POSICIONAMIENTO 2 DE SEDISA

ADAPTACIÓN AL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS PARA EL SECTOR SANITARIO

Mayo 2018

sedisa
sociedad española de directivos de la salud

Edita y distribuye:

sedisa
sociedad española de directivos de la salud

C/ José Silva, 3 - 1°A. 28043 Madrid

www.sedisa.net

POSICIONAMIENTO 2 DE SEDISA
ADAPTACIÓN AL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS PARA EL SECTOR SANITARIO

Mayo 2018

Coordinadora:
Carmen Pérez Canal

Autores:
Carmen Pérez Canal
Rosario Heras Carrasco
Andrés Calvo Medina

Contenidos

1 Introducción

La Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (la Directiva), con más de 20 años de existencia, ha sido sustituida por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en los que respecta al tratamiento se datos personales y a la libre circulación de estos datos (RGPD), en vigor desde mayo de 2016 y plenamente aplicable a partir de 25 de mayo de 2018.

"La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos de carácter personal. La magnitud de la recogida y el intercambio de datos personales han aumentado de manera significativa. La tecnología permite que tanto las empresas como las autoridades públicas utilicen datos personales a una escala sin precedentes a la hora de realizar sus actividades. Las personas fiscas difunden un volumen cada vez mayor de información personal a escala mundial" (Considerando número 6 del Reglamento (UE) 2016/679)

Continua en el Considerando número 7:

"Estos avances requieren un marco más sólido y coherente para la protección de datos en la Unión Europea … Las personas físicas deben tener el control de sus propios datos personales"

El RGPD supone una importante revisión del marco legal de la protección de Datos en la Unión Europea, siendo las características principales su intención armonizadora de las normas sobre esta materia en los Estados de la Unión Europea, su aplicación directa sin ninguna norma estatal interpuesta y el reforzamiento de la seguridad jurídica y la transparencia.

La Ley Orgánica de Protección de Datos (LOPD) y el Real Decreto 1720/2007, de 21 de diciembre por el que se aprueba el Reglamento de desarrollo de la LOPD (RDLOPD) planteaban un modelo declarativo donde el primer paso para llevar a cabo un tratamiento se basaba en la declaración del fichero que iba a contener los datos de los interesados a la autoridad de control, por otro lado el Título VIII del RDLOPD planteaba una batería de controles mínimos para garantizar la seguridad de los datos. Frente a este planteamiento el RGPD plantea un modelo de autoanálisis que se inicia de manera previa a la puesta en marcha de un tratamiento de datos y que continúa durante todo el ciclo de vida del tratamiento, podría decirse que esta nueva norma implica un nuevo modelo de cumplimiento y también un nuevo modelo de gobernanza de los tratamientos que debe permitir a quienes ostentan responsabilidades en los tratamientos de datos personales, la capacidad de poder rendir cuentas en todo momento sobre las decisiones que hubieran tomado, los motivos que les llevaron a ello y de poderlo acreditar documentalmente.

Por tanto, el RGPD supone un cambio importante en el concepto de modelo de privacidad, pasando de la gestión de los datos al gobierno responsable de la información, de una actividad reactiva y de cumplimiento a una actitud proactiva, de anticipación y prevención, lo que se conoce como **Responsabilidad Proactiva**.

Este principio de responsabilidad activa no se limita únicamente a los responsables y encargados de los tratamientos, engloba a todas aquellas personas que se encuentran implicadas en un tratamiento de datos a lo largo de todo su ciclo de vida. La posición proactiva frente a los tratamientos de datos personales corresponde a todo el personal de una organización quienes deben ser conscientes de su responsabilidad a fin de garantizar el derecho fundamental a la protección de datos por lo que, el factor de concienciación es fundamental para llevar a cabo esta proactividad por parte de todas aquellas personas que están implicadas en los tratamientos de datos personales.

El RGPD mantiene el concepto de dato personal en los mismos términos que hacía la Directiva, como toda información sobre una persona física identificada o identificable, por tanto, toda persona cuya identidad pueda determinarse directa o indirectamente, que puede ser mediante un identificador como es el nombre, un número de identificación, datos de localización, un identificador en línea, o elementos de identidad física, fisiológica, genética, psíquica, económica, cultural o social de la persona.

En las "*categorías especiales de datos*" se exigen mayores garantías en el tratamiento, destacar la definición de "datos relativos a la salud" como los datos personales relativos a la salud física o mental, incluida la prestación de servicios de atención sanitaria que revelen información sobre su estado de salud y se incorporan las categorías de datos genéticos y los datos biométricos.

Se refuerza el consentimiento, el ciudadano propietario de sus datos aparece en primera línea en el control de su información, incorporando nuevos derechos a los ya consolidados, se amplía el contenido de la información que se debe facilitar a las personas, se refuerza el derecho de acceso con el derecho de portabilidad, al derecho de supresión se añade el derecho al olvido y el derecho a la limitación del tratamiento y el de oposición se amplía con el derecho de oposición a no ser objeto de decisiones individualizadas.

El enfoque de la protección de datos está basado en conocer el riesgo que supone el tratamiento de datos, para los derechos y libertades de las personas. Este análisis de riesgos se realiza teniendo en cuenta la naturaleza de los datos y los riesgos a los que están expuestos con referencia al volumen y el estado de la tecnología y como consecuencia de este proceso, disponer de mecanismos de seguridad, de medidas técnicas y organizativas apropiadas para garantizar la protección. Para ello el Reglamento incorpora un modelo de mayor responsabilidad y exige medidas como son desde el inicio, la protección de datos desde el diseño o las evaluaciones de impacto, de continuidad, con la incorporación obligatoria de la figura del Delegado de protección de datos en organizaciones como las Administraciones Públicas y los hospitales, el mantenimiento de registros de actividad de tratamiento, novedades como la notificaciones de las violaciones de seguridad, un régimen de sanciones más severo y otras medidas correctivas como son, apercibimientos, advertencias u ordenar determinadas actividades y operaciones que suponen alternativas a las multas y ofrece la posibilidad de valorar mejor el desarrollo y el cumplimiento de una organización en protección de datos y por último, desaparecen obligaciones como son la inscripción de ficheros o la de iniciar los tratamientos de las AAPP mediante una disposición general.

Se fortalece la protección de datos con un sistema de calidad que facilite y oriente la implantación y demuestre el cumplimiento con fórmulas como son los códigos de conducta y la creación de certificaciones, de sellos y marcas de protección de datos.

En definitiva, el Reglamento supone un mayor compromiso de las organizaciones, públicas o privadas, con la protección de datos y por tanto de todos aquellos centros que tienen como fin último la atención sanitaria.

2 Situación actual de los hospitales

El 26 de septiembre de 2017 la AEPD publicó en su página web el "Plan de inspección sectorial de oficio a los hospitales públicos". En este documento contiene las deficiencias detectadas así como una serie de recomendaciones a tener en cuenta para poder subsanarlas, además su contenido permite a cualquier hospital revisar cuál es su nivel de adaptación a la normativa de protección de datos.

Aunque el documento refleja la fotografía obtenida por la AEPD de los hospitales públicos, con cierta seguridad, los hospitales privados también pueden ver reflejada su situación en el mismo. Es por ello que los Directivos que dirigen los hospitales, público y/o privados, así como cualquier centro sanitario deben tener en cuenta el informe para emprender acciones que les permita adaptar sus organizaciones a lo que dispone el nuevo RGPD.

Asimismo es importante añadir que, aunque se han detectado deficiencias, los hospitales tienen mucho trabajo avanzado para estar en disposición de cumplir con el principio de responsabilidad proactiva así como en materia de seguridad de la información; la única cuestión a tener en cuenta es que deben adaptar lo ya existente a las nuevas exigencias, así por ejemplo las medidas de seguridad implantadas son válidas en la medida que den respuesta al **análisis de riesgos** que debe realizar el hospital y sobre cuyo resultado podrán ser ampliadas o modificadas para ajustarlas al riesgo detectado.

En el informe son muchas las deficiencias detectadas sin embargo sólo van a reflejarse las que se consideran más significativas:

- **Calidad de datos,** hace referencia a que el hospital no verifica la identidad del paciente al que se va a prestar asistencia sanitaria, es decir no solicita un documento de identidad junto a la tarjeta sanitaria.
- **Cancelación y borrado de datos** porque no tienen previsto un protocolo para hacerlo efectivo aunque se contempla que el hospital debe conservar la documentación clínica el tiempo necesario para prestar asistencia al paciente y como mínimo cinco años desde la fecha de alta de cada proceso asistencial. No obstante, los hospitales antes de cancelar o borrar datos personales deben tener en cuenta lo que establece cada Comunidad Autónoma al respecto.
- **Información** por falta de carteles informativos en las áreas donde se recaban los datos personales como en Urgencias o Admisión.
- **Falta de información a los pacientes sobre los derechos** que les reconoce la legislación en protección de datos personales.
- **Deber de secreto,** porque no siempre existen normas internas que informen a todos los empleados (personal sanitario, administrativos, ordenanzas o estudiantes) de la obligación que tienen de preservar la confidencialidad de los datos de los pacientes a los que acceden.
- **Derecho de acceso** porque en algunas ocasiones el paciente no puede utilizar un método sencillo y gratuito para tener acceso a su historia clínica.
- No se contempla la posibilidad de que el paciente ingresado se oponga a que el hospital facilite a terceros información sobre la dependencia del hospital donde se encuentra.
- **Prestación de servicios** porque no están reguladas en un contrato adecuado a la normativa de protección de datos.

- **Medidas de seguridad.** Este apartado es el que ha arrojado mayor número de deficiencias, por citar algunas estaría la falta de procedimientos de gestión de incidencias, falta de limitación en el acceso a la historia clínica para algunos perfiles profesionales o permitir el acceso a datos que exceden de lo necesario para su puesto de trabajo, falta de control en el número de intentos para acceder a la historia clínica o aplicaciones que no exigen cambio de contraseña en el primer inicio de sesión así como la posibilidad de visualizar las contraseñas almacenadas. También destacan deficiencias en cuanto a la gestión de las historias clínicas en soporte papel sobre todo en lo relacionado con su traslado y custodia, ya que se realiza sin la debida diligencia para impedir que terceros accedan a la información o incluso se pierdan.

  Respecto de las medidas de seguridad es importante recordar que los hospitales públicos deben cumplir con el Esquema Nacional de Seguridad (ENS) que establece las medidas de seguridad a implantar. Para su gestión y cumplimiento disponen de una herramienta, PILAR, que ha sido actualizada incorporando los riesgos de cumplimiento del RGPD con la finalidad de que las Administraciones Públicas cumplan con la obligación de realizar un análisis de riesgos teniendo en cuenta los derechos y libertades de las personas.

El documento hace una referencia especial a la Historia Clínica y a que sólo puedan acceder a la misma las personas autorizadas pero…

¿Quién puede acceder a la Historia Clínica?

- **Asistencia sanitaria:** Según el artículo 16, apartados 1,4 y 6 de la Ley 41/2002:
  - *Profesionales asistenciales* del centro que realizan el diagnostico o el tratamiento del paciente.
  - *Personal de administración y gestión* de los centros sanitarios, acceso relacionado con sus funciones.
  - *El paciente o su representante* autorizado y acreditado
  - *Paciente fallecido* (artículo 18, 4 de la ley 41/2002):
    - *Personas vinculadas por razones familiares* o, de hecho, salvo que el paciente fallecido haya dejado constancia de su negativa.
    - También puede acceder a la historia clínica de un fallecido, un *tercero* justificado por a un riesgo para su salud, aunque se limitará a los datos necesarios y pertinentes.

El *Acceso a la Historia Clínica Digital del Sistema Nacional de Salud* (HCDSNS) garantiza el acceso por vía telemática a un conjunto de datos clínicos, *Historia Clínica Resumida*, en la red de centros pertenecientes al Sistema Nacional de Salud; este acceso es posible para los ciudadanos a sus propios datos y los profesionales sanitarios para asistencia sanitaria del paciente. Su legitimación se basa en la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud, artículo 56 y la Ley 41/2002 se 14 de noviembre, básica reguladora de la autonomía del paciente, en su disposición adicional tercera, dirigen al ministerio de sanidad, Servicios Sociales e Igualdad, el mandato de coordinar los mecanismos de intercambio electrónico de información clínica y salud individual para permitir el acceso profesionales y usuarios en los términos estrictamente necesarios para garantizar la calidad de la asistencia y la confidencialidad e integridad de la información.

- **Otros usos y accesos:** a la Historia Clínica, contemplados en el artículo 16,3 de la Ley 41/2002:
  - Docencia: consentimiento o disociación. Tener en cuenta la Orden SSI/81/2017 de 19 de enero Del Ministerio de Sanidad, Servicios Sociales e Igualdad.
  - Investigación: se requiere consentimiento previo del paciente o disociación (separar los datos personales de los clínicos).
  - Epidemiología: Consentimiento o disociación (datos de identificación personal separados de los datos clínicos).

  Excepto en situaciones de necesidad para la prevención de un riesgo o peligro grave para la salud de la población, las Administraciones

sanitarias podrán acceder a la identificación de los pacientes por razones epidemiológicas o de protección de la salud pública. (artículo 16, 3 Ley 41/2002, después de la modificación por la Ley 33/2011 General de salud Pública).

- Judicial. Se necesita el consentimiento del paciente o separar los datos de identificación personal de los datos clínico-asistenciales.
  Excepto el supuesto de investigación judicial que se estará a lo que dispongan los jueces y tribunales en el procedimiento correspondiente, limitado a los fines especifico de cada caso.

- **Inspección, evaluación, acreditación y planificación,** (artículo 16,5 Ley 41/2002) personal sanitario acreditado en sus funciones de Administración sanitaria.
  En todos los casos existe obligación de deber de secreto (artículo 16, 6 Ley 41/2002).

3 La responsabilidad proactiva. Nuevo enfoque

El RGPD plantea un modelo de mejora continua encaminado a garantizar los derechos y libertades de las personas evitando la posibilidad de daños y perjuicios para los interesados que puedan llegar a materializarse, en definitiva se plantea un modelo proactivo que lleva asociada la obligación de responsables y encargados del tratamiento de estar en disposición de demostrar en todo momento que esta proactividad se está llevando con diligencia. En su versión inglesa, el RGPD utiliza el término **"accountability"** para describir esta proactividad de responsables y encargados del tratamiento pero carece de una traducción directa al castellano.

"Acountability" es un término heredado de la cultura empresarial anglosajona y refleja el compromiso del responsable de una entidad para con las acciones que toma en su organización, de manera que el responsable pueda facilitar en todo momento una explicación demostrable de los motivos que le llevaron a realizar determinadas acciones. De alguna manera puede decirse que el RGPD plantea líneas generales para abordar el cumplimiento dejando en manos de los responsables el detalle o la forma concreta de abordar dicho cumplimiento.

El RGPD es en resumen un nuevo modelo de cumplimiento donde son los propios responsables y encargados de los tratamientos quienes tienen que asumir la responsabilidad de decidir el marco de desarrollo de los tratamientos de datos personales que llevan a cabo, tomando decisiones que en todo momento permitan establecer garantías para los derechos y libertades de las personas, no se trata de fijar unas normas estáticas de cumplimiento sino más bien de asignar a responsables y encargados de los tratamientos la obligación de decidir acerca de aquellas medidas concretas que garanticen esos derechos y libertades de las personas cuyos datos están siendo tratados y, además, de llevar a cabo un proceso de mejora continua de aquellas medidas o mecanismos de garantía que hubieran sido implementados.

El RGPD plantea un modelo de cumplimiento basado en obligaciones generales que deben de adecuarse al caso específico de cada tratamiento y mediante las que responsables y encargados de los tratamientos pueden estar en condiciones de demostrar que los tratamientos se llevan a cabo de conformidad con el RGPD. Dichas obligaciones son:

1. Elaboración de un **registro de actividades de tratamiento** en el que se detallen los tratamientos que el responsable lleva a cabo.
2. Establecer medidas de **protección de datos desde el diseño** de los tratamientos, es decir, anticipar la protección de datos al desarrollo del tratamiento que vaya a ser necesario para la puesta en marcha de un producto o servicio. Es decir, cuando un hospital se plantea ofertar un nuevo servicio o producto, desde el momento "cero" debe tener en cuenta cómo va a afectar la puesta en marcha de ese servicio o producto a los derechos y libertades de sus pacientes y usuarios.
3. Fijar medidas de **protección de datos por defecto** o, en otros términos, garantizar al paciente

en todo momento su capacidad de decidir acerca de su información personal. En este apartado entrarían, por ejemplo, aquellas opciones que por defecto se implanten en un producto o servicio de forma que dichas opciones garanticen al interesado la posibilidad de decidir, en todo momento, sobre sus datos personales.

4. Realizar **evaluaciones de impacto** que permitan llevar a cabo un análisis de los riesgos para los derechos y libertades de las personas cuyos datos van a ser tratados y, en caso necesario, la realización de una **consulta previa** a la autoridad de control. Tanto las medidas de protección de datos desde el diseño como las medidas de protección de datos por defecto serán tenidas en cuenta a la hora de realizar una evaluación de impacto.
5. Obligación de notificar a la autoridad de control y a los interesados **las violaciones o brechas de seguridad**. Los responsables están obligados a notificar las brechas de seguridad a la autoridad de control en un plazo inferior a las 72 horas contado desde el momento en el que se tenga constancia de la misma exceptuando aquellos casos en los que dicha brecha de seguridad no suponga un riesgo para los derechos y libertades de las personas físicas.
6. Adoptar **códigos de conducta.** La gran ventaja de los códigos de conducta es que dan respuesta a las necesidades comunes de un determinado sector de actividad, como por ejemplo el sector sanitario. El compromiso de los responsables con un código de conducta sectorial puede quedar plasmado en documentos que permitan la trazabilidad de este compromiso, aspectos como por ejemplo, modelos de consentimiento o modelos de cláusulas informativas para los interesados pueden ser comunes a todo un sector, como por ejemplo el sanitario, facilitando el cumplimiento y proactividad de responsables.
7. Adoptar mecanismos de **certificación,** también puede ser un recurso para acreditar la proactividad de los responsables. La certificación siempre implica a un tercero que lleva a cabo la tarea de auditoría sobre un proceso o servicio en los que existe un tratamiento de datos personales y supone un grado de garantía adicional a la diligencia del responsable o del encargado del tratamiento.
8. Establecer **medidas técnicas y organizativas** que garanticen que el tratamiento de datos personales se lleva a cabo de acuerdo con lo previsto en el RGPD y en función del estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento para garantizar los riesgos para los derechos y libertades de las personas. Medidas que deben ser el resultado de un proceso objetivo, consciente, repetible y verificable por parte de los responsables y, en ningún caso, estar definidas en un checklist o lista fija de elementos.
9. Designar un **delegado de protección de datos** (DPD) sobre cuya figura recae el papel de supervisión y asesoramiento al responsable con relación al cumplimiento de estas obligaciones.

Sobre esta base el RGPD otorga a los responsables y encargados un marco flexible de cumplimiento que debe estar en constante adecuación y puesta al día con relación a los tratamientos que lleven a cabo o que hubiera sido previsto llevar a cabo. Así lo ponía de manifiesto el Grupo de Trabajo del artículo 29 (GT29) que reúne a las autoridades europeas de protección de datos en su declaración del 30 de mayo de 2014, frente a un modelo escalable basado en medidas de cumplimiento que finalmente se reducen a un "checklist", el nuevo modelo de cumplimiento permite a cada responsable adaptar la protección de los interesados en consonancia con su organización, el volumen de datos tratados o las especificidades concretas de cada caso, por lo tanto se trata de un modelo en el que los riesgos que implican los tratamientos deben ser tenidos en cuenta de forma específica para cada tratamiento y en el contexto de su propia evolución tecnológica u organizativa.

El RGPD es un modelo de cumplimiento orientado al riesgo de los tratamientos y con el objeti-

vo de salvaguardar el derecho fundamental a la protección de datos que recoge el Artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea, derecho que debe garantizarse con independencia de los riesgos que implique un tratamiento de datos. De acuerdo con este enfoque de riesgos y teniendo en cuenta la mencionada declaración del GT29, a la existencia de distintos riesgos debe dar lugar a escenarios de medidas distintos y a su vez a mecanismos de "accountability" diferentes con el objeto de poder acreditar en todo momento que se han establecido salvaguardas para este derecho fundamental.

La herramienta que plantea el RGPD para llevar a cabo esta adecuación específica y constante de cada tratamiento teniendo en cuenta el ámbito, contexto, alcance y objetivos de los mismos es el **enfoque de riesgos**. Los responsables tienen ahora la obligación de llevar a cabo un análisis de los riesgos implícitos a cada tratamiento, aplicar las medidas apropiadas para reducir los niveles de riesgo de los tratamientos a un mínimo aceptable, revisar la eficacia de las medidas implantadas para reducir los riesgos y disponer de capacidad para demostrar que el tratamiento es en todo momento acorde a las medidas previstas en el RGPD.

4 Delegado de Protección de Datos

El Delegado de Protección de Datos (DPD) es una figura nueva que nace con la aprobación del RGPD. Hasta esa fecha distintos profesionales estaban relacionados con el cumplimiento de la normativa de protección de datos: responsables de seguridad, CEO, consultores, auditores, pero ninguno de ellos con un perfil definido como el que exige el Reglamento al DPD.

El RGPD establece que el DPD será designado atendido a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones que le atribuye en el artículo 39.

Por tanto, el DPD, para poder ejercer, no tiene que disponer de ninguna titulación oficial ni certificación que acredite su cualificación profesional, sin embargo la Agencia Española de Protección de Datos ha optado por elaborar un Esquema de Certificación (EC) que regule esta profesión y que se encuentra publicado desde julio de 2017 en su página web: www.agpd.es. Es una manera de dar seguridad y valor al trabajo de estos profesionales y confianza a las empresas que necesitan contratarlo.

El Grupo de Trabajo del artículo 29 señala que el DPD es la piedra angular de la rendición de cuentas y que el nombramiento de un DPD puede facilitar el cumplimiento y, además, convertirse en una ventaja competitiva para las empresas. Es importante señalar que los DPD no son personalmente responsables en caso de incumplimiento del RGPD, el responsable o el encargado del tratamiento es quien está obligado a garantizar y ser capaz de demostrar que el tratamiento se realiza de conformidad con sus disposiciones.

Perfil

Dado lo genérico del perfil del DPD, en el EC se han identificado las áreas sobre las que tiene que tener conocimientos y habilidades para poder desempeñar adecuadamente sus funciones:

- Cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos
- Identificación de las bases jurídicas de los tratamientos
- Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos
- Determinación de la existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos
- Diseño e implantación de medidas de información a los afectados por los tratamientos de datos
- Establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados
- Valoración de las solicitudes de ejercicio de derechos por parte de los interesados
- Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado

- Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia
- Diseño e implantación de políticas de protección de datos
- Auditoría de protección de datos
- Establecimiento y gestión de los registros de actividades de tratamiento
- Análisis de riesgo de los tratamientos realizados
- Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos
- Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos
- Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados
- Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos
- Realización de evaluaciones de impacto sobre la protección de datos
- Relaciones con las autoridades de supervisión
- Implantación de programas de formación y sensibilización del personal en materia de protección de datos.

Funciones

La Agencia Española de Protección de Datos, siguiendo lo señalado en el RGPD, ha establecido en el EC las siguientes funciones que debe desempeñar el DPD:

a) Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;
b) Supervisar el cumplimiento de lo dispuesto en el Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales,
c) Supervisar la asignación de responsabilidades,
d) Supervisar la concienciación y formación del personal que participa en las operaciones de tratamiento
e) Supervisar las auditorías correspondientes;
f) Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos
g) Supervisar su aplicación de conformidad con el artículo 35 del Reglamento;
h) Cooperar con la autoridad de control;
i) Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y
j) Realizar consultas a la autoridad de control, en su caso, sobre cualquier otro asunto.

Capacitación

Para poder desempeñar sus funciones debe ser capaz de:

a) Recabar información para determinar las actividades de tratamiento,
b) Analizar y comprobar la conformidad de las actividades de tratamiento, e
c) Informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento.
d) Recabar información para supervisar el registro de las operaciones de tratamiento.
e) Asesorar en la aplicación del principio de la protección de datos por diseño y por defecto.
f) Asesorar sobre:
- si se debe llevar a cabo o no una evaluación de impacto de la protección de datos,

- qué metodología debe seguirse al efectuar una evaluación de impacto de la protección de datos,
- si se debe llevar a cabo la evaluación de impacto de la protección de datos con recursos propios o con contratación externa,
- qué salvaguardas (incluidas medidas técnicas y organizativas) aplicar para mitigar cualquier riesgo para los derechos e intereses de los afectados,
- si se ha llevado a cabo correctamente o no la evaluación de impacto de la protección de datos y
- si sus conclusiones (si seguir adelante o no con el tratamiento y qué salvaguardas aplicar) son conformes con el Reglamento.

g) priorizar sus actividades y centrar sus esfuerzos en aquellas cuestiones que presenten mayores riesgos relacionados con la protección de datos.

h) asesorar al responsable del tratamiento sobre:

- qué metodología emplear al llevar a cabo una evaluación de impacto de la protección de datos,
- qué áreas deben someterse a auditoría de protección de datos interna o externa,
- qué actividades de formación internas proporcionar al personal o los directores responsables de las actividades de tratamiento de datos y a qué operaciones de tratamiento dedicar más tiempo y recursos.

Recursos

Para poder desempeñar sus tareas, el responsable y encargado del tratamiento deben poner a su disposición distintos recursos, en el RGPD se recogen los siguientes:

- Garantizar que el DPD participa de forma adecuada y en tiempo en todas las cuestiones relativas a la protección de datos personales.
- Respaldarán al DPD en el desempeño de sus funciones
- Le facilitarán los recursos que necesite para ello
- Le permitirán el acceso a los datos personales y operaciones de tratamiento
- Le facilitarán formación para el mantenimiento de sus conocimientos
- Garantizarán que no recibe ninguna instrucción en lo que respecta al desempeño de sus funciones
- No puede ser destituido ni sancionado por desempeñar sus funciones
- El DPD rendirá cuentas al más alto nivel jerárquico del responsable o encargado

¿Quién debe nombrar un DPD?

- Administración u organismo público
- Responsables o encargados de tratamiento cuando sus actividades principales consistan en operaciones de tratamiento que requieran una observación habitual y sistemática de personas a gran escala. El Grupo de Trabajo del artículo 29 señala como ejemplo de tratamiento que requieran una observación habitual y sistemática el seguimiento de los datos de bienestar, estado físico y mental mediante dispositivos ponibles.
- Responsables o encargados de tratamiento cuando sus actividades principales consistan en tratamientos a gran escala de categorías especiales de datos personales. El Grupo de Trabajo del artículo 29 señala como ejemplo de tratamiento a gran escala el tratamiento de pacientes en el desarrollo de la actividad de un hospital y no considera tratamiento a gran escala el tratamiento de pacientes realizado por un solo médico

El tratamiento de datos relativos a salud, como historias clínicas de pacientes, debe considerarse una de las actividades principales de cualquier hospital y, por ello, los hospitales deben designar un DPD.

Además, es importante señalar que:

- Un grupo empresarial puede nombrar un único DPD siempre que cada establecimiento del grupo tenga fácil acceso al DPD

- En el caso de administración u organismo público, se podrá designar un único DPD para varias administraciones u organismos pero teniendo en cuenta su estructura organizativa y tamaño y sin olvidar las funciones que debe desempeñar
- El DPD podrá ser interno, en este caso el responsable o encargado debe garantizar que no se produzcan conflicto de intereses si opta por una persona que desempeñe otras funciones además de la de DPD
- Puede ser externo y desempeñar las funciones en el marco de un contrato de servicios

No olvidar que:

- El DPD es el punto de contacto entre el responsable o encargado del tratamiento y las personas cuyos datos tratan
- El responsable o encargado del tratamiento deben publicar los datos de contacto del DPD
- También deben comunicar estos datos a la AEPD

5 Principios

El RGPD establece que los datos personales deben ser tratados teniendo en cuenta los siguientes principios:

- **Licitud:** Solo se podrán tratar datos personales cuando se cuente con el consentimiento de la persona cuyos datos se van a tratar o cuando el tratamiento es necesario para:
  - la ejecución de un contrato
  - cumplir una obligación legal
  - proteger los intereses vitales de la persona
  - el cumplimiento de una misión realizada en interés público
  - satisfacer los intereses legítimos del responsable del tratamiento
- **Lealtad y transparencia:** Se debe facilitar a las personas cuyos datos se van a tratar, como mínimo, la siguiente información:
  - Identidad y datos de contacto del responsable
  - Datos de contacto del delegado de protección de datos
  - Fines del tratamiento
  - Base jurídica del tratamiento
  - Interés legítimo del que trata los datos
  - Posibilidad de revocar el consentimiento
  - Plazo del tratamiento
  - Destinatarios de los datos
  - Si se producen transferencias internacionales
  - Plazo de conservación cuando sea posible
  - Existencia del derecho a solicitar el acceso, rectificación, supresión, oposición, portabilidad o limitación del tratamiento así como del derecho a retirar el consentimiento
  - Derecho a presentar reclamación ante una autoridad de control
  - Existencia de decisiones automatizadas, incluida la elaboración de perfiles

Esta información se facilitará por escrito o por medios electrónicos, de forma concisa, transparente, inteligible y de fácil acceso. Se utilizará un lenguaje claro y sencillo, además siempre con carácter previo a la recogida de los datos, en textos informativos, carteles, impresos, cuestionarios, etc.

- **Limitación de la finalidad:** los datos serán recogidos con fines determinados, explícitos y legítimos y no pudiendo ser tratados ulteriormente de manera incompartible con dichos fines.
- **Minimización de los datos:** los datos serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
- **Exactitud:** los datos serán exactos y si fuera necesario, actualizados.
- **Delimitación del plazo de conservación:** los datos serán mantenidos por el tiempo necesario para los fines del tratamiento.
- **Integridad y confidencialidad:** los datos serán tratados de tal manera que se garantice una seguridad adecuada.
- **Principio de responsabilidad proactiva:** el responsable del tratamiento será responsable del cumplimento de lo dispuesto en el Reglamento y deberá demostrarlo.

6 Registro de actividades de tratamiento

A diferencia de la inscripción de ficheros, el registro de actividades plantea a los responsables la necesidad de revisar y mantenerlo actualizado, por lo que es necesario establecer medidas de concienciación para que todo el personal conozca dicho registro y la forma de realizar las modificaciones. Sobre la base de este registro el RGPD añade la necesidad de tener en cuenta, cuando sea posible, una descripción de las medidas de seguridad.

Además, es un registro que, a diferencia del registro de ficheros, debe elaborarlo el responsable del tratamiento y tenerlo a disposición de la AEPD cuando se lo solicite, pero desaparece la obligación de inscripción.

Debe constar por escrito y se admite de forma expresa en el RGPD el formato electrónico.

El RGPD establece la información que debe contener:

- Nombre y datos de contacto del responsable del tratamiento y del DPD
- Fines del tratamiento
- Descripción de las categorías de interesados
- Descripción de las categorías de datos personales
- Categorías de destinatarios a los que se comunicarán los datos personales
- Categorías de destinatarios en terceros países u organizaciones, en su caso
- Transferencias internacionales de datos personales a un tercer país u organizaciones, en su caso
- Plazos previstos de supresión de las categorías de datos personales cuando sea posible su determinación
- Descripción general de las medidas técnicas y organizativas de seguridad cuando sea posible

El encargado del tratamiento también debe llevar un registro de las categorías de actividades de tratamiento que realiza por cuenta de un responsable y el RGPD establece el contenido de dicho registro:

- Nombre y datos de contacto del encargado y de cada responsable por cuenta del que actúa
- Nombre y datos de contacto del DPD
- Categorías de tratamientos que efectúa por cuenta del responsable
- Transferencias internacionales de datos personales a un tercer país u organizaciones, en su caso
- Descripción general de las medidas técnicas y organizativas de seguridad cuando sea posible

El RGPD también regula que el encargado debe tener el registro de actividades de tratamiento a disposición de la autoridad de control.

Es importante señalar que, aunque no se encuentra dentro de la información que debe contener el registro de actividades, el identificar la base jurídica que regula el tratamiento que se está registrando es un aspecto a tener muy en cuenta por las implicaciones que va a tener en la implantación de las medidas a adoptar por parte de responsables y encargados para cumplir con el RGPD.

Aunque en un principio podría parecer que esta es una nueva actividad marcada por el RGPD, las organizaciones ya cuentan con un trabajo previo a partir del cual elaborar este registro, son los ficheros notificados al Registro General de Protección de Datos de la AEPD. Partiendo de dicha información se pueden extraer los tratamientos que se realizan e ir completando el resto de la información exigida para confeccionar los registro de actividades de tratamiento.

7 Legitimación del tratamiento

"*Para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento del interesado o sobre alguna otra base legitima establecida conforme a Derecho*". Considerando numero 40 RGPD.

El punto de partida para el tratamiento de datos personales es determinar la base jurídica que permite realizar lícitamente las distintas operaciones de tratamiento. Como ya se ha citado, el tratamiento se considera lícito si se da alguna de las siguientes condiciones:

Consentimiento

El Consentimiento lo define el RGPD, como una *manifestación de voluntad libre, especifica, informada e inequívoca por la que el interesado acepta, mediante una declaración o una clara acción afirmativa* (artículo 4). Se exige además consentimiento *explícito* para los datos pertenecientes a las categorías especiales como son los datos de salud y los datos genéticos o biométricos (artículo 9.2,a).

Se debe tener en cuenta que:

- Desparece el consentimiento tácito
- No a las casillas premarcadas

Con el RGPD:

- Si se presta el consentimiento para varios fines, este deberá prestarse para cada uno de ellos.
- Si el consentimiento recabado con anterioridad cumple los criterios del Reglamento, no es necesario recogerlo de nuevo.
- El responsable del tratamiento deberá demostrar la validez del consentimiento.
- El consentimiento es esencialmente revocable, por lo que se tiene que informar de esta posibilidad.

Relación contractual

El Reglamento es muy escueto en relación a esta base jurídica como legitimadora del tratamiento de datos personales, limitándose a establecer en su artículo 6.1b), que será licito el tratamiento "*necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales*".

En los contratos de prestación de servicios se deberán adaptar a lo que dispone el RGPD para que el tratamiento de los datos personales sea conforme.

Se deberá incluir en los pliegos de contratación las condiciones que se deben dar para que la prestación de servicios sea conforme al RGPD.

Interés vital

El Reglamento no recoge una definición de interés vital, solamente el Considerando 46 se refiere a:" *un interés para la vida del interesado o de otra persona*" y añade que solamente se puede legitimar el tratamiento sobre la base del interés vital cundo

no se pueda basar en otra base jurídica diferente y cita como ejemplos tratamientos necesarios para fines humanitarios, incluido el control de epidemias o situaciones de emergencia humanitaria.

En circunstancias excepcionales, puntuales y urgentes podría invocarse el interés vital como base jurídica del tratamiento.

Asimismo, podría ser de aplicación respecto del tratamiento de datos de salud para la prestación de asistencia sanitaria por profesionales sanitarios sujetos al secreto profesional o por otra persona sujeta a una obligación equivalente de secreto, para la prevención, diagnóstico, prestación de asistencia o tratamientos sanitarios o la gestión de servicios sanitarios.

Tratamientos necesarios para el cumplimento de una obligación legal o para el cumplimento de una misión realizada en interés público o en el ejercicio de poderes públicos

Es la base jurídica para el tratamiento de datos personales por parte de las Administraciones Públicas, y por tanto la legitimación del tratamiento de los datos relativos a la salud para la asistencia sanitaria por los centros del Sistema Nacional de Salud, en esta red de centros comprenden los centros de titularidad pública y los de titularidad privada que mediante concierto u otra habilitación legal y cumpliendo todas las normas exigidas en materia de protección de datos y confidencialidad, prestan asistencia a una población determinada, (el considerando 45 del RGPD recoge la legitimación de personas de Derecho privado para el cumplimiento de misiones de interés público en fines sanitarios como la gestión de los servicios públicos).

Se tendrán en cuenta las leyes sectoriales de Sanidad que contemplan preceptos relacionados con la protección de datos, derecho a la intimidad del paciente, confidencialidad y deber de secreto.

- 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.
- Ley 14/1986, de 25 de abril, General de Sanidad.
- Y la Ley 16/2003 de 28 de mayo de Cohesión y Calidad del Sistema nacional de salud: artículo 56: *coordinar los mecanismos de intercambio electrónico de información clínica y salud individual, para permitir el acceso, tanto al usuario como a los profesionales, con la finalidad de garantizar la calidad de la asistencia y la confidencialidad e integridad de la información*
- Ley 14/2007, de 3 de julio de Investigación Biomédica, en su artículo 5,2 requiere el consentimiento expreso y escrito, lo mismo el artículo 58, 1, para la investigación con muestras bilógicas; y en relación con los usos secundarios, el articulo 58.2 requiere consentimiento, pero añade excepciones a la obtención del consentimiento, cuando no sea posible o suponga un esfuerzo no razonable y previo dictamen favorable del Comité de Ética de la Investigación correspondiente.

Respecto de los tratamientos para la investigación biomédica hay que tener en cuenta el reciente *Informe Jurídico de la Agencia Española de Protección de Datos de marzo de 2018, número: 073667/2018*; dictamina que, con la aplicación del Reglamento General de Protección de Datos, resulta inalterable la regulación actual de investigación biomédica, añadiendo que incluso permite realizar una interpretación más flexible del alcance que se puede dar al consentimiento prestado conforme a la Ley de Investigación Biomédica.

Por tanto, en el caso de la Sanidad Pública queda clara la base jurídica de los tratamientos asistenciales, pero existen otros casos como el de docencia cuyo acceso a la información debe estar controlado ya que no pueden acceder a la base de datos donde se encuentren los datos de los pacientes o la realización de investigación con tecnología Big Data.

8 Responsable-encargado del tratamiento

El RGPD mantiene que la responsabilidad última del tratamiento de los datos personales corresponde al responsable, es la figura que determina cuál va a ser el tratamiento y su finalidad, siendo el encargado la persona física o jurídica, autoridad pública, servicio u otro organismo que presta un servicio al responsable que conlleve un tratamiento de datos personales por cuenta del mismo.

Los tipos de encargado y las formas en que se regulará su relación pueden ser muy variados, tanto como tipos de servicios, pero lo que siempre ha de tener en cuenta el responsable al elegir un encargado de tratamiento es que debe cumplir con sus instrucciones respecto de cómo ha de tratar los datos personales para prestar el servicio. Por tanto, su elección debe basarse en encargados que ofrezcan garantías suficientes para demostrar que cumplen con los requisitos del RGPD, es decir que aplican medidas técnicas y organizativas adecuadas.

El RGPD contiene obligaciones que están expresamente dirigidas a los encargados de tratamientos y que son susceptibles de supervisión por las autoridades de control independientemente del responsable al que prestan un servicio. Entre las obligaciones estarían las de mantener el registro de actividades de tratamiento, realizar el análisis de riesgos para determinar las medidas de seguridad aplicables a los tratamientos de datos que realizan y en su caso, designar un DPD. También, al igual que los responsables, pueden adherirse a códigos de conducta o acudir a los sistemas de certificación.

El encargado del tratamiento debe formalizar su relación con el responsable mediante un contrato de prestación de servicios o en un acto jurídico que vincule a ambos, que debe constar por escrito, inclusive en formato electrónico. Si se regula la relación mediante un acto jurídico unilateral del responsable ha de establecerse y definir la posición del encargado cuando ese acto le vincule.

En cualquier caso, el RGPD regula el contenido mínimo que debe incluir el documento donde se formaliza la realización para considerarse válido, y ese contenido es el siguiente:

- Objeto del contrato
- Duración del mismo
- Naturaleza
- Finalidad del tratamiento
- Tipo de datos personales y categorías de interesados
- Obligaciones y derechos del responsable

Además, en particular, el documento debe contener:

- Las instrucciones del responsable del tratamiento, es decir documentar e identificar los tratamientos de datos a realizar atendiendo al servicio prestado y forma de prestarlo.
- Deber de confidencialidad, es decir establecer cómo debe garantizar el encargado que las personas autorizadas a tratar los datos personales su compromiso, de forma expresa, a respetar la confidencialidad, además debe constar por escrito.

- Medidas de seguridad, en este caso aunque el responsable haya realizado su análisis de riesgos, el encargado debe evaluar también los suyos incluyendo todas las circunstancias que puedan incidir en la seguridad de los datos.
- Si es necesario, régimen de subcontratación. En este caso el RGPD exige la autorización previa por escrito del responsable, que puede ser específica (identificando la entidad concreta) o general (autorizando la subcontratación pero sin concretar la entidad).
- Los derechos de los interesados donde se establezca la forma en la que el encargado asistirá al responsable en el cumplimiento de la obligación de responder a solicitudes recibidas ejerciendo los derechos establecidos en el RGPD (acceso, rectificación, supresión, limitación del tratamiento, portabilidad, oposición o no ser objeto de decisiones automatizadas incluido perfilado). Es decir si va a responder el responsable o el encargado.
- Notificación violaciones de seguridad, se debe establecer la forma en que el encargado asistirá al responsable respecto de la notificación de violaciones de seguridad.
- Regular el procedimiento sobre cómo gestionar el destino de los datos al finalizar la prestación, si el encargado suprimirá o devolverá los datos.

Aunque el Responsable del tratamiento, cuando encarga a un tercero la realización de un servicio, no tiene obligación de informar a los interesados, la AEPD en la guía que ha publicado "*Directrices para la elaboración de contratos entre responsables y encargados del tratamiento*" recomienda que en determinadas circunstancias como puede ser la naturaleza del tratamiento o los datos tratados o si concurren ambas circunstancias, aconseja dar esta información para una mayor transparencia en el tratamiento de los datos personales.

9 Enfoque del riesgo

El riesgo es inherente a cualquier actividad realizada por el ser humano, los tratamientos de datos personales no se encuentran exentos de riesgo y suponen una interpretación del riesgo en dos sentidos. Por una parte, el riesgo que un tratamiento de datos implica para la propia organización que lleva a cabo el tratamiento,así una gestión del riesgo no apropiada para el contexto de un tratamiento puede suponer consecuencias negativas para la organización responsable: daños reputacionales, responsabilidad civil, pérdida de negocio, etc. De otra parte una gestión del riesgo que no esté en consonancia con el tratamiento de datos personales que se esté llevando a cabo podría traer consecuencias para los interesados como por ejemplo aislamiento social, dificultades para acceder a un puesto de trabajo, discriminación racial, etc. en el caso de los datos de sanitarios el riesgo aumenta y su repercusión en la persona cuyos datos pudieran verse afectados negativamente podrían variar en función del tipo de paciente. A modo de ejemplo, un centro sanitario que perdiera el control de los datos de pacientes VIH seropositivos supondría un perjuicio para el propio centro y, además, un perjuicio para los propios interesados cuyos datos hubieran sido revelados a terceros, además, el impacto si el paciente es menor se agrava, en el caso del menor el aislamiento social podría condicionar su desarrollo como persona.

Con esta doble interpretación del riesgo se plantea la necesidad de hacer uso de metodologías de análisis y gestión del riesgo que ayuden a los responsables y encargados del tratamiento a mantener en constante revisión los riesgos existentes dentro de su organización.

Estas metodologías tienen por objetivo final maximizar el éxito de las actividades de una organización y con relación a los tratamientos de datos personales este éxito se traduciría en la eliminación de riesgos tanto para la entidad que lleva a cabo el tratamiento como para las personas físicas cuyos datos están siendo tratados.

Pasos para realizar un análisis de riesgos:

1. Definir con exactitud aquello que se quiere proteger, cualquier elemento que necesitamos para la consecución de un fin y que por definición llamaremos “activo”.
2. Elaborar un mapa de activos donde incluir todos los medios necesarios para llevar a cabo los objetivos de una organización.
   Por ejemplo, para que un centro sanitario pueda desempeñar sus funciones sin ocasionar perjuicios a los derechos de los pacientes será necesario disponer de fluido eléctrico permanente, sistemas de información para la gestión de medicamentos e historiales médicos, sistemas finales (PC, dispositivos móviles) que permitan al personal llevar a cabo sus funciones, mecanismos que garanticen los derechos de los interesados (información, acceso, rectificación y supresión, portabilidad, limitación), etc.
   Por tanto, es de especial importancia disponer ya del registro de actividades de tratamiento

que, en definitiva, puede significarse como activo o recurso de base para la puesta en marcha de los análisis de riesgos que pudieran ser necesarios.

3. Elaborar una relación de posibles "amenazas" o dicho en otros términos, definir aquello de lo que necesariamente necesitamos proteger a nuestros activos para evitar consecuencias negativas sobre los mismos, es decir, el "impacto".
4. En ocasiones, la amenaza es el resultado de una "vulnerabilidad" de un producto o servicio, o de lo que podríamos llamar una debilidad de los activos que puede contribuir a la materialización de una amenaza. El análisis y la gestión de riesgos tiene en cuenta mapas de activos, mapas de amenazas, y mapas de vulnerabilidades específicos para cada tratamiento.
5. Una vez que se han analizado los distintos mapas necesarios para llevar a cabo el análisis y la gestión del riesgo es necesario asignar un valor cuantitativo o cualitativo. Para determinar el valor del riesgo es necesario tener en cuenta el factor de la "probabilidad" de que una amenaza pueda llegar a materializarse. En términos generales el riesgo se mide teniendo en cuenta la probabilidad de que una amenaza se materialice y el impacto que podría suponer para la organización o para los propios interesados, en resumen:

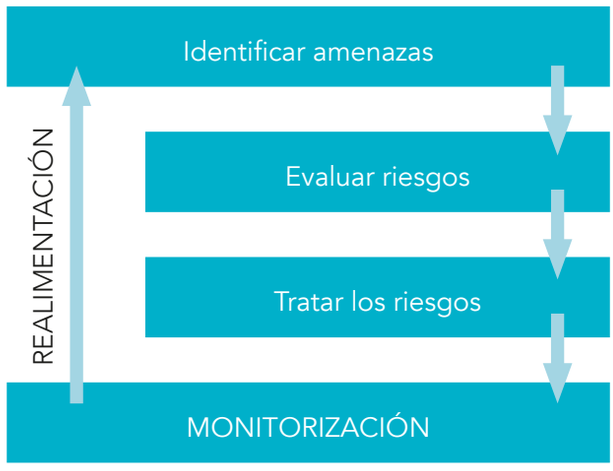
Riesgo= Impacto x probabilidad

En definitiva el análisis y la gestión del riesgo trata de poner una cifra de referencia (umbral de riesgo aceptable) sobre el que una organización tiene que marcar sus objetivos de riesgo para, posteriormente, llevar a cabo un proceso de gestión de los mismos y la revisión de la eficacia de las medidas utilizadas (auditoría) para eliminar o atenuar el nivel de riesgo.

Algunas normas de referencia a tener en cuenta con relación a la gestión y análisis de riesgos son las normas ISO 31000 y 31010. Las fases que la ISO 31000 tiene en cuenta a la hora de establecer una política de riesgos en una organización son las siguientes:

- Comunicación y consulta a toda la organización implicada
- Determinar el contexto del análisis del riesgo: identificar normativas aplicables, definir y categorizar activos, categorizar el impacto y definir el nivel de riesgo aceptable.
- Identificar riesgos: definir procesos, inventario de soportes, identificar riesgos asociados a la tecnología utilizada (redes de comunicaciones, entorno físico, etc.)
- Analizar y evaluar riesgos: cuantificación del riesgo mediante escalas cuantitativas o cualitativas.
- Gestionar o tratar los riesgos: valorar la relación coste-beneficio de los controles que sean necesarios para salvaguardar los activos y llevar a cabo la puesta en marcha de los mismos.
- Proceso de seguimiento y revisión: definir los mecanismos periódicos de seguimiento que permitan visualizar el resultado de los controles que hubieran sido puestos en marcha para atenuar el riesgo o eliminarlo: auditorías periódicas, informes, incorporación de nuevos activos que supongan modificación del riesgo, seguimiento de brechas de seguridad, etc.

El planteamiento de las metodologías de análisis de riesgos podría resumirse con carácter general en, al menos, las cuatro fases siguientes:



El análisis y la gestión de riesgos es un proceso consciente, metodológico y estructurado que debe adecuarse en todo momento a la evolución del riesgo con el fin de mantener un nivel de riesgo aceptable para la organización y para los interesados. Por tanto, es un proceso de mejora continua y no puede ser interpretado como un proceso cerrado, tras la monitorización de los resultados mediante auditorías es necesario realimentar el proceso añadiendo de nuevas amenazas que hubieran sido identificadas de las que pudiera tenerse constancia de cualquier fuente de información (registro de incidencias, información de proveedores de productos, servicios de alerta, noticias de prensa, comunicados de fuerzas y cuerpos de seguridad, etc.) con el objetivo de volver a tratar el riesgo resultante.

Análisis de riesgos en protección de datos

Con carácter general el análisis y la gestión de riesgos en el RGPD, se encuentran estrechamente relacionados con el cumplimiento de lo previsto en los artículos 32 y 35 del RGPD:

- Artículo 32.1: *"Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, …"*
- Artículo 35.1: *"Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales…".*

En definitiva el enfoque de riesgos del RGPD puede traducirse en dar respuesta a las medidas necesarias para garantizar la seguridad de los datos personales y a la necesidad de evaluar con carácter previo el impacto que un tratamiento de datos pueda tener para los derechos y libertades de las personas físicas. Entre los posibles riesgos para las personas físicas a los que se refiere el RGPD se encuentran los mencionados en el considerando 75:

"daños y perjuicios físicos, discriminación, usurpación de identidad, pérdida de reputación, daños a la confidencialidad y perjuicios sociales".

El RGPD determina dos niveles de riesgos con relación a los tratamientos de datos personales: tratamientos de alto y de escaso riesgo. En función de estos niveles de riesgo se plantea la necesidad de llevar a cabo análisis de riesgos y evaluaciones de impacto.

En el caso de tratamientos de escaso riesgo para los derechos y libertades de las personas, sería posible abordar el tratamiento de datos personales únicamente con la implantación de las medidas mínimas necesarias para garantizar la seguridad de los datos. En otros casos, como, por ejemplo en el caso de datos sanitarios relativos a los pacientes que reciben asistencia sanitaria, sería necesario llevar a cabo un análisis de riesgos para implantar las medidas técnicas y organizativas a fin de garantizar la seguridad de los datos y, en consecuencia, garantizar los derechos y libertades de las personas, pero también sería necesaria la realización de una evaluación de impacto cuando se pretenda realizar un cambio sobre un tratamiento de alto riesgo ya existente o cuando se esté diseñando un tratamiento de datos de alto riesgo (protección de datos desde el diseño).

La AEPD en su guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD plantea el análisis de riesgos partiendo de la base de la descripción de las operaciones de actividades de tratamiento teniendo en cuenta el

ciclo de vida de los datos que podría definirse al menos en cinco fases:

1. Captura de los datos
2. Clasificación y almacenamiento
3. Uso o tratamiento de los datos
4. Cesiones o transferencias a terceros
5. Destrucción

Esta guía propone un análisis partiendo del registro de actividades de tratamiento y para cada una de las fases indicadas debe ser tenidos en cuenta todos los elementos implicados: actividades y operaciones de tratamiento realizadas, tecnología utilizada, datos necesarios para el objetivo de los tratamientos y personas involucradas en estas operaciones.

Desde un punto de vista práctico, el análisis de riesgo proporciona una visión general a los responsables y encargados del tratamiento que habitualmente suele representarse mediante mapas de calor que llevan asociado un valor cuantitativo:

PROBABILIDAD					
	MÁXIMA (4)	4	8	12	16
	SIGNIFICATIVA (3)	3	6	9	12
	LIMITADA (2)	2	4	6	8
	DESPRECIABLE (1)	1	2	3	4
		DESPRECIABLE (1)	LIMITADO (2)	SIGNIFICATIVO (3)	MÁXIMO (4)
		IMPACTO			

En la tabla se muestra una posible política de riesgos en la que se que incluye una escala de riesgos altos, medios y mínimos. La política de riesgos asociada debería establecer las medidas necesarias para eliminar de los tratamientos de datos elementos de medio y alto riesgo para la confidencialidad, integridad, disponibilidad de los datos así como la resiliencia de los sistemas y servicios de tratamiento (color rojo y naranja con valor numérico entre 3 y 16) fijando criterios generales para llevar a cabo únicamente tratamientos de bajo riesgo (color verde y valor numérico entre 1 y 2).

Los responsables y encargados del tratamiento deben de tener en cuenta una política de riesgos que sirva para la toma de decisiones sobre las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales a la que se refiere el artículo 32 del RGPD, las medidas de seguridad deben ser el resultado de la gestión del riesgo y nunca un listado cerrado de medidas.

A modo de ejemplo, en un tratamiento que implicara un almacenamiento en la nube (cloud computing) de un tercero donde no existieran garantías suficientes estaríamos hablando de un riesgo

máximo si se tratara de datos sensibles, y aplicando mecanismos de cifrado de manera oportuna este riesgo podría variar desde un nivel máximo (16) a un nivel despreciable o limitado (1-2) acorde con la política de riesgos preestablecida en la organización. En este caso estaríamos gestionando los riesgos y, mediante los controles de seguridad aplicados, obtendríamos un umbral de riesgo aceptable para la organización, finamente sería necesario incluir procesos de auditoría y mejora de la gestión del riesgo, entre las medidas que propone el RGPD para mejorar el nivel de riesgo se incluyen los procesos de seudonimización[1] y cifrado de datos personales.

El resultado de los análisis de riesgos y de los informes de seguimiento de la efectividad de las medidas de seguridad (proceso de auditoría), deben incluir un informe ejecutivo disponible para la toma de decisiones de una organización. Este informe, que también formará parte de la base documental para acreditar la proactividad de los responsables y encargados del tratamiento, será de utilidad para la alta dirección a la hora de orientar esfuerzos y recursos económicos con el fin de reducir, eliminar o trasladar los riesgos a un tercero mediante la suscripción de una posible póliza para cubrir posibles daños a las personas físicas.

[1] La AEPD ha publicado una guía con recomendaciones para llevar a cabo procesos de anonimización de datos que se encuentra disponible en su página web: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2016/Orientaciones_y_garantias_Anonimizacion.pdf

10 Evaluaciones de impacto

¿Qué es una evaluación de impacto?

La evaluación de impacto en protección de datos está estrechamente relacionada con la protección de datos desde el diseño y es una herramienta orientada a evaluar y tratar los riesgos potenciales que un tratamiento de datos personales puede suponer para los derechos y libertades de las personas con carácter previo a la puesta en marcha del mismo y que, además, también debería llevarse a cabo cuando se produzcan cambios en un tratamiento que se estuviera siendo realizando con anterioridad a la aplicación del RGPD y estos cambios pudieran implicar un alto riesgo para los derechos y libertades de las personas. Los cambios que podrían dar lugar a la necesidad de realizar una evaluación de impacto en un tratamiento que ya se estuviera llevando a cabo con anterioridad a la aplicación del RGPD podrían ser cambios tecnológicos en los sistemas de información, cambios en la finalidad del tratamiento, inclusión de nuevos datos de las mismas o diferentes fuentes, y en general cualquier cambio que pudiera suponer una variación de los riesgos para los derechos y libertades de las personas cuyos datos estuvieran siendo tratados.

De la misma forma que el análisis de riesgos orientado a determinar las medidas técnicas y organizativas necesarias para garantizar los datos personales son el resultado de un proceso de mejora continua, la evaluación de impacto no puede significarse como una tarea cerrada tras su realización. Existirá también un proceso de mejora continuada de manera que los responsables lleven a cabo revisiones periódicas de los riesgos y la efectividad de las medidas establecidas para reducir los niveles de riesgo del tratamiento a un nivel aceptable.

Tanto el resultado del análisis de riesgos encaminado a determinar las medidas de seguridad que garanticen la seguridad de los datos personales (Art. 32 RGPD) como el resultado de la evaluación de impacto (Art. 35 RGPD) dan lugar a un mapa de riesgos con elementos que deben de ser revisados de forma periódica, como ya se ha comentado antes, los procesos de análisis y gestión de riesgos requieren de un ciclo de mejora continua.

La EIPD forman parte del principio de responsabilidad activa del RGPD, los documentos generados en su realización deben de integrarse en una base documental con el fin de poder acreditar en todo momento la diligencia de los responsables con relación a los tratamientos que llevan a cabo.

Elementos de una EIPD

El artículo 35.7 del RGPD define el contenido mínimo que debe de tener una EIPD:

- Descripción sistemática de las operaciones de tratamiento.
- Evaluación de necesidad y proporcionalidad de las operaciones de tratamiento con relación a su finalidad.
- Una evaluación de los riesgos para los derechos y libertades de los interesados.

- Medidas previstas para afrontar los riesgos: garantías, medidas de seguridad, mecanismos de protección de los datos personales.

Para la descripción sistemática de las operaciones de tratamiento, el registro de actividades de tratamiento será el punto de referencia inicial. Es posible que la nueva actividad de tratamiento que se esté diseñando pueda tener relación con otras actividades de tratamiento o que tenga similitud total o parcial con algunas de las actividades de tratamiento que previamente hayan sido puestas en marcha. En caso afirmativo será recomendable partir de la experiencia previa reutilizando los mapas de riesgo existentes con el consecuente ahorro de esfuerzo.

Fases de una EIPD

Una vez que se ha consultado el registro de actividades de tratamiento será necesario llevar a cabo un primer análisis sobre la necesidad de realizar o no la evaluación de impacto. En este análisis previo a la realización de la EIPD, se debe de valorar la posibilidad de aplicar técnicas de anonimización y seudonimización que pudieran ser suficientes para eliminar los riesgos para los derechos y libertades de las personas, si el resultado de las mismas supone la desaparición del riesgo hasta un nivel de riesgo escaso podría ser posible llevar a cabo el tratamiento sin necesidad de realizar la EIPD, llevando a cabo los controles necesarios que permitan asegurar a lo largo del ciclo de vida del tratamiento, que las medidas de anonimización y seudonimización siguen siendo efectivas.

Si tras el análisis de necesidades, se concluye que es necesario llevar a cabo la EIPD, al menos, se tendrán en cuenta las siguientes fases:

1. Definición del contexto:
   - Descripción del ciclo de vida de los datos: del mismo modo que ocurría en el análisis de riesgos relativo al artículo 32 del RGPD, para la EIPD es esencial tener una visión general del ciclo de vida completo del tratamiento en el que se incluyan todas las fases que sean necesarias para llevar a cabo la finalidad del mismo. La AEPD en sus guías utiliza un modelo de ciclo de vida de cinco fases: captura de datos, clasificación, almacenamiento, uso/tratamiento, cesión/transferencia y destrucción. Para la definición del contexto será también necesario identificar todos los elementos implicados en cada una de las fases (activos): operaciones de tratamiento, datos necesarios, tecnología e intervinientes.
   - Análisis de proporcionalidad: se llevará a cabo un análisis de base de legitimación del tratamiento aplicando el principio de minimización de datos. Podrá ocurrir que al reducir los datos a los mínimamente necesarios para obtener la finalidad del tratamiento, el nivel de riesgo se reduzca evitando de esta forma llevar a cabo un tratamiento de datos de alto riesgo.

2. Gestión de riesgos:

La EIPD es una metodología de análisis de riesgos y comparte fases y filosofía con el análisis de riesgos encaminado a determinar las medidas de seguridad (Art. 32 RGPD) para proteger los datos personales:

- Identificar amenazas: análisis de riesgos potenciales para los tratamientos, entre los posibles riesgos se incluirán los que en contextos similares hubieran sido evaluados en el análisis de riesgos para determinar las medidas de seguridad y, además, cualquier riesgo que el tratamiento pudiera implicar para los derechos y libertades de las personas.
- Evaluar riesgos: su resultado será el obtenido como consecuencia de considerar la probabilidad y el impacto dando lugar a un mapa de calor o mapa de riesgos cuantitativo o cualitativo.
- Tratar los riesgos: medidas encaminadas a minimizar las consecuencias negativas que pudieran sobrevenir de la materialización de una amenaza.

3. Conclusión y validación:
Informe de medidas llevadas a cabo para la gestión de riesgos identificados con el fin de garantizar los derechos y libertades de las personas físicas y, en caso necesario, el resultado de la consulta previa a la autoridad de control. El resumen ejecutivo de este informe será para el responsable del tratamiento un marco de referencia para la toma de decisiones relacionadas con el tratamiento de datos que se pretende llevar a cabo.

4. Supervisión y revisión:
Antes de la puesta en marcha del tratamiento se llevará a cabo un plan para la supervisión y revisión del mismo, el plan contemplará la posibilidad de llevar a cabo auditorías con el objetivo de determinar la eficacia de las medidas utilizadas para reducir el riesgo. De las conclusiones obtenidas mediante este plan de supervisión, se procederá a la realimentación de todo el proceso con el objetivo de llevar a cabo un proceso de mejora continua de las conclusiones de la EIPD.

Es preciso señalar que en la realización de una EIPD será necesario definir un equipo de trabajo donde se establecerán roles y responsabilidades a cada uno de sus miembros. Entre los miembros de este equipo de trabajo debe tenerse en cuenta al DPD con el objetivo de informar y asesorar al responsable y, en caso necesario, llevar a cabo la consulta previa a la autoridad de control, el equipo de trabajo también contará con integrantes especializados en el contexto de los datos que van a ser tratados y con expertos y responsables de cada una de las fases y componentes del ciclo de vida del tratamiento con una clara asignación de funciones.

La obligación de llevar a cabo una EIPD será siempre del responsable o del encargado y nunca del DPD.

11 Derechos de los pacientes

Los derechos de los ciudadanos-pacientes relativos a la protección de sus datos de salud, están recogidos en el RGPD como norma general de protección de datos y en las leyes españolas sectoriales de sanidad y salud.

El RGPD refuerza los derechos de la protección de datos, ampliando el contenido, incorporando nuevos derechos, aplicando el principio de transparencia, y otorgando mayor protagonismo y garantías de control al ciudadano.

Referencia a las normas sectoriales de Sanidad e Investigación que contienen preceptos relacionados con la protección de datos, siendo las más importantes:

- 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.
- Ley 14/1986, de 25 de abril, General de Sanidad.
- Y la Ley 16/2003 de 28 de mayo de Cohesión y Calidad del Sistema nacional de salud: artículo 56: *coordinar los mecanismos de intercambio electrónico de información clínica y salud individual, para permitir el acceso, tanto al usuario como a los profesionales, con la finalidad de garantizar la calidad de la asistencia y la confidencialidad e integridad de la información*
- Ley 14/2007, de 3 de julio de Investigación Biomédica.

Las organizaciones sanitarias deben tener en cuenta las consideraciones siguientes para desarrollar sus procedimientos de gestión de los derechos que asisten a los pacientes o interesados con relación al tratamiento de datos:

- Facilitar a los interesados el ejercicio de sus derechos, con la posibilidad de presentación de la solicitud por medios electrónicos, especialmente cuando el tratamiento se realiza por estos medios.
- Obligación del responsable de tratamiento de informar sobre los medios para ejercitar los derechos y facilitar su accesibilidad.
- Podrán ejercitarse directamente o por medio de representante legal o voluntario acreditado. (artículo 18.2 Ley 41/2002 y articulo 12,1 Proyecto de Ley de Protección de datos).
- El ejercicio del derecho será gratuito para el interesado, excepto que se formulen solicitudes manifiestamente infundadas o excesivas (que se deberá demostrar), en este caso, se podría cobrar un canon que compense los costes administrativos exclusivamente.
- El plazo de contestación es de un mes, ampliable a dos meses cuando se trate de solicitudes especialmente complejas, que se deberá informar de la ampliación dentro del primer mes
- Si el resultado es no atender la solicitud, es obligatorio contestar con la información y la motivación.
- Posibilidad de colaboración para el cumplimiento de estos derechos de los encargados de tratamiento (empresas de gestión de archivos) pero deberá incluir estos términos en el contrato de encargo de tratamiento.

Derecho de Acceso:

El derecho de acceso es el derecho del interesado a obtener información sobre sus datos y en el ámbito de la asistencia sanitaria, se concreta básicamente en el acceso a la historia clínica.

La información incluida en el derecho de acceso, contempla la historia clínica completa, con las excepciones o limitaciones que recoge la legislación.

La Ley de Autonomía del Paciente en su artículo 15: "La historia clínica incorporara la información que se considere transcendental para el conocimiento veraz y actualizado del estado de salud del paciente. Todo paciente o usuario tiene el derecho a que quede constancia de la información obtenida en todos sus procesos asistenciales…" y en su apartado segundo especifica el contenido mínimo de la historia clínica.

- Conocer y obtener *copia* de la Historia Clínica, (artículo 15, 3 RGPD y artículo 18,1 Ley 41/2002)
- *No se contempla* dentro del derecho de acceso, conocer quien ha accedido a la Historia Clínica.
- *Limitaciones*: no acceso a datos de terceros que constan en la Historia Clínica y tampoco a los comentarios y anotaciones subjetivas de los profesionales (este derecho es de los profesionales que las han escrito, no del centro), (artículo 15, 4 RGPD y articulo 18,3 Ley 41/2002)

Derecho de Rectificación:

Este derecho hace referencia a que el responsable de tratamiento debe rectificar aquellos datos que estén incompletos o sean inexactos.

Para ejercer el derecho de rectificación, el interesado debe indicar el dato erróneo y si es necesario documentación justificativa de la inexactitud o carácter incompleto de los datos.

Se justifica este derecho por el principio de calidad de los datos, que deben ser veraces (ciertos), actuales (puestos al día) y exactos (que coincidan con la realidad).

Los requerimientos de la normativa de protección de datos en general se alinea con la especifica sanitaria, así, la Ley 41/2002 en su artículo 15.1,exige que la historia clínica tenga información veraz y actualizada del estado de la salud del paciente

Derecho de Oposición:

Mediante este derecho de oposición se puede oponer al tratamiento de los datos personales por motivos relacionados con su situación particular.

El responsable del tratamiento podrá denegar el ejercicio de este derecho, alegando motivos legítimos imperiosos para que el tratamiento prevalezca sobre el interés del solicitante o para el ejercicio o defensa de reclamaciones.

El RGPD reconoce explícitamente el derecho de oposición al tratamiento de sus datos con fines de investigación científica o estadísticos salvo que sea necesario por razones de interés público (artículo 21,6).

Derecho de Supresión:

Es el derecho a la supresión de los datos personales sin dilación cuando exista tratamiento ilícito o desaparece la finalidad que motivó el tratamiento o recogida.

Existen excepciones al ejercicio en la práctica de la asistencia sanitaria este derecho, por lo que resulta casi imposible la posibilidad de supresión (antes de cancelación) de los datos de salud, debido a los plazos de obligación legal de conservación, otras obligaciones de conservación y el derecho de asistencia sanitaria del paciente.

La Ley 41/2002 en el artículo 17, 1 y 2, exige plazos mínimos de conservación, además de prohibir la

destrucción de datos clínicos relacionados con el nacimiento del paciente y la obligación de conservar la documentación clínica a efectos judiciales. Cuando existan razones epidemiológicas, de investigación o de organización y funcionamiento del Sistema Nacional de Salud se deberá conservar la documentación, aunque separando la identificación personal de los datos sanitarios.

El propio RGPD, recoge en el apartado 3 del artículo 17 sobre el derecho de supresión que no se aplica cuando el tratamiento sea necesario para, el cumplimento de un misión realizada en interés público o en el ejercicio de poderes públicos, por interés público en el ámbito de la salud pública, cuando se trate con fines de investigación científica o estadística en la medida que el ejercicio del derecho de supresión pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento o para el ejercicio o defensa de reclamaciones.

El Proyecto de Ley de LOPD, recoge la obligación de bloqueo de los datos cuando se realicen operaciones de rectificación o supresión, quedando a disposición exclusiva de los jueces y tribunales, Ministerio Fiscal o Administraciones Públicas competentes, para la exigencia de responsabilidades derivadas del tratamiento y por el plazo de prescripción de las mismas.

Existe la obligación de contestar siempre, aunque sea denegándolo de forma motivada y en un plazo de 1 mes desde la solicitud

En relación con el **derecho al Olvido**, este es una manifestación de los derechos de supresión u oposición en el *entorno online*.

Derecho de portabilidad:

Es el derecho a recibir los datos a solicitud del interesado, en un formato estructurado, de uso común y lectura mecánica, con la intención de transmitirlos a otro responsable de tratamiento, cuando el tratamiento está basado en un contrato o en el consentimiento y se efectúe por medios automatizados.

No es aplicable a las Administraciones Públicas, "*Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en ejercicio de poderes públicos conferidos al responsable del tratamiento*" (artículo 20, 3 RGPD).

Derecho de Indemnización y responsabilidad:

En el supuesto de sufrir daños y perjuicios materiales o inmateriales como consecuencia de una infracción del Reglamento.

Este derecho es ante el responsable y/o encargado del tratamiento.

Derecho de Limitación del tratamiento:

A solicitud del interesado, no se podrán tratar sus datos, cuando se den las condiciones siguientes:

- Mientras se verifica la exactitud de los datos en casos de impugnación por el interesado.
- Cuando el tratamiento sea ilícito y el interesado se oponga a la supresión.
- Cuando el interesado necesite que el responsable conserve los datos para el ejercicio o defensa de reclamación.
- Mientras se verifican las circunstancias en el derecho de oposición.

Durante el tiempo que dure la limitación, el responsable sólo podrá tratar los datos del afectado para, su conservación o para ejercicio y defensa de reclamaciones o para la protección de derechos de otra persona física o jurídica o por razones de interés público importante (artículo 18.2 RGPD).

Ejercicio de los derechos por menores:

En relación a la edad en que los menores y sus representantes legales pueden ejercer los derechos sobre protección de datos, hay diversos pronunciamientos de la AEPD con diferentes Informes jurídicos, haremos referencia al último del año 2014, Informe Jurídico 0222/2014 (teniendo en cuenta que la LOPD 15/1999 mantiene que a partir de 14 años se puede dar el consentimiento y ejercer los derechos de protección de datos):

"El menor de edad mayor de 14 años, podrá, en general, ejercitar por si solo el derecho de acceso a la historia clínica.
Los titulares de la patria potestad podrán también acceder a los datos del menor de edad sujeto a aquella mientras esa situación persista, para el cumplimiento de las obligaciones previstas en el Código Civil.
No podrá oponerse a ese acceso la mera oposición del menor salvo que así lo reconociera una norma con rango de Ley"

El RGPD autoriza el margen de edad a concretar por cada Estado hasta los 13 años.

12 Violaciones de seguridad

Con anterioridad al RGPD la obligación de notificar brechas o violaciones de seguridad a la autoridad de control se limitaba a los operadores de servicios de telecomunicaciones electrónicas disponibles al público o que exploten redes públicas de comunicaciones según lo previsto en el artículo 41 de la Ley 9/2014 (Ley General de Telecomunicaciones). El RGPD hará extensible esta obligación a todos los responsables de un tratamiento de datos personales.

El Artículo 33 del RGPD establece la obligación del responsable de notificar las violaciones de seguridad en un plazo máximo de 72 horas desde el momento en que se tuviera constancia de la misma y también determina la obligación del encargado del tratamiento de notificar sin dilación al responsable del tratamiento acerca de las violaciones de seguridad de los datos personales de las que tuviera constancia.

La notificación a la autoridad de control debe de contener al menos:

- Descripción de la naturaleza de la violación con el detalle de las categorías de los datos y de los afectados, así como el número de personas que podrían haberse visto afectadas.
- Información sobre la identidad del responsable y del delegado de protección de datos o punto de contacto donde sea posible obtenerse más información.
- Descripción de las consecuencias de la violación de seguridad y de las medidas puestas en marcha por el responsable del tratamiento para remediar los posibles efectos negativos.

Las violaciones de seguridad deben estar documentadas y formarán parte de la base documental que permitirá al responsable demostrar en cualquier momento que realiza el tratamiento según los requisitos establecidos en el RGPD.

El RDLOPD ya hacía referencia a la obligación de incluir en el documento de seguridad un procedimiento de notificación, gestión y respuesta ante las incidencias que debería incluir un registro de incidencias, podría decirse que el RGPD mantiene la necesidad de disponer mantener en vigor un procedimiento de gestión y respuesta a incidencias de seguridad que debe de incluir la notificación a la autoridad de control y también la necesidad de seguir disponiendo de un registro de incidencias o base documental de las mimas.

Otra de las novedades del RGPD en relación a las violaciones de seguridad, es la comunicación a los interesados (Art. 34 RGPD) cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas. Esta comunicación no sería necesaria cuando el responsable haya adoptado medidas técnicas y organizativas que hagan que los datos personales sean ininteligibles o cuando se hubieran utilizado medidas que impidan la existencia de un riesgo alto para los derechos y libertades de los interesados.

El método para comunicar la violación de seguridad a los interesados deberá utilizar un lengua-

je claro y sencillo para informar con relación a la naturaleza de la violación de seguridad y en caso que requiera esfuerzos desproporcionados podrá realizarse por los medios de comunicación al público general.

No hay que olvidar que no se debe comunicar cualquier violación de seguridad, la pérdida de un pendrive que el hospital ha facilitado a un médico, pero no contiene datos de pacientes, no es necesario que tal pérdida se comunique a la AEPD.

13 ¿Y ahora qué? Hoja de ruta

El derecho a la protección de datos personales persigue garantizar a la persona el control de sus datos personales, su uso y su destino con el propósito de impedir su tratamiento ilícito y lesivo para sus derechos y libertades personales

Los datos relativos a la salud pertenecen a nuestro mayor grado de reserva personal, y en relación a la información e identificación que contienen, va a suponer el máximo interés por parte de los ciudadanos, en garantizar el uso y tratamiento de los datos para los fines con los que han sido obtenidos.

El derecho a la protección de los datos personales se ha convertido en un derecho básico e importante en nuestra sociedad, una sociedad en donde las nuevas tecnologías con su rapidez e innovación nos hacen la vida mejor, pero añaden nuevos riesgos sobre intimidad y confidencialidad, y como consecuencia se necesita que el control de nuestros datos esté garantizado y en lo referente a los datos de salud, esas garantías de control de la información que generan los datos y su tratamiento, adquieren relevancia muy especial en el ámbito sanitario

El Reglamento General de Protección de Datos, representa una continuidad en las medidas de protección actuales y añade nuevos requisitos para que todas las partes implicadas adquieran el compromiso de garantizar, avalar y demostrar el aseguramiento de la protección en el tratamiento de datos en el ámbito sanitario.

La garantía de la protección solamente se consigue pensando y operando en "modo protección de datos", por ello es muy importante que los Directores se pongan en marcha para que se realicen las siguientes acciones para adaptar sus instituciones a lo que dispone el RGPD:

- Designar un delegado de protección de datos
- Establecer el registro de actividades de tratamiento
- Determinar la legitimación de los tratamientos
- Revisar la información que se facilita a los pacientes
- Revisar los contratos con encargados de tratamientos
- Revisar los procedimientos para atender el ejercicio de los derechos
- Realizar el análisis de riesgos
- Realizar evaluaciones de impacto
- Revisar las medidas de seguridad
- Desarrollar y aplicar una política de privacidad
- Formar y concienciar

-Valores como la confidencialidad, la privacidad y su protección están presentes en la actualidad como valores a asegurar. La sociedad, los ciudadanos- pacientes son cada vez más conscientes de sus derechos y los que tratan los datos más implicados con el compromiso adquirido ante el usuario y en el complimiento de las normas, una política de calidad de protección de datos en la que la mejora continua este presente, va a responder con mayor garantía de éxito y ayudara, además de evitar sanciones, a la mejora reputacional y de credibilidad de la organización ante sus clientes y la sociedad.

Por eso es muy importante la labor de los Directivos de los hospitales en todo este proceso de cambio que impulsa el RGPD y que su cumplimiento genera valor, seguridad y calidad al servicio prestado.

Mayo 2018

sedisa

sociedad
española de
directivos
de la salud