I. Comunidad Autónoma

3. Otras disposiciones

Consejería de Transparencia, Participación y Administración Pública

4883 Orden de la Consejería de Transparencia, Participación y Administración Pública por la que se aprueba la aplicación Corporativa SIRAT.

El 25 de mayo de 2018 entró en vigor el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, Reglamento General de Protección de Datos.

Asimismo, el 7 de diciembre de 2018 entró en vigor la Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digítales, que tiene por objeto adaptar al ordenamiento jurídico español el citado reglamento, así como garantizar los derechos digitales de la ciudadanía conforme al mandato establecido por el artículo 18.4 de la Constitución.

La entrada en vigor del Reglamento General de Protección de Datos (en adelante RGPD), ha tenido un enorme impacto sobre la actividad de las Administraciones Públicas, estableciendo un nutrido grupo de obligaciones a las mismas, y, más concretamente, a los responsables y encargados del tratamiento.

Entre otras obligaciones, y por citar solo algunas, estos tienen que identificar con precisión las finalidades y la base jurídica de los tratamientos que llevan a cabo, deben establecer un Registro de Actividades de Tratamiento, deben establecer mecanismos visibles, accesibles y sencillos para el ejercicio de derechos, tienen que hacer un análisis de riesgo para los derechos y libertades de los ciudadanos de todos los tratamientos de datos que se desarrollen, etc.

El cumplimiento de las obligaciones impuestas a las Administraciones Públicas, y, en concreto, a la Administración Pública Regional, conlleva la necesidad de contar con las herramientas tecnológicas necesarias que les procuren el adecuado soporte material, sobre todo, teniendo en cuenta que el ejercicio de competencias y las relaciones administrativas han de estar basadas, desde la entrada en vigor de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, exclusivamente en medios electrónicos.

Por otro lado, la asignación eficiente de los recursos económicos y la contención racional del gasto impone la necesidad de la existencia de una única herramienta tecnológica cuyo uso sea compartido por toda la organización y las entidades que integran la Administración Pública Regional.

Por tanto, coherente con esta necesidad surge la de proceder a la aprobación de una aplicación corporativa que dé soporte a las actividades que a la Administración Pública Regional le competen en materia de protección de los derechos de las personas en el tratamiento de sus datos personales.

Esta herramienta, además, ha de integrarse armónicamente con el resto de herramientas y servicios de la plataforma de administración electrónica de la

CARM, con objeto de usar y proporcionar la información requerida, a través de la interoperabilidad con servicios electrónicos y las herramientas de gestión interna integradas en aquel, reutilizando la información y funcionalidades existentes.

Por otro lado, hay que considerar que la seguridad de la información, constituye un valor fundamental reiterado largamente en el RGPD, de forma que, como expresa su artículo 6.1.f), los datos deben ser tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas. De ahí, la importancia de observar, especialmente, las previsiones contenidas en el Esquema Nacional de Seguridad.

En este sentido, hay que tener en cuenta lo establecido en la Orden de 28 de marzo de 2017, del Consejero de Hacienda y Administración Pública por la que se establece la política de seguridad de la información y las atribuciones en dicha materia al órgano con competencias en materia de informática.

El Decreto 302/2011, de 25 de noviembre, de Régimen Jurídico de la Gestión Electrónica de la Administración Pública de la Comunidad Autónoma de la Región de Murcia, regula el régimen de aprobación de aplicaciones informáticas corporativas mediante orden en su artículo 6.4, estableciendo que la aprobación de aplicaciones y sistemas informáticos corporativos le corresponde al titular de la Consejería competente en materia de innovación de los servicios públicos, previo informe favorable de la Dirección General competente en materia de planificación informática, sistemas de información y aplicaciones corporativas.

El Decreto del Presidente 174/2019, de 6 de septiembre, por el que se establecen los órganos directivos de la Consejería de Transparencia, Participación y Administración pública atribuye en su artículo 5 a la Dirección General de Regeneración y Modernización Administrativa las competencias en materia de modernización y calidad de los servicios públicos.

En base a todo lo anterior, y al amparo de las facultades atribuidas en el artículo 16 de la Ley 7/2004, de 28 de diciembre, de Organización y Régimen Jurídico de la Administración Pública de la Comunidad Autónoma de la Región de Murcia, previo informe favorable de la Dirección General de Informática y Transformación Digital,

Dispongo:

Artículo 1. Objeto y ámbito de aplicación.

1. Se aprueba la aplicación informática corporativa Sistema de Información Registro de Actividades de Tratamiento.- SIRAT

2. Esta orden se aplicará a la Administración Pública de la Región de Murcia, es decir, a su Administración General, organismos autónomos, entidades de derecho público vinculados o dependientes de ella, así como a sus fundaciones y consorcios. Entendiéndose, a estos efectos, todos aquellos incluidos en el ámbito de aplicación de los Presupuestos Generales de la Comunidad Autónoma de la Región de Murcia.

3. Se declara SIRAT, como aplicación corporativa en el ámbito indicado en el párrafo anterior. El acceso a la aplicación se realizará a través de la intranet de la CARM y desde Internet en la dirección https://sirat.carm.es

Artículo 2. Características de la aplicación.

1 SIRAT es una solución a medida, disponible a través de un portal web corporativo de la Comunidad Autónoma de la Región de Murcia (CARM), ajustándose a la normativa de desarrollo propia del entorno de desarrollo de CARM en el ámbito de la Administración Electrónica.

SIRAT se ubica en el contexto de la administración electrónica de la CARM, con objeto de usar y proporcionar la información requerida, reutilizando la información y funcionalidades existentes, entre otras, la herramienta para la definición de los procedimientos (DEXEL) o la herramienta para la gestión de expedientes electrónicos en trámite (SANDRA). Sobre todas estas funcionalidades se han añadido las específicas de SIRAT.

Desde el punto de vista de la transparencia, SIRAT proporciona la información requerida para el Portal de la Transparencia de la CARM relativa a las actividades de tratamiento.

Artículo 3. Funcionalidades de la aplicación.

La aplicación corporativa SIRAT gestiona los aspectos requeridos por la normativa en materia de protección de datos, en relación con:

1.- Registro de Actividades de Tratamiento.

Esta funcionalidad da cumplimiento a lo establecido en el RGPD de que todos los responsables y encargados de tratamiento, lleven un registro de las actividades de tratamiento efectuadas bajo su responsabilidad o por cuenta del responsable. El registro contiene toda la información que señala el artículo 30 del RGPD.

2.- Información de los tratamientos a los interesados.

Esta funcionalidad permite cumplir con las obligaciones impuestas, en los artículos 13 y 14 del RGPD, a los responsables del tratamiento del deber de informar.

Así, por un lado, permite componer las cláusulas de información en materia de protección de datos personales que deben incorporarse a las solicitudes de los interesados de inicio de los procedimientos, y, por otro, componer la comunicación de información a los interesados que debe dirigirse para el caso de que los datos personales no se hayan obtenido de los interesados.

3.- Ejercicio de los derechos de los interesados para la protección de sus datos personales.

Esta funcionalidad da cobertura al ejercicio de los derechos de los interesados previstos en los artículos 15 a 22 del RGPD. Estos derechos se pueden ejercitar, ante el responsable del tratamiento, a través de un formulario electrónico. Las solicitudes presentadas quedarán registradas, lo que permitirá hacer un seguimiento del estado de las solicitudes.

4.- Transparencia.

Esta funcionalidad permitirá publicar la información requerida en el Portal de la Transparencia de la CARM relativa a las actividades de tratamiento.

5.- Cuadro de mandos.

Esta funcionalidad permitirá realizar una explotación de la información residente en SIRAT, en concreto, se podrá obtener información sobre el cumplimiento de la normativa de protección de datos respecto al Registro de Actividades de Tratamiento, información y legitimación de los tratamientos, sobre

las cláusulas de información de los distintos procedimientos y actividades de tratamiento y sobre el ejercicio de derechos por los interesados en materia de protección de datos de carácter personal.

6.- Gestión de terceros.

Esta funcionalidad permitirá identificar los contratos con terceros y su adecuación de estos al RGPD.

7.- Notificaciones y Comunicaciones de violaciones de seguridad.

Esta funcionalidad permitirá, ante una violación de seguridad, realizar las notificaciones a la Agencia Española de Protección de Datos, así como las comunicaciones del encargado del tratamiento al responsable, y de este al interesado previstas en los artículos 33 y 34 del RGPD.

8.- Guías, herramientas y utilidades.

Esta funcionalidad contiene un repositorio con guías técnicas, herramientas, y otras utilidades, bien creadas por la Agencia Española de Protección de Datos, a las que se accederá a través del correspondiente enlace, o que puedan desarrollarse por la propia Administración Pública Regional.

9.- Consultas e Informes Delegado de Protección de Datos.

Esta funcionalidad permitirá realizar el seguimiento de las consultas que se soliciten al Delegado de Protección de datos, así como la contestación a las mismas e informes que se emitan.

Artículo 4. Requisitos técnicos de la aplicación.

La aplicación SIRAT deberá cumplir las guías técnicas definidas por la Dirección General competente en materia de planificación informática, sistemas de información y aplicaciones informáticas corporativas.

Artículo 5. Acceso y perfiles de usuario que intervienen en la aplicación.

1. El acceso a la aplicación SIRAT se realizará mediante la Plataforma de Acceso a los Servicios Electrónicos.- PASE, el servicio corporativo de identificación de usuarios, admitiendo las modalidades de acceso que dicho servicio proporcione y que sean compatibles con el nivel de aseguramiento en la calidad de la información (nivel QAA) que requiera el Esquema Nacional de Seguridad para este sistema de información.

2. Se establecen los siguientes perfiles de usuarios:

• SuperAdm: Administrador informático de la aplicación (permisos de desarrollo y soporte).

• Gestor de la aplicación: Administrador funcional de la aplicación. Accederá a la gestión de la aplicación (Parametrización, gestión de usuarios y permisos).

• Delegados de Protección de datos (DPD): Con acceso a toda la información de los organismos en los que está designado con esas funciones y órganos relacionados. Accederá a:

o Actividades de Tratamiento.

o Información.

o Aceptaciones.

o Ejercicios de Derechos.

• Director General: Con acceso a toda la información de su centro directivo. Es un perfil implícito, la pertenencia al mismo se deduce de la información de puestos de trabajo de la CARM. Accederá a:

o Actividades de Tratamiento.

o Información.

o Aceptaciones.

o Ejercicios de Derechos.

• Jefes de Servicio/Departamento responsable: Con acceso a la información del servicio/departamento correspondiente. Es un perfil implícito, la pertenencia al mismo se deduce de la información de puestos de trabajo de la CARM. Accederá a:

o Actividades de Tratamiento.

o Información.

• Informática: Como centro directivo encargado del tratamiento de la CARM, todo el personal perteneciente al mismo podrá acceder con este perfil. Es un perfil implícito, la pertenencia al mismo se deduce de la información de puestos de trabajo de la CARM. Accederá a:

o Actividades de Tratamiento (automatizados y mixtos).

Artículo 6. Responsabilidad sobre el correcto funcionamiento de la aplicación.

1. Conforme a lo establecido en el Decreto 44/2021, de 9 de abril, por el que se establecen los Órganos Directivos de la Consejería de Economía, Hacienda y Administración Digital, la Dirección General de Informática y Transformación Digital, como órgano directivo encargado de ejercer las competencias relativas a sistemas de información y comunicaciones corporativas incluida la planificación informática, así como sistemas de información, aplicaciones informáticas y seguridad informática garantizará la disponibilidad de la aplicación SIRAT y velará por el cumplimiento de lo dispuesto en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad.

El citado órgano directivo será el responsable del mantenimiento, supervisión y control de calidad (soporte y evolución tecnológica), así como de la auditoría del sistema de información.

2. Conforme a lo establecido en el Decreto 174/2019, de 6 de septiembre, por el que se establecen los Órganos Directivos de la Consejería de Transparencia, Participación y Administración Pública, la Dirección General de Regeneración y Modernización Administrativa, como órgano directivo encargado de ejercer las competencias relativas a administración electrónica y de interoperabilidad, así como de cumplimiento de la normativa aplicable en materia de protección de datos garantizará las funcionalidades de la aplicación SIRAT y velará por el cumplimiento de lo dispuesto en el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad.

El citado órgano directivo será el responsable funcional de la aplicación.

Artículo 7. Exclusiones.

De conformidad con lo establecido en el artículo 6.4 del Decreto 302/2011, podrá excluirse del uso de la aplicación SIRAT a aquellas unidades u órganos administrativos y demás sujetos incluidos dentro del ámbito de aplicación de la presente orden, que acrediten técnicamente que disponen de aplicaciones interoperables con dicha aplicación.

Disposición adicional primera.

Se entenderán incluidas en la aprobación de esta aplicación, cualesquiera otras nuevas funcionalidades, así como otros aspectos técnicos que la evolución tecnológica exija o demande o que, simplemente, aporten un valor añadido.

Disposición adicional segunda.

Se aprueba el formulario electrónico de Resolución de alta/baja/modificación de procedimientos en el Registro de Actividades de Tratamiento, así como el de Categorización de los Sistemas de Información contenidos, respectivamente, en los anexos I y II de esta orden.

Disposición transitoria.

En el plazo de 15 días desde la entrada en vigor de esta Orden, los órganos administrativos y demás sujetos incluidos dentro del ámbito de aplicación de la presente orden, centros y organismos de la Administración Regional que dispongan de aplicaciones informáticas específicas, solicitarán a la Dirección General de Regeneración y Modernización Administrativa la exclusión prevista en el artículo 7 de esta Orden.

Disposición final primera.

Se habilita al titular de la Dirección General competente en materia de modernización, innovación y calidad de los servicios para la realizar las adaptaciones que se consideren necesarias en los formularios electrónicos que se contienen en los anexos I y II de esta orden.

Disposición final segunda.

Entrada en vigor. La presente Orden entrará en vigor el día siguiente al de su publicación en el Boletín Oficial de la Región de Murcia.

Murcia, 1 de julio de 2021.—El Consejero de Transparencia, Participación y Administración Pública, Antonio Sánchez Lorente.

Anexo I

Resolución de (Órgano Directivo) por la que se acuerda (Alta/ Baja/Modificación) de procedimientos al Registro de Actividades de Tratamiento

Resultando: Que este órgano directivo, para mantener permanentemente actualizados los contenidos de los servicios y procedimientos de los que es responsable para su tramitación y resolución, ha procedido a dar de alta/baja/ modificación en la aplicación corporativa Dexel el/los procedimiento/s reseñados en el anexo a esta resolución, con el contenido que se indica en el mismo.

Resultando: Que, dada la naturaleza de las actividades y servicios que presta la Administración Pública Regional, los procedimientos administrativos y servicios se convierten en el principal medio para las distintas relaciones que esta tiene con los interesados, ya sean ciudadanos, empresas, instituciones públicas o privadas, o empleados públicos.

Por esta razón, son los procedimientos y servicios mismos los que se integran en el Registro de Actividades de Tratamiento, de tal modo que un procedimiento constituye una actividad de tratamiento.

Resultando: Que, como resultado de este proceso, es preciso incorporar su contenido al Registro de Actividades de Tratamiento de (nombre del centro directivo).

Vistos: El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD).

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD).

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

La Orden de 28 de marzo de 2017, del Consejero de Hacienda y Administración Pública por la que se establece la política de seguridad de la información en la Administración Regional.

Considerando: Que el artículo 30.1 del RGPD, relativo al registro de actividades que debe realizar el responsable del tratamiento señala que "cada responsable y, en su caso, su representante llevará un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:

a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;

b) los fines del tratamiento;

c) una descripción de las categorías de interesados y de las categorías de datos personales;

d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;

e) en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país

u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;

f) cuando sea posible, los Criterios previstos para la supresión de las diferentes categorías de datos;

g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1".

Considerando: Que el artículo 31.2 de LOPD adiciona, al contenido del Registro de Actividades de Tratamiento, además, la base legal del tratamiento.

Considerando: Que el artículo 31 en relación con el 77.1 de la LOPD destaca la obligación que tienen la Administración General del Estado, las Administraciones de las Comunidades Autónomas y las entidades que integran la Administración Local de hacer público, por medios electrónicos, un inventario de todas sus actividades de tratamiento y, en especial, de aquellas que incluyan categorías especiales de datos o de menores, donde se deje constancia de quién trata los datos, con qué finalidad y qué base jurídica legitima ese tratamiento.

Considerando: Que el artículo 4 del RGPD establece que es responsable del tratamiento "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento".

Considerando: Que, en el ámbito de CARM, hemos de acudir a lo que dispone la normativa regional para determinar quién es el responsable del tratamiento.

Así, la Ley 7/2004, de 28 de diciembre, de Organización y Régimen Jurídico de la administración pública de la Comunidad Autónoma de la Región de Murcia, establece en su artículo 19 que "los directores generales son los titulares de los órganos directivos encargados de la gestión de una o varias áreas funcionalmente homogéneas de cada Consejería".

Por otro lado, la Orden de 28 de marzo de 2017, que establece la política de seguridad de la información, en su artículo 12 establece que "el responsable de la información será, para cada sistema de información, el titular del órgano administrativo con competencia suficiente para decidir sobre la finalidad, contenido, uso y tratamiento de la información contenida en aquél".

Considerando: Que el artículo 31.1 de la LOPD determina que cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos deberán comunicarle cualquier adición, modificación o exclusión en el contenido del registro.

En virtud de todo ello

Resuelvo:

1.- Incorporar/dar de baja/ en el Registro de Actividades de Tratamiento de (nombre del Centro Directivo) el/los procedimiento/s contenidos en el anexo de esta resolución.

2.- El contenido del anexo se incorporará de forma automatizada en la aplicación corporativa SIRAT al Registro de Actividades de Tratamiento de (nombre del Centro Directivo).

3.- Para dar cumplimiento a las obligaciones de publicidad contenidas en el artículo 77.1 de la LOPD, la información del Registro de Actividades de

Tratamiento de este centro directivo se publicará en el Portal de la Transparencia de la CARM. Asimismo, en cumplimiento del 31.1 de la LOPD deberá comunicarse el contenido de esta resolución al Delegado de Protección de Datos a través de la dirección electrónica dpdigs@listas.carm.es

FIRMA DEL TITULAR DEL ÓRGANO DIRECTIVO.

ANEXO RESOLUCIÓN

NÚMERO Y NOMBRE DEL PROCEDIMIENTO O SERVICIO	
Responsable de tratamiento	
Departamento Tramitador	
Dirección del departamento tramitador	
Datos de contacto del delegado de protección de datos	
Base jurídica del tratamiento	
Norma con rango de ley que contiene la base jurídica para realizar el tratamiento	
Finalidad del tratamiento	
Descripción de los interesados	
Categoría de datos	
Destinatarios de la Cesión de los datos	
Transferencias internacionales	
Criterio para la conservación de datos	
Medidas de seguridad	

Anexo II

Resolución de categorización de Sistemas de Información conforme al Esquema Nacional de Seguridad

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, tiene por objeto determinar la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos.

El mencionado esquema está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la Información, y deberá ser aplicado por las Administraciones Públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ámbito de sus competencias.

El Capítulo X del mencionado Real Decreto, por su parte, regula la categorización de los sistemas de información. El artículo 43.1, contenido en dicho capítulo, establece que la categoría de un sistema de información en materia de seguridad modulará el equilibrio entre la importancia de la información que maneja, los servicios que presta y el esfuerzo de seguridad requerido, en función de los riesgos a los que está expuesto, bajo el criterio de proporcionalidad.

La determinación de la categoría de un sistema de información, conforme expresa el punto 2 del mencionado artículo 43, se efectuará en función de la valoración de impacto que tendría un incidente que afectara a la seguridad de la información o de los servicios con perjuicio de la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad, como dimensiones de seguridad. Para dicha determinación se ha de seguir el procedimiento establecido en el Anexo I del mencionado Real Decreto.

La valoración de las consecuencias de un impacto negativo sobre la seguridad de la información y de los servicios se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos (artículo 43.3).

El anexo IV del Real Decreto 3/2010 define el sistema de información como un conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

Por su parte, el artículo 44 del Real Decreto 3/2010 establece dos tipos de facultades para la categorización de los sistemas de información:

1. La facultad para efectuar las valoraciones a las que se refiere el mencionado artículo 43, así como la modificación posterior, en su caso, que corresponderá dentro del ámbito de su competencia al responsable de cada información o servicios, y

2. La facultad para determinar la categoría del sistema que corresponde al responsable del mismo.

El procedimiento para categorizar los sistemas de información está establecido en el Anexo I del Real Decreto 3/2010, estableciendo los fundamentos para la determinación de la categoría de un sistema, las dimensiones de seguridad, la determinación del nivel requerido en una dimensión de seguridad y, por último, la determinación de la categoría de un sistema de información, y, para ello se definen tres categorías: Básica, Media y Alta.

1. Un sistema de información será de categoría alta si alguna de sus dimensiones de seguridad alcanza el nivel alto.

2. Un sistema de información será de categoría media si alguna de sus dimensiones de seguridad alcanza el nivel media, y ninguna alcanza un nivel superior.

3. Un sistema de información será de categoría baja si alguna de sus dimensiones de seguridad alcanza el nivel bajo y ninguna alcanza un nivel superior.

Por su parte, la Orden de 28 de marzo de 2017, del Consejero de Hacienda y Administración Pública establece la política de seguridad de la información en la Administración Regional y fija el reparto de funciones y responsabilidades en materia de seguridad de la información entre los distintos órganos y unidades.

Así, su artículo 12.1 determina quién es el responsable de la información, que lo será, para cada sistema de información, el titular del órgano administrativo con competencia suficiente para decidir sobre la finalidad, contenido, uso y tratamiento de la información contenida en aquel.

Al mencionado responsable de la información, como señala el artículo 12 en su punto 2, le corresponde determinar, dentro del marco establecido en el Anexo I del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad, los niveles de seguridad de la información tratada.

A tales efectos, fijará los niveles de seguridad de la información tratada, valorando los impactos de los incidentes que afecten a la seguridad de la información, conforme con lo establecido en el artículo 44 del Real Decreto citado.

Por otra parte, el artículo 16.1 de la citada Orden de 28 de marzo de 2017, determina que el Responsable de Seguridad será designado por el titular del órgano con competencias en materia de informática entre personal adscrito a dicho órgano, y, en su punto 2 letra c), establece que le corresponde a dicho Responsable de Seguridad proponer al Responsable de la Información la determinación de los niveles de seguridad en cada dimensión de seguridad siempre que se solicite.

Visto el informe emitido en fecha XX XX de XXXX, por la Dirección General de Informática y Transformación Digital siguiendo los principios recogidos en el Real Decreto 3/2010, y, en especial, las dimensiones de seguridad en el recogidas, así como lo que establece en relación a la aplicación del principio de proporcionalidad a la categorización, teniendo en cuenta la importancia de la información, el servicio que se presta y el esfuerzo de seguridad requerido en función de los riesgos identificados.

Vista la propuesta de resolución formulada en fecha XX XX de XXXX por el Responsable de Seguridad de la Consejería de XXXXXXXXXXXXXXXXXXX

En virtud de todo lo expuesto anteriormente, y, como Responsable de la Información se dicta la presente

Resolución

Asignando las categorías de los sistemas de información que dan soporte a los procedimientos administrativos que se determinan y especifican en el anexo a la presente resolución

FIRMA DEL TITULAR DEL CENTRO DIRECTIVO

Anexo Resolución

Propuesta de categorización de Sistema de Información conforme al Esquema Nacional de Seguridad

El Real Decreto 3/2010, de 8 de enero, regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, y determina la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos.

El Esquema Nacional de Seguridad está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información, que deben de ser aplicados por las Administraciones públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias. Entre tales requisitos se encuentra la categorización en niveles de los distintos sistemas de información.

La Orden de 28 de marzo de 2017, del Consejero de Hacienda y Administración Pública por la que se establece la política de seguridad de la información en la Administración Regional, fija el reparto de funciones y responsabilidades en materia de seguridad de la información entre los distintos órganos y unidades.

El Responsable de la información es, para cada sistema de información, el titular del órgano administrativo con competencia suficiente para decidir sobre la finalidad, contenido, uso y tratamiento de la información contenida en aquél y le corresponde determinar, dentro del marco establecido en el Anexo I del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad, los niveles de seguridad de la información tratada.

Por su parte, el artículo 16 de la citada orden regula la figura del responsable de seguridad, que será designado por el titular del órgano con competencias en materia de informática entre el personal adscrito a dicho órgano. Entre sus funciones, recoge la letra e) de su apartado 2 proponer al Responsable de la Información la determinación de los niveles de seguridad en cada dimensión de seguridad siempre que se le solicite.

La presente propuesta se ha elaborado a la vista del informe emitido por la Dirección General de Informática y Transformación Digital siguiendo los principios recogidos en el Real Decreto 3/2010 y, en especial, teniendo en cuenta que la categorización debe realizarse teniendo en cuenta el principio de proporcionalidad entre la importancia de la información, el servicio que se presta y el esfuerzo de seguridad requerido en función de los riesgos identificados.

A la vista de lo anterior y de los datos recabados, procede realizar la siguiente categorización del sistema de información.

Número y Nombre del procedimiento	
Nombre, en su caso, de la aplicación de gestión	
Dimensión de seguridad más relevante	
Tipo de perjuicio	
Nivel del Perjuicio	
Consecuencias del perjuicio	
Determinación Categoría del Sistema de Información	

(Insertar tantos cuadros como procedimientos se categoricen).

FIRMA DEL RESPONSABLE DE SEGURIDAD

D.L. MU-395/1985 - ISSN: 1989-1474