CONSEJERÍA DE ECONOMÍA, INNOVACIÓN Y CIENCIA

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.

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

D I S P O N G O

CAPÍTULO I

Disposiciones generales

Artículo 1. Objeto.

1. El Decreto tiene por objeto definir y regular la política de seguridad de la información y comunicaciones de la Administración de la Junta de Andalucía que se ha de aplicar en el tratamiento de los activos de tecnologías de la información y

comunicaciones de su titularidad o cuya gestión tenga encomendada, conformando, junto a la normativa que lo desarrolle, el marco normativo de seguridad TIC de la Administración de la Junta de Andalucía.

2. Sin perjuicio de las directrices establecidas en el marco normativo de seguridad TIC de la Administración de la Junta de Andalucía, cada entidad incluida en el ámbito de aplicación del Decreto desarrollará y aprobará el documento de política de seguridad TIC de la entidad, así como las normas y procedimientos que adecuen, en su caso, las directrices comunes de la Administración de la Junta de Andalucía a sus particularidades.

Artículo 2. Definiciones y estándares.

1. 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.

2. Se reconocen como referencias válidas en lo que a la seguridad de los activos TIC de la Administración de la Junta de Andalucía se refiere, entre otros, los estándares recogidos en el Anexo II. Este Anexo podrá ser modificado por Orden de la persona titular de la Consejería competente en materia de Telecomunicaciones y Sociedad de la Información, previo acuerdo de la Comisión Interdepartamental de la Sociedad de la Información de la Junta de Andalucía.

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. Responsabilidad general.

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 estas responsables del uso correcto de los activos de tecnologías de la información y comunicaciones puestos a su disposición.

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 miembro de la Comisión Interdepartamental de la Sociedad de la Información de la Junta de Andalucía (CISI), elegidas en el seno de la misma.

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.

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 entidades incluidas en el ámbito de aplicación del Decreto.

4. El Comité se reunirá al menos una vez por trimestre 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.

5. El Comité nombrará entre sus miembros 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.

6. Las labores de soporte y asesoramiento al Comité serán realizadas por la persona responsable de la Coordinación en Seguridad TIC y el Grupo de Personas Expertas en Seguridad TIC de la Administración de la Junta de Andalucía.

Artículo 8. Responsable de la Coordinación en Seguridad TIC de la Junta de Andalucía.

1. La persona responsable de la Coordinación en Seguridad TIC, garantizando el principio de función diferenciada recogido en el artículo 5.j), será nombrada por el Comité de Seguridad TIC de la Junta de Andalucía. Esta persona tendrá que ser funcionaria de carrera de la Administración de la Junta de Andalucía del Grupo A.1 y que desempeñe un puesto de trabajo con un nivel igual o superior a 27.

2. La persona responsable de la Coordinación en Seguridad TIC tendrá las siguientes atribuciones:

a) Labores de coordinación del Grupo de Personas Expertas en Seguridad TIC y enlace con el Comité de Seguridad TIC de la Junta de Andalucía.

b) Elevación de propuestas e informes al Comité de Seguridad TIC de la Junta de Andalucía.

c) Labores de soporte y asesoramiento al Comité de Seguridad TIC de la Junta de Andalucía.

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

1. Las personas miembro del Grupo de Personas Expertas en Seguridad TIC serán nombradas por el Comité de Seguridad TIC de la Junta de Andalucía. Estas personas serán empleadas públicas de la Administración de la Junta de Andalucía.

2. El Grupo de Personas Expertas en Seguridad TIC tendrá las siguientes atribuciones:

a) Definición del planteamiento técnico y operativo de los objetivos, iniciativas y planes estratégicos en seguridad TIC.

b) Elaboración de propuestas relativas a la revisión del marco normativo de seguridad TIC, a las que hace referencia el artículo 7.3.c).

c) Elaboración de informes y propuestas de cumplimiento legal y normativo.

d) Elaboración de informes del nivel de seguridad TIC de los activos.

3. El Grupo de Personas Expertas en Seguridad TIC se reunirá al menos una vez por trimestre, 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.

4. En la composición del Grupo de Personas Expertas en Seguridad TIC, 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 10. Comités de Seguridad TIC de las Entidades.

1. Sin perjuicio de las competencias propias del Comité de Seguridad TIC de la Junta de Andalucía y en el marco de las directrices e iniciativas estratégicas emanadas de éste, en cada entidad incluida en el ámbito de aplicación del Decreto se creará un Comité de Seguridad TIC, como órgano colegiado de dirección y seguimiento en materia de seguridad de los activos TIC de su titularidad o cuya gestión tenga encomendada. En la composición de este Comité 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.

2. La composición, atribuciones, funcionamiento y método de trabajo del Comité de Seguridad TIC de las entidades incluidas en el ámbito de aplicación del presente Decreto deberá ser aprobada por el máximo órgano de dirección de la entidad, en el caso de las Consejerías mediante Orden de la persona titular de la misma.

Artículo 11. Responsable de seguridad TIC.

1. En cada una de las entidades incluidas en el ámbito de aplicación del presente Decreto deberá existir una persona, garantizando el principio de función diferenciada recogido en el artículo 5.j), que ejerza las funciones de responsable de seguridad TIC de la entidad, debiendo ser nombrada por el Comité de Seguridad TIC de la misma.

2. La persona responsable de seguridad TIC tendrá las siguientes funciones:

a) Definición y seguimiento de las actuaciones relacionadas con la seguridad TIC de los activos de información de la entidad y la gestión del riesgo.

b) Asesoramiento y soporte al Comité de Seguridad TIC de su entidad.

c) Coordinación en materias de seguridad TIC en su entidad.

d) Desarrollo y seguimiento de programas de formación y concienciación.

e) Asunción de las funciones incluidas en el artículo 95 del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre.

f) Asunción de las funciones incluidas en los artículos 10, 27.3, 34.6, Anexo II (apartado 2.3) y Anexo III (apartados 2.1.b y 2.2.b) del 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.

CAPÍTULO IV

Gestión de la seguridad TIC

Artículo 12. Gestión de la seguridad TIC en la Administración de la Junta de Andalucía.

1. La Consejería a la que se adscribe la Red Corporativa de Telecomunicaciones de la Administración de la Junta de Andalucía, garantizando el principio de función diferenciada recogido en el artículo 5.j), realizará acciones de prevención, detección y respuesta a incidentes y amenazas de seguridad TIC.

2. La gestión de la seguridad TIC en la Administración de la Junta de Andalucía se desarrollará a través de Andalucía-

Cert, centro especializado y orientado a la prevención, detección y respuesta a incidentes y amenazas de seguridad en el ámbito de la administración, el sector empresarial y la ciudadanía de la Comunidad Autónoma de Andalucía.

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.

ANEXO II

Estándares

a) UNE-ISO/IEC 27001, Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos (ISO/IEC 27001).

b) UNE 71599-1:2010. Gestión de la continuidad del negocio. Parte 1: Código de práctica.

c) UNE 71599-2:2010. Gestión de la continuidad del negocio. Parte 2: Especificaciones.