LEGISLACIÓN APLICABLE A CENTROS SANITARIOS

JUAN NIETO PAJARES

4 DE DICIEMBRE DE 2018

1. Introducción.

El presente trabajo realiza una revisión de la legislación actual en materia de informática y tecnología de la información, aplicable a un centro sanitario público.

En la primera parte reviso la legislación relativa aspectos generales como derechos de autor, nombres de dominio y firma electrónica. Para facilitar el análisis he seguido en esta parte los apartados de los contenidos del libro de la asignatura, estudiando los casos en los que cada norma tiene aplicación en un centro sanitario público.

La segunda parte está referida al derecho al honor y la intimidad y todo lo relacionado con la protección de los datos de carácter personal y la normativa aplicable. Esta es la parte más importante en un ámbito sanitario público. Hago una revisión detalla de las normas en conjunto revisando los aspectos más importantes.

En el último punto reviso el impacto legal en cuanto a herramientas de uso general como el correo electrónico, redes sociales.

2. Marco normativo.

1. Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

2. Directiva 91/250/CEE del Consejo, de 14 de mayo de 1991, sobre la protección jurídica de programas de ordenador.

3. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (CP).

4. Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual (LPI).

5. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LODP)

6. Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI).

7. Ley 59/2003, de 19 de diciembre, de firma electrónica (FE).

8. Orden ITC/1542/2005, de 19 de mayo, que aprueba el Plan Nacional de nombres de dominio de Internet bajo el código de país correspondiente a España («.es»).

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

10. Reglamento (UE) 2016/679 del parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD).

11. 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 (LAP).

12. Borrador. 121/000013 de 9 de octubre de 2018. Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal.

3. Normativa general.

3.1. Protección jurídica del software.

Los programas de ordenador están protegidos por la Directiva 91/250/CEE y por LPI. Un centro sanitario, desde el punto de vista de los programas de ordenador puede desempeñar el rol de usuario de aplicaciones desarrolladas por terceros y de creador de programas suponiendo que dispongo de un departamento de informática con personal propio o subcontratado. A continuación analizamos los aspectos normativos para cada situación; obligaciones como usuario y derechos como creador.

3.1.1. Aplicaciones desarrolladas por terceros.

Desde el punto de vista de usuario de los programas, el modo más habitual de compra es la licencia por uso. Podemos diferenciar los siguientes tipos.

1. Programas con **licencias de código abierto**. Aunque no suele estar implantada la cultura del uso de software de fuentes abiertas, en el caso de existir alguna aplicación bajo este tipo de licencia, las consideraciones a tener en cuenta en su uso son las relativas al tipo de licencia. Siendo excepcional la modificación del código, las obligaciones legales del centro se cumplen utilizando el programa como usuario final.

2. En cuanto al **software privativo o propietario** su uso está condicionado a los términos de la licencia. El aspecto más relevante a tener en cuenta es que gran parte de los programas (sistemas operativos Windows, programas de ofimáticas, visores PDF, etc.) cada instalación de cada ordenador, debe disponer de su correspondiente licencia. Para evitar ilegalidades la instalación de cualquier programa debe estar controlada evitando que los usuarios puedan instalar aplicaciones sin la correspondiente licencia.

En el uso fraudulento de software, además de suponer una violación de los legítimos derechos de las compañías, es un delito regulado por el art. 270 del CP. Las penas previstas para los administradores son multas de hasta 280.000 euros y prisión de hasta cuatro años de cárcel; para la empresa: multa de hasta cuatro veces el valor de mercado del software ilícitamente copiado y utilizado. El art. 1903 del código civil hace responsable al empresario de los actos de sus empleados realizados en el ámbito laboral.

3.1.2. Aplicaciones desarrolladas en el propio centro.

En relación con los derechos de autor, el art 191/250/CEE dice: "*protegerán mediante derechos de autor los programas de ordenador como obras literarias*" el art. 10 de la LPI "*Son objeto de propiedad intelectual todas las creaciones originales; Los programas de ordenador* ". Suponiendo que el empleado que lo realiza, está contratado para tal fin, los derechos de explotación son de la empresa si bien el empleado tiene el derecho moral y se debe hacer referencia a su autoría (art. 113 LPI).

3.2. Propiedad intelectual en internet.

En relación con internet, el primer aspecto aplicable a un centro sanitario tiene relación con su posicionamiento en internet. Suponiendo que el centro tenga presencia en internet mediante una página web y un dominio reservado a efectos de correo electrónico corporativo, es aplicable la orden ITC/1542/2005, relativa a los nombres de dominio.

Para reservar un nombre de dominio .es; "*está legitimado cualquier persona física o jurídica y a las entidades sin personalidad que tengan intereses o mantengan vínculos con España"*. (art. 6). Por lo que en principio el centro cumple los requisitos para hacer la reserva de nombre.

En cuanto a las limitaciones del nombre (art. 7), no deben coincidir con nombres de dominio de primer nivel (.com, .edu, .gov, etc.), ni nombres conocidos de internet, ni nombres reservados a instituciones del estado, nombres de organizaciones internacionales, topónimos y topónimos de la lista ISO 3166-1. Si el nombre a reservar es ***mihospital.es*** cumple los criterios y no se encuentra en la lista de nombre prohibidos[1].

El procedimiento de reserva se puede hacer directamente en red.es o mediante los agentes reguladores autorizados [2]. La tarifas que hay que pagar por la reserva del nombre y su mantenimiento en función del dominio elegido mihospital.es o un dominio de tercer nivel mihospital.gob.es son:

Indicativo	Alta*	Renovación*
.es	33,38€	33,38€
.com.es	14,08€	14,08€
.nom.es	14,08€	14,08€
.org.es	14,08€	14,08€

Tabla 1 Tarifas de reserva de nombres de dominio

Indicativo	Alta*	Renovación*
.edu.es	36,51€	36,51€
.gob.es	36,51€	36,51€

Tabla 2 Tarifas de reserva de nombres de dominio con verificación

En relación con el contenido de la página web, considerando que ha sido realizada por un empleado contratado para tal fin, cabría aplicar la LPI en los siguientes puntos:

1. En cuanto al diseño de la página desde un punto de vista de creación sería aplicable el art. 10 de la LPI, pero considerando la relación laboral, los derechos de explotación de la página son del empresario (art. 51 y 97) el trabajador sería el propietario de los derechos morales (art. 113).
2. En el desarrollo de los contenidos de la página el creador debe tener en cuenta la propiedad intelectual de contenidos, de modo que si las imágenes, fotos, sonidos, videos no son de dominio público (art. 41), se debe contar con la autorización del titular de los derechos.
3. En relación con el uso de enlaces ensamblados y marcos, si referencia contenidos que no son de dominio público se debe contar con la autorización del titular para no incumplir el art. 41.

Por último en relación con la página web sería aplicable el derecho de información y acceso (art 13, 14 RGPD) y proteger a los ciudadanos frente a la elaboración de perfiles que combinen protocolos, direcciones de internet, identificadores de sesión (cookies). El responsable debe informar de la instalación de las cookies y de su finalidad; políticas de cookies, esta información debe contener:

1. Un mensaje de aviso en la página principal.
2. Contenido de la política de cookies:
3. Definición de cookie.
4. Tipos de cookies propias.
5. Tipos de cookies de terceros.
6. Mensaje de aceptación.
7. Procedimiento de bloqueo en los navegadores.

Ver ejemplo en el Anexo II. Ejemplo de política de cookies.

3.3. Contratación electrónica.

Una de las actividades pública más comunes es la contratación y en cuanto a materia de informática y legislación es aplicable el sistema de contratación electrónica. La Guía sobre contratación publica electrónica de Inteco (I) revista en detalle todas las cuestiones relativas a la contratación.

[1] http://www.dominios.es/dominios/es/todo-lo-que-necesitas-saber/normativa/plan-de-dominios

[2] http://www.dominios.es/dominios/es/agentes-registradores/todos-los-agentes-registradores

Define contratación pública electrónica como "*el conjunto formado por las diferentes fases y actos administrativos que van desde la publicación de los pliegos, pasando por el proceso licitación, evaluación y adjudicación del contrato, hasta la propia gestión interna de la ejecución del mismo*".

El marco legal que se debe aplicar, según la guía es:

- Ley 30/2007 Ley de Contrato del Sector Público (LCSP)
- Ley 31/2007 Contratación en sectores del agua, energía, transportes y servicios postales
- Ley 34/2010 Modificación de la Ley 30/2007, 31/2007 y 29/1998
- RD 817/2009 Reglamento de desarrollo de la LCSP
- Orden EHA/1307/2005 Empleo de medios electrónicos en los procedimientos de contratación
- Ley 11/2007 Acceso electrónico de los Ciudadanos a los Servicios Públicos (LAECSP)
- RD 1671/2009 Reglamento de desarrollo de la LAECSP
- RD 3/2010 y 4/2010 Esquema Nacional de Seguridad e Interoperabilidad.

	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad
Fase 1: Anuncio	Bajo	Medio	Alto	*Sin valorar*	Medio
Fase 2: Pliegos	Bajo	Alto	Alto	*Sin valorar*	Medio
Fase 3: Ofertas	Medio	Medio	Alto	Alto	Alto
Fase 4: Evaluación	Alto	Alto	Alto	Alto	Alto
Fase 5: Adjudicación	*Sin valorar*	Medio	Alto	*Sin valorar*	Medio
Fase 6: Pedido	Bajo	Medio	Alto	Bajo	Bajo

Tabla 3 Categoría de seguridad de cada fase de contratación.

En cuanto a la firma electrónica a usar en las distintas fase del procedimiento, es la que ofrece más garantías en las relaciones de los ciudadanos, empresas y profesionales con sus Administraciones Públicas, que es la **firma electrónica reconocida**, por lo que es la que se usa como mecanismo de autenticación con las plataformas de licitación y contratación electrónicas.

El punto 4 hace referencia a los aspectos de seguridad e interoperabilidad. Seguridad jurídica de los actos y seguridad técnica. En la Tabla 3, se muestra un resumen las categorías de seguridad de las distintas fases de contratación de un plataforma de contratación electrónica.

El punto 5 define las funcionalidades y la referencia legal que debe tener una plataforma de contratación electrónica:

- Perfil del contratante.
- Notificaciones y certificaciones.
- Interoperabilidad.
- Procedimiento de contratación: licitación y contratación.
- Registro de licitadores.
- Subasta electrónica.

3.4. Factura electrónica.

El pedido y facturación es el paso siguiente tras la contratación. A partir de l de enero del 2015 las facturas dirigidas a las Administraciones Públicas deberán ser electrónicas. Así lo indica la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el sector público, de acuerdo con el artículo 2 de la Ley, resulta de aplicación a las facturas emitidas en el marco de las relaciones jurídicas entre proveedores de bienes y servicios y las Administraciones Públicas.

4. Normativa relativa a la protección de datos.

La Constitución Española, en el artículo 18.4 reconoce el derecho a la protección de los datos personales en lo que se refiere a su tratamiento como un derecho fundamental al señalar que "*la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos*".

La LOPD, regula el tratamiento de datos personales y la protección de derechos fundamentales como el honor y la intimidad. Es aplicable a datos personales en cualquier soporte (fichas, historias clínicas en papel, grabaciones de video vigilancia, etc.) y a cualquier fichero excepto a los personales de actividades domésticas y a los que tiene otra regulación: ficheros clasificados, censo electoral, registro civil, ficheros sobre terrorismo, etc. Analizaré en este punto los aspectos aplicables da los datos informatizados exclusivamente.

El RLOPD desarrolla la LOPD y establece las medidas de seguridad que se deben de aplicar a los datos de carácter personal.

El RGPD (en vigor desde el 25 de mayo de 2018), es una revisión del marco legal de la protección de Datos en la Unión Europea, para armonizar las normas de los Estados, es de aplicación directa y refuerza la seguridad jurídica de los ciudadanos y la transparencia respecto a la protección de datos personales. Define un nuevo modelo de cumplimiento (frente a las medidas estáticas de RLOPD), donde son los propios responsables de los tratamientos quien tienen la responsabilidad de decidir el marco de desarrollo de los tratamientos de datos y las medidas que garanticen los derechos y libertades de las personas cuyos datos están siendo tratados y, de llevar a cabo un proceso de mejora continua sobre los mecanismos de garantía. El artículo 5 establece los siguientes principios:

- **Licitud, lealtad y transparencia**: Los datos personales deben ser tratados de manera lícita, leal y transparente en relación con el interesado.
- **Limitación de la finalidad**: Los datos se deben recoger con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.
- **Minimización de datos**: Los datos deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
- **Exactitud**: Los datos deben ser exactos, y si fuera necesario, actualizados. Además, se establece que se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación si los datos son inexactos con respecto a los finales para los que se tratan.
- **Limitación del plazo de conservación**: Los datos deben ser mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales.
- **Integridad y confidencialidad**: Los datos deben ser tratados de tal manera que se garantice una seguridad adecuada mediante la aplicación de medidas de control apropiadas.

El responsable del tratamiento deberá garantizar el cumplimiento de los principios relativos al tratamiento, por lo que es fundamental definir adecuadamente las actividades de tratamiento y documentar los análisis realizados, así como,

dejar trazabilidad de los mismos y de las conclusiones que los soportan para poder garantizar el cumplimiento de las normas.

En el supuesto de estudio de un centro hospitalario, estas normas son aplicables a los pacientes, a los trabajadores, a personas que realicen contratos y si el centro tiene sistema de videovigilancia, la AEPD ha publicado un guía sobre uso, que es recomendable aplicar [III].

4.1. La Agencia de Protección de Datos de Carácter Personales.

La Agencia Española de Protección de Datos (AEPD), creada en 1993, es el organismo público encargado de velar por el cumplimiento de la Ley Orgánica de Protección de Datos de Carácter Personal en España. Tiene su sede en Madrid y su ámbito de actuación se extiende al conjunto de España.

Es un ente de derecho público con personalidad jurídica propia y plena capacidad pública y privada que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones y se relaciona con el Gobierno a través del Ministerio de Justicia. Su principal misión es velar por el cumplimiento de la legislación de protección de datos por parte de los responsables de los ficheros (entidades públicas, empresas privadas, asociaciones, etc.) y controlar su aplicación a fin de garantizar el derecho fundamental a la protección de datos personales de los ciudadanos. Lleva a cabo sus potestades de investigación fundamentalmente a instancias de los ciudadanos, aunque también está facultada para actuar de oficio. El Real Decreto 428/1993, de 26 de marzo, Estatuto de la Agencia de Protección de Datos, regula su funcionamiento.[II] .

Como indica su página web , "*El objetivo de este espacio es, por un lado, fomentar que los ciudadanos conozcan sus derechos y las posibilidades que la Agencia les ofrece para ejercerlos y, por otro, que los sujetos obligados tengan a su disposición un instrumento ágil que les facilite el cumplimiento de la normativa*".

4.2. Datos de carácter personal.

Definiciones según el art. 3 LOPD y el 5 de RGPD.

- **Dato de carácter personal** es cualquier información (numérica, alfabética, gráfica, fotográfica, acústica, o de cualquier otro tipo) de una persona identificada o identificable. Persona física identificable es toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador o relacionando datos personales.
- **Fichero** es conjunto organizado de datos personales.
- **Tratamiento** es cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.
- **Datos de salud** (art. 5.1.g LOPD) son datos de carácter personal relacionados con la salud. Incluye datos genéticos, de baja laboral, discapacidad, etc.
- **Dato disociado** (RLOPD art. 5.1.e) Son aquellos que no permiten la identificación del interesado. *Seudonimización* es el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional.

Se establecen las siguientes categorías sobres los datos (art. 7 y 8 LOPD):

- Datos personales que revelan la ideología, afiliación, sindical, religión o creencias.
- Datos personales que hagan referencia al origen racial, a la salud y a la vida sexual.
- Datos de carácter personal relativos a la comisión de infracciones penales o administrativas.
- El RLOPD añade los datos genéticos y biométricos que identifiquen a una persona física.

Sólo se deben recoger y tratar los datos de carácter personal que sean **adecuados, pertinentes y no excesivos** (principio de proporcionalidad) y sólo podrán usarse para la finalidad determinada, explicita y legítima para la cual fueron recabados (de acuerdo a la finalidad), y no podrán usarse para una finalidad incompatible a la que motivó la recogida de datos. Deberán ser exactos y puestos al día (calidad), de manera que respondan con veracidad a la realidad de la situación de su titular.

Plazo de conservación; Los datos de carácter personal deberán ser almacenados durante el tiempo necesario para los fines del tratamiento (Principio de limitación del plazo de conservación) y serán cancelados cuando hayan dejado de ser necesarios. En el caso de los datos de salud, se deben considerar otras normas, como la LAP que estable un plazo de 5 años desde la fecha de alta del paciente (salvo algunas excepciones). Finalizado el fin de los datos, se deben bloquear hasta que finaliza el plazo de conservación y su destrucción se debe realizar mediante procedimientos habilitados que garanticen su destrucción. Los datos deben ser cancelados a petición del interesado; derecho de cancelación.

4.3. Agentes relacionados con los datos.

Interesado como persona física titular de los datos objeto de tratamiento. Debe dar consentimiento expreso para que puedan tratarse sus datos personales, lo puede revocar y el responsable le tiene que proporcionar mecanismos para ejercer sus derechos.

Responsable del fichero o responsable del tratamiento: persona física o jurídica que decida sobre la finalidad, contenido y uso del tratamiento. El RGPD mantiene que la responsabilidad última del tratamiento de los datos personales corresponde al responsable. Es quien determina cuál va a ser el tratamiento y su finalidad. Sus responsabilidades son:

1. Aplicar medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente RGPD. Dichas medidas se revisarán y actualizarán cuando sea necesario.
2. Aplicar políticas de protección de datos al tratamiento.
3. Aplicar las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento
4. La adhesión a códigos de conducta podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento

Tiene que poder demostrar que el tratamiento es conforme al RGPD.

Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento. El responsable tiene que tener en cuenta al elegir un encargado de tratamiento que debe cumplir con sus instrucciones respecto de cómo ha de tratar los datos personales para prestar el 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.

El encargado del tratamiento debe formalizar su relación con el responsable mediante un contrato de prestación de servicios u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable, en el que debe constar por escrito, inclusive en formato electrónico y debe contener:

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

- Obligaciones y derechos del responsable.
- 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, compromiso escrito de confidencialidad de las personas autorizadas a tratar los datos.
- Medidas de seguridad y evaluación de riesgos incluyendo todas las circunstancias que puedan incidir en la seguridad de los datos.
- 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.

Delegado de protección de datos (DPD) (art. 37 RGPD). Es una nueva figura que debe ser nombrada por el responsable del tratamiento atendido a sus cualidades profesionales y, en particular, a sus conocimientos especializados del derecho y la práctica en materia de protección de datos. El DPD es el contacto entre el responsable o encargado del tratamiento y las personas cuyos datos tratan, sus datos deben ser publicados por el responsable y es el interlocutor en la empresa con la AEPD.

La AEPD ha elaborado un Esquema de Certificación (EC) [IV] que define como mínimo las siguientes funciones:

a) Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del 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.
j) Realizar consultas a la autoridad de control, en su caso, sobre cualquier otro asunto.

Para ello deberá 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.

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:

1. Cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos.

2. Identificación de las bases jurídicas de los tratamientos.

3. Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.

4. Determinación de la existencia de normativa sectorial que pueda determinar condiciones de tratamiento específico distintas de las establecidas por la normativa general de protección de datos.

5. Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.

6. Establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados.

7. Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.

8. Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado.

9. 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.

10. Diseño e implantación de políticas de protección de datos.

11. Auditoría de protección de datos.

12. Establecimiento y gestión de los registros de actividades de tratamiento.

13. Análisis de riesgo de los tratamientos realizados.

14. 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.

15. Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.

16. 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.

17. Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos.

18. Realización de evaluaciones de impacto sobre la protección de datos.

19. Relaciones con las autoridades de supervisión.

20. Implantación de programas de formación y sensibilización del personal en materia de protección de datos.

El responsable debe poner a disposición del DPD recursos que garanticen que participa de forma adecuada en las cuestiones relativas a la protección, debe respaldarlo en el desempeño de sus funciones, facilitar los recursos que le permitan acceso a los datos y operaciones de tratamiento, formación, garantizar sus funciones y no puede ser cesado en el desempeño de sus funciones.

4.4. Obligaciones de los responsables.

4.4.1. Principio de Información o de Transparencia.

Se define como **consentimiento del interesado** (art. 3.h LOPD) toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

El art. 4 RGPD, define **consentimiento** como una manifestación de voluntad libre, especifica, informada e inequívoca por la que el interesado acepta, mediante una declaración o una clara acción afirmativa . Se exige además consentimiento explícito para los datos pertenecientes a las categorías especiales.

Con el RGPD, desparece el consentimiento tácito y no se pueden usar las casillas premarcadas y si existen varios fines se debe prestar consentimiento para cada uno de ellos. Si hay consentimiento previo que cumple los criterios del RGPD, no es necesario recogerlo de nuevo y la demostración de la validez del consentimiento es responsabilidad del responsable del tratamiento.

El consentimiento es revocable, siendo necesario informar al interesado de esta posibilidad.

Licitud del tratamiento (art.6 RGPD). 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:

a. La ejecución de un contrato.
b. Cumplir una obligación legal.
c. Proteger los intereses vitales de la persona.
d. El cumplimiento de una misión realizada en interés público.
e. Satisfacer los intereses legítimos del responsable del tratamiento.

Para el tratamiento de datos especiales (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 sexual o las orientación sexuales de una persona física) el interesado debe dar su consentimiento explícito (art. 9.2.a RGPD).

Según art. 5 LOPD y 12 a 14 RGPD, cuando se soliciten datos personales, se le deberá informar con carácter previo a la recogida, de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, mediante la correspondiente cláusula de privacidad, por escrito o por medios electrónicos, en textos informativos, carteles, impresos, cuestionarios, de lo siguiente:

a. De la existencia de un fichero o tratamiento de datos de carácter personal.
b. De la finalidad de la recogida de éstos,.
c. De los destinatarios de la información, del carácter obligatorio o no de la revelación de los datos personales, así como de las consecuencias de la negativa a suministrarlos.
d. De la identidad y dirección del responsable del tratamiento.
e. Del plazo de conservación de los datos o, cuando no sea posible, los criterios utilizados para determinar este plazo.
f. De la base jurídica del tratamiento de datos de carácter personal.
g. De la posibilidad de ejercitar ante el responsable del tratamiento, además de los tradicionales derechos de acceso, rectificación, cancelación y oposición, los nuevos derechos a la portabilidad de los datos y a la limitación de su tratamiento.
h. Del derecho a retirar el consentimiento en el que se basa el tratamiento de los datos en cualquier momento.
i. Del derecho a la presentación de una reclamación ante la AEPD.

j. Los datos del DPD.
k. De la intención de transferir los datos a un tercer país, con referencia a las garantías adecuadas prestadas para dicha transferencia y el derecho a obtener copia de las mismas, la existencia de la elaboración de perfiles, junto con información sobre la lógica aplicada, y la importancia y consecuencias de este tratamiento.
l. Existencia de decisiones automatizadas, incluida la elaboración de perfiles.

El art. 12.3 del RLOPD dice que es responsabilidad del responsable del tratamiento la acreditación del cumplimiento del deber de información así como de haber obtenido el consentimiento.

4.4.2. Principio de seguridad.

Seguridad (art. 9 LOPD). El encargado del tratamiento deberá adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal, eviten su alteración, pérdida o acceso no autorizado. Sin estas medidas no se deben registraran datos en ficheros.

En el RLOPD se definen diferentes niveles de seguridad en función de los tipos de datos que sean objeto de tratamiento.

- **Nivel Alto**: Datos sensibles, entre los que se encuentran los datos de salud, vida sexual, religión.
- **Nivel Medio**: Datos de infracciones y servicios financieros.
- **Nivel Básico**: Resto de datos.

El mismo reglamento establece las medidas de seguridad a aplicar para cada nivel, que se muestran en la Tabla 4.

Medidas De Seguridad Por Niveles	
Medidas de seguridad de Nivel Básico	Documento de seguridad. Régimen de funciones y obligaciones del personal. Registro de incidencias. Identificación y autenticación de usuarios. Control y Registro de acceso. Gestión de soportes. Copias de respaldo y recuperación.
Medidas de seguridad de Nivel Medio	Medidas de seguridad de nivel básico Responsable de seguridad Controles periódicos de verificación Auditoria bianual (interna o externa que verifique el cumplimiento) Medidas adicionales de identificación y autenticación Control de acceso físico Medidas adicionales de gestión de soportes Registro de incidencias Pruebas con o sin datos reales
Medidas de seguridad de Nivel Alto	Medidas de seguridad de nivel básico y medio Seguridad en la distribución de soportes Registro de accesos Medidas adicionales para copias de respaldo Cifrado de telecomunicaciones

Tabla 4 Medidas de seguridad según RLOPD en función del nivel de los datos.

El RLOPD establece la obligatoriedad de tener y mantener actualizado el **Documento de Seguridad** (art. 81 (el RGPD habla de registro de actividades); "*El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información*". Debe contener:

1. Ámbito de aplicación: con especificación detallada de los recursos protegidos;
2. Funciones y obligaciones del personal,
3. Procedimientos de notificación, gestión y respuesta ante incidencias.
4. Medidas adoptadas en el transporte, destrucción y/o reutilización de soportes y documentos.
5. Medidas, normas, procedimientos, reglas y estándares de seguridad.
6. Estructura y descripción de los ficheros y sistemas de información.
7. Procedimiento de copias de respaldo y recuperación de datos.
8. Identificación del responsable de seguridad.
9. Control periódico del cumplimiento del documento.
10. En caso de haber contratado la prestación de servicios por terceros, indicar referencia al contrato de acceso a datos por cuenta de terceros y su vigencia.

El art 32 RGPD, "*el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo*". Que incluyan:

a) La seudonimización y el cifrado de datos personales.
b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
c) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.
d) Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

En el caso de violación de seguridad, el responsable del tratamiento debe comunicar a la AEPD a más tardar 72 horas después de que haya tenido constancia de ella (art 33 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, el responsable del tratamiento lo debe comunicará al interesado (art 34 RGPD).

4.4.3. Principio de confidencialidad.

El art. 10 de la LOPD, supone la obligación de guardar secreto y confidencialidad sobre los datos objeto de tratamiento y es aplicable a todos aquellos que tratan datos de carácter personal. Cualquiera que trate dados de carácter personal está obligado al secreto incluso después de finalizar las relaciones contractuales con el responsable del fichero.

4.4.4. Registro de actividades de tratamiento (art. 30 RGDP).

El responsable del tratamiento debe llevar un registro de actividades tratamiento. Ya no es obligatorio dar de alta al fichero en la AEPD, pero el registro debe estar a su disposición. Este registro debe contener la siguiente información:

- 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.
- 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 AEPD. Es el principio de **responsabilidad proactiva**, que supone que el responsable del tratamiento deberá ser capaz de demostrar que cumple con las obligaciones derivadas de la normativa de protección de datos y en ese sentido la necesidad de generar evidencias de cumplimiento y adopción de medidas como políticas internas de protección de datos.

4.4.5. Análisis de riesgos (art. 32 y 35 RGPD).

El RGPD plantea el análisis de riesgos como necesidad de evaluar con carácter previo el impacto que un tratamiento de datos puede tener en los derechos de las personas; "*daños y perjuicios físicos, discriminación, usurpación de identidad, pérdida de reputación, daños a la confidencialidad y perjuicios sociales*".

"*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, …";* art. 32.1.

"*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…*"; art. 35.1.

En los tratamientos de riesgos escaso, se puede realizar el tratamiento únicamente con la implantación de las medidas mínimas necesarias para garantizar la seguridad de los datos.

Cuando el riesgo para los derechos y libertades de las personas sea alto, como los datos sanitarios relativos a los pacientes, es 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 los derechos y libertades de las personas.

La AEPD ha publicado una guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD [V].

4.4.6. Cesión de datos a terceros.

El art. 11 de la LOPD, indica la necesidad de que para cualquier comunicación de datos que se realice a un tercero deba recabarse el consentimiento del interesado debidamente informado y, además, sólo podrá realizarse para el

cumplimiento de los fines directamente relacionados con las funciones del cedente. Salvo cesiones autorizadas por ley, datos de salud en casos de urgencia o estudios, cuando se tenga interés legítimo en el tratamiento.

Para realizar transferencias de datos entre países (RGDP art. 44 a 46) los responsables deben cumplir el reglamento, y el país tiene que garantizar la protección según la Comisión o en su caso hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.

4.4.7. Códigos de conducta y certificación (art. 40 y 42 RGDP).

Las autoridades promoverán la elaboración de códigos de conducta destinados a contribuir a la correcta aplicación RGPD, teniendo en cuenta las características específicas de los distintos sectores de tratamiento y las necesidades específicas de las microempresas y las pequeñas y medianas empresas. Los códigos de conducta deberán referirse al modo de aplicar el reglamento y se deben presentar a la AEPD para que indique su adecuación al reglamento.

También promoverán la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el RGPD en las operaciones de tratamiento de los responsables y los encargados.

4.5. Derechos de los interesados.

La LOPD reconoce los derechos de acceso, rectificación, cancelación y oposición (son conocidos como derechos ARCO), y el RGPD el derecho de limitación de tratamiento y la portabilidad de los datos. Los responsales del tratamiento tienen que habilitar procedimientos para que dichos derechos puedan ser ejercitarlos. En la Tabla 5 se pueden ver un resumen de los derechos.

Resumen de derechos					
Acceso	**Rectificación**	**Cancelación**	**Oposición**	**Limitación**	**Portabilidad**
Conocer qué datos son tratados por el Responsable del Fichero, con qué finalidad y en qué fi cheros están incluidos	Derecho del interesado a rectificar sus datos de carácter personal, cuando sean inexactos o incompletos	Derecho del interesado a que se cancelen en el tratamiento los datos personales que resulten inadecuados o excesivos	Cese en el tratamiento de los datos	Obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumplan algunas condiciones	A recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común
1 mes	10 días	10 días	10 días		
El responsable del fichero debe proporcionar los medios para su ejercicio Su ejercicio será gratuito salvo cuando se pida otra copia por el interesado que se podrá cobrar un canon razonable basado en los costes administrativos.					

Tabla 5 Derechos de los interesados.

4.5.1. Derecho de acceso (arts. 15 LOPD, 27-30 RLOPD y 15 RGPD).

"El interesado tiene derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos". Este derecho se puede ejercitar una vez cada 12 meses según el RLOPD.

La solicitud de acceso deberá hacerse por escrito o por medios electrónicos, acreditando la identidad del interesado y el responsable debe atender obligatoriamente la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud.

La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, correo electrónico u otros sistemas de comunicaciones electrónicas, cualquier otro sistema adecuado y siempre en forma legible e inteligible, sin utilizar claves. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.

El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos.

En el caso de pacientes fallecidos, sólo se facilitará el acceso a su historia clínica a las personas vinculadas a ellos (herederos), previa su acreditación, salvo que el fallecido lo hubiese prohibido expresamente y así se acredite. No se facilitará información de las historia clínica que afecte a la intimidad del fallecido ni a las anotaciones subjetivas de los profesionales (art. 18 LPA), ni que perjudique a terceros.

En el caso de menores, el menor de edad mayor de 14 años podrá ejercitar el derecho de acceso los datos de su historia clínica, así como los titulares de la patria potestad.

4.5.2. Derecho de rectificación (arts. 16 LOPD y 31-33 RLOPD y 15 RGPD).

A través de este derecho el interesado indica que se modifiquen sus datos personales cuando estos sean inexactos o incompletos. El procedimiento a seguir será el siguiente:

1. La solicitud, por escrito o medios electrónicos, deberá indicar a qué datos se refiere y la corrección a efectuar, justificando documentalmente lo solicitado.
2. Se deberá proceder a la rectificación de los datos en el plazo máximo de diez días desde la recepción de la solicitud, que además se comunicará oportunamente.
3. En caso de que los datos rectificados hubieran sido cedidos con anterioridad a la solicitud, el responsable deberá comunicar la rectificación efectuada al cesionario en idéntico plazo a fin de que éste proceda asimismo a rectificar los datos.
4. Se debe comunicar la rectificación al interesado.

4.5.3. Derecho de cancelación (arts. 16 LOPD y 31-33 RLOPD y 15 RGPD).

A través de este derecho el interesado puede solicitar que se ponga fin al tratamiento de sus datos personales que resulten ser inadecuados o excesivos.

El RGPD lo llama derecho al **olvido** "*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.
b) El interesado retire el consentimiento en que se basa el tratamiento.
c) El interesado se oponga al tratamiento.
d) Los datos personales hayan sido tratados ilícitamente.
e) Los datos personales deban suprimirse para el cumplimiento de una obligación legal.

f) Los datos personales se hayan obtenido en los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información".

El procedimiento a seguir será el siguiente:

1. En la solicitud, por escrito o medios electrónicos, el interesado deberá indicar a qué datos se refiere la cancelación, justificando documentalmente lo solicitado.
2. Se deberá resolver la solicitud en el plazo máximo de diez días desde su recepción.
3. En caso de que los datos cancelados hubieran sido cedidos con anterioridad a la solicitud, se deberá comunicar la cancelación efectuada al cesionario en idéntico plazo a fin de que éste proceda asimismo a cancelar los datos;
4. Sólo se cancelarán aquellos datos de carácter personal cuyo tratamiento no deriva del cumplimiento de una relación contractualmente entre la persona interesada en la cancelación o los que exista obligación legal. En el caso de las historias clínicas la LAP impone la obligación de conservar los datos contenidos en las historias clínicas por el plazo que resulte pertinente, nunca inferior a cinco años.
5. Se debe comunicar la cancelación al interesado.

4.5.4. Derecho de oposición (art. 5, 6, 17, 18, 28,30 LOPD, 34-36 RLOPD y 21 RGPD).

El derecho de oposición es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los siguientes supuestos:

1. Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario.
2. Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, en los términos previstos en el art. 51 del RGPD, cualquiera que sea la empresa responsable de su creación.
3. Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal, en los términos previstos en el art. 36.

El interesado lo deberá ejercitar mediante solicitud, por escrito o medios electrónicos y el responsable deberá atender la solicitud en el plazo máximo de diez días desde su recepción, excluyendo del tratamiento los datos relativos al interesado, o denegando motivadamente la solicitud (por ejemplo porque el tratamiento sea imprescindible para la prestación del servicio sanitario).

Para evitar la publicidad no deseada de entidades o empresas a las que no haya facilitado sus datos o sea cliente existen las **listas Robinson.** Son directorios creados con la finalidad de ayudar a particulares a librarse del acoso publicitario a través de llamadas telefónicas, SMS, correos electrónicos, por correo postal o fax, practicado por varias compañías, particularmente las operadoras telefónicas. La más difundida en España fue creada por la Federación de Comercio Electrónico y Marketing Directo FECEMD en 1993.

4.5.5. Derecho a la limitación del tratamiento (art. 18 RGPD).

El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumplan algunas condiciones: el interesado impugne la exactitud de los datos personales, el tratamiento sea ilícito, el responsable ya no necesite los datos personales para los fines del tratamiento, el interesado se haya opuesto al tratamiento.

4.5.6. Derecho a la portabilidad de los datos (art. 20 RGPD).

El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando

El interesado tendrá derecho bien recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, para transmitirlos, si lo desea, a otro responsable del tratamiento, o incluso para otros usos particulares, o bien a que los datos personales se transmitan directamente de responsable a responsable, siempre y cuando sea técnicamente posible; cuando:

1. El tratamiento de datos debe basarse en el consentimiento del interesado o en la ejecución de un contrato; por lo que este derecho no será aplicable cuando la base jurídica para el tratamiento sea otra (obligación legal, tratamiento de datos por Administraciones Públicas…);
2. El tratamiento de los datos personales se efectúe por medios automatizados; por lo que no es aplicable al tratamiento de datos en soporte papel.

4.6. Infracciones y sanciones.

El incumplimiento de las obligaciones establecidas en materia de protección de datos de carácter personal puede suponer importantes sanciones que de detallan a continuación en la Tabla 6.

Sanciones y multas			
LOPD	Leves	1. Incumplimiento del deber de información al paciente 2. La transmisión de datos a un encargado del tratamiento sin formalizar contrato de acceso a datos por cuenta de terceros	900 a 40.000 €
	Graves	1.Introducir datos médicos de un paciente en otra historia clínica 2. No adoptar las debidas medidas de seguridad 3. No obtener el consentimiento del paciente cuando sea necesario 4. Entregar a un paciente para que firme un documento con datos de otro paciente 5. Obstaculizar el ejercicio de los derechos 6. No atender los requerimientos de la AEPDD	40.001 a 300.000 €
	Muy graves	1. Cesión de datos de salud sin el consentimiento del paciente 2. No cesar en el tratamiento de datos personales cuando lo hubiera requerido el Director de la AEPD	Hasta 300.000 €
RGPD art. 83		1.Incumplimiento de la obligación del responsable en relación con el Delegado de Protección de Datos. 2. La transmisión de datos a un encargado del tratamiento sin formalizar contrato de acceso a datos por cuenta de terceros	10.000.000 o 2% volumen negocio total anual
		1. Incumplimiento de los principales básicos del tratamiento 2. No atender los derechos de los ciudadanos	20.000.000 o 4% volumen negocio total anual

Tabla 6 Tabla resumen de sanciones.

Existe la posibilidad de que el interesado pueda reclamar frente al responsable del tratamiento indemnización por daños y perjuicios sufridos como consecuencia de una infracción de la normativa en materia de protección de datos.

4.7. Borrador de la nueva Ley de Protección de datos.

Con fecha 9 de octubre de 2018 se ha publicado en el diario Boletín Oficial de Las Cortes Generales, el informe de la ponencia 121/000013 Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal. Este proyecto (cuando se apruebe) es la adaptación de la normativa española al RGPD. En general mantiene las definiciones, derechos, deberes del reglamento. En los puntos siguientes muestro los aspectos que considero novedosos o relevantes.

Datos de pacientes fallecidos. Detalla que el acceso puede ser por hederos, padres o representantes legales o instituciones (ministerio Fiscal y expresamente autorizadas por el difunto) salvo que la persona fallecida lo hubiese prohibido (art. 3).

El art. 9 traslada las definiciones del reglamento de las categorías especiales de datos y en el 10 hace mención particular a los datos de naturaleza penal.

En los art. 19 al 26 detalla disposiciones aplicables a tratamientos concretos.
Artículo 19. Tratamiento de datos de contacto, de empresarios individuales **y de profesionales liberales.**
Artículo 20. Sistemas de información crediticia (listas de morosos).
Artículo 21. Tratamientos relacionados con la realización de determinadas operaciones mercantiles; miembros de sociedades, transmisiones de negocios, etc.
Artículo 22. Tratamientos con fines de videovigilancia.
Artículo 23. Sistemas de exclusión publicitaria (listas robinson).
Artículo 24. Sistemas de información de denuncias internas.
Artículo 25. Tratamiento de datos en el ámbito de la función estadística pública.
Artículo 26. Tratamiento de datos con fines de archivo en interés público por parte de las Administraciones Públicas.
Artículo 27. Tratamiento de datos relativos a infracciones y sanciones administrativas.

Respecto a los códigos de conducta y entidades de acreditación, estos conceptos son nuevos en la ley ya que no estaban recogidos en la LOPD previa, si bien están transcritos del reglamento.

El título VII, está dedicado a las autoridades de protección y en particular a La Agencia Española de Protección de Datos. En los art. 44 al 62 detalla todos los aspectos de organización, régimen jurídico, económico, órganos de gobierno, así como las diferentes competencias.

En relación con los incumplimientos, detallas el régimen jurídico y el procedimiento para realizar denuncias o auditorias sobre vulneración de derechos. En los art. 72 a 74 enumera de forma detallada los distintos tipos de infracciones: muy graves, graves y leves. Se mantienen las sanciones de Reglamento.

El aspecto más novedoso en la incorporación en el Título X de la garantía de derechos digitales, entre los que destacan derechos de los trabajadores (a la desconexión, limitar la geolocalización o la intimidad en el uso de dispositivos de la empresa o en videovigilancia en el trabajo), derechos de los menores y el derecho al testamento digital.

Artículo 80. Derecho a la neutralidad de Internet.
Artículo 81. Derecho de acceso universal a Internet.
Artículo 82. Derecho a la seguridad digital.
Artículo 83. Derecho a la educación digital.
Artículo 84. Protección de los menores en Internet.
Artículo 85. Derecho de rectificación en Internet.
Artículo 86. Derecho a la actualización de informaciones en medios de comunicación digitales.
Artículo 87. Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral.
Artículo 88. Derecho a la desconexión digital en el ámbito laboral.

Artículo 89. Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.
Artículo 90. Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral.
Artículo 91. Derechos digitales en la negociación colectiva.
Artículo 92. Protección de datos de los menores en Internet.
Artículo 93. Derecho al olvido en búsquedas de Internet.
Artículo 95. Derecho de portabilidad en servicios de redes sociales y servicios equivalentes.
Artículo 96. Derecho al testamento digital.

Artículo 58 bis. Utilización de medios tecnológicos y datos personales en las actividades electorales. Los políticos se autorizan a si mismo a recopilar nuestros datos de las páginas web y también se autorizan para podernos mandar propaganda a nuestros correos y redes sociales.

5. Herramientas comunes de usuario.

5.1. Correo electrónico.

Los contenidos del correo electrónico son de escasa significación creativa por lo que no es aplicable la protección de derechos de autor.

Si es aplicable el art. 197 del CP sobre descubrimiento y revelación de secretos; "*El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses*".

En relación con los contenidos que se pueden enviar en el correo, es necesario considerar que pudieran estar protegidos por la LPI art. 10, por lo que en su caso debería contarse con la autorización del propietario de los derechos.

Respecto al uso de correo para el envió de informes médicos entres profesionales el Informe Jurídico 285/2008 de la AEPD indica la necesidad de controlar el acceso a esos datos (art. 103 RLOP) y en caso de remitirse los datos a través de redes publicas o redes inalámbricas de comunicaciones electrónicas, la transmisión "*se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros*", tal y como dispone el art. 105 del RLOPD.

Respecto al cifrado, en el Informe 0494/2009 la AEGP indica: *"Los productos que generan archivos PDF o el realizado por WinZip tienen vulnerabilidades conocidas y se disponen de herramientas de libre distribución que aprovechan dichas vulnerabilidades. Más concretamente, no sólo se pueden obtener en Internet fácilmente utilidades que rompen las protecciones de los archivos PDF o ZIP, sino que el propio algoritmo en el que descansa la cifra de documentos PDF, el algoritmo RC4, es manifiestamente vulnerable"*.

Por lo tanto para el envío de informes médicos por correo es necesario usar un sistema robusto de cifrado.

5.2. Whatsapp y redes sociales.

Para transmitir datos de salud mediante los nuevos sistemas de comunicación, se deben garantizar la seguridad, confidencialidad e integridad de la información. Considerando que son datos especialmente protegidos y que no se pueden garantizar la seguridad y la confidencialidad no se deben usar estos canales para transmitir datos personales y menos aún los especialmente protegidos como los de salud.

6. Anexos I.

6.1. Referencias.

I. Guía sobre contratación publica electrónica de Inteco.
II. Estatuto de la Agencia de Protección de Datos.
III. Guía sobre el uso de videocámaras para seguridad y oras finalidades.
IV. Esquema de certificación de delegados de protección de datos de la Agencia Española de Protección de Datos.
V. Guía práctica de Análisis de riesgos en los tratamientos de datos personales sujetos al RGPD. para el cumplimiento de la normativa sobre Guía práctica del Ilustre Colegio Oficial de Médicos de Madrid sobre protección de datos de carácter personal.
VI. Adaptación al reglamento General de protección De datos para el sector Sanitario. SEDISA.

6.2. Tablas.

7. Anexo II. Ejemplo de política de cookies.

7.1. Política de cookies

Cookies (mensaje de alerta). Utilizamos cookies propias y de terceros para mejorar nuestros servicios y mostrarle publicidad relacionada con sus preferencias mediante el análisis de sus hábitos de navegación. Si continua navegando, consideramos que acepta su uso. Puede cambiar la configuración u obtener más información 'aquí'.

POLITICA DE COOKIES

Cookie es un fichero que se descarga en su ordenador al acceder a determinadas páginas web. Las cookies permiten a una página web, entre otras cosas, almacenar y recuperar información sobre los hábitos de navegación de un usuario o de su equipo y, dependiendo de la información que contengan y de la forma en que utilice su equipo, pueden utilizarse para reconocer al usuario.. El navegador del usuario memoriza cookies en el disco duro solamente durante la sesión actual ocupando un espacio de memoria mínimo y no perjudicando al ordenador. Las cookies no contienen ninguna clase de información personal específica, y la mayoría de las mismas se borran del disco duro al finalizar la sesión de navegador (las denominadas cookies de sesión).

La mayoría de los navegadores aceptan como estándar a las cookies y, con independencia de las mismas, permiten o impiden en los ajustes de seguridad las cookies temporales o memorizadas.

Sin su expreso consentimiento –mediante la activación de las cookies en su navegador–XXXXX no enlazará en las cookies los datos memorizados con sus datos personales proporcionados en el momento del registro o la compra.

¿Qué tipos de cookies utiliza esta página web?

- Cookies técnicas: Son aquéllas que permiten al usuario la navegación a través de una página web, plataforma o aplicación y la utilización de las diferentes opciones o servicios que en ella existan como, por ejemplo, controlar el tráfico y la comunicación de datos, identificar la sesión, acceder a partes de acceso restringido, recordar los elementos que integran un pedido, realizar el proceso de compra de un pedido, realizar la solicitud de inscripción o participación en un evento, utilizar elementos de seguridad durante la navegación, almacenar contenidos para la difusión de videos o sonido o compartir contenidos a través de redes sociales.

- Cookies de personalización: Son aquéllas que permiten al usuario acceder al servicio con algunas características de carácter general predefinidas en función de una serie de criterios en el terminal del usuario como por ejemplo serian el idioma, el tipo de navegador a través del cual accede al servicio, la configuración regional desde donde accede al servicio, etc.

- Cookies de análisis: Son aquéllas que bien tratadas por nosotros o por terceros, nos permiten cuantificar el número de usuarios y así realizar la medición y análisis estadístico de la utilización que hacen los usuarios del servicio ofertado. Para ello se analiza su navegación en nuestra página web con el fin de mejorar la oferta de productos o servicios que le ofrecemos.

- Cookies publicitarias: Son aquéllas que, bien tratadas por nosotros o por terceros, nos permiten gestionar de la forma más eficaz posible la oferta de los espacios publicitarios que hay en la página web, adecuando el contenido del anuncio al contenido del servicio solicitado o al uso que realice de nuestra página web. Para ello podemos analizar sus hábitos de navegación en Internet y podemos mostrarle publicidad relacionada con su perfil de navegación.

- Cookies de publicidad comportamental: Son aquéllas que permiten la gestión, de la forma más eficaz posible, de los espacios publicitarios que, en su caso, el editor haya incluido en una página web, aplicación o plataforma desde la que presta el servicio solicitado. Estas cookies almacenan información del comportamiento de los usuarios obtenida a

través de la observación continuada de sus hábitos de navegación, lo que permite desarrollar un perfil específico para mostrar publicidad en función del mismo.

Cookies de terceros: La Web de XXXXX puede utilizar servicios de terceros que, por cuenta de XXXXX, recopilaran información con fines estadísticos, de uso del Site por parte del usuario y para la prestacion de otros servicios relacionados con la actividad del Website y otros servicios de Internet.

En particular, este sitio Web utiliza Google Analytics, un servicio analítico de web prestado por Google, Inc. con domicilio en los Estados Unidos con sede central en 1600 Amphitheatre Parkway, Mountain View, California 94043. Para la prestación de estos servicios, estos utilizan cookies que recopilan la información, incluida la dirección IP del usuario, que será transmitida, tratada y almacenada por Google en los términos fijados en la Web Google.com. Incluyendo la posible transmisión de dicha información a terceros por razones de exigencia legal o cuando dichos terceros procesen la información por cuenta de Google.

El Usuario acepta expresamente, por la utilización de este sitio, el tratamiento de la información recabada en la forma y con los fines anteriormente mencionados. Y asimismo reconoce conocer la posibilidad de rechazar el tratamiento de tales datos o información rechazando el uso de Cookies mediante la selección de la configuración apropiada a tal fin en su navegador. Si bien esta opción de bloqueo de Cookies en su navegador puede no permitirle el uso pleno de todas las funcionalidades del sitio.

Puede usted permitir, bloquear o eliminar las cookies instaladas en su equipo mediante la configuración de las opciones del navegador instalado en su ordenador:

- Chrome, desde http://support.google.com/chrome/bin/answer.py?hl=es&answer=95647
- Explorer, desde https://support.microsoft.com/es-es/help/17442/windows-internet-explorer-delete-manage-cookies
- Firefox, desde http://support.mozilla.org/es/kb/habilitar-y-deshabilitar-cookies-que-los-sitios-we
- Safari, desde http://support.apple.com/kb/ph5042

Si tiene dudas sobre esta política de cookies, puede contactar con XXXXX en info@XXXXX(punto)com.

7.2. Tabla ejemplo tomada del sitio red.es.

Cookie	Tipo	Temporalidad	Titularidad	Finalidad	Opt-Out
JavaScript/Sesión	Técnica	Temporal	Propia	Garantizar el correcto funcionamiento del sitio, detectando si el usuario que ha accedido tiene habilitada la posibilidad de utilizar JavaScript (lenguaje de programación interpretado que, entre otras cosas, permite una mejora en la experiencia de usuario de este Sitio), o de mantener la sesión en el gestor de contenidos.	Neutro, por lo que no utiliza cookies
Google Analytics I	Analítica	Permanente	Ajena	Generar un identificador de usuario único, que es el que se utiliza para hacer recuento de cuántas veces visita el sitio un usuario, así como la fecha de la primera y la última vez que visitó la web.	Neutro
Google Analytics II	Analítica	Temporal	Ajena	Registrar la fecha y hora de acceso a cualquiera de las páginas del Sitio.	Neutro
Google Analytics III	Analítica	Temporal	Ajena	Comprobar la necesidad de mantener la sesión de un usuario abierta o crear una nueva.	Neutro
Google Analytics IV	Analítica	Temporal	Ajena	Identificar la sesión del usuario, para recoger la ubicación geográfica aproximada del ordenador que accede al Sitio con efectos estadísticos.	Neutro
Piwik I	Analítica	Temporal	Propia	Recoger la sesión del usuario que accede al Sitio, para identificar información estadística relativa a motores y términos de búsqueda usados, idiomas utilizados, proveedores de servicio de Internet, origen de los visitantes en relación al país, navegadores y plugins usados, remitentes (sitios web visitados inmediatamente antes), duración de las visitas, páginas de inicio, páginas de salida y tasas de interrupción entre otros. Esta información se recoge y se utiliza únicamente para mejorar el uso del sitio web y no se comunica a tercero alguno.	Neutro
Piwik II	Analítica	Temporal	Propia	Misma que la anterior	Neutro
Adaptive Image	Técnica	Temporal	Propia	Controla el tamaño correcto de las imagenes segun resolución de pantalla.	Neutro
ais	Técnica	Temporal	Propia	Controla el tamaño correcto de las imagenes segun resolución de pantalla.	Neutro
lang	Técnica	Temporal	Propia	Controla el idioma del navegador para servir el portal en el idioma especificado.	Neutro
Sociales (Facebook, YouTube, Twitter, LinkedIn, etc.).	Sociales	Depende de cada red social.			