado presenta una reclamación ante la AEPD o, en su caso, ante una autoridad autonómica de protección de datos. La cual elevará la reclamación al DPD. La autoridad continuará el procedimiento abierto en los términos previstos en el Título VIII de la LO y normativa posterior si, transcurrido este plazo, el DPD no ha notificado a la autoridad de protección de datos correspondiente la resolución aportada a la reclamación.

3.6.4 Obligaciones del responsable y del encargado del tratamiento.

De conformidad con los principios generales de protección de datos, el responsable del tratamiento debe adoptar y aplicar las siguientes medidas:

- Análisis de riesgos: con carácter previo a la realización de las operaciones de tratamiento, el responsable del tratamiento debe valorar siempre, de acuerdo con la ponderación que ordena el principio de proporcionalidad, el nivel de perjuicio que el tratamiento de los datos puede causar a los ciudadanos y la finalidad.

- Adopción de las medidas técnicas y organizativas necesarias con el fin de garantizar el cumplimiento de la ley. Adopción de medidas de seudonimización (anonimización de datos personales) y minimización de datos personales. Adopción de restricciones de acceso a los datos personales por parte de los responsables de su almacenamiento. Si hay dos o más responsables del tratamiento, deben determinar las medidas que deben adoptarse conjuntamente mediante un acuerdo.

Se permite la transferencia del tratamiento a la figura del encargado del tratamiento, ya sea persona física o jurídica, pública o privada. Sólo podrá hacerse si se ofrecen garantías suficientes de que el tratamiento se llevará a cabo de conformidad con la ley, y no podrá transmitirse a otro encargado sin el consentimiento previo del responsable del tratamiento. La transmisión debe realizarse mediante la firma de un contrato o acuerdo en el que se establezcan las condiciones y obligaciones del encargado del tratamiento de conformidad con lo dispuesto en la ley.

- Llevar un registro de las actividades de tratamiento: cada responsable y encargado del tratamiento está obligado a llevar y mantener un registro de todas las actividades que se realicen con dicho tratamiento. El encargado del tratamiento también debe mantener el registro por escrito, aunque puede mantenerlo electrónicamente, y la AEPD debe tener acceso a él en todo momento.

- Los responsables y encargados del tratamiento están obligados a mantener un registro de las operaciones realizadas durante el tratamiento automatizado de datos. Debe abarcar la recogida, modificación, consulta, comunicación, incluidas las transferencias, comunicación y supresión de datos personales. Los registros de consulta y comunicación deben incluir la fecha, hora, justificación y, si es posible, la identidad de la persona que consultó o comunicó los datos, así como la identidad de los destinatarios. La AEPD debe tener acceso a este registro para verificar la legalidad del tratamiento y garantizar la seguridad de los datos.

- Se requiere una colaboración constante con AEPD.

- Realizar una evaluación de impacto en relación con el tratamiento de datos: cuando la operación de tratamiento suponga un alto riesgo para los derechos de los ciudadanos, el responsable del tratamiento deberá realizar en primer lugar una evaluación del impacto que la operación de tratamiento tendrá en los derechos y libertades de las personas. La AEPD puede establecer una lista de operaciones de tratamiento que requieren una evaluación de impacto y otra lista de operaciones de tratamiento que no requieren una evaluación de impacto. Ambas categorías deberán tener carácter indicativo. Dicha evaluación requerirá la consulta previa a la AEPD. Además de ejercer sus facultades de investigación, rectificación y consulta, la Agencia también podrá proporcionar orientaciones por escrito al responsable o al encargado del tratamiento con el fin de proteger los derechos de los ciudadanos.

- Medidas de seguridad para el tratamiento: el responsable y el encargado del tratamiento deben aplicar las medidas de seguridad técnicas y organizativas necesarias y apropiadas para garantizar un nivel de seguridad adecuado en cada fase del tratamiento, en particular en lo que respecta a las categorías de datos sensibles. Control de acceso a las aplicaciones; control de los soportes de datos para impedir el acceso de personas no autorizadas que puedan leerlos, copiarlos o suprimirlos; control de fiabilidad e integridad, etc. Toda esta protección de datos debe ser desde el diseño y por defecto.

- Notificación a la AEPD de cualquier vulneración de la seguridad: Cualquier violación, brecha o quebrantamiento de la seguridad deberá ser notificado a la AEPD, salvo que sea improbable que suponga una amenaza para los derechos y libertades de los afectados. La notificación deberá realizarse en el plazo de setenta y dos horas desde el descubrimiento de la violación de seguridad, y deberá contener la información especificada en el artículo 38.3 de la Ley (naturaleza de la violación, categorías de datos e individuos afectados; posibles consecuencias de la violación; información de contacto del DPD; medidas adoptadas para remediar la violación o mitigar sus efectos). Si existe un alto riesgo para los derechos y libertades de las personas, también deberá notificarse la violación al interesado.

Dicha notificación podrá evitarse si el responsable del tratamiento ha adoptado medidas previas (por ejemplo, cifrado) o posteriores para evitar ese alto riesgo para los derechos de las personas, o si exigiera un esfuerzo desproporcionado debido al gran número de personas potencialmente afectadas, en cuyo caso será necesario publicar la violación de una manera accesible a los interesados (boletín oficial, sede electrónica u otro canal oficial que permita una comunicación efectiva).

La notificación podría aplazarse, limitarse u omitirse si concurriera alguna de las causas de fuerza mayor señaladas en el artículo 24 de la Orden Legislativa 7/2021 (salvaguardar derechos de terceros, que pudiera comprometer una investigación, que afecte a la seguridad nacional, etc.).

3.7 Organismos de ciberseguridad

La creación de una cultura de ciberseguridad lleva años siendo una preocupación de la gran mayoría de instituciones de cierta entidad, es por ello, que existen varios organismos que sirven de gran apoyo a la Policía Nacional. Destacan los siguientes:

CCN. El Centro Criptológico Nacional se creó en el año 2004 a través de Real Decreto 421/2004 y está adscrito al Centro Nacional de Inteligencia con el que comparte medios, procedimientos y recursos. Tiene encomendadas las funciones relativas a la seguridad de las Tecnologías de la Información y protección de la información clasificada. Su misión es contribuir a la mejora de la ciberseguridad española constituyéndose como centro de alerta y respuesta ante ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas capacidades de respuesta a incidentes o Centro de Operaciones de Ciberseguridad. Forma a personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas para ello.
Entre todas las herramientas que ofrece destacan especialmente las Guías CCN-STIC de Seguridad, las cuales son normas, instrucciones, guías y recomendaciones que son actualizadas periódicamente. Aunque algunas de ellas están dirigidas al personal de las Administraciones Públicas, otras son de difusión pública para todos los usuarios. Su temática abarca temas como el uso de productos de cifrado, herramientas de gestión de red, organización y gestión de la seguridad de los sistemas TIC, seguridad en dispositivos móviles, herramientas de análisis de vulnerabilidades, dispositivos biométricos, productos de Microsoft, configuración segura de sistemas Linux, securización de bases de datos y servidores, procedimiento de investigación de código dañino, procedimientos de empleo seguro, etc.
En este marco, el Esquema Nacional de Seguridad, o ENS, se encarga de llevar a cabo la política de seguridad en relación al acceso, la integridad y la veracidad de los datos, así como de mantener la protección esencial de la información. El Centro Criptológico Nacional (CCN) y los Ministerios de la Presidencia, Política Territorial y Administraciones Públicas trabajaron de forma conjunta para construir el ENS en 2017. Todos los organismos públicos y empresas privadas que ofrezcan servicios a los primeros deberán utilizar este ENS, el cual debe especificar las garantías que deben aplicarse en caso de tratamiento de datos para evitar su pérdida, manipulación o acceso. Los responsables y encargados del tratamiento de datos, como no puede ser de otra forma, también están obligados a implantar las medidas de seguridad necesarias.

INCIBE. Desde octubre de 2014 abandona su anterior denominación como INTECO (Instituto Nacional de Tecnologías de la Comunicación) y depende del Ministerio de Asuntos Económicos y Transformación Digital. Su misión es el desarrollo de la ciberseguridad y la confianza digital de ciudadanos, redes académicas y de investigación, profesionales, empresas. Ofrece «*kits de concienciación*», organización de eventos, ayudas a la investigación, guías temáticas, formación asesoramiento, etc. OSI. Perteneciente a INCIBE y financiado por la Unión Europea mediante el instrumento *Next Generation* EU, proporciona información para reforzar la confianza en el ámbito digital a través de la formación en ciberseguridad. Entre otros servicios, ofrece un canal de avisos con alertas actualizadas de seguridad clasificadas por fecha y criticidad. Además, incluye talleres, recursos descargables, test de ciberseguridad, juegos educativos…

IS4K. Es un portal perteneciente a INCIBE cuyo objetivo es la promoción del uso seguro y responsable de Internet y nuevas tecnologías entre los menores. Además, ofrece un servicio de ayuda a familias y profesionales del ámbito de los menores para hacer frente a los riesgos de Internet. Da soporte a Fuerzas y Cuerpos de Seguridad para reducir la disponibilidad de contenido criminal en la red.

OCC. Es la nueva denominación que el Real Decreto 734/2020 establece para la antigua Oficina de Coordinación Cibernética. Está integrada orgánicamente dentro del CNPIC (Centro Nacional de Protección de Infraestructuras Críticas), el cual depende de la Secretaría de Estado de Seguridad. Desarrolla la colaboración técnica en materia de ciberseguridad entre la Secretaría de Estado de Seguridad y sus organismos dependientes. Actúa como punto de contacto nacional de coordinación operativa para el intercambio de información con la Comisión Europea y los Estados miembros.

Europol EC3. El European Cybercrime Centre fue fundado en 2013, está ubicado en La Haya y ofrece apoyo operativo, estratégico, analítico y forense a las investigaciones de los Estados Miembros. Aunque está más enfocado en la ciberdelincuencia sirviendo como punto central de información e inteligencia, también proporciona apoyo técnico inmediato 24 horas ante ciberincidentes o «*cibercrisis*» a través del Protocolo de Respuesta de Emergencia para cuerpos policiales de la Unión Europea (EU LE ERP). Asimismo, ofrece formación y refuerzo de capacidades en su campo de actividad.

3.8 Autoridades de control. Organismos de Protección de Datos

La AEPD y las autoridades autonómicas de protección de datos se rigen por los artículos 48 y siguientes de la ley en sus respectivos ámbitos de competencia.

En todo caso, la AEPD cumple las funciones de asesoramiento, supervisión, investigación y control del cumplimiento de las disposiciones relativas al derecho a la protección de datos, así como la gestión de las reclamaciones, la sanción de las infracciones y la cooperación con otras agencias europeas de protección de datos. La AEPD es la autoridad estatal de referencia y la representante española ante el Comité Europeo de Protección de Datos (CEPD) previsto en el RGPD.

En Europa, el Comité Europeo de Protección de Datos (CEPD)

El Comité Europeo de Protección de Datos (CEPD) es una entidad independiente de la Unión Europea (UE) encargada de supervisar y garantizar la aplicación coherente de las normativas de protección de datos en todos los estados miembros de la UE. Fue establecido por el Reglamento General de Protección de Datos. El CEPD desempeña un papel clave en la promoción de la cooperación entre las autoridades de protección de datos de los diferentes países de la UE.

Las principales funciones y responsabilidades del Comité Europeo de Protección de Datos incluyen:

- Coordinación y Asesoramiento: El CEPD facilita la coordinación entre las autoridades de protección de datos de los estados miembros para garantizar la aplicación uniforme y coherente de las leyes de protección de datos en toda la UE. También emite orientaciones y asesoramientos sobre cuestiones relacionadas con la protección de datos.
- Opiniones y Recomendaciones: El CEPD emite opiniones y recomendaciones sobre cuestiones relevantes de protección de datos, como acuerdos internacionales que involucren transferencias de datos personales fuera de la UE.
- Decisiones Conjuntas: En situaciones en las que una autoridad de protección de datos de un estado miembro desee tomar una decisión que tenga un impacto significativo en toda la UE, el CEPD puede tomar decisiones conjuntas para garantizar la coherencia.
- Mediación y Resolución de Conflictos: El CEPD puede facilitar la mediación y la resolución de conflictos entre las autoridades de protección de datos de diferentes países de la UE cuando surjan desacuerdos sobre casos transfronterizos.
- Promoción de Conciencia Pública: El CEPD trabaja para aumentar la conciencia pública sobre la importancia de la protección de datos y los derechos de privacidad.

En resumen, el CEPD es una entidad clave en la supervisión y promoción de la protección de datos en la Unión Europea. Su objetivo principal es garantizar que las normativas de protección de datos, se apliquen de manera coherente en todos los estados miembros, protegiendo así los derechos y la privacidad de los ciudadanos en el entorno digital.

En España, la Agencia Española de Protección de Datos (AEPD)

Es una Autoridad Administrativa independiente de ámbito estatal, con personalidad jurídica y plena capacidad pública y privada. Se relaciona con el Gobierno a través del Ministerio de Justicia. Tiene la condición de representante común de las autoridades de PD de España en el Comité Europeo de Protección de Datos (CEPD).

Tanto la AEPD como el Consejo General del Poder Judicial (CGPJ) colaboran en las competencias que la LO 6/1985 del Poder Judicial, les atribuye en materia de Protección de Datos.

Entre sus funciones y potestades, se encuentran:

- Supervisar la aplicación de la LO 3/2018 y del Reglamento (UE) 2016/679, o la LO 7/2021 y la Directiva 2016/680 según proceda.
- El desempeño de las funciones y potestades que le atribuyan otras Leyes o normas Europeas.
- Regulación y Acción Exterior.
- Dictar las Circulares de la AEPD.

Su Presidente será nombrado por el Gobierno (en Consejo de Ministros), a propuesta del Ministerio de Justicia, mediante Real Decreto, entre personas de reconocida competencia profesional, previa evaluación del mérito, capacidad, competencia e idoneidad en particular en materia de protección de datos.

3.9 Entendiendo los riesgos. Consecuencias administrativas, civiles y penales.

El procesamiento de datos personales conlleva una serie de obligaciones de naturaleza administrativa, civil y, en algunos casos, penal. Estas obligaciones requieren abordar tanto las sanciones administrativas o penales impuestas como resultado de la comisión de actos considerados ilícitos, así como la reparación de los daños causados por dicho procesamiento de datos. Los responsables de archivos, los encargados del tratamiento, los responsables de la seguridad y otras personas relacionadas directa o indirectamente con el archivo, a quienes se les atribuyan responsabilidades en virtud de sus facultades o acciones, asumirán estas responsabilidades, ya sea individualmente o en conjunto, según corresponda.

Responsabilidades derivadas de infracciones administrativas: En cuanto a las responsabilidades derivadas de infracciones administrativas, el responsable y, en su caso, el encargado del tratamiento, junto con el titular del fichero, serán responsables solidarios de las acciones (u omisiones) ilícitas que se produzcan en las distintas fases de creación y utilización del fichero y que estén previstas en la normativa de protección de datos. Estas acciones también pueden dar lugar a sanciones disciplinarias, si procede, en el caso de los archivos de la Administración Pública.

Responsabilidades civiles: El responsable y, en su caso, el encargado del tratamiento, junto con el titular del archivo, responderán solidariamente de las acciones u omisiones que sean competencia de la ley. Estas responsabilidades se incumplen en virtud de contratos, lo que da lugar a responsabilidades contractuales, y actividades perjudiciales que tienen lugar fuera de una relación contractual, lo que da lugar a responsabilidades extracontractuales.
Es necesario que se haya cometido un daño real, concreto, personal, directo y que afecte a los intereses legítimos de la víctima para exigir esta responsabilidad civil. Tanto el aspecto patrimonial como el moral del daño pueden repercutir en el bienestar espiritual de la víctima, especialmente si se vulneran sus derechos al honor, a la intimidad o a la propia imagen. El aspecto patrimonial incluye la pérdida efectiva y el lucro cesante. El aspecto moral incluye cualquier daño que pueda tener un impacto en el bienestar espiritual de la víctima.
Es importante tener en cuenta que la responsabilidad civil ha pasado de un punto de vista subjetivo que exigía la existencia de culpa o negligencia a una perspectiva objetiva que se centra en la reparación del daño en sí a la hora de atribuir a terceros la responsabilidad de reparar el daño causado. La noción de responsabilidad objetiva suele aplicarse en los casos de pérdidas ocasionadas por el tratamiento automatizado de datos personales en los que los riesgos son asumidos por las partes afectadas debido a los procedimientos tecnológicos a los que se someten los datos. Sin embargo, esta responsabilidad objetiva debe tener en cuenta las precauciones tomadas para disminuir los riesgos relacionados con el tratamiento automatizado de datos, y estas precauciones deben cumplir las normas establecidas por la ley.

Responsabilidades penales: En relación con las responsabilidades penales, el autor del acto ilícito asumirá personalmente las consecuencias de sus propias acciones. Algunos delitos relacionados con el tratamiento de los datos personales y su protección son los siguientes:

- Los delitos de daños son aquellos que tienen como resultado el deterioro de activos de información físicos, lógicos o intangibles en equipos, soportes u otros materiales físicos ajenos. Esto incluye aplicaciones, programas, documentos electrónicos, etc.
- Delito de coacciones: cometido por cualquiera que, sin una razón válida, prohíba a otro hacer algo, como en el caso de los ataques a la disponibilidad de datos provocados por el cierre de sistemas informáticos o el borrado de datos.
- Estafa: cometida por cualquiera que consiga la transferencia no consentida de cualquier bien patrimonial en perjuicio de un tercero para obtener un beneficio económico mediante la manipulación informática o artimañas similares.
- Delito de descubrimiento o revelación de secretos: cometido por quien acceda, revele o ceda datos sin autorización a un tercero, así como por quien utilice los datos con conocimiento de la actividad ilícita, en perjuicio del titular del fichero o de la persona en cuestión. Como en el caso de la revelación realizada por el encargado del tratamiento, este delito suele tener un tipo agravado que supone la revelación de secretos ajenos que conoce por razón de su empleo u oficio. Además, cuando se divulga material muy sensible y los actos se realizan con ánimo de lucro, se consideran agravantes.
- Contra la propiedad intelectual: Quien copie, plagie, distribuya o transmita públicamente una obra protegida por la propiedad intelectual, en todo o en parte, con ánimo de lucro a costa de un tercero, es culpable de un delito contra la propiedad intelectual. Recuerde que las bases de datos, las recopilaciones de datos y los programas informáticos se encuentran entre las obras que protege la propiedad intelectual.
- Descubrimiento de secretos de empresa: Quien se apodere de datos, documentos electrónicos, soportes informáticos u otros materiales comparables con el fin de conocer un secreto de empresa es culpable del delito de descubrimiento de secretos de empresa.

«*Conviene por último recordar que la responsabilidad penal suele llevar aparejada la correspondiente responsabilidad civil*.».[35]

Respecto al papel de la AEPD en la aplicación de la LOPDGDD y del RGPD, en un artículo de *Business Insider*[36] se destaca cómo el RGPD ha ayudado a Europa a convertirse en líder mundial en la protección de datos personales. El artículo también recalca que, debido a que la mayoría de las empresas tecnológicas importantes tienen su sede en Irlanda, se ha producido un cuello de botella en la Comisión de Protección de Datos irlandesa, lo que ha dificultado la aplicación de la noción de «*ventanilla única*».

El informe señala que, desde la aplicación del RGPD en 2018, las multas impuestas a las empresas que lo han infringido han ido aumentado constantemente. De 436.000 euros en 2018 a casi 1,304 millones de euros en 2021, incrementaron las multas. Sin embargo, las multas disminuyeron ligeramente hasta casi 900 millones de euros en 2022, aunque siguieron siendo extremadamente elevadas.

[35] *Responsabilidades derivadas de tratamientos de datos nominativos* [en línea] [10 de agosto 2023] http://www.iee.es/pages/bases/articulos/derint026.html#_ftn4
[36] *Business insider* [en línea] [23 de agosto de 2023] https://www.businessinsider.es/5-mayores-multas-vulnerar-rgpd-espana-2022-1165298

Menciona algunas multas importantes que se han propuesto para *Meta* (antes *Facebook*) y *Clearview* AI en varios países de la UE. Empresas como *Google* o *Amazon* tampoco se han escapado, y han sido sancionadas con multas millonarias en España por la AEPD.

En el artículo se destacan las multas impuestas a empresas de telecomunicaciones por no tomar las precauciones adecuadas para impedir el «un método utilizado por los piratas informáticos para acceder a los datos de las tarjetas SIM de las víctimas.

Por último, se resalta que *Google* recibió de la AEPD la multa más elevada de 2022, por un total de 10.000.000€, por revelar indebidamente datos a terceros y obstaculizar el derecho a ser eliminado. *Google* colaboró con el proyecto *Lumen*, que investigaba las demandas de eliminación de enlaces de los resultados del buscador. La AEPD consideró que esto otorgaba a Google discrecionalidad para decidir cómo debía aplicarse el RGPD, lo que era contrario a la ley según las leyes de protección de datos personales.

Además de estas sanciones del 2022 vistas en este artículo, cabe destacar otras sanciones importantes como cuando la AEPD sancionó con 20.000 euros a un centro médico por vulnerar la confidencialidad de las pruebas Covid de una trabajadora.[37]Cuando *CaixaBank* fue multada con 6 millones de euros por el uso indebido de datos personales de sus clientes[38], o cuando *BBVA* fue sancionado por la AEPD con 5 millones de euros por el uso de datos de sus clientes sin consentimiento, siendo una de las multas más elevadas de la protección de datos.[39]

En resumen, se debe cumplir con la protección de datos o nos arriesgamos a recibir desde sanciones derivadas del incumplimiento del RGPD y LOPDGDD importantes como las que hemos visto, perder la confianza y reputación de los usuarios o incluso llegar a tener consecuencias penales.

[37]*Confi Legal* [en línea] [25 de junio de 2023] https://confilegal.com/20220509-aepd-sanciona-con-20-000-euros-a-un-centro-medico-por-vulnerar-la-confidencialidad-de-las-pruebas-covid-de-una-trabajadora/
[38] *20 Minutos* [en línea] [28 de julio de 2023] https://www.20minutos.es/noticia/4545209/0/multa-millonaria-caixabank-ilicito-datos-clientes/
[39] *AEPD* [en línea] [28 de julio de 2023] https://www.aepd.es/es/documento/ps-00070-2019.pdf

4. Problemas y soluciones

Una vez vista la base legal con la que trabajamos, la problemática de no tener en cuenta la relación entre ciberseguridad y privacidad en consideración desde un principio en las organizaciones, la falta de estandarización en la ciberseguridad, las consecuencias administrativas, civiles y/o penales a las que se puede enfrentar en el caso de no poner en práctica la normativa legal vigente... Se va a proporcionar una guía de buenas prácticas para ayudar y orientar a todo encargado de protección de datos, con el fin de que realice sus labores diarias de la manera más eficaz y eficiente posible.

Se propone facilitar una guía que englobe todos los trámites obligatorios y posibles junto a la documentación requerida. Desde la firma de un contrato legal que lo una al responsable del tratamiento hasta un listado de buenas prácticas para ayudar a su propia ciberseguridad, y por ende, a la ciberseguridad de los usuarios finales. Con ello esperamos evitar que el EPD tenga que revisar o utilizar manuales de diferentes fuentes, lo que puede hacer que, como procesadores de datos personales, se cometan errores, se omitan pasos, se pierda más tiempo del debido o, lo que es peor, generemos una brecha de seguridad irreparable.

4.1 Solución propuesta

Las siguientes características se incorporarán a una guía de buenas prácticas de un EPD:

1. La formalización del contrato con el responsable del tratamiento. Debe utilizarse un contrato u otro acuerdo jurídicamente vinculante entre el responsable del tratamiento y el encargado del tratamiento para establecer las normas que rigen su relación. El acuerdo, contrato o acción legal debe realizarse por escrito, incluso en formato electrónico.
2. Registro de Actividades del tratamiento:
   2.1. Herramienta FACILITA
   2.2. Herramienta RAT
   2.3. Plantilla de registro de la actividad de tratamiento
3. Legitimación del Tratamiento:
4. Designación de un DPD, en su caso.
5. Análisis de Riesgos.
6. Establecer medidas de seguridad
7. Tareas de Concienciación
8. Notificación de Incidentes de seguridad.

4.2 Plan de trabajo

En este epígrafe se ofrece una breve estimación del tiempo empleado en la creación de esta obra. Hemos dividido el procedimiento en 5 pasos, que se representan gráficamente en la imagen adjunta mediante una línea de tiempo. La fecha de inicio data de abril del presente año, donde tras tener un primer contacto con el tema del mismo, se crea un primer esbozo de lo que iba a ser el trabajo final, concertando una cita con el Tutor que lo dirige y poniéndolo encima de la mesa.

Estas etapas se han solapado en el tiempo, ya que no era necesario la finalización de una para comenzar la siguiente. El cómputo total de horas ha sido aproximadamente unas 320 horas, con una carga mayoritaria en los meses de verano.

Ilustración 5 Proceso de trabajo. Elaboración propia

5. Diseño de la solución: El buen encargado del tratamiento

5.1 Contrato

Como se ha mencionado anteriormente, para establecer formalmente la relación entre un responsable del tratamiento y un encargado del tratamiento es necesario un contrato u otro acuerdo jurídico que vinculara a ambos. Por lo tanto, si la relación aún no se ha formalizado, el responsable del tratamiento debe hacerlo.

Se debe incluir al menos:

- La naturaleza, duración e intención del tratamiento.
- Las categorías de interesados y los tipos de datos personales.
- El encargado del tratamiento sólo debe utilizar los datos personales de acuerdo con las instrucciones escritas del responsable del tratamiento.
- Requisitos para que el responsable del tratamiento apruebe previamente la subcontratación, ya sea de forma específica o general.
- La obligación de discreción.
- Las precauciones de seguridad que el responsable debe tomar para garantizar el cumplimiento del GDPR.
- La ubicación de los datos cuando finalice la prestación del servicio.

Aunque el responsable del tratamiento es en última instancia el responsable del tratamiento y determina su existencia e intención, tanto el Encargado del tratamiento como el Responsable del tratamiento pueden enfrentarse a sanciones en virtud del RGPD si incumplen sus compromisos.

En algunos casos, los Encargados del tratamiento están sujetos a responsabilidades descritas en el RGPD que van más allá de los términos del contrato que le vincula al Responsable del tratamiento y pueden estar sujetos a una supervisión independiente por parte de las autoridades de protección de datos.

En la guía este debe ser nuestro primer punto como EPD, la realización del acto jurídico que nos une a un Responsable del tratamiento.

Esta plantilla estándar se proporciona adjunta en formato PDF en el anexo de este TFG.

CONTRATO ESTÁNDAR

1. Objeto del encargo del tratamiento

Mediante las presentes cláusulas se habilita a la entidad [ ], encargada del tratamiento, para tratar por cuenta de [ ], responsable del tratamiento, los datos de carácter personal necesarios para prestar el servicio de [ ].

El tratamiento consistirá en: *(descripción detallada del servicio)*

[ ]

Concreción de los tratamientos a realizar:

- ☐ Recogida
- ☐ Registro
- ☐ Estructuración
- ☐ Modificación
- ☐ Conservación
- ☐ Extracción
- ☐ Consulta
- ☐ Comunicación por transmisión
- ☐ Difusión
- ☐ Interconexión
- ☐ Cotejo
- ☐ Limitación
- ☐ Supresión
- ☐ Destrucción
- ☐ Conservación
- ☐ Comunicación
- ☐ Otros: [ ]

2. Identificación de la información afectada

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, la *entidad/órgano* [ ], responsable del tratamiento, pone a disposición de la entidad [ ], encargada del tratamiento, la información que se describe a continuación:

- [ ]
- [ ]

Ilustración 6 Modelo de contrato tipo. Elaboración propia

5.2 Registro de Actividades del tratamiento:

Todas las operaciones de tratamiento realizadas por el responsable o el encargado del tratamiento deben estar documentadas. Para que la autoridad de control competente pueda utilizar los registros y hacer un seguimiento de las operaciones de tratamiento, tanto los responsables como los encargados están obligados a colaborar con ella. En consecuencia, deben poner el registro de actividades del tratamiento a su disposición cuando los solicite.

FACILITA es una plataforma que permite a las empresas que manejan datos personales de forma segura cumplir con el RGPD. Se trata de una utilidad gratuita y fácil de usar. Una vez finalizada su implantación, se elimina toda la información remitida durante su creación, lo que garantiza que la Agencia nunca sabrá qué información se ha facilitado.

Para que el usuario evalúe su situación respecto al tratamiento de datos personales que realiza, y saber si cumple los requisitos para utilizar *FACILITA* RGPD o si es necesario realizar un análisis de riesgos, sólo son necesarias tres pantallas de preguntas muy concretas. Esto la convierte en una herramienta ideal para cualquier empresa o profesional.

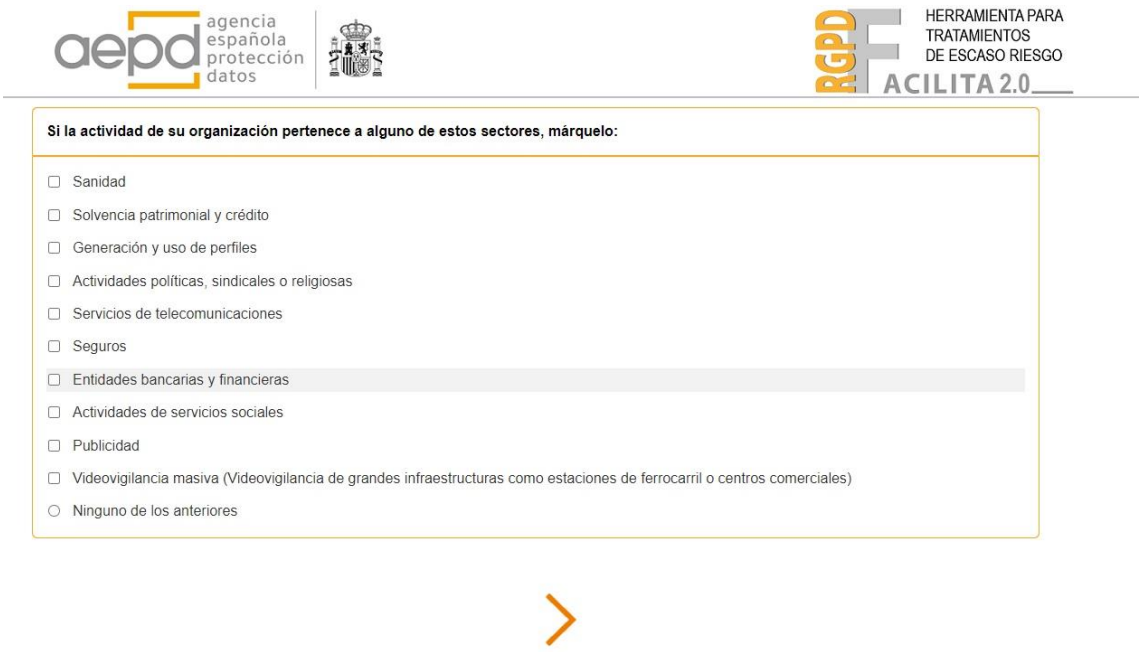

Ilustración 7 Herramienta Facilita - AEPD -

Se trata de un cuestionario en línea de unos20 minutos como máximo que permite a profesionales y empresas confirmar mediante una serie de preguntas que los datos que tratan pueden considerarse de bajo riesgo y obtener el mínimo de documentación que se considera necesaria para facilitar el cumplimiento de la normativa.

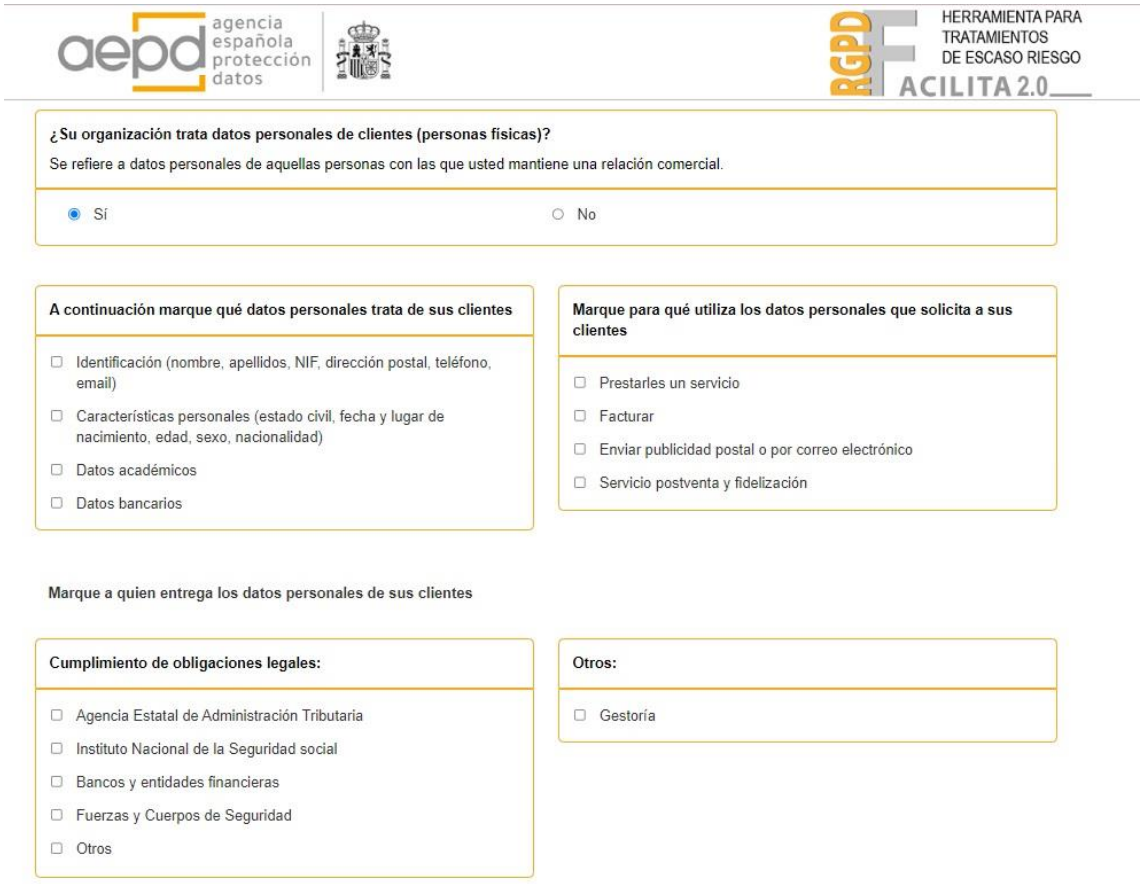

Ilustración 8 Facilita RGPD -AEPD-

El tratamiento de datos especiales como los sanitarios, de ideología política, etc. que implican un alto riesgo para los derechos y libertades de las personas son sólo algunos ejemplos de lo que no puede hacerse utilizando FACILITA RGPD.

Otra herramienta muy interesante es el *RAT* de la APDCat, especialmente útil para las pequeñas empresas a la hora de elaborar, administrar y supervisar el registro de actividades de tratamiento.

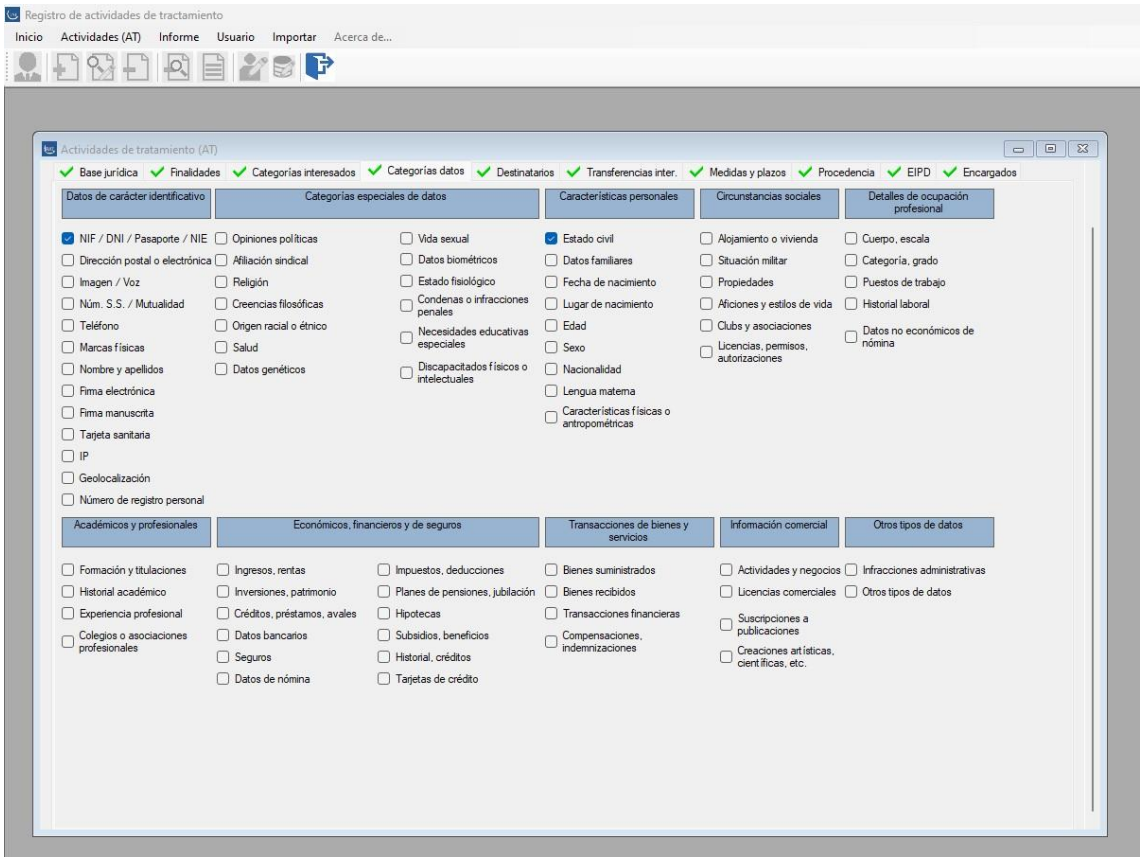

Ilustración 9 Aplicación RAT -APDCat-

En los registros de las actividades de tratamiento debe incluirse la siguiente información, de acuerdo con los requisitos para responsables y encargados del tratamiento:

- El nombre y los datos de contacto del responsable del tratamiento.
- Objetivos del tratamiento.
- Nombre e información de contacto del DPD si lo hubiera.
- Grupos de datos personales.
- Subgrupos de sujetos de datos.
- Una explicación de las medidas de seguridad organizativas y técnicas.
- Receptores específicos de la comunicación, como terceros países u organizaciones internacionales.
- Documentación de las protecciones adecuadas en caso de transferencias al extranjero.
- Plazos previstos para la supresión de los distintos tipos de datos, siempre que sea posible.

Las organizaciones con menos de 250 empleados están exentas de mantener un registro de las actividades de tratamiento a menos que este tratamiento pueda poner en peligro los derechos y libertades de los interesados, sea rutinario, implique categorías especiales de datos o implique información sobre condenas e infracciones penales.

Deben documentarse las siguientes operaciones del sistema de tratamiento automatizado: recogida, modificación, consulta, comunicación, transmisión, combinación y supresión de datos.

Si se conoce la identidad de la persona que consulta o transmite los datos personales, el responsable o el encargado del tratamiento deben asegurarse de que es posible justificar las operaciones de tratamiento.

Los registros sólo deben utilizarse en relación con procedimientos penales, para verificar la legalidad del tratamiento de datos, para autocontrol, para garantizar la exactitud y seguridad de los datos y para garantizar el autocontrol.

Al igual que con el contrato jurídico, se adjunta al cuerpo de este TFG un formulario para facilitar este Registro de Actividades, evitando así que se tengan que consultar diferentes fuentes o aplicaciones.

PLANTILLA PARA EL REGISTRO DE ACTIVIDADES DEL TRATAMIENTO

DENOMINACIÓN REGISTRO

DENOMINACIÓN	REGISTRO ACTIVIDADES 1

RESPONSABLE DEL TRATAMIENTO

NOMBRE Y DATOS DEL CONTACTO	NOMBRE_RESP APELLIDO1 APELLIDO2

DPD (SI PROCEDE)

NOMBRE Y DATOS DEL CONTACTO	NOMBREDPD APELLIDO1 APELLIDO2

BASE JURÍDICA

☒ Consentimiento	☐ Obligación Legal	☐ Misión Realizada En Interés Público o Ej. Poderes Públicos
☐ Contrato	☐ Proteger Intereses Vitales	☐ Interés Legítimo

☒ CATEGORÍAS ESPECIALES DE DATOS

- ☒ Consentimiento explícito
- ☐ Tratamiento necesario para cumplir obligaciones y ejercer los derechos específicos del responsable del tratamiento o del interesado, en el ámbito del derecho laboral y de la seguridad y la protección social
- ☐ Tratamiento necesario para proteger intereses vitales del interesado o de otra persona física
- ☐ Tratamiento efectuado por una fundación, una asociación o cualquier otro organismo sin animo de lucro que tenga una finalidad política, filosófica, religiosa o sindical
- ☐ Tratamiento relativo a datos personales que el interesado ha hecho manifiestamente público
- ☐ Tratamiento necesario para formular, ejercer o defender reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial
- ☐ Tratamiento necesario por razones de interés público esencial
- ☐ Tratamiento necesario para finalidades de medicina preventiva o laboral, de evaluación de la capacidad laboral de trabajador, de diagnostico medico, de prestación de asistencia o de tratamiento de tipo sanitario o social, o de gestión de los sistemas y los servicios de asistencia sanitaria o social
- ☐ Tratamiento necesario por razones de interés público en el ámbito de la salud publica
- ☐ Tratamiento necesario para finalidades de archivo en interés público, de investigación científica o histórica o estadísticas

☐ CONDENAS O INFRACCIONES PENALES

- ☐ Tratamientos de datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas con fines distintos de los de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales
- ☐ Registro completo de los datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas conforme a la regulación del sistema de registros administrativos de apoyo a la Admón de Justicia.
- ☐ Tratamientos de datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas llevados a cabo por abogados y procuradores que tengan por objeto recoger la información facilitad por sus clientes para el ejercicio de sus funciones.

Ilustración 10 Plantilla Registro de Actividades. Elaboración Propia

5.3 Legitimación del Tratamiento.

El fundamento jurídico por el que se realizan las operaciones de tratamiento debe constar explícitamente por escrito. Aunque no se menciona directamente, puede deducirse de algunos artículos del RGPD y de la idea más amplia de "responsabilidad activa".

Al facilitar la información a los interesados en el momento de la recogida de datos, debe revelarse el fundamento jurídico del tratamiento.

En la identificación y documentación deben tenerse en cuenta el método de tratamiento y las características de las organizaciones:

Tanto el tratamiento de datos personales como su comunicación dependen fundamentalmente del consentimiento del interesado. El tratamiento de datos personales y su cesión están sujetos a la normativa vigente, que, salvo que la ley disponga otra cosa, necesitan el consentimiento expreso del interesado cuyos datos personales se traten o cedan.

Hay situaciones en las que el consentimiento debe ser explícito además de inequívoco como por ejemplo en el tratamiento de datos sensibles, la adopción de decisiones automatizadas o las transferencias transfronterizas.

Cuando se deduce implícitamente del comportamiento del interesado (por ejemplo, cuando sigue visitando un sitio web y consiente el uso de cookies para rastrear su navegación), el consentimiento puede ser claro e implícito.

La información facilitada a los interesados debe ser sucinta, directa, comprensible y fácilmente accesible, utilizando un lenguaje sencillo, tanto en lo que respecta a los términos de las operaciones de tratamiento que les afectan como en las respuestas al ejercicio de derechos. Deben evitarse las fórmulas especialmente complejas o que recurran a textos legales. Las cláusulas informativas deben, independientemente del nivel de conocimientos del lector, transmitir de forma clara y concisa la información a la que se refieren inmediatamente. Además debe darse antes de la operación para la que se solicita el consentimiento, es decir, debe tener conocimiento de los fines que se persiguen previa autorización.

- El derecho debe ser libre, lo que implica que debe haber sido adquirido en condiciones reguladas por el código civil sin la interferencia de ningún vicio del consentimiento.
- Específico, es decir, relacionado con un procedimiento de tratamiento concreto y que se lleve a cabo con una finalidad determinada, clara y legal por parte del responsable del tratamiento.
- Inequívoco, lo que significa que debe haber una acción u omisión explícita que implique la presencia del consentimiento. Esto implica que no está permitido inferir el consentimiento de simples actos realizados por el interesado (consentimiento presunto).

Se adjunta a este trabajo un modelo de política de privacidad.

5.4 Designación de un DPD .

Solo en caso de que proceda, se adjunta un formulario típico para comunicar la designación.

NOTA: La Agencia Catalana de Protección de Datos (APDCAT) ha impulsado la primera red de aprendizaje y colaboración de delegados y responsables de protección de datos de Cataluña con la intención de fomentar la formación, la comunicación, el intercambio de experiencias y el trabajo en grupo entre los responsables de velar por el cumplimiento de la normativa de protección de datos en las organizaciones del sector público catalán.

Esta nueva plataforma llamada «DPD en xarxa» está dirigida a las personas que ejercen de DPD en las empresas que son competencia de la APDCAT. Dispone de espacios para grupos de trabajo, foros, noticias, formación y documentación, entre otros. Es necesario registrarse antes de acceder.

FORMULARIO PARA COMUNICAR DESIGNACIONES, MODIFICACIONES DE DATOS O CESE DE FUNCIONES DE DELEGADOS DE PROTECCIÓN DE DATOS (DPD)

Indique el tipo de información a comunicar:

☒ **Designación de DPD** ☐ **Modificación de datos de un DPD existente** ☐ **Cese de funciones de un DPD**

1 DATOS DEL ORGANISMO O ENTIDAD QUE NOMBRA O DESIGNA AL DELEGADO DE PROTECCIÓN DE DATOS

TIPO:
☐ INSTITUCIÓN AUTONÓMICA ☒ ADMINISTRACIÓN AUTONÓMICA ☐ ENTIDAD DE DERECHO PÚBLICO O PRIVADO DEPENDIENTE DE LA ADMÓN. AUTONÓMICA ☐ OTROS
☐ UNIVERSIDAD ☐ ADMINISTRACIÓN LOCAL ☐ ENTIDAD DE DERECHO PÚBLICO O PRIVADO DEPENDIENTE DE LA ADMÓN. LOCAL

DENOMINACIÓN DEL ORGANISMO O ENTIDAD: | NIF:

DIRECCIÓN POSTAL:

CÓDIGO POSTAL: | LOCALIDAD: | PROVINCIA:

TELÉFONO: | CORREO ELECTRÓNICO:

DENOMINACIÓN DEL CARGO QUE NOMBRA O DESIGNA AL DPD:

En su caso, DENOMINACIÓN de la Institución, Consejería, Ayuntamiento, Diputación, Universidad, etc., de la que depende el organismo o entidad:

2 IDENTIFICACIÓN DEL DELEGADO DE PROTECCIÓN DE DATOS

FECHA DE NOMBRAMIENTO O BAJA: 01/09/2023 | DEDICACIÓN A LAS FUNCIONES DE DPD EN EL ORGANISMO O ENTIDAD QUE LO NOMBRA: ☐ PARCIAL ☒ COMPLETA

TIPO:
☒ ES UNA PERSONA FÍSICA PERTENECIENTE AL ORGANISMO O ENTIDAD
☐ ES UN ÓRGANO COLEGIADO, GRUPO DE TRABAJO O SIMILAR, PERTENECIENTE AL ORGANISMO O ENTIDAD
Denominación:
☐ ES EXTERNO, DESEMPEÑANDO SUS FUNCIONES EN EL MARCO DE UN CONTRATO DE SERVICIOS O SIMILAR
Razón social del prestador del servicio: | NIF del prestador del servicio:
☐ El servicio lo presta una persona física de la plantilla del prestador del servicio
☐ El servicio lo presta un grupo o departamento, denominado:

NOMBRE Y APELLIDOS[1]: | SEXO[2]: ☐ H ☐ M | DNI:

[1] Se deberá identificar al DPD, en caso de ser persona física, o a la persona física que representa al DPD o coordina/dirige sus funciones [2] Dato opcional

3 DATOS PÚBLICOS PARA CONTACTO CON EL DELEGADO DE PROTECCIÓN DE DATOS

DIRECCIÓN POSTAL:

CÓDIGO POSTAL: | LOCALIDAD: | PROVINCIA:

TELÉFONO CONTACTO[2]: | CORREO ELECTRÓNICO DE CONTACTO DEL DPD:

INDICAR LA DIRECCIÓN (URL) DONDE SE PUBLICAN, EN LA WEB DEL ORGANISMO O ENTIDAD, LOS DATOS DE CONTACTO DEL DPD (Art. 37.7 RGPD):

[2] Dato opcional

Ilustración 11 Formulario Comunicación DPD Elaboración Propia

5.5 Análisis de riesgos

La evaluación de impacto es necesaria para que cualquier un tratamiento bajo la RGPD sea completo. La buena noticia es que no suele ser estrictamente necesaria cuando se trata de la evaluación de impacto de la protección de datos.

Aunque el RGPD no obliga a publicar un EIPD, deben tenerse en cuenta sus ventajas. La publicación puede ayudar a aumentar la confianza, además de demostrar el cumplimiento. Así que, si es posible, le aconsejamos que publique su EIPD, eliminando cualquier dato sensible si es necesario.

Para establecer las medidas de seguridad adecuadas, nuestro objetivo es identificar y cuantificar la cantidad de riesgo inherente al procedimiento mediante la Evaluación de Impacto.

Las amenazas, los riesgos y causas deben analizarse en la evaluación de impacto.

Definiremos riesgo como un evento y sus consecuencias, estimadas en términos de impacto y probabilidad. Así, la gestión de riesgos es el conjunto de aquellas actividades y tareas que son realizadas en una organización para monitorizar y controlar la exposición ante los riesgos. En primer lugar identificar las amenazas y los riesgos potenciales a los que esta expuestos las actividades del tratamiento. Evaluar los riesgos, la probabilidad y el impacto de que se materialice. Tratar los riesgos, dar respuesta para minimizar la probabilidad que se den y el impacto de que estos se materialicen hasta un nivel de riesgo aceptable (que nos permita garantizar los derechos y libertades de las personas físicas).

Ilustración 12 Gestión de Riesgos. Elaboración propia

Dado que la plantilla que proporciona la ICO es una de las más completas y sencillas que me he encontrado, se adjunta a la guía traducida y modificada para así continuar con el cumplimiento del RGPD por parte del EPD.

5.6 Buenas prácticas del Encargado de tratamiento de datos. Medidas de Seguridad.

Es habitual encontrar en la red numerosos artículos que pretenden ser un decálogo de consejos para el uso, con ciertas garantías de seguridad, de las TIC. Destaca el ofrecido por el Centro Criptológico Nacional y las propias infografías que ha elaborado el Servicio de Seguridad TIC. Entre recomendaciones fundamentales dirigidas al usuario que realice funciones de encargado de tratamiento de datos, se encuentran diferenciadas las medidas técnicas de seguridad, y las medidas las medidas de seguridad organizativas

En primer lugar, **las medidas técnicas de seguridad** son aquellas que implantamos en los propios sistemas de información que vamos a utilizar. Normalmente, las más típicas son las siguientes:

- Crear contraseñas largas y seguras. No compartirlas con nadie.
- Nunca dejar desatendidos los dispositivos móviles corporativos.
- Solamente navegar y descargar contenido de sitios web de confianza.
- No facilitar información confidencial corporativa por redes sociales o correo electrónico.
- Proteger los datos sensibles. Uno de los mecanismos habituales es la utilización de técnicas de cifrado.
- La instalación de cortafuegos, software antivirus, o cualquier otra medida de seguridad que proteja los equipos, dispositivos y la intranet corporativa.
- Desconfiar de los emails sobre facturas, bancos, ofertas, premios… No se deben abrir sus archivos adjuntos ni hacer clic en los enlaces que contengan sino se tiene la certeza de la autenticidad del remitente.
- No subir documentos corporativos a la nube, ya que ello podría ocasionar fugas de información, con la consiguiente responsabilidad penal o disciplinaria.
- Siempre que sea posible utilizar el doble factor de autenticación: «algo que tengo» (por ejemplo, un teléfono, una tarjeta, o un *tokem*) y «algo que conozco» (por ejemplo, una contraseña).
- Hacer copia de seguridad. Tener un sistema de *backup* operativo que permita recuperar la información en caso de pérdida de la misma.

Según diversa normativa sobre el cumplimiento de las normas de seguridad en uso del correo electrónico, se debe utilizar el correo electrónico corporativo única y exclusivamente para propósitos profesionales, debiéndose abstener del reenvío a listas de distribución u otros usuarios individuales de correos con contenidos lúdicos.

La dirección de correo electrónico corporativo podrá ser utilizada para intercambio de información, alta o registro en organismos oficiales nacionales e internacionales, así como en comunicaciones con empresas privadas por motivos relacionados estrictamente con la actividad profesional.

No se debe utilizar dicho correo en: foros, páginas web fuera del ámbito profesional, webs de información comercial, etc.

Gran parte de los mensajes de correo electrónico no deseados que llegan a los buzones del correo corporativo y tienen su origen en un uso no profesional de las cuentas de correo.

Utilizar el correo electrónico únicamente para fines profesionales reduce la posibilidad de sufrir un ataque.

En segundo lugar, las **medidas de seguridad organizativas** son aquellas que engloban las políticas y procedimientos aprobados por la dirección de la empresa para concienciar y formar a los empleados en materia de seguridad de la información. Las más habituales son:

- Planes de seguridad de la información y de tratamiento de datos.
- Creación de una normativa de ciberseguridad propia.
- Política para el manejo y tratamiento de información confidencial.
- Inclusión de cláusula de seguridad y confidencialidad para proveedores.
- Política de controles de acceso.
- Realización periódica de auditorías de seguridad y de protección de datos.
- El Seguro de Protección de Datos
- Establecimiento de procedimientos de seguridad.
- Protocolos para el control de documentos y registros.

medidas de seguridad de nivel básico

Con carácter general, cada fichero de datos de carácter personal y su tratamiento deberán respetar el nivel mínimo de seguridad.
A las personas con derecho de acceso a estos ficheros se les facilitará un documento de seguridad en el que se detallarán las medidas de seguridad tecnológicas y organizativas que deben conocer, adoptar y seguir. Este tipo de fichero suele incluir datos identificativos de la persona, como la filiación, el número de DNI, la dirección de correo electrónico y el número de teléfono móvil.

medidas de seguridad de nivel medio
Como mínimo cada dos años, estos ficheros también deben ser objeto de una auditoría interna o externa para garantizar que se cumplen los requisitos de seguridad. Debe examinar si las medidas son suficientes, si existen fallos y las posibles sugerencias de mejora. El responsable de seguridad examinará el dictamen de la auditoría y presentará sus conclusiones al responsable del tratamiento para que tome las medidas necesarias. Toda esta información se facilitará también a la AEPD.
Cuando dicho acceso sea persistente, será necesario desarrollar un sistema de seguimiento de entrada y salida de soportes y documentos, así como un dispositivo que impida o restrinja la posibilidad de que cualquier persona no autorizada intente acceder al sistema de información.
Los ficheros enumerados en el artículo 81 del Reglamento de Protección de Datos, a los que sean de aplicación las medidas de nivel medio y que incluyan los relativos a la comisión de infracciones administrativas o penales; o aquellos otros de los que sean responsables la Agencia Tributaria o las entidades financieras, también deberán adherirse a las medidas de nivel básico.

medidas de seguridad de nivel alto

Estarán sometidos a medidas de nivel alto los siguientes ficheros o tratamientos de datos de carácter personal:
«*Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual. Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas. Aquellos que contengan datos derivados de actos de violencia de género*». Los ficheros sujetos a requisitos de seguridad de nivel alto deben contar también con medidas de seguridad de nivel básico y medio, igual que en el ejemplo anterior.
Las medidas de alto nivel exigen identificar los soportes con métodos de etiquetado claros que permitan a las personas con acceso a ellos comprender su contenido, al tiempo que dificulten que otros lo hagan.
Además, obliga a cifrar cualquier información personal que se encuentre en dichos archivos o a utilizar otras medidas de seguridad que garanticen que nadie pueda acceder a ella ni alterarla.

Según el Reglamento, es mejor abstenerse de tratar datos personales en dispositivos portátiles que no admitan el cifrado. Se trata de una medida de seguridad que debe tenerse en cuenta ante el rápido desarrollo del uso de la tecnología.

5.7 Tareas de concienciación

Más del 80 % de los ciberincidentes se deben a errores humanos. Las empresas gastan millones para recuperarse de incidentes relacionados con sus propios trabajadores. Sin embargo, los programas de formación tradicionales normalmente no logran conseguir los cambios de comportamiento y la motivación deseados. Algunos ejemplos a poner en práctica podrían ser los siguientes:

1) programa de formación proporcionada a los encargados y responsables:

Cómo reconocer un posible escenario de ataque en un incidente de equipo aparentemente benigno. Cómo recopilar datos de los incidentes para remitírselos a los equipos de seguridad de IT. Cómo detectar síntomas malintencionados, y consolidar así el papel de todos los miembros del equipo de IT como primera línea de defensa y seguridad

2) Evaluación de la cultura de la ciberseguridad

Analizar el comportamiento diario actual y la actitud hacia la ciberseguridad en todos los niveles de la empresa, mostrando cómo perciben los empleados sus diferentes aspectos:

- Mentalidad de ciberseguridad (percepción de la seguridad y las políticas)
- Gestión de riesgos (orientación, comentarios, mejoras)
- Compromiso (actitud y comportamiento en relación con la seguridad)
- Impacto en el negocio (el equilibrio entre la seguridad y la eficiencia empresarial)

3) Seguimiento y estadísticas de campañas:
   - Configuración de dispositivos móviles. Aprender a configurarlo y protegerse de los riesgos de privacidad.
   - Compras seguras en la red
   - Detección de bulos, noticias falsas, fraudes en la red
   - Internet de las cosas, la domótica, los dispositivos conectados a la red..
4) Test de autoevaluación

5.8 Notificación de violaciones

El instituto INCIBE dispone de una guía[40] muy interesante y amplia para la notificación y gestión de ciberincidentes. La guía se consolida como una referencia de mínimos en el que toda entidad, pública o privada, ciudadano u organismo, encuentre un esquema y la orientación precisa acerca de a quién y cómo debe reportar un incidente de ciberseguridad acaecido en el seno de su ámbito de influencia.

Sistema de Ventanilla Única:

1. El perjudicado comunicará la incidencia mediante el envío de un correo electrónico (o ticket) al CSIRT correspondiente (INCIBE-CERT o CCN-CERT).

2. En función de la incidencia, el CSIRT de referencia disponen de herramientas de notificación y *ticketing* de incidentes para lograr una mejor gestión y seguimiento del incidente con los usuarios. Cada CSIRT puede proporcionar diversos métodos de interacción con estas herramientas para facilitar la interacción durante todo el ciclo de vida del incidente.: Si afecta a la Defensa Nacional, al CSIRT de referencia es ESP-DEF-CERT.

- Si afecta a una Infraestructura Crítica de la Ley PIC 8/2011, al CNPIC
- Si afecta al RGPD, a la AEPD.
- Si es un incidente de AAPP bajo el ENS de peligrosidad ALTA, MUY ALTA, CRÍTICA, al CCN-CERT
- Si es un incidente de obligado reporte según el RD 12/2018, a la Autoridad Nacional correspondiente:
  - RGPD: se envía a la URL del portal de la AEPD.
  - BDE: se envía la plantilla de notificación .XLS del BDE.
  - PIC: se envía la plantilla de notificación .XLS del CNPIC.
  - ENS: se envía la plantilla de notificación .DOC al CCN-CERT.
  - NIS: se envía la plantilla de notificación de la Autoridad Nacional competente.

3. Para recabar la información necesaria, el Organismo Receptor o la Autoridad Nacional Competente se pone en contacto con la parte afectada.

- RGPD: Se envía la URL del portal de la AEPD.

- BDE: Se envía el modelo de notificación en formato .XLS.

- PIC: Se envía la plantilla de notificación en formato CNPIC.XLS.

- ENS: Se envía la plantilla de notificación en formato.DOC al CCN-CERT.

- NIS: Se envía la plantilla de notificación de la Autoridad Nacional correspondiente.

4. El sujeto afectado comunica los datos necesarios al Organismo receptor implicado o Autoridad Nacional competente.

---

[40] *INCIBE* [en línea] [2 de mayo de 2023] Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

5. Si procede, desde la Oficina de Coordinación Cibernética (CNPIC), se pone la información a disposición de las Fuerzas y Cuerpos de Seguridad del Estado y Ministerio Fiscal para iniciar la investigación policial y judicial (art. 14.3 RD Ley 12/2018).

De acuerdo con el artículo 11.2 del RD Ley 12/2018, de 7 de septiembre[41], en los casos de especial gravedad, que se determinen reglamentariamente, y que requieran un nivel de coordinación superior al habitual, el CCN-CERT se encargará de la coordinación nacional de la respuesta técnica de los CSIRT.

Ilustración 13 Sistema de Ventanilla Única. Fuente: https://www.incibe.es/

[41] ESPAÑA. Jefatura del Estado. Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. Real Decreto-ley n.º 12/2018 de 7 de septiembre de 2018. Boletín Oficial del Estado [en línea]. 8 de septiembre de 2018, (218) [consultado el 5 de septiembre de 2023]. https://www.boe.es/buscar/act.php?id=BOE-A-2018-12257

5.6.1 Brechas De Datos Personales

Se considera violación de datos personales cuando se comete un acto, deliberado o involuntario, que pone en peligro la confidencialidad, la integridad o la disponibilidad de los mismos. No existe violación de la seguridad de los datos si el hecho no tiene repercusiones sobre los datos personales.

Algunos ejemplos son:

- Enviar información personal a la persona incorrecta.
- Entrada no autorizada en la información sanitaria de un paciente.
- Pérdida o robo de dispositivos electrónicos portátiles (como ordenadores portátiles, lápices de memoria, etc.).
- Datos encriptados por ransomware.
- Robo de la información de acceso al correo electrónico.
- Divulgación de datos al público como resultado de un fallo de configuración del sistema.
- Robo de registros en papel.
- Mal funcionamiento del sistema que hace que los datos no estén disponibles.
- Revelación de datos al público como consecuencia de una destrucción incorrecta de registros en papel.

Cuando la infracción pueda causar un perjuicio (físico, material o inmaterial) a los interesados afectados. A título ilustrativo, considérense los siguientes: pérdida de control sobre los datos, restricción de los derechos de los interesados, discriminación, usurpación de identidad, pérdida financiera, daño a la reputación, anulación ilícita de la seudonimización o pérdida de la confidencialidad de los datos sujetos al secreto profesional.

La falta de notificación implica el incumplimiento de un requisito del RGPD. Por lo tanto, además de dañar la reputación del responsable del tratamiento, también puede dar lugar a una investigación y, en su caso, a una sanción. El RGPD impone que se debe informar sin demora, y a más tardar en un plazo de 72 horas desde que se haya tenido constancia. No habrá repercusiones si el retraso está justificado, en caso de no serlo, puede considerarse una infracción y, en su caso, dar lugar a una sanción. Si los detalles de la infracción no están claros en el plazo marcado de 72 horas, se presentará una notificación preliminar. La notificación complementaria se presentará inmediatamente después de que se haya respondido a todas las preguntas y se disponga de más información.

Si el encargado del tratamiento es el que primero tiene constancia de la infracción debe notificarlo inmediatamente al responsable del tratamiento para que éste pueda cumplir sus obligaciones, que pueden incluir, si es necesario, la denuncia de la infracción a la autoridad competente.

Si está estipulado en el contrato, un encargado del tratamiento también puede revelar una infracción en nombre del responsable del tratamiento e incluso informar a los interesados. Sin embargo, el responsable del tratamiento siempre está obligado por ley a informar y comunicarlo a los interesados.

Cuando exista un alto riesgo para sus derechos y libertades (probabilidad de que la violación de la seguridad perjudique significativamente a los interesados), el incidente se comunicará a los

afectados. Esto significa que es necesario evaluar la probabilidad y la gravedad de las repercusiones de la violación para los afectados. Se tendrán en cuenta aspectos como si es probable que cause perjuicios económicos, afecte a datos sensibles, provoque la usurpación de identidad, dé acceso a más información personal sobre las personas implicadas (si se han obtenido contraseñas, por ejemplo) o afecte a grupos vulnerables.

Podría hacerse un anuncio público, por ejemplo, en el sitio web de la organización o en la prensa. En esta comunicación también debe incluirse toda la información necesaria. Es crucial proporcionar esta información a las partes afectadas para que puedan tomar medidas de protección contra las repercusiones negativas de la violación.

Ejemplo:

Se ha hecho pública información sobre los empleados de una empresa alimentaria. La información incluye datos guardados de los últimos reconocimientos médicos, así como direcciones personales, familiares y financieras. Dado que la violación de seguridad afecta a datos personales sensibles, incluida información sanitaria, la empresa alimentaria está obligada a notificarlo tanto a los empleados como a la autoridad de control (en este caso, la AEPDCat).

5.9 Fases de Gestión de un Incidente

Se conoce como gestión de ciberincidentes a una serie metódica de medidas diseñadas para evitar en la medida de lo posible que se produzcan ciberincidentes, minimizar la posibilidad de que se produzcan y, en caso de que se produzcan, restablecer rápidamente los niveles operativos. Aunque todas las fases del proceso de gestión de incidentes son esenciales, algunas de ellas pueden combinarse con otras, tratarse simultáneamente o incluirse como partes de otras fases.

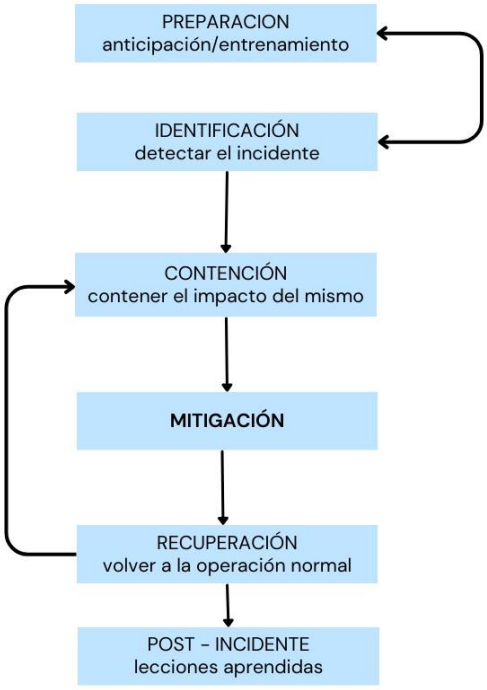

Ilustración 14 Fases de la gestión de un ciberincidente. Fuente: Elaboración propia

/

- Preparación: Es la primera etapa, en la que toda organización debe estar preparada para cualquier suceso que pueda ocurrir. La gestión eficaz de incidentes se basa en la preparación y la formación, y se apoya en tres pilares fundamentales: personas, procedimientos y tecnología.
- Identificación: El objetivo de este paso es poder identificar o advertir rápidamente cualquier incidente cibernético que pueda sufrir una empresa u otra entidad, por lo que es fundamental realizar un seguimiento lo más exhaustivo posible. Recordando la máxima de que no todos los eventos o alertas de ciberseguridad son incidentes cibernéticos.
- Contención: En cuanto se descubre un ciberincidente, la máxima prioridad es limitar sus efectos en la organización para evitar su propagación a otros sistemas o redes, produciendo un mayor impacto, y la extracción de información desde fuera de la organización.

- Mitigación: Dependiendo del tipo de ciberincidente, pueden ser necesarias diferentes medidas de mitigación. Por ejemplo, en el caso de un ataque de denegación de servicio distribuido (*DDoS*), puede ser necesario el apoyo del proveedor de servicios. En otros casos, puede ser necesario el borrado completo del sistema y la recuperación de las copias de seguridad.
- Recuperación: El objetivo de la fase de recuperación es devolver los niveles operativos a la normalidad para que los sectores empresariales afectados puedan continuar donde lo dejaron. Es crucial no poner en marcha demasiado rápido los sistemas que se han visto implicados en ciberincidentes.
- Acción posterior al incidente: Una vez resuelto el ciberincidente y reanudada la actividad con normalidad, es el momento de completar un proceso que a menudo se infravalora: «las lecciones aprendidas». Conviene tomarse un momento para reflexionar sobre lo sucedido, investigar las causas del problema, la evolución de la actividad durante la gestión del ciberincidente y todas las cuestiones relacionadas con él.

6. Conclusiones

En el inicio de este trabajo, se destacó la importancia de la privacidad en nuestra sociedad globalizada, donde garantizar tanto la seguridad como la privacidad resulta un desafío complejo. Establecimos varios objetivos, el primero de ellos fue examinar todas las normativas y regulaciones relacionadas con la ciberseguridad y la protección de datos. A lo largo del trabajo, se identificaron numerosas leyes, circulares, directivas… todas con el propósito principal de salvaguardar el derecho a la intimidad y la privacidad de las personas.

Analizamos minuciosamente las implicaciones prácticas de la implementación de estas normas de ciberseguridad en el ámbito del tratamiento de datos personales. Se hizo evidente la problemática derivada del crecimiento exponencial de las Tecnologías de la Información y la Comunicación (TIC) en relación con la protección de la privacidad debido a la falta de diligencia en muchos casos. A través de ejemplos, observamos cómo año tras año aumentan los ciberataques, dejándonos vulnerables y nuestros datos expuestos a ser vendidos.

En resumen, ha quedado patente que la relación entre ciberseguridad y privacidad en España está intrínsecamente conectada mediante la LO 3/2018 o LOPDGDD y el RGPD. Para asegurar la integridad de la privacidad y la información en el entorno digital, es imperativo que las organizaciones implementen medidas sólidas de ciberseguridad. La colaboración y el cumplimiento adecuado de estas regulaciones son esenciales para garantizar tanto la seguridad como la privacidad en nuestra era digital.

El resultado de este trabajo es una guía que abarca las obligaciones que deben ser consideradas por los encargados de tratamiento de datos para cumplir con todas las normativas relacionadas con la protección de datos en el contexto de la ciberseguridad. El diseño de esta guía permitió presentar estas obligaciones y recomendaciones de manera sistemática y ordenada, cumpliendo así otro de los objetivos que se establecieron al iniciar este proyecto.

7. Relación del trabajo desarrollado con los estudios cursados

Este Trabajo Final de Grado comprende múltiples objetivos alcanzados de diferentes asignaturas que han sido cursadas durante el Grado en Ingeniería Informática. Se enumeran algunos ejemplos a continuación:

Gestión de Proyectos: Se ha conseguido localizar información relevante desde diferentes fuentes e investigar las novedades tecnológicas en el ámbito trabajado. Hemos conseguido emprender, analizar, diseñar, planificar y liderar este proyecto, en el ámbito de la Ingeniería Informática.

De la asignatura Análisis y especificación de requisitos se ha podido poner en práctica el entendimiento de las necesidades del proyecto; entender el dominio y el contexto en el cual se iba a aplicar; elicitar, analizar, negociar y documentar los requisitos; se ha aprendido de manera autónoma nuevos conocimientos y técnicas adecuados para la concepción, el desarrollo, la evaluación o la explotación del software presentado.

Deontología y profesionalismo, impartida por Juan Vicente Oltra y tutor de este trabajo, motivo por el cual quizás es la asignatura que más importancia ha adquirido en este TFG. En ella se han puesto de manifiesto los aspectos Legales en la Informática. Se ha dado una visión de la legislación más importante que afecta al desarrollo profesional (Protección de datos, Ciberseguridad y otras). Se ha hecho asentamiento de la teoría, relacionándolo con la actualidad, por ejemplo, mediante diferentes noticias aportadas.

8. Trabajos Futuros

Y tras finalizar el desarrollo de este Trabajo Final de Grado, vienen a la cabeza de la autora que lo escribe diferentes ideas o problemáticas que considero de interés y que pueden servir para la ampliación de este trabajo y realizarse por otros alumnos en un futuro.

8.1 Privacidad e Identificación Biométrica

En mayo de 2022, el Comité Europeo de Protección de Datos (CEPD) publicó las Directrices 05/2022 sobre el uso de técnicas de reconocimiento facial (TRF) en la aplicación de la ley. Estas directrices buscan aclarar cuestiones relacionadas con el tratamiento de datos biométricos y su impacto en la privacidad, especialmente en el contexto de investigaciones penales.

Una identificación biométrica se produce cuando los datos biométricos de una persona se comparan con otras personas (comparación uno a varios), mientras que una autenticación biométrica compara los datos de una persona con la información biométrica ya disponible de esa misma persona (comparación uno a uno).

Las Directrices señalan la importancia de velar por la calidad, la fiabilidad y la exactitud de los conjuntos de datos utilizados en los tratamientos de reconocimiento facial, así como el derecho de los interesados a la rectificación de los datos personales inexactos tal como se establece en el art. 16 de la Directiva 2016/680. Si no se cumplen estas garantías es posible que se produzcan sesgos y errores que supongan un riesgo para el interesado.

Las Directrices abordan varios aspectos clave, como la calidad y precisión de los datos utilizados en el reconocimiento facial, los derechos de los interesados para corregir datos inexactos, y la consideración de los datos biométricos como una intromisión grave en los derechos fundamentales de privacidad y protección de datos.

El CEPD establece que cualquier tratamiento de datos biométricos es una intromisión seria en los derechos fundamentales, pero puede justificarse en circunstancias específicas, siempre que se cumplan ciertos requisitos legales, como la necesidad y proporcionalidad.

Sin embargo, surge una discrepancia con la posición de la AEPD en lo que respecta a la autenticación biométrica. El CEPD considera que la autenticación biométrica implica el tratamiento de categorías especiales de datos, mientras que la AEPD ha sostenido una posición diferente, argumentando que la autenticación no siempre implica el uso de categorías especiales de datos, pidiendo que se tenga en cuenta: (i) el contexto de cada caso; (ii) el fin que se persigue con el tratamiento; y (iii) la interpretación más favorable para la protección de los derechos de los afectados.

Esta discrepancia entre las posturas del CEPD y la AEPD crea incertidumbre legal para las entidades y empresas que desean implementar técnicas de reconocimiento facial en España. La interpretación del CEPD podría llevar a requisitos adicionales, como el consentimiento explícito. Si el uso de TRF para autenticar constituye un tratamiento de categorías especiales de datos podrían surgir problemas en cuanto al proceso de autenticación de los empleados (p. ej., aquellas empresas que utilicen un sistema de huella dactilar para el registro horario)42. Este cambio de interpretación supondría un obstáculo para los empleadores, que actualmente deben cumplir menos requisitos en caso de sólo autenticar a sus empleados.

En resumen, las Directrices del CEPD sobre el reconocimiento facial en el ámbito de la aplicación de la ley buscan aclarar cuestiones clave relacionadas con la protección de datos biométricos, pero su discrepancia con la posición de la AEPD crea incertidumbre y plantea desafíos para la implementación de estas tecnologías en España. Parece imprescindible que la AEPD debe clarificar su posición a fin de asegurar un uso adecuado de las TRF y generar un entorno de certidumbre.

[42] *Mercadona y el reconocimiento facial*. [en línea] https://elpais.com/tecnologia/2020-07-06/proteccion-de-datos-abre-una-investigacion-sobre-las-camaras-de-vigilancia-facial-de-mercadona.html.

8.2 La protección de datos en el Metaverso.

Existe una gran preocupación en la recogida de datos y su posterior tratamiento por parte de las grandes empresas que operan en el llamado metaverso[43].

El metaverso englobará inevitablemente la generación y el tratamiento de cantidades sustanciales de datos, que abarcarán tanto información personal como no personal. Desde el punto de vista de la protección de datos, la presencia de múltiples entidades dentro de los espacios virtuales del metaverso plantea retos en términos de rastreo y asignación de responsabilidades y obligaciones a los actores individuales. La asignación de responsabilidades por el tratamiento de datos o la obtención del consentimiento de los interesados, sobre todo cuando requiere que se produzca con regularidad, plantea un reto especialmente intrincado.

Otros ámbitos de preocupación son las transferencias internacionales de datos y la jurisdicción competente. Esto se debe a que la movilidad sin restricciones a través de diversos dominios metaversos plantea un reto a la hora de garantizar que todas las entidades participantes mantengan normas suficientes de protección de datos. Por lo tanto, es imperativo desarrollar criterios inequívocos para determinar la jurisdicción. El estudio del Parlamento incluye recomendaciones sobre criterios como la ubicación del usuario, el avatar utilizado y los servidores implicados. Es imperativo disponer de un marco claro y cohesionado para resolver disputas dentro del metaverso.

El término «*datos sensibles*» se refiere a la información que requiere un mayor nivel de protección debido a su potencial para causar daños o perjuicios.

Sin duda, un aspecto crucial a tener en cuenta es el tratamiento extensivo de información sensible, incluidas las respuestas emocionales y el análisis proxémico, que implica el estudio de la disposición espacial en la comunicación lingüística no verbal y la evaluación biomecánica de los individuos. El estudio de la Eurocámara pone de relieve la posible violencia de la elaboración de perfiles intrusivos, que puede llevar a los individuos a perder el control sobre sus propias vidas y elecciones personales, incluida la capacidad de ejercer su derecho al voto. Esto es especialmente preocupante para las poblaciones marginadas y vulnerables.

Dadas las circunstancias mencionadas, es pertinente evaluar la idoneidad de los esfuerzos reguladores emprendidos por la Comisión Europea, así como los previstos en un futuro próximo, incluida la Ley de Datos, la Ley del Mercado Digital y la Comunicación sobre la interpretación revisada del artículo 22 del Reglamento sobre concentraciones. La cuestión que se plantea es si estas medidas abordarán eficazmente los retos inminentes que plantea la llegada del metaverso, aunque sea a corto plazo.

[43] *XATAKA Qué es el Metaverso, qué posibilidades ofrece y cuándo será real* [en línea] [25 de junio de 2023] https://www.xataka.com/basics/que-metaverso-que-posibilidades-ofrece-cuando-sera-real

9. Referencias

BARRIO ANDRÉS, Moisés, 2017. *Ciberdelitos. Amenazas criminales del ciberespacio*. Madrid: REUS. ISBN 978-84-290-1972-8.

BUDAPEST, 2010. Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001 [en línea]. Recuperado a partir de: https://www.boe.es/boe/dias/2010/09/17/pdfs/BOE-A-2010-14221.pdf

ESPAÑA. Constitución Española. Boletín Oficial del Estado, 29 de diciembre de 1978, núm. 311. Disponible en: https://www.boe.es/eli/es/c/1978/12/27/(1)/con.

ESPAÑA, 1979. Instrumento de Ratificación del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950, y enmendado por los Protocolos adicionales números 3 y 5, de 6 de mayo de 1963 y 20 de enero de 1966, respectivamente. [en línea]. Recuperado a partir de: https://www.boe.es/boe/dias/1979/10/10/pdfs/A23564-23570.pdf

ESPAÑA. Ministerio de Asuntos Exteriores. Declaración formulada por España relativa al artículo 25 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950. Nota Diplomática de 11 de junio de 1981. Boletín Oficial del Estado [en línea]. 30 de junio de 1981, (155) [consultado el 9 de junio de 2023]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1981-14565

ESPAÑA. Jefatura del Estado. Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981. Boletín Oficial del Estado [en línea]. 15 de noviembre de 1985, (274) [consultado el 9 de junio de 2023]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1985-23447

ESPAÑA. Jefatura del Estado. Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Boletín Oficial del Estado [en línea]. 14 de mayo de 1982, (115) [consultado el 9 de junio de 2023]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1982-11196

ESPAÑA. Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. Boletín Oficial del Estado, 31 de octubre de 1992, núm. 262, p. 37037-37045. Disponible en: https://www.boe.es/eli/es/lo/1992/10/29/5

ESPAÑA. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Boletín Oficial del Estado, 14 de diciembre de 1999, núm. 298. Disponible en: https://www.boe.es/eli/es/lo/1999/12/13/15/con

ESPAÑA. Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal. Boletín Oficial del Estado, 25 de junio de 1999, núm. 151, p. 24241-24245. Disponible en: https://www.boe.es/eli/es/rd/1999/06/11/994

ESPAÑA. Jefatura del Estado. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Boletín Oficial del Estado [en línea]. 14 de diciembre de 1999, (298) [consultado el 5 de junio de 2023]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750

ESPAÑA. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Boletín Oficial del Estado, 19 de enero de 2008, núm. 17. Disponible en: https://www.boe.es/eli/es/rd/2007/12/21/1720/con

ESPAÑA. Tribunal Constitucional. Conflicto positivo de competencia n.º 2761-2016, en relación con diversos preceptos del Real Decreto 56/2016, de 12 de febrero, por el que se transpone la Directiva 2012/27/UE del Parlamento Europeo y del Consejo, de 25 de octubre de 2012. Providencia n.º 2761/2016 de 7 de junio de 2016. Boletín Oficial del Estado [en línea]. 15 de junio de 2016, (144) [consultado el 8 de mayo de 2023]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2016-5797

ESPAÑA. Jefatura del Estado. Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. Real Decreto-ley n.º 12/2018 de 7 de septiembre de 2018. Boletín Oficial del Estado [en línea]. 8 de septiembre de 2018, (218) [consultado el 5 de septiembre de 2023]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2018-12257

ESPAÑA. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. Boletín Oficial del Estado, 6 de diciembre de 2018, número 294. Disponible en: https://www.boe.es/eli/es/lo/2018/12/05/3/con

ESPAÑA. Jefatura del Estado. Ley 2/2019, de 1 de marzo, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva

2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017. Boletín Oficial del Estado [en línea]. 2 de marzo de 2019, (53) [consultado el 8 de mayo de 2023]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2019-2974

ESPAÑA. Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. Boletín Oficial del Estado, 27 de mayo de 2021, número 126. Disponible en: https://www.boe.es/eli/es/lo/2021/05/26/7

ESPAÑA, 2021. Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos. A [en línea]. Recuperado a partir de : https://www.boe.es/eli/es/rd/2021/06/01/389

ESPAÑA, 2021. Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021 [en línea]. Recuperado a partir de : https://www.boe.es/boe/dias/2021/12/31/pdfs/BOE-A-2021-21884.pdf

ESPAÑA. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Boletín Oficial del Estado [en línea]. 4 de mayo de 2022, (106) [consultado el 4 de agosto de 2023]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2022-7191

GÓMEZ HERVÁS, Nuria del Carmen, 2021. *Normativa de ciberseguridad*. Paracuellos de Jarama, Madrid: Ra-Ma. ISBN 978-84-18971-23-5.

GUTIÉRREZ MAYO, Escarlata, 2021. *Delitos informáticos: Análisis detallado de las conductas delictivas más comunes en el entorno informático*. Galicia Editorial Colex. ISBN 978-84-13-59257-2.

GUTIÉRREZ MAYO, Escarlata, 2022. *La prueba digital: Guía práctica sobre la prueba digital en los diferentes órdenes jurisdiccionales*. Galicia: Editorial Colex. ISBN 978-84-13-59520-7.

MONTERO ROMERO, Fernando et al., 2020. *Manual Básico de Ciberseguridad y Protección de Datos*. Madrid: Exit Editorial S.L. ISBN 978-84-9744-320-3.

MONTESINOS RODRIGO, Laura, 2022. *Guía para la realización del Privacy Impact Assessment (PIA, Evaluación de Impacto en la Protección de Datos Personales) para encargados y responsables de tratamiento de datos.*. . Trabajo Fin de Grado. Universidad Politécnica de Valencia.

MULLOR BERENGUER, Marta, 2022. *Guía sobre protección de datos e implantación de la LOPDGDD en centros sanitarios*. . Trabajo Fin de Grado . Universidad Politécnica de Valencia.

NACIONES UNIDAS, 1948. La Declaración Universal de los Derechos Humanos [en línea]. Recuperado a partir de: https://cnrha.sanidad.gob.es/documentacion/bioetica/pdf/Universal_Derechos_Humanos.pdf

OLTRA GUTIÉRREZ, Juan Vicente, sin fecha. Incorporación de Inteligencia Artificial al tratamiento de datos personales. *RiuNet: repositorio UPV* [en línea]. Recuperado a partir de: https://polimedia.upv.es/visor/?id=323a0890-b2cc-11ed-9a61-93bba90db995

RODRÍGUEZ FERRER, Marc, 2020. *Guía para la evaluación de impacto requerida en el Reglamento Europeo de Protección de Datos*. . Trabajo Fin de Grado. Universidad Politécnica de Valencia.

SEVILLANO JAÉN, Fernando y BELTRÁN PARDO, Marta, 2020. *Dirección de seguridad y gestión del ciberriesgo*. Paracuellos de Jarama, Madrid: Ra-Ma. ISBN 978-84-9964-934-4.

UNION EUROPEA, 2013. DIRECTIVA (UE) 2013/40 del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo. [en línea]. Recuperado a partir de: https://boe.es/doue/2013/218/L00008-00014.pdf

UNION EUROPEA, 2016. 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) [en línea]. Recuperado a partir de: https://www.boe.es/doue/2016/119/L00001-00088.pdf

UNION EUROPEA, 2016. 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 y por la que se deroga la Decisión

Marco 2008/977/JAI del Consejo [en línea]. Recuperado a partir de: https://www.boe.es/doue/2016/119/L00089-00131.pdf

UNION EUROPEA, 2016. DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión [en línea]. Recuperado a partir de: https://www.boe.es/doue/2016/194/L00001-00030.pdf

UNION EUROPEA, 2019. REGLAMENTO (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación. [en línea]. Recuperado a partir de: https://www.boe.es/doue/2019/151/L00015-00069.pdf

PAGINAS WEB:

Qué es el Metaverso, qué posibilidades ofrece y cuándo será real. [en línea] Disponible en: https://www.xataka.com/basics/que-metaverso-que-posibilidades-ofrece-cuando-sera-real.

Mercadona y el reconocimiento facial. [en línea] Disponible en: https://elpais.com/tecnologia/2020-07-06/proteccion-de-datos-abre-una-investigacion-sobre-las-camaras-de-vigilancia-facial-de-mercadona.html

INCIBE | INCIBE [en línea] [consultado el 5 de agosto de 2023] Disponible en: https://www.incibe.es/sites/default/files/paginas/que-hacemos/balance_ciberseguridad_2022_incibe.pdf

APDCAT. Autoritat Catalana de Protecció de Dades [en línea]. [consultado el 8 de mayo de 2023]. Disponible en: https://apdcat.gencat.cat/ca/inici

CCN-CERT. [en línea]. [consultado el 8 de mayo de 2023]. Disponible en: https://www.ccn-cert.cni.es/

National Institute of Standards and Technology. NIST [en línea]. [consultado el 9 de junio de 2023]. Disponible en: https://www.nist.gov/

Informaticon Commissioner's Office [en línea] https://ico.org.uk/

El encargado del tratamiento en el Reglamento General de Protección de Datos (RGPD) [en línea] Recuperado a partir de: https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/Guia-encargado-del-tratamiento-RGPD-CAST.pdf

10. Términos y definiciones más utilizados

AEPD Agencia española de Proteccion de Datos

Autoridad de Control: Cada Estado miembro tiene la responsabilidad de asignar una o varias autoridades públicas independientes encargadas de supervisar la implementación del Reglamento, con el objetivo de proteger los derechos y las libertades fundamentales de las personas en relación con el tratamiento de datos y facilitar la libre circulación de datos personales en la Unión Europea.

cookies Las cookies son pequeños archivos de datos que los sitios web almacenan en tu dispositivo para rastrear tus actividades y preferencias en línea.

Cookies: Pequeños archivos de información generados por un servidor web y enviados a un navegador web.

DoS o *DDoS*: Ataque de Denegación de Servicio Distribuido (DDoS), en el cual múltiples sistemas coordinadamente envían solicitudes, a menudo sin el conocimiento de sus legítimos propietarios, con el propósito de saturar y dejar inoperable un servicio o recurso en línea.

DPD. DPO. Delegado de Protección de Datos.Data Protection Officer .

ENS Esquema Nacional de Seguridad

EPD: 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»* (art. 4.8 del RGPD).

ICO *Informaticon Commissioner's Office* Autoridad de Protección de Datos del Reino Unido

INCIBE Instituto Nacional de Ciberseguridad Autoridad Catalana de Protección de Datos

NIST Instituto Nacional de Normas y Tecnología

NIST National Institute of Standards and Technology

phising ciberataque o estafa en línea en la que los perpetradores se hacen pasar por entidades legítimas para engañar a las personas y obtener información confidencial, como contraseñas, números de tarjetas de crédito

RAT: Aplicación para registrar y gestionar las actividades de tratamiento de datos. Desarrollada por la Autoridad Catalana de Protección de Datos.

RGPD: reglamento General de Protección de Datos

Seudonimización es un proceso de protección de datos que reemplaza información identificable por un identificador único, manteniendo la privacidad.

Seudonimización: El tratamiento de datos personales de manera que ya no puedan ser atribuidos a un individuo sin el uso de información adicional, siempre que esta información adicional esté separada y sujeta a medidas técnicas y organizativas diseñadas para asegurar que los datos personales no se puedan relacionar con una persona identificada o identificable.Tratamiento de datos: «operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, registro, organización, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias, así como la limitación, supresión o destrucción.» adaptado de (art. 3 LO 15/1999, de 13 de diciembre) y (art. 4 RGPD).

Sniffers: Herramientas, ya sea de software o hardware, que permiten a los usuarios monitorear en tiempo real el tráfico de red y capturar toda la información de datos que ingresa o sale de un dispositivo o equipo bajo observación.

Spyware: Una forma de software malicioso que se oculta en un dispositivo, supervisa las actividades del usuario y roba información confidencial, como datos bancarios y contraseñas.

11. Anexos

11.1 Objetivos de Desarrollo sostenible

Grado de relación del trabajo con los Objetivos de Desarrollo Sostenible (ODS).

Objetivos de Desarrollo Sostenibles	**Alto**	**Medio**	**Bajo**	**No Procede**
ODS 1. **Fin de la pobreza.**				**X**
ODS 2. **Hambre cero.**				**X**
ODS 3. **Salud y bienestar.**	**X**			
ODS 4. **Educación de calidad.**		**X**		
ODS 5. **Igualdad de género.**			**X**	
ODS 6. **Agua limpia y saneamiento.**				**X**
ODS 7. **Energía asequible y no contaminante.**				**X**
ODS 8. **Trabajo decente y crecimiento económico.**				**X**
ODS 9. **Industria, innovación e infraestructuras.**	**X**			
ODS 10. **Reducción de las desigualdades**.				**X**
ODS 11. **Ciudades y comunidades sostenibles**.				**X**
ODS 12. **Producción y consumo responsables.**				**X**
ODS 13. **Acción por el clima.**				**X**
ODS 14. **Vida submarina.**				**X**
ODS 15. **Vida de ecosistemas terrestres.**				**X**
ODS 16. **Paz, justicia e instituciones sólidas.**	**X**			
ODS 17. **Alianzas para lograr objetivos.**	**X**			

Reflexión sobre la relación del TFG/TFM con los ODS y con el/los ODS más relacionados:

A lo largo de este trabajo se ha podido ver la importancia de las raíces que guían el mismo:
La Ciberseguridad y la Privacidad, son temas de creciente importancia en un mundo cada vez más interconectado y digitalizado. A medida que la tecnología avanza, también lo hacen las amenazas cibernéticas, lo que pone de manifiesto la necesidad de proteger los datos y la infraestructura digital de manera efectiva. En este contexto, la relación entre las responsabilidades de un encargado de tratamiento de datos en el ámbito de la ciberseguridad y los Objetivos de Desarrollo Sostenible (ODS) es de gran relevancia, ya que la seguridad cibernética es fundamental para avanzar en la consecución de estos objetivos globales.
Los ODS son una iniciativa de las Naciones Unidas que busca abordar los desafíos más apremiantes que enfrenta nuestro mundo, desde la pobreza y el hambre hasta la igualdad de género, la educación de calidad, la salud, la igualdad de acceso al agua potable y, en última instancia, la construcción de un futuro sostenible para todos. Los 17 ODS y sus numerosas metas proporcionan un marco global para abordar cuestiones críticas que afectan a la humanidad y al planeta.
En este contexto, la ciberseguridad puede no parecer una prioridad evidente, pero es esencial para el logro de varios ODS. A continuación, reflexionaré sobre cómo las responsabilidades de un encargado de tratamiento de datos en relación con la ciberseguridad se vinculan con algunos de los ODS clave.

ODS 9: Industria, Innovación e Infraestructura
El ODS 9 se centra en la construcción de infraestructuras resilientes, la promoción de la industrialización inclusiva y sostenible, y el fomento de la innovación. La ciberseguridad es esencial para garantizar la integridad de las infraestructuras digitales y la protección de la propiedad intelectual. Los encargados de tratamiento de datos desempeñan un papel vital en la protección de los sistemas y datos que respaldan la innovación y la infraestructura tecnológica. Al adoptar prácticas de ciberseguridad sólidas, contribuyen a un entorno digital más seguro y, por lo tanto, al logro del ODS 9.

ODS 3: Salud y Bienestar
El ODS 3 busca garantizar una vida saludable y promover el bienestar para todos en todas las edades. La atención médica se está volviendo cada vez más digitalizada, y los datos de salud son extremadamente sensibles. Los encargados de tratamiento de datos en el sector de la salud tienen la responsabilidad de proteger la privacidad y la seguridad de estos datos, evitando brechas de seguridad que puedan poner en riesgo la salud y la seguridad de las personas. La ciberseguridad en el ámbito de la salud es, por lo tanto, un componente crítico para alcanzar el ODS 3.

ODS 4: Educación de Calidad
El ODS 4 se enfoca en garantizar una educación inclusiva, equitativa y de calidad para todos. La educación está cada vez más influenciada por la tecnología y la recopilación de datos. Las instituciones educativas recopilan información sensible sobre estudiantes y profesores, y los encargados de tratamiento de datos deben garantizar la seguridad de estos datos para proteger la privacidad y la calidad de la educación. La ciberseguridad contribuye directamente a lograr una educación de calidad, al proteger la integridad y la disponibilidad de los sistemas de información educativa.

ODS 5: Igualdad de género.

El quinto Objetivo de Desarrollo Sostenible (ODS) se enfoca en «*Alcanzar la igualdad de género y empoderar a todas las mujeres y niñas*». Su principal propósito es abordar las disparidades de género en todas las facetas de la sociedad y promover el empoderamiento de las mujeres y las niñas.

Aunque la Agencia Española de Protección de Datos (AEPD) no tiene como misión central la promoción de la igualdad de género, ya que su principal mandato consiste en supervisar y hacer cumplir la legislación de protección de datos en España, es relevante destacar que la AEPD ha establecido un Plan de Igualdad interno. Este plan tiene como objetivo lograr una igualdad de trato efectiva entre hombres y mujeres, erradicando cualquier forma de discriminación basada en el género. Una de las metas específicas es alcanzar una representación femenina del 50% en los niveles directivos de la agencia. Además, es importante subrayar que, su labor contribuye a garantizar que se respeten los derechos de todas las personas, incluyendo mujeres y niñas, en lo que respecta a la protección de sus datos personales y su privacidad. La igualdad de género es un componente esencial de los derechos humanos, y la protección de datos desempeña un papel importante en la creación de un entorno en el que todas las personas puedan ejercer sus derechos de manera segura y equitativa.

ODS 16: Paz, Justicia e Instituciones Sólidas

El ODS 16 busca promover sociedades pacíficas, justas e inclusivas mediante la construcción de instituciones sólidas. La ciberseguridad es esencial para la integridad de las instituciones gubernamentales y la administración de justicia. Los encargados de tratamiento de datos en el sector público desempeñan un papel crucial al proteger los datos confidenciales y asegurar la continuidad de los servicios públicos. La ciberseguridad es un pilar fundamental para el funcionamiento adecuado de las instituciones y, por lo tanto, para el logro del ODS 16.

ODS 17: Alianzas para lograr los Objetivos

El ODS 17 se enfoca en fortalecer las alianzas para la implementación efectiva de la Agenda 2030. La ciberseguridad es un desafío global que requiere colaboración y cooperación entre gobiernos, empresas y la sociedad civil. Los encargados de tratamiento de datos, al adoptar prácticas de ciberseguridad sólidas, contribuyen a la construcción de un entorno digital más seguro y a la promoción de alianzas para abordar las amenazas cibernéticas. La ciberseguridad es un componente esencial para lograr el ODS 17.

En resumen, la ciberseguridad desempeña un papel fundamental en la consecución de varios Objetivos de Desarrollo Sostenible al proteger los datos, las infraestructuras y la privacidad en un mundo cada vez más digitalizado. Los encargados de tratamiento de datos tienen una responsabilidad importante en este contexto, ya que son guardianes de la integridad y la seguridad de los datos. Al adoptar prácticas de ciberseguridad sólidas, contribuyen al logro de los ODS al garantizar la confianza en la tecnología, la protección de la privacidad y la continuidad de servicios esenciales en áreas como la salud, la educación, la justicia y la infraestructura. La ciberseguridad no solo es una necesidad técnica, sino también un habilitador clave para un futuro sostenible y resiliente.

11.2 Guía para un Encargado

CONTRATO ESTÁNDAR

1. Objeto del encargo del tratamiento

Mediante las presentes cláusulas se habilita a la entidad _____, encargada del tratamiento, para tratar por cuenta de _____, responsable del tratamiento, los datos de carácter personal necesarios para prestar el servicio de _____.

El tratamiento consistirá en: *(descripción detallada del servicio)*

_____

Concreción de los tratamientos a realizar:

- ☐ Recogida
- ☐ Registro
- ☐ Estructuración
- ☐ Modificación
- ☐ Conservación
- ☐ Extracción
- ☐ Consulta
- ☐ Comunicación por transmisión
- ☐ Difusión
- ☐ Interconexión
- ☐ Cotejo
- ☐ Limitación
- ☐ Supresión
- ☐ Destrucción
- ☐ Conservación
- ☐ Comunicación
- ☐ Otros: _____.

2. Identificación de la información afectada

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, la *entidad/órgano* _____, responsable del tratamiento, pone a disposición de la entidad _____, encargada del tratamiento, la información que se describe a continuación:

- _____
- _____

3. Duración

El presente acuerdo tiene una duración de [1]

Una vez finalice el presente contrato, el encargado del tratamiento debe *suprimir/devolver al responsable/devolver a otro encargado que designe el responsable (indicar la opción que proceda)* los datos personales y suprimir cualquier copia que esté en su poder.

4. Obligaciones del encargado del tratamiento

El encargado del tratamiento y todo su personal se obliga a:

a. Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.

b. Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento.

Si el encargado del tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, el encargado informará inmediatamente al responsable.

c. Llevar, por escrito, un registro[2] de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, que contenga:

1. 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.
2. Las categorías de tratamientos efectuados por cuenta de cada responsable.
3. 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 del RGPD, la documentación de garantías adecuadas.
4. Una descripción general de las medidas técnicas y organizativas de seguridad relativas a:

    a) La seudoanimización y el cifrado de datos personales.
    b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

[1] En algunos casos, en particular determinados casos sometidos al derecho administrativo (convenios, contratos de gestión de servicios públicos, etc.), la duración del encargo puede estar limitada por la duración establecida por la legislación vigente para la prestación de servicios.

[2] "Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, salvo que el tratamiento que realice pueda suponer un riesgo para los derechos y las libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1 del RGPD, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10 de dicho Reglamento." (Art. 30.5 RGPD).

c) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
d) El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

d. No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles.

El encargado puede comunicar los datos a otros encargados del tratamiento del mismo responsable, de acuerdo con las instrucciones del responsable. En este caso, el responsable identificará, de forma previa y por escrito, la entidad a la que se deben comunicar los datos, los datos a comunicar y las medidas de seguridad a aplicar para proceder a la comunicación.

Si el encargado debe transferir datos personales a un tercer país o a una organización internacional, en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, informará al responsable de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones importantes de interés público.

e. Subcontratación

(Escoger una de las opciones)

☐ *Opción A* *No subcontratar ninguna de las prestaciones que formen parte del objeto de este contrato que comporten el tratamiento de datos personales, salvo los servicios auxiliares necesarios para el normal funcionamiento de los servicios del encargado.*

Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito al responsable, con una antelación de [ ][3]*, indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo establecido.*

El subcontratista, que también tendrá la condición de encargado del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el encargado del tratamiento y las instrucciones que dicte el responsable. Corresponde al encargado inicial regular la nueva relación de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad…) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.

[3] Se recomienda establecer un plazo mínimo de antelación para realizar la comunicación.

☐ *Opción B* *Se autoriza al encargado a subcontratar con la empresa* [ ] *las prestaciones que comporten los tratamientos siguientes:*

[ ]

Para subcontratar con otras empresas, el encargado debe comunicarlo por escrito al responsable, identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo de [ ][4]*.*

El subcontratista, que también tiene la condición de encargado del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el encargado del tratamiento y las instrucciones que dicte el responsable. Corresponde al encargado inicial regular la nueva relación, de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad…) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.

f. Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice su objeto.

g. Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad[5] y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.

h. Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

i. Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

j. Asistir al responsable del tratamiento en la respuesta al ejercicio de los derechos de:

1. Acceso, rectificación, supresión y oposición
2. Limitación del tratamiento
3. Portabilidad de datos
4. A no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles)

(Escoger una de las opciones)

☐ *Opción A* *El encargado del tratamiento debe resolver, por cuenta del responsable, y dentro del plazo establecido, las solicitudes de ejercicio de los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento,*

[4] Se recomienda establecer un plazo mínimo de antelación para realizar la comunicación.

[5] Si existe una obligación de confidencialidad de naturaleza estatutaria deberá quedar constància expresa de la naturaleza y extensión de esta obligación.

portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, en relación con los datos objeto del encargo.[6]

☐ *Opción B* *Cuando las personas afectadas ejerzan los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, ante el encargado del tratamiento, éste debe comunicarlo por correo electrónico a la dirección* [ ] *(dirección que indique el responsable). La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción de la solicitud*[7]*, juntamente, en su caso, con otras informaciones que puedan ser relevantes para resolver la solicitud.*

k. Derecho de información

(Escoger una de las opciones)

Opción A *El encargado del tratamiento, en el momento de la recogida de los datos, debe facilitar la información relativa a los tratamientos de datos que se van a realizar. La redacción y el formato en que se facilitará la información se debe consensuar con el responsable antes del inicio de la recogida de los datos.*

Opción B *Corresponde al responsable facilitar el derecho de información en el momento de la recogida de los datos.*

l. Notificación de violaciones de la seguridad de los datos

El encargado del tratamiento notificará al responsable del tratamiento, sin dilación indebida, y en cualquier caso antes del plazo máximo de [ ][8], y a través de [ ], las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.

No será necesaria la notificación cuando sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Si se dispone de ella se facilitará, como mínimo, la información siguiente:

a) Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

b) El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

c) Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

[6] A pesar de que la delegación en el encargado es una decisión que corresponde al responsable, resulta especialmente recomendable en aquellos supuestos en que los datos se traten exclusivamente con los sistemas del encargado**.**

[7] Plazo y medio recomendados a fin de que el responsable pueda resolver la solicitud dentro del plazo establecido.

[8] El plazo debe ser inferior a 72 horas en cualquier caso.

d) Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

(Escoger alguna o las dos opciones)[9]

☐ *Opción A*

Corresponde al encargado del tratamiento comunicar las violaciones de la seguridad de los datos a la Autoridad de Protección de Datos.

La comunicación contendrá, como mínimo, la información siguiente:

a) Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

b) Nombre y datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

c) Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

d) Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

☐ *Opción B*

Corresponde al encargado del tratamiento comunicar en el menor tiempo posible las violaciones de la seguridad de los datos a los interesados, cuando sea probable que la violación suponga un alto riesgo para los derechos y las libertades de las personas físicas.

La comunicación debe realizarse en un lenguaje claro y sencillo y deberá, como mínimo:

a) Explicar la naturaleza de la violación de datos.
b) Indicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
c) Describir las posibles consecuencias de la violación de la seguridad de los datos personales.

[9] Pese a que la notificación de las violaciones de seguridad a la autoridad de control o a los interesados corresponde al responsable del tratamiento, en aquellos supuestos en que los datos se traten exclusivamente con los sistemas del encargado puede ser recomendable atribuir dichas funciones al encargado.

d) *Describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.*

m. Dar apoyo al responsable del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.

n. Dar apoyo al responsable del tratamiento en la realización de las consultas previas a la autoridad de control, cuando proceda.

o. Poner disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.

p. Implantar las medidas de seguridad siguientes:

(Escoger una o las dos opciones)

☐ *Opción A Las medidas de seguridad siguientes, de acuerdo con la evaluación de riesgos realizada por*[10] _____ *, en fecha* _____ *:*

- _____.
- _____.
- _____.

☐ *Opción B Las medidas de seguridad establecidas en*[11]

_____

En todo caso, deberá implantar mecanismos para:

a) Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
b) Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
c) Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.
d) Seudonimizar y cifrar los datos personales, en su caso.

q. Designar un delegado de protección de datos[12] y comunicar su identidad y datos de contacto al responsable.

[10] Indicar si la evaluación de riesgos ha sido realizada por el responsable o por el encargado del tratamiento.
[11] Indicar el código de conducta, el sello, la certificación u otro estándar donde están definidas las medidas aplicables.
[12] El delegado de protección de datos debe designarse cuando:
a) El tratamiento lo lleve a cabo una autoridad o un organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;
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;
c) Las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales.

r. Destino de los datos

(Escoger una de las tres opciones)

☐ *Opción A* *Devolver al responsable del tratamiento los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida la prestación.*

La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por el encargado.

No obstante, el encargado puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

☐ *Opción B* *Devolver al encargado que designe por escrito el responsable del tratamiento, los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida prestación.*

La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por el encargado.

No obstante, el encargado puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

☐ *Opción C* *Destruir los datos, una vez cumplida la prestación. Una vez destruidos, el encargado debe certificar su destrucción por escrito y debe entregar el certificado al responsable del tratamiento.*

No obstante, el encargado puede conservar una copia, con los datos debidamente boqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

5. Obligaciones del responsable del tratamiento

Corresponde al responsable del tratamiento:

a) Entregar al encargado los datos a los que se refiere la cláusula 2 de este documento.

b) Realizar una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por el encargado.

c) Realizar las consultas previas que corresponda.

d) Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del encargado.

e) Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.

PLANTILLA PARA EL REGISTRO DE ACTIVIDADES DEL TRATAMIENTO

DENOMINACIÓN REGISTRO

DENOMINACIÓN

RESPONSABLE DEL TRATAMIENTO

NOMBRE Y DATOS DEL CONTACTO

DPD (SI PROCEDE)

NOMBRE Y DATOS DEL CONTACTO

BASE JURÍDICA

- ☐ Consentimiento
- ☐ Obligación Legal
- ☐ Misión Realizada En Interés Público o Ej. Poderes Públicos
- ☐ Contrato
- ☐ Proteger Intereses Vitales
- ☐ Interés Legítimo

☐ CATEGORÍAS ESPECIALES DE DATOS

- ☐ Consentimiento explícito
- ☐ Tratamiento necesario para cumplir obligaciones y ejercer los derechos específicos del responsable del tratamiento o del interesado, en el ámbito del derecho laboral y de la seguridad y la protección social
- ☐ Tratamiento necesario para proteger intereses vitales del interesado o de otra persona física
- ☐ Tratamiento efectuado por una fundación, una asociación o cualquier otro organismo sin animo de lucro que tenga una finalidad política, filosófica, religiosa o sindical
- ☐ Tratamiento relativo a datos personales que el interesado ha hecho manifiestamente público
- ☐ Tratamiento necesario para formular, ejercer o defender reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial
- ☐ Tratamiento necesario por razones de interés público esencial
- ☐ Tratamiento necesario para finalidades de medicina preventiva o laboral, de evaluación de la capacidad laboral de trabajador, de diagnostico medico, de prestación de asistencia o de tratamiento de tipo sanitario o social, o de gestión de los sistemas y los servicios de asistencia sanitaria o social
- ☐ Tratamiento necesario por razones de interés público en el ámbito de la salud publica
- ☐ Tratamiento necesario para finalidades de archivo en interés público, de investigación científica o histórica o estadísticas

☐ CONDENAS O INFRACCIONES PENALES

- ☐ Tratamientos de datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas con fines distintos de los de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales
- ☐ Registro completo de los datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas conforme a la regulación del sistema de registros administrativos de apoyo a la Admón de Justicia.
- ☐ Tratamientos de datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas llevados a cabo por abogados y procuradores que tengan por objeto recoger la información facilitad por sus clientes para el ejercicio de sus funciones.

FINALIDADES

☐ ¿ Se elaboran perfiles (por ejemplo, análisis o predicción de aspectos referidos al rendimiento laboral, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos o impacto publicitario muy invasivo o intrusivo, entre otros) que afectan a la privacidad o a los derechos del interesado?

☐ ¿Se produce en este tratamiento una observación sistemática de una zona de acecso público (por ejemplo, a través de videovigilancia, vía CCTV o similares)?

CATEGORÍAS DE INTERESADOS

Descripción de las categorías de interesados de la actividad de tratamiento

☐ Empleados ☐ Cargos públicos ☐ Proveedores ☐ Personaes de contacto

☐ Propietarios o arrendatarios ☐ Estudiantes ☐ Asociados o miembros ☐ Solicitantes

☐ Contribuyentes y sujetos obligados ☐ Demandantes de ocupación ☐ Representantes legales ☐ Inmigrantes

☐ Beneficiarios ☐ Otras categorías

☐ ¿La actividad de tratamiento implica el tratamiento de datos de carácter personal de colectivos vulnerables?

CATEGORÍAS DE DATOS

DATOS DE CARÁCTER IDENTIFICATIVO

☐ NIF / DNI/ Pasaporte / NIE ☐ Dirección postal o electrónica ☐ Imagen / Voz ☐ Núm S. S / Mutualidad

☐ Teléfono ☐ Marcas físicas ☐ Nombre y apellidos ☐ Firma electrónica

☐ Firma manuscrita ☐ Tarjeta sanitaria ☐ IP ☐ geolocalización

☐ N.º de registro personal

CATEGORÍAS ESPECIALES DE DATOS (*)

☐ Opiniones políticas ☐ Vida sexual ☐ Afiliación sindical ☐ Datos biométricos

☐ Religión ☐ Estado fisiológico ☐ Creencias filosóficas ☐ Condenas o infracciones penales

☐ Origen Racial o étnico ☐ Necesidades educativas especiales ☐ Salud ☐ Discapacitados físicos o intelectuales

☐ Datos genéticos

CARACTERÍSTICAS PERSONALES

☐ Estado Civil ☐ Datos familiares ☐ Fecha de Nacimiento ☐ Lugar de Nacimiento

☐ Edad ☐ Sexo ☐ Nacionalidad ☐ Lengua Materna

☐ Características físicas o antropométricas

CIRCUNSTANCIAS SOCIALES

☐ Alojamiento o vivienda ☐ Situación militar ☐ Propiedades ☐ Aficiones y estilos de vida

☐ Clubs y asociaciones ☐ Licencias, permisos, autorizaciones

DETALLES DE OCUPACIÓN PROFESIONAL

☐ Cuerpo, escala ☐ Categoría, grado ☐ Puestos de trabajo ☐ Historial laboral

☐ Datos no económicos de nómina

ACADÉMICOS Y PROFESIONALES

☐ Formación y titulaciones ☐ Experiencia profesional

☐ Historial Académico ☐ Colegios o asociaciones profesionales

ECONÓMICOS, FINANCIEROS Y DE SEGUROS

☐ Ingresos, Rentas ☐ Impuestos, deducciones ☐ Inversiones, patrimonio ☐ Planes de pensiones, jubilación

☐ Créditos, préstamos, avales ☐ Hipotecas ☐ Datos bancarios ☐ Subsidios, beneficios

☐ Seguros ☐ Historial, créditos ☐ Datos de nómina ☐ Tarjetas de crédito

TRANSACCIONES DE BIENES Y SERVICIOS

☐ Bienes suministrados ☐ Bienes recibidos

☐ Transacciones financieras ☐ Compensaciones, indemnizaciones

INFORMACIÓN COMERCIAL

☐ Actividades y negocios ☐ Licencias comerciales ☐ Suscripciones a publicaciones ☐ Creaciones artísticas, científicas, etc

OTROS TIPOS DE DATOS

☐ Infracciones administrativas ☐ Otros tipos de datos

DESTINATARIOS

NOMBRE DESTINATARIO: _____

NOMBRE DESTINATARIO: _____

NOMBRE DESTINATARIO: _____

(*) si procede, adjuntar base jurídica de consentimiento

TRANSFERENCIAS INTERNACIONALES

País: _____

Organización Internacional: _____

Documentación de garantías adecuadas: _____

Enlace web al documento (*): _____

MEDIDAS Y PLAZOS

DESCRIPCIÓN GENERAL DE MEDIDAS TÉCNICAS Y ORGANIZATIVAS DE SEGURIDAD

Descripción general:	
Metodología utilizada:	
Lista de medidas aplicables:	

SISTEMA DE TRATAMIENTO DE LA ACTIVIDAD DE TRATAMIENTO

☐ Manual ☐ Automatizado

Descripción:	

PLAZOS PREVISTOS PARA SUPRIMIR DATOS

PROCEDENCIA

IDENTIFICACIÓN DE LA PROCEDENCIA

☐ Del mismo interesado o de su representante legal ☐ Lugares de acceso público

☐ De otras personas físicas diferentes del interesado ☐ De registros públicos

☐ De entidades privadas ☐ De administraciones públicas

☐ Otras

IDENTIFICACIÓN DEL PROCEDIMIENTO DE RECOGIDA

☐ Encuestas o entrevistas ☐ Formularios

☐ Transmisión electrónica ☐ Otros

EIPD

☐ Procede

Motivo	

INFORMACION BÁSICA DE LA POLÍTICA DE PRIVACIDAD
¿Quién es responsable del tratamiento? • Nombre: • CIF: • Dirección: • Correo electrónico: ¿Qué datos tratamos sobre ti?
¿Cómo obtenemos y de dónde proceden tus datos?
¿Para qué y por qué utilizamos tus datos?
¿Durante cuánto tiempo conservamos tus datos?
¿Cuál es la legitimación para el tratamiento de tus datos?
¿Cuáles son tus derechos y cómo puedes controlar tus datos?
¿Quién tiene acceso a tus datos?
¿Cómo protegemos tus datos?

¿Hacemos transferencias internacionales de datos?
Cambios:

FORMULARIO PARA COMUNICAR DESIGNACIONES, MODIFICACIONES DE DATOS O CESE DE FUNCIONES DE DELEGADOS DE PROTECCIÓN DE DATOS (DPD)

Indique el tipo de información a comunicar:

☐ **Designación de DPD** ☐ **Modificación de datos de un DPD existente** ☐ **Cese de funciones de un DPD**

1 DATOS DEL ORGANISMO O ENTIDAD QUE NOMBRA O DESIGNA AL DELEGADO DE PROTECCIÓN DE DATOS

TIPO:

☐ INSTITUCIÓN AUTONÓMICA	☐ ADMINISTRACIÓN AUTONÓMICA	☐ ENTIDAD DE DERECHO PÚBLICO O PRIVADO DEPENDIENTE DE LA ADMÓN. AUTONÓMICA	☐ OTROS
☐ UNIVERSIDAD	☐ ADMINISTRACIÓN LOCAL	☐ ENTIDAD DE DERECHO PÚBLICO O PRIVADO DEPENDIENTE DE LA ADMÓN. LOCAL	

DENOMINACIÓN DEL ORGANISMO O ENTIDAD: NIF:

DIRECCIÓN POSTAL:

CÓDIGO POSTAL: LOCALIDAD: PROVINCIA:

TELÉFONO: CORREO ELECTRÓNICO:

DENOMINACIÓN DEL CARGO QUE NOMBRA O DESIGNA AL DPD:

En su caso, DENOMINACIÓN de la Institución, Consejería, Ayuntamiento, Diputación, Universidad, etc., de la que depende el organismo o entidad:

2 IDENTIFICACIÓN DEL DELEGADO DE PROTECCIÓN DE DATOS

FECHA DE NOMBRAMIENTO O BAJA: DEDICACIÓN A LAS FUNCIONES DE DPD EN EL ORGANISMO O ENTIDAD QUE LO NOMBRA: ☐ PARCIAL ☐ COMPLETA

TIPO:

☐ ES UNA PERSONA FÍSICA PERTENECIENTE AL ORGANISMO O ENTIDAD

☐ ES UN ÓRGANO COLEGIADO, GRUPO DE TRABAJO O SIMILAR, PERTENECIENTE AL ORGANISMO O ENTIDAD
Denominación:

☐ ES EXTERNO, DESEMPEÑANDO SUS FUNCIONES EN EL MARCO DE UN CONTRATO DE SERVICIOS O SIMILAR
Razón social del prestador del servicio: NIF del prestador del servicio:

☐ El servicio lo presta una persona física de la plantilla del prestador del servicio

☐ El servicio lo presta un grupo o departamento, denominado:

NOMBRE Y APELLIDOS[1]: SEXO [2]: ☐ H ☐ M DNI:

[1] Se deberá identificar al DPD, en caso de ser persona física, o a la persona física que representa al DPD o coordina/dirige sus funciones [2] Dato opcional

3 DATOS PÚBLICOS PARA CONTACTO CON EL DELEGADO DE PROTECCIÓN DE DATOS

DIRECCIÓN POSTAL:

CÓDIGO POSTAL: LOCALIDAD: PROVINCIA:

TELÉFONO CONTACTO[2]: CORREO ELECTRÓNICO DE CONTACTO DEL DPD:

INDICAR LA DIRECCIÓN (URL) DONDE SE PUBLICAN, EN LA WEB DEL ORGANISMO O ENTIDAD, LOS DATOS DE CONTACTO DEL DPD (Art. 37.7 RGPD):

[2] Dato opcional

4 ÁMBITO DE ACTUACIÓN DEL DELEGADO DE PROTECCIÓN DE DATOS: RESPONSABLES DE TRATAMIENTOS

DE ACUERDO CON EL REGISTRO DE ACTIVIDADES DE TRATAMIENTO (RAT), CUMPLIMENTE LOS DATOS DE LOS DISTINTOS RESPONSABLES DEL TRATAMIENTO PARA LOS QUE EJERCE SUS FUNCIONES EL DPD. EN PARTICULAR, SI ES EL CASO, DEBERÁ INCLUIR EL PROPIO ORGANISMO O ENTIDAD CONSIGNADO EN EL APARTADO 1.

#	DENOMINACIÓN DEL RESPONSABLE	NIF DEL RESPONSABLE [3]	DIRECCIÓN POSTAL [3]
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			

INDICAR LAS DIRECCIONES DE INTERNET (URL) DONDE SE PUBLICA/N EL/LOS INVENTARIO/S DE ACTIVIDADES DE TRATAMIENTO CORRESPONDIENTE/S A LOS RESPONSABLES ANTERIORES (Art. 31.2 LOPDGDD):

[3] No será necesario cumplimentar el NIF o la dirección postal si coinciden con los datos aportados en el apartado 1

5 DOCUMENTACIÓN QUE SE ADJUNTA

- ☐ Documentación sobre la designación o nombramiento del DPD, o sobre el cese de sus funciones
- ☐ En su caso, documentación sobre la representación de la persona que realiza la comunicación de los datos del DPD
- ☐ .....
- ☐ .....

6 DATOS DE LA PERSONA QUE REALIZA LA COMUNICACIÓN

NOMBRE Y APELLIDOS:	SEXO [2]: ☐ H ☐ M	DNI:

CARGO, PUESTO DE TRABAJO O RELACIÓN DE LA PERSONA QUE REALIZA LA COMUNICACIÓN CON EL ORGANISMO O ENTIDAD:

TELÉFONO [2]:	CORREO ELECTRÓNICO:

[2] Dato opcional

7	PRESENTACIÓN, LUGAR, FECHA Y FIRMA

PRESENTO la presente comunicación, solicitando su admisión , y **DECLARO** que son ciertos los datos consignados en ella y la documentación que se adjunta a la misma, así como que he leído la información sobre protección de datos personales que figura en el formulario y que se ha informado al DPD y a los responsables del tratamiento de la realización de la presente comunicación.

En ....., a ..... de ..... de .....

LA PERSONA QUE REALIZA LA COMUNICACIÓN,

Fdo.[3]: .....

[3] Si se presenta electrónicamente, no es necesaria la firma manual

Código Directorio Común de Unidades Orgánicas y Oficinas:

Plantilla de EIPD

Debe comenzar a completar la plantilla al inicio de cualquier proyecto importante que involucre el uso de datos personales, o si está realizando un cambio significativo en un proceso existente. Los resultados finales deben integrarse nuevamente en el plan de su proyecto.

Paso 1: Identificar la necesidad de una EIPD

Explique ampliamente qué pretende lograr el proyecto y qué tipo de procesamiento implica. Puede resultarle útil consultar o vincular otros documentos, como una propuesta de proyecto. Resuma por qué identificó la necesidad de una EIPD.

Paso 2: describir el procesamiento

Describa la naturaleza del procesamiento: ¿ cómo recopilará, utilizará, almacenará y eliminará los datos? ¿Cuál es la fuente de los datos? ¿Compartirás datos con alguien? Puede resultarle útil consultar un diagrama de flujo u otra forma de describir los flujos de datos. ¿Qué tipos de procesamiento identificados como probablemente de alto riesgo están involucrados?

Describa el alcance del procesamiento: ¿ cuál es la naturaleza de los datos? ¿Incluyen datos de categorías especiales o delitos penales? ¿Cuántos datos recopilará y utilizará? ¿Con qué frecuencia? ¿Cuánto tiempo lo conservarás? ¿Cuántas personas se ven afectadas? ¿Qué zona geográfica cubre?

Describa el contexto del procesamiento: ¿cuál es la naturaleza de su relación con las personas? ¿Cuánto control tendrán? ¿Esperarían que usted usara sus datos de esta manera? ¿Incluyen a niños u otros grupos vulnerables? ¿Existen preocupaciones previas sobre este tipo de procesamiento o fallas de seguridad? ¿Es novedoso en algún sentido? ¿Cuál es el estado actual de la tecnología en este ámbito? ¿Hay algún tema actual de interés público que deba tener en cuenta? ¿Está usted inscrito en algún código de conducta o esquema de certificación aprobado (una vez que haya sido aprobado)?

Describa los fines del procesamiento: ¿qué desea lograr? ¿Cuál es el efecto deseado sobre los individuos? ¿Cuáles son las ventajas del procesamiento, para usted y en general?

Paso 3: proceso de consulta

Considere cómo consultar con las partes interesadas relevantes: describa cuándo y cómo buscará las opiniones de las personas – o justifique por qué no es apropiado hacerlo. ¿A quién más necesita involucrar dentro de su organización? ¿Necesita pedir ayuda a sus procesadores? ¿Planea consultar a expertos en seguridad de la información o a cualquier otro experto?

Paso 4: Evaluar la necesidad y la proporcionalidad

Describa las medidas de cumplimiento y proporcionalidad, en particular: ¿ cuál es su base legal para el procesamiento? ¿El procesamiento realmente logra su propósito? ¿Existe otra forma de lograr el mismo resultado? ¿Cómo evitará el deterioro de la función? ¿Cómo garantizará la calidad y minimización de los datos? ¿Qué información le dará a las personas? ¿Cómo ayudarás a apoyar sus derechos? ¿Qué medidas se toman para garantizar que los procesadores cumplan? ¿Cómo se protegen las transferencias internacionales?

Paso 5: Identificar y evaluar los riesgos

Describa la fuente del riesgo y la naturaleza del impacto potencial en las personas. Incluir riesgos corporativos y de cumplimiento asociados. según sea necesario.	**Probabilidad de daño**	**Impacto**	**Riesgo general**

Paso 6: Identificar medidas para reducir el riesgo

Identifique medidas adicionales que podría tomar para reducir o eliminar los riesgos identificados como de riesgo medio o alto en el paso 5.				
Riesgo	**Opciones para reducir o eliminar el riesgo**	**Efecto sobre el riesgo**	**Riesgo residual**	**Medida aprobada**

Paso 7: cerrar sesión y registrar los resultados

Artículo	**Nombre fecha**	**Notas**
Medidas aprobadas por:		Integrar acciones nuevamente en el plan del proyecto, con fecha y responsabilidad de finalización.
Riesgos residuales aprobados por:		Si acepta algún alto riesgo residual, consulte con el ICO antes de seguir adelante.
Asesoramiento DPO proporcionado:		El DPO debe asesorar sobre el cumplimiento, las medidas del paso 6 y si el procesamiento puede continuar
Resumen del asesoramiento del DPO:		
Asesoramiento del DPO aceptado o anulado por:		Si se anula, deberá explicar sus motivos.
Comentarios:		
Respuestas a la consulta revisadas por:		Si su decisión se aparta de las opiniones de las personas, debe explicar sus motivos.
Comentarios:		
Esta EIPD será revisada por:		El DPO también debería revisar el cumplimiento continuo de la EIPD.