3. Otras disposiciones

CONSEJERÍA DE HACIENDA, INDUSTRIA Y ENERGÍA

Resolución de 6 de julio de 2020, de la Agencia Tributaria de Andalucía, por la que se aprueba la Política de Seguridad de la Información de esta Agencia, así como la estructura organizativa responsable de su ejecución.

EXPOSICIÓN DE MOTIVOS

Desde la creación de la Agencia Tributaria de Andalucía (en adelante, la Agencia) la implantación de las Tecnologías de la Información y las Comunicaciones (en adelante, TIC) ha permitido un gran avance en la calidad del servicio ofrecido al ciudadano y en la lucha contra el fraude fiscal. Paralelamente, ha producido un incremento en la eficacia y eficiencia de toda la organización, así como del personal en el desempeño de sus funciones, con la consecuente mejora continua de sus resultados y del valor entregado a la sociedad andaluza en el cumplimiento de su misión.

La evolución de la sociedad, de las TIC y de la normativa aplicable ha generado cambios en el escenario en el que la Agencia presta sus servicios. En este sentido, deben garantizarse las condiciones para que esta evolución pueda ser asumida como oportunidad para ofrecer mejores servicios, cumpliendo en todo momento la normativa relacionada con la protección de datos y la seguridad en el uso de las TIC.

La presente resolución aprueba la Política de Seguridad de la Información de la Agencia, conforme al 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 (en adelante, ENS), creando la estructura organizativa recogida en el mismo para la Agencia. Y como entidad incluida en el ámbito de aplicación del Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía (en adelante, el decreto), deberá disponer formalmente de su propio documento de política de seguridad TIC, así como de las disposiciones de desarrollo que adecúen las directrices comunes de la Administración de la Junta de Andalucía a sus particularidades. Adicionalmente, la Política de Seguridad de la Información de la Agencia debe de ser conforme a la Orden de 21 de octubre de 2019, de la Consejería de Hacienda, Industria y Energía, por la que se establece la política de seguridad de la Consejería (en adelante, la orden), como entidad instrumental dependiente de la misma a las indicaciones del Comité de Seguridad TIC de la Consejería competente en materia de Hacienda, que tiene entre sus funciones, coordinar a los Comités de Seguridad TIC de las entidades instrumentales vinculadas o dependientes de la Consejería.

El modelo organizativo que se utiliza en la prestación de servicios digitales integrales e integrados a la Agencia, es el de Acuerdo de Nivel de Servicio (en adelante, ANS), a prestar a la Agencia, mediante el establecimiento de un acuerdo formal, escrito, suscrito entre la entonces Consejería de Hacienda y Administración Pública (en la actualidad la Consejería de Hacienda, Industria y Energía), a través de la Dirección General de Tecnologías para Hacienda y la Administración Electrónica (en la actualidad, la Dirección General de Transformación Digital y en adelante DGTD), y la Agencia, en el que se definen las bases del intercambio e interoperabilidad de los servicios a contemplar en el mismo. Todo ello, de conformidad con la Disposición Adicional Primera de la Orden de 18 de noviembre de 2010, de la Consejería de Hacienda y Administración Pública, por la que se definen las competencias de aplicación de la política informática de la Consejería en la Administración Tributaria de la Junta de Andalucía. Dicho acuerdo se incorpora como Anexo al contrato de gestión y al plan de acción anual de la Agencia, previstos en el

00174655

artículo 4 de la Ley 23/2007, de 18 de diciembre, por la que se crea la Agencia Tributaria de Andalucía y se aprueban medidas fiscales.

A tal efecto la Agencia Tributaria de Andalucía comunicará a su personal las normas de seguridad de la información y comunicaciones de la Consejería competente en materia de Hacienda procedentes de la Dirección General de Transformación Digital.

En el ámbito tributario, cobra especial importancia el artículo 95 de la Ley 58/2003, de 17 de diciembre, General Tributaria (en adelante, la LGT), por lo que se refiere a la adopción de las medidas necesarias para garantizar la confidencialidad de la información tributaria y su uso adecuado, lo cual es especialmente trascendente, por el carácter reservado de dicha información y la exclusiva utilización de ésta para la efectiva aplicación de los tributos o recursos cuya gestión tiene encomendada la Administración Tributaria. Este precepto debe relacionarse con lo dispuesto en el artículo 82 del Reglamento General de las actuaciones y los procedimientos de gestión e inspección tributaria y desarrollo de las normas comunes de los procedimientos de aplicación de los tributos, aprobado mediante Real Decreto 1065/2007, de 27 de julio, de acuerdo con el cual «en la utilización de técnicas y medios electrónicos, informáticos o telemáticos deberá respetarse el derecho a la protección de datos de carácter personal». En este sentido, se pronuncian tanto 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 (en adelante, el RGPD) como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, la LOPDPGDD).

La citada Orden de 18 de noviembre de 2010, regula en su artículo 12 el tratamiento de la información tributaria, señalando que se ajustará a la normativa sobre protección de datos y que la Dirección de la Agencia acordará las operaciones o procedimientos de tratamiento de la información contenida en los ficheros de los que la Agencia sea responsable y que la entonces Dirección General de Tecnologías para Hacienda y la Administración Electrónica realizará por cuenta de ésta. Además, para la cesión de datos de carácter personal se remite a lo dispuesto en el artículo 95 de la LGT y en su normativa de desarrollo, indicando, que, en su caso, dicha información será suministrada mediante la utilización de medios informáticos o telemáticos, puestos a disposición por la citada Dirección General, en cumplimiento de lo dispuesto en el artículo 96.2 de la LGT.

En la elaboración de esta resolución se han seguido también las directrices del Centro Criptológico Nacional, concretamente de la Guía CCN-STIC-801 sobre responsabilidades y funciones en el ENS al que se refiere el artículo 156.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, para establecer la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

La presente resolución se ajusta al ordenamiento jurídico, nacional y de la Unión Europea, como documento que se integra en un marco normativo estable, que persigue claridad, transparencia y certidumbre en la política de seguridad de la información de la Agencia Tributaria de Andalucía. De ahí que se incorpore en su parte final una recopilación normativa.

En virtud de lo expuesto, esta Presidencia de la Agencia, de conformidad con lo establecido en el artículo 11 de la Ley 23/2007, de 18 de diciembre, por la que se crea la Agencia Tributaria de Andalucía y se aprueban medidas fiscales, en el artículo 12 del Estatuto de la Agencia, aprobado por Decreto 4/2012, de 17 de enero, en el artículo 10 del Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía, y en el artículo 14 de la Orden de 21 de octubre de 2019, por la que se establece la política de seguridad de la información de la Consejería de Hacienda, Industria y Energía, a propuesta de la Dirección de la Agencia Tributaria de Andalucía,

00174655

R E S U E L V O

Primero. Aprobación de la Política de Seguridad de la Información de la Agencia Tributaria de Andalucía.

Se aprueba la Política de Seguridad de la Información de la Agencia Tributaria de Andalucía que se incorpora como anexo «Documento de Política de Seguridad TIC» de esta resolución.

Segundo. Ámbito de aplicación.

1. La Resolución será de aplicación a:

a) Los órganos y unidades centrales y territoriales de la Agencia, en todos sus sistemas de información, y al personal destinado en dichos órganos y unidades.

b) El personal de otros organismos o entidades que, en virtud de norma jurídica, acuerdo o convenio, realicen tratamientos por encargo de la Agencia o tengan acceso a los sistemas de información de la Consejería competente en materia de Hacienda, puestos a disposición de la Agencia.

2. La resolución se aplicará en el marco del ANS y del contrato de gestión de la Agencia, e incluirá las infraestructuras de soporte para la actividad relativa a las tecnologías de la información y comunicación de la Agencia, servidores, centro de respaldo y almacenamiento, entorno de virtualización, gestión de portales, licencias y las necesarias medidas de seguridad, con las que se asegura el funcionamiento y custodia de la información derivada de la gestión tributaria, aprovechando las economías de escala de la integración en el conjunto de la Consejería competente en materia de Hacienda.

Tercero. Finalidad de la Política de Seguridad de la Información.

La finalidad de la Política de Seguridad de la Información es la creación de las condiciones necesarias de confianza a través de medidas para garantizar la seguridad de los sistemas de información, los datos, las comunicaciones y los servicios electrónicos, que permitan a los ciudadanos ejercer sus derechos y cumplir con sus deberes, proporcionando a la Agencia un instrumento para la prestación de los servicios ofrecidos a la ciudadanía y aquellos destinados a la lucha contra el fraude fiscal, con la adecuada calidad y seguridad.

Cuarto. Política de gestión documental.

La información tratada por la Agencia, cualquiera que sea su soporte, se ajustará a lo dispuesto en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, en el Acuerdo de 1 de agosto de 2017, del Consejo de Gobierno, por el que se aprueba la política de gestión de documentos electrónicos de la Junta de Andalucía, y en la Ley 7/2011, de 3 de noviembre, de Documentos, Archivos y Patrimonio Documental de Andalucía, en relación con la información que sea susceptible de integrar el patrimonio documental.

Quinto. No incremento del gasto público.

La aplicación de esta resolución no conllevará incremento del gasto público para la Agencia, en atención a la estructura organizativa y competencias de la Consejería competente en materia de Hacienda, y a lo dispuesto en la Orden de 21 de octubre de 2019, todo ello sin perjuicio de las actuaciones en materia de seguridad que se llevan a cabo en el marco del ANS por la DGTD y cuyo coste se imputa a la Agencia.

Sexto. Efectos.

Esta resolución producirá efectos el día siguiente al de su publicación en el Boletín Oficial de la Junta de Andalucía.

Sevilla, 6 de julio de 2020.- El Presidente, Jorge Ramírez López.

00174655

A N E X O

«Documento de Política de Seguridad TIC»

I. Política de Seguridad de la Información.

1. La presente resolución constituye el «Documento de Política de Seguridad TIC» de la Agencia Tributaria de Andalucía, en cumplimiento de lo establecido en el artículo 10 del Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía y tiene por objeto definir y regular la política de seguridad de la información de la Agencia, que ha de aplicar en el tratamiento de la información, así como de los activos de tecnologías de la información y comunicaciones de su titularidad, o cuya gestión tenga encomendada.

2. La Política de Seguridad de la Información:

a) Identifica responsabilidades y establece principios y directrices para una protección apropiada y consistente de los servicios y activos de información gestionados por medio de las Tecnologías de la Información y de las Comunicaciones.

b) Es el instrumento en que se apoya la Agencia para alcanzar sus objetivos utilizando de forma segura los sistemas de información y las comunicaciones. La seguridad y la protección de datos de carácter personal, concebidas como proceso integral, comprenden todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información y las comunicaciones, y debe entenderse no como un producto, sino como un continuo proceso de adaptación y mejora, que debe ser controlado, gestionado y monitorizado, implantando la cultura de la seguridad en la Agencia.

c) Pretende dar soporte al desarrollo, coordinación y racionalización de la normativa específica y a la actualización de los conceptos según la evolución de las TIC, el entorno social y las disposiciones legales y reglamentarias, para alcanzar de esta forma un conjunto normativo equilibrado y completo.

d) Afectará a la información tratada por medios electrónicos que la Agencia gestione en el ámbito de sus competencias, así como aquella que sea tratada por encargo de otros organismos o entidades en virtud de norma jurídica, acuerdo o convenio.

II. Definiciones, estándares y objetivos de la política de seguridad TIC.

A los efectos previstos en esta resolución serán de aplicación los artículos 2 y 4 del decreto.

III. Principios de la política de seguridad TIC.

1. Principios básicos.

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información, siendo de aplicación a tal efecto los establecidos en el artículo 4 del Real Decreto 3/2010, de 8 de enero, así como los establecidos en el artículo 5 del decreto.

2. Principios particulares y responsabilidades específicas.

Las directrices fundamentales de seguridad se concretan en un conjunto de principios particulares y responsabilidades específicas, que se configuran como objetivos instrumentales que garantizan el cumplimiento de los principios básicos de la Política de Seguridad de la Información y que inspiran las actuaciones de la Agencia, en el marco del ANS, en dicha materia. Se establecen los siguientes:

a) Protección de datos de carácter personal: La Agencia adoptará las medidas técnicas y organizativas destinadas a garantizar el nivel de seguridad exigido por la normativa vigente en relación con el tratamiento de los datos de carácter personal.

b) Gestión de activos de información: Los activos de información de la Agencia se encontrarán inventariados, categorizados y estarán asociados a un responsable.

00174655

c) Seguridad ligada a las personas: La Agencia implantará los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.

d) Seguridad física: Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

e) Seguridad en la gestión de comunicaciones y operaciones: La Agencia establecerá los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las TIC. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.

f) Control de acceso: La Agencia limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.

g) Adquisición, desarrollo y mantenimiento de los sistemas de información: La Agencia contemplará los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.

h) Gestión de los incidentes de seguridad: La Agencia implantará los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.

i) Gestión de la continuidad: La Agencia implantará los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo a las necesidades de nivel de servicio de sus usuarios.

j) Cumplimiento: La Agencia adoptará las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

IV. Misión y estructura normativa.

El artículo 181 del Estatuto de Autonomía para Andalucía establece que la misión de la Agencia ayudar a hacer efectivo el deber de contribuir al sostenimiento de los gastos públicos de acuerdo con los principios consagrados en el artículo 31 de la Constitución Española, luchando contra el fraude fiscal y velando especialmente por la efectiva aplicación de los recursos a su cargo.

El marco normativo en el que la Agencia desarrolla sus actividades, establecido, esencialmente, por la Ley 23/2007, de 18 de diciembre, por la que se crea la Agencia Tributaria de Andalucía y se aprueban medidas fiscales, y su Estatuto, aprobado por Decreto 4/2012, de 17 de enero, concreta sus funciones y competencias, definiendo los principios en que se basa su actuación. En el desarrollo de sus actividades de aplicación de los tributos, la Agencia actuará de conformidad con el sistema de fuentes del ordenamiento tributario al que se refieren los artículos 5.3 y 7 de la Ley 58/2003, de 17 de diciembre, General Tributaria.

En cuanto a la estructura normativa sobre seguridad de la información de obligado cumplimiento, se desarrolla en tres niveles relacionados jerárquicamente.

Esta estructura jerárquica permite adaptar con eficiencia los niveles normativos inferiores a los cambios en los entornos operativos de la Agencia, sin necesidad de revisar su estrategia de seguridad.

00174655

El personal de la Agencia tendrá la obligación de conocer y cumplir, además de la Política de Seguridad de la Información, todas las Normas y Procedimientos de Seguridad de la Información que puedan afectar a sus funciones.

Son niveles normativos relacionados jerárquicamente:

a) Primer nivel normativo: Política de Seguridad de la Información.

Constituye el primer nivel normativo la Política de Seguridad de la Información, recogida en el presente documento y aprobada por Resolución de la Presidencia de la Agencia.

En el ámbito de sus funciones, el Comité de Seguridad TIC de la Agencia propondrá a la Presidencia de la Agencia las medidas que considere necesarias para el desarrollo o adecuación de la Política de Seguridad de la Información.

b) Segundo nivel normativo: Normas de Seguridad de la Información.

El segundo nivel normativo desarrolla la Política de Seguridad de la Información mediante normas específicas que abarcan un área o aspecto determinado de la seguridad de la información. Las Normas de Seguridad de la Información desarrollarán, al menos, los aspectos recogidos en los principios particulares y responsabilidades específicas de la referida Política de Seguridad de la Información.

Las Normas de Seguridad de la Información tienen aplicabilidad en todo el ámbito de la Agencia, siendo el órgano responsable de su preparación y aprobación el Comité de Seguridad TIC de la Agencia, siempre que la atribución de competencias del Comité lo permitan.

c) Tercer nivel normativo: Procedimientos de Seguridad de la Información.

El tercer nivel normativo está constituido por los Procedimientos de Seguridad de la Información, instrucciones de carácter técnico o procedimental que se deben observar en tareas o actividades relacionadas con la seguridad de la información y la protección de la información y de los servicios. Se aplicarán a un ámbito específico o a un sistema determinado, dependiendo del aspecto tratado.

Todos estos niveles prestarán especial atención a las exigencias derivadas del ENS. Debido al carácter personal y reservado de la información manejada y a los servicios puestos a disposición de los ciudadanos en el ámbito de la Administración Electrónica, la Agencia desarrolla sus actividades de acuerdo con las normas vigentes en dichas materias, entre las que cabe destacar, 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 (RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDPGDD).

V. Organización de la seguridad.

1. La seguridad deberá comprometer a todos los miembros de la organización, deberá de identificar a unos claros responsables de velar por su cumplimiento y ser conocida por todos los miembros de la organización administrativa. La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.

2. La Agencia, como entidad dependiente de la Consejería de Hacienda, Industria y Energía, procede a aprobar su política de seguridad de la información de forma coherente con la política de seguridad de la información de la Consejería (artículo 10.3 del decreto, y artículo 14.1 de la orden) y bajo el modelo de relación de ANS. A tal efecto, ambos Comités de Seguridad TIC articularán mecanismos de colaboración y coordinación necesarios de acuerdo con el artículo 10.5 del decreto.

3. De acuerdo con el ENS, el decreto y la orden la estructura organizativa de la seguridad de la información de la Agencia Tributaria de Andalucía es la siguiente:

a) Comité de Seguridad TIC.

b) Responsable de Seguridad TIC.

00174655

c) Responsable de la Información.
d) Responsables del Servicio.
e) Responsable del Sistema.
f) Grupo de trabajo permanente y comisión técnica de seguridad funcional

4. Creación y funcionamiento del Comité de Seguridad TIC.

En cumplimiento de lo establecido en el artículo 10 del decreto, se crea el Comité de Seguridad TIC de la Agencia, como órgano colegiado de dirección y seguimiento en materia de seguridad de los activos TIC de titularidad de aquélla o cuya gestión o explotación tenga encomendada.

El Comité de Seguridad TIC de la Agencia tendrá la siguiente composición, garantizándose, en la medida de lo posible, la representación paritaria de mujeres y hombres, conforme a lo establecido en el artículo 19.2 de la Ley 9/2007, de 22 de octubre.

a) Presidencia: la persona titular de la Presidencia de la Agencia.
b) Vicepresidencia: la persona titular de la Vicepresidencia de la Agencia.
c) Vocalías:
1.º La persona titular de la Dirección de la Agencia.
2.º La persona titular de Subdirección de Coordinación y Relaciones Institucionales
3.º Las personas titulares de los Departamentos de la Agencia.
4.º Las personas titulares de dos Gerencias Provinciales de la Agencia, designadas por la Presidencia de la Agencia, a propuesta de la Dirección de la Agencia.
5.º La persona designada Responsable de Seguridad de la Agencia.
d) Secretaría: la persona titular de Departamento de Organización y Gestión de Recursos.

En caso de vacante, ausencia, enfermedad u otras causas legales, la persona titular de la Presidencia será sustituida por la persona titular de la Vicepresidencia. Tanto la Vicepresidencia como las Vocalías y la Secretaría podrán designar a una persona que les sustituya, con carácter permanente y aplicando un criterio de paridad entre mujeres y hombres, de entre personal funcionario a su servicio que ocupen puestos de trabajo de nivel 28 o superior, con la excepción de la Secretaría cuyo suplente podrá ocupar puestos de nivel inferior, sin perjuicio de que posteriormente pueda designarse a otro suplente. Dicha designación será comunicada a la Secretaría.

Quien ostente la condición de Delegado de Protección de Datos asistirá en calidad de asesor a las reuniones del Comité de Seguridad TIC. El Comité se reunirá con carácter ordinario dos veces al año y, con carácter extraordinario, cuando así lo acuerde la Presidencia de la Agencia. También podrá celebrar reuniones extraordinarias, adicionales a las ordinarias, si se produjeran incidentes de seguridad graves o se produjeran conflictos que pudieran afectar gravemente a los servicios prestados por la Agencia. Todas las reuniones se realizarán previa convocatoria y de las mismas se levantará acta.

El Comité podrá convocar, a través de la Presidencia por iniciativa propia o a propuesta de alguno de sus miembros, y cuando el tratamiento de determinados temas específicos lo requiera, a personal técnico de la organización a los efectos de recibir asesoramiento especializado.

El Comité designará entre sus miembros a personas que den respuesta a incidentes TIC en el ámbito de la Agencia, cuya función será tanto la comunicación o reporte a los usuarios potencialmente afectados, a los órganos de gestión y responsables de los servicios de los incidentes advertidos como la adopción de medidas urgentes para contener el problema, evitar que crezca dentro de la organización e impedir que se transmita a otras organizaciones.

5. Funciones del del Comité de Seguridad TIC.

Son funciones del Comité:

a) La definición, aprobación y seguimiento de los objetivos, iniciativas y planes estratégicos en seguridad TIC en la Agencia.

00174655

b) Velar por la disponibilidad de los recursos necesarios para desarrollar las iniciativas y planes estratégicos y, a tal fin, proponer a la Comisión de Seguridad TIC de la Consejería competente en materia de Hacienda la adquisición de productos y servicios corporativos de seguridad TIC, en aquellos supuestos para los que se determine su conveniencia por criterios de oportunidad y eficacia.

c) Elevación de propuestas de revisión de la Política de Seguridad de la Información para su aprobación por parte de la Presidencia de la Agencia.

d) Establecimiento de directrices comunes y supervisión del cumplimiento de la Política de Seguridad de la Información de la Agencia, por parte de los órganos y unidades centrales y territoriales de la Agencia y otros organismos o entidades que en virtud de norma, acuerdo o convenio tengan acceso a los sistemas de información de la Consejería competente en materia de Hacienda, puestos a disposición de la Agencia.

e) Supervisión del nivel de riesgo y toma de decisiones, en coordinación con el responsable del servicio, según el artículo 10 del ENS, en la respuesta a incidentes de seguridad que afecten a los activos TIC puestos a disposición de la Agencia.

f) Promoción de la educación, entrenamiento y concienciación sobre las medidas legales y organizativas relativas a la Seguridad TIC entre el personal de la Agencia y el personal dependiente de otros encargados del tratamiento.

g) La adopción de decisiones en caso de conflicto entre los diferentes responsables que componen la estructura organizativa de la Política de Seguridad de la Información de la Agencia.

h) Atender a las indicaciones del Comité de Seguridad TIC de la Consejería competente en materia de Hacienda, que tiene entre sus funciones, el coordinar a los Comités de Seguridad TIC de las entidades instrumentales vinculadas o dependientes de la Consejería, artículo 6 de la Orden de 21 de octubre de 2019, de la Consejería de Hacienda, Industria y Energía por la que se establece la política de seguridad de la Consejería (en adelante, la orden).

El Comité aprobará, por mayoría simple de sus miembros, sus propias reglas de organización, funcionamiento y adopción de acuerdos.

6. Responsable de Seguridad TIC.

El Comité de Seguridad TIC de la Agencia nombrará al Responsable de Seguridad TIC de la misma entre personas que ostenten como mínimo nivel de Jefe de Servicio, debiéndose cumplir, además, el principio de función diferenciada respecto a la responsabilidad sobre la prestación de los servicios.

Corresponde al Responsable de Seguridad TIC adoptar las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los Responsables de la Información y de los Servicios.

El Responsable de Seguridad TIC será jerárquicamente independiente del Responsable del Sistema. En caso de servicios externalizados, corresponderá la responsabilidad última a la entidad del Sector Público destinataria de los servicios, aun cuando la responsabilidad inmediata pueda corresponder, por contrato, convenio, encomienda, u otro instrumento similar, a la organización prestataria del servicio.

El Responsable de Seguridad TIC de la Agencia, en el ámbito de su competencia y a los efectos de las atribuciones del artículo 11 del decreto, operará conjuntamente con la Unidad de Seguridad TIC de la Consejería competente en materia de Hacienda, conforme al ANS.

7. Responsable de la Información.

El titular de la Dirección de la Agencia tendrá la condición de Responsable de la Información y con las funciones, según el ENS, para toda información sobre la que tenga capacidad para decidir sobre su finalidad, contenido y uso.

8. Responsables del Servicio.

A propuesta del titular de la Dirección de la Agencia se designarán, por el Comité de Seguridad TIC, responsables del servicio de acuerdo con la estructura territorial y

00174655

las áreas funcionales de la Agencia, con las funciones, según el ENS, en atención a sus características y requisitos.

9. Responsable del Sistema.

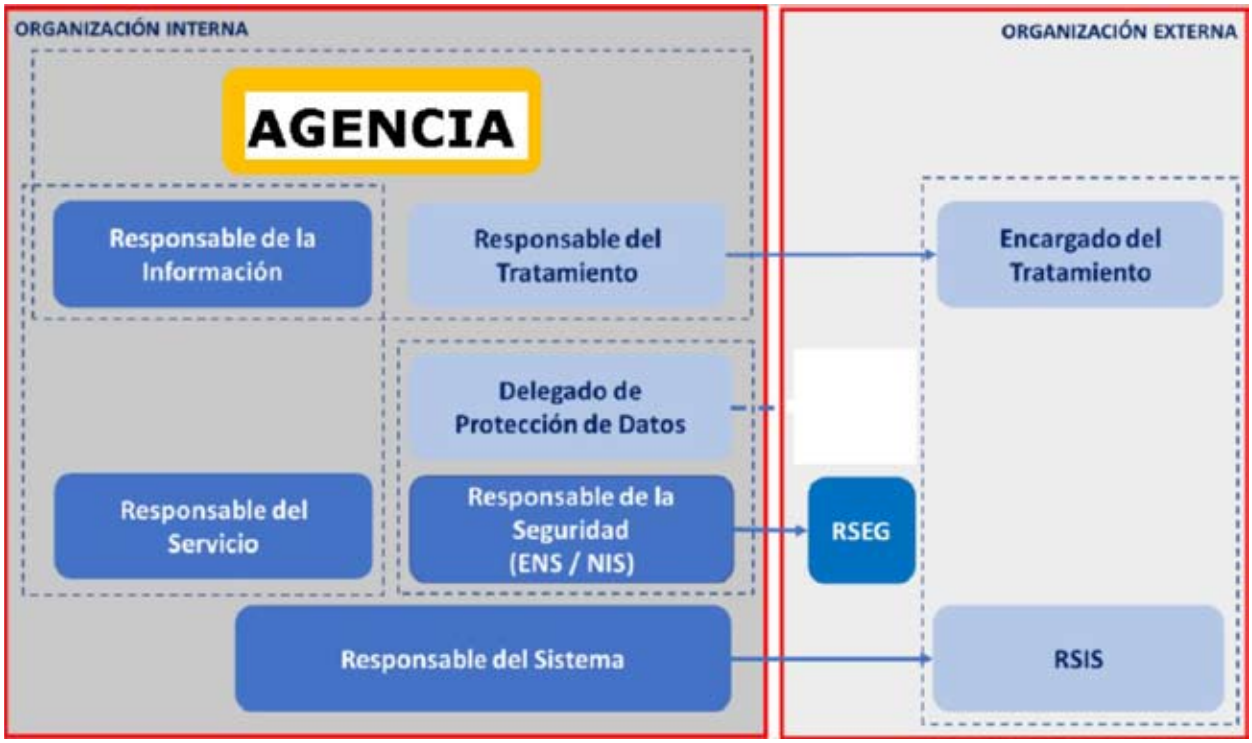
El titular de la Dirección de la Agencia, a propuesta del titular del Departamento competente en materia de sistemas de la información, designará al Responsable del Sistema, de entre el personal con rango de jefe de servicio de dicho Departamento.

Corresponderá al Responsable del Sistema las funciones que le asigna el ENS, así como la operación del sistema de información, atendiendo a las medidas de seguridad determinadas por el Responsable de Seguridad.

Su responsabilidad puede extenderse al ámbito interno de la organización (utilización de sistemas propios) o estar compartimentada entre una responsabilidad mediata (de la propia organización) y una responsabilidad inmediata (de terceros, públicos o privados), cuando los sistemas de información se encuentran externalizados.

10. Esquema conceptual de la Seguridad de la Información y la Protección de Datos.

De acuerdo con la Guía CCN-STIC-801 sobre responsabilidades y funciones en el ENS, la ubicación o posibles ubicaciones de las figuras mencionadas, independientemente de su posición concreta en la Agencia es la siguiente, de acuerdo con el ANS.



De acuerdo con la citada GUIA, la responsabilidad máxima en materia de seguridad de la información ENS y protección de datos corresponde a la persona titular de la Dirección de la Agencia que, generalmente, personificará la figura del Responsable del Tratamiento del RGPD.

En la operativa de la Agencia para el ámbito de aplicación del ENS y del RGPD participan terceros externos a la propia organización (públicos o privados). Por este motivo, en la figura aparecen los roles correspondientes a la organización interna y también aquellos otros que pudieran ubicarse en organizaciones externas.

En la Agencia, dado el modelo de relación tecnológica de la Agencia con la Consejería competente en materia de Hacienda que establece el ANS, coincidirán el Delegado de

00174655

Protección de Datos con el Responsable de la Seguridad del ENS. Así lo prevé la AEPD para aquellas organizaciones que, por su tamaño y recursos, no pudieran separar ambas figuras, en las que sería admisible la designación como delegado de protección de datos de la persona que ejerza las funciones de responsable de seguridad del ENS, siempre que en ésta última concurran los requisitos de formación y capacitación previstos en el RGPD.

El Esquema Nacional de Seguridad diferencia tres bloques de responsabilidad:

1. La responsabilidad legal y la especificación de las necesidades o requisitos, que corresponde a la Presidencia de la Agencia y a los responsables del tratamiento, de la información y del servicio.
2. La supervisión, que corresponde al Responsable de la Seguridad y al Delegado de Protección de Datos, en sus respectivos ámbitos.
3. La operación del sistema de información, que corresponde al Responsable del Sistema.

11. Grupo de trabajo permanente y comisión técnica de seguridad funcional.

Para dotar de una mayor operatividad a la política de seguridad se crea un grupo de trabajo permanente y una técnica de seguridad funcional.

Primero. Grupo de trabajo permanente.

Uno. Composición.

El grupo de trabajo permanente estará integrado por los siguientes participantes:

a) Responsable de la Información

b) Responsable de Seguridad

c) Responsable del Sistema

d) Responsable funcional de servicios, tanto a nivel territorial como central, relacionados con el uso de la información. En representación de los responsables funcionales de cada uno de los servicios territoriales y centrales la Dirección de la Agencia designará dos funcionarios, uno por nivel territorial, con nivel 28.

Dos. Funciones.

El grupo de trabajo permanente tendrá, entre otras funciones, las siguientes:

a) Elevar, a través de la Dirección de la Agencia, al Comité de Seguridad TIC una propuesta de plan anual de actuaciones a realizar en materia de Seguridad. En esta propuesta se diseñará la estrategia de seguridad TIC y se concretarán los objetivos, actividades e indicadores para la evaluación del grado de consecución de los objetivos previstos.

b) Elaborar un informe anual de las actividades realizadas por la Agencia en materia de seguridad TIC.

c) Elaboración de propuestas de normas, directrices, criterios, recomendaciones sobre procedimientos de Seguridad de la Información e instrucciones de carácter técnico o procedimental que se deben observar en tareas o actividades relacionadas con la seguridad de la información y la protección de la información y de los servicios en materia de seguridad para reducir riesgos para su aprobación por el Comité de Seguridad TIC

d) Elaborar propuestas para mejorar y reforzar los sistemas de seguridad y control.

e) Elaboración de protocolos de actuación en caso de incidente de seguridad

f) Detección de necesidades formativas en materia de seguridad.

g) Diseño de campañas de concienciación entre el personal.

h) Elaboración de campañas de control de uso de la información

i) Cualquier otra función que le atribuya el Comité de Seguridad TIC con arreglo a la política de seguridad de la Agencia.

Tres. Organización y funcionamiento.

El Grupo de trabajo permanente aprobará, por mayoría simple de sus miembros, sus propias reglas de organización, funcionamiento y adopción de acuerdos.

Segundo. Comisión técnica de seguridad funcional.

Uno. Composición.

00174655

La Comisión técnica de seguridad funcional estará integrada por:

a) Responsable funcional de servicios, tanto a nivel territorial como central, relacionados con el uso de la información. En representación de los responsables funcionales de cada uno de los servicios territoriales y centrales la Dirección de la Agencia designará dos funcionarios, uno por nivel territorial, con nivel 28.

b) Un funcionario de cada una de las siguientes áreas de trabajo:

• Organización y gestión de recursos, que comprende los siguientes servicios:
  i. Personal, gestión económica, control interno y asistencia jurídica.
• Aplicación de los tributos, que comprende los siguientes servicios:
  i. Información y asistencia, gestión tributaria, inspección, valoración y recaudación.
• Innovación y análisis de la información:
  i. Informática, procedimiento y estadística.

Dos. Funciones.

a) Establecer y mantener actualizados de forma permanente los criterios y directrices generales sobre seguridad aprobados por el Comité de Seguridad TIC.

b) Detectar e inventariar las áreas y puntos de riesgo más relevantes en el desarrollo de las funciones y competencias de la Agencia.

c) Analizar y evaluar, para cada una de las áreas de riesgo delimitadas, las deficiencias y debilidades de control existentes. A tales efectos, se considerarán los aspectos legales, organizativos y procedimentales, así como los derivados de los medios personales y de las aplicaciones y sistemas informáticos

d) Analizar y evaluar los riesgos de funcionamiento de los servicios a fin de establecer las correspondientes medidas preventivas.

Tres. Organización y funcionamiento.

La Comisión técnica de seguridad aprobará, por mayoría simple de sus miembros, sus propias reglas de organización, funcionamiento y adopción de acuerdos.

VI. Organización en materia de protección de datos de carácter personal.

1. De acuerdo con la normativa aplicable en materia protección de datos de carácter personal, en el ámbito de la Agencia, y conforme al ANS, se establecen las siguientes funciones y responsabilidades:

a) La Dirección de la Agencia asume las funciones de responsable del tratamiento en virtud de lo establecido en el artículo 4, apartado 7 y en el artículo 24 del RGPD.

b) La Dirección General de Transformación Digital, dado el modelo de relación tecnológica de la Agencia con la Consejería competente en materia de Hacienda que establece el ANS, asume las funciones de encargado del tratamiento, en virtud de lo establecido en el artículo 4, (apartado 8), y en el artículo 28 del RGPD.

c) Las personas titulares de los Registros de la Propiedad a las que la Resolución del Consejo Rector de 19 de diciembre de 2019 de la Agencia delega determinadas funciones y competencias en el Impuesto sobre Transmisiones Patrimoniales y Actos Jurídicos Documentados y en el Impuesto sobre Sucesiones y Donaciones, como encargadas del tratamiento de los datos de carácter personal, en el ámbito de las funciones atribuidas a éstas por la citada resolución.

La información será accesible a través los sistemas de información y las soluciones tecnológicas puestas a su disposición por la Agencia.

Serán encargados del tratamiento, con las obligaciones inherentes, las personas titulares de las oficinas y todo su personal.

d) Los organismos o entidades que traten datos por cuenta del responsable del tratamiento, en virtud de norma, acuerdo o convenio, que asumen las funciones de encargados del tratamiento, en virtud de lo establecido en el artículo 4, apartado 8, y en el artículo 28 del RGPD.

e) La persona Delegada de Protección de Datos en la Agencia, con las funciones de supervisión y asesoramiento establecidas en el artículo 39 del RGPD.

00174655

2. En lo referente a los datos de carácter personal que sean objeto de tratamiento por parte de la Agencia o de los encargados (o subencargados) del tratamiento por cuenta de ésta, se adoptarán las medidas técnicas y organizativas que correspondan, según lo expresado en los artículos 24 y 32 del RGPD y lo dispuesto expresamente en la ORDEN.

En caso de conflicto entre los diferentes actores, prevalecerá lo dispuesto en el instrumento jurídico de encargo y, en su defecto, las mayores exigencias derivadas de la protección de datos de carácter personal.

VII. Gestión de riesgos.

1. La gestión de riesgos debe realizarse de manera continua sobre los tratamientos y los sistemas de información, conforme a los principios de gestión de la seguridad basada en los riesgos y reevaluación periódica.

2. En el marco del ANS, el Comité de Seguridad TIC de la Agencia es responsable de los riesgos sobre la información y sobre los servicios y, por tanto, de aceptar los riesgos residuales calculados en los análisis que se lleven a cabo. La selección de las medidas de seguridad a aplicar será propuesta por la persona Responsable de Seguridad TIC al Comité de Seguridad TIC de la Agencia.

Igualmente, en el citado marco del ANS, el proceso de gestión de riesgos, que comprende las fases de categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, que deberán ser proporcionales a los riesgos y estar justificadas, deberá revisarse cada año por parte de la persona responsable de Seguridad TIC, que elevará un informe al Comité de Seguridad TIC.

3. El análisis de riesgos sobre protección de datos y sobre la seguridad TIC deberá realizarse una vez al año, cuando cambie la información, su tratamiento, los servicios prestados, cuando ocurra un incidente de seguridad y cuando se reporte una vulnerabilidad grave en el marco del ANS.

4. Por lo que se refiere a la Notificación de violaciones de la seguridad de los datos, se estará a lo dispuesto en el RGPD y en el ENS.

VIII. Auditorías de seguridad.

Al menos cada dos años, se realizará una auditoría de seguridad, que verifique el cumplimiento de los requerimientos del RGPD y su normativa de desarrollo, así como del ENS, para cada tratamiento y cada sistema de información, en el ámbito de la Agencia y del ANS. Estas auditorías se ajustarán a lo establecido en el ENS.

Los informes de auditoría serán elevados a las personas Responsables de la Información y del Sistema, a la persona Delegada de Protección de Datos y al Responsable de Seguridad TIC y serán analizados por esta última, que presentará sus conclusiones a las personas Responsables de la Información y del Sistema, para que adopten las medidas correctoras adecuadas.

Los resultados obtenidos determinarán las líneas de actuación a seguir y las posibles modificaciones a realizar sobre los controles y la normativa de seguridad.

IX. Formación, concienciación y obligaciones de los usuarios.

1. La Agencia desarrollará actividades específicas orientadas a la formación y concienciación de su personal en materia de seguridad de la información, así como a la difusión de su Política de Seguridad de la Información y su desarrollo normativo, en particular entre el personal de nueva incorporación.

A estos efectos, los planes anuales de formación de la Agencia incluirán actividades formativas específicas sobre esta materia.

2. La Agencia promoverá una cultura de la seguridad de la información alineada con la Política de Seguridad de la Información entre aquellas organizaciones, entidades y usuarios externos que tengan acceso, en virtud de norma, acuerdo o convenio, a los sistemas de información de la Consejería competente en materia de Hacienda, puestos a

00174655

disposición de la Agencia para el ejercicio de sus funciones y competencias y en el marco del ANS.

Obligaciones de los usuarios de los sistemas de información:

a) Conocer la Política de Seguridad de la Información de la Agencia. Para ello, se dispondrán los medios necesarios para su difusión, prestando especial atención a las nuevas incorporaciones de personal.

b) Conocer el manual de comportamiento de los empleados públicos en el uso de los sistemas informáticos y redes de comunicaciones de la Administración de la Junta de Andalucía, aprobado por Resolución de 27 de septiembre de 2004, de la Secretaría General para la Administración Pública.

c) Atenderán a una acción de concienciación en materia de seguridad relativa a las TIC en la Agencia.

d) Las personas con responsabilidad en la operación o administración de sistemas, recibirán por parte del responsable del servicio formación para el manejo seguro de los sistemas en la medida que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir su trabajo tanto si es su primera asignación como si se trata de un cambio de puesto o funciones.

X. Actualización y revisión periódica.

La Política de Seguridad de la Información de la Agencia deberá mantenerse actualizada permanentemente para adecuarla al progreso de los servicios de la Administración Electrónica, a la evolución tecnológica, al desarrollo de la sociedad de la información, a los estándares internacionales de seguridad, así como a los cambios normativos en la Junta de Andalucía. A tal efecto, el Decreto 622/2019, de 27 de diciembre, de administración electrónica, simplificación de procedimientos y racionalización organizativa de la Junta de Andalucía y la singularidad de la materia tributaria concretamente la disposición adicional quinta y disposición transitoria cuarta.

Las propuestas de revisión de la Política de Seguridad de la Información se elaborarán por el Comité de Seguridad TIC de la Agencia, que con tal objetivo revisará regularmente la oportunidad, idoneidad, completitud y precisión de lo establecido en la Política de Seguridad de la Información vigente.

00174655