UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería Informática

Guía sobre protección de datos e implantación de la LOPDGDD en centros sanitarios.

.

Trabajo Fin de Grado

Grado en Ingeniería Informática

AUTOR/A: Mullor Berenguer, Marta

Tutor/a: Oltra Gutiérrez, Juan Vicente

CURSO ACADÉMICO: 2022/2023

RESUMEN

El trabajo se centra en la elaboración de una guía de buenas prácticas en el ámbito de la protección de datos, cuyo objetivo consiste en la fácil implementación del cumplimiento de la normativa vigente para los profesionales TIC e informáticos en organizaciones que manipulen datos de carácter sanitario como hospitales, ambulatorios, clínicas privadas, etc. La normativa vigente queda representada por dos pilares fundamentales como la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) a nivel nacional y el Reglamento 2016/679 o Reglamento General de Protección de Datos (RGPD) a nivel europeo, además existe material adicional elaborado por la AEPD que trata temas mucho más específicos. A lo largo de este, se hace un repaso de los principales aspectos de cuáles son los derechos y las responsabilidades de los agentes involucrados (profesionales sanitarios, terceros involucrados, pacientes y figuras responsables en la protección de datos sensibles) en la protección de datos en una organización del ámbito sanitario. Por otro lado, se proporcionan herramientas y guías obtenidas por la Agencia Española de Protección de Datos con la finalidad de controlar que se cumpla el deber de informar.

Una vez se ha detallado el contexto socio-legal, se procede al desarrollo de la guía la cual sirve como herramienta de apoyo para los técnicos e informáticos que junto a los responsables del tratamiento les sirva como una primera aproximación o como punto de partida para obtener la información requerida en materia de protección de datos sanitarios. En último lugar, se realiza una reflexión sobre el alcance de los objetivos propuestos y se dejan abiertas distintas líneas de trabajo para desarrollar posibles futuros trabajos.

ABSTRACT

The project focuses on the development of a guide of good practices in the field of data protection, the aim of which is the easy implementation of compliance with current regulations for the Technical and IT managers in organisations that handle health data such as hospitals, clinics, private clinics, etc. The current regulations are represented by two fundamental pillars such as Organic Law 3/2018 of 5 December, on the Protection of Personal Data and guarantee of digital rights (LOPDGDD) at national level and Regulation 2016/679 or General Data Protection Regulation (RGPD) at European level. There is also additional material produced by the AEPD that deals with much more specific issues. Throughout the work, a review is made of the main aspects of the rights and responsibilities of the agents involved (healthcare professionals, third parties involved, patients and responsible figures for the protection of sensitive data) in the protection of data in healthcare organisations. On the other hand, tools and guidelines obtained from the Spanish Data Protection Agency are provided for the purpose of controlling compliance with the duty to inform.

Once the socio-legal context has been detailed, we proceed with the development of the guide which serves as a support tool for those for technical and IT manager with data processing responsible, serve as that wish to make a first approach or as a starting point for obtaining the information required in the field of health data protection. Finally, a reflection is made on the scope of the proposed objectives and different lines of work are left open for the development of possible future projects.

ABREVIATURAS

AEPD: Agencia Española de Protección de Datos.

AR: Análisis de Riesgos.

ARCO: derechos de Acceso, Rectificación, Cancelación y Oposición.

ARCO+: Acceso, Rectificación, Cancelación, Oposición, Portabilidad, Limitación del tratamiento y a no ser Objeto de decisiones individuales automatizadas.

CCAA: Comunidades Autónomas.

CCN-CERT: Centro Criptológico Nacional *Computer Emergency Response Team*.

CET: Contratos con los Encargados de Tratamiento.

CI: Cláusulas Informativas.

CSIC: Consejo Superior de Investigaciones Científicas.

DPD: Delegado de Protección de Datos.

EIPD: Evaluación de Impacto de Protección de Datos.

GVA: Generalidad Valenciana.

HIS: Sistema de Información Hospitalario.

IIP: Información de Identificación Personal.

IP: Información Personal.

IPS: Información Personal Sensible.

LOPD: Ley Orgánica de Protección de Datos de carácter personal.

LOPDGDD: Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales.

PAMS: Plan de Acción y Medidas de Seguridad.

RAE: Real Academia Española.

RAT: Registro de Actividades de Tratamiento.

RGPD: Reglamento General de Protección de Datos de la Unión Europea.

SCCs: *Standard Contractual Clauses* - cláusulas contractuales estándar.

TI: Tecnologías de la Información.

UE: Unión Europea.

UNE: Una Norma Española.

TABLA DE CONTENIDO

TABLA DE FIGURAS

1. INTRODUCCIÓN

La obtención, tratamiento y almacenamiento de información está cobrando más y más relevancia con el paso del tiempo. Por ello, es importante contar con sistemas capacitados para obtener, tratar y almacenar grandes volúmenes de información, que sea de interés, en forma de datos para cualquier tipo de entidad, pública o privada, y cualquier tipo de sector. El sector salud no es una excepción. No sólo es importante disponer de tecnología suficiente para la gestión de toda la información si no que es de vital importancia velar por la seguridad de esta. Para ello, se debe cumplir con la legislación vigente encargada de regular el tratamiento de los datos clínicos de los usuarios del sistema sanitario. Con ello se preserva el derecho de confidencialidad de la información sanitaria de las personas y evitar accesos no autorizados. Por tanto, estar al orden de la legislación vigente en seguridad y protección de datos es un requisito fundamental para cualquier entidad pública sanitaria con tal de asegurar al usuario una transparencia lícita.

El desarrollo y confección de una guía de buenas prácticas sirve de ayuda para concienciar de la importancia de los derechos y deberes en el tratamiento de información de una forma clara y lícita. Para la estructuración y creación de las directrices presentes en la guía se ha hecho uso de un amplio abanico normativo. Así encontramos legislación autonómica, nacional y supranacional por parte de la Unión Europea. El cumplimiento y seguimiento de la normativa se vigila mediante organismos encargados de notificar los derechos y obligaciones de los agentes. Los hospitales como infraestructura representativa de la Sanidad Pública deben ser conscientes de la transformación que está acarreando estos reglamentos para estar al tanto en la forma de gestionar los datos y los riesgos que ello implica. Cumplir las normativas y seguir las advertencias que ofrecen las distintas organizaciones debería ser por motivo propio además de pasar a ser de un ámbito primordial de intervención y dejar de ser cumplidas por obligación. Ya que estas normativas y recomendaciones tienen la capacidad de apaciguar y disminuir de forma significativa los riesgos a los que de forma exponencial se enfrentan dichas infraestructuras.

Apoyándome en la noticia del CCN-CERT que ya en 2014 publicó:

> *Atacar los sistemas informáticos de los hospitales para robar datos sensibles se ha convertido en una práctica tristemente usual en los últimos meses. La práctica de sustraer información médica ha aumentado en un 600% en 2014. La tendencia en alza de compartir datos entre hospitales, a pesar de ser beneficiosa para el paciente, ha empezado a generar un serio problema de seguridad para la industria sanitaria. La explicación es muy sencilla: la información médica es demasiado valiosa. Ahí está el dinero.*

Para que cualquiera pueda hacerse una idea, mientras que una tarjeta de crédito tendría un valor de pocos euros en el mercado negro, un historial clínico puede llegar a costar en torno a los 80 euros. Hay mucha diferencia. El coste de esa información es alto por su contenido: no solo se obtienen datos sanitarios sino también información personal detallada: números de la seguridad social, direcciones, cuentas bancarias..., que pueden utilizarse para la suplantación de identidad.

Además, hay que recordar que, en Estados Unidos, donde el problema es mayor, la sanidad tiene un coste muy elevado y está mayoritariamente en manos de empresas privadas, que cotizan en Bolsa. Por eso están intentando contener la preocupación generalizada sobre el asunto, aunque con bastantes dificultades.

En agosto tuvo lugar uno de los robos de datos médicos más importantes hasta el momento, aunque no es el único ni probablemente será el último. La información personal de más de cuatro millones de pacientes de la red de hospitales de "Community Health Systems" fue comprometida.

«Ahora ni hospitales, ni centros de salud, ni departamentos sanitarios o empresas dedicadas a dispositivos relacionados están a salvo. Todas las personas que habían recibido tratamiento en alguna consulta vinculada a esta red se vieron afectadas.

Por eso el FBI aseguró que iba a destinar recursos y esfuerzos para orientar, interrumpir, desmantelar y detener a los autores. Por eso llevó a cabo una investigación para determinar de dónde procedían los ataques: al parecer los cibercriminales trabajan desde China y utilizaron un "malware[1]" sofisticado. Están acostumbrados a espiar a la industria médica y a robar fórmulas de diferentes medicamentos y drogas, y llevan actuando más de cuatro años, aunque es ahora cuando están teniendo mayor impacto por la modernización tecnológica del sector.

También quiso tomar medidas para advertir a las empresas de servicios de salud de la necesidad de establecer todas las medidas de seguridad posibles. Desde hace un par de meses, lanza cada cierto tiempo alertas que pueden ayudar a prevenir ataques informáticos o a detectar que han sucedido para remediar sus posibles consecuencias.

[1] Definición en GLOSARIO

Además, los hospitales no suelen estar adaptados para este tipo de ataques, mucho menos cuando una gran cantidad de los dispositivos que utilizan cada día están conectados a la red. Sin embargo, es más que necesario que se adapten al nuevo entorno favorecido por el Internet de las cosas. Según Kristopher Kushe, experto en servicios de información médica, actualmente existen en el país unos 20.000 dispositivos utilizados en el ámbito sanitario y conectados a la Red.

Es por eso que considera necesario que las diferentes organizaciones lleven a cabo auditorías para evaluar el riesgo en sus instalaciones con acceso a Internet. No obstante, lo más complicado es enseñar a prevenir de forma generalizada y rápida, para hacer frente a los ataques que ya están ocurriendo. Aunque una de las formas más sencillas de comenzar con la tarea es instalar programas capaces de detectar el "malware", algo que en el corto plazo podría ayudar a proteger a los dispositivos frente a infecciones.

Además, los ataques crean mucha inseguridad en el entorno médico, más allá del robo de datos, porque muchos de estos dispositivos son los que se utilizan de forma habitual para ayudar a los pacientes. Los médicos se preguntan si alguien podría piratear los aparatos de tal forma que llegue a perjudicar la salud de las personas. No sería la primera vez que alguien logra manipular un marcapasos... [16]».

Estas amenazas tienen significativas consecuencias tanto para las organizaciones como para los posibles afectados.

1.1.Motivación

Se ha elegido este trabajo de fin de grado principalmente por su temática: la protección de datos. Como cualquier otra persona dada de alta en la Sanidad Pública, he experimentado el proceso que va desde tener que comunicar tus síntomas al trabajador que se encuentra en la recepción del hospital hasta el tiempo de espera para que el médico proceda a realizar la consulta u otro en su lugar que en teoría conoce tu problemática e intenta darte solución a través de una llamada de un par de minutos. Este proceso despertó en mí el interés cuando tomé consciencia que la persona de recepción era la encargada de derivar tu caso dentro de los distintos roles sanitarios que puede haber en un hospital. Esto despertó en mi la curiosidad sobre qué suponía el trabajo de los informáticos dentro del ámbito sanitario, qué tipo de herramientas, convenios y protocolos deben seguir para el tratamiento de datos. Por otra parte, tomé consciencia de que cualquier tipo de

sanitario, con un DNI y algún que otro dato más, era capaz de acceder a tu historial clínico, sin ningún tipo de impedimento, como consecuencia vi la oportunidad en la realización de este trabajo, la oportunidad de conocer la privacidad alrededor de los datos de nuestra salud física y mental, además de estudiar los posibles riesgos sobre la confidencialidad de estos y empezando por la investigación de qué datos son los que se recogen. He de añadir que había otros trabajos de fin de grado con la misma temática, pero me decidí por este ya que era el que me permitía realizar mi propia investigación sobre el tratamiento de datos clínicos, cual es la legislación, normas, reglamentos y guías que garantizan la privacidad de los estos todo ello enfocado al perfil del informático.

1.2.Objetivos

El principal objetivo de este trabajo fin de grado es elaborar una guía clara y de fácil entendimiento con el objetivo de informar a los profesionales TIC e informáticos de los centros sanitarios y les resulte sencillo aplicar la normativa vigente en lo que respecta a la protección de datos en centros sanitarios, hospitales, clínicas privadas y toda institución que trate datos relacionados con la salud.

El segundo objetivo principal de esta guía es dar respuesta a las preguntas frecuentes y procedimientos a desarrollar a través de las herramientas y guías oportunas que van a facilitar a los profesionales TIC e informáticos que intervienen en el proceso de tratamiento de datos en el desarrollo de la prestación de servicios sanitarios y así poder contribuir a la aplicación del cumplimiento de los derechos de los pacientes y usuarios cuando administraciones y profesionales sanitarios tengan dudas sobre estos.

El tercer objetivo principal sería, refiriéndonos concretamente a los profesionales TIC o informáticos recién llegados a este tipo de puesto de trabajo, facilitarles la implementación y seguimiento de la normativa vigente recopilando las guías y herramientas necesarias para el desarrollo de este rol.

Como objetivo secundario: contribuir a que la protección de los datos personales sea un tema de interés y tome especial relevancia entre trabajadores no implicados en el proceso del tratamiento de protección de datos ya que, aunque no sean partícipes directos en dicho tratamiento del ámbito sanitario es muy probable que estén involucrados en otro ámbito y no tengan consciencia de ello.

1.3.Impacto esperado

Se espera que este trabajo desarrolle efecto en distintos ámbitos:

En el ámbito práctico, al ser una guía facilitaría la correcta implantación de las normativas asociadas, también podrá tener utilidad en la promulgación de la protección y tratamiento de datos dentro del entorno relacionado con la salud, así como promover la finalidad de los métodos empleados en dicho desarrollo.

En el ámbito metodológico, se destaca la principal motivación de identificar la problemática además de la búsqueda proactiva de soluciones que a través de herramientas y métodos pueden ayudar al conocimiento y la divulgación metodológica.

En el ámbito investigativo, se llega a aportar un conocimiento teórico a nivel tanto académico como empresarial, debido al enfoque que se realiza en los estudios de nivel superior ya que se podrán desarrollar proyectos que involucren la misma naturaleza o tengan relación con la misma temática.

En el ámbito laboral, la guía pretende añadir valor, no solo a los encargados y responsables del tratamiento y protección de datos, sino también al personal responsable técnico y/o informático dentro del ámbito sanitario que trate en algún momento con datos personales sensibles, ya que proporciona las bases para conocer y divulgar sobre todo el proceso de informar y los derechos de los pacientes y empleados. Por otra parte, pretende promover la sensibilización del público con la materia, la comprensión de los riesgos y las normas, incluyendo los derechos y las garantías y facilitar un primer acercamiento a los responsables y encargados del tratamiento en cuanto a las obligaciones dentro de la materia de protección de datos, además de esclarecer la normativa vigente en este tipo de contexto.

1.4.Metodología

Los objetivos de este trabajo se han ido alcanzando de forma progresiva ya que se ha dividido el proceso en cuatro fases:

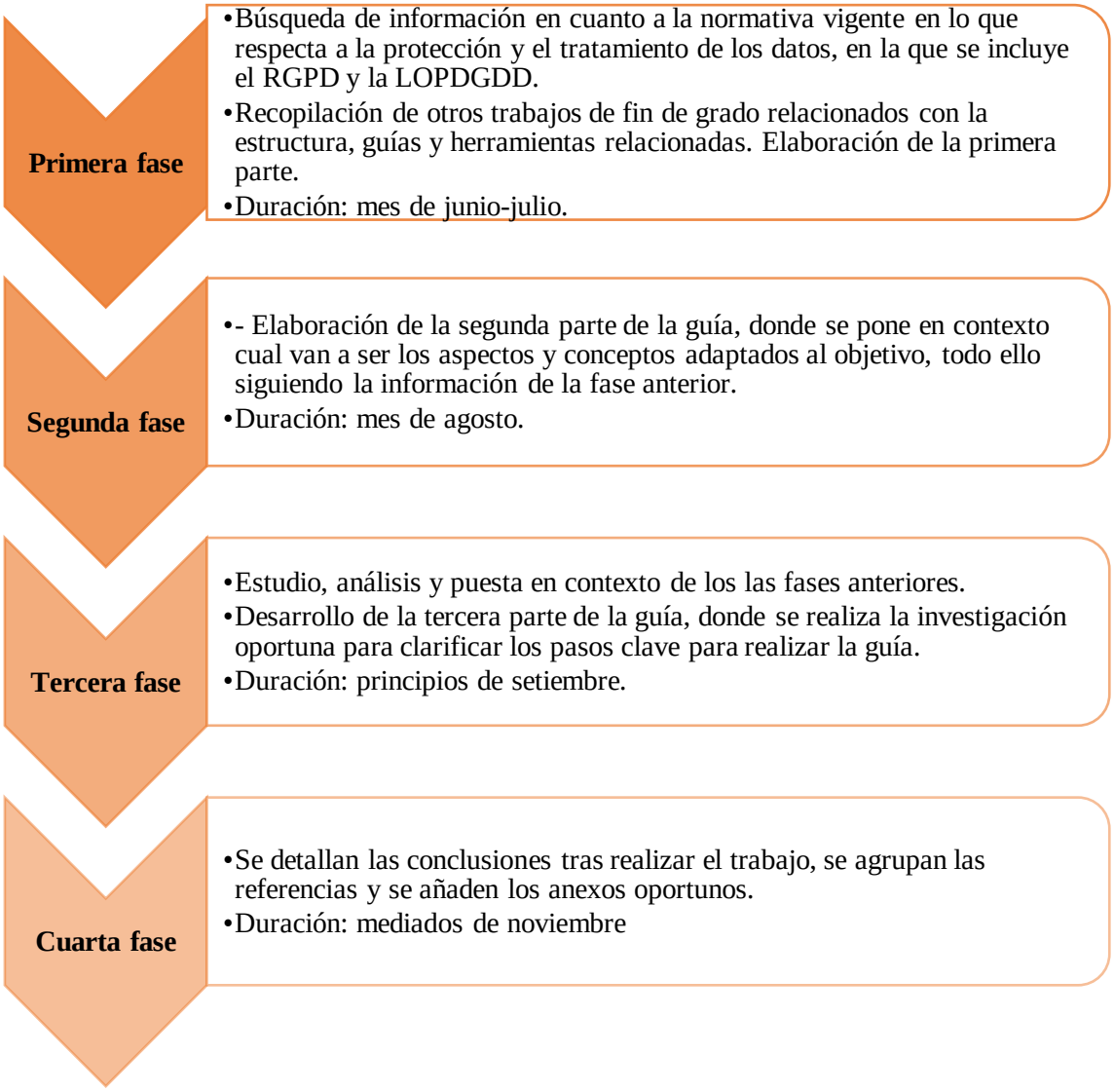


Ilustración 1. Cronología de la metodología del trabajo. Fuente: elaboración propia

1.5.Estructura

El trabajo se ha divido en tres partes:

La primera parte trata introducción, donde se detalla cuáles son los motivos por el que he realizado este trabajo, los objetivos que se persiguen, el impacto esperado de la elaboración del trabajo y cuál es la metodología que se ha seguido durante la realización. También se incluye el estado del arte al cual se acoge a la temática principal, su análisis y el marco legal. La segunda parte engloba los aspectos y conceptos generales de la protección de datos para contextualizar en el ámbito

sanitario, empezando por la legitimización para el tratamiento de los datos siguiendo con la clasificación de los tipos de información que se recogen en los tratamientos de datos y finalmente se describe la historia clínica como documento legal representativo. La tercera parte es el desarrollo de la guía en la cual se detalla los procedimientos necesarios empezando por cuáles son las obligaciones en el tratamiento de datos, los distintos protocolos en la protección de datos para el personal empleado, la gestión de los derechos involucrados, la cesión de datos a terceros, como quedan involucradas las políticas de privacidad y por último los distintos tipos de sanciones.

Por último, queda recogida la conclusión donde se aclara la obtención de los objetivos que previamente se han descrito, los posibles trabajos futuros relacionados con la temática que se podrían desarrollar tras la elaboración de este, también hay tres anexos donde se recogen: en el primero; los ejes principales de la guía, en el segundo; los artículos 9.1, 9.2, 10, 13, 14, 17 y 36.2, Considerandos: 51, 53, 71, 81 del RGPD, lo que permite un mayor conocimiento de los artículos nombrados a lo largo del trabajo y el tercer anexo contiene la relación de los Objetivos de Desarrollo Sostenible (ODS) con el trabajo. Finalmente, se encuentra el glosario el cual recoge las definiciones de la nomenclatura utilizada y de interés para la total comprensión de este trabajo de fin de grado.

1.6.Estado del arte

Para la elaboración de este trabajo se exploró en distintas fuentes que hacían referencia al cumplimento del Reglamento General de Protección de Datos, entre las que destacan los trabajos de fin de grado de Bañó Juan, A. (2021), Llorca Mena, P (2021), los cuales han desarrollado guías para el cumplimiento del Reglamento General de Protección de Datos, ya sea en su totalidad o centrándose en ciertos aspectos del reglamento. En base a estos trabajos se pudo recopilar valiosa información y aspectos para este trabajo, además, aparecieron varias ideas para la implementación y desarrollo de la guía, incluyendo su aplicación. Asimismo, los datos recogidos de estos trabajos facultaron consultar otros trabajos de temática similar y dotaron de motivos para llevar a cabo este trabajo, ya que, hasta la fecha, no se ha llevado a la práctica ningún trabajo relacionado con el tema del presente. Adicionalmente, también se consultó la información que proporciona la Agencia Española de Protección de Datos (en adelante AEPD), entre la cual destacan: la Guía para Profesionales del sector sanitario, la Guía para pacientes y usuarios de la Sanidad, el documento sobre la Privacidad en DNS, La introducción al hash como técnica de seudonimización de datos personales, el documento sobre los 14 equívocos con relación a la

identificación y autenticación biométrica, el documento sobre las tecnologías y protección de datos en las AA.PP., la protección de datos en las relaciones laborales, la guía para la notificación de brechas de datos personales. Y herramientas como: Gestiona EIPD, Comunica-Brecha RGPD, Evalúa-brecha RGPD, Asesora-Brecha y el Canal de DPD relacionadas con el deber de informar y el Reglamento (UE) 2016/679. Por último, también se consultó el documento sobre (la K-anonimidad como medida de la privacidad, AEPD) que se dirige a responsables y encargados de tratamiento que aborden procesos de anonimización sobre conjuntos de datos. Ya que al abordar fuentes de datos independientes que se interconectan y que, por diseño, pueden compartir atributos comunes, cabe la posibilidad de crear un rastro electrónico de los individuos, incluso cuando se hayan suprimido los datos que explícitamente les identifican, pudiendo llegar a establecerse vínculos entre dichas fuentes de información y constituir así una amenaza para la privacidad de los interesados cuyos datos están sujetos a tratamiento. Dada la existencia de tales ataques en los que se pueden inferir atributos sensibles para *k* -datos de anonimato, se creó el método de *l* -diversidad para promover el *k* -anonimato manteniendo adicionalmente la diversidad de campos sensibles.

1.6.1. Crítica al estado del arte

El primer trabajo titulado *Creación de una guía para el control del deber de informar en cumplimiento del Reglamento de Protección de Datos Europeo*, realizado por Adrián Bañó Juan en 2021 para la Universidad Politécnica de Valencia, tiene como objetivo la creación de un documento para el colaborar en el apoyo hacia los responsables y encargados de tratamiento de datos personales a la adaptación de las nuevas directrices y obligaciones que presenta el Reglamento General de Protección de Datos. Esta aplicación podrá ser aprovechada como guía y como lista de verificación para comprobar si se realizan las acciones correctas para atenerse al reglamento mencionado anteriormente. Además, se plantea el uso de la normativa desde un lenguaje claro, sencillo y eficiente para ser entendido, consiguiendo que los responsables y encargados puedan llegar a usarla fácilmente. [2] Con todo esto, se contribuye al desarrollo del presente trabajo ya que el rol de responsable y del encargado del tratamiento de datos personales cumple un papel muy importante en el deber de informar, que, aunque no sea el punto principal, se sigue contribuyendo a uno de los puntos clave de la guía que se va a elaborar.

El segundo trabajo se titula *Elaboración de una guía de buenas prácticas en protección de datos para pequeñas empresas*, realizado por Pau Llorca Mena en 2021 para la Universidad Politécnica de Valencia (2021) tiene como objetivo la realización de una guía de buenas prácticas en materia de protección de datos y de ciberseguridad para pequeñas y medianas empresas, con el objetivo

de facilitar el cumplimiento de las medidas de seguridad establecidas en las diferentes normativas para el responsable de datos de una empresa [13]. Contribuye en este trabajo en hacer un repaso de los principales aspectos a tener en cuenta desde una organización para tratar los datos de terceros de forma correcta, cumpliendo con la normativa vigente y mitigando el riesgo de sufrir brechas de seguridad. Adicionalmente, ofrece un cuestionario que permite la autoevaluación de la situación de la empresa en materia de seguridad informática y protección de datos, para el posterior análisis y contacto con expertos en caso de ser necesario

El tercer y último trabajo se titula *Guía Interactiva para el cumplimiento de normas de Protección de Datos en el entorno laboral*, realizado por Josep Mompó en 2020 para la Universidad Politécnica de Valencia, tiene como objetivo el desarrollo de una guía interactiva que permite la ejecución del cumplimiento de las normas de protección de datos en el entorno laboral. Donde se da a conocer la figura del delegado de Protección de Datos y cuáles son sus responsabilidades y obligaciones [15]. Ahora bien, este trabajo contribuye al desarrollo del presente trabajo ya que la figura del delegado de Protección de Datos cumple un rol transcendental a la hora de controlar el deber de informar e incluso a la hora de informar, con lo que será importante conocer sus funciones a la hora de realizar la guía.

La Guía para Profesionales del sector sanitario realizada por la AEPD, destinada a los profesionales sanitarios, tiene la finalidad de que estos puedan desarrollar sus actividades a nivel de título individual teniendo en cuenta que las pautas que se detallan también podrán aplicarse sobre los profesionales cuya actividad se desarrollen el marco de establecimientos sanitarios. Esta guía ha contribuido en el cumplimiento del principio de responsabilidad proactiva del Reglamento, donde se facilitan las directrices sobre las medidas que se deben aplicar y la garantía de derechos de los afectados, todo ello con las referencias específicas de las limitaciones que la normativa sanitaria atribuye. Además, en esta guía se realiza un análisis exhaustivo sobre cuáles son las bases jurídicas para el tratamiento de datos sanitarios diferenciando claramente aquellas que son específicas de los derechos de autonomía del paciente en contra de las que respecta a las de tratamiento de derechos personales todo ello, teniendo en cuenta que es uno de los puntos más relevantes dentro del desarrollo de esta guía.

La Guía para pacientes y usuarios de la sanidad tiene como finalidad ser de utilidad a todos los usuarios del sistema sanitario, facilitando a cada uno de ellos, los conocimientos necesarios en lo que respecta a los derechos dentro del marco del tratamiento de datos de carácter personal. Esta guía da respuesta a algunas de las preguntas que más preocupan a los usuarios de la sanidad española referidas al tratamiento de los datos. Esta guía ha servido como referencia para detallar

los derechos y obligaciones de pacientes y usuarios de la sanidad, en concreto a los derechos del marco legislativo del tratamiento de datos personales.

1.7.Marco legal

La Protección de Datos personales es considerada como derecho primordial de todas las personas, por tal afecta al derecho de control sobre uso de los datos personales, de forma que se preserve el respeto a la intimidad y al resto de derechos fundamentales y libertades públicas. La normativa más importante a tener en cuenta en la seguridad y tratamiento de los datos de las organizaciones se puede resumir en:

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD). Norma de carácter nacional.

Las normas de protección de datos exigen coherencia y uniformidad en la interpretación de las normas relativas al uso y tratamiento de datos por parte de los Estados miembros. La protección de datos se aplica a todos los datos relativos a una persona física identificada o a una persona identificable, quien, para ser identificada como tal, debe tener en cuenta los medios en los cuales exista una probabilidad de ser empleados por el DPD para llevar a cabo el proceso de identificar de forma directa o indirecta a una persona, a través de medios pertinentes para tal proceso.

- Reglamento (UE) 2016/679 del Parlamento Europeo y el 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. (RGPD). Norma de carácter europeo sobre la que se fundamenta la LOPDGDD.

Una normativa de privacidad específica que se debe conocer es el Reglamento General de Protección de Datos (RGPD) de la UE, que entró en vigor en 2018. Establece la privacidad de los datos para los ciudadanos de la UE (o los interesados), impone obligaciones a las organizaciones que procesan sus datos e impone severas sanciones por incumplimiento. La sanción por incumplimiento del RGPD puede ser de hasta 20 millones de euros o el 4 % de los ingresos totales, lo que sea mayor. El RGPD está dirigido a:

- Todas las organizaciones establecidas en la Unión Europea que procesan datos personales.

- Organizaciones establecidas fuera de la Unión Europea, si procesan los datos personales de personas dentro de la Unión Europea cuando les proporcionan bienes y servicios o controlan su comportamiento.

Sobre los flujos de datos transfronterizos: al coordinar las leyes de protección de datos en toda Europa, el RGPD facilita el libre flujo de datos personales dentro de la Unión Europea. La Unión Europea designa países «apropiados» como aquellos que brindan un nivel de protección de datos comparable al del RGPD. Esto permite que los datos personales se transfieran hacia y desde estos países sin restricciones adicionales. Se pueden utilizar varios mecanismos para permitir la transferencia de datos personales a países que no cuentan con leyes de protección de datos adecuadas. Estos incluyen, entre otros: cláusulas contractuales estándar (SCCs), reglas vinculantes de la empresa (BCR) y el marco de protección de la privacidad. A estas normas hay que añadir muchas otras derivadas de estas y que las complementan y profundizan en aspectos concretos. En el anexo se podrán encontrar artículos referenciados, leyes o normas que se citen en el trabajo.

A lo largo de este trabajo se van a nombrar reiteradamente estas dos directivas, destacar que comparten tantas similitudes que parece que llegan a ser paralelas. Para aclarar en que disciernen el siguiente cuadro sinóptico aclara las posibles dudas:

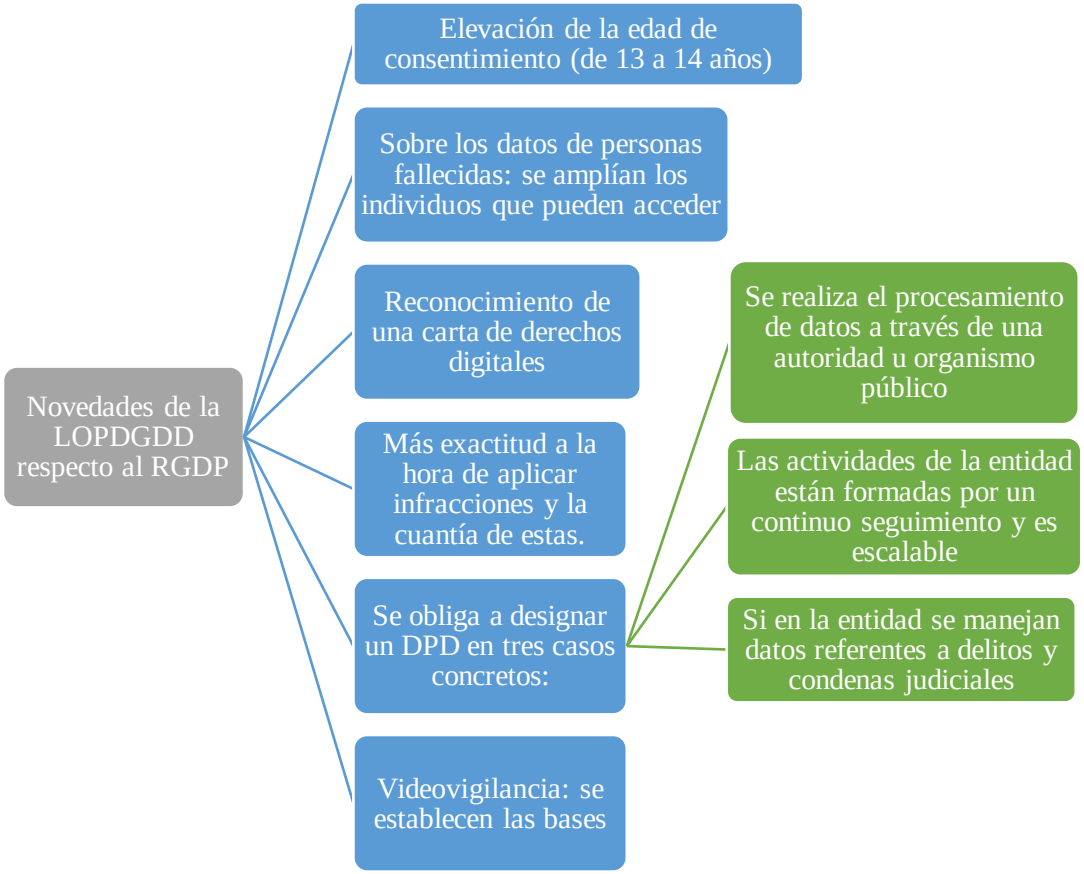


Ilustración 2. Novedades de la LOPDGDD respecto al RGPD. Fuente elaboración propia

Por otro lado, organizaciones como la AEPD proporcionan muchas pautas y documentos para los diferentes problemas y situaciones que puede encontrar una organización que tiene que tratar con datos. Además, a partir de la Asociación Española de Normalización se han creado numerosas entidades globales en el ámbito de la protección de datos y la ciberseguridad, siendo el único organismo de normalización en España.

- La Ley 14/1986, de 25 de abril, General de Sanidad. La cual instaura el Sistema Nacional de Salud mediante la integración de diversos subsistemas sanitarios públicos. Norma nacional.

Donde se destaca en el artículo 105 bis: «el tratamiento de datos personales en la investigación en salud se regirá por lo dispuesto en la Disposición adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales».

Respecto a las entidades responsables respecto a la protección de datos se categorizan según el nivel geográfico al que nos ciñamos:

- Comité europeo protección de datos – a nivel europeo [9].
- AEPD es el órgano de gobierno – a nivel nacional.
- Delegación de Protección de Datos GVA - a nivel regional (CCAA) [11].

2. ASPECTOS Y CONCEPTOS GENERALES

Cabe señalar que entre los pilares básicos de la protección de datos en el ámbito médico se encuentran el respeto a la confidencialidad de los datos médicos del paciente, la obtención del consentimiento del paciente o el tratamiento de los datos conforme al RGPD, la LOPDGDD y Ley de Autonomía del Paciente.

Se recomienda consultar la (Guía para profesionales del sector sanitario, AEPD)

2.1.Legitimación para el tratamiento de los datos

2.1.1. La confidencialidad con el paciente

Los hospitales y centros médicos deben respetar la ley de confidencialidad del paciente, es decir, lo estipulado en la ley 41/2002 de autonomía del paciente, la cual señala lo siguiente: los datos que se refieren a la salud de toda persona son de carácter confidencial, y sin autorización lícita previa expedida previamente nadie podrá acceder a estos. Es obligatorio cumplir el secreto profesional para aquellas personas que puedan acceder a los datos del paciente. Aún incluso cuando haya terminado la relación que vincule a los dos componentes. Los centros médicos deben adoptar ciertas medidas, según la ley de confidencialidad de los datos del paciente, las cuales son necesarias para garantizar la confidencialidad del procedimiento legal de acceso y los datos de salud relacionados.

2.1.2. El consentimiento del paciente

Según la ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, se argumenta que:

para que todo paciente pueda decidir libremente si va a seguir o no un procedimiento médico tiene el derecho de poder recibir toda la información sobre este. Asimismo, se realizará la formalización del consentimiento de forma escrita para que quede aprobado. La finalidad de esto es que los procedimientos médicos que se refieran a los pacientes sean delimitados por directrices relacionadas con la comprensión, participación voluntaria, y la información. Hay excepciones en las que el consentimiento no será necesario para aquellos casos en los que no se requiera el consentimiento del paciente para elaborar el diagnóstico médico, apoyo, medicina preventiva o evaluación de la competencia del personal. Tampoco cuando los datos se recopilan para el bien público, como para garantizar la calidad de la atención médica o para proteger contra amenazas graves a la salud pública.

2.1.3. El tratamiento de datos

Un centro de salud público o privado que atienda al paciente y tenga historia clínica actuará como observador. Están obligados a adoptar las medidas técnicas y organizativas necesarias para el correcto tratamiento y almacenamiento, y para evitar la pérdida de la información o su caída en manos de terceros no autorizados. El Reglamento General de Protección de Datos destaca un conjunto de principios que los encargados y responsables del tratamiento deben observar al tratar datos personales, se van a enfocar sus definiciones al ámbito destacado, el sanitario:

- «Principio de licitud, transparencia y lealtad».
- «Principio de responsabilidad activa o responsabilidad demostrada». Se protegerán los datos frente a la destrucción, pérdida o daño accidental.
- «Principio de exactitud» Los datos han de ser reales, exactos y estar actualizados.
- «Principio de finalidad»: limitación de la finalidad, significa que, se recogerán con fines detallados y concretos además de ser explícitos y no se usarán para otras finalidades posteriormente.
- «Principio de minimización de los datos». Se limitará el uso de los datos del paciente a aquellos que sean pertinentes, adecuados y limitados a las necesidades para el cumplimiento del objetivo.
- «Principio de limitación del plazo de conservación», al cumplimiento del fin para el que fueron captados.
- «Principio de seguridad», se obliga al responsable del tratamiento de datos a determinar las medidas organizativas y técnicas necesarias para garantizar tanto la disponibilidad

como la integridad y además la confidencialidad de los datos personales que se vayan a tratar [1].

2.1.4. Informar al cliente sobre sus datos

Según los artículos 13 y 14 del RGPD, se describe el deber de informar ya que uno de los requisitos para la protección de datos médicos es la provisión de información completa al paciente. Más concretamente, cualquier centro médico debe informar a sus pacientes de lo siguiente:

- Cómo ejercer los derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición.
- Identidad del responsable del tratamiento o sus representantes.
- Finalidad y base jurídica del tratamiento.
- Destinatarios de los datos.
- Datos de contacto del DPD (si hubiese).
- La cesión de los datos a terceros países u organizaciones internacionales.
- Plazo de conservación de los datos. Solo se han de guardar el tiempo necesario para garantizar la correcta asistencia de los pacientes, un mínimo de cinco años.
- Derecho a presentar una reclamación ante la autoridad de control (Agencia Española de Protección de Datos).
- Derecho a revocar el consentimiento.

2.2.Clasificación de la información

Remarcar que es de importancia la manutención de la disponibilidad, integridad y protección de la información personal de los individuos y de la información confidencial para nuestra organización o entidad. Para llevarla a cabo, nos enfocamos en distintas actividades en el tratamiento de datos, entre las que se incluyen la recopilación, el almacenamiento, la divulgación, la transferencia y la eliminación de datos, tanto en formato electrónico como en papel. Se debe tener en cuenta que en algún caso las distintas categorías se pueden solapar. Por ejemplo:

- Los datos sobre un cliente o empleado específico puede ser información confidencial pero también personal.

- La información de acceso público que reconoce e identifica a una persona también puede considerarse información personal.

> Se recomienda consultar el documento (Introducción al Hash como técnica de seudonimización de datos personales, AEPD)

2.2.1. Información personal

Su objetivo principal es la identificación de una persona de manera inequívoca. Se debe tener en cuenta que dependiendo de la jurisdicción y el sector las definiciones exactas pueden variar, pero en términos generales la información personal (IP) se puede usar por sí sola o en combinación con otros datos para cumplir su objetivo. Se recalca que esto puedo incluir información relacionado con las personas a título personal y profesional. Se añade que la información personal (IP) hace referencia como información de identificación personal (IIP) o datos personales. Los ejemplos más comunes de este tipo de datos son:

- Nombre
- Fecha de nacimiento
- Dirección postal
- Dirección de correo electrónico
- Número de teléfono

La IP abarca otro tipo de datos en los que en un principio no se suele tener en cuenta, tales como:

- Nombre de usuario en inicio de sesión
- Información de internet (incluyendo historiales de búsqueda y navegación)
- Datos de geolocalización

Algunos tipos de IP son considerados más sensibles que otros y necesitan un tratamiento especial ya que están expuestos a un mayor riesgo, que en caso de divulgación puede provocar daños, causar inconvenientes, avergonzar o incluso dar lugar a un tratamiento injusto hacia una persona. Estos son algunos ejemplos de información personal sensible:

- Números de tarjetas de crédito, cuentas bancarias u otras cuentas

- Números de identificación emitidos por las administraciones (por ejemplo, número de pasaporte o número de carné de conducir)
- Información médica y sanitaria (incluidos los diagnósticos, resultados de análisis y medicamentos)
- Datos biométricos (incluidos los datos relacionados con la tecnología de reconocimiento facial, las huellas digitales, las grabaciones de voz y la información de ADN).

2.2.2. Información confidencial

La información confidencial son datos sobre la entidad u organización y sus operaciones, incluidos los productos de trabajo, secretos comerciales y todo relacionado con la propiedad intelectual que no debe hacerse pública.

2.2.3. Información pública

La información pública es cualquier dato que se encuentre disponible en foros públicos:

- Contenido publicado en sitios web públicos
- Registros públicos de la administración pública
- Información de contacto corporativa pública
- Información incluida en medios de comunicación de amplia difusión (por ejemplo, comunicados de prensa o comunicaciones de inversores)

Si en algún caso la información pública identifica a una persona de manera inequívoca, se recomienda tomar precauciones adicionales antes de usarla o compartirla.

2.2.4. RGPD Clasificación de la información

Reconocimiento de la información personal, según el RGPD se considerará información personal aquella información personal que se haya hecho pública y se deberá proteger y tratar siguiendo el reglamento. Manejo de información personal sensible, el RGPD identifica categorías especiales de datos personales que incluyen información sobre el origen racial o étnico, las opiniones políticas y las convicciones religiosas o filosóficas, la afiliación sindical, los datos genéticos, biométricos y los relativos a la salud, a la vida sexual o a la orientación sexual de la persona. Como síntesis, la información personal es aquella que sirve para reconocer o identificar de manera unívoca incluyendo los datos de carácter personal, aunque en el RGPD se contemplan definiciones distintas para según qué datos personales sean los de los afectados. La información

confidencial son aquellos datos que no deben hacerse públicos y la información pública es aquella que es visible y accesible en foros públicos ya sea una página web, la tarjeta de visita o en formato documento.

Se recomienda consultar el documento (14 equívocos con relación a la identificación y autenticación biométrica, AEPD)

2.3.Historia clínica

La información relacionada con temas de salud, cómo, por ejemplo, la historia clínica, se considera datos sensibles, en consecuencia, tienen sus propias normas de protección. En general, los centros médicos como hospitales, clínicas o ambulatorios están obligados a seguir ciertas normas especiales respecto al tratamiento de los datos médicos de sus pacientes. Existen dos tipos de datos en las bases de datos sanitarias:

- Datos identificativos: nombre, apellidos, DNI, dirección, número de la tarjeta sanitaria.
- Datos relacionados con la salud: operaciones, antecedentes familiares, alergias, tratamientos, diagnósticos, medicamentos, etc.

El conjunto de estas dos categorías forma la historia clínica. La primera vez que una persona acude a un centro de atención sanitaria o un hospital para realizarse un diagnóstico de salud o tratar alguna enfermedad, se crea la historia clínica. Este documento médico se califica como documento legal ya que va a recoger toda la información relativa a los tratamientos o a la salud del paciente, es el documento que surge de la relación entre médico y paciente, cuyo objetivo principal es que el paciente a lo largo de su vida pueda recibir una atención adaptada y personalizada a su estado de salud. A continuación, queda detallada más información que tiene relación con el paciente, recogida en la historia clínica:

- Registros de alta e ingresos
- Evolución del estado del paciente
- Interconsultas
- Antecedentes familiares
- Tratamientos
- Órdenes médicas
- Tratamientos terapéuticos

- Informes de evolución del parto
- Exploraciones complementarias
- Cuidados de enfermería
- Informes de quirófano
- Exploraciones físicas
- Informes sobre anatomía, anestesias y urgencia
- Hoja clínico-estadística

Según la Guía para profesionales del sector sanitario elaborada por la AEPD:

> «El paciente tiene derecho a conocer los accesos que se han producido a su historia clínica (cuántos accesos, finalidad del acceso, etc.) Pero, hoy en día, ni la normativa sobre protección de datos, ni la normativa estatal sanitaria reconocen expresamente que este derecho incluya la identificación (nombre y apellidos) de los profesionales que han accedido a la historia clínica de un paciente (aunque podrían conocerse estos datos a propósito de una investigación judicial en curso por sospecha de acceso indebido). No obstante, algunas normas autonómicas sí reconocen la posibilidad de conocer la identidad de quién ha accedido, como Navarra y Extremadura, en cuyo caso el paciente podrá también solicitar estos datos cuando ejercite su derecho de acceso. En cualquier caso, la administración o centro sanitario tiene la obligación de implantar las medidas de seguridad necesarias para controlar y, en su caso impedir, el acceso por a la historia clínica por parte de personas no autorizadas.»

El acceso a la historia clínica del paciente está exclusivamente limitado al personal médico encargado del tratamiento del paciente. Por tanto, ninguna otra persona, aunque se trate de familiares o se actúe de buena fe, podrán acceder a ella.

Se recomienda consultar la (Guía para pacientes y usuarios de la Sanidad, AEPD)

3. DESARROLLO DE LA GUÍA

3.1.Obligaciones en el tratamiento de datos

Los centros sanitarios deben cumplir los siguientes puntos recogidos en la normativa de protección de datos sanitarios:

Ilustración 3. Puntos importantes para el desarrollo de la guía. Fuente: elaboración propia

> Se recomienda consultar la guía sobre (La protección de datos en las relaciones laborales, AEPD)

3.1.1. Generar y recopilar la documentación necesaria:

- Certificado de cumplimiento normativo RGPD UE 2016/679.
- Acuerdos de confidencialidad con todo aquel que tenga autorización para acceder a los datos personales.
- En relación con el artículo 28 RGPD UE 2016/679 se redactan los contratos con los encargados de tratamiento (CET).

- En cuanto a los formularios de recogida de datos en formato papel se redactan las cláusulas informativas (CI).
- Creación de los documentos del Registro de Actividades de Tratamiento (RAT), con su posterior generación en la cual quedan recogidos el Plan de Acción y las Medidas de Seguridad (PAMS).
- Por último, una evaluación sobre los Análisis de Riesgos (AR) y elaborar un informe ejecutivo del resumen de riesgos detectados, interpretación de datos y activos afectados [12].

Se recomienda consultar la herramienta (Evalúa-Riesgo RGDP, AEPD)

3.1.2. Designar a las figuras profesionales

Según el Dictamen 1/2010 sobre los conceptos de responsable del tratamiento y encargado del tratamiento, adoptado el 16 de febrero de 2010, la definición de estos es la siguiente:

- Responsable del tratamiento: «persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que solo o conjuntamente con otros, determine los fines y los medios del tratamiento de datos personales». A continuación, se detalla más sobre esta figura.
- Encargado del tratamiento: «persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que evita situaciones en las que el tratamiento por terceros por cuenta del responsable del tratamiento del fichero tenga el efecto de reducir el nivel de protección del que goza el interesado».

Responsable del tratamiento

Es la figura que tiene como obligaciones desde elaborar la historia hasta la de tomar las medidas de seguridad necesarias para que su confidencialidad y disponibilidad no estén expuestas a ningún riesgo, todo ello sin olvidar la custodia de esta como una de sus obligaciones. El RGPD determina que es el centro sanitario (privado o público) o el médico quien queda como responsable del tratamiento de la información personal que forma parte de la historia clínica. En concreto, cuando el médico desarrolle su tarea como profesional individual será cuando ejerza de responsable, por ejemplo, una consulta privada.

Según el artículo 34 del RGPD, responsabilidad del responsable de tratamiento, se declara que:

> «teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos».

Encargado del tratamiento

Cómo hemos mencionado anteriormente el encargado de tratamiento es una figura independiente del responsable del tratamiento. Según la AEPD:

> «el encargado puede realizar todos los tratamientos, automatizados o no, que el responsable del tratamiento le haya encomendado formalmente. La definición de tratamiento nos permite concretarlos atendiendo al ciclo de vida de la información: recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción. En todo caso, deben quedar claramente delimitados en el acuerdo que se adopte».

El Considerando 81 del RGPD prevé que el encargado del tratamiento debe ofrecer suficientes garantías en lo referente a conocimientos especializados, fiabilidad y recursos, con vistas a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del Reglamento, incluida la seguridad del tratamiento. Según la AEPD:

> «el encargado del tratamiento puede adoptar todas las decisiones organizativas y operacionales necesarias para la prestación del servicio que tenga contratado. En ningún caso puede variar las finalidades y los usos de los datos ni los puede utilizar para sus propias finalidades. Las decisiones que adopte deben respetar en todo caso las instrucciones dadas por el responsable del tratamiento».

Delegado de Protección de Datos

Según el artículo 34 de la Ley Orgánica 3/2018, de 5 de diciembre:

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

en la que se destaca:

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

Asimismo, según el artículo 36 de la Ley Orgánica 3/2018, de 5 de diciembre, destacando los puntos 1 y 3, (en el anexo se puede encontrar más detalladamente el capítulo al que se refiere esta ley):

> «1. El delegado de protección de datos actuará como interlocutor del responsable o encargado del tratamiento ante la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos. El delegado podrá inspeccionar los procedimientos relacionados con el objeto de la presente ley orgánica y emitir recomendaciones en el ámbito de sus competencias».
>
> «En el ejercicio de sus funciones el delegado de protección de datos tendrá acceso a los datos personales y procesos de tratamiento, no pudiendo oponer a este acceso el responsable o el encargado del tratamiento la existencia de cualquier deber de confidencialidad o secreto, incluyendo el previsto en el artículo 5 de esta ley orgánica».

Con esta información quedan destacadas las siguientes funciones del delegado de protección de datos:

- Asesorar e informar al responsable de datos y aquellos empleados que tengan relación con el tratamiento de datos de sus obligaciones legales:
  - Orientación y resolución de dudas
  - Educación y formación
- Supervisión de la asignación de responsabilidades, así como del cumplimiento de las leyes aplicables, además de la formación del personal en temas de auditoría y protección de datos.
- Cooperación con la AEPD (autoridad de control), ya que este actúa como representante.
- En lo que respecta a la protección de datos, ofrecer asesoramiento.

- Punto de encuentro entre la empresa y la autoridad.

> Se recomienda consultar la guía sobre (Tecnologías y Protección de Datos en las Administraciones Públicas, AEPD)

En la imagen inferior, se clarifica a modo de resumen las principales funciones de cada figura involucrada en el tratamiento.

Ilustración 4. Diferencias entre las figuras responsables. Fuente: (Conversia, 2017) [4]

Respecto a la designación del DPD

Atendiendo al artículo 37.1.c del RGPD donde se argumenta que todo aquel responsable o encargado que vaya a realizar un tratamiento de datos sensibles tiene la obligación de designar a un DPD. Los datos y el nombramiento del DPD deben hacerse de manera pública además de ser comunicados a las autoridades responsables de supervisión, como marca el RGPD. Se destaca que la figura del DPD la podrá representar una persona perteneciente a la plantilla de la empresa o en otro caso, se podría contratar de forma externa a la organización o empresa que tenga en sus

ofertas dicho servicio. El DPD involucrado en una organización de sanidad, respecto al volumen de datos que trata, va a ser el profesional, que tras la formación y cualificación necesaria en esta materia que consiste en la supervisión del cumplimento de la ley en las políticas y los procesos internos del tratamiento de datos sensibles, tome el cargo de responsabilidad en la entidad. Por último, se añade que la LOPDGDD indica que no será necesario la figura del DPD en las clínicas privadas donde los profesionales sanitarios desarrollen su profesión de manera individual.

Se recomienda consultar la herramienta (Canal del DPD, AEPD)

3.1.3. Registro de actividades de tratamiento

El responsable ha de mantener un registro en el que se almacene de cada uno de los registros la elaboración del análisis de datos previo, ya que para cumplir con la protección de datos sanitarios en el hospital o clínica se deberá responder a una serie de información que queda detallada en el artículo 30 del RGPD. Se podría sintetizar dicha información de la siguiente manera:

- Entidad responsable
- Tipos de datos que se recopilan.
- Objetivos del tratamiento.
- Política de almacenamiento de dichos datos.
- Si se ceden los datos o se transfieren a otros países.
- Cuáles van a ser los medios de tratamiento.
- Responsable y delegado de protección de datos.
- Los plazos previstos para la eliminación de según que categorías de datos.
- Una descripción de las medidas organizativas y técnicas de seguridad y privacidad.

El RAT ha de constar por escrito y, en su caso, en soporte electrónico, y estará a disposición de la Agencia de Protección de Datos o, si el responsable fuera una entidad pública, de la autoridad de control competente. Sin embargo, en el caso de las entidades públicas el inventario (art.31 LOPDGDD) con los tratamientos de datos personales deberá hacerse público y estar accesible por medios electrónicos (por ej., a través de la respectiva página web).

Por ejemplo, se podría aplicar para gestionar los comunicados y publicación de notas de prensa además de noticias y eventos en redes sociales de un hospital concreto. Para el cual se deberá

identificar la fecha de creación de este, las posibles modificaciones del registro, además de asignársele un nombre a este (por ejemplo: comunicación y prensa), que describirá de forma resumida de que se trata. Se podría detallar un poco más las diferentes actividades que engloba este tratamiento. Por ejemplo, la publicación de noticias y eventos en redes también sería una actividad de tratamiento.

A continuación, se introducirá la categoría de datos personales que se van a tratar además del tiempo mínimo de conservación de los datos. Refiriéndonos a este tratamiento incluiría: imagen y/o voz, nombre y apellidos, teléfonos, dirección postal, DNI u otro documento identificativo, identidad electrónica. En cuanto al tiempo mínimo de conservación de los datos hay que añadir que sería para un periodo indeterminado ya que se mantendrían los datos durante el tiempo necesario para cumplir con el objetivo para el cual se obtuvieron. En el siguiente apartado, se incluirá la categoría de titulares de los datos, es decir, quienes son los interesados o afectados. Para este caso serían los trabajadores, autores y titulares de artículos, pacientes y ciudadanos. Se recalca que la licitud del tratamiento quedará representada por el art. 6.1 a) RGPD el cual argumenta que el interesado da su consentimiento para el tratamiento de su información personal. Por último, se procederá a registrar la información necesaria que requiera las medidas de seguridad, englobaría tanto las organizativas como las técnicas que realice el hospital para la protección de los datos. En concreto, las medidas de seguridad de nuestro caso quedan recogidas en el Real decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.

3.1.4. Evaluación de impacto en protección de datos personales

Una EIPD (Evaluación de Impacto de Protección de Datos) es una evaluación de impacto que tiene relación con la privacidad, su finalidad es la identificación y el análisis de determinadas consecuencias que ciertas actividades o acciones pueden afectar a la privacidad. Estas evaluaciones determinan el nivel de riesgo que un tratamiento puede causar en las libertades y derechos de los afectados, asimismo permiten la identificación de riesgos y amenazas potenciales y la evaluación tanto del impacto como de la posibilidad de que se produzcan sobre la vida de los titulares de la información. La evaluación de impacto es un proceso totalmente documentado donde la AEPD recoge los procedimientos establecidos para evaluar qué consecuencias puede tener para los derechos y libertades de los pacientes involucrados en el tratamiento de su información personal.

Dicho procedimiento debe quedar documentado, su revisión debe ser de forma periódica y deberá recoger todo el ciclo de vida del dato, desde la recogida de datos del paciente hasta la eliminación, pasando por el proceso de tratamiento y su posible almacenamiento.

Las empresas que deberían realizar dicho procedimiento son aquellas que elaboren perfiles, y en base a estos posteriormente se produzcan tratamientos jurídicos hacia las personas físicas o de alguna manera les afecten significativamente, se incluyen también las organizaciones o entidades que traten categorías especiales de datos o información personal relativa a infracciones penales y condenas. Finalmente, aquellas empresas que mantengan observada una zona de acceso público de forma sistemática a gran escala. Los responsables de protección de datos destacan que para evaluar si alguna directiva del tratamiento podría ocasionar una situación restrictiva sobre algún derecho fundamental, dicha directiva u operación debería pasar los tres puntos del juicio de proporcionalidad:

- Juicio de proporcionalidad: si hablamos de una medida equilibrada y ponderada, se deben ocasionar más ventajas o beneficios sobre el interés general que no perjuicios sobre valores u otros bienes en conflicto.
- Juicio de idoneidad: la medida obtiene la finalidad propuesta.
- Juicio de necesidad: si fuese necesario, es decir, en el sentido de que no cupiese la posibilidad de conseguir otra más moderada con el fin de obtener el propósito esperado con la misma eficacia, que no incluye la eficiencia.

En este apartado, se destacarán, distintos artículos del RGPD relacionados con la EIPD:

- Artículo 35 Evaluación de impacto relativa a la protección de datos, en concreto el punto 5 se refiere a las cualidades profesionales que recaen sobre el DPD en este tipo de evaluaciones.
- Artículo 35. 7 describe cual sería la cantidad mínima de contenido válida para realizar una evaluación de forma adecuada
- Artículo 39.1 que recoge las funciones del delegado de protección de datos para este tipo de procedimientos

Pasos necesarios para realizar una EIPD:

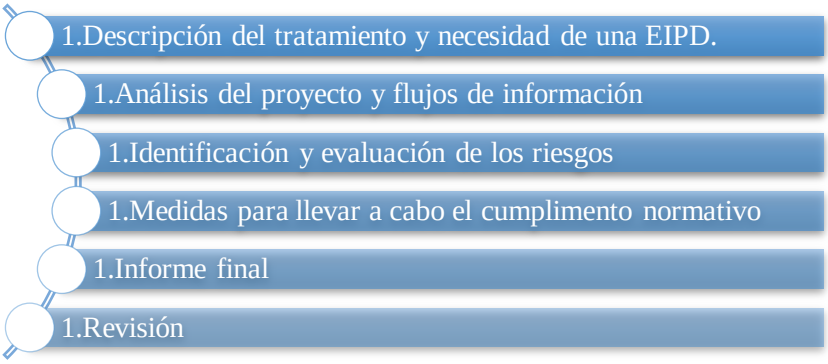


Ilustración 5. Fases para realizar EIPD. Fuente: elaboración propia

Algunos ejemplos de empresas obligadas a llevar a cabo una EIPD son: aquellas que su actividad esté relacionada con el comercio electrónico, colegios, farmacéuticas, las involucradas en vigilancia y control, comercializadoras de energía, actividades relacionadas con la seguridad privada y hospitales y clínicas. Para este caso, los hospitales o clínicas habrán de realizar una EIPD para reducir las posibles afectaciones sobre las libertades o derechos de los afectados, ya que se tratan categorías especiales de datos (información sobre la salud de los pacientes) y posteriormente, se deberán implementar las adecuadas restricciones en ámbito de seguridad. Por último, se añade que dicha EIPD no será un requisito necesario en caso de que lo realizase un profesional de la salud, (por ejemplo, un médico), considerando que no sería un tratamiento realizado a gran escala.

Se recomienda consultar la herramienta (GESTIONA EIPD, AEPD)

3.1.5. Análisis de riesgos

Previamente a realizar un tratamiento de datos personales, es conveniente y necesario realizar un AR (Análisis de Riesgos) ya que es el paso primordial en el proceso de la protección de datos. Esto permitirá identificar las posibles amenazas que podrían producirse debido a dicho tratamiento y además poder determinar el nivel de riesgo si se llegan a materializar sobre las libertades y los derechos de los afectados. Para llevar a cabo una gestión de riesgos de forma adecuada es obligatorio desarrollar un proceso extenso y laborioso de identificación, evaluación y tratamiento de los posibles riesgos derivados de alguna de las actividades que formen el tratamiento. Finalmente, se destaca que para la correcta evaluación de un riesgo sería necesario

la consideración de todos los escenarios en los que el riesgo sería clave o efectivo. Se incluyen los que implican un abuso o mal uso de la información y las alteraciones del entorno y técnicas. En resumen, el nivel de riesgo se medirá en función de la probabilidad de materialización y el impacto que se obtendría en caso de hacerlo. A continuación, algunos ejemplos de riesgos para la protección de datos:

- La cesión de información a otra organización o entidad.
- Emplear sistemas de videovigilancia.
- Los incidentes no previstos (cortes de suministro eléctrico, incendios…). Aquellos que puedan destruir los soportes en los que quedan almacenados los datos o en general los equipos.
- Crear un nuevo tratamiento de datos personales (formulario de suscripción a un canal o de contacto).
- La utilización de una base de datos en la nube para almacenar los datos personales.

Se destaca de entre la normativa aplicable al análisis de riesgos en la protección de datos, el artículo 25 del RGPD «Protección de datos desde el diseño y por defecto», los tres puntos descritos. Es de vital importancia que, de acuerdo con el RGPD, el AR lo lleve a cabo el DPD en caso de que hubiese, en las entidades obligadas a ello. Para el caso de no exista esta figura, la organización tiene como deber el nombramiento de un responsable para llevar a cabo esta tarea, que se podrá realizar con otro responsable o encargado de la entidad, por ejemplo, el personal del departamento TIC. Para cualquier de estos casos nombrados anteriormente, se requieren tener conocimientos en la materia de protección de datos y seguridad de la información.

Quedan identificadas **siete** fases para realizar un AR según el RGPD:

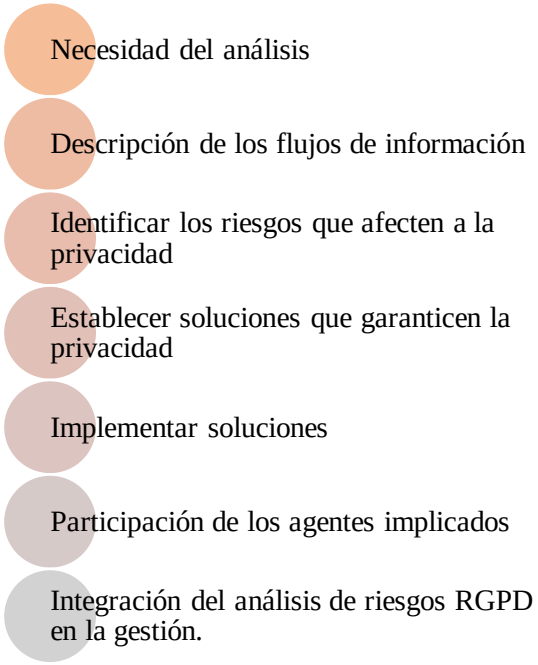


Ilustración 6. Fases para realizar un AR. Fuente: elaboración propia

Para la primera parte, se deben realizar las siguientes preguntas sobre los distintos tratamientos de datos que se vayan a hacer:

- ¿Los datos obtenidos pertenecen a la categoría personal?
- ¿Son tratados datos que pertenecen a categorías especiales?
- ¿Los datos personales serán comunicados a terceros?
- ¿La tecnología invasiva es empleada para la privacidad en el tratamiento?
- ¿Se utilizarán aquellos datos personales obtenidos para obtener acciones de marketing?

En cuanto al tipo de tratamiento:

- ¿Dónde se van a almacenar los datos?
- ¿Cuánto tiempo va a ser?
- ¿En una base de datos o en un documento?
- ¿Cuáles van a ser los equipos?

Para la clasificación de la naturaleza de los datos, se separarán entre:

- Identificativos
- Bancarios
- De salud

Tener en cuenta cual será el número de interesados afectados

- 2.000
- 6.000
- 50.000…

Si fuese el caso de que en alguna de las preguntas anteriores la respuesta es afirmativa, se deberá realizar el AR del tratamiento de datos personales. La segunda fase es ser consciente de todo lo que tiene relación con el tratamiento de los datos personales, es decir:

a. Cómo se van a recopilar
b. Con qué finalidad se van a utilizar
c. Cuál es su objetivo
d. Cuáles son las personas que tendrán acceso a los datos
e. Cuál será el tiempo mínimo que se van a almacenar

En la tercera fase se identificarán los riesgos que afecten a la privacidad y se clasificarán según su categoría:

1. Para la confidencialidad
2. Para la integridad
3. Para la disponibilidad

En la cuarta fase, se establecen las posibles soluciones que garanticen la privacidad, en esta fase se recuerda que la realización de un AR no elimina completamente los riesgos, aunque irregularmente pueda ocurrir el caso de que sí los elimine. El objetivo es reducirlos a un nivel adecuado para permitir a la entidad u organización la implementación del servicio, producto o tratamiento de datos personales. Teniendo en cuenta que se debe valorar el beneficio y coste de desarrollar estas soluciones. Se aconseja realizar una comparativa entre costes y beneficios. En la quinta fase se lleva a cabo la implementación de soluciones donde es importante que quede registrado todos y cada uno de los riesgos y de las posibles soluciones que se van a adoptar. También quedan registrados los responsables de arrancarlas y ponerlas en funcionamiento. Para la penúltima fase, se describe y detalla la participación de los agentes implicados, ya que, es necesario que en las fases ya descritas la información fluya entre los diferentes agentes implicados y departamentos. Con el objetivo de obtener, a través de la colaboración entre estos, un completo y absoluto análisis de los tratamientos de datos en materia de carácter personal. La última fase consiste en la integración del AR en la gestión. Es decir que el análisis forme parte de la gestión de la organización o entidad responsable. Así, se conseguirá garantizar de forma segura la

privacidad de servicios y productos. Se destaca que la AEPD facilita una plantilla como ejemplo de AR para la documentación de un AR nivel básico.

Diferencia entre un EIPD y un AR: se aclara que son procedimientos complementarios a la vez que diferentes.

Objetivos del AR:

- Tras una amenaza cuantificar la pérdida de potencial
- Justificar el costo de la solución (la implementación de directrices para la protección de la información personal de la entidad u organización)

En un principio se necesitaría saber cuáles serían los recursos y procesos críticos objeto de análisis, para poder estimar el gasto en la futura protección y prevención.

Objetivos de EIPD:

- Prevenir cual sería los resultados obtenidos de un evento no previsto sobre la información personal de la entidad.
- Objetos de estudio: los afectados, la infraestructura física, la información, la tecnología y los terceros involucrados.

En general el AR acota los eventos previstos, pudiendo así realizar un análisis previo de los objetos afectados sobre dichas amenazas:

- Controles de seguridad lógica, ambiental y física.
- Evaluando cual es el grado de efectividad para la contención de aquellas amenazas implicadas.

En cambio, en la EIPD quedan detallados los riesgos que un producto, servicio o sistema pueda interrumpir en el respeto hacia las libertades y derechos de los afectados. Después de dicho análisis se podrían controlar esos peligros previos a su ocurrencia.

En el RGPD se detalla cuando sería conveniente realizar una EIPD que complemente el AR en los artículos 35.3, 35.4 y 35.5. Asimismo, en el artículo 35.1 del RGPD se detalla cuáles son las condiciones para que sea de obligación realizar una EIPD.

3.1.6. Medidas de seguridad

Tras realizar los análisis mencionados anteriormente es de importancia que se apliquen altas medidas de seguridad para intentar paliar los ataques informáticos actuales. Una medida sería

limitar el acceso a datos críticos. En la antigua LOPD se detallaban las medidas de seguridad que un hospital debía adoptar para la correcta protección de los datos de sus pacientes, actualmente el RGPD no determina exactamente cuáles son las medidas de seguridad que se tienen que seguir. Se especifica que el primer paso sería realizar un AR para conocer y evaluar los tipos de riesgos a los que los datos personales pueden estar expuestos y además contar con la posibilidad de desarrollar un plan de acción el cual contenga medidas reguladas y detalladas utilizando la tecnología necesaria para proteger los datos.

Hay que destacar que el cumplimiento de las medidas de seguridad es uno de los temas por lo que los centros hospitalarios han sido sancionados la mayoría de las veces. Es necesario destinar esfuerzo para el correcto desarrollo de un buen sistema de gestión hospitalario (HIS) el cual tiene que garantizar que se cumplan los requisitos indispensables y básicos con lo que respecta a la seguridad de la información (registros de accesos, contraseñas robustas, cambios de contraseña periódicos…) También es necesario que se tengan en cuenta ciertas acciones las cuales no son tan notorias, pero tienen cierta importancia, como pueden ser: la correcta formación del personal o la correcta gestión de archivos en papel. Detallar que sería recomendable que los cambios de contraseña al menos se realizasen una vez al año, y que las mismas contraseñas no sean obvias, es decir: «1234abc», «EnfermeraMaria», etc. El sistema de permisos de acceso es el encargado de recopilar los roles, grupos y permisos por lo que es una herramienta crítica. El HIS debe recoger cada acceso al historial del paciente, quedando detallado cuales han sido las acciones realizadas sobre este: modificaciones, borrados, adiciones, o simplemente quien ha sido el visor. Y finalmente, habría que tener especial cuidado en situaciones de traslados de historiales o procesos de destrucción ya que son acontecimientos que pueden provocar accidentes graves.

Ilustración 7. Medidas de seguridad básicas. Fuente: elaboración propia

3.1.7. Brechas de seguridad

Una brecha de seguridad es la acción cuyo resultado es el acceso no autorizado a datos de aplicaciones, redes, ordenadores o dispositivos. Suele pasar cuando un no autorizado no tiene en cuenta los mecanismos de seguridad, por lo que acaba accediendo a información sin autorización. Es de especial importancia conocer las diferencias entre la definición de violación de seguridad y la de un incidente de seguridad. Un ataque DDoS[2], una infección del *malware* o simplemente un empleado que se olvida de un portátil en un bus puede involucrar un incidente, no se calificarían como una violación de seguridad si no acceden a la red o causan una pérdida de datos. En el caso de que un incidente de seguridad provoque el acceso a sistemas con protección se consideraría como violación de seguridad. Para el caso de que sea una violación de datos, el atacante dispondrá acceso a datos confidenciales. En función de los datos y de las consecuencias o de los objetivos las brechas de seguridad pueden clasificarse en tres tipos distintos, teniendo en cuenta que pueden haber sido causado tanto por un ataque premeditado como uno que no:

- Brecha de integridad: cuando la información original o los datos son modificados en el sistema, dicha acción puede causar inconvenientes a la entidad además de los afectados.

[2] Definición en el GLOSARIO

- Brecha de confidencialidad: ocurre cuando un descuido o un ataque puede facilitar datos no autorizados.
- Brecha de disponibilidad: un incidente provocado o no, cuyas consecuencias son la pérdida de información almacenada, ya sea de forma temporal o permanentemente.

¿Cómo se gestiona una brecha de seguridad?

1. Encontrar e identificar
2. Clasificación: nombrada anteriormente
3. Elaborar el plan de contingencia para paliar sus consecuencias.
4. Contención: la aplicación de los siguientes ejemplos muestra una actitud proactiva con lo que se refiere a las brechas de seguridad:
    a. Restringir el acceso a la red
    b. Deshabilitar usuarios con permisos comprometidos y actualizar las contraseñas
    c. Los parches como método temporal para resolver los errores y vulnerabilidades.
    d. Las aplicaciones críticas y sistemas se deben poner en cuarentena o directamente apagarlos.
5. Tras la aplicar la solución se tendrá la información para resolver las siguientes preguntas:
    a. Tiempo durante el cual la violación estuvo activa.
    b. Qué datos han sido modificados, dañados o revelados.
    c. Cuál ha sido el impacto.
    d. Qué terceros se han visto involucrados.
6. Recuperación: incluye las fases de parcheo de sistemas, configurar correctamente los permisos y reconstrucción de sistemas para que no vuelva a suceder el mismo problema.
7. Comunicación: es la parte la cual se debe redactar un informe posterior al incidente con la información actualizada la cual detalle la raíz del problema y como se ha desarrollado la respuesta hacia el incidente.

¿Cómo notificar la brecha de seguridad?

En el artículo 33 del RGPD «Notificación de una violación de datos personales a la autoridad supervisora», desarrolla cómo sería el procedimiento adecuado para notificar una violación de datos. Señala que «la persona física o moral, autoridad pública, dependencia u otro organismo que solo, o en conjunto con otros, determina la finalidad y los medios para procesar los datos personales», es decir el responsable del tratamiento, será el encargado de notificar las brechas de seguridad.

El procedimiento de notificación se podría resumir de la siguiente manera:

- Valoración de riesgo: es la acción a través de la cual se determina el nivel de riesgo que pueden afectar a las libertades y los derechos de los afectados que pueden sufrir brechas de seguridad informática.
- Daños de software o hardware: detecta los posibles daños que puede sufrir la empresa tras la amenaza, también se puede hablar de daños materiales o inmateriales.
- Alcance: las distintas operativas donde las consecuencias se pueden ver reflejadas.
- Contenido mínimo que debe incluir la notificación a la AEPD:
    - El alcance y la naturaleza en la cantidad de interesados, de registros y de categorías de datos involucrados en la quiebra de datos.
    - Cuál va a ser la respuesta de la empresa para solucionar el incidente y que los interesados verifiquen las limitaciones impuestas.
    - Consecuencias tras producirse la violación.
    - Identificación del DPD con sus respectivos datos de contacto. O en otro caso, los datos de otro punto de contacto.

72 horas es el plazo en el cual, si las organizaciones no comunican que han sufrido una violación de los datos, aunque puedan explicar los motivos de la tardanza, se siguen exponiendo a las posibles sanciones y/o multas.

Se recomienda consultar la (Guía para la notificación de brechas de datos personales, AEPD)

Se recomienda consultar la herramienta (Asesora-Brecha RGPD, AEPD)

Se recomienda consultar la herramienta (Comunica-Brecha RGPD, AEPD)

3.2. Protocolo en la protección de datos para el personal empleado

3.2.1. Contratos con empleados

Los empleados además de tener la obligación de seguir las medidas de seguridad para que se cumpla reglamentariamente la protección de datos sobre los datos personales, al tener acceso a toda la información que contiene y administra la entidad, es necesario que firmen un contrato de confidencialidad para contener que dicha información privada pueda ser revelada a personas no autorizadas.

En las organizaciones sanitarias, clínicas y hospitales normalmente se tiene acceso a un correo electrónico interno el cual posibilita la comunicación entre los empleados internos de la entidad. Asimismo, también serviría para comunicarse con proveedores y pacientes. Por lo que les convierte en objetivos de los posibles atacantes, porque las amenazas como el *phishing*[3] y la ingeniería social son las tácticas de ataque más usadas en los últimos años teniendo en cuenta el éxito que conlleva para los *crackers*[4].

Por ejemplo, una de las últimas noticias respecto a ciberataques que hayan afectado a datos sanitarios españoles es «Ciberataque masivo contra el CSIC: el instituto de investigación se defiende de un *ransomware*[5]». Donde se comunica cómo el ciberataque masivo ha encriptado de una forma muy compleja por una parte la información que se almacena en la sede central y por otra parte cierta información de algunos centros repartidos por el territorio español [14].

3.2.2. Confidencialidad de los empleados

La Orden SSI/81/2017, de 19 de enero, por la que se publica el «Acuerdo de la Comisión de Recursos Humanos del Sistema Nacional de Salud, por el que se aprueba el protocolo mediante el que se determinan pautas básicas destinadas a asegurar y proteger el derecho a la intimidad del paciente por los alumnos y residentes en Ciencias de la Salud» en el anexo de dicha ley se detalla

[3] Definición en el GLOSARIO

[4] Definición en el GLOSARIO

[5] Definición en el GLOSARIO

el protocolo a través del cual se determinan y nombran las directrices básicas las cuales están destinadas a asegurar y garantizar la protección del derecho a la intimidad del paciente.

Se destaca que el artículo 5.1.c) de la Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias, detalla porqué los profesionales sanitarios deben respetar la personalidad, dignidad e intimidad de las personas a su cuidado, debiendo respetar la participación de estos en la toma de decisiones que les afecten, sin crear cotilleo, ni comentarios inapropiados. Por lo que, los empleados del centro sanitario, clínica privada u hospital que tengan acceso deliberado a la información personal del paciente, se incluyen los datos de salud, están obligados a mantener la requerida confidencialidad y no solo a lo que se refiere con el deber de cumplir con la confidencialidad detallado en la Ley de Autonomía del Paciente sino también en lo relacionado a la ley de protección de datos médicos. Hay que añadir que se puede reforzar este deber si se añade una cláusula de confidencialidad en protección de datos en los contratos de los empleados.

3.2.3. Deber de secreto

Según la RAE: «Obligación de las autoridades y empleados públicos de guardar el secreto de informaciones a las que pueden acceder por razón de su cargo y cuya difusión esté legalmente prohibida». El secreto profesional se define como un deber y derecho fundamental, ya que dicha garantía de confidencialidad no podría desarrollarse a través de la confianza que por parte del paciente se crea para que este preste la información necesaria para ser atendido

Los datos de carácter personal que componen la historia clínica del paciente son revelados por ellos mismos dentro de un ámbito sanitario. Estos se consideran como datos de especial protección por la LOPDGDD y en ningún otro cualquier caso se podrán recopilar, tratar y ceder para cualquier otra finalidad, que no se haya designado inicialmente a no ser que por motivos de interés propio el afectado consienta expresamente el permiso. En casos muy concretos, los códigos deontológicos consideran la posibilidad de no cumplir este secreto a pesar de lo nombrado anteriormente. El no cumplimiento del secreto profesional, en España, no sólo supone llenar de desconfianza la relación con el paciente, sino que tiene un tratamiento punitivo, es decir, puede crear como consecuencia la inhabilitación profesional, una sanción administrativa, y/o la pena de prisión. A continuación, se detallan los tres tipos de secreto profesional:

1. Secreto confiado: antes de recibir el secreto se crea la promesa. La confidencia pasa a ser totalmente confidencial o profesional.
2. Secreto natural: aunque el receptor del secreto no haya prometido guardarlo, por obligación debe callar, ya que, el precepto moral, en virtud, evidencia que queda

prohibido perjudicar al resto sin tener una razón. Es independiente de todo contrato. Se aplica a cualquier secreto que, por investigación personal, por confidencia o que se haya descubierto por casualidad, no puede divulgarse.

3. Secreto prometido: a causa de investigación personal, por confidencia, bien por casualidad o después de haber conocido el hecho, la consecuencia es un contrato que refleja la promesa de guardar silencio. Un secreto puede pertenecer a la vez a la categoría de prometido y natural. Será prometido cuando haya de por medio una promesa, pero también será natural cuando se requiera discreción [10].

Casos en los que el secreto profesional puede ser vulnerado:

Ilustración 8. Vulneración del secreto profesional. Fuente: elaboración propia

El secreto profesional respeta en todo momento la intimidad del paciente, por lo que supone una obligación de confidencialidad, la cual es causada por la total necesidad de que en la relación entre el profesional y los pacientes exista una absoluta confianza. En lo que respecta en la normativa vigente, la Ley General de Sanidad (artículo 10) detalla la protección de la intimidad del paciente, aunque la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica (artículos 7 y 16), también detallan los derechos de los pacientes sobre la confidencialidad relacionada con la información respectiva a su salud. Los empleados del sector sanitario deberán tener en cuenta en todo momento la intimidad de los pacientes, evitando que cualquier dato personal sobre estos sea facilitado, ya que, si ocurriese lo contrario, se podrían exponer a una compensación económica ya que los pacientes no solo solicitarían una sanción directa para el profesional.

Se debe remarcar e incidir, además de aconsejar a trabajadores de la sanidad y profesionales involucrados que tengan consciencia sobre esta obligación profesional por todos los perjuicios que puede crear y desarrollar la violación del secreto profesional. Por ejemplo, fuera del ámbito laboral deben seguir siendo cautelosos ya que si ocurriese un descuido como hemos detallado anteriormente se podría crear una situación incómoda además de propiciar una reclamación por parte de alguno de los pacientes. En síntesis, el secreto profesional permite el correcto ejercicio de la profesión dentro del centro sanitario, ya que al ser una obligación que establece la garantía de que se desarrolle correctamente la relación de confianza con el cliente, asegura que en todo momento la intimidad de este queda resguardada y protegida.

Se recomienda consultar el artículo 7 de los Principios Fundamentales (Código Ético y Deontológico de la Ingeniería Informática, CCII).

3.3.Gestión de los derechos

3.3.1. Derechos de privacidad de los datos individuales

Según la AEPD:

> «la normativa de protección de datos permite que puedas ejercer ante el responsable del tratamiento tus derechos de acceso, rectificación, oposición, supresión ("derecho al olvido"), limitación del tratamiento, portabilidad y de no ser objeto de decisiones individualizadas».

Estos derechos se caracterizan por lo siguiente:

- El responsable podrá cobrar un canon en proporción a los costes administrativos o directamente negarse a actuar si las solicitudes son infundadas o excesivas.
- Se podría prorrogar el plazo de respuesta hasta dos meses, si se tiene en cuenta la complejidad y el número de solicitudes, pero en un principio se deberían responder en el plazo de un mes.
- Para el ejercicio de estos derechos la figura del responsable es el que tiene la obligación de informar sobre los medios analizados y empleados. No se va a poder denegar este

derecho solo por el motivo de que se opte por otro medio, aunque cumpla el objetivo de ser accesible.

- A excepción de que el interesado cree una solicitud para que cambie el medio por el que se está realizando el ejercicio, la información se le facilitará por dicho medio siempre y cuando sea posible. Ejemplo: la solicitud se presenta por medios electrónicos.
- Si el responsable no da curso a la solicitud, se deberá informar y en el plazo de un mes, se dará la oportunidad de reclamar y actuar ante una Autoridad de Control, conociendo las razones de su no actuación.
- Se podrá ejercer los derechos a través de un representante voluntario o legal.
- Es posible que sea el encargado quien atienda la solicitud en vez del responsable, si ambos lo han establecido en el acto jurídico o contrato donde se les vincula.

Además de regular el uso de la información, muchas regulaciones definen y protegen la privacidad de los datos de una persona (también conocida como «derechos de los interesados»). Los permisos exactos pueden variar según la jurisdicción y la industria, a continuación, se describe cada uno:

Derecho de acceso: también conocido como «derecho a conocer» y «derecho a ser informado», este derecho le permite a una persona saber qué información personal se ha recopilado sobre ellos, las fuentes de las que se recopiló y los fines para los que se recopiló ese contrato, obteniendo la siguiente información:

- Copia de la información personal que van a ser objeto del tratamiento.
- Las categorías que se van a tratar en cuanto a los datos personales.
- Las categorías de los destinatarios a las que serán comunicados los datos personales, sería el caso de organizaciones internacionales o países terceros.
- El reglamento que se va a utilizar para determinar el plazo previsto para la conservación de datos personales.
- El derecho a presentar una reclamación ante una Autoridad de Control.
- Reclamar el conocimiento de la fuente de origen de datos personales que no se hayan obtenido directamente del afectado.
- El derecho de ser informado en las garantías adecuadas si se transfirieran a una organización internacional o a un tercer país los datos personales.

En el caso de la información pública, es la Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno (Ley 41/2002) la que lo regula. La Ley del Procedimiento Administrativo Común de las Administraciones Públicas (Ley 39/2015) se encarga de regular este derecho

cuando el afectado se trata de un interesado en un procedimiento administrativo. En el caso de acceso al historial médico de un paciente, se regula por la Ley de Autonomía del Paciente (Ley 19/2013).

Derecho de rectificación: en algunas jurisdicciones, existe un «derecho de rectificación» asociado que permite a una persona solicitar la corrección de un error de datos en la información personal almacenada por una entidad. En la solicitud se deberá indicar cuales son los datos a los que se refiere, además de la corrección a realizar. En caso de que sea necesario, se deberá acompañar la solicitud de la justificación en forma de documentación que ratifique la inexactitud o la incompletitud de los datos.

Derecho de supresión: también conocido como el «derecho al olvido», este derecho le permite a una persona exigir que la organización elimine la información personal que se ha recopilado. Dependiendo de la situación, esta solicitud se puede cumplir eliminando, anonimizando o recopilando datos. Hay ciertas excepciones a este derecho, como la custodia legal, los requisitos de retención legal y los casos en los que se requiere información para completar una transacción solicitada o proporcionar un servicio solicitado. Este derecho se va a poder ejercitar cuando ocurra alguna de las siguientes circunstancias:

- Si actualmente no son necesarios los datos personales en relación con los fines para los que fueron recogidos o tratados de otro modo.
- Si los datos personales son objeto de mercadotecnia directa, siendo incluidos la elaboración de perfiles relacionados con esta y el afectado se opone a dicho tratamiento.
- Si el cumplimiento de una misión de interés público o el tratamiento de la figura responsable es fundamentado en el interés de carácter legítimo y no se ha prevalecido de otros motivos para legitimar el tratamiento de datos, oponiéndose el afectado a esto.
- Tratamiento ilícito de datos personales.
- En el caso de que los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida por los Derechos de la Unión o de los Estados miembros que se aplique a la persona responsable del tratamiento.

No obstante, este derecho es limitado ya que, aunque el afectado tiene derecho a que se eliminen sus datos siempre que se cumplan los requisitos legales establecidos (art. 17.1 RGPD), hay excepciones (art. 17.3 RGPD), ya sea por interés público, por el cumplimiento de una misión realizada en el ámbito de la salud pública, por libertad de expresión o por reclamaciones.

Derecho a la limitación del tratamiento: las personas tienen el derecho de restringir el tratamiento de su información y optar por qué no se recoja, venda o comparta información sobre ellas. Este derecho también se denomina «derecho a la exclusión voluntaria» (art. 18.2 RGPD). Teniendo en cuenta que su ejercicio de divide en dos ramas, consiste en obtener la limitación del tratamiento de los datos que va a elaborar el responsable. Se puede solicitar la suspensión del tratamiento de los datos:

- Cuando se impugne la exactitud de los datos personales, durante un plazo que permita al responsable su verificación.
- Cuando se opone al tratamiento de los datos personales que el responsable realiza en base a la misión de interés público o al interés legítimo, mientras se verifica si estos motivos prevalecen sobre los del afectado.

Solicitar al responsable la conservación tus datos:

- Cuando el tratamiento sea ilícito y el afectado se haya opuesto a la supresión de los datos y en su lugar se solicita la limitación de su uso.
- Cuando el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, la defensa o el ejercicio de reclamaciones.

Derecho de oposición: este derecho protege a las personas de la mercadotecnia directa no deseada y la elaboración de perfiles. Si la persona se opone, la organización ya no podrá utilizar su información personal con ese propósito. A continuación, se detallan un par de casos donde se supone que se puede en ciertos casos se puede realizar una oposición a que se realice el tratamiento de los datos personales. En el caso de que sean tratados como objeto para el tratamiento de carácter público o esté basado en el interés legítimo, la elaboración de perfiles queda incluido. A excepción de que consten motivos agravantes por los que los derechos, intereses y libertades del interesado o la formulación, la defensa y el ejercicio de reclamaciones, el responsable deberá dejar de tratar los datos.

Cuando el tratamiento tenga como finalidad la mercadotecnia directa, incluida también la elaboración de perfiles anteriormente citada. La información personal deberá de no tratarse para los fines declarados, si se ejerce este derecho con dicha finalidad.

Derecho de portabilidad de los datos: este derecho le otorga a una persona el derecho a recibir su información personal en un formato que le permita transferir o copiar fácilmente de un entorno informático a otro de forma segura y sin pérdida de confidencialidad, lo cual es útil. Este derecho

a menudo se denomina «derecho de transferencia de los datos». Este nuevo derecho se podrá ejercer:

- Los medios automatizados sean los elegidos para el tratamiento de datos.
- El consentimiento o el contrato sea la base del tratamiento.
- Cuando el afectado solicite a aquella entidad u organización que esté tratando sus datos y además le concierne a expensas de saber que él mismo ha sido quien los ha proporcionado, incluyendo la información derivada de su propia actividad.

La Agencia Española de Protección de Datos sugiere a las entidades u organizaciones que empiecen a progresar en los medios que como las interfaces de programación de aplicación o herramientas de descarga que cooperan en la resolución de las solicitudes de portabilidad de los datos.

Derecho a no ser objeto de decisiones individuales automatizadas: la pretensión de este derecho es garantizar el no ser objeto de basarse únicamente en una decisión sobre el tratamiento de los datos, incluyendo la elaboración de perfiles donde puedan producirse efectos jurídicos sobre el afectado o que tome afectación de alguna otra forma similar. Es decir, la elaboración de perfiles es tratada desde la evaluación de aspectos personales en el tratamiento de dichos datos personales cuya finalidad sea analizar o predecir aspectos relacionados con la situación económica, rendimiento en el trabajo, intereses o preferencias personales, comportamiento o fiabilidad. No se podrá aplicar este derecho cuando:

- El contrato entre el responsable y el interesado sea necesario para la ejecución o celebración.
- El consentimiento ofrecido anteriormente sea fundamentado en el tratamiento de los datos del interesado.

A su vez, estas excepciones no se aplicarán sobre las categorías especiales de datos (art.9.1), salvo que se aplique el artículo 9.2. letra a) o g).

Se recomienda consultar el documento (Privacidad en DNS, AEPD)

3.3.2. Gestión del derecho a ser informado

Para el correcto cumplimiento de este derecho la AEPD recomienda que la información sea facilitada por niveles o capas, de forma que:

- La facilitación de información básica en el primer nivel sea de forma sintetizada, requiriendo que se facilite en el mismo momento y a través del mismo medio en el que se vayan a recoger los datos personales del interesado.
- Que la remisión de la información sea a través de un medio adaptado para la presentación, compresión y si se quisiera, en formato archivo.

Se definen las dos capas como: la primera; información básica de carácter resumido y la segunda; información adicional detallada. La primera se refiere al ejercicio de derechos, descripción de la base jurídica del tratamiento, descripción sencilla de los fines del tratamiento, incluyendo si hubiese la elaboración de perfiles, y, por último, pero no menos importante, la identidad del responsable del tratamiento, además de la previsión o no de cesiones y transferencias a terceros países. La segunda se refiere a:

- Cómo ejercer los derechos nombrados anteriormente.
- Categorías de destinatarios o destinatarios. Situaciones específicas aplicables, normas corporativas vinculantes, decisiones de adecuación o garantías.
- Obligación o no de facilitar los datos y posibles consecuencias de no hacerlo. Detalle de la base jurídica del tratamiento y si hubiese obligación legal, detallar interés público o interés legítimo.
- Descripción detallada de los objetivos del tratamiento incluyendo los criterios y plazos de conservación de los datos. Y la posible realización de decisiones automatizadas, perfiles y lógica que se aplicaría.
- Datos del contacto de delegado de protección de datos, si hubiese. Datos de contacto responsable con su identidad y datos del representante, si existiese.

Además, si se obtuviesen datos no directamente desde el afectado se indicaría: en la capa primera, el origen de la procedencia de los datos y en la segunda capa además del origen la especificación de si su procedencia es de acceso público o no y la categoría del tratamiento. Toda esta información se trataría desde un plazo de tiempo responsable de un mes como máximo, aunque haya ciertas excepciones.

3.3.3. Gestión de los derechos sobre los datos de los pacientes

Qué son los datos sensibles: son reconocidos como los especialmente protegidos por el RGPD:

> «Ideología, religión, afiliación sindical, creencias, salud, origen racial o étnico, vida sexual, datos genéticos y biométricos (Art. 9 del RGPD) así como datos relativos a condenas e infracciones penales (Art. 10 del RGPD)».

El considerando 51 del RGPD define que debe incluirse:

> «los datos de carácter personal que revelen el origen racial o étnico, entendiéndose que el uso del término "origen racial" en el presente Reglamento no implica la aceptación por parte de la Unión de teorías que traten de determinar la existencia de razas humanas separada».

El considerando 53 del RGPD destaca que:

> «el presente Reglamento debe establecer condiciones armonizadas para el tratamiento de categorías especiales de datos personales relativos a la salud, en relación con necesidades específicas, en particular si el tratamiento de esos datos lo realizan, con fines relacionados con la salud, personas sujetas a la obligación legal de secreto profesional».

El considerando 71 del RGPD remarca que sobre la elaboración de perfiles y las decisiones automatizadas la figura del responsable del tratamiento debe aplicar métodos que rectifiquen

> «los factores que introducen inexactitudes en los datos personales y reduzcan al máximo el riesgo de error, asegurar los datos personales de forma que se tengan en cuenta los posibles riesgos para los intereses y derechos del interesado e impedir, entre otras cosas, efectos discriminatorios en las personas físicas por motivos de raza u origen étnico, opiniones políticas, religión o creencias, afiliación sindical, condición genética o estado de salud u orientación sexual, o tratamiento que dé lugar a medidas que produzcan tal efecto».

Respecto a las directrices que recoge la LOPDGDD en cuanto a las categorías que pertenecen a datos sensibles coincide con el RGPD, pero sí que considera que este tipo de categorías de datos deben tratarse con mayor cautela y se debe ser más exigente. Dicha ley argumenta que la legitimación para el tratamiento de datos especialmente protegidos el consentimiento del interesado no es suficiente.

> El artículo 9 del Título 1 «Disposiciones generales de la LOPDGDD detalla que: en particular, dicha norma podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte».

Por lo que, la información recabada relacionada con la orientación sexual, referente a la raza o sobre creencias religiosas son considerados datos personales sensibles. Ninguna persona tiene por qué comunicar a otra persona este tipo de datos. Solo se podrían tratar formalizando el consentimiento con el afectado y además por escrito. Las empresas u organizaciones que recopilen estos tipos especiales de datos, más aún si lo realizan a gran escala, están obligados a desarrollar una EIPD y contar en todo momento con un DPD. A continuación, se describen algunos ejemplos sobre datos que se consideran sensibles:

- Si una persona pertenece a un sindicato.
- La huella dactilar al ser un dato biométrico es sensible. Cuando se registra para un control de accesos es un dato que se debe proteger.
- El informe médico de un paciente. Todo dato relacionado con la salud es de tipo sensible. Cuando el software de vigilancia de la salud almacena dicho documento se considera un conjunto de datos que se debe proteger.

3.3.4. Derechos sobre la historia clínica

Anteriormente ya se ha descrito cuales son los derechos de acceso, rectificación, cancelación, limitación del tratamiento, portabilidad y oposición. Los cuales también se aplican a la ley de protección de datos sanitarios.

Acceso a la historia clínica: en cualquier momento, los pacientes de centros de salud, hospitales y centros sanitarios tanto privados como públicos tienen el derecho de solicitar al responsable del tratamiento el acceso a la historia clínica. El plazo máximo en el que debe ser otorgado el expediente es de un mes, y si es posible, a través de los mismos medios por los que fue demandada.

Rectificación de la historia clínica: el afectado, en este caso el paciente, tiene el derecho de solicitar al responsable del tratamiento que rectifique los datos personales que son incorrectos, incompletos o inexactos. Para poder realizar dicha reclamación, se deberán aportar los documentos necesarios que argumenten dicho error. La figura que decide si se va a aplicar la rectificación de los datos sanitarios o no será el profesional sanitario o médico.

Supresión de datos de la historia clínica: cuando se trata de eliminar datos de la historia clínica, se vuelve más compleja la situación ya que se trata de datos que se utilizan con objetivos hacia la medicina preventiva, prestación de asistencia sanitaria, capacidades del trabajador, diagnóstico médico, etc. Se incluyen este tipo de datos para cuando se usan para la continua mejora de la calidad de la prevención de amenazas graves para la salud pública o para la calidad de los servicios en general. Solo podrá realizarse la supresión de datos en la historia clínica si lo indica un profesional sanitario, ya que este tipo de modificación tiene un carácter especial.

3.4.Cesión de datos a terceros

Si se transfieren datos de los pacientes a los laboratorios o una empresa informática es la encargada de realizar el mantenimiento de los equipos en la clínica, son dos ejemplos de cesión de datos personales a terceros. Se entiende como terceros: encargados de tratamiento. Aun teniendo el registro de actividades de tratamiento, se debe establecer una relación con dichas empresas externas que son proveedoras de ciertos servicios y tener consciencia asegurando que sigan la normativa de protección de datos. Es común que los hospitales y clínicas recurran con frecuencia al software de gestión de pacientes. Se debe tener muy en cuenta los aspectos técnicos de dicho software como dónde y de qué forma almacena y procesa los datos personales, más todavía si es un SaaS (basado en la nube). Por esta razón, es importante aclarar con los proveedores de software y de TI (tecnologías de información) cual va a ser la forma en la que dichos sistemas van a adaptarse a la normativa actual. Respecto a los datos que las páginas web de este tipo de entidades recopilan, destacar que los pacientes en todo momento deben saber qué datos se están almacenando. Por lo que se tendrá que firmar un contrato de encargo de tratamiento de datos donde se establezcan cuáles son las responsabilidades y obligaciones de dichos terceros para la protección de datos personales. El contrato debe incluir la siguiente información:

1. Obligaciones del encargado y responsable del tratamiento de datos
2. Categorías de interesados
3. Objetivo de realizar esta cesión
4. Información personal a la que se tendrá acceso
5. Plazo mínimo de conservación de los datos
6. Duración prevista del tratamiento
7. Completa identificación del tercero al que se le cederán los datos

La LOPDGDD destaca que será nulo el consentimiento de cesión de datos cuando la finalidad para la cual se van a utilizar los datos no sea conocida desde un primer momento por el interesado, además si al tercero al cual se le pretende ceder dichos datos ni el tipo de actividad que se va a realizar no está clara, el afectado podrá rescindir su consentimiento en cualquier momento. Para el caso en el que el encargado del tratamiento necesite subcontratar cierto servicio el acceso de un tercero a la información, será necesario el consentimiento explícito del responsable del tratamiento como sería un contrato a tres bandas o añadir una cláusula contractual que describa detalladamente el expreso mandato del responsable del fichero para poder realizar dicha subcontratación de los servicios.

Debida diligencia

Para seleccionar un proveedor de servicios externos, en el proceso se debe incluir la debida diligencia del tercero, una revisión de las condiciones y términos que se ofrecen, además de una AR, todo ello para obtener la garantía de que la entidad no se va a exponer a ciertos riesgos indebidos. Conlleva el seguimiento, el asesoramiento y el proceso de consultoría en miembros de la entidad que estén involucrados en informática, protección de datos, seguridad de la información, derecho contractual y recursos humanos. Dicho proceso también debe recopilar, si son aceptadas por la entidad, la consideración de cualquier política de seguridad de la información o similar del tercero.

3.5.Políticas de privacidad

¿Qué es? Recoge los datos del usuario o cliente en un documento legal que explica como la entidad los maneja, procesa y retiene. Se suele aplicar a sitios de internet. Se puede interpretar como una especia de contrato donde la organización se compromete a guardar los datos personales del usuario. La principal responsabilidad del usuario es leerla y cerciorarse de que no se apliquen ciertas condiciones por las cuales se pueda propiciar una violación de privacidad como podría ser una transferencia de información del usuario.

¿Para qué sirve? Su principal función es la de comunicar a los usuarios del sitio web al que acceden que categoría de datos es la que se va a recopilar durante la visita. Además de informar sobre la finalidad con la que se van a utilizar y si se van a poder actualizar, cancelar o modificar. Es decir, se asegura que los usuarios conocen el fin específico para el cual sus datos van a ser

recogidos y que se hará tras aprobar su consentimiento, consiguiendo así proteger su privacidad. Tener en cuenta que los datos recopilados no podrán ser cedidos a terceros.

¿Por qué se necesita? Al almacenarse la información personal de los usuarios, se pueden calcular ciertas estadísticas de interés como por ejemplo la de posicionamiento web, la cantidad de suscripciones por correo electrónico o el porcentaje de registros mensuales en la plataforma. A parte de este tipo de utilidades, la finalidad más importante que se consigue tras implantar la política de privacidad es establecer el cumplimiento con la ley y además garantizar la protección y seguridad de los datos recopilados.

¿Qué se debe incluir en la política de privacidad? Se debe redactar una política detallada y clara, además de entendible, la información que se detalla debe ser comprensible en todo momento para cualquier tipo de perfil que quiera informarse sobre esta, ya que para poder realizar el seguimiento de los datos de los usuarios se debe obtener el previo consentimiento. El esquema inferior, detalla algunos de los puntos los cuales sería interesante que recopilara la política de privacidad:

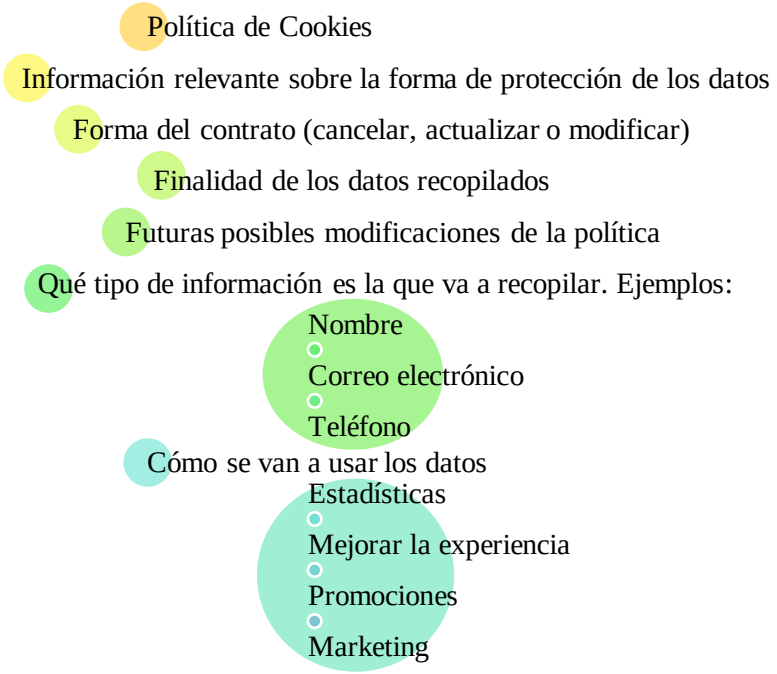


Ilustración 9. Puntos importantes en el desarrollo de la Política de Privacidad. Fuente: elaboración propia

Conseguir cumplir los objetivos de la Política de Privacidad en un hospital o centro sanitario es laborioso ya que las distintas fuentes de las cuales se captan los datos son diferentes (hospitalización, urgencias, consultas, etc.) Por ello es de vital importancia que el completo

personal del hospital o centro médico esté totalmente concienciado sobre la importancia de este tema. El paciente de un centro sanitario debe en primer lugar recibir y firmar, una política de privacidad correctamente detallada. Se debe tener en cuenta que al centro sanitario u hospital en cualquier momento se le puede pedir una demostración de su cumplimiento con esta obligación, por ello, será necesario que dicha organización o entidad deberá implantar y revisar un proceso de captación y almacenamiento de dicha documentación. Se recalca que siempre que se aporte la total garantía de que la firma del documento no haya podido ser manipulada se podrá realizar dicha acción en formato electrónico o en su defecto escanear los consentimientos firmados.

3.6.Sanciones

Las sanciones RGPD para médicos se aplican en función de diversos criterios:

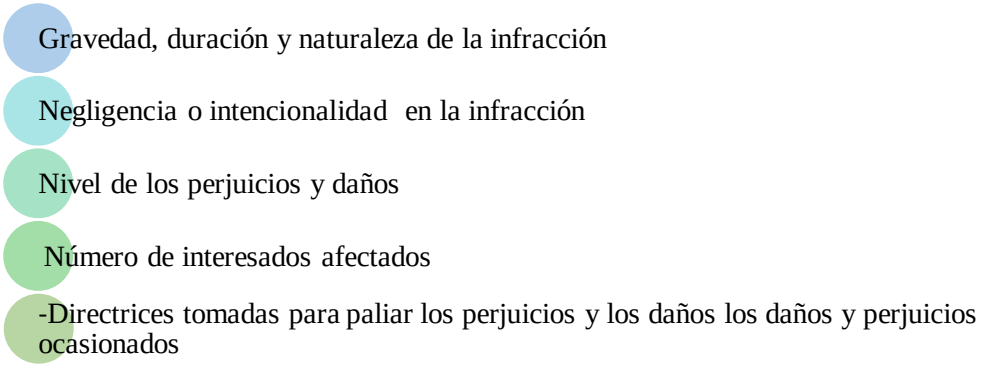


Ilustración 10. Criterios para determinar las sanciones. Fuente: elaboración propia

Dependiendo de la gravedad de la infracción que se comete la LOPDGDD establece los siguientes niveles:

- Infracciones leves: multas de hasta 40.000 euros (art. 74)
- Infracciones graves: multas de 40.001 euros a 300.000 euros (art. 73)
- Infracciones muy graves: multas de 300.001 euros a 20 millones de euros o el 4% de la facturación anual (art. 72)

Sanciones por tratar datos especialmente protegidos: en un principio el tratamiento de datos sensibles no sería motivo de sanción ya que normalmente se cuenta con el consentimiento expreso de las personas interesadas. En el caso contrario, en el cual se recopilen o se traten datos sensibles sin la legitimación jurídica o sin el consentimiento para ellos, se estará cometiendo una infracción

clasificada como muy grave por la LOPDGDD, la cual implica una sanción cuya multa oscila entre los 300.0001 euros y los 20 millones de euros.

Sanciones por no cumplir el deber de secreto: el Código Penal detalla en el artículo 199:

> «El que revele secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses».
>
> «El profesional que, con incumplimiento de su obligación de silencio, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años».

Sanciones si no se notifica la brecha adecuadamente: el hecho de no comunicar las brechas de seguridad que se han podido producir es catalogado como una infracción grave y las multas podrían a llegar a alcanzar los 10 millones de euros o el 2% del volumen de negocio de la entidad aplicada al ejercicio anterior.

EJEMPLOS DE SANCIONES EN CENTROS SANITARIOS

A continuación, se nombran titulares de noticias en los centros médicos y hospitales reales son denunciados por protección de datos por parte de la AEPD:

1. Sanción a un médico de Gijón: a causa de arrojar a la vía pública envases de biopsias con datos personales, la multa que la AEPD le impuso fue de 60.101 euros, ya que se cometió una infracción tipificada como muy grave por la LOPD [8].
2. Apertura de expediente a un hospital por infracción: la causa que motivó a la AEPD para abrir un expediente a un hospital de Inca fue la filtración de datos personales de pacientes [5].
3. Sanción de 6.000 euros a un centro médico: un centro médico de Cartagena fue sancionado por la AEPD con la cifra de 6.000 euros por hacer uso de los datos personales de un cliente de la empresa con la cual se había fusionado [18].
4. La AEPD denuncia a sanidad: un hospital de Cuenca fue apercibido por ceder datos personales e historiales médicos de los pacientes a una clínica privada sin cifrar la información, pese a tratarse de datos especialmente protegidos. La multa ascendió a un total de 40.001 euros [7].

4. CONCLUSIONES

Durante el desarrollo de este trabajo se ha establecido el objetivo de informar a través del previo estudio y posterior análisis sobre la normativa vigente en lo que respecta a protección y tratamiento de datos, incluye el Reglamento General de Protección de Datos y la LOPDGDD, además de herramientas, guías obtenidas por la Agencia Española de Protección de Datos y trabajos de fin de grado relacionados. Todo ello establecido con la finalidad de controlar que se cumpla el deber de informar a los profesionales TIC e informáticos involucrados en instituciones sanitarias.

Esta guía cumple el objetivo de ayudar a que se cumplan las normativas, de informar sobre cuáles son los procedimientos que aplicar, destacando los aspectos técnicos a tener en cuenta y las herramientas involucradas para facilitar el proceso al perfil más técnico como podría ser el delegado de Protección de Datos o los profesionales TIC e informáticos involucrados en instituciones sanitarias, además de que también podría ser entendida por un público menos entendido como podría ser una persona con la curiosidad de conocer más sobre dicha temática. Por lo que esta guía se puede tomar como referente para aplicarla en organizaciones que traten datos sensibles relacionados con la salud.

El anterior punto confirma que esta guía contribuye a que la protección de los datos personales sea un tema de interés y de fácil entendimiento entre entendidos y aquellos trabajadores no implicados en el proceso de tratamiento de datos, por lo que se consigue acercar este tema de especial relevancia haciéndolo accesible y conscientes de ello.

Dentro de las competencias transversales del grado en Ingeniería Informática de la Universidad Politécnica de Valencia para la elaboración de este trabajo se destacan:

Comprensión e integración
Demostrar la comprensión e integración del conocimiento tanto de la propia especialización como en otros contextos más amplios.

Aplicación y pensamiento práctico
Aplicar los conocimientos teóricos y establecer el proceso a seguir para alcanzar determinados objetivos, llevar a cabo experimentos y analizar e interpretar datos para extraer conclusiones.

Innovación, creatividad y emprendimiento

Innovar para responder satisfactoriamente y de forma original a las necesidades y demandas personales, organizativas y sociales con una actitud emprendedora.

Conocimiento de problemas contemporáneos

Identificar e interpretar los problemas contemporáneos en su campo de especialización, así como en otros campos del conocimiento.

Instrumental específico

Seleccionar y aplicar de forma adecuada las herramientas, las tecnologías y en general los instrumentos disponibles para cualquier actuación de diseño o proyecto relacionados con el ámbito de la profesión.

En lo que respecta a lo personal, este trabajo me ha proporcionado conocimientos a cerca de la normativa vigente respecto a la protección de datos, que es un tema el cual se encuentra a la orden del día y del cual conviene encarecidamente estar informado. Además, vi la oportunidad perfecta en relacionarlo con la sanidad, puesto que es uno de los temas de actualidad más relevantes.

Todo esto me proporciona, nuevas oportunidades en el ámbito laboral ya que los conocimientos que he ido aprendiendo a lo largo del desarrollo de esta guía, me pueden introducir en el mercado laboral de protección de datos.

Relación del trabajo desarrollado con los estudios cursados

Tras cursar asignaturas como Fundamentos de Organización en la Empresa (FOE), Deontología y Profesionalismo (DYP) y Comportamiento Organizativo y gestión del cambio (COR) he podido desarrollar correctamente este trabajo, puesto que se me ha proporcionado la teoría y los conocimientos necesarios para ayudarme a ponerlo en práctica y resolver satisfactoriamente un problema del mundo real como la aplicación de la normativa vigente de protección de datos al ámbito sanitario.

Algunos de los problemas o errores que me he encontrado han sido:

- No tener soltura en la interacción y búsqueda de la normativa vigente que interviene en casos como este o la realización de procesos involucrados en la aplicación de la normativa
    - Gracias a la realización de este trabajo puedo afirmar que he adquirido mucho conocimiento de causa.

- Destacaría también que tras varios acontecimientos no esperados he tenido que ir adaptando la planificación para la realización de este trabajo. Aunque, finalmente los sucesos de diferentes acontecimientos no ha sido un impedimento para llevarlo a cabo.

5. TRABAJOS FUTUROS

Tras finalizar el desarrollo del trabajo de fin de grado, destacan una serie de trabajos los cuales pueden servir como ampliación de este y realizarse por otros investigadores:

- Realizar un estudio exhaustivo sobre las brechas de seguridad y sus consecuencias en entornos sanitarios, con el propósito de aprender los efectos que se producen para aplicar soluciones de manera proactiva, además de tomar consciencia de la alta probabilidad de que dicha situación ocurra en entornos más concretos.

- Implementar un sistema de apoyo para el delegado de protección de datos de un hospital. Teniendo en cuenta desde la captación de todo tipo de datos sensibles que se manejan en un hospital hasta el desarrollo de una interfaz intuitiva y de fácil manejo para que todo personal sanitario pueda hacer uso de este.

- Desarrollar una aplicación la cual genere toda la documentación requerida en el proceso de tratamiento de datos personales, documentos de seguridad, evaluaciones requeridas, personas responsables involucradas, procedimientos a realizar en los análisis de datos, contratos de confidencialidad y documentos informativos.

- Ampliar la aplicación de la guía en cuanto a datos potencialmente sensibles como datos biométricos, huellas dactilares, información identificativa del paciente, etc. Este tipo de datos necesitarían protocolos más concretos y exclusivos ya que son los necesarios para la elaboración de perfiles automatizados.

6. REFERENCIAS

[1] Agencia Española Protección Datos. (2022, 14 junio). *Principios*. AEPD. Recuperado 15 de julio de 2022, de https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/principios.

[2] Bañó Juan, A. (2021). *Creación de una guía para el control del deber de informar en cumplimiento del Reglamento de Protección de Datos Europeos*. Universitat Politécnica de Valencia.

[3] Centro Criptográfico Nacional. (2015, julio). *GUÍA DE SEGURIDAD (CCN-STIC-401)*.

[4] Conversia (2017). Diferencias en los perfiles de protección de datos. Blog Mundo LOPD I CONVERSIA. Recuperado el 2 de junio de 2021, de: https://www.mundolopd.com/lopd/diferencias-dpo-responsables-tratamiento-privacidad-lopd-rgpd/

[5] Efe. (2019, 6 febrero). *La Agencia de Protección de Datos abre un expediente al Hospital de Inca*. Ultima Hora. Recuperado 11 de agosto de 2022, de https://www.ultimahora.es/noticias/local/2011/05/13/40271/la-agencia-de-proteccion-de-datos-abre-un-expediente-al-hospital-de-inca.html

[6] eldelegadodeprotecciondedatos.com. (s. f.). *Autoridad de control*. Delegado de protección de datos DPO. Recuperado 16 de agosto de 2022, de https://www.eldelegadodeprotecciondedatos.com/autoridad-de-control/

[7] ElDiario.es. (2016, 8 febrero). *Una clínica privada, multada por filtrar datos de pacientes en Cuenca*. Recuperado 12 de agosto de 2022, de https://www.eldiario.es/castilla-la-mancha/proteccion-datos-consentimiento-pacientes-cuenca_1_4199618.html

[8] Europa Press. (2009, 28 diciembre). *La Agencia de Protección de Datos sanciona a un médico de Gijón por tirar envases de biopsias con datos personales*. europapress.es. Recuperado 9 de agosto de 2022, de https://www.europapress.es/asturias/noticia-agencia-proteccion-datos-sanciona-medico-gijon-tirar-envases-biopsias-datos-personales-20091228134816.html

[9] European Union. (s. f.). *EDPB*. Recuperado 5 de agosto de 2022, de https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/edpb_en

[10] Fernández Martínez, Á., & García Rodríguez, E. (2020, 24 febrero). *Análisis del secreto profesional en el ámbito de la sanidad*. Ocronos - Editorial Científico-Técnica. Recuperado 11 de agosto de 2022, de https://revistamedica.com/secreto-profesional-ambito-de-la-sanidad/

[11] Generalitat Valenciana. (s. f.). *Delegación de Protección de Datos GVA - Generalitat Valenciana*. Delegación de Protección de Datos GVA. Recuperado 17 de junio de 2022, de https://participacio.gva.es/es/web/delegacion-de-proteccion-de-datos-gva

[12] Inforaser. (2021, 10 mayo). *Implantación RGPD + LOPDGDD* •. Recuperado 6 de julio de 2022, de https://inforaser.com/implantacion-rgpd-lopgdd/

[13] Llorca Mena, P. (2021). *Elaboración de una guía de buenas prácticas en protección de datos para pequeñas empresas*. Universitat Politécnica de Valencia.

[14] Mercader, A., & Cid, S. (2022, 21 julio). *Ciberataque masivo contra el CSIC: el instituto de investigación se defiende de un 'ransomware'*. Crónica Global. Recuperado 18 de agosto de 2022, de https://cronicaglobal.elespanol.com/business/ciberataque-masivo-csic-instituto-ransomware_701072_102.html

[15] Mompó, J. (2020). *Guía Interactiva para el cumplimiento de normas de Protección de Datos en el entorno laboral*. Universitat Politécnica de Valencia.

[16] Panda Security. (2014, 13 octubre). *Los hospitales, en el punto de mira de los ciberdelincuentes*. Centro Criptológico Nacional (CCN-CERT). Recuperado 25 de julio de 2022, de https://www.ccn-cert.cni.es/en/gestion-de-incidentes/lucia/23-noticias/1171-los-hospitales-en-el-punto-de-mira-de-los-ciberdelincuentes.html

[17] Portal Administración Electrónica. (2022, 15 julio). *El Gobierno de España adopta la Carta de Derechos Digitales*. Recuperado 16 de agosto de 2022, de https://administracionelectronica.gob.es/general/error.htm;jsessionid=03B9E6FA6E8FE3B0D7DA7E1F6BFF9D17.node2_paeaplic

[18] Ribes, V. (2011, 25 noviembre). *La AEPD sanciona con 6.000€ a un Centro Médico de Cartagena | Gestión de la Protección de Datos*. ADELOPD. Recuperado 13 de agosto de 2022, de https://www.adelopd.com/la-aepd-sanciona-con-6000e-a-un-centro-medico-de-cartagena/

[19] Salesforce. (s. f.). *¿Qué es el software como servicio (SaaS)?* Salesforce.com. Recuperado 16 de agosto de 2022, de https://www.salesforce.com/es/learning-centre/tech/saas/

[20] Sendiblue. (2021, 28 agosto). *¿Qué es el marketing directo? Ventajas, canales y ejemplos*. Sendinblue. Recuperado 16 de agosto de 2022, de https://es.sendinblue.com/blog/marketing-directo/

[21] Tablado, F. (2020, 5 noviembre). *Base de datos en la nube ¿Qué es? ¿Cómo funciona?* Ayuda Ley Protección Datos. Recuperado 16 de agosto de 2022, de https://ayudaleyprotecciondatos.es/bases-de-datos/en-la-nube/

7. ANEXO 1 – GUÍA SIMPLIFICADA

En este anexo se desarrolla una guía simplificada la cual tiene como objetivo dar apoyo al trabajo en lo que respecta a la protección de datos. Se detalla el orden de los procedimientos incluyendo el total desarrollo e implementación de este, teniendo en cuenta los aspectos más importantes a destacar en los temas técnicos, además de enlaces de interés en los que se puede encontrar información sobre el tema más detallada y consejos para su aplicación. Las partes de la guía quedan resumidas en:

- Generar y recopilar la documentación necesaria
- Designar a las figuras profesionales
- Registro de actividades de tratamiento
- Evaluación de impacto en protección de datos personales
- Análisis de riesgos
- Medidas de seguridad
- Brechas de seguridad
- Deber de secreto para los empleados
- Gestión de los derechos
  - Derechos de privacidad de los datos individuales
  - Gestión del derecho a ser informado
  - Gestión de los derechos sobre los datos de los pacientes
  - Derechos sobre la historia clínica
- Cesión de datos a terceros
- Políticas de privacidad
- Sanciones

Se recomienda consultar la guía de (La protección de datos en las relaciones laborales, AEPD)

Generar y recopilar la documentación necesaria:

- Certificado de cumplimiento normativo RGPD UE 2016/679.
- Acuerdos de confidencialidad con todo aquel que tenga autorización para acceder a los datos personales.
- En relación con el artículo 28 RGPD UE 2016/679 se redactan los contratos con los encargados de tratamiento (CET).
- En cuanto a los formularios de recogida de datos en formato papel se redactan las cláusulas informativas (CI).
- Creación de los documentos del Registro de Actividades de Tratamiento (RAT), con su posterior generación en la cual quedan recogidos el Plan de Acción y las Medidas de Seguridad (PAMS).
- Por último, una evaluación sobre los Análisis de Riesgos (AR) y elaborar un informe ejecutivo del resumen de riesgos detectados, interpretación de datos y activos afectados [12].

Se recomienda consultar la herramienta (Evalúa-Riesgo RGDP, AEPD)

Designar a las figuras profesionales

En concreto al: **delegado de Protección de Datos**

Según el artículo 34 de la Ley Orgánica 3/2018, de 5 de diciembre:

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

en la que se destaca:

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

Asimismo, según el artículo 36 de la Ley Orgánica 3/2018, de 5 de diciembre, destacando los puntos 1 y 3, (en el anexo se puede encontrar más detalladamente el capítulo al que se refiere esta ley):

> «1. El delegado de protección de datos actuará como interlocutor del responsable o encargado del tratamiento ante la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos. El delegado podrá inspeccionar los procedimientos relacionados con el objeto de la presente ley orgánica y emitir recomendaciones en el ámbito de sus competencias».
>
> «En el ejercicio de sus funciones el delegado de protección de datos tendrá acceso a los datos personales y procesos de tratamiento, no pudiendo oponer a este acceso el responsable o el encargado del tratamiento la existencia de cualquier deber de confidencialidad o secreto, incluyendo el previsto en el artículo 5 de esta ley orgánica».

Con esta información quedan destacadas las siguientes funciones del delegado de protección de datos:

- Asesorar e informar al responsable de datos y aquellos empleados que tengan relación con el tratamiento de datos de sus obligaciones legales:
  - Orientación y resolución de dudas
  - Educación y formación
- Supervisión de la asignación de responsabilidades, así como del cumplimiento de las leyes aplicables, además de la formación del personal en temas de auditoría y protección de datos.
- Cooperación con la AEPD (autoridad de control), ya que este actúa como representante.
- En lo que respecta a la protección de datos, ofrecer asesoramiento.
- Punto de encuentro entre la empresa y la autoridad.

Se recomienda consultar la guía sobre (Tecnologías y Protección de Datos en las Administraciones Públicas, AEPD)

En la imagen inferior, se clarifica a modo de resumen las principales funciones de cada figura involucrada en el tratamiento.

Ilustración 11. Diferencias entre las figuras responsables. Fuente: (Conversia, 2017) [4]

Respecto a la designación del DPD

Atendiendo al artículo 37.1.c del RGPD donde se argumenta que todo aquel responsable o encargado que vaya a realizar un tratamiento de datos sensibles tiene la obligación de designar a un DPD. Los datos y el nombramiento del DPD deben hacerse de manera pública además de ser comunicados a las autoridades responsables de supervisión, como marca el RGPD. Se destaca que la figura del DPD la podrá representar una persona perteneciente a la plantilla de la empresa o en otro caso, se podría contratar de forma externa a la organización o empresa que tenga en sus ofertas dicho servicio. El DPD involucrado en una organización de sanidad, respecto al volumen de datos que trata, va a ser el profesional, que tras la formación y cualificación necesaria en esta materia que consiste en la supervisión del cumplimento de la ley en las políticas y los procesos internos del tratamiento de datos sensibles, tome el cargo de responsabilidad en la entidad. Por último, se añade que la LOPDGDD indica que no será necesario la figura del DPD en las clínicas privadas donde los profesionales sanitarios desarrollen su profesión de manera individual.

Se recomienda consultar la herramienta (Canal del DPD, AEPD)

Registro de actividades de tratamiento

El responsable ha de mantener un registro en el que se almacene de cada uno de los registros la elaboración del análisis de datos previo, ya que para cumplir con la protección de datos sanitarios en el hospital o clínica se deberá responder a una serie de información que queda detallada en el artículo 30 del RGPD.

El RAT ha de constar por escrito y, en su caso, en soporte electrónico, y estará a disposición de la Agencia de Protección de Datos o, si el responsable fuera una entidad pública, de la autoridad de control competente. Sin embargo, en el caso de las entidades públicas el inventario (art.31 LOPDGDD) con los tratamientos de datos personales deberá hacerse público y estar accesible por medios electrónicos (por ej., a través de la respectiva página web).

A continuación, se introducirá la categoría de datos personales que se van a tratar además del tiempo mínimo de conservación de los datos. Refiriéndonos a este tratamiento incluiría: imagen y/o voz, nombre y apellidos, teléfonos, dirección postal, DNI u otro documento identificativo, identidad electrónica.

En cuanto al tiempo mínimo de conservación de los datos hay que añadir que sería para un periodo indeterminado ya que se mantendrían los datos durante el tiempo necesario para cumplir con el objetivo para el cual se obtuvieron. En el siguiente apartado, se incluirá la categoría de titulares de los datos, es decir, quienes son los interesados o afectados. Para este caso serían los trabajadores, autores y titulares de artículos, pacientes y ciudadanos.

Se recalca que la licitud del tratamiento quedará representada por el art. 6.1 a) RGPD el cual argumenta que el interesado da su consentimiento para el tratamiento de su información personal. Por último, se procederá a registrar la información necesaria que requiera las medidas de seguridad, englobaría tanto las organizativas como las técnicas que realice el hospital para la protección de los datos.

PARA SABER MÁS - Las medidas de seguridad de nuestro caso quedan recogidas en el Real decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica

RECUERDA - Se destaca la elaboración del análisis de datos previo ya que para cumplir con la protección de datos sanitarios en el hospital o clínica se deberá responder a una serie de información que se podría sintetizar dicha información de la siguiente manera:

- Entidad responsable
- Tipos de datos que se recopilan.
- Objetivos del tratamiento.
- Política de almacenamiento de dichos datos.
- Si se ceden los datos o se transfieren a otros países.
- Cuáles van a ser los medios de tratamiento.
- Identificación del responsable y delegado de protección de datos.
- Los plazos previstos para la eliminación de según que categorías de datos.
- Una descripción de las medidas organizativas y técnicas de seguridad.

¡IMPORTANTE! Este documento se puede pedir en el caso de que se realice una inspección por la AEPD. Por esta razón, se debe mantener actualizado además de constar por escrito, aunque también pueda sea válido en formato electrónico.

Evaluación de impacto en protección de datos personales

Una EIPD (Evaluación de Impacto de Protección de Datos) es una evaluación de impacto que tiene relación con la privacidad, su finalidad es la identificación y el análisis de determinadas consecuencias que ciertas actividades o acciones pueden afectar a la privacidad. Estas evaluaciones determinan el nivel de riesgo que un tratamiento puede causar en las libertades y derechos de los afectados, asimismo permiten la identificación de riesgos y amenazas potenciales y la evaluación tanto del impacto como de la posibilidad de que se produzcan sobre la vida de los titulares de la información.

Dicho procedimiento debe quedar documentado, su revisión debe ser de forma periódica y deberá recoger todo el ciclo de vida del dato, desde la recogida de datos del paciente hasta la eliminación, pasando por el proceso de tratamiento y su posible almacenamiento.

Las empresas que deberían realizar dicho procedimiento son aquellas que elaboren perfiles, y en base a estos posteriormente se produzcan tratamientos jurídicos hacia las personas físicas o de alguna manera les afecten significativamente, se incluyen también las organizaciones o entidades que traten categorías especiales de datos o información personal relativa a infracciones penales y condenas. Finalmente, aquellas empresas que mantengan observada una zona de acceso público de forma sistemática a gran escala.

Pasos necesarios para realizar una EIPD:

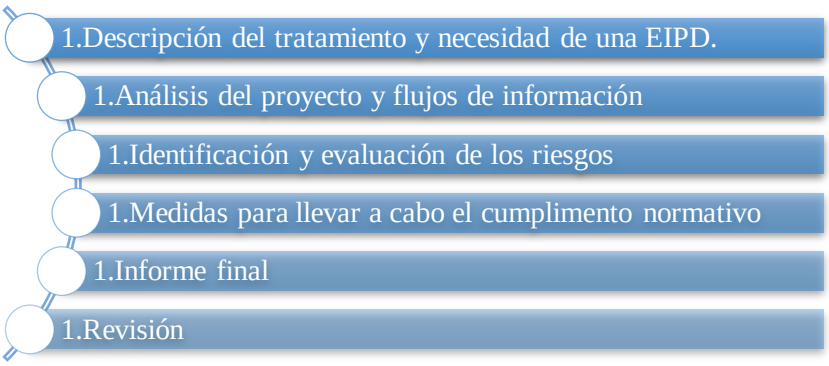


Ilustración 12. Fases para realizar EIPD. Fuente: elaboración propia

Se recomienda consultar la herramienta (GESTIONA EIPD, AEPD)

PARA SABER MÁS – Consulta la Gestión del riesgo y Evaluación de Impacto en tratamientos de Datos Personales.

¡IMPORTANTE! - Los hospitales o clínicas habrán de realizar una EIPD para reducir las posibles afectaciones sobre las libertades o derechos de los afectados, ya que se tratan categorías especiales de datos (información sobre la salud de los pacientes) y posteriormente, se deberán implementar las adecuadas restricciones en ámbito de seguridad.

Análisis de riesgos

Se destaca que para la correcta evaluación de un riesgo sería necesario la consideración de todos los escenarios en los que el riesgo sería clave o efectivo. Se incluyen los que implican un abuso o mal uso de la información y las alteraciones del entorno y técnicas. En resumen, el nivel de riesgo se medirá en función de la probabilidad de materialización y el impacto que se obtendría en caso de hacerlo. A continuación, algunos ejemplos de riesgos para la protección de datos:

- La cesión de información a otra organización o entidad.
- Emplear sistemas de videovigilancia.

- Los incidentes no previstos (cortes de suministro eléctrico, incendios…). Aquellos que puedan destruir los soportes en los que quedan almacenados los datos o en general los equipos.
- Crear un nuevo tratamiento de datos personales (formulario de suscripción a un canal o de contacto).
- La utilización de una base de datos en la nube para almacenar los datos personales.

Quedan identificadas **siete** fases para realizar un AR según el RGPD:

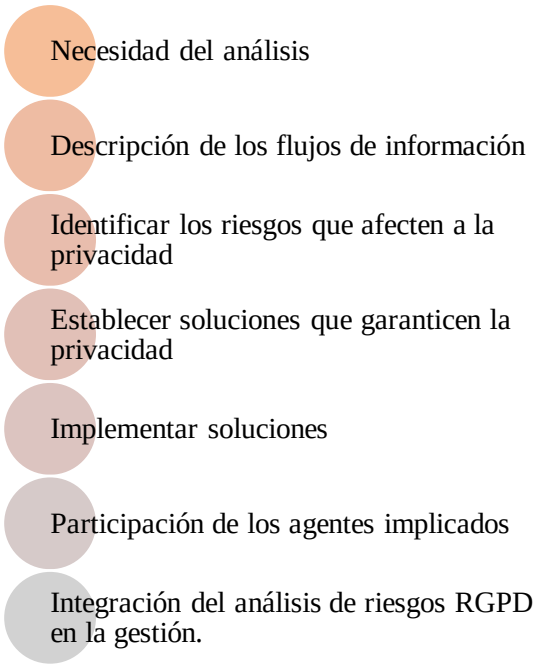


Ilustración 13. Fases para realizar un AR. Fuente: elaboración propia

Medidas de seguridad

Tras realizar los análisis mencionados anteriormente es de importancia que se apliquen altas medidas de seguridad para intentar paliar los ataques informáticos actuales. Una medida sería limitar el acceso a datos críticos.

Ilustración 14. Medidas de seguridad básicas. Fuente: elaboración propia

El sistema de permisos de acceso es el encargado de recopilar los roles, grupos y permisos por lo que es una herramienta crítica.

El HIS debe recoger cada acceso al historial del paciente, quedando detallado cuales han sido las acciones realizadas sobre este: modificaciones, borrados, adiciones, o simplemente quien ha sido el visor. Y finalmente, habría que tener especial cuidado en situaciones de traslados de historiales o procesos de destrucción ya que son acontecimientos que pueden provocar accidentes graves.

PARA SABER MÁS - Brechas de seguridad: El Top 5 de las medidas técnicas que debes tener en cuenta.

Brechas de seguridad

Una brecha de seguridad es la acción cuyo resultado es el acceso no autorizado a datos de aplicaciones, redes, ordenadores o dispositivos. Suele pasar cuando un no autorizado no tiene en cuenta los mecanismos de seguridad, por lo que acaba accediendo a información sin autorización.

En función de los datos y de las consecuencias o de los objetivos las brechas de seguridad pueden clasificarse en tres tipos distintos, teniendo en cuenta que pueden haber sido causado tanto por un ataque premeditado como uno que no:

- Brecha de integridad: cuando la información original o los datos son modificados en el sistema, dicha acción puede causar inconvenientes a la entidad además de los afectados.
- Brecha de confidencialidad: ocurre cuando un descuido o un ataque puede facilitar datos no autorizados.
- Brecha de disponibilidad: un incidente provocado o no, cuyas consecuencias son la pérdida de información almacenada, ya sea de forma temporal o permanentemente.

¿Cómo se gestiona una brecha de seguridad?

8. Encontrar e identificar
9. Clasificación: nombrada anteriormente
10. Elaborar el plan de contingencia para paliar sus consecuencias.
11. Contención: la aplicación de los siguientes ejemplos muestra una actitud proactiva con lo que se refiere a las brechas de seguridad:
    a. Restringir el acceso a la red
    b. Deshabilitar usuarios con permisos comprometidos y actualizar las contraseñas
    c. Los parches como método temporal para resolver los errores y vulnerabilidades.
    d. Las aplicaciones críticas y sistemas se deben poner en cuarentena o directamente apagarlos.
12. Tras la aplicar la solución se tendrá la información para resolver las siguientes preguntas:
    a. Tiempo durante el cual la violación estuvo activa.
    b. Qué datos han sido modificados, dañados o revelados.
    c. Cuál ha sido el impacto.
    d. Qué terceros se han visto involucrados.
13. Recuperación: incluye las fases de parcheo de sistemas, configurar correctamente los permisos y reconstrucción de sistemas para que no vuelva a suceder el mismo problema.
14. Comunicación: es la parte la cual se debe redactar un informe posterior al incidente con la información actualizada la cual detalle la raíz del problema y como se ha desarrollado la respuesta hacia el incidente.

¿Cómo notificar la brecha de seguridad?

Se recomienda consultar la Guía para la notificación de brechas de datos personales por la AEPD.

¡IMPORTANTE! 72 horas es el plazo en el cual, si las organizaciones no comunican que han sufrido una violación de los datos, aunque puedan explicar los motivos de la tardanza, se siguen exponiendo a las posibles sanciones y/o multas.

Se recomienda consultar la herramienta (Asesora-Brecha RGPD, AEPD)

Se recomienda consultar la herramienta (Comunica-Brecha RGPD, AEPD)

Deber de secreto

Según la RAE: «Obligación de las autoridades y empleados públicos de guardar el secreto de informaciones a las que pueden acceder por razón de su cargo y cuya difusión esté legalmente prohibida». El secreto profesional se define como un deber y derecho fundamental, ya que dicha garantía de confidencialidad no podría desarrollarse a través de la confianza que por parte del paciente se crea para que este preste la información necesaria para ser atendido.

Los datos de carácter personal que componen la historia clínica del paciente son revelados por ellos mismos dentro de un ámbito sanitario. Estos se consideran como datos de especial protección por la LOPDGDD y en ningún otro cualquier caso se podrán recopilar, tratar y ceder para cualquier otra finalidad, que no se haya designado inicialmente a no ser que por motivos de interés propio el afectado consienta expresamente el permiso. En casos muy concretos, los códigos deontológicos consideran la posibilidad de no cumplir este secreto a pesar de lo nombrado anteriormente. A continuación, se detallan los tres tipos de secreto profesional:

4. Secreto confiado: antes de recibir el secreto se crea la promesa. La confidencia pasa a ser totalmente confidencial o profesional.
5. Secreto natural: aunque el receptor del secreto no haya prometido guardarlo, por obligación debe callar, ya que, el precepto moral, en virtud, evidencia que queda prohibido perjudicar al resto sin tener una razón. Es independiente de todo contrato. Se

aplica a cualquier secreto que, por investigación personal, por confidencia o que se haya descubierto por casualidad, no puede divulgarse.

6. Secreto prometido: a causa de investigación personal, por confidencia, bien por casualidad o después de haber conocido el hecho, la consecuencia es un contrato que refleja la promesa de guardar silencio. Un secreto puede pertenecer a la vez a la categoría de prometido y natural. Será prometido cuando haya de por medio una promesa, pero también será natural cuando se requiera discreción [10].

Casos en los que el secreto profesional puede ser vulnerado:

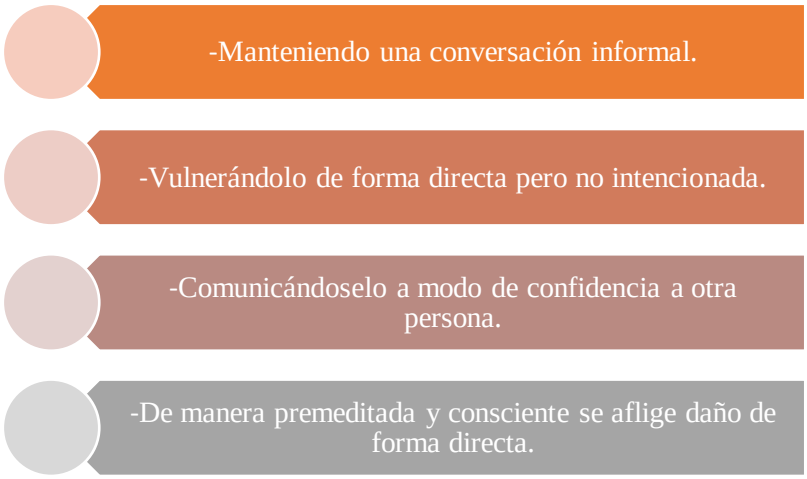


Ilustración 15. Vulneración del secreto profesional. Fuente: elaboración propia

Se debe remarcar e incidir, además de aconsejar a trabajadores de la sanidad y profesionales involucrados que tengan consciencia sobre esta obligación profesional por todos los perjuicios que puede crear y desarrollar la violación del secreto profesional. Por ejemplo, fuera del ámbito laboral deben seguir siendo cautelosos ya que si ocurriese un descuido como hemos detallado anteriormente se podría crear una situación incómoda además de propiciar una reclamación por parte de alguno de los pacientes. En síntesis, el secreto profesional permite el correcto ejercicio de la profesión dentro del centro sanitario, ya que al ser una obligación que establece la garantía de que se desarrolle correctamente la relación de confianza con el cliente, asegura que en todo momento la intimidad de este queda resguardada y protegida.

Se recomienda consultar el artículo 7 de los Principios Fundamentales (Código Ético y Deontológico de la Ingeniería Informática, CCII).

EJEMPLO - La resolución del Expediente Nº: E/01427/2018 de la AEPD el 5 de marzo de 2018. «Tras el reconocimiento médico anual en QUIRON PREVENCION SALUD, S.L.U, han sido enviados a su teléfono móvil personal y, simultáneamente, al departamento de administración de su empresa los datos de acceso (clave y login), para descargar los resultados de las pruebas realizadas. Tuvo conocimiento de este hecho porque la persona del departamento de RR. HH receptora del correo electrónico, en la dirección ***EMAIL.1, procedió a su reenvío al denunciante».

Gestión de los derechos

Derechos de privacidad de los datos individuales

Según la AEPD:

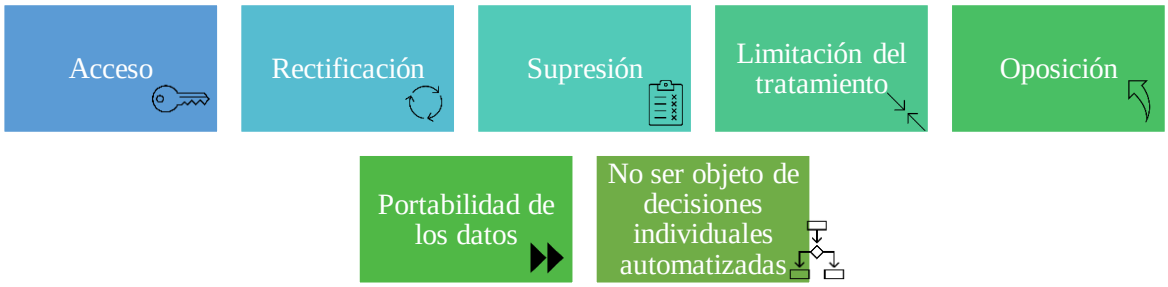
> «la normativa de protección de datos permite que puedas ejercer ante el responsable del tratamiento tus derechos de acceso, rectificación, oposición, supresión ("derecho al olvido"), limitación del tratamiento, portabilidad y de no ser objeto de decisiones individualizadas».

Estos derechos se caracterizan por lo siguiente:

- El responsable podrá cobrar un canon en proporción a los costes administrativos o directamente negarse a actuar si las solicitudes son infundadas o excesivas.
- Se podría prorrogar el plazo de respuesta hasta dos meses, si se tiene en cuenta la complejidad y el número de solicitudes, pero en un principio se deberían responder en el plazo de un mes.
- Para el ejercicio de estos derechos la figura del responsable es el que tiene la obligación de informar sobre los medios analizados y empleados. No se va a poder denegar este derecho solo por el motivo de que se opte por otro medio, aunque cumpla el objetivo de ser accesible.
- A excepción de que el interesado cree una solicitud para que cambie el medio por el que se está realizando el ejercicio, la información se le facilitará por dicho medio siempre y cuando sea posible. Ejemplo: la solicitud se presenta por medios electrónicos.

- Si el responsable no da curso a la solicitud, se deberá informar y en el plazo de un mes, se dará la oportunidad de reclamar y actuar ante una Autoridad de Control, conociendo las razones de su no actuación.
- Se podrá ejercer los derechos a través de un representante voluntario o legal.
- Es posible que sea el encargado quien atienda la solicitud en vez del responsable, si ambos lo han establecido en el acto jurídico o contrato donde se les vincula.

Además de regular el uso de la información, muchas regulaciones definen y protegen la privacidad de los datos de una persona (también conocida como «derechos de los interesados»). Los permisos exactos pueden variar según la jurisdicción y la industria, a continuación, se nombran cada uno:



Se recomienda consultar el documento (Privacidad en DNS, AEPD)

Gestión del derecho a ser informado

Para el correcto cumplimiento de este derecho la AEPD recomienda que la información sea facilitada por niveles o capas, de forma que:

- La facilitación de información básica en el primer nivel sea de forma sintetizada, requiriendo que se facilite en el mismo momento y a través del mismo medio en el que se vayan a recoger los datos personales del interesado.
- Que la remisión de la información sea a través de un medio adaptado para la presentación, compresión y si se quisiera, en formato archivo.

Se definen las dos capas como: la primera; información básica de carácter resumido y la segunda; información adicional detallada. La primera se refiere al ejercicio de derechos, descripción de la base jurídica del tratamiento, descripción sencilla de los fines del tratamiento, incluyendo si hubiese la elaboración de perfiles, y, por último, pero no menos importante, la identidad del

responsable del tratamiento, además de la previsión o no de cesiones y transferencias a terceros países. La segunda se refiere a:

- Cómo ejercer los derechos nombrados anteriormente.
- Categorías de destinatarios o destinatarios. Situaciones específicas aplicables, normas corporativas vinculantes, decisiones de adecuación o garantías.
- Obligación o no de facilitar los datos y posibles consecuencias de no hacerlo. Detalle de la base jurídica del tratamiento y si hubiese obligación legal, detallar interés público o interés legítimo.
- Descripción detallada de los objetivos del tratamiento incluyendo los criterios y plazos de conservación de los datos. Y la posible realización de decisiones automatizadas, perfiles y lógica que se aplicaría.
- Datos del contacto de delegado de protección de datos, si hubiese. Datos de contacto responsable con su identidad y datos del representante, si existiese.

Además, si se obtuviesen datos no directamente desde el afectado se indicaría: en la capa primera, el origen de la procedencia de los datos y en la segunda capa además del origen la especificación de si su procedencia es de acceso público o no y la categoría del tratamiento. Toda esta información se trataría desde un plazo de tiempo responsable de un mes como máximo, aunque haya ciertas excepciones.

Gestión de los derechos sobre los datos de los pacientes

Qué son los datos sensibles: son reconocidos como los especialmente protegidos por el RGPD:

> «Ideología, religión, afiliación sindical, creencias, salud, origen racial o étnico, vida sexual, datos genéticos y biométricos (Art. 9 del RGPD) así como datos relativos a

Respecto a las directrices que recoge la LOPDGDD en cuanto a las categorías que pertenecen a datos sensibles coincide con el RGPD, pero sí que considera que este tipo de categorías de datos deben tratarse con mayor cautela y se debe ser más exigente. Dicha ley argumenta que la legitimación para el tratamiento de datos especialmente protegidos el consentimiento del interesado no es suficiente.

> El artículo 9 del Título 1 «Disposiciones generales de la LOPDGDD detalla que: en particular, dicha norma podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte».

Por lo que, la información recabada relacionada con la orientación sexual, referente a la raza o sobre creencias religiosas son considerados datos personales sensibles. Ninguna persona tiene por qué comunicar a otra persona este tipo de datos. Solo se podrían tratar formalizando el consentimiento con el afectado y además por escrito. Las empresas u organizaciones que recopilen estos tipos especiales de datos, más aún si lo realizan a gran escala, están obligados a desarrollar una EIPD y contar en todo momento con un DPD. A continuación, se describen algunos ejemplos sobre datos que se consideran sensibles:

- Si una persona pertenece a un sindicato.
- La huella dactilar al ser un dato biométrico es sensible. Cuando se registra para un control de accesos es un dato que se debe proteger.
- El informe médico de un paciente. Todo dato relacionado con la salud es de tipo sensible. Cuando el software de vigilancia de la salud almacena dicho documento se considera un conjunto de datos que se debe proteger.

Derechos sobre la historia clínica

Acceso a la historia clínica: en cualquier momento, los pacientes de centros de salud, hospitales y centros sanitarios tanto privados como públicos tienen el derecho de solicitar al responsable del tratamiento el acceso a la historia clínica. El plazo máximo en el que debe ser otorgado el expediente es de un mes, y si es posible, a través de los mismos medios por los que fue demandada.

Rectificación de la historia clínica: el afectado, en este caso el paciente, tiene el derecho de solicitar al responsable del tratamiento que rectifique los datos personales que son incorrectos, incompletos o inexactos. Para poder realizar dicha reclamación, se deberán aportar los documentos necesarios que argumenten dicho error. La figura que decide si se va a aplicar la rectificación de los datos sanitarios o no será el profesional sanitario o médico.

Supresión de datos de la historia clínica: cuando se trata de eliminar datos de la historia clínica, se vuelve más compleja la situación ya que se trata de datos que se utilizan con objetivos hacia la medicina preventiva, prestación de asistencia sanitaria, capacidades del trabajador, diagnóstico médico, etc. Se incluyen este tipo de datos para cuando se usan para la continua mejora de la calidad de la prevención de amenazas graves para la salud pública o para la calidad de los servicios en general. Solo podrá realizarse la supresión de datos en la historia clínica si lo indica un profesional sanitario, ya que este tipo de modificación tiene un carácter especial.

EJEMPLO: La resolución del Expediente Nº: E/05043/2015 de la AEPD el 20 de julio de 2015. «El hecho denunciado es que el cirujano pediátrico, desde su puesto de trabajo en el hospital accedió irregularmente al historial clínico del denunciante».

Cesión de datos a terceros

Si se transfieren datos de los pacientes a los laboratorios o una empresa informática es la encargada de realizar el mantenimiento de los equipos en la clínica, son dos ejemplos de cesión de datos personales a terceros. Se entiende como terceros: encargados de tratamiento. Aun teniendo el registro de actividades de tratamiento, se debe establecer una relación con dichas empresas externas que son proveedoras de ciertos servicios y tener consciencia asegurando que sigan la normativa de protección de datos. Es común que los hospitales y clínicas recurran con frecuencia al software de gestión de pacientes. Se debe tener muy en cuenta los aspectos técnicos de dicho software como dónde y de qué forma almacena y procesa los datos personales, más todavía si es un SaaS (basado en la nube). Por esta razón, es importante aclarar con los proveedores de software y de TI (tecnologías de información) cual va a ser la forma en la que dichos sistemas van a adaptarse a la normativa actual. Respecto a los datos que las páginas web de este tipo de entidades recopilan, destacar que los pacientes en todo momento deben saber qué datos se están almacenando. Por lo que se tendrá que firmar un contrato de encargo de tratamiento de datos donde se establezcan cuáles son las responsabilidades y obligaciones de dichos terceros para la protección de datos personales.

RECUERDA - El contrato debe incluir la siguiente información:

8. Obligaciones del encargado y responsable del tratamiento de datos
9. Categorías de interesados
10. Objetivo de realizar esta cesión
11. Información personal a la que se tendrá acceso
12. Plazo mínimo de conservación de los datos
13. Duración prevista del tratamiento
14. Completa identificación del tercero al que se le cederán los datos

Políticas de privacidad

¿Qué es? Recoge los datos del usuario o cliente en un documento legal que explica como la entidad los maneja, procesa y retiene. Se suele aplicar a sitios de internet. Se puede interpretar

como una especia de contrato donde la organización se compromete a guardar los datos personales del usuario. La principal responsabilidad del usuario es leerla y cerciorarse de que no se apliquen ciertas condiciones por las cuales se pueda propiciar una violación de privacidad como podría ser una transferencia de información del usuario.

¿Para qué sirve? Su principal función es la de comunicar a los usuarios del sitio web al que acceden que categoría de datos es la que se va a recopilar durante la visita. Además de informar sobre la finalidad con la que se van a utilizar y si se van a poder actualizar, cancelar o modificar. Es decir, se asegura que los usuarios conocen el fin específico para el cual sus datos van a ser recogidos y que se hará tras aprobar su consentimiento, consiguiendo así proteger su privacidad. Tener en cuenta que los datos recopilados no podrán ser cedidos a terceros.

¿Qué se debe incluir en la política de privacidad? Se debe redactar una política detallada y clara, además de entendible, la información que se detalla debe ser comprensible en todo momento para cualquier tipo de perfil que quiera informarse sobre esta, ya que para poder realizar el seguimiento de los datos de los usuarios se debe obtener el previo consentimiento. El esquema inferior, detalla algunos de los puntos los cuales sería interesante que recopilara la política de privacidad:

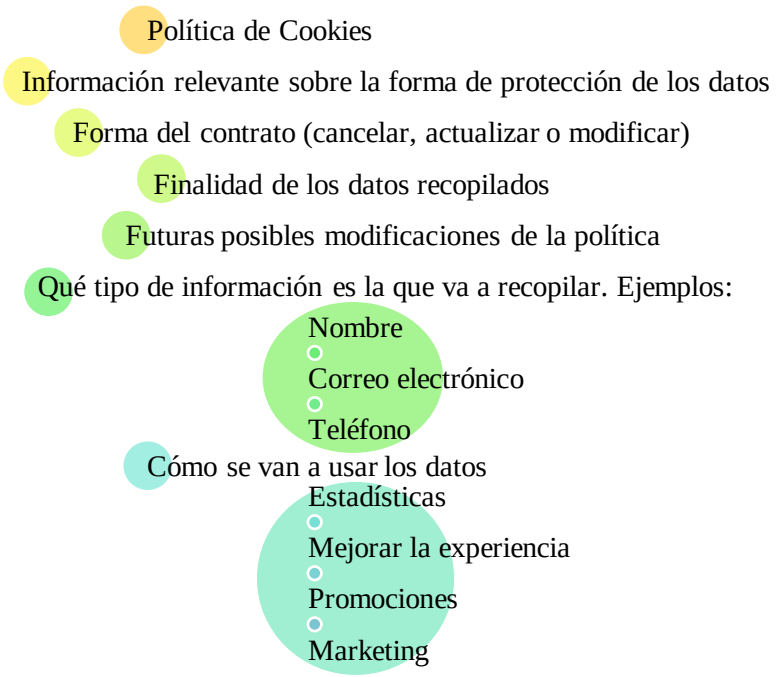


Ilustración 16. Puntos importantes en el desarrollo de la Política de Privacidad. Fuente: elaboración propia

Conseguir cumplir los objetivos de la Política de Privacidad en un hospital o centro sanitario es laborioso ya que las distintas fuentes de las cuales se captan los datos son diferentes (hospitalización, urgencias, consultas, etc.) Por ello es de vital importancia que el completo personal del hospital o centro médico esté totalmente concienciado sobre la importancia de este tema. El paciente de un centro sanitario debe en primer lugar recibir y firmar, una política de privacidad correctamente detallada. Se debe tener en cuenta que al centro sanitario u hospital en cualquier momento se le puede pedir una demostración de su cumplimiento con esta obligación, por ello, será necesario que dicha organización o entidad deberá implantar y revisar un proceso de captación y almacenamiento de dicha documentación.

¡IMPORTANTE! - Se recalca que siempre que se aporte la total garantía de que la firma del documento no haya podido ser manipulada se podrá realizar dicha acción en formato electrónico o en su defecto escanear los consentimientos firmados.

Sanciones

Las sanciones RGPD para médicos se aplican en función de diversos criterios:

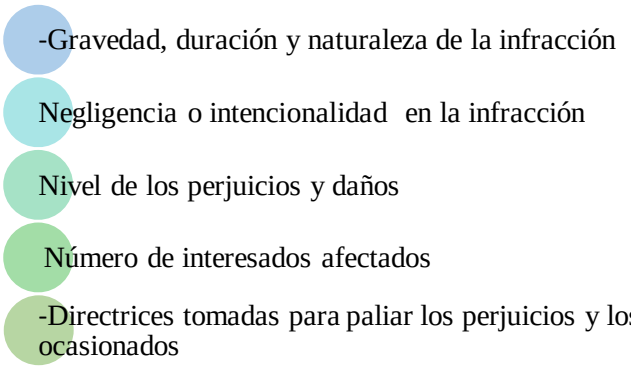


Ilustración 17. Criterios para determinar las sanciones. Fuente: elaboración propia

Sanciones por tratar datos especialmente protegidos: en un principio el tratamiento de datos sensibles no sería motivo de sanción ya que normalmente se cuenta con el consentimiento expreso de las personas interesadas. En el caso contrario, en el cual se recopilen o se traten datos sensibles sin la legitimación jurídica o sin el consentimiento para ellos, se estará cometiendo una infracción clasificada como muy grave por la LOPDGDD, la cual implica una sanción cuya multa oscila entre los 300.0001 euros y los 20 millones de euros.

Sanciones por no cumplir el deber de secreto: el Código Penal detalla en el artículo 199:

> «El que revele secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses».
>
> «El profesional que, con incumplimiento de su obligación de silencio, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años».

Sanciones si no se notifica la brecha adecuadamente: el hecho de no comunicar las brechas de seguridad que se han podido producir es catalogado como una infracción grave y las multas podrían a llegar a alcanzar los 10 millones de euros o el 2% del volumen de negocio de la entidad aplicada al ejercicio anterior.

8. ANEXO 2 – DESCRIPCIÓN DEL MARCO LEGAL

Artículos 9.1, 9.2, 10, 13, 14, 17, Considerandos: 51, 53, 71, 81 del RGPD

Artículo 9. Tratamiento de categorías especiales de datos personales

1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida o las orientaciones sexuales de una persona física.

2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

    a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;
    b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;
    c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;
    d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;
    e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;
    f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;
    g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser

proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;

h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;

i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional,

j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

Artículo 10. Tratamiento de datos personales relativos a condenas e infracciones penales

El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas sobre la base del artículo 6, apartado 1, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas.

Artículo 13. Información que deberá facilitarse cuando los datos personales se obtengan del interesado

1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

    a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;
    b) los datos de contacto del delegado de protección de datos, en su caso;

c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;
e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;
b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;
d) el derecho a presentar una reclamación ante una autoridad de control;
e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;
f) la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.

4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información.

Artículo 14. Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado

1. Cuando los datos personales no se hayan obtenidos del interesado, el responsable del tratamiento le facilitará la siguiente información:
    a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;
    b) los datos de contacto del delegado de protección de datos, en su caso;
    c) los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento;
    d) las categorías de datos personales de que se trate;
    e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
    f) en su caso, la intención del responsable de transferir datos personales a un destinatario en un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de ellas o al hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente respecto del interesado:

    a) el plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo;
    b) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable del tratamiento o de un tercero;
    c) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, y a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
    d) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basada en el consentimiento antes de su retirada;
    e) el derecho a presentar una reclamación ante una autoridad de control;
    f) la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público;
    g) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. El responsable del tratamiento facilitará la información indicada en los apartados 1 y 2:

a) dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos;
b) si los datos personales han de utilizarse para comunicación con el interesado, a más tardar en el momento de la primera comunicación a dicho interesado, o
c) si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.

4. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de los datos personales para un fin que no sea aquel para el que se obtuvieron, proporcionará al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y cualquier otra información pertinente indicada en el apartado 2.

5. Las disposiciones de los apartados 1 a 4 no serán aplicables cuando y en la medida en que:

a) el interesado ya disponga de la información;
b) comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, a reserva de las condiciones y garantías indicadas en el artículo 89, apartado 1, o en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información;
c) la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado, o
d) cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza estatutaria.

Artículo 17. Derecho de supresión («el derecho al olvido»)

1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:

a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;

b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;
c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;
d) los datos personales hayan sido tratados ilícitamente;
e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;
f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.

2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

3. Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario:

a) para ejercer el derecho a la libertad de expresión e información;
b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;
c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;
d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer

imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o

e) para la formulación, el ejercicio o la defensa de reclamaciones.

Artículo 36. Consulta previa

2. Cuando la autoridad de control considere que el tratamiento previsto a que se refiere el apartado 1 podría infringir el presente Reglamento, en particular cuando el responsable no haya identificado o mitigado suficientemente el riesgo, la autoridad de control deberá, en un plazo de ocho semanas desde la solicitud de la consulta, asesorar por escrito al responsable, y en su caso al encargado, y podrá utilizar cualquiera de sus poderes mencionados en el artículo 58. Dicho plazo podrá prorrogarse seis semanas, en función de la complejidad del tratamiento previsto. La autoridad de control informará al responsable y, en su caso, al encargado de tal prórroga en el plazo de un mes a partir de la recepción de la solicitud de consulta, indicando los motivos de la dilación. Estos plazos podrán suspenderse hasta que la autoridad de control haya obtenido la información solicitada a los fines de la consulta.

Considerando 51

(51) Especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales.

Debe incluirse entre tales datos personales los datos de carácter personal que revelen el origen racial o étnico, entendiéndose que el uso del término «origen racial» en el presente Reglamento no implica la aceptación por parte de la Unión de teorías que traten de determinar la existencia de razas humanas separadas.

El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física.

Tales datos personales no deben ser tratados, a menos que se permita su tratamiento en situaciones específicas contempladas en el presente Reglamento, habida cuenta de que los Estados miembros pueden establecer disposiciones específicas sobre protección de datos con objeto de adaptar la aplicación de las normas del presente Reglamento al cumplimiento de una obligación legal o al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

Además de los requisitos específicos de ese tratamiento, deben aplicarse los principios generales y otras normas del presente Reglamento, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento.

Se deben establecer de forma explícita excepciones a la prohibición general de tratamiento de esas categorías especiales de datos personales, entre otras cosas cuando el interesado dé su consentimiento explícito o tratándose de necesidades específicas, en particular cuando el tratamiento sea realizado en el marco de actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales.

Considerando 53

(53) Las categorías especiales de datos personales que merecen mayor protección únicamente deben tratarse con fines relacionados con la salud cuando sea necesario para lograr dichos fines en beneficio de las personas físicas y de la sociedad en su conjunto, en particular en el contexto de la gestión de los servicios y sistemas sanitarios o de protección social, incluido el tratamiento de esos datos por las autoridades gestoras de la sanidad y las autoridades sanitarias nacionales centrales con fines de control de calidad, gestión de la información y supervisión general nacional y local del sistema sanitario o de protección social, y garantía de la continuidad de la asistencia sanitaria o la protección social y la asistencia sanitaria transfronteriza o fines de seguridad, supervisión y alerta sanitaria, o con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, basados en el Derecho de la Unión o del Estado miembro que ha de cumplir un objetivo de interés público, así como para estudios realizados en interés público en el ámbito de la salud pública.

Por tanto, el presente Reglamento debe establecer condiciones armonizadas para el tratamiento de categorías especiales de datos personales relativos a la salud, en relación con necesidades específicas, en particular si el tratamiento de esos datos lo realizan, con fines relacionados con la salud, personas sujetas a la obligación legal de secreto profesional.

El Derecho de la Unión o de los Estados miembros debe establecer medidas específicas y adecuadas para proteger los derechos fundamentales y los datos personales de las personas físicas.

Los Estados miembros deben estar facultados para mantener o introducir otras condiciones, incluidas limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud.

No obstante, esto no ha de suponer un obstáculo para la libre circulación de datos personales dentro de la Unión cuando tales condiciones se apliquen al tratamiento transfronterizo de esos datos.

Considerando 71

(71) El interesado debe tener derecho a no ser objeto de una decisión, que puede incluir una medida, que evalúe aspectos personales relativos a él, y que se base únicamente en el tratamiento automatizado y produzca efectos jurídicos en él o le afecte significativamente de modo similar, como la denegación automática de una solicitud de crédito en línea o los servicios de contratación en red en los que no medie intervención humana alguna.

Este tipo de tratamiento incluye la elaboración de perfiles consistente en cualquier forma de tratamiento de los datos personales que evalúe aspectos personales relativos a una persona física, en particular para analizar o predecir aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el

comportamiento, la situación o los movimientos del interesado, en la medida en que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

Sin embargo, se deben permitir las decisiones basadas en tal tratamiento, incluida la elaboración de perfiles, si lo autoriza expresamente el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento, incluso con fines de control y prevención del fraude y la evasión fiscal, realizada de conformidad con las reglamentaciones, normas y recomendaciones de las instituciones de la Unión o de los órganos de supervisión nacionales y para garantizar la seguridad y la fiabilidad de un servicio prestado por el responsable del tratamiento, o necesario para la conclusión o ejecución de un contrato entre el interesado y un responsable del tratamiento, o en los casos en los que el interesado haya dado su consentimiento explícito.

En cualquier caso, dicho tratamiento debe estar sujeto a las garantías apropiadas, entre las que se deben incluir la información específica al interesado y el derecho a obtener intervención humana, a expresar su punto de vista, a recibir una explicación de la decisión tomada después de tal evaluación y a impugnar la decisión.

Tal medida no debe afectar a un menor.

A fin de garantizar un tratamiento leal y transparente respecto del interesado, teniendo en cuenta las circunstancias y contexto específicos en los que se tratan los datos personales, el responsable del tratamiento debe utilizar procedimientos matemáticos o estadísticos adecuados para la elaboración de perfiles, aplicar medidas técnicas y organizativas apropiadas para garantizar, en particular, que se corrigen los factores que introducen inexactitudes en los datos personales y se reduce al máximo el riesgo de error, asegurar los datos personales de forma que se tengan en cuenta los posibles riesgos para los intereses y derechos del interesado y se impidan, entre otras cosas, efectos discriminatorios en las personas físicas por motivos de raza u origen étnico, opiniones políticas, religión o creencias, afiliación sindical, condición genética o estado de salud u orientación sexual, o que den lugar a medidas que produzcan tal efecto.

Las decisiones automatizadas y la elaboración de perfiles sobre la base de categorías particulares de datos personales únicamente deben permitirse en condiciones específicas.

Considerando 81

(81) Para garantizar el cumplimiento de las disposiciones del presente Reglamento respecto del tratamiento que lleve a cabo el encargado por cuenta del responsable, este, al encomendar actividades de tratamiento a un encargado, debe recurrir únicamente a encargados que ofrezcan suficientes garantías, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del presente Reglamento, incluida la seguridad del tratamiento.

La adhesión del encargado a un código de conducta aprobado o a un mecanismo de certificación aprobado puede servir de elemento para demostrar el cumplimiento de las obligaciones por parte del responsable.

El tratamiento por un encargado debe regirse por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros que vincule al encargado con el responsable, que fije el objeto y la duración del tratamiento, la naturaleza y fines del tratamiento, el tipo de datos personales y las categorías de interesados, habida cuenta de las funciones y responsabilidades específicas del encargado en el contexto del tratamiento que ha de llevarse a cabo y del riesgo para los derechos y libertades del interesado.

El responsable y el encargado pueden optar por basarse en un contrato individual o en cláusulas contractuales tipo que adopte directamente la Comisión o que primero adopte una autoridad de control de conformidad con el mecanismo de coherencia y posteriormente la Comisión.

Una vez finalizado el tratamiento por cuenta del responsable, el encargado debe, a elección de aquel, devolver o suprimir los datos personales, salvo que el Derecho de la Unión o de los Estados miembros aplicable al encargado del tratamiento obligue a conservar los datos.

9. ANEXO 3 – 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**
Fin de la pobreza.				**x**
Hambre cero.				**x**
Salud y bienestar.	**x**			
Educación de calidad.		**x**		
Igualdad de género.				**x**
Agua limpia y saneamiento.				**x**
Energía asequible y no contaminante.				**x**
Trabajo decente y crecimiento económico.	**x**			
Industria, innovación e infraestructuras.				**x**
Reducción de las desigualdades.				**x**
Ciudades y comunidades sostenibles.				**x**
Producción y consumo responsables.				**x**
Acción por el clima.				**x**
Vida submarina.				**x**
Vida de ecosistemas terrestres.				**x**
Paz, justicia e instituciones sólidas.				**x**
Alianzas para lograr objetivos.				**x**

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

De los anteriores objetivos de desarrollo sostenibles mencionados, el proyecto relacionado está relacionado con:

- Salud y Bienestar

Personalmente creo que es un trabajo el cual contribuye firmemente a la mejora de lo que respecta en la salud y el bienestar de los posibles afectados, ya que la temática principal de este trabajo de fin de grado es mejorar la puesta en práctica de los procedimientos necesarios de la legislación actual en centros sanitarios, relacionados con los datos sensibles sobre la salud de los involucrados.

- Trabajo decente y crecimiento económico

También tiene relación con el trabajo decente ya que reconoce las figuras responsables en protección de datos y promueve que se realicen los procedimientos involucrados de forma óptima. Por ello, al reconocer estas figuras se contribuye al crecimiento económico ya que fomenta puestos de trabajo especializados en protección de datos.

- Educación de calidad.

A su vez, en su justa medida a través de la promulgación de contenido lícito y de interés para aquellos profesionales que estén involucrados en los procedimientos de protección de datos sanitarios, incluyendo perfiles menos especializados en el tema, contribuye a una educación de calidad.

10. GLOSARIO

Ataque DDOS: Ataque de Denegación de Servicio Distribuido (DDoS), mediante el cual las peticiones son enviadas, de forma coordinada entre varios equipos, que pueden estar siendo utilizados para este fin sin el conocimiento de sus legítimos dueños [3].

Autoridad de Control: cada Estado miembro establecerá que sea responsabilidad de una o varias autoridades públicas independientes supervisar la aplicación del Reglamento, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión [6].

Base de Datos *cloud*: las bases de datos en la nube son una nueva modalidad de almacenamiento que difieren de las bases tradicionales. A diferencia de estas, las bases de datos en *cloud* no se almacenan en un equipo o sistema local, sino que se ejecuta desde la infraestructura de un proveedor de servicios [21].

Carta de derechos digitales: Sin tener carácter normativo, esta Carta ofrece un marco de referencia para garantizar los derechos de la ciudadanía en la nueva realidad digital y tiene como objetivo reconocer los retos que plantea la adaptación de los derechos actuales al entorno virtual y digital [17].

Códigos deontológicos: un código deontológico es un documento que incluye un conjunto más o menos amplio de criterios, apoyados en la deontología con normas y valores que formulan y asumen quienes llevan a cabo correctamente una actividad profesional. Los códigos deontológicos se ocupan de los aspectos éticos del ejercicio de la profesión que regulan. Estos códigos cada vez son más frecuentes en otras actividades.

Confidencialidad: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. (RD 3/2010, de 8 de enero) y (UNE 71504).

Crackers: ciberdelincuentes.

Debida diligencia: El término diligencia debida se emplea para conceptos que impliquen la investigación de una empresa o persona previa a la firma de un contrato o una ley con cierta diligencia de cuidado. Puede tratarse de una obligación legal, pero el término comúnmente es más aplicable a investigaciones voluntarias.

Fichero: «todo conjunto organizado de datos de carácter personal, independiente de cómo se haya realizado su creación, almacenamiento, organización y acceso, funcional o geográfica y de forma centralizada o descentralizada» adaptado de (art. 3 LO 15/1999, de 13 de diciembre), (art. 4 RGPD) y (Chicano Tejada, 2014).

Ingeniería social: La ingeniería social es la práctica ilegítima de obtener información confidencial a través de la manipulación de usuarios legítimos. Es un conjunto de técnicas que pueden usar ciertas personas para obtener información, acceso o permisos en sistemas de información que les permitan realizar daños a la persona u organismo comprometidos y es utilizado en diversas formas de estafas y suplantación de identidad. El principio que sustenta la ingeniería social es el de que, en cualquier sistema, los usuarios son el «eslabón débil».

Malware: «software malicioso» es un término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas.

Mercadotecnia directa: el marketing directo o mercadotecnia directa consiste en tener una comunicación promocional directa con el público objetivo. Usualmente se envía información de la empresa, producto o servicio que sea de interés para el consumidor [20].

Phishing: es el delito de engañar a las personas para que compartan información confidencial como contraseñas y números de tarjetas de crédito.

Ransomware: es un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos.

SaaS: El software como servicio (SaaS) es un modelo de distribución y de licencias usado para entregar aplicaciones de software a través de Internet, es decir, como un servicio [19].

Sistema de gestión de la seguridad de la información (SGSI). «Sistema de gestión que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos» (RD 3/2010, de 8 de enero).

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).