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.

Texto refundido tras Decreto 70/2017, de 6 de junio, de modificación

Índice

Los avances tecnológicos en los campos de la informática y las telecomunicaciones, de la sociedad de la información, son ya un hecho consolidado, que afecta no sólo a la sociedad sino también a los poderes públicos. Son los poderes públicos los responsables de generar confianza en el uso por parte de la ciudadanía de los medios tecnológicos en sus relaciones con la Administración Pública. Y para conseguir esta confianza, los medios tecnológicos utilizados deben ser seguros, para ello se debe garantizar la confidencialidad, integridad y disponibilidad de los sistemas, de las comunicaciones y de los servicios telemáticos, permitiendo tanto a la ciudadanía como a las Administraciones Públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

El Estatuto de Autonomía para Andalucía, en su artículo 34, reconoce el derecho a acceder y usar las nuevas tecnologías y a participar activamente en la sociedad del conocimiento, la información y la comunicación, mediante los medios y recursos que la ley establezca. Asimismo, el artículo 58.1.2.º atribuye a la Comunidad Autónoma de Andalucía competencias exclusivas sobre el régimen de las nuevas tecnologías relacionadas con la Sociedad de la Información y del Conocimiento, en el marco de la legislación del Estado.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, señala entre sus fines el crear las condiciones de confianza en el uso de los medios electrónicos, estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos. Estos fines han sido desarrollados por 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.

Otra Ley estatal, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y sus normas de desarrollo aportan criterios para establecer la proporcionalidad entre las medidas de seguridad y la información a proteger.

La Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, señala en su artículo 45.5 que los documentos emitidos, cualquiera que sea su soporte, por medios electrónicos, informáticos o telemáticos por las Administraciones Públicas, o los que éstas emitan como copias de originales almacenados por estos mismos medios, gozarán de la validez y eficacia de documento original siempre que quede garantizada su autenticidad, integridad y conservación.

Por otro lado, en nuestra Comunidad Autónoma, la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía, señala en su artículo 7.2 que los principios que rigen las relaciones que mantenga la Administración de la Junta de Andalucía con la ciudadanía y con otras Administraciones Públicas a través de redes abiertas de telecomunicación son los de simplificación y agilización de trámites, libre acceso, accesibilidad universal y confidencialidad en el tratamiento de la información, y de seguridad y autenticidad en orden a la identificación de las partes y el objeto de la comunicación, para ello establece que estos sistemas

deben de cumplir con el requisito de existencia de medidas de seguridad que eviten la interceptación y alteración de las comunicaciones, así como los accesos no autorizados. En este mismo texto legal se abunda en materia de seguridad señalándose que los medios o soportes en que se almacenen los documentos electrónicos contarán con las medidas de seguridad que garanticen la integridad, protección y conservación de los documentos almacenados, así como la identificación de las personas usuarias y el control de acceso de los mismos.

En la elaboración de este Decreto se han tenido en cuenta las características técnicas y funcionales de la Red Corporativa de Telecomunicaciones de la Administración de la Junta de Andalucía, creada por el Acuerdo del Consejo de Gobierno de 2 de junio de 1998, y de los principales sistemas de información corporativos de las entidades que forman parte del ámbito de aplicación del presente Decreto.

Este Decreto establece el compromiso de la Administración de la Junta de Andalucía con la seguridad de los sistemas de la información, define los objetivos y criterios básicos para el tratamiento de la misma, sienta los pilares del marco normativo de seguridad de esta administración y la estructura organizativa y de gestión que velará por su cumplimiento.

Este compromiso de la Comunidad Autónoma de Andalucía con la seguridad de las tecnologías de la información y las comunicaciones ha quedado plasmado recientemente con la aprobación por el Consejo de Gobierno el 16 de noviembre de 2010, del Plan Director de Seguridad de los sistemas de información y telecomunicaciones de la Administración de la Junta de Andalucía (2010/2013). Este Plan contiene entre sus medidas el desarrollo y aprobación del marco normativo de seguridad de la Administración de la Junta de Andalucía, contemplando concretamente la aprobación de «un documento de política de seguridad, que ha de mostrar el compromiso expreso de la dirección con la gestión de la seguridad, sus objetivos y principios básicos, el marco de referencia común y la descripción de la estructura organizativa en la que se apoyará el gobierno de la seguridad en la Administración de la Junta de Andalucía».

Por otra parte, de acuerdo con el artículo 5 de la Ley 12/2007, de 26 de noviembre, para la promoción de la igualdad de género en Andalucía, este Decreto integra el principio de igualdad de género de forma transversal en su elaboración, garantizando con ello un impacto positivo en la igualdad de oportunidades entre mujeres y hombres.

La aplicación de las previsiones contenidas en este Decreto, no supondrá incremento del gasto público. Por tanto, los órganos y entidades afectadas deberán desarrollar las medidas derivadas de su cumplimiento ateniéndose a sus disponibilidades presupuestarias ordinarias, no dando lugar, en ningún caso, a planteamientos de necesidades adicionales de financiación.

La norma se estructura en cuatro capítulos, una disposición adicional y dos disposiciones finales.

En su virtud, a propuesta del Consejero de Economía, Innovación y Ciencia, conforme a lo establecido en el artículo 27.9 de la Ley 6/2006, de 24 de octubre, del Gobierno de la Comunidad Autónoma de Andalucía, y previa deliberación del Consejo de Gobierno en su reunión del día 11 de enero de 2011

DISPONGO

CAPÍTULO I. Disposiciones generales

Artículo 1. Objeto.

El presente Decreto tiene por objeto definir y regular la política de seguridad de las tecnologías de la información y comunicaciones de la Administración de la Junta de Andalucía, conformando, junto a las disposiciones y documentos técnicos que la desarrollen, el marco regulador de seguridad TIC.

Artículo 2. Definiciones.

A los efectos previstos en este Decreto, las definiciones han de ser entendidas en el sentido indicado en el Glosario de términos incluido como Anexo I.

Artículo 3. Ámbito de aplicación.

El Decreto será de aplicación a la Administración de la Junta de Andalucía y a sus entidades instrumentales, así como a los consorcios a los que se refiere el artículo 12.3 de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía.

Artículo 4. Objetivos de la política de seguridad de las tecnologías de la información y las comunicaciones.

La política de seguridad de las tecnologías de la información y comunicaciones de la Administración de la Junta de Andalucía, en adelante política de seguridad TIC de la Administración de la Junta de Andalucía, persigue la consecución de los siguientes objetivos:

a) Garantizar a toda la ciudadanía andaluza que sus datos serán gestionados de acuerdo a los estándares y buenas prácticas en seguridad TIC.

b) Aumentar el nivel de concienciación en materia de seguridad TIC de todas las entidades a las que es de aplicación el Decreto, garantizando que el personal a su servicio es consciente de sus obligaciones y responsabilidades.

c) Establecer las bases de un modelo integral de gestión de la seguridad TIC en la Administración de la Junta de Andalucía, que cubra en un ciclo continuo de mejora los aspectos técnicos, organizativos y procedimentales.

d) Garantizar el cumplimiento de la legislación vigente en materia de seguridad TIC.

CAPÍTULO II. Principios de seguridad TIC

Artículo 5. Principios de la política de seguridad TIC.

La política de seguridad TIC de la Administración de la Junta de Andalucía se desarrollará, con carácter general, de acuerdo a los siguientes principios:

a) Principio de confidencialidad: los activos TIC deberán ser accesibles únicamente para aquellas personas usuarias, órganos y entidades o procesos expresamente autorizados para ello, con respeto a las obligaciones de secreto y sigilo profesional.

b) Principio de integridad y calidad: se deberá garantizar el mantenimiento de la integridad y calidad de la información, así como de los procesos de tratamiento de la misma, estableciéndose los mecanismos para asegurar que los procesos de creación, tratamiento, almacenamiento y distribución de la información contribuyen a preservar su exactitud y corrección.

c) Principio de disponibilidad y continuidad: se garantizará un alto nivel de disponibilidad en los activos TIC y se dotarán de los planes y medidas necesarias para asegurar la continuidad de los servicios y la recuperación ante posibles contingencias graves.

d) Principio de gestión del riesgo: se deberá articular un proceso continuo de análisis y tratamiento de riesgos como mecanismo básico sobre el que debe descansar la gestión de la seguridad de los activos TIC.

e) Principio de proporcionalidad en coste: la implantación de medidas que mitiguen los riesgos de seguridad de los activos TIC deberá hacerse bajo un enfoque de proporcionalidad en los costes económicos y operativos.

f) Principio de concienciación y formación: se articularán iniciativas que permitan a las personas usuarias conocer sus deberes y obligaciones en cuanto al tratamiento seguro de la información se refiere. De igual forma, se fomentará la formación específica en materia de seguridad TIC de todas aquellas personas que gestionan y administran sistemas de información y telecomunicaciones.

g) Principio de prevención: se desarrollarán planes y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la seguridad TIC.

h) Principio de mejora continua: se revisará el grado de eficacia de los controles de seguridad TIC implantados, al objeto de adecuarlos a la constante evolución de los riesgos y del entorno tecnológico de la Administración de la Junta de Andalucía.

i) Principio de seguridad TIC en el ciclo de vida de los activos TIC: las especificaciones de seguridad se incluirán en todas las fases del ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

j) Principio de función diferenciada: la responsabilidad de la seguridad de los sistemas de tecnologías de la información y comunicaciones estará diferenciada de la responsabilidad sobre la prestación de los servicios.

CAPÍTULO III. Organización de la seguridad TIC

Artículo 6. Organización de la seguridad TIC.

1. La preservación de la seguridad TIC será considerada objetivo común de todas las personas al servicio de la Administración de la Junta de Andalucía, siendo éstas responsables del uso correcto de los recursos de tecnologías de la información y comunicaciones puestos a su disposición.

2. La organización de la seguridad TIC en la Administración de la Junta de Andalucía se conforma mediante la siguiente estructura:

a) Organización corporativa:

1º Comité de Seguridad TIC de la Junta de Andalucía y su Grupo de Respuesta a Incidentes.

2º Unidad de Seguridad TIC Corporativa.

3º Grupo de Personas Expertas en Seguridad TIC.

b) Organización en Consejerías:

1º Comité de Seguridad TIC.

2º Unidad de Seguridad TIC.

c) Organización en entidades vinculadas o dependientes:

1º Comité de Seguridad TIC.

2º Responsable de Seguridad TIC.

3. El modelo organizativo establecido en el apartado anterior tiene el carácter de mínimo, pudiendo cada Consejería y entidad incluida en el ámbito de aplicación del Decreto crear comités o perfiles con responsabilidad en seguridad adicionales para una mejor consecución de los objetivos y principios del Decreto, en el marco de lo establecido en el Real Decreto 3/2010, de 8 de enero.

Artículo 7. Comité de Seguridad TIC de la Junta de Andalucía.

1. Se crea en el seno de la Comisión Interdepartamental de la Sociedad de la Información de la Junta de Andalucía (CISI), como órgano colegiado de coordinación y gobierno en materia de seguridad en el ámbito de la Administración de la Junta de Andalucía, el Comité de Seguridad TIC de la Junta de Andalucía, al amparo de lo establecido en el artículo 7.7 del Decreto 166/2001, de 10 de julio, de coordinación de actuaciones para el desarrollo de la Sociedad de la Información.

2. El Comité estará formado por aquellas personas elegidas por la propia Comisión Interdepartamental de la Sociedad de la Información de la Junta de Andalucía entre las personas que la componen, debiendo tener representación de todas las Consejerías de la Administración de la Junta de Andalucía. Formará parte también del Comité la persona titular de la Dirección General competente en la coordinación de la evaluación de las necesidades de protección contra riesgos de intrusión en los edificios públicos de la Administración de la Junta de Andalucía. La presidencia recaerá en la persona titular del centro directivo de mayor rango con competencias en la coordinación y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones de la Administración de la Junta de Andalucía, y la secretaría recaerá en la persona titular del Servicio que tenga asignadas las funciones de la Unidad de Seguridad TIC corporativa.

3. Serán funciones propias del Comité:

a) Definición, aprobación y seguimiento de los objetivos, iniciativas y planes estratégicos en seguridad TIC.

b) Velar por la disponibilidad de los recursos necesarios para desarrollar las iniciativas y planes estratégicos definidos y proponer a la Unidad de Seguridad TIC Corporativa la realización de los procedimientos de compra centralizada de productos y servicios corporativos de seguridad TIC, en aquellos supuestos en que se determine su conveniencia en razón a criterios de oportunidad, eficacia y de economías de escala.

c) Elevación de propuestas de revisión del marco normativo de seguridad TIC al órgano competente para su reglamentaria tramitación.

d) Establecimiento de directrices comunes y supervisión del cumplimiento de la normativa en materia de seguridad TIC.

e) Supervisión del nivel de riesgo y toma de decisiones en la respuesta a incidentes de seguridad TIC que afecten a los activos TIC.

f) Definición y aprobación del modelo de relación con los Comités de Seguridad TIC de las Consejerías y entidades incluidas en el ámbito de aplicación del Decreto.

g) Promoción de la educación, entrenamiento y concienciación sobre las medidas legales y organizativas relativas a la Seguridad TIC entre el personal de la Administración Pública.

4. El Comité se reunirá al menos una vez por semestre y se regirá por este Decreto y por las normas sobre los órganos colegiados que contiene la Sección 1.ª del Capítulo II del Título IV de la Ley 9/2007, de 22 de octubre, así como por la normativa de carácter básico, establecida en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

5. El Comité nombrará un Grupo de Respuesta a Incidentes TIC cuya función será la toma urgente de decisiones en caso de contingencia grave que afecte a la seguridad de sistemas de información críticos de la Administración de la Junta de Andalucía.

Artículo 8. Unidad de Seguridad TIC Corporativa de la Junta de Andalucía.

1. La Dirección General competente en materia de coordinación y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones de la Administración de la Junta de Andalucía contará con

una Unidad de Seguridad TIC Corporativa, cuyas funciones se asignarán a una unidad administrativa con nivel orgánico mínimo de Servicio.

2. La Unidad de Seguridad TIC Corporativa tendrá las siguientes atribuciones:

a) Labores de soporte, asesoramiento e información al Comité de Seguridad TIC de la Junta de Andalucía y su Grupo de Respuesta a Incidentes, así como de ejecución de las decisiones y acuerdos adoptados.

b) Diseño y ejecución de los programas de actuación de carácter horizontal, así como la dirección de los proyectos y servicios corporativos de seguridad TIC.

c) Desarrollo, mantenimiento y supervisión del marco regulador de seguridad TIC.

d) Generación y supervisión de criterios y directrices corporativas de gestión de la seguridad TIC.

e) Recogida sistemática de información y supervisión del estado de las principales variables de seguridad TIC de la Administración de la Junta de Andalucía, mediante el reflejo, cuando proceda, de los datos referidos a personas desagregados por sexo

f) Coordinación y seguimiento de la actividad de las Unidades de seguridad TIC de las Consejerías.

g) Realización de los procedimientos de compra centralizada de productos y servicios corporativos de seguridad TIC a propuesta del Comité de Seguridad TIC en aquellos supuestos en que se determine su conveniencia en razón a criterios de oportunidad, eficacia y de economías de escala.

h) Realización de auditorías técnicas y de cumplimiento normativo, en aquellos supuestos en que se determine su conveniencia en razón a criterios de oportunidad, eficacia, eficiencia y de economías de escala.

i) Representación de la Administración de la Junta de Andalucía ante los foros y agentes de relevancia del sector.

j) Coordinación del Grupo de Personas Expertas en Seguridad TIC.

k) Y cuantas otras le sean encomendadas por la Dirección General competente en materia de coordinación y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones.

Artículo 9. Grupo de Personas Expertas en Seguridad TIC de la Junta de Andalucía.

1. Las personas que componen el Grupo de Personas Expertas en Seguridad TIC serán nombradas por la Dirección General competente en materia de coordinación y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones de la Administración de la Junta de Andalucía, a propuesta de las personas titulares de los centros directivos presentes en el Comité de Seguridad TIC. Estas personas serán personal de la Administración Pública de la Junta de Andalucía y podrán estar adscritas a cualquier Consejería o entidad incluidas en el ámbito de aplicación del presente Decreto.

2. El Grupo actuará como equipo técnico consultivo, mediante la redacción de informes y asesoramiento verbal, en la definición de los programas de actuación de carácter horizontal y se reunirá previa convocatoria de la persona responsable de la Unidad de Seguridad TIC Corporativa.

3. Las personas titulares de los centros directivos que forman parte del Comité de Seguridad TIC serán responsables de mantener actualizada su lista de personas expertas en el Grupo en el caso de producirse cambios en la organización institucional o ante cambios de puesto de trabajo u Organismo.

4. En la composición del Grupo de Personas Expertas en Seguridad TIC, ha de garantizarse, en la medida de lo posible, la representación equilibrada de mujeres y hombres, conforme a lo establecido en el artículo 19.2 de la Ley 9/2007, de 22 de octubre, y a la definición de representación equilibrada contenida en el artículo 3.3 de la Ley 12/2007, de 26 de noviembre, para la Promoción de la Igualdad de Género en Andalucía.

Artículo 10. Política y comité de seguridad TIC.

1. Sin perjuicio de las directrices establecidas en el marco regulador de seguridad TIC de la Administración de la Junta de Andalucía, cada Consejería y entidad incluida en el ámbito de aplicación del presente Decreto deberá disponer formalmente de su propio documento de política de seguridad TIC, así como de las disposiciones de desarrollo que adecuen, en su caso, las directrices comunes de la Administración de la Junta de Andalucía a sus particularidades. Asimismo, cada Consejería y entidad deberá contar con un Comité de Seguridad TIC, que no tendrá carácter colegiado y que actuará como órgano de dirección y seguimiento en materia de seguridad de los activos TIC de su titularidad o cuya gestión tenga encomendada.

2. El documento de política de seguridad TIC será aprobado por la persona titular de la Consejería o entidad correspondiente y se plasmará en los términos descritos en el Real Decreto 3/2010, de 8 de enero, debiendo hacer referencia y ser coherente con lo establecido en el documento de seguridad que exige el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, aprobado por el Real Decreto 1720/2007, de 21 de diciembre.

3. El documento de política de seguridad TIC de las Consejerías y sus documentos complementarios también serán de obligado cumplimiento para sus entidades vinculadas o dependientes.

4. El documento de política de seguridad TIC deberá recoger la composición, atribuciones, y funcionamiento del Comité de Seguridad TIC y del resto de perfiles con responsabilidad en seguridad, incluyendo, en su caso, los recogidos en el Real Decreto 3/2010, de 8 de enero, definiendo para cada uno de ellos, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.

5. Los Comités de Seguridad TIC de las Consejerías articularán los mecanismos de colaboración y coordinación necesarios con los de sus entidades vinculadas o dependientes.

6. Las atribuciones de los Comités de Seguridad TIC de las entidades vinculadas o dependientes podrán ser asumidas por los comités de dirección existentes en dichas entidades, lo cual deberá ser recogido expresamente en el correspondiente documento de política de seguridad TIC.

7. En la composición de estos comités ha de garantizarse, 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.

Artículo 11. Gestión de la seguridad TIC.

1. Cada Consejería contará con una Unidad de Seguridad TIC, garantizando el principio de función diferenciada recogido en el artículo 5.j), que ejerza las funciones de responsabilidad de seguridad TIC de la Consejería, debiendo ser nombrada por el Comité de Seguridad TIC de la misma. La Unidad de Seguridad TIC tendrá las siguientes atribuciones:

a) Labores de soporte, asesoramiento e información al Comité de Seguridad TIC de la Consejería, así como de ejecución de las decisiones y acuerdos adoptados por éste.

b) Diseño y ejecución de los programas de actuación propios de la Consejería, incluyendo, entre otros, planes directores de seguridad, proyectos de desarrollo normativo, auditorías de cumplimiento y planes de adecuación legal.

c) Definición, implantación y mantenimiento de los controles de carácter organizativo para la protección de los datos, aplicaciones y sistemas, así como la realización y mantenimiento de los análisis de riesgos de la Consejería.

d) Supervisión sistemática de los controles de carácter procedimental, operacional y medidas técnicas de protección de los datos, aplicaciones y sistemas de la Consejería.

e) Definición y supervisión de los criterios y requisitos técnicos de seguridad aplicados en las distintas fases del ciclo de vida de los soportes, sistemas y aplicaciones de la Consejería por parte de los Servicios o Departamentos responsables de la prestación de los servicios de tecnologías de la información y comunicaciones. Antes de la puesta en producción de nuevos sistemas de información o de evolutivos de los existentes, la Unidad de Seguridad TIC deberá evaluar los aspectos de seguridad y comunicar los posibles riesgos al centro o centros directivos responsables de la información y del servicio.

f) Definición y ejecución de los programas formativos y de concienciación relacionados con buenas prácticas de seguridad TIC en el ámbito de la Consejería, procurando promover, en el proceso de selección de las personas participantes en estos programas, la concurrencia de mujeres.

g) Coordinación, dirección y seguimiento de la actividad en materia de seguridad TIC de las entidades vinculadas o dependientes de la Consejería.

h) Aplicación de los criterios y directrices de gestión de la seguridad TIC emanadas de la Unidad de Seguridad TIC Corporativa.

i) Y cuantas otras le sean encomendadas por el órgano directivo de la Consejería del que dependa funcional u orgánicamente.

2. Las entidades vinculadas o dependientes contarán, al menos, con una persona Responsable de Seguridad TIC que será nombrada por el Comité de Seguridad TIC de las mismas y que tendrá las siguientes atribuciones:

a) Labores de soporte, asesoramiento e información al Comité de Seguridad TIC de la entidad, así como de ejecución de las decisiones y acuerdos adoptados por éste.

b) Diseño y ejecución de los programas de actuación propios de la entidad, incluyendo, entre otros, planes directores de seguridad, proyectos de desarrollo normativo, auditorías de cumplimiento y planes de adecuación legal.

c) Definición, implantación y mantenimiento de los controles de carácter organizativo para la protección de los datos, aplicaciones y sistemas, así como la realización y mantenimiento de los análisis de riesgos de la entidad.

d) Definición y ejecución de los programas formativos y de concienciación relacionadas con buenas prácticas de seguridad TIC en el ámbito de la entidad, procurando promover, en el proceso de selección de las personas participantes en estos programas, la concurrencia de mujeres.

e) Aplicación de los criterios y directrices de gestión de la seguridad TIC emanadas de la Unidad de Seguridad TIC de la Consejería de la que dependa la entidad.

3. La persona responsable de la Unidad de Seguridad TIC de las Consejerías y, en su caso, la persona Responsable de Seguridad TIC de las entidades vinculadas o dependientes tendrá la condición de Responsable de Seguridad, en los términos establecidos en el Real Decreto 3/2010, de 8 de enero, y en el Real Decreto 1720/2007, de 21 de diciembre, en caso de que dicha designación fuera única para todos los sistemas, ficheros o tratamientos de datos de carácter personal. En caso de que fuesen varias las personas designadas, la persona responsable de la Unidad de Seguridad TIC tendrá atribuciones de coordinación y dirección de la labor desempeñada por el resto de personas responsables de seguridad designadas.

CAPÍTULO IV. Operación de la seguridad TIC.

Artículo 12. Operación de la seguridad TIC.

1. La Consejería competente en materia de coordinación y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones desarrollará acciones centralizadas de prevención, detección y respuesta a incidentes en el ámbito de la Administración de la Junta de Andalucía. Tales acciones serán llevadas a cabo a través de AndalucíaCERT, centro especializado y orientado a la prevención, detección y respuesta a incidentes y amenazas de seguridad.

2. Los Servicios o Departamentos responsables de la prestación de los servicios de tecnologías de la información y comunicaciones de las Consejerías y entidades incluidas en el ámbito de aplicación del presente Decreto, deberán realizar la implantación y mantenimiento de los controles de carácter procedimental y operacional, así como de las medidas técnicas de protección de los datos, aplicaciones y sistemas de información en los términos previstos en el Anexo II del Real Decreto 3/2010, de 8 de enero, y, en su caso, en la normativa vigente en materia de protección de datos personales en lo referente a la adopción de medidas de seguridad específicas. Asimismo, dichos Servicios o Departamentos deberán velar por el cumplimiento de los términos previstos en la Política de seguridad TIC de la Junta de Andalucía y, en su caso, de la de su propia entidad o de la de su organismo de adscripción.

Disposición adicional primera. Marco regulador de seguridad TIC.

1. El marco regulador de seguridad TIC se conformará por las siguientes disposiciones y documentos:

a) Decreto 1/2011, de 11 de enero, y sus Órdenes de desarrollo.

b) Resoluciones de la Dirección General competente en materia de coordinación y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones de la Administración de la Junta de Andalucía.

c) Documentos técnicos, que se agruparán en las categorías de procedimientos y guías técnicas.

2. La Consejería competente en materia de coordinación y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones pondrá en marcha las acciones necesarias para dar a conocer y formar en el cumplimiento del marco regulador de seguridad TIC a las Consejerías y entidades incluidas en el ámbito de aplicación de este Decreto.

Disposición adicional segunda. Servicio Andaluz de Salud y Servicio Andaluz de Empleo.

Las disposiciones relativas a Consejerías contenidas en los artículos 6.2.b y 11.1, específicamente, en lo referente a la Unidad de Seguridad TIC, también serán de obligado cumplimiento para el Servicio Andaluz de Salud y el Servicio Andaluz de Empleo.

Disposición final primera. Desarrollo y ejecución.

Se faculta al Consejero de Economía, Innovación y Ciencia para dictar cuantas disposiciones sean precisas para el desarrollo y ejecución de lo previsto en el Decreto.

Disposición final segunda. Entrada en vigor.

El Decreto entrará en vigor el día siguiente al de su publicación en el Boletín Oficial de la Junta de Andalucía.

Sevilla, 11 de enero de 2011

José Antonio Griñán Martínez

Presidente de la Junta de Andalucía

Antonio Ávila Cano

Consejero de Economía, Innovación y Ciencia

ANEXO I. Glosario de términos

Activo de tecnologías de la información y comunicaciones: cualquier información o sistema de información que tenga valor para la organización. Incluye datos, servicios, aplicaciones, equipos, comunicaciones, instalaciones, procesos y recursos humanos.

Contingencia grave: Incidente de seguridad TIC cuya ocurrencia causaría la reducción significativa de la capacidad de la organización para atender eficazmente a sus obligaciones fundamentales, el sufrimiento de un daño significativo a los activos de la organización, el incumplimiento material de alguna ley o regulación, o un perjuicio significativo de difícil reparación a personas.

Incidente de seguridad TIC: Suceso, accidental o intencionado, a consecuencia del cual se ve afectada la integridad, confidencialidad o disponibilidad de la información.

Plan director de seguridad: Estrategia y conjunto de iniciativas planificadas, plasmadas en un documento escrito, cuyo objetivo es alcanzar un determinado nivel de seguridad en la organización.

Política de seguridad de la información y comunicaciones: Conjunto de directrices plasmadas en un documento escrito, que rigen la forma en que una organización gestiona y protege sus activos de tecnologías de la información y comunicaciones.

Riesgo: Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. Posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización.

Sistema de información: Conjunto organizado de recursos destinado a recoger, almacenar, procesar, presentar o transmitir la información.

Sistema de información crítico: Sistema de información cuyo adecuado funcionamiento es indispensable para el funcionamiento de la organización y el cumplimiento de sus obligaciones fundamentales.

Disposiciones adicional, transitoria y finales del Decreto 70/2017, de modificación

Disposición adicional única. Disponibilidades presupuestarias ordinarias.

1. Las Consejerías y entidades incluidas en el ámbito de aplicación de este Decreto deberán desarrollar las medidas derivadas de su cumplimiento ateniéndose a sus disponibilidades presupuestarias ordinarias.

2. Las obligaciones derivadas de todas las actuaciones que se desarrollen en el ámbito de la política de seguridad de las TIC en la Administración de la Junta de Andalucía deberán ser asumidas por los distintos

centros directivos gestores de las mismas, de acuerdo a la envolvente que les sea asignada, dentro de las disponibilidades presupuestarias de la Junta de Andalucía.

3. Para posibilitar la ejecución práctica de algunas de las previsiones organizativas de este Decreto y en línea con lo exigido por la normativa estatal en cuanto a diferenciación de funciones, deberá procederse, en su caso, a realizar las reorganizaciones y reasignaciones de puestos que sean necesarias para que la Unidad de Seguridad TIC y el responsable de seguridad TIC dispongan de los perfiles profesionales necesarios y cumplan el principio de función diferenciada.

Disposición transitoria única. Adecuación normativa.

Las Consejerías y entidades incluidas en el ámbito de aplicación del Decreto 1/2011, de 11 de enero, dispondrán de un plazo de seis meses, contados a partir de la fecha de entrada en vigor del presente Decreto, para la adecuación a lo dispuesto en el mismo.

Disposición final primera. Desarrollo y ejecución.

Se faculta a la persona titular de la Consejería competente en materia de coordinación y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones de la Administración de la Junta de Andalucía para dictar cuantas disposiciones sean precisas para el desarrollo y ejecución de lo previsto en el Decreto.

Disposición final segunda. Entrada en vigor.

El presente Decreto entrará en vigor el mismo día de su publicación en el Boletín Oficial de la Junta de Andalucía.

Sevilla, 6 de junio de 2017

SUSANA DÍAZ PACHECO

Presidenta de la Junta de Andalucía

JOSÉ SÁNCHEZ MALDONADO

Consejero de Empleo, Empresa y Comercio