PERFIL SIREN - StRS

Protección de Datos Personales – PDP2019

Grupo de Investigación en Ingeniería del Software – Departamento de Informática y Sistemas – Universidad de Murcia

Esta plantilla se proporciona como punto de comienzo para asistir en el proceso de definición de la estructura del documento **Stakeholder Requirements Specification** (**StRS**) o Especificación de Requisitos de Stakeholder. Esta plantilla está basada en el estándar ISO/IEC/IEEE Std 29148, adaptada a las necesidades impuestas por las características de un perfil (conjunto de requisitos relacionados entre sí y pertenecientes a un sector "horizontal" específico).

El StRS especifica los requisitos para los interesados y los métodos a emplear para asegurar que cada requisito ha sido cumplido. La representación y contenido de esta plantilla puede ser expandida o contraída por el cliente o por la comunidad técnica.

Preguntas y sugerencias: jnr@um.es, aleman.um.es

Perfil SIREN PDP ALTO

Stakeholder Requirements Specification (StRS)
Especificación de Requisitos de Stakeholder

Revisión 1.0 28/01/2019

Historial de Revisiones

Fecha	Revisión	Descripción	Autores
20/12/2018	Revisión 0.1	Inicial	Francisco Marquina Joaquín Nicolás José L. Fernández
28/01/2019	Revisión 0.3	Seguimiento	Francisco Marquina Joaquín Nicolás José L. Fernández
04/03/2019	Revisión 0.5	Seguimiento	Francisco Marquina Joaquín Nicolás José L. Fernández
08/05/2019	Revisión 1.0	Final	Francisco Marquina Joaquín Nicolás José L. Fernández

Índice de contenido

1. Introducción

Para realizar la organización del apartado de historias de usuario (HU) (Sección 5) nos hemos basado en el Reglamento Europeo 2016/679 cuya entrada en vigor fue el 25 de mayo de 2018 [art. 99], el nuevo proyecto de Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (actualmente en fase avanzada de tramitación), el RD 1720/2007 de desarrollo de la actual LOPD y el RD 3/2003 por el que se regula el Esquema Nacional de Seguridad.

1.1 Propósito de negocio

Los catálogos pueden ser dominios de aplicación horizontales (denominados perfiles: seguridad, portales, comercio electrónico, firma digital, etc.) y verticales (denominados dominios: seguros, banca, automoción, administración local, etc.). En este caso, y como aplicación de SIREN, presentamos el siguiente perfil desarrollado en este documento:

PDP, Protección de Datos Personales, compatible con la nueva Ley Orgánica de Protección de Datos de Carácter Personal (LOPD), el Real Decreto 1720/2007 [RD 1720/2007], el reglamento Europeo 2016/679 [R. UE 2016/679] y el Esquema Nacional de Seguridad RD 3/2003.

Este perfil PDP (Protección de Datos Personales) sigue la propuesta SIREN (ver glosario de términos, Sección 1.3) basada en la utilización de un repositorio de requisitos estructurado por catálogos. Esta propuesta también se puede utilizar con cualquier metodología de desarrollo, pues fundamentalmente se trata de utilizar requisitos textuales con atributos. Si partimos de un conjunto de requisitos que ya han sido especificados para otros proyectos y/o dominios, podremos reutilizarlos y mejorar así la precisión y completitud de las especificaciones de requisitos del proyecto actual, reduciendo, además, el tiempo de producir dicha especificación.

La nueva LOPD, que adapta el reglamento europeo de PD a la legislación española, tiene por objeto recoger los requisitos para que un sistema de información garantice la protección en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal. Por otra parte, el Real Decreto 1720/2007 tiene como propósito desarrollar aquellos aspectos de la LOPD que se ha visto necesario legislar con mayor precisión. El ENS pretende homogeneizar las políticas y principios de seguridad en las Administraciones Públicas en la utilización de medios electrónicos para una eficaz protección de la información.

Cualquier sistema de información que incorpore los requisitos definidos en este perfil debería superar con éxito sino todas, la mayor parte de las exigencias que la legislación impone al tratamiento de datos personales incluyendo las medidas del ENS, de acuerdo con el nivel de protección exigido.

La especificación de requisitos de Stakeholder (StRS), del estándar 29148 (ISO, IEC, & IEE., 2011), debe incluir: (1) requisitos del negocio, organizativos y de usuario; (2) requisitos de seguridad (security), seguridad a terceros (safety) y privacidad; (3) requisitos de ingeniería de factores humanos o ergonomía (estudio de datos biológicos y tecnológicos aplicados a problemas de mutua adaptación entre el hombre y la máquina); (4) requisitos de operaciones y

mantenimiento; (5) y restricciones de diseño. Estos requisitos serán adaptados para el fin de que sea un perfil suponiendo que nuestro "negocio" es el cumplimiento de la legislación española existente sobre PDP y nuestro "sistema" el catálogo de requisitos SIREN.

1.2 Alcance del negocio

El alcance de este perfil es cubrir en materia de sistemas informáticos el reglamento europeo de PD, la nueva LOPD en tramitación que lo adapta, el RD que desarrolla la anterior LOPD y el Esquema Nacional de Seguridad. Todo ello para conseguir un alto nivel de adecuación a la normativa española vigente tanto para las Administraciones Públicas como resto de entidades jurídicas para las que sea de aplicación.

Los requisitos del presente documento serán de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

Todo tratamiento de datos de carácter personal (ya sea automatizado o no) se regirá por la normativa de Protección de Datos Europea, cuando el responsable o encargado del tratamiento estén establecidos en la Unión, con independencia de donde se realice el tratamiento de los datos. También se aplicará al tratamiento de datos personales de interesados que residan en la Unión por parte de un posible responsable o encargado no establecido en la Unión cuando las actividades del tratamiento estén relacionadas con el control de su comportamiento o la oferta de bienes o servicios a dichos interesados. Además de esto, si el responsable o encargado del tratamiento está establecido en España le será de aplicación la legislación española, nueva LOPD y GDD, reglamento de desarrollo. Con la particularidad de que si es una Administración Pública también le será de aplicación el ENS, así como también a aquellos entes jurídicos que se relacionen con las AAPP y se les exija el cumplimiento con el ENS.

Por ejemplo, cuando una base de datos se encuentre localizada fuera de territorio español pero su responsable y el tratamiento se realicen en una AAPP, el fichero debe seguir tanto la normativa europea como española. El régimen de protección de los datos de carácter personal que se establece en el presente perfil no será de aplicación al tratamiento de datos personales:

a. en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión

b. por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE

c. efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas

d. por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención

Los tratamientos a los que no sea directamente aplicable el Reglamento (UE) 2016/679 por afectar a actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea, se regirán por lo dispuesto en su legislación específica si la hubiere y supletoriamente

por lo establecido en el citado reglamento y en la nueva LOPD. Se encuentran en esta situación, entre otros, los tratamientos realizados al amparo de la legislación orgánica del régimen electoral general, los tratamientos realizados en el ámbito de instituciones penitenciarias y los tratamientos derivados del Registro Civil, los Registros de la Propiedad y Mercantiles.

El alcance del RD es establecer las medidas de índole técnica y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos de carácter personal sujetos al régimen de la Ley Orgánica 15/1999, de 13 de diciembre.

La finalidad del ENS es la creación de condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita a los ciudadanos y a las AAPP, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios. Como por ejemplo todo sistema o medio electrónico que sirva para el tratamiento de datos de personas físicas.

1.3 Visión general del negocio

Con este perfil se pretende conseguir que cualquier sistema de información construido siguiendo los requisitos incluidos en el mismo, cumpla con éxito toda la normativa relacionada con el tratamiento de datos personales.

El perfil es completo y autosuficiente e incluye también las excepciones y sanciones reflejadas en la ley. Su uso permitirá que queden reflejados en el proceso de análisis de requisitos los aspectos legales relacionados con la nueva LOPD y el vigente RD, teniendo en cuenta la horizontalidad del ENS cuando estas normas actúen en el ámbito de las AAPP. La organización de los documentos es la que se refleja en la Figura 1: Perfil SIREN PDP2019. En esta Figura se muestra que partimos del nuevo reglamento europeo del cual se deriva el proyecto de ley de la nueva LOPD. Teniendo en cuenta además la normativa en materia de seguridad cuando estemos tratando en el ámbito de la Administración Pública.

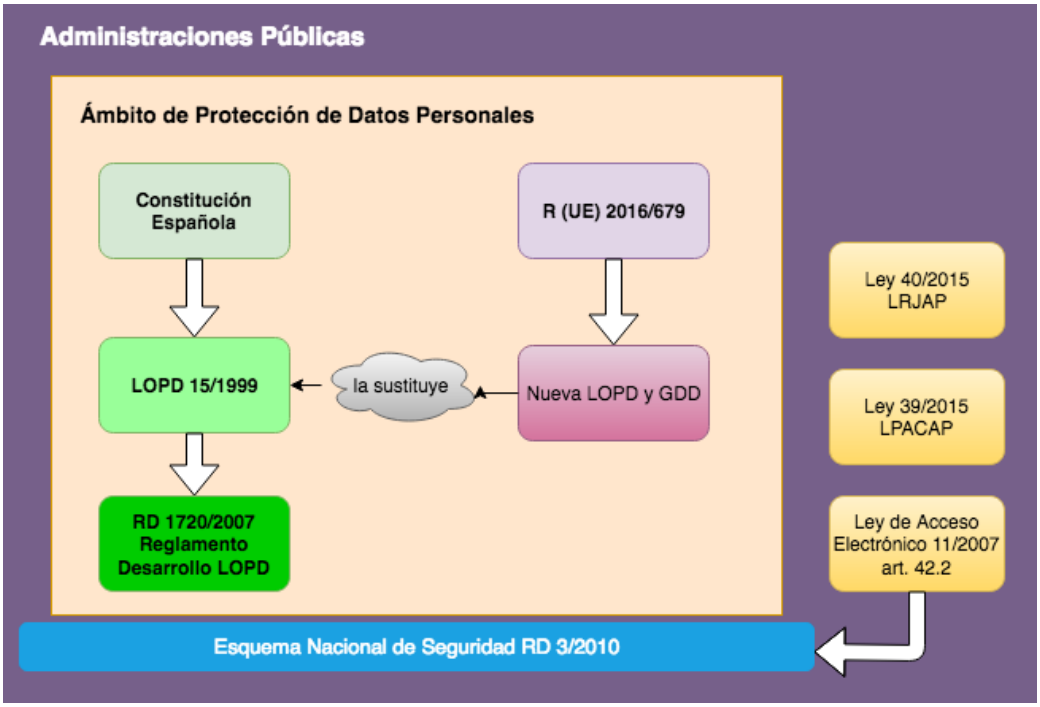

Figura 1. Perfil SIREN PDP 2019

En la *Figura 2: Modelo conceptual PDP* se muestra un vocabulario semántico con los distintos conceptos existentes y sus relaciones realizado en OWL2 con la herramienta Protégé. La figura muestra una clasificación de las clases que conforman la ontología y que integra la nueva LOPD con el RD1720/2007 y el RGPD. Para su diseño se ha utilizado PROV-O, una ontología para recoger conocimiento sobre *provenance* y que forma parte de las recomendaciones del W3C. PROV-O permite recoger información sobre entidades, actividades y personas (incluyendo software) implicados en la producción de datos o componentes y que nos puede servir para conocer la calidad, fiabilidad o integridad de dichos datos. Ha sido utilizado en varios dominios y aplicaciones como base para repositorios de *provenance*. ovPDP2019.owl extiende PROV-O y añade los conceptos de protección de datos de la normativa española a la ontología. De este modo muchas de los conceptos o clases en los que se basa ya existen y están normalizados por el W3C en un vocabulario de uso común.

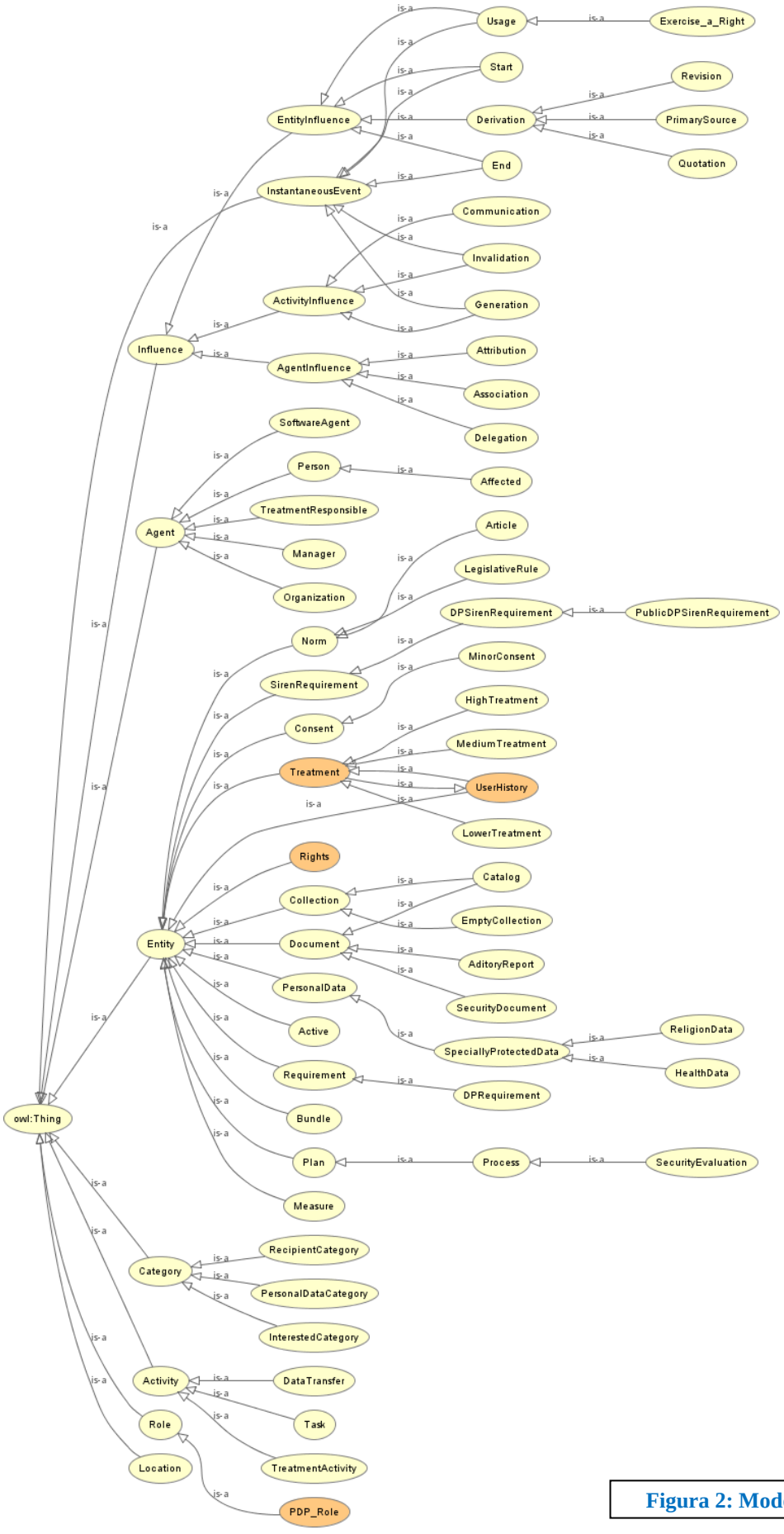

Figura 2: Modelo conceptual PDP

1.4 Definiciones, acrónimos y abreviaturas (Glosario de Términos)

Esta sección de definiciones constituye el glosario de términos unificado para todos los documentos del perfil de Protección de Datos Personales.

Accesos autorizados. Autorizaciones concedidas a un usuario para la utilización de los diversos recursos.

Administración Pública. Según la ley 39/2015, en su artículo 2, tienen la consideración de Administraciones Públicas los siguientes:

a) La Administración General del Estado
b) Las Administraciones de las Comunidades Autónomas.
c) Las Entidades que integran la Administración Local.
d) Los organismos públicos y entidades de derecho público dependientes o vinculados a una Administración Pública.

Afectado o interesado. Persona física titular de los datos que sea objeto del tratamiento de datos.

Agencia de Protección de Datos (APD). 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, en España.

Algoritmo de cifrado. Sistema de encriptación que permite transmitir información por las redes telemáticas con seguridad. Existen varios algoritmos, destacando entre otros MD5, DES, DES2, RC3, RC4 y, sobre todo SSL (Secure Sockets Layer) de Netscape. Estos sofisticados algoritmos se caracterizan pos sus claves de encriptación que oscilan entre 40 y 120 bits.

Auditoría de Sistemas de Información. Proceso sistemático de recoger, agrupar y evaluar evidencias para determinar si un Sistema de Información salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y usa eficientemente los recursos.

Autenticación. Procedimiento de comprobación de la identidad de un usuario.

Autor de una base de datos. Persona física o el grupo de personas físicas que haya creado dicha base de datos o, cuando la legislación de los Estados miembros lo permita, la persona jurídica que dicha legislación designe como titular del derecho.

Autoridad de control. La autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51 del RUE 2016/679. En España tal autoridad es la Agencia de Protección de Datos.

Autoridad de control interesada. La autoridad de control a la que afecta el tratamiento de datos personales.

Base de datos. Recopilaciones de obras, de datos o de otros elementos independientes dispuestos de manera sistemática o metódica y accesibles individualmente por medios electrónicos o de otra forma.

Bloqueo de datos. Identificación y reserva de datos con el fin de impedir su tratamiento.

Bus del sistema. Grupo de conexiones eléctricas usadas para conectar un ordenador a otro mecanismo auxiliar o a otro ordenador.

Cesión o comunicación de datos. Toda revelación de datos realizada a una persona distinta del interesado.

Código tipo. Publicación que establece las condiciones de organización de un sistema particular, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno en programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la LOPD. Podemos acceder a publicaciones de códigos tipo en el siguiente enlace de la Agencia de Protección de Datos: https://www.agpd.es/index.php?idSeccion=95

Consentimiento del interesado. Toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

Contraseña. Información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario.

Control de acceso. Mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

Copia de respaldo. Copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

Datos biométricos. Datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

Datos de carácter personal. Toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Datos genéticos. Datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.

Datos relativos a la salud. Datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

Derecho sui generis de bases de datos. Derecho por el cual se protege la inversión sustancial realizada para obtener y presentar el contenido de la base de datos, evitando la apropiación de los resultados del esfuerzo del fabricante. Este derecho, por tanto, recae sobre la base de datos, y no sobre el contenido. Mediante este derecho el fabricante de la base de datos puede prohibir la extracción y/o reutilización del total o parte del contenido de la misma. El plazo de protección es de 15 años desde la puesta a disposición al público por primera vez, o a partir del 1 de Enero tras la finalización de su creación, pero si se realizan modificaciones en la base de datos que a su vez impliquen una nueva inversión sustancial, el resultado tendrá su propio plazo de protección. Por ejemplo, un buscador de vuelos no puede obtener datos de la base de datos de una aerolínea utilizando funciones de búsqueda sobre la propia web de la aerolínea.

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

Distribución o transferencia de datos. Transmisión de datos fuera del sistema de información, ya sea mediante un soporte extraíble o de otra forma, como la que se produce por correo electrónico o por cualquier otro medio convencional.

Documento de seguridad. Documento que debe implantar el responsable del fichero en el que se refleja la normativa de seguridad del sistema de información. Es de obligado cumplimiento para el personal con acceso a los datos y a los sistemas de información, siendo obligada su continua revisión y actualización de acuerdo con la normativa vigente.

Encargado del tratamiento (outsourcing). La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

Algunos aspectos que caracterizan la figura del encargado del tratamiento son:

Que no debe inscribir en el registro los ficheros que trata por cuenta de los responsables, pero sí sus ficheros propios y cumplir con ellos todas las disposiciones legales de la LOPD.

Que si existen varios encargados del tratamiento (la gestoría que realiza las nóminas, la empresa de informática que gestiona las bases de datos, etc.), existen diversas posibilidades a la hora de notificar ese extremo a la APD, como son especificar como encargado del tratamiento a la entidad principal que realice dichas funciones, notificar el encargado principal y el resto comunicarlos mediante un escrito adjunto a la notificación o hacerse constar el encargado que realice el tratamiento de datos que pueda implicar una mayor duración en el tiempo, o riesgos mayores según el tipo y la cantidad de datos tratados.

Elaboración de perfiles. Toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

Establecimiento principal.

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

Extracción del contenido de una base de datos. La transferencia permanente o temporal de la totalidad o de una parte sustancial del contenido de una base de datos a otro soporte, cualquiera que sea el medio utilizado o la forma en que se realice.

Fabricante de la base de datos. El que toma la iniciativa y asume el riesgo de realizar la inversión.

Fichero automatizado. Todo conjunto organizado de datos de carácter personal que sean objeto de un tratamiento automatizado, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

Ficheros de Nivel Básico de Seguridad. Todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico. Un fichero con datos de una persona física como el nombre, apellidos, dirección, correo electrónico y teléfono es un caso típico de ficheros de datos de nivel básico. También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

Ficheros de Nivel Medio de Seguridad. Aquellos ficheros que contengan datos relativos a:

a) Los relativos a la comisión de infracciones administrativas o penales.

b) Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre.

c) Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.

d) Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.

e) Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo,

aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

f) Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

Ficheros de Nivel Alto de Seguridad. Aquellos ficheros que contengan datos relativos a:

a) Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

b) Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.

c) Aquéllos que contengan datos derivados de actos de violencia de género.

d) Ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización.

Fichero. Todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

Fichero de titularidad pública. Ficheros creados o gestionados por las corporaciones de derecho público representativas de intereses económicos y profesionales del estado, siempre y cuando dichos ficheros sean creados o gestionados para el ejercicio de potestades de derecho público. Por ejemplo, los ficheros de las Fuerzas y Cuerpos de Seguridad.

Fichero de titularidad privada. Ficheros cuyo responsable es una persona física o jurídica de naturaleza privada.

Fichero temporal. Fichero distinto del original, y creado por la aplicación informática que lo gestiona, cuya finalidad es un procesamiento paralelo de los datos originales sin afectar al fichero original y/o con la finalidad de copia de seguridad temporal ante una parada anormal del sistema.

Fuentes accesibles al público. Aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencias que, en su caso, el abono de una contraprestación. Tienen consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

Identificación. Procedimiento de reconocimiento de la identidad de un usuario.

Incidencia. Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

Limitación del tratamiento. El marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro.

LOPD actual (LOPD antigua). Es la actual Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal. Sustituyo a la LORTAD 5/1992. Aunque tiene por encima el Reglamento Europeo 2016/679 sigue en vigor en todo lo que no contradiga a dicho reglamento, de hecho su última actualización se produjo el 30 de julio de 2018 para adaptarla a la normativa europea tras la entrada en vigor del Reglamento.

LOPD y GDD (LOPD nueva). Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales. Está en avanzado estado de tramitación, sustituirá a la LOPD 15/1999. Crea una norma más adaptada al Reglamento Europeo de PD, introduce novedades significativas como los datos referidos a las personas fallecidas, y reconoce y garantiza varios derechos digitales de los ciudadanos como la neutralidad de la Red, el derecho al olvido o el testamento digital. También incluye la obligatoriedad para las AAPP, empresas o fundaciones vinculadas a las mismas sujetas al Derecho privado de cumplir con las medidas del ENS. Las empresas o terceros que presten un servicio en régimen de concesión, encomienda de gestión o contrato también deberán cumplir con las medidas del ENS de aplicación a la AAPP vinculada.

Nivel de Seguridad. Las medidas de seguridad exigibles se clasifican en tres niveles: básico, medio y alto y en dos dimensiones LOPD y ENS.

De acuerdo a la LOPD dichos niveles se establecen atendiendo a la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información. Son desarrolladas en el RD 1720/2007. En este caso es preceptivo conocer qué tipo de datos tratamos, esto es si los datos son de nivel básico, medio o alto, para conocer qué medidas de seguridad aplicaremos.

Por otro lado, atendiendo al ENS las medidas son establecidas de acuerdo a la categoría con la que sea catalogada cada una de las dimensiones de seguridad del sistema de información que trate los datos personales.

Medidas de seguridad de nivel básico. Las medidas de seguridad que exige la legislación de PD para el nivel bajo son la elaboración del documento de seguridad, la definición de las funciones del personal, la creación de un registro de incidencias, el establecimiento de obligaciones referidas a la identificación y autenticación de los usuarios, normas sobre controles de acceso, gestión de soportes y copias de respaldo y recuperación.

Medidas de seguridad de nivel medio. Las medidas de seguridad que exige la legislación de PD para el nivel medio son, además del cumplimiento de todas las medidas de seguridad señaladas para el nivel bajo, ciertos requisitos complementarios en el documento de seguridad, como son la designación de un responsable de seguridad, una auditoria cada 2 años, requisitos suplementarios respecto a la identificación y autenticación, el control de acceso físico, la gestión de soportes, el registro de incidencias y las pruebas con datos reales.

Medidas de seguridad de nivel alto. Las medidas de seguridad que exige la legislación de PD para el nivel alto, son además de reunir las medidas de nivel básico y medio, aquellas referidas a distribución de soportes, registro de accesos, copias de respaldo y recuperación y telecomunicaciones.

Normas corporativas vinculantes. Las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta.

Objeción pertinente y motivada. La objeción a una propuesta de decisión sobre la existencia o no de infracción de la legislación en materia de protección de datos, o sobre la conformidad con la misma de acciones previstas en relación con el responsable o el encargado del tratamiento, que demuestre claramente la importancia de los riesgos que entraña el proyecto de decisión para los derechos y libertades fundamentales de los interesados y, en su caso, para la libre circulación de datos personales dentro de la Unión.

Organización internacional. Una organización internacional y sus entes subordinados de Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo.

Perfil (Concepto del método SIREN). Conjunto de requisitos relacionados entre sí y pertenecientes a un sector "horizontal" -perfil- especifico (seguridad, portales, comercio electrónico, firma digital, etc.). Los requisitos de perfiles pueden usarse en una amplia variedad de dominios.

Procedimiento de disociación. Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona determinada o determinable.

Recurso: cualquier parte componente de un sistema de información.

Registro General de Protección de Datos. Órgano integrado en la Agencia de Protección de Datos, en el cual son objeto de inscripción los ficheros de que sean titulares las Administraciones Públicas, los ficheros de titularidad privada, las autorizaciones a que se refiere la LOPD, los códigos tipo, y los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición. La nueva ley no lo menciona ya que ahora se debe registrar internamente por las empresas o entes jurídicos un registro de actividades de tratamiento, es posible que desaparezca.

Representante. Persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 27, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento.

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

Reutilización del contenido de una base de datos. Toda forma de puesta a disposición del público de la totalidad o de una parte sustancial del contenido de la base mediante la distribución de copias, alquiler, transmisión en línea o en otras formas. La primera venta de una copia de una base de datos en la Comunidad por el titular de los derechos o con su

consentimiento extinguirá el derecho de control de las ventas sucesivas de dicha copia en la Comunidad.

RGPD. Reglamento General de Protección de Datos (en inglés GDPR: General Data Protection Regulation). Es el Reglamento Europeo 2016/679.

Seudonominación. El tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

Sistema informático. En este perfil, con este término nos referiremos al conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.

Soporte informático. Objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos. Por ejemplo, un disquete, un CD-ROM, o una cinta de back-up, entre otros, son soportes informáticos.

Telecomunicaciones. Toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos.

Tercero. Persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

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

Tratamiento de datos. Operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Tratamiento transfronterizo. Puede tener la consideración de tratamiento transfronterizo alguno de los siguientes:

a) El tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro.
b) El tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que

afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro.

Usuario. Sujeto o proceso autorizado para acceder a datos o recursos.

Violación de seguridad de los datos personales. Toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

1.5 Stakeholders

En esta sección se van a definir los roles que aparecen en la LOPD. Estos ya han sido mostrados anteriormente en la Figura 2 y volverán a aparecer mencionados en las historias de usuario.

Delegado de protección de datos (DPD). La persona física que se encargará de garantizar la correcta aplicación en materia de protección de datos de la normativa vigente. Debe de existir obligatoriamente en toda Administración Pública, será una figura con independencia ejecutiva, es decir no recibirá ninguna instrucción en lo que respecta al desempeño de sus funciones. Y entre sus cometidos tiene la misión de asesorar, informar, supervisar y cooperar con la AEPD.

Encargado del tratamiento. La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

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

Responsable del sistema. Puesto operativo, no directivo ni de gobierno. Suele recibir también la denominación de Responsable de Producción o Explotación, de manera que en él viene a recaer la responsabilidad de la prestación material del servicio. Debe asumir las siguientes responsabilidades:

- Desarrollar, operar y mantener del Sistema durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y política de gestión del Sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba del mismo.
- Implantar y controlar las medidas específicas de seguridad del Sistema y cerciorarse de que éstas se integren adecuadamente dentro del marco general de seguridad.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.

- Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
- Llevar a cabo el preceptivo proceso de análisis y gestión de riesgos en el Sistema.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.
- Elaborar y aprobar la documentación de seguridad del Sistema.
- Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.
- Velar por el cumplimiento de las obligaciones del Administrador de Seguridad del Sistema (ASS).
- Investigar los incidentes de seguridad que afecten al Sistema, y en su caso, comunicación al Responsable de Seguridad o a quién éste determine.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Además, el responsable del sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el responsable de seguridad, antes de ser ejecutada.

Responsable de seguridad. Persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables. En el ENS es la persona designada por la Dirección, según procedimiento descrito en su Política de Seguridad. Su función esencial es planificar lo que se ha de hacer en materia de seguridad, así como supervisar que se haya hecho adecuadamente. Otras de sus funciones son también:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de la Organización.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

Responsable del servicio. Según el ENS es el responsable de establecer los niveles de seguridad de los servicios.

Responsable de la información. De acuerdo al ENS tiene la responsabilidad del uso que se haga de una cierta información y, por tanto, de su protección. El Responsable de la Información es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad. Es el responsable de establecer los niveles de seguridad de la información.

Usuario, afectado o interesado: persona que hace uso del sistema y de la cual se van a obtener datos de carácter personal.

2 Referencias

2.1 Artículos y documentación SIREN

- Toval, A., Nicolas, J., Moros, B., & Garcia, F. (2002). Requirements reuse for improving information systems security: A practitioner's approach. Requirements Engineering, 6(4), 205–219. https://doi.org/10.1007/PL00010360
- Ambrosio Toval; Joaquín Nicolás; Begoña Moros. (2002). SIREN: Un Proceso de Ingeniería de Requisitos Basado en Reutilización. Applying Requirements Engineering" (ISBN 84- 96086-06-2), (Catedral Publicaciones), 57–72.

2.2 Artículos y documentación de versiones anteriores de catálogos de PDP

- Olmos, A., Toval, A., Lasheras, J., Martínez, M. A., & Nicolás, J. (2007). SyRS-PDP. Documentos Internos Del DIS.
- Olmos, A., Toval, A., Lasheras, J., Martínez, M. A., & Nicolás, J. (2007). SRS-PDP. Documentos Internos Del DIS.
- CATÁLOGO PDP-LOPD_RMS. (2015). Documentos Internos Del DIS. (SyRS-PDP + SRS-PDP).
- Martínez, M. A. (2015). Revisión de los perfiles SIREN de protección de datos personales y de seguridad y aplicación a un caso de estudio real. Documentos Internos Del DIS, 1–84.
- Montesinos Rodríguez, Diego (2018). Trabajo Fin de Grado. Actualización del catálogo de requisitos de privacidad según el nuevo Reglamento Europeo de Protección de Datos.

2.3 Fuentes sobre normativa jurídica vigente en materia de Protección de Datos y Seguridad Informática

- Jefatura del Estado. (1999). 23750 LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. BOE, 298, 43088–43099.

  Ley orgánica de protección de datos de carácter personal en vigor hasta que se sustituya con la nueva ley que está en trámite en el congreso de los diputados y se prevé que entre en vigor el 25 de mayo de 2018, fecha máxima en la que es obligatorio que los estados miembro de la Unión Europea adapten sus legislaciones a la nueva normativa europea.

- 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. (2007). BOE Núm. 17, 19 de enero de 2008.

  Reglamento que desarrolla la ley anterior de protección de datos de carácter personal y que se prevé que también sea actualizado por un nuevo reglamento que se adapte a la nueva ley.

- Agencia Española de Protección de Datos. (2018). Retrieved April 15, 2018, from https://www.agpd.es

Página de la Agencia de Protección de Datos, donde van apareciendo noticias, directivas y recomendaciones sobre protección de datos. La AEPD tiene competencias en materia de interpretación de protección de datos.

- El Parlamento Europeo y el Consejo de la Unión Europea. (2016). Reglamento (UE) 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46CE. Diario Oficial de La Unión Europea, 2014(119), 1–88.

  Nuevo reglamento europeo sobre protección de datos que los estados miembro están obligados a adaptar sus leyes a este antes del 25 de mayo de 2018. En castellano RGPD, en inglés GDPR

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Jefatura del Estado. «BOE» núm. 294, de 6 de diciembre de 2018. Referencia: BOE-A-2018-16673

  Nueva ley orgánica de Protección de Datos, viene a sustituir la anterior ley 15/1999. Desarrolla y adapta el RGPD a la normativa española. Cabe destacar como novedades: los nuevos derechos de las personas fallecidas, el acceso universal a internet y la neutralidad de la red.

- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. «BOE» núm. 25, de 29 de enero de 2010

  Establece la política de seguridad en la utilización de medios electrónicos en las Administraciones Públicas. Está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

- Jefatura del Estado. (2007). Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. «BOE» núm. 150, de 23 de junio de 2007. Referencia: BOE-A-2007-12352

  Regula los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa , en las relaciones entre las Administraciones Públicas, así como en las relaciones de los ciudadanos con las mismas con la finalidad de garantizar sus derechos, un tratamiento común ante ellas y la validez y eficacia de la actividad administrativa en condiciones de seguridad jurídica.

3 Gestión empresarial

3.1 Entorno de negocio

3.1.1 Entrada en vigor de la nueva ley de Protección de Datos y Garantías de los Derechos Digitales

Todas las medidas de seguridad, en sus diferentes niveles (básico, medio, alto) de la actual LOPD, entraron en vigor a partir del 26 de junio de 2002.

El Reglamento Europeo 2016/679 entro en vigor el 25 de mayo de 2018.

3.2 Meta y objetivo

El objetivo de este catálogo es proporcionar una serie de requisitos reutilizables en cualquier software que haga uso de datos personales conforme a la normativa vigente española.

3.3 Modelo de negocio

No se han descrito.

3.4 Entorno de información.

No se han descrito.

4 Negocio operativo

4.1 Procesos de negocio

4.1.1 Niveles de seguridad de los ficheros

Para establecer los niveles de seguridad se han tenido en cuenta toda las medidas que se exigen en el RGPD, el RD 1720/2007, el ENS y el nuevo proyecto de LOPD. Tras el análisis de todas ellas para este repositorio se ha decidido establecer tres niveles de seguridad: BAJO, MEDIO y ALTO.

Todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico.

Se ha suprimido el nivel medio atenuado que había antes con el fin de poder facilitar la aplicación de esta herramienta de acuerdo al marco legal vigente, ya que tanto el RD como el ENS describen tres niveles de medidas de seguridad.

El RGPD nos exige unos requisitos mínimos que debemos cumplir en todo tratamiento en cuanto a los derechos de los interesados y deberes de los responsables de los tratamientos. Sin embargo no concreta medidas de seguridad. Con el nuevo RGPD ya no existe la obligación de disponer de medidas mínimas y concreta de acuerdo al tipo o naturaleza de dato a tratar, sino que el responsable del tratamiento tendrá que realizar un análisis de riesgos del tratamiento en cuestión, evaluar si las actividades a realizar entrañan un alto riesgo o no y decidir que medidas a aplicar en cada caso. Es lo que denomina diseño proactivo de la seguridad.

Por otro lado el ENS nos obliga a realizar este mismo análisis de riesgos del que habla el RGPD pero desde la perspectiva de 5 dimensiones de seguridad concretas: disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad. Como resultado se establecerá un nivel requerido de seguridad que podrá ser bajo, medio o alto para cada una de ellas y de acuerdo al nivel asignado se exigen unas medidas concretas. Es decir es una norma muy taxativa. Son medidas orientadas a la seguridad en general.

El RD 1720/2007 al igual que el ENS nos concreta unos mínimos de medidas a aplicar de acuerdo a que el tratamiento de datos sea catalogado de criticad baja, media o alta. Estás medidas están orientadas a la protección de datos.

La nuevo LOPD viene a desarrollar el RGPD ratificando lo que en ella se pide y detallando algunas casuísticas más como los derechos de las personas fallecidas.

Para poder cumplir con todas las normas y con un principio de simplificación, se proponen tres categorías de seguridad: baja, media y alta. Cada una de ellas definirá unos requisitos que podrán ser aplicados de forma flexible gracias a la metainformación que llevarán asociada.

Para conocer el nivel de requisitos que se debe aplicar al sistema se propone realizar el análisis de riesgos exigido por el RGPD con la finalidad de conocer si nuestro tratamiento conlleva un alto riesgo o no para los derechos y libertades del interesado. En caso negativo, consideramos que aplicando los de nivel básico será suficiente. Estos se compondrán de las medidas mínimas exigibles por el RD y las exigibles por el ENS, ya que entendemos que todas las dimensiones tendrán un nivel de exigencia BAJO, es decir que en caso de materializarse los riesgos causarían un perjuicio limitado.

Si el tratamiento conlleva un alto riesgo el siguiente paso que recomendamos es realizar la Evaluación de Impacto relativa a la Protección de Datos (EIPD) que se pide en el RGPD. Los criterios para decidir si es necesario llevar a cabo el EIPD o no, los encontramos en los artículos 35.1 (análisis de la naturaleza, alcance, contexto y fines del tratamiento) y 35.3, 35.4, 35.5 (análisis de las listas de tratamientos que describen).

Tras la EIPD tendremos que decidir si la materialización del algún riesgo conlleva consecuencias de nivel MEDIO (suponen perjuicio grave para las personas) o ALTO (suponen un perjuicio muy grave). De acuerdo al nivel de consecuencias que declaremos aplicaremos el catalogo de requisitos MEDIO o ALTO.

En el proceso de realización del EIPD podremos entrar en la evaluación de cada una de las dimensiones del ENS y definir su categoría. Recomendamos usar el nivel de requisitos correspondiente al nivel de la categoría que haya resultado con mayor nivel de riesgos.

Es decir los niveles que en este catalogo se recogen se establecen atendiendo al **análisis de riesgos** y la **evaluación de impacto** de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información.

A diferencia de antes de la entrada en vigor del RGPD ya no es tan necesario conocer qué tipo de datos tratamos, esto es si los datos son de nivel básico, medio o alto, para conocer qué medidas de seguridad aplicaremos. Por ejemplo, antes de la aplicación del RGPD un fichero con datos de una persona física como el nombre, apellidos, dirección y teléfono era un caso típico de ficheros de datos de nivel básico, pero ahora ya no. Porque dependiendo del tratamiento a realizar y los perjuicios que impliquen la perdida o robo de algún dato se deberán aplicar unas medidas u otras.

Sin embargo mientras el RD 1720/2017 no se modifique o derogue los seguiremos teniendo en cuenta, de modo que si estamos analizando uno o varios tratamientos que aplican a datos del tipo medio descrito en el artículo 81 del RD, le aplicaremos como mínimo aquellos requisitos que sean de tipo medio, y lo mismo con los de nivel alto.

Las medidas que exige el RD para el **nivel básico** son las siguientes:

1. Elaboración del documento de seguridad (art. 88). Este documento debe recoger las medidas de tipo técnicas y organizativas que apliquemos al sistema.

2. Definición de las funciones del personal (art. 89).

3. Creación de un registro de incidencias (art. 90). Además el art. 33 del RGPD nos obliga a notificar las violaciones de seguridad a la AEPD como máximo en 72 horas.

4. Control de acceso de usuarios (art. 91). Los usuarios sólo tendrán acceso a los recursos que necesiten para el desarrollo de sus funciones.

5. Gestión de soportes y copias de respaldo y recuperación (art. 92).

6. Medidas de identificación y autenticación (art. 93).

Estas medidas de nivel básico se exigirán siempre.

Los ficheros que contengan datos relativos a la comisión de Infracciones Administrativas o Penales, Hacienda Pública, servicios financieros y aquellos ficheros sobre prestación de servicios de información sobre solvencia patrimonial y crédito, deberán reunir, además de las medidas de nivel básico, las calificadas como de nivel medio.

Las medidas que exige el RD1720/2007 para el **nivel medio** son además del cumplimiento de todas las medidas de seguridad señaladas para el nivel básico, los siguientes requisitos complementarios en el documento de seguridad:

1. La designación de un responsable de seguridad (art. 95). Este responsable de seguridad podría ser el mismo que el exigido por el ENS para toda la organización en materia de seguridad informática.

2. Una auditoria cada dos años (art. 96). Puede ser tanto interna como externa.

3. Requisitos suplementarios respecto a la identificación y autenticación (art. 98). Se limitarán los reintentos de acceso no autorizados.

4. Control de acceso físico (art. 99).

5. Gestión de soportes y documentos (art. 97). Registro de entrada y salida de soportes.

6. Registro de incidencias (art. 100). Información sobre los procesos de recuperación de datos.

Los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas deberán reunir, además de las medidas de nivel básico y medio, las calificadas de **nivel alto**.

Las medidas que exige el RD 1720/2007 para el **nivel alto** son, además de reunir las medidas de nivel básico y medio, las siguientes:

1. Medidas sobre **gestión y distribución de soportes** (art. 101). Entre ellas la identificación de soportes utilizando sistemas de etiquetado que permitan su identificación para el personal autorizado y lo dificulten para el resto de personas.

2. Medidas de **copia de respaldo y recuperación** (art. 102). Copias de respaldo y del proceso de recuperación de datos en lugar diferente de aquel en donde se encuentren los equipos informáticos que los tratan.

3. Medidas de **registro de accesos** (art. 103). Entre ellas guardar como mínimo la identificación del usuario, la fecha y hora del acceso, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

4. Medidas de **transmisión de datos** (art. 104). Transmisión de datos cifrados cuando se utilicen redes públicas o inalámbricas.

4.1.2 Metainformación asociado a los requisitos del catalogo

Todos los requisitos disponen de un conjunto común de atributos que proporcionan información complementaria y necesaria al texto del requisito. Estos atributos pueden verse en el proyecto correspondiente (Pantalasa). Destacan, por su importancia para asegurar un catálogo completo, los atributos de “nivel de seguridad”, “excepciones” y “fuente”:

- Nivel de seguridad. Este atributo hace referencia a los tres niveles de seguridad que se establecen en el RD1720/2007 y en el ENS (básico, medio, alto) atendiendo a la naturaleza de la información tratada en relación con la mayor o menor necesidad de garantizar la confidencialidad e integridad de la información.

- Excepciones. Este atributo hace referencia a las excepciones contempladas en la normativa de protección de datos. Este atributo, garantizará que el nivel de cumplimiento de la ley sea más elevado.

- Fuente. Este atributo es un campo de texto que indica la procedencia del requisito. Cuando estemos haciendo un proyecto concreto nos servirá para reflejar de qué catálogo proviene un requisito reutilizado y en particular a partir de qué requisito. En el caso de este catálogo, este atributo almacena la procedencia del requisito, sea la LOPD o el RD, y el artículo correspondiente.

4.2 Políticas y normas de funcionamiento de negocio

No se han descrito.

4.3 Restricciones operativas de negocio

No se han descrito.

4.4 Modo de operación de negocios

No se han descrito.

4.5 Calidad de las operaciones de negocio

No se han descrito.

4.6 Estructura de negocio.

No se han descrito.

5 Historias de Usuario

Esta sección está organizada teniendo en cuenta la organización del proyecto de ley de la nueva LOPD y se ha intentado armonizar tanto con el nuevo reglamento europeo, como con el RD1720/2007, como el Esquema Nacional de Seguridad.

5.1 Seguridad

5.1.1 Información y Derechos de los Afectados

GR.1. **Licitud del tratamiento.** Como responsable del tratamiento quiero que el tratamiento de los datos personales sea lícito. El tratamiento será lícito si el interesado dio su

consentimiento, es necesario para el cumplimiento de una obligación legal o en el ejercicio de poderes públicos entre otros.

Sólo AAPP: No

Fuentes: RGPD art 6., Nueva LOPD: art. 19 (datos de contacto de trabajadores, empresarios individuales y de profesionales liberales), art. 20 (obligaciones dinerarias, financieras o de crédito), art. 21 (operaciones mercantiles), art. 22 (videovigilancia), art. 23 (sistemas de exclusión publicitaria), art. 24 (sistemas de información de denuncias internas), art. 25 (función estadística pública), art. 26 (archivo en interés público), art. 27 (sanciones e infracciones administrativas).

Excepciones: -

GR.2. **Consentimiento para finalidades varias.** Como responsable del tratamiento quiero que, cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades (comercial, de identificación, sindical, etc.) sea preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para cada una de ellas.

Sólo AAPP: No

Fuentes: Nueva LOPD art 6.2.

Excepciones: -

GR.3. **Consentimiento de menores.** Como responsable del tratamiento quiero que el tratamiento de los datos personales de un menor de edad únicamente pueda fundarse en su consentimiento cuando sea mayor de catorce años.

Sólo AAPP: No

Fuentes: Nueva LOPD art 7.1.

Excepciones: -

GR.3.1 **Consentimiento de menores de 14 años.** Cuando sea menor de 14 años el tratamiento sólo será lícito si consta el consentimiento del titular de la patria potestad o tutela.

Sólo AAPP: No

Fuentes: Nueva LOPD art 7.1.

Excepciones: -

GR.4. **Información básica.** Como responsable del tratamiento y del servicio debo facilitar al afectado la siguiente información.

a) La identidad y datos de contacto del responsable del tratamiento
b) La finalidad del tratamiento
c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del RGPD.
d) Dirección electrónica u otro medio donde obtener el resto de información básica del artículo 13 del RGPD.

Sólo AAPP: No

Fuentes: Nueva LOPD art 11.1; RGPD art 13.

Excepciones: -

GR.5. **Información complementaria de perfiles.** Como responsable del tratamiento quiero que cuando los datos obtenidos vayan a ser tratados para la elaboración de decisiones individualizadas automatizadas que produzcan efectos jurídicos sobre el afectado o

que le afecten significativamente de modo similar, se le de debe informar de esta circunstancia y de su derecho de oposición.

Sólo AAPP: No
Fuentes: Nueva LOPD art 11.2; RGPD art 22.
Excepciones: -

GR.6. **Información complementaria de datos indirectos.** Como responsable del tratamiento debo facilitar al afectado la siguiente información cuando los datos no sean obtenidos directamente del interesado.

a) Las categorías de datos objeto de tratamiento
b) Las fuentes de las que procedieron los datos

Sólo AAPP: No
Fuentes: Nueva LOPD art 11.3; RGPD art 14.
Excepciones: -

GR.7. **Información sobre el uso de derechos.** Como responsable del tratamiento quiero informar al usuario sobre los medios a su disposición para poder ejercer los derechos que le corresponden.

Sólo AAPP: No
Fuentes: Nueva LOPD art 12.1
Excepciones: -

GR.8. **Derecho de acceso.** Como interesado quiero conocer si están tratando o no datos personales míos y en caso afirmativo poder acceder a ellos y obtener una copia. Si presento la solicitud por medios electrónicos se me facilitará la información en un formato electrónico de uso común. Este derecho de acceso lo entenderé otorgado si el responsable del tratamiento me un sistema de acceso remoto, directo y seguro que garantice de modo permanente el acceso a su totalidad.

Sólo AAPP: No
Fuentes: Nueva LOPD art 13; RGPD art 15.
Excepciones: -

GR.9. **Derecho de rectificación.** Como interesado quiero poder rectificar mis datos personales. En la solicitud deberé indicar los datos a los que me refiero y la corrección que haya de realizarse. Este derecho de acceso lo entenderé otorgado si el responsable del tratamiento me facilita un sistema de rectificación remoto, directo y seguro que garantice de modo permanente el acceso al mismo.

Sólo AAPP: No
Fuentes: Nueva LOPD art 14; RGPD art 16.
Excepciones: -

GR.9.1 **Derecho de rectificación. Aporte de documentación.** Como responsable quiero que el interesado aporte la documentación necesaria para la rectificación cuando se pertinente.

Sólo AAPP: No
Fuentes: Nueva LOPD y GDD art 14; RGPD art 16.
Excepciones: -

GR.10. **Derecho de supresión por parte del interesado.** Como interesado quiero poder solicitar la supresión de mis datos personales. Como responsable del tratamiento y del sistema quiero que, cuando la supresión derive del ejercicio del derecho de oposición, se puedan conservar los datos identificativos del afectado necesarios con el fin de impedir tratamientos futuros para fines de mercadotecnia directa. Este derecho de acceso se entenderá otorgado si el responsable del tratamiento facilita al afectado un sistema de supresión remoto, directo y seguro que garantice de modo permanente el acceso al mismo.

Sólo AAPP: No

Fuentes: Nueva LOPD art 15; RGPD art 17.

Excepciones: Este requisito no se aplicará cuando el tratamiento de los datos sea necesario para cumplir con el art. 17.5, por ejemplo por razones de interés público en el ámbito de la salud pública.

GR.11. **Derecho de supresión por parte del responsable.** Como responsable del tratamiento quiero poder suprimir aquellos datos personales que ya no sean necesarios en relación con los fines para los que fueron recogidos incluidos campos ocultos, meta-datos, comentarios o revisiones anteriores.

Sólo AAPP: No

Fuentes: Nueva LOPD art 15; RGPD art 17., ENS mp.info.6.

Excepciones: Este requisito no se aplicará cuando el tratamiento de los datos sea necesario para cumplir con el art. 17.5, por ejemplo por razones de interés público en el ámbito de la salud pública.

GR.12. **Derecho a la limitación del tratamiento.** Como interesado quiero poder limitar el tratamiento cuando este sea ilícito, los datos sean inexactos y resto de casos del art. 18 del RGPD. En caso de que el tratamiento esté limitado este hecho debe constar claramente en el sistema de información.

Sólo AAPP: No

Fuentes: Nueva LOPD art. 16; RGPD art. 18.

Excepciones: -

GR.13. **Derecho a la portabilidad.** Como interesado quiero poder pedir y recibir mis datos personales en un formato estructurado, de uso común y lectura mecánica. También podré pedir que el responsable los transmita a un tercero.

Sólo AAPP: No

Fuentes: Nueva LOPD art. 17; RGPD art. 20.

Excepciones: -

GR.14. **Derecho de oposición.** Como interesado quiero poder oponerme al tratamiento de mis datos personales incluida la mercadotecnia y la elaboración de perfiles.

Sólo AAPP: No

Fuentes: Nueva LOPD art. 18; RGPD art. 21, 22.

Excepciones: No podrá ejercerse cuando los datos sean necesarios para una misión realizada en interés público o en el ejercicio de poderes públicos.

GR.15. **Derecho de las personas fallecidas.** Como responsable del tratamiento quiero que los datos de las personas fallecidas puedan ser accedidos, modificados o suprimidos por sus familiares, herederos. También lo podrán ser por las personas e instituciones

que el fallecido hubiera designado expresamente. En el caso de menores podrán acceder además sus representantes legales o el Ministerio Fiscal.

Sólo AAPP: No

Fuentes: Nueva LOPD art. 3.1.

Excepciones: No se podrán acceder, modificar o suprimir estos datos cuando el fallecido así lo hubiera establecido expresamente o lo establezca una ley. Sin embargo los herederos sí podrán en cualquier caso acceder a los datos patrimoniales del fallecido.

GR.16. **Evaluación del nivel de seguridad.** Como responsable del tratamiento quiero que se realice una evaluación de seguridad con el fin de determinar el nivel de seguridad a aplicar al tratamiento. Se deben incluir los siguientes aspectos:

a) Identificación de los activos más valiosos del sistema.
b) Identificación de las amenazas más probables.
c) Identificación de las medidas a aplicar.
d) Identificación de los principales riesgos residuales.

Sólo AAPP: No

Fuentes: RGPD art. 31, ENS op.pl.1.

Excepciones: No será aplicará si los datos son necesarios para una misión realizada en interés público o en el ejercicio de poderes públicos.

GR.17. **Deber de confidencialidad.** Como responsable del tratamiento quiero que los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de éste estén sujetas al deber de confidencialidad.

Sólo AAPP: No

Fuentes: Nueva LOPD art. 5.1.

Excepciones: -

GR.17.1. **Mantenimiento.** Como responsable del tratamiento quiero que las obligaciones establecidas en el requisitos GR.17. se mantengan aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

Sólo AAPP: No

Fuentes: Nueva LOPD art. 5.3.

Excepciones: -

GR.18. **Transferencia internacional de datos.** Como responsable del tratamiento quiero que las transferencias internacionales de datos a países u organizaciones internacionales que no cuenten con decisión de adecuación aprobada por la Comisión o que no se amparen en alguna de las garantías previstas, requieran una previa autorización de la Agencia Española de Protección de Datos o, en su caso, autoridades autonómicas de protección de datos.

Sólo AAPP: No

Fuentes: Nueva LOPD art. 42.1.

Excepciones: Podrán concederse sin la autorización de la AEPD en los siguientes supuestos.

a) Cuando la transferencia pretenda fundamentarse en la aportación de garantías adecuadas con fundamento en cláusulas contractuales que no correspondan a las cláusulas tipo previstas.

b) Cuando la transferencia se lleve a cabo por alguno de los responsables o encargados y se funde en disposiciones incorporadas a acuerdos internacionales no normativos con

otras autoridades u organismos públicos de terceros Estados, que incorporen derechos efectivos y exigibles para los afectados (derechos vistos en apartado anterior), incluidos los memorandos de entendimiento.

GR.18.1. **Transferencia internacional de datos. Informar.** Como responsable del tratamiento quiero que los responsables del tratamiento deban informar a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos, de cualquier transferencia internacional de datos que pretendan llevar a cabo sobre la base de su necesidad para fines relacionados con intereses legítimos imperiosos perseguidos por aquéllos y la concurrencia del resto de los requisitos previstos.

Sólo AAPP: No
Fuentes: Nueva LOPD art. 43.
Excepciones: -

GR.19. **Calidad de los datos.** Como responsable del tratamiento quiero que los datos se mantengan exactos y actualizados, adoptando los procesos necesarios para que los mismos se supriman o rectifiquen en el menor tiempo posible.

Sólo AAPP: No
Fuentes: RGPD art. 1.
Excepciones: -

5.1.2 Requisitos de sistema para alcanzar el nivel BÁSICO de seguridad (RD 1720/2007 y ENS)

LW.1. **Exigencia de Requisitos Básicos.** Como responsable del tratamiento, del sistema y de seguridad quiero que el sistema aplique los requisitos de seguridad de nivel básico para todos los ficheros que contengan datos de carácter personal.

Sólo AAPP: No
Fuentes: RD 1720/2007 y ENS mp.info.1.
Excepciones: -

LW.2. **Documento de Seguridad.** Como responsable del tratamiento y del sistema quiero redactar un documento de seguridad mediante el cual se implantará la normativa de seguridad de protección de datos. Este documento contendrá la calificación de la información contenida.

Sólo AAPP: No
Fuentes: RD 1720/2007 art. 88, ENS mp.info.2.
Excepciones: -

LW.2.1. **Contenido.** Como responsable del tratamiento y del sistema quiero que el documento de seguridad contenga como mínimo los siguientes aspectos:

a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido.
c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.

d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
e) Procedimiento de notificación, gestión y respuesta ante las incidencias.
f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.
g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.
h) Mecanismo para conocer el grado de implantación de las medidas de seguridad.

Sólo AAPP: No
Fuentes: RD 1720/2007 art. 88, ENS op.exp.7, ENS op.mon.2.
Excepciones: -

LW.2.2 **Actualización.** Como responsable de seguridad quiero saber si cuando se ha producido cambios en el sistema de información o en la organización del mismo, así como en las disposiciones vigentes en materia de seguridad de los datos de carácter personal, se ha actualizado el documento de seguridad.

Sólo AAPP: No
Fuentes: RD 1720/2007 art. 88.
Excepciones: -

LW.3. **Política de seguridad.** Como responsable del sistema quiero redactar un documento de política de seguridad mediante el cual se implantará la normativa de seguridad informática. Debe ser coherente con el Documento de Seguridad.

Sólo AAPP: SÍ
Fuentes: ENS org.1.
Excepciones: -

LW.4. **Normativa de seguridad.** Como responsable del sistema quiero documentar:
a) El uso correcto de equipos, servicios e instalaciones.
b) Lo que se considera uso indebido.
c) La responsabilidad del personal con respecto al cumplimiento o violación de estas normas.

Sólo AAPP: SÍ
Fuentes: ENS org.2.
Excepciones: -

LW.5. **Procedimientos de seguridad.** Como responsable del sistema quiero documentar:
a) Cómo llevar a cabo las tareas habituales de seguridad.
b) Quien debe hacer cada tarea.
c) Como identificar y reportar anomalías.

Sólo AAPP: SÍ
Fuentes: ENS org.3.
Excepciones: -

LW.6. **Proceso de autorización.** Como responsable del sistema quiero documentar un proceso formal de autorizaciones para la entrada de equipos y aplicaciones en producción, utilización de instalaciones y medios varios.

Sólo AAPP: SÍ
Fuentes: ENS org.4.

Excepciones: -

LW.7. **Arquitectura de seguridad.** Como responsable del sistema quiero documentar la arquitectura de seguridad del sistema incluyendo:

a) Documentación de las instalaciones: áreas, puntos de acceso.
b) Documentación del sistema: equipos, redes, puntos de acceso.
c) Esquema de líneas de defensa: cortafuegos, dmz, etc.
d) Sistema de identificación y autenticación de usuarios.

Sólo AAPP: SÍ
Fuentes: ENS op.pl.2.
Excepciones: -

LW.8. **Inventario de activos.** Como responsable del sistema quiero documentar un inventario de todos los elementos del sistema.
Sólo AAPP: SÍ
Fuentes: ENS op.exp.1.
Excepciones: -

LW.9. **Registro de equipamiento.** Como responsable del sistema quiero llevar un registro de entrada y salida del equipamiento del sistema, incluyendo la identificación de la persona que autoriza el movimiento.
Sólo AAPP: SÍ
Fuentes: ENS mp.if.7.
Excepciones: -

LW.10. **Configuración de seguridad.** Como responsable del sistema y de seguridad quiero que los equipos se configuren previamente retirando las cuentas y contraseñas estándar, aplicando la regla de "mínima funcionalidad" y de "seguridad por defecto", y aplicándoles un mantenimiento constante.
Sólo AAPP: SÍ
Fuentes: ENS op.exp.2, op.exp.4, op.exp.6.
Excepciones: -

LW.11. **Normas de Seguridad.** Como responsable de seguridad quiero dar a conocer al personal con acceso a los datos automatizados de carácter personal, las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de su incumplimiento. Se especificarán las medidas de disciplinarias y el deber de confidencialidad.
Sólo AAPP: No
Fuentes: RD 1720/2007 art. 89.2, ENS mp.per.2.
Excepciones: -

LW.11.1 **Formación.** Como responsable de seguridad quiero establecer políticas que permitan recordar a los usuarios de forma regular lo siguiente: las medidas de seguridad, la importancia del papel que ellos tienen en la aplicación efectiva de las mismas, cómo identificar incidentes o comportamientos sospechosos, cómo reportarlos y reaccionar ante ellos, gestión de la información y otras cuestiones de seguridad que tengan relevancia.

Sólo AAPP: No

Fuentes: RD 1720/2007 art. 89.2, ENS mp.per.3, ENS mp.per.4.
Excepciones: -

LW.12. **Protección de locales.** Como responsable del sistema y del servicio quiero que en los locales esté garantizado el suministro eléctrico, unas adecuadas condiciones de temperatura, y la protección frente a incendios fortuitos o deliberados aplicando al menos la normativa industrial pertinente.
Sólo AAPP: SÍ
Fuentes: ENS mp.if.3, ENS mp.if.4, ENS mp.if.5.
Excepciones: -

LW.13. **Puestos de trabajo. Protección.** Como responsable del sistema quiero que los puestos de trabajo estén despejados, sin más material que el indispensable para realizar la actividad en cada momento.
Sólo AAPP: SÍ
Fuentes: ENS mp.eq.1.
Excepciones: -

LW.14. **Registro de incidencias.** Como responsable del tratamiento quiero que exista un procedimiento de notificación y respuesta ante incidencias que se incorpore al sistema de información. Por cada incidencia se hará constar:
a) El tipo de incidencia.
b) El momento en el que se ha producido o detectado.
c) La persona que realiza la notificación.
d) La persona a la que se le comunica.
e) Los efectos que se hubieran derivado de la misma.
f) Las medidas correctoras aplicadas.
Sólo AAPP: No
Fuentes: RD 1720/2007 art. 89.2.
Excepciones: -

LW.15. **Control de acceso.** Como responsable del tratamiento y del sistema quiero encargarme de que exista una relación actualizada de los usuarios que tengan acceso autorizado al sistema de información. Esta relación contendrá las autorizaciones concedidas a cada usuario, para la utilización de los diversos recursos.
Sólo AAPP: No
Fuentes: RD 1720/2007 art. 91, ENS op.acc.1, ENS mp.if.1.
Excepciones: -

LW.16. **Procedimiento de acceso.** Como responsable del tratamiento y del sistema quiero establecer un [procedimiento de identificación] (por ejemplo usuario) y un [procedimiento de autenticación] (por ejemplo contraseña) de forma inequívoca y personalizada para acceder al sistema. Se admitirá el uso de cualquier mecanismo de autenticación sustentado en un solo factor (“algo que se sabe”, “algo que se tiene”, “algo que se es”).
Sólo AAPP: No
Fuentes: RD 1720/2007 art. 91, RD 1720/2007 art. 93.1, RD 1720/2007 art. 93.2, ENS op.acc.1, ENS op.acc.5, ENS mp.if.2, ENS mp.com.3.
Excepciones: -

LW.17. **Procedimiento de acceso. Información de Obligaciones.** Como responsable del sistema quiero informar al usuario de sus obligaciones inmediatamente después de obtener acceso.

Sólo AAPP: SÍ
Fuentes: ENS op.acc.6.
Excepciones: -

LW.18. **Gestión de contraseñas.** Como responsable del tratamiento y del sistema quiero establecer un procedimiento de asignación, distribución y almacenamiento de contraseñas que garantice su confidencialidad e integridad, cuando el mecanismo de autenticación se base en la existencia de contraseñas.

Sólo AAPP: No
Fuentes: RD 1720/2007 art. 93.3.
Excepciones: -

LW.18.1. **Gestión de contraseñas. Almacenamiento.** Como responsable del tratamiento y del sistema quiero que el sistema garantice que las contraseñas se almacenarán de forma ininteligible mientras estén vigentes.

Sólo AAPP: No
Fuentes: RD 1720/2007 art. 93.3, ENS op.exp.11.
Excepciones: -

LW.18.2. **Gestión de contraseñas. Generación automática.** Como responsable del tratamiento y del sistema quiero que si las contraseñas se generan automáticamente los sistemas que las generen estarán aislados de los medios de explotación.

Sólo AAPP: No
Fuentes: RD 1720/2007 art. 93.3, ENS op.exp.11.
Excepciones: -

LW.18.3. **Gestión de contraseñas. Caducidad de contraseñas.** Como responsable del sistema quiero que el sistema establezca que las contraseñas deben ser cambiadas periódicamente, apareciendo dicha frecuencia en el documento de seguridad que en ningún caso podrá se superior a un año.

Sólo AAPP: No
Fuentes: RD 1720/2007 art. 93.4.
Excepciones: -

LW.19. **Acceso mínimo a recursos.** Como responsable del sistema quiero que los usuarios tengan acceso autorizado únicamente a aquellos datos y recursos mínimos que precisen para el desarrollo de sus funciones.

Sólo AAPP: No
Fuentes: RD 1720/2007 art. 91, ENS op.acc.2, ENS op.acc.4
Excepciones: -

LW.20. **Registro de actividad.** Como responsable del sistema quiero que se registren las actividades de los usuarios en el sistema. Los registros de actividades de los servidores deberán estar activos.

Sólo AAPP: SÍ

Fuentes: ENS op.exp.8, ENS mp.if.2.
Excepciones: -

LW.21. **Evitar acceso no autorizados.** Como responsable del sistema quiero establecer mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.
Sólo AAPP: No
Fuentes: RD 1720/2007 art. 91, ENS op.acc.2.
Excepciones: -

LW.22. **Permitir accesos autorizados.** Como responsable del sistema quiero que el sistema garantice que únicamente el personal autorizado para ello en el documento de seguridad pueda conceder, alterar o anular el acceso autorizado sobre datos y recursos, conforme a los criterios establecidos por el responsable del fichero.
Sólo AAPP: No
Fuentes: RD 1720/2007 art. 91.
Excepciones: -

LW.23. **Limitación de intentos de acceso.** Como responsable del tratamiento y del sistema quiero que el sistema limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema.
Sólo AAPP: No
Fuentes: RD 1720/2007 art. 98, ENS op.acc.6.
Excepciones: -

LW.24. **Prevención de ataques activos.** Como responsable del sistema quiero que se establezcan procedimiento para detectar ataques de alteración de información en tránsito, de secuestro de sesión o inyección de información espuria.
Sólo AAPP: SÍ
Fuentes: ENS mp.com.3.
Excepciones: -

LW.25. **Control de acceso remoto.** Como responsable de seguridad quiero que se garantice la seguridad del sistema cuando accedan remotamente usuarios u otras entidades.
Sólo AAPP: SÍ
Fuentes: ENS op.acc.7.
Excepciones: -

LW.26. **Cortafuegos.** Como responsable del sistema quiero que se separe la red interna del exterior y que todo el tráfico atraviese un cortafuegos que sólo debe transitar los flujos previamente autorizados.
Sólo AAPP: SÍ
Fuentes: ENS mp.com.1.
Excepciones: -

LW.27. **Identificación de información.** Como responsable del tratamiento y del sistema quiero que los soportes informáticos que contengan datos de carácter personal permitan identificar el tipo de información que contienen. Deberán indicar el nivel de seguridad de la información contenida de mayor calificación sin revelar su contenido.

Sólo AAPP: No
Fuentes: RD 1720/2007 art. 92.1, ENS mp.si.1.
Excepciones: no se aplicará cuando las características físicas del soporte no lo permitan.

LW.28. **Inventariado de soportes.** Como responsable del tratamiento quiero que los soportes informáticos que contengan datos de carácter personal sean inventariados.
Sólo AAPP: No
Fuentes: RD 1720/2007 art. 92.1.
Excepciones: no se aplicará cuando las características físicas del soporte no lo permitan.

LW.28.1. **Inventariado de soportes. Acceso.** Como responsable del tratamiento quiero que los soportes informáticos que contengan datos de carácter personal solo sean accesibles por el personal autorizado en el documento de seguridad.
Sólo AAPP: No
Fuentes: RD 1720/2007 art. 92.1.
Excepciones: no se aplicará cuando las características físicas del soporte no lo permitan.

LW.29. **Autorización de salida de soportes por responsable.** Como responsable del tratamiento quiero ser el único capaz de autorizar expresamente la salida de soportes informáticos que contengan datos de carácter personal, así como su tratamiento fuera de los locales donde esté ubicado el fichero, garantizándose el nivel de seguridad correspondiente al tipo de fichero tratado.
Sólo AAPP: No
Fuentes: RD 1720/2007 art. 92.2.
Excepciones: -

LW.30. **Autorización de salida de soportes por Documento de Seguridad.** Como responsable del tratamiento quiero que el Documento de Seguridad pueda recoger casos autorizados para la salida de soportes.
Sólo AAPP: No
Fuentes: RD 1720/2007 art. 92.2.
Excepciones: -

LW.31. **Salida de soportes. Medidas de seguridad.** Como responsable del tratamiento y de seguridad quiero que durante el proceso de traslado se adoptarán las medidas dirigidas a evitar robos, pérdidas o accesos indebidos a la documentación.
Sólo AAPP: No
Fuentes: RD 1720/2007 art. 92.3, ENS mp.si.4.
Excepciones: -

LW.32. **Borrado de soportes. Medidas de seguridad.** Como responsable del fichero y de seguridad quiero que durante el proceso de borrado de datos se adopten medidas para impedir su acceso o recuperación posterior.
Sólo AAPP: No
Fuentes: RD 1720/2007 art. 92.4, ENS mp.si.5.
Excepciones: -

LW.33. **Procedimientos de copias de respaldo.** Como responsable del tratamiento quiero verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo.

Sólo AAPP: No
Fuentes: RD 1720/2007 art. 92.2, ENS mp.info.9.
Excepciones: -

LW.34. **Procedimientos de recuperación de copias.** Como responsable del tratamiento y de la información quiero verificar la definición y correcta aplicación de los procedimientos de recuperación de los datos almacenados en copias de respaldo.

Sólo AAPP: No
Fuentes: RD 1720/2007 art. 92.2.
Excepciones: -

LW.34.1. **Procedimientos manuales de recuperación de copias.** Como responsable del tratamiento y de la información quiero que se tenga en cuenta que la recuperación podrá ser manual en aquellos tratamientos o ficheros semi-automatizados siempre que la documentación existente (documentos físicos por ejemplo) lo permita.

Sólo AAPP: No
Fuentes: RD 1720/2007 art. 92.2.
Excepciones: -

LW.35. **Test de recuperación.** Como responsable del tratamiento y de la información quiero verificar cada 6 meses que los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos garanticen su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. Este proceso no se realizará con datos reales.

Sólo AAPP: No
Fuentes: RD 1720/2007 art. 94.3 y RD 1720/2007 94.4.
Excepciones: El proceso podrá realizarse con datos reales siempre que se realice previamente una copia de seguridad, se garantice un adecuado nivel de seguridad y se anote su realización en el documento de seguridad.

LW.36. **Periodicidad de copias.** Como responsable del tratamiento y del sistema quiero que las copias de respaldo se realicen, al menos, semanalmente.

Sólo AAPP: No
Fuentes: RD 1720/2007 art. 94.1.
Excepciones: No se aplicará si no se hubiera producido ninguna actualización de los datos.

LW.37. **Proceso de adquisición de nuevos componentes.** Como responsable del sistema quiero crear un proceso formal para planificar la adquisición de nuevos componentes del sistema que será acorte con el análisis de riesgos y la arquitectura de seguridad elegida.

Sólo AAPP: SÍ
Fuentes: ENS op.pl.3.
Excepciones: -

LW.38. **Protección de portátiles.** Como responsable del sistema quiero que se realicen acciones de control, gestión de incidentes, conexión remota y clave de acceso en los portátiles.

Sólo AAPP: SÍ
Fuentes: ENS mp.eq.3.
Excepciones:-

LW.38.1. **Protección de portátiles. Control.** Como responsable del sistema quiero que se establezca un control periódico para verificar que la persona responsable de un equipo portátil sigue teniendo el dispositivo bajo su control.

Sólo AAPP: SÍ
Fuentes: ENS mp.eq.3.
Excepciones:-

LW.38.2. **Protección de portátiles. Gestión de incidentes.** Como responsable del sistema quiero que se establezca un protocolo para la comunicación de incidentes, perdidas o sustracciones de los equipos portátiles.

Sólo AAPP: SÍ
Fuentes: ENS mp.eq.3.
Excepciones:-

LW.38.3. **Protección de portátiles. Conexión remota.** Como responsable de seguridad quiero que se limiten la información y servicios disponibles para las conexiones remotas que realicen los portátiles cuando se conecten desde redes que no estén bajo el estricto control de la organización.

Sólo AAPP: SÍ
Fuentes: ENS mp.eq.3.
Excepciones:-

LW.38.4. **Protección de portátiles. Clave de acceso.** Como responsable de seguridad quiero que los dispositivos portátiles no almacenen claves de acceso remoto a la organización.

Sólo AAPP: SÍ
Fuentes: ENS mp.eq.3.
Excepciones:-

LW.38.5. **Protección de portátiles. Inventario.** Como responsable del sistema y del sistema quiero que se lleve un inventario de los equipos portátiles que puedan salir de las instalaciones de la organización junto con la persona responsable del mismo.

Sólo AAPP: SÍ
Fuentes: ENS mp.eq.3.
Excepciones: -

LW.39. **Aplicaciones. Puesta en servicio.** Como responsable de seguridad quiero que las aplicaciones sean suficientemente probadas de forma que se garantice que cumplen con los criterios de seguridad y de que no afecta a la misma. Las pruebas se realizarán en un entorno de pre-producción y con datos no reales.

Sólo AAPP: SÍ

Fuentes: ENS mp.sw.2.
Excepciones:-

LW.40. **Firma electrónica.** Como responsable de seguridad y del servicio quiero que para cualquier tipo de firma electrónica que tenga que ser usado en el tratamiento se utilice alguno de los tipos previstos en la legislación vigente.
Sólo AAPP: SÍ
Fuentes: ENS mp.info.4.
Excepciones:-

LW.41. **Correo electrónico.** Como responsable de seguridad quiero que el correo electrónico se proteja frente a las amenazas que le son propias como spam, programas dañinos, código tipo "applet", etc.
Sólo AAPP: SÍ
Fuentes: ENS mp.s.1.
Excepciones:-

LW.41.1. **Correo electrónico. Normas de uso.** Como responsable de seguridad quiero que se establezcan unas normas de uso para el personal que use el correo electrónico que contengan limitación a su uso para comunicaciones privadas actividades de concienciación y formación.
Sólo AAPP: SÍ
Fuentes: ENS mp.s.1.
Excepciones:-

LW.42. **Servicios y aplicaciones web.** Como responsable de seguridad y del servicio quiero que los sistemas dedicados a la publicación de información sean protegidos frente a las amenazas que le son propias: accesos por vías alternativas a los datos, ataques de manipulación de URL, mediantes cookies, inyección de código, *cross site scripting*, proxies, caches, etc..
Sólo AAPP: SÍ
Fuentes: ENS mp.s.2.
Excepciones:-

LW.43. **Certificados de sistemas.** Como responsable de seguridad y del servicio quiero que los sistemas dedicados a la publicación de información utilicen certificados de autenticación acordes a la normativa europea.
Sólo AAPP: SÍ
Fuentes: ENS mp.s.2.
Excepciones:-

5.1.3 Requisitos de sistema para alcanzar el nivel MEDIO de seguridad (RGPD, LOPD, RD 1720/2007 y ENS)

MD.1. **Evaluación de Impacto.** Como responsable del tratamiento quiero que se realice una evaluación de impacto que identifique los posibles riesgos del tratamiento y evalué los riesgos que conlleva y el alcance de los mismos. Amplia el requisito LW.16 incluyendo un análisis semi-formal y los siguientes aspectos:

a) Valoración cualitativa de los activos más valiosos del sistema
b) Cuantificación de las amenazas más probables
c) Valoración de las medidas elegidas
d) Valoración del riesgo residual
e) Los requisitos de disponibilidad de cada servicio y los elementos que son críticos de los mismos

Sólo AAPP: No
Fuentes: RGPD art. 35, ENS op.cont.1.
Excepciones: -

MD.2. **Arquitectura de seguridad.** Amplía el requisito **LW.7** incluyendo:
e) Sistema de gestión de los recursos relativos a la seguridad del a información.

Sólo AAPP: SÍ
Fuentes: ENS op.pl.2.
Excepciones: -
*Extiende: **LW.7**.*

MD.3. **Documento de Seguridad. Contenido.** Como responsable del tratamiento quiero que el documento de seguridad contenga como mínimo los siguientes aspectos:
a) La identificación del responsable o responsables de seguridad.
b) La revisión de los registros de actividad buscando patrones anormales.
b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

Sólo AAPP: No
Fuentes: RD 1720/2007 art. 88, RD 1720/2007 art. 95, ENS op.exp.8.
Excepciones: -

MD.4. **Encargados del tratamiento. Contratación y acuerdos.** Como responsable del tratamiento quiero que previo a la contratación o el establecimiento de acuerdos con terceros encargados del tratamiento se detallen contractualmente los servicios prestados y las responsabilidades de las partes, incluyendo la calidad mínima del servicio, las consecuencia de su incumplimiento, los mecanismos de coordinación en caso de incidentes y para el mantenimiento.

Sólo AAPP: SÍ
Fuentes: ENS op.ext.1, ENS op.ext.2.
Excepciones: -

MD.5. **Encargados del tratamiento. Supervisión.** Como responsable del tratamiento quiero que se mida rutinariamente el cumplimiento de las obligaciones de servicios de los contratos con terceros encargados del tratamiento para detectar si se cumple la calidad mínima de ***MD.4***.

Sólo AAPP: SÍ
Fuentes: ENS op.ext.2.
Excepciones: -
*Referencia: **MD.4**.*

MD.6. **Revisión continúa.** Como responsable del tratamiento quiero que se establezca un procedimiento para que se gestione de forma continua la configuración de los componentes del sistema y de los cambios realizados o que se vayan a realizar.

Sólo AAPP: SÍ
Fuentes: ENS op.pl.3, ENS op.pl.5.
Excepciones: -

MD.7. **Auditoría.** Como responsable del fichero quiero que los sistemas de información e instalaciones de tratamiento de datos se sometan a una auditoría interna o externa, que verifique el cumplimiento de todo lo dispuesto en los requisitos de seguridad vigentes, al menos, cada dos años.

Sólo AAPP: No
Fuentes: RD 1720/2007 art. 96.
Excepciones: Se deberá volver a realizar la auditoría siempre que se realicen cambios sustanciales en el sistema de información que puedan afectar al funcionamiento de las medidas de seguridad implantadas.

MD.8. **Informe de auditoría.** Como responsable del tratamiento quiero que el informe de auditoría contenga la siguiente información:

a) Dictamen sobre la adecuación de las medidas y controles al presente conjunto de requisitos.
b) Identificación de las deficiencias y propuestas de medidas correctoras o complementarias necesarias.
c) Datos, hechos y observaciones en las que se basen los dictámenes alcanzados y las recomendaciones propuestas, en los dos puntos anteriores.

Sólo AAPP: No
Fuentes: RD 1720/2007 art. 96.2.
Excepciones: -

MD.9. **Análisis de resultados de auditoría.** Como responsable de seguridad quiero analizar los informes de auditoría e informar de sus conclusiones al responsable del fichero.

Sólo AAPP: No
Fuentes: RD 1720/2007 art. 96.3.
Excepciones: -

MD.10. **Almacenamiento de informes de auditoría.** Como responsable de seguridad quiero que los informes sean correctamente almacenados para su futura consulta.

Sólo AAPP: No
Fuentes: RD 1720/2007 art. 96.3.
Excepciones: -

MD.11. **Auditoría. Aplicación de medidas correctoras.** Como responsable del fichero quiero adoptar las medidas correctoras pertinentes según los informes del responsable de seguridad.

Sólo AAPP: No
Fuentes: RD 1720/2007 art. 96.3.
Excepciones: -

MD.12. **Protección de locales.** Como responsable del sistema quiero que el suministro eléctrico a los sistemas deberá estar garantizado en caso de fallo al menos el tiempo suficiente para un apagado ordenado de los procesos sin perdidas de información. Además los locales deberán ser protegidos frente a incidentes producidos por el agua como inundaciones.

Sólo AAPP: SÍ
Fuentes: ENS mp.if.4, ENS mp.if.6.
Excepciones: -

MD.13. **Puestos de trabajo.** Como responsable de seguridad quiero que se cree una relación de los puestos de trabajo del sistema identificando por cada puesto las responsabilidades que tiene asociadas en materia de seguridad, los requisitos de las personas que usen el puesto y que estos se tengan en cuenta para seleccionar la persona que lo vaya a ocupar.
Sólo AAPP: SÍ
Fuentes: ENS mp.per.1.
Excepciones: -

MD.13.1. **Puestos de trabajo. Protección del material.** Como responsable de seguridad quiero que el material del puesto de trabajo que no se esté usando en el momento de realizar la actividad esté guardado en lugar cerrado.
Sólo AAPP: SÍ
Fuentes: ENS mp.eq.1.
Excepciones: -

MD.13.2. **Puestos de trabajo. Bloqueo de sesión.** Como responsable de seguridad quiero que el puesto de trabajo se bloquee cuando se supere un cierto periodo de inactividad. El usuario podrá reanudar la sesión tras una nueva autenticación.
Sólo AAPP: SÍ
Fuentes: ENS mp.eq.2.
Excepciones: -

MD.14. **Procedimiento de acceso.** Se admitirá el uso de cualquier mecanismo de autenticación sustentado en dos factores de autenticación.
Sólo AAPP: SÍ
Fuentes: ENS op.acc.5.
Excepciones: -
*Extiende: **LW.16**.*

MD.14.1. **Procedimiento de acceso. Información del último acceso.** Como responsable del sistema quiero que este informe al usuario del último acceso efectuado con su identidad.
Sólo AAPP: SÍ
Fuentes: ENS op.acc.6.
Excepciones: -

MD.15. **Detección de intrusiones.** Como responsable del fichero quiero implantar el uso de herramientas de detección o prevención de intrusiones.
Sólo AAPP: SÍ
Fuentes: ENS op.mon.2.
Excepciones: -

MD.16. **Control de acceso físico.** Como responsable del fichero quiero establecer mecanismos para que solamente el personal autorizado en el documento de seguridad

pueda tener acceso físico a los locales donde se encuentran los sistemas de información con datos de carácter personal.

Sólo AAPP: No
Fuentes: RD 1720/2007 art. 99.
Excepciones: -

MD.17. **Control de acceso remoto. Política de acceso.** Como responsable del sistema quiero establecer una política de lo que puede hacerse remotamente, requiriendo autorización positiva.

*Sólo AAPP: **SÍ***
Fuentes: ENS op.acc.7.
Excepciones: -

MD.18. **Uso de claves criptográficas.** Como responsable del sistema quiero que se usen algoritmos acreditados por el Centro Criptológico Nacional.

*Sólo AAPP: **SÍ***
Fuentes: ENS op.exp.11.
Excepciones: -

MD.19. **Sistema de registro de entrada.** Como responsable del fichero quiero establecer un sistema de registro de entrada de soportes que permita obtener la siguiente información:

a) Tipo de soporte.
b) Fecha y hora de la entrada.
c) El emisor.
d) Número de documentos o soportes.
e) Tipo de información que contienen.
f) Forma de envío.
g) Persona responsable de la recepción debidamente autorizada.

Sólo AAPP: No
Fuentes: RD 1720/2007 art. 97.1, ENS mp.info.2.
Excepciones: -

MD.20. **Sistema de registro de salida.** Como responsable del fichero quiero establecer un sistema de registro de salida de soportes que permita obtener la siguiente información:

a) Tipo de soporte.
b) Fecha y hora de la salida.
c) El destinatario.
d) Número de documentos o soportes.
e) Tipo de información que contienen.
f) Forma de envío.
g) Persona responsable de la entrega debidamente autorizada.

Sólo AAPP: No
Fuentes: RD 1720/2007 art. 97.2, ENS mp.info.2.
Excepciones: -

MD.21. **Soportes de información. Custodia.** Como responsable de seguridad quiero que esté garantizado el control de acceso a los soportes de información.

*Sólo AAPP: **SÍ***
Fuentes: ENS mp.si.3.

Excepciones: -

MD.22. **Soportes de información. Mantenimiento.** Como responsable de seguridad quiero que esté garantizado el mantenimiento de acuerdo con el fabricante de los soportes de información.
*Sólo AAPP: **SÍ***
Fuentes: ENS mp.si.3.
Excepciones: -

MD.23. **Dispositivos removibles.** Como responsable de seguridad quiero que el contenido de los dispositivos removibles esté encriptado mediantes mecanismos que garanticen la confidencialidad y la integridad.
*Sólo AAPP: **SÍ***
Fuentes: ENS mp.si.2.
Excepciones: -

MD.24. **Registro de incidencias.** Como responsable del tratamiento quiero que se registren todas las actuaciones relacionadas con la gestión de incidentes:
a) Reporte inicial, actuaciones de emergencia y las modificaciones implementadas.
b) Tiempo empleado en resolver la incidencia.
c) Registro de evidencias para sustentar o hacer frente a demandas judiciales.
d) Revisión de los elementos auditables.
e) En el caso de procedimientos de recuperación de datos se añadirá además:
    1) La persona que los ejecuto
    2) Los datos restaurados
    3) Los datos que han sido necesarios grabar manualmente
Sólo AAPP: No
Fuentes: ENS op.exp.10, ENS op.mon.2, RD 1720/2007 art. 100.1.
Excepciones: -

MD.25. **Procedimiento de recuperación de datos.** Como responsable del tratamiento quiero que no se ejecute ningún procedimiento de recuperación de datos sin mi autorización.
Sólo AAPP: No
Fuentes: RD 1720/2007 art. 100.2.
Excepciones: -

MD.26. **Dimensionamiento / gestión de capacidades.** Como responsable del sistema quiero realizar un estudio que cubra las necesidades de recursos de almacenamiento, procesamiento, personal, etc. que necesita el sistema.
*Sólo AAPP: **SÍ***
Fuentes: ENS op.pl.4.
Excepciones: -

MD.27. **Segregación de funciones y tareas.** Como responsable del sistema quiero se exigirá la concurrencia de dos o más personas para realizar tareas críticas. Como mínimo se separarán las siguientes funciones:
a) Desarrollo de operación.
b) Configuración y mantenimiento del sistema de operación.
c) Auditoría o supervisión de cualquier otra función.

Sólo AAPP: SÍ
Fuentes: ENS op.acc.3.
Excepciones: -

MD.28. **Redes virtuales.** Como responsable de seguridad quiero que cuando las comunicaciones discurran por redes externas se usen redes privadas virtuales con algoritmos acreditados por el Centro Criptológico Nacional.
Sólo AAPP: SÍ
Fuentes: ENS mp.com.2, ENS mp.com.3.
Excepciones: -

MD.29. **Desarrollo de aplicaciones.** Como responsable de seguridad quiero que las aplicaciones que se desarrollen se realice sobre un sistema diferente y separado del de producción. No se utilizarán herramientas o datos de desarrollo en el entorno de producción.
Sólo AAPP: SÍ
Fuentes: ENS mp.sw.1.
Excepciones: -

MD.29.1. **Metodologías.** Como responsable del tratamiento quiero que las aplicaciones que se desarrollen utilicen una metodología reconocida que aplique la protección de datos desde el diseño de las mismas y por defecto.
Sólo AAPP: No
Fuentes: RGPD art. 25, ENS mp.sw.1.
Excepciones: -

MD.30. **Aplicaciones. Puesta en servicio.** Como responsable de seguridad quiero se realicen pruebas de penetración y análisis de vulnerabilidades de las aplicaciones antes de su puesta en servicio.
Sólo AAPP: SÍ
Fuentes: ENS mp.sw.2.
Excepciones: -
*Extiende: **LW.39**.*

MD.31. **Firma electrónica avanzada.** Como responsable de seguridad quiero que cuando se tengan que emplear sistemas de firma electrónica avanzada basados en certificados, estos sean cualificados.
Sólo AAPP: SÍ
Fuentes: ENS mp.info.4.
Excepciones: -
*Extiende: **LW.40**.*

MD.32. **Firma electrónica. Seguridad.** Como responsable de seguridad quiero que cuando se tengan que emplear sistemas de firma electrónica se empleen algoritmos y parámetros acreditados por el Centro Criptológico Nacional.
Sólo AAPP: SÍ
Fuentes: ENS mp.info.4.
Excepciones:-
*Extiende: **LW.40**.*

MD.33. **Firma electrónica. Validación.** Como responsable de seguridad quiero que cuando se tengan que emplear sistemas de firma electrónica se agreguen a la firma toda la información pertinente para su verificación y validación: certificados y datos de verificación y validación.

*Sólo AAPP: **SÍ***
Fuentes: ENS mp.info.4.
Excepciones: -
*Extiende: **LW.40**.*

MD.34. **Denegación de servicio.** Como responsable de seguridad quiero que se planifique el sistema para atender la carga prevista con holgura y se desplegarán tecnologías adecuadas para prevenir ataques conocidos.

*Sólo AAPP: **SÍ***
Fuentes: ENS mp.s.9.
Excepciones: -

5.1.4 Requisitos de sistema para alcanzar el nivel ALTO de seguridad (RGPD, LOPD, RD 1720/2007 y ENS)

HG.1. **Evaluación de Impacto.** El análisis debe ser formal e incluir además la identificación de las vulnerabilidades habilitantes de dichas amenazas.

*Sólo AAPP: **SÍ***
Fuentes: ENS op.pl.1.
Excepciones: -
*Extiende: **MD.1**.*

HG.2. **Consulta de asesoramiento.** Como responsable del tratamiento quiero realizar una consulta a la autoridad de control sobre el tratamiento a realizar para conocer si las medidas adoptadas para reducir el riesgo del tratamiento son adecuadas o si el propio tratamiento puede estar infringiendo el reglamento.

Sólo AAPP: No
Fuentes: RGPD art 36.
Excepciones: -

HG.3. **Arquitectura de seguridad.** Se incluye además:

f) Sistema de gestión de seguridad de la información con actualización y aprobación periódica.
g) Controles técnicos internos.

*Sólo AAPP: **SÍ***
Fuentes: ENS op.pl.2.
Excepciones: -
*Extiende: **MD.2**.*

HG.4. **Plan de continuidad.** Como responsable del sistema quiero que se desarrolle un plan de continuidad que establezca las acciones a realizar en caso de interrupción de los servicios prestados.

*Sólo AAPP: **SÍ***
Fuentes: ENS op.cont.2.

Excepciones: -

HG.4.1. **Tests del plan de continuidad.** Como responsable del sistema quiero que se realicen pruebas del plan de continuidad de forma periódico con el fin de depurarlos y corregir las deficiencias que pudiera tener.

Sólo AAPP: SÍ
Fuentes: ENS op.cont.3.
Excepciones: -

HG.5. **Medios alternativos.** Como responsable del tratamiento quiero disponer de los medios alternativos suficientes donde poder trabajar en caso de que los habituales no estén disponibles (incluidas las instalaciones). Los medios alternativos deberán contar con las mismas condiciones de seguridad que los habituales.

Sólo AAPP: SÍ
Fuentes: ENS mp.eq.9, ENS mp.if.9, ENS mp.com.9, ENS mp.s.9.
Excepciones: -

HG.6. **Personal alternativo.** Como responsable del sistema quiero que se garantice que en caso de indisponibilidad del personal habitual otras personas puedan realizar sus funciones. El personal sustituto deberá estar sometido a las mismas garantías de seguridad que el personal habitual.

Sólo AAPP: SÍ
Fuentes: ENS mp.per.9.
Excepciones: -

HG.7. **Puestos de trabajo. Cierre de sesiones.** Como responsable de seguridad quiero que el puesto de trabajo cierre automáticamente todas las sesiones que tuviera abiertas tras superar un cierto periodo después del bloqueo de la sesión activa.

Sólo AAPP: SÍ
Fuentes: ENS mp.eq.2.
Excepciones: -

HG.8. **Distribución de soportes cifrados.** Como responsable del tratamiento quiero que la distribución de soportes que contengan datos de carácter personal se realice cifrando los datos o utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte, garantizando así la confidencialidad y la integridad de los mismos.

Sólo AAPP: No
Fuentes: RD 1720/2007 art. 101.2.
Excepciones: -

HG.9. **Uso de dispositivos portátiles.** Como responsable del tratamiento quiero que únicamente se usen dispositivos portátiles para el tratamiento que permitan el cifrado de sus datos.

Sólo AAPP: No
Fuentes: RD 1720/2007 art. 101.3.
Excepciones: En caso de que los datos sea necesario tratarlos por dispositivos portátiles que no permitan el cifrado de sus datos se hará constar motivadamente en el documento de seguridad y se adoptarán las medidas pertinentes.

HG.10. **Cifrado de dispositivos portátiles.** Como responsable del tratamiento quiero que los que datos de carácter personal que contengan los dispositivos portátiles que salgan fueran de las instalaciones se encuentren cifrados.

Sólo AAPP: No
Fuentes: RD 1720/2007 art. 101.2, ENS mp.eq.3, ENS mp.info.3.
Excepciones: -

HG.11. **Identificación de soportes codificada.** Como responsable del tratamiento quiero que los sistemas de etiquetado de los soportes estén codificados de forma que sean comprensibles para el personal con acceso autorizado pero dificulten su identificación para el resto de personas.

Sólo AAPP: No
Fuentes: RD 1720/2007 art. 101.1.
Excepciones: -

HG.12. **Cifrado de soportes.** Como responsable del tratamiento quiero que los datos se almacenen encriptados en los soportes de información mediante algoritmos certificados por el Centro Criptológico Nacional.

*Sólo AAPP: **SÍ***
Fuentes: ENS mp.info.3.
Excepciones: -

HG.13. **Borrado de soportes. Productos certificados.** Como responsable de seguridad quiero que para el borrado de soportes se utilicen productos certificados de acuerdo al requisito **HG.24**.

Sólo AAPP: No
Fuentes: RD 1720/2007 art. 92.4, ENS mp.si.5.
Excepciones: -
*Referencia: **HG.24**.*

HG.14. **Copia de respaldo de datos.** Como responsable del fichero quiero que deba conservarse al menos una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente a aquel en que se encuentren los equipos informáticos que los tratan, cumpliendo siempre con las medidas de seguridad exigidas en este documento o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

Sólo AAPP: No
Fuentes: RD 1720/2007 art. 102.
Excepciones: -

HG.15. **Copia de respaldo de procedimientos de recuperación.** Como responsable del fichero quiero que deba conservarse al menos una copia de respaldo de los procedimientos de recuperación de datos en un lugar diferente a aquel en que se encuentren los equipos informáticos que los tratan, cumpliendo siempre con las medidas de seguridad exigidas en este documento o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

Sólo AAPP: No

Fuentes: RD 1720/2007 art. 102.
Excepciones: -

HG.16. **Registro de intentos de acceso.** Como responsable de seguridad quiero que de cada intento de acceso se guarde la siguiente información:

a) La identificación del usuario.
b) La fecha y hora en que se realizó.
c) El fichero accedido.
d) El tipo de acceso.
e) Si el acceso ha sido autorizado o denegado.
f) En caso de que sea autorizado, la información necesaria para identificar el registro accedido.

Sólo AAPP: No
Fuentes: RD 1720/2007 art. 103.1, RD 1720/2007 art. 103.2, RD 1720/2007 art. 103.6.
Excepciones: Esta información no será necesaria registrarla cuando el responsable del tratamiento garantice que únicamente él tiene acceso y trata los datos personales o cuando dicho responsable sea una persona física.

HG.17. **Control de mecanismo de acceso.** Como responsable de seguridad quiero controlar directamente los mecanismos que permiten el registro de la información para los accesos, sin que se deba permitir, en ningún caso, la desactivación de los mismos. Para ellos se utilizará un sistema automático y protegido de recolección de registros y correlación de eventos.

*Sólo AAPP: **SÍ***
Fuentes: RD 1720/2007 art. 103.3, ENS op.exp.8, ENS op.exp.10.
Excepciones: -

HG.18. **Procedimiento de acceso.** Las credenciales se suspenderán tras un periodo definido de no utilización. En el caso de utilización de "algo que se tiene", se requerirá el uso de elementos criptográficos hardware usando algoritmos y parámetros acreditados por el Centro Criptológico Nacional.

*Sólo AAPP: **SÍ***
Fuentes: ENS op.acc.5.
Excepciones: -
*Extiende: **MD.14**.*

HG.19. **Limitación de acceso por horas, fechas y lugar.** Como responsable del sistema quiero que el acceso esté limitado por horario, fechas y lugar desde donde se accede. Se definirán aquellos puntos en los que el sistema requerirá de una renovación regular del acceso, no bastando con la sesión establecida.

*Sólo AAPP: **SÍ***
Fuentes: ENS op.acc.6.
Excepciones: -

HG.20. **Revisión de información de acceso.** Como responsable de seguridad quiero encargarme de revisar la información de control de acceso registrada, al menos, cada mes.

Sólo AAPP: No
Fuentes: RD 1720/2007 art. 103.5.
Excepciones: -

HG.21. **Informe de revisión de información de acceso.** Como responsable de seguridad elaboraré y mantendré un documento de las revisiones realizadas y los problemas detectados.
Sólo AAPP: No
Fuentes: RD 1720/2007 art. 103.5.
Excepciones: -

HG.22. **Conservación de información de acceso.** Como responsable del fichero quiero que la información de control de los registros de accesos deberá conservarse como mínimo durante un periodo de dos años.
Sólo AAPP: No
Fuentes: RD 1720/2007 art. 103.4.
Excepciones: -

HG.23. **Transmisión de datos.** Como responsable del fichero quiero que en caso de que la transmisión de datos de carácter personal sea a través de redes de telecomunicaciones públicas o inalámbricas se realice utilizando algoritmos de cifrado que garantice que la transmisión no sea inteligible ni manipulada por terceros.
Sólo AAPP: No
Fuentes: RD 1720/2007 art. 104.
Excepciones: -

HG.24. **Componentes y dispositivos certificados.** Como responsable del sistema quiero utilizar sistemas, productos o equipos cuyos certificados estén reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.
Sólo AAPP: SÍ
Fuentes: ENS op.pl.5, ENS mp.si.3.
Excepciones: -

HG.25. **Encargados del tratamiento. Servicio garantizado.** Como responsable del sistema quiero que esté prevista la provisión del servicio por medios alternativos en caso de indisponibilidad del servicio contratado.
Sólo AAPP: SÍ
Fuentes: ENS op.ext.9.
Excepciones: -

HG.26. **Encargados del tratamiento. Medios alternativos.** Como responsable del tratamiento quiero que los servicios contratados dispongan de medios alternativos que garanticen su continuidad en caso de indisponibilidad. Los servicios alternativos disfrutarán de las mismas garantías que los servicios habituales.
Sólo AAPP: SÍ
Fuentes: ENS op.ext.9.
Excepciones: -

HG.27. **Protección de portátiles. Manipulación.** Como responsable de seguridad quiero que se instalen en el dispositivo detectores de violación que permitan saber que el equipo ha sido manipulado y activen los procedimientos adecuados.
Sólo AAPP: SÍ

Fuentes: ENS mp.eq.3.
Excepciones: -

HG.28. **Cortafuegos. Duplicidad.** Como responsable de seguridad quiero que se disponga de un sistema redundante de dos cortafuegos de distinto fabricante en cascada.
Sólo AAPP: SÍ
Fuentes: ENS mp.com.2.
Excepciones: -

HG.29. **Redes virtuales. Dispositivos hardware.** Como responsable de seguridad quiero que las redes virtuales se establezcan y utilicen usando dispositivos hardware certificados como se indica en ***HG.24***.
Sólo AAPP: SÍ
Fuentes: ENS mp.com.2.
Excepciones: -
*Referencia: **HG.24**.*

HG.30. **Cifrado durante la transmisión.** Como responsable del tratamiento quiero que los datos que se transmitan por los distintos canales de comunicación se encuentren cifrados mediante algoritmos certificados por el Centro Criptológico Nacional.
Sólo AAPP: SÍ
Fuentes: ENS mp.info.3.
Excepciones: -

HG.31. **Segregación de redes.** Como responsable de seguridad quiero que la red esté segmentada de forma que por cada segmento se controle la entrada de usuarios y la salida de información.
Sólo AAPP: SÍ
Fuentes: ENS mp.com.3.
Excepciones: -

HG.32. **Aplicaciones. Puesta en servicio.** Como responsable de seguridad quiero se realicen pruebas de coherencia con el resto de procesos de las aplicaciones antes de su puesta en servicio. Se considerará realizar también una auditoría del código fuente.
Sólo AAPP: SÍ
Fuentes: ENS mp.sw.2.
Excepciones:-
*Extiende: **MD.30**.*

HG.33. **Firma electrónica. Productos certificados.** Como responsable de seguridad quiero que cuando se tengan que emplear sistemas de firma electrónica se empleen productos certificados de acuerdo al requisitos ***HG.24***.
Sólo AAPP: SÍ
Fuentes: ENS mp.info.4.
Excepciones:-
*Referencia: **HG.24**.*

HG.34. **Sellado de tiempo.** Como responsable del tratamiento quiero que cuando se utilicen sistemas de sellado cualificados de tiempo electrónico acordes con la normativa

europea en aquella información que sea susceptible de ser utilizada como evidencia electrónica en el futuro. Se utilizarán productos certificados de acuerdo al requisito **HG.24**.

Sólo AAPP: SÍ
Fuentes: ENS mp.info.5.
Excepciones:-
*Referencia: **HG.24**.*

HG.35. **Servicios y aplicaciones web. Certificados cualificados.** Como responsable de seguridad quiero que los sistemas dedicados a la publicación de información utilicen certificados cualificados de autenticación acordes a la normativa europea.

Sólo AAPP: SÍ
Fuentes: ENS mp.s.2.
Excepciones:-
*Extiende: **LW.42**.*

HG.36. **Denegación de servicio. Detección.** Como responsable de seguridad quiero que se implante un sistema de detección de ataques DOS, procedimientos de reacción y que se impida la ejecución de ataques desde las propias instalaciones perjudicando a terceros.

Sólo AAPP: SÍ
Fuentes: ENS mp.s.9.
Excepciones:-
*Extiende: **MD.34**.*