I. Comunidad Autónoma

3. Otras disposiciones

Consejería de Hacienda y Administración Pública

2617 Orden de 28 de marzo de 2017, del Consejero de Hacienda y Administración Pública por la que se establece la política de seguridad de la información en la Administración Regional.

La necesaria generalización de la sociedad de la información es subsidiaria, en gran medida, de la confianza que genere en los ciudadanos la relación a través de medios electrónicos.

En el ámbito de las Administraciones públicas, la consagración del derecho a comunicarse con ellas a través de medios electrónicos comporta una obligación correlativa de las mismas, que tiene, como premisas, la promoción de las condiciones para que la libertad y la igualdad sean reales y efectivas, y la remoción de los obstáculos que impidan o dificulten su plenitud, lo que demanda incorporar las peculiaridades que exigen una aplicación segura de estas tecnologías.

La finalidad del Esquema Nacional de Seguridad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

El Esquema Nacional de Seguridad persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas. Se desarrollará y perfeccionará en paralelo a la evolución de los servicios y a medida que vayan consolidándose los requisitos de los mismos y de las infraestructuras que lo apoyan.

Actualmente los sistemas de información de las Administraciones públicas están fuertemente relacionados entre sí y con sistemas de información del sector privado: empresas y administrados. De esta manera, la seguridad tiene un nuevo reto que va más allá del aseguramiento individual de cada sistema. Es por ello que cada sistema debe tener claro su perímetro y los responsables de cada dominio de seguridad deben coordinarse efectivamente para evitar «tierras de nadie» y fracturas que pudieran dañar a la información o a los servicios prestados.

En este contexto se entiende por seguridad de la información, la capacidad de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que los sistemas de información ofrecen o hacen accesibles.

Los sistemas de información deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la autenticidad, confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios.

Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes órganos de la Administración Regional sus organismos y entes públicos en su caso deben cerciorarse de que la seguridad de los sistemas de información es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos relacionados con los sistemas de información.

La Política de Seguridad de la Información define el marco global para la gestión de la seguridad de la información protegiendo todos los activos de información y garantizando la continuidad en el funcionamiento de los sistemas de información. Se pretende de esta forma minimizar los riesgos derivados de una posible falla en la seguridad y asegurar el cumplimiento de los objetivos del Gobierno de la Región de Murcia ante un hipotético incidente de seguridad de la información.

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD), tiene como objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y especialmente de su honor e intimidad personal y familiar. Su artículo 9.1 dispone que «el responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural».

El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, establece las medidas de seguridad mínimas que deben aplicarse a los ficheros automatizados y no automatizados que contengan datos de carácter personal, entre las que se incluye el nombramiento de una serie de figuras con responsabilidades específicas.

La Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, tiene entre sus fines la creación de las condiciones de confianza en el uso de los medios electrónicos mediante el establecimiento de 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. En su disposición final octava esta Ley establece que corresponde al Gobierno y a las Comunidades Autónomas, en el ámbito de sus respectivas competencias, dictar las disposiciones necesarias para el desarrollo y aplicación de dicha Ley.

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, desarrolla la Ley 11/2007, de 22 de junio, y fija una serie de requisitos mínimos que deben concretarse en el correspondiente plan de adecuación. Entre tales requisitos están la aprobación formal de la política de seguridad y la organización de la seguridad. En este sentido, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, determina que las Administraciones Públicas deberán ajustarse a lo previsto en el Esquema Nacional de Seguridad en lo que se refiere al establecimiento de la política de seguridad en la utilización de medios electrónicos.

Asimismo la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, establece que la tramitación electrónica debe constituir la actuación habitual de las Administraciones Públicas, para servir mejor a los principios de eficacia, eficiencia, al ahorro de costes, a las obligaciones de transparencia y a las garantías de los ciudadanos. Del mismo modo, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, recoge, con las adaptaciones necesarias, las normas hasta ahora contenidas en la Ley 11/2007, de 22 de junio, en lo relativo al funcionamiento electrónico del sector público.

El Reglamento del Parlamento Europeo y del Consejo 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 (2016/679) fija un nuevo marco europeo en la protección de datos de carácter personal de aplicación en los estados miembros de La Unión.

En el ámbito autonómico el Decreto n.º 302/2011, de 25 de noviembre, de Régimen Jurídico de la Gestión Electrónica de la Administración Pública de la Comunidad Autónoma de la Región de Murcia, tiene como objeto establecer el régimen jurídico de la gestión electrónica de la Administración Pública de la Comunidad Autónoma de la Región de Murcia, con la finalidad de hacer efectivos los principios de eficacia, eficiencia, racionalización, agilidad y transparencia en la actuación administrativa, así como garantizar el principio de servicio a los ciudadanos y la efectividad de los derechos reconocidos en la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.

La Orden de 15 de enero de 2013, de la Consejería de Economía y Hacienda por la que se dispone la puesta en marcha de la sede electrónica de la Administración Pública de la Comunidad Autónoma de la Región de Murcia, establece que la integración de información y servicios en la sede electrónica se formalizará a través de las Secretarias Generales de las Consejerías, así como a través de los organismos públicos y de las entidades de derecho público. Por otra parte, la Dirección General competente en materia de planificación informática, sistemas de información y aplicaciones informáticas, será quien determinará los requisitos técnicos y de seguridad de los servicios propuestos en la sede electrónica. Asimismo la Dirección General competente en materia de innovación de los servicios públicos, tendrá la competencia para gestionar los servicios ofrecidos desde la sede electrónica.

El Decreto n.º 105/2015, de 10 de julio, por el que se establecen los Órganos Directivos de la Consejería de Economía y Hacienda y atribuye las competencias en sistemas de información y seguridad informática, a la Dirección General de Patrimonio e Informática, quedando encuadrada finalmente en la Consejería de Hacienda y Administración Pública mediante Decreto de la Presidencia18/2015, de 4 de julio, de reorganización de la Administración Regional.

En virtud de lo expuesto,

Dispongo:

Artículo 1.- Objeto.

La presente Orden tiene por objeto definir y regular la política de seguridad de la información que se ha de aplicar en el tratamiento de la información situada bajo la responsabilidad de los distintos órganos de la Administración de la Comunidad Autónoma de la Región de Murcia y sus organismos públicos y entidades de derecho público y privadas vinculadas y dependientes de ella.

Asimismo se establece el reparto de funciones y responsabilidades en materia de seguridad de la información entre los distintos órganos y unidades.

Artículo 2.- Ámbito de aplicación.

La política de seguridad y la organización de la seguridad de la información regulada en la presente Orden deberá aplicarse a toda la información bajo la responsabilidad de la Administración de la Comunidad Autónoma de la Región de Murcia y sus organismos públicos y entidades de derecho público y privadas vinculadas y dependientes de ella que les sea de aplicación. No se limita a los datos de carácter personal y es independiente de que el tratamiento sea manual o automatizado y su soporte sea electrónico o en papel. Será de aplicación a todos los sistemas de información.

La política de seguridad de la información será de obligado cumplimiento para todos los órganos de la Administración de la Comunidad Autónoma de la Región de Murcia y sus organismos públicos y entidades de derecho público y privadas vinculados o dependientes de ella que no tengan establecida su propia política de seguridad, asimismo deberá ser observada por todo el personal de los mismos, así como por aquellas personas que, no perteneciendo a su organización tengan acceso a sus sistemas de información o a la información gestionada por ellos.

En aquellos organismos o entidades que tengan su propia política de seguridad, prevalecerá en caso de discrepancia la definida en esta Orden.

Artículo 3.- Sistema de Información y otros términos.

1. Sistema de Información. Se considera sistema de información al conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir. Se incluyen todos los sistemas de información que prestan servicio a Consejerías, Organismos Autónomos (en adelante OOAA) y demás entidades de derecho público y privadas vinculados o dependientes, ya se emplee soporte papel o electrónico. En soporte electrónico se consideran servidores, ordenadores de puesto de trabajo, equipos portátiles y tabletas electrónicas, teléfonos móviles, impresoras y otros periféricos y dispositivos de salida de datos, sistemas de localización, redes internas y externas, sistemas multiusuario y servicios de comunicaciones (transmisión telemática de voz, imagen, datos o documentos) y almacenamiento que sean de su propiedad o le presten servicio, así como las aplicaciones informáticas que estén alojadas en cualquiera de los sistemas o infraestructuras referidos y la información contenida en ellos.

2. Otros términos.

Los términos empleados en este articulado tendrán el sentido que se establece en el anexo de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en el anexo IV del el Real Decreto 3/2010, de 8 de enero por el que se regula el Esquema Nacional de Seguridad (en adelante ENS) en el ámbito de la Administración Electrónica, en el anexo del

Real decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad (en adelante ENI) en el ámbito de la Administración electrónica y en el Glosario de términos incluidos en el anexo.

Se reconocen como referencias válidas en lo que a la seguridad de los activos de la Administración Pública de la Comunidad Autónoma de la Región de Murcia se refiere a los estándares; UNE-ISO/IEC 27001:2014 y UNE-ISO/IEC 27002:2015.

Artículo 4.- Prevención.

Los organismos afectados por esta Orden deben prevenir en la medida de lo posible, que los servicios prestados y la información que los sustentan no se vean perjudicados por incidentes de seguridad en los sistemas de información. Para ello deben identificar e implementar las medidas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Artículo 5.- Detección.

Según lo establecido en el Artículo 9 del ENS, debe monitorizarse de manera continua la operación de los sistemas de información.

La monitorización de los sistemas de información se basará en el establecimiento de mecanismos de detección de anomalías de seguridad, análisis e informe que se activarán cuando se produzca una desviación significativa de los parámetros establecidos como aceptables.

Artículo 6.- Respuesta.

Se creará en el seno de la Dirección General competente en materia informática un Equipo de Respuesta ante Incidentes de Seguridad que coordinará su formalización procedimental, análisis y resolución.

Todos los organismos comprendidos en el alcance de esta Orden aplicarán procedimientos para responder eficazmente a los incidentes de seguridad, entre ellos los procedimientos de comunicación de los incidentes de seguridad detectados y los protocolos de comunicación de información sobre los incidentes con otras organizaciones.

Artículo 7.- Recuperación.

Los distintos organismos comprendidos en el alcance de esta Orden formalizarán, en coordinación con la Dirección General competente en la materia informática, planes de continuidad de los sistemas de información.

Artículo 8.- Misión.

1. La Administración de la Comunidad Autónoma de la Región de Murcia establece el alineamiento con la gestión de la seguridad de la información según lo establecido 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, reconociendo como activos estratégicos la información y los sistemas que la soportan.

2. Principios generales de protección en materia de seguridad de la información:

a) Seguridad como proceso integral. La vigilancia y mejora de la seguridad de los sistemas de información engloba a todos y cada uno de los elementos humanos, técnicos, materiales y organizativos que participan de forma directa o indirecta en el ciclo de vida de los servicios y los sistemas de información que los sustentan.

b) Gestión orientada a la reducción de riesgos. La naturaleza cambiante de las amenazas sobre los sistemas de información, requiere la adopción de las decisiones en materia de seguridad basadas en el análisis y gestión de riesgos dentro de un ciclo de mejora continua.

c) Defensa proactiva. Incorporando, siempre que sea posible, mecanismos preventivos y de detección para evitar la ocurrencia de incidentes de seguridad o, al menos, minimizar su impacto sobre los sistemas de información cuando éstos sucedan.

d) Segregación de funciones. La responsabilidad de la seguridad de los sistemas de información estará diferenciada de otras responsabilidades sobre la prestación de los servicios.

e) Proporcionalidad en el coste. La implantación de medidas que mitiguen los riesgos de seguridad de los sistemas de información deberá hacerse bajo un enfoque de proporcionalidad en los beneficios, costes económicos y operativos.

f) Concienciación y formación en materia de seguridad. Todo el personal al servicio de los organismos a los que es de aplicación esta Orden deberán recibir la información y formación necesaria de forma que sean conscientes de los riesgos, sus obligaciones y responsabilidades en la interacción con los sistemas de información.

g) Auditoría y mejora continua. Los niveles de protección de los sistemas de seguridad deberán ser verificados mediante revisiones periódicas que detecten el nivel de robustez de las medidas de seguridad aplicadas, propongan las correcciones a las deficiencias halladas con la finalidad de lograr una mayor eficacia y eficiencia en la protección.

Artículo 9.- Marco normativo

Sin carácter exhaustivo, la legislación en materia de seguridad de la información que debe servir de referencia es la siguiente:

a) Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y sus normas de desarrollo.

b) El Reglamento del Parlamento Europeo y del Consejo 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 (2016/679).

c) Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

d) Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

e) Ley 59/2003, de 19 de diciembre, de firma electrónica.

f) Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.

g) Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad.

h) Decreto 302/2011, de 25 de noviembre, de Régimen Jurídico de la Gestión Electrónica de la Administración Pública de la Comunidad Autónoma de la Región de Murcia.

i) Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

j) Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

k) Orden de 30 de enero de 2017, de la Consejería de Hacienda y Administración Pública por la que se aprueba el manual de uso de medios electrónicos para el personal de la Administración Pública Regional.

Artículo 10.- Organización de la seguridad

1. La seguridad de los sistemas de información y de la información contenida en ellos corresponde, a los siguientes órganos y responsables:

a) Comité de Seguridad de la Información.

b) Responsables de la Información.

c) Responsables del Servicio.

d) Encargado del Tratamiento.

e) Responsables del Sistema.

f) Responsable de Seguridad.

g) Coordinador Operativo de la Seguridad.

h) Personal propio

Artículo 11.- Comité de Seguridad de la Información

1. El Comité de Seguridad de la Información (en adelante CSI) se crea como órgano colegiado dependiente de la Consejería competente en materia informática.

2. Al Comité de Seguridad de la Información le corresponden las siguientes funciones:

a) Asesoramiento, consultoría y propuesta en materia de seguridad de la información y protección de datos de carácter personal.

b) Informar del estado de la seguridad de la información al Gobierno de CARM.

c) Proponer al Consejero competente en materia informática la creación y las funciones en materia de seguridad de la información de Comités de la Seguridad de la Información Delegados.

d) Promover la mejora continua del sistema de gestión de la seguridad de la información.

e) Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información evitando duplicidades.

f) Elaborar y revisar regularmente la Política y Organización de la Seguridad de la Información elaborando, en su caso, propuestas de cambio.

h) Informar la aprobación de las normas de seguridad de la información.

i) Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones en materia de seguridad.

h) Proponer planes de mejora de la seguridad de la información de la organización.

j) Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos informáticos desde su especificación inicial hasta su puesta en operación y posterior mantenimiento, así como en la preservación de la información que sea requerida tras el cese en la utilización del mismo.

k) Velar por la adecuada divulgación de la normativa en materia de seguridad de los sistemas de información.

3. El Comité de Seguridad de la Información se compone de los siguientes miembros:

a) Presidente: El titular de la Dirección General competente en materia informática.

b) El Secretario será nombrado por el titular de la Dirección General competente en materia de informática entre su personal.

c) Vocales:

i Un representante de cada una de las Consejerías y Organismos Públicos de la Comunidad Autónoma de la Región de Murcia. Designados, de entre su personal, por los titulares de cada una de las Secretarías Generales u órganos asimilables en los Organismos Públicos.

ii. Un representante de la Inspección General de Servicios. Designado por la Dirección General competente en la materia.

iii. El Responsable de las funciones generales de Aplicaciones de la Dirección General competente en materia de informática.

iv. El Responsable de Sistemas de la Dirección General competente en materia de informática.

v. El Responsable de Infraestructuras de la Dirección General competente en materia de informática.

vi. El Responsable de Seguridad de la Dirección General competente en materia de informática.

vii. A las sesiones del Comité podrán asistir en calidad de asesores, con voz pero sin voto, las personas que en cada caso acepte el Presidente.

En caso de vacante, ausencia o enfermedad, los suplentes serán designados del mismo modo por el mismo órgano.

4. Cuando lo justifique la complejidad, la separación física de sus elementos o el número de usuarios de la información en soporte electrónico, o de los sistemas que la manejen, podrán crearse Comités de Seguridad de la Información Delegados, (en adelante CSID) dependientes funcionalmente del CSI, que serán responsables en su ámbito, de las actuaciones que se les deleguen.

Artículo 12.- Responsables de la Información.

1 El Responsable de la información será, para cada sistema de información, el titular del órgano administrativo con competencia suficiente para decidir sobre la finalidad, contenido, uso y tratamiento de la información contenida en aquél.

2. Al Responsable de la Información le corresponden las siguientes funciones:

a) Determinará, dentro del marco establecido en el Anexo I del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, los requisitos de seguridad de la información tratada. A tal efecto:

b) Fijará los niveles de seguridad de la información tratada, valorando los impactos de los incidentes que afecten a la seguridad de la información, conforme con lo establecido en el artículo 44 del Real Decreto citado.

c) Realizará, junto al Responsable del Servicio y el Responsable de Seguridad, los preceptivos análisis de riesgos, y seleccionarán las salvaguardas que se han de implantar.

d) Aceptará los riesgos residuales, respecto de los sistemas de información, obtenidos en el análisis de riesgos.

e) Realizará el seguimiento y control de los riesgos, con la participación del Responsable de Seguridad.

f) Asumirá dentro de su ámbito competencial y para los ficheros con datos de carácter personal, las funciones atribuidas al Responsable del Fichero y/o Tratamiento por la normativa en vigor sobre Protección de Datos de Carácter Personal.

Artículo 13.- Responsables del Servicio.

1. El Responsable del Servicio será, para cada sistema de información, el titular del órgano administrativo con competencia suficiente para decidir sobre la finalidad y prestación del servicio que aquel sustenta.

2. Al Responsable del Servicio le corresponden las siguientes funciones:

a) Determinará dentro del marco establecido en el Anexo I del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, los requisitos de seguridad de los servicios prestados.

b) En coordinación con el Responsable de la Información y de Seguridad, realizará los preceptivos análisis de riesgos, y seleccionarán las salvaguardas que se han de implantar.

c) Realizarán el seguimiento y control de los riesgos, con la participación del Responsable de Seguridad.

d) En su caso, suspenderá, de acuerdo con el Responsable de la Información y el Responsable de Seguridad, la prestación de un servicio electrónico o el manejo de una determinada información, si es informado de deficiencias de seguridad que pudieran afectar al cumplimiento de los requisitos establecidos.

Artículo 14.- Encargado del tratamiento.

La Dirección General competente en materia informática ejercerá, para los sistemas de información de Consejerías y Organismos Autónomos, las funciones de Encargado del tratamiento recogidas en la normativa en vigor sobre protección de datos de carácter personal..

Artículo 15.- Responsable del Sistema.

1. El Responsable del sistema será, para cada sistema de información, el responsable informático destacado en la Consejería y/o OOAA a la que corresponda el sistema de información.

2. El Responsable del Sistema desarrollará las siguientes funciones:

a) Informar al Responsable de la Información, del Servicio y de Seguridad cualquier cambio que conozca y pueda afectar a la seguridad del sistema de información.

b) Ejecutar, con el visto bueno de aquellos, la suspensión del manejo de información o prestación de un servicio si tiene conocimiento de deficiencias de seguridad que pudieran afectar al cumplimiento de los requisitos establecidos.

c) Coordinar y controlar la aplicación de las medidas definidas en el Documento de Seguridad, conforme a lo dispuesto en el artículo 95 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter Personal.

d) Coordinar, en lo que aplique, la ejecución de las medidas del plan de seguridad aprobado por el Comité de Seguridad de la Información.

Artículo 16.- Responsable de Seguridad.

1. El Responsable de Seguridad será designado por el titular del órgano con competencias en materia de informática entre personal adscrito a dicho órgano.

2. El Responsable de Seguridad desarrollará las siguientes funciones:

a) Determinará las decisiones para satisfacer los requisitos de seguridad de los sistemas de información.

b) Las atribuidas al responsable de Seguridad 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.

c) Las funciones atribuidas al Delegado de Protección de Datos por el artículo 39 del Reglamento 2016/679 del Parlamento Europeo y del Consejo 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.

d) Auditar las medidas definidas en el Documento de Seguridad, conforme a lo dispuesto en el artículo 95 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter Personal.

e) Proponer al Responsable de la Información la determinación de los niveles de seguridad en cada dimensión de seguridad siempre que se le solicite.

f) Realizar o promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información.

g) Realizar el seguimiento, control e informe del estado de seguridad de los sistemas de información.

h) Proponer al Comité de Seguridad de la Información las normas de seguridad y los procedimientos de seguridad.

3. Cuando lo justifique la complejidad, la separación física de sus elementos o el número de usuarios de la información en soporte electrónico, o de los sistemas que la manejen, el Director general en materia informática podrá designar «responsables de seguridad delegados» que, bajo la dirección del Responsable de Seguridad, ejercerán en su ámbito de las actuaciones las funciones que aquél le delegue.

Artículo 17.- Coordinador Operativo de la Seguridad

1. El Coordinador Operativo de la Seguridad será, para cada área de conocimiento y/o funcional el personal informático designado por la Dirección General competente en la materia y tendrán encomendada la tarea de la coordinación y asesoramiento en la implementación, coordinación de la gestión y mantenimiento de las medidas de seguridad aplicables en el área técnica y funcional que le corresponda

2. El Coordinador Operativo de la Seguridad asumirá las siguientes funciones:

a) Coordinar y supervisar la aplicación de los procedimientos operativos de seguridad, configuraciones de seguridad y medidas de seguridad, tanto en los servicios existentes como en los nuevos proyectos y contratos.

b) Coordinar la configuración de los sistemas para enviar eventos, logs, alertas al servicio de detección de amenazas e incidencias de seguridad.

c) Coordinar la resolución de incidencias y amenazas de seguridad.

d) Ser informado e informar a los Responsables de la Seguridad y del Sistema de cualquier cambio, anomalía, compromiso o vulnerabilidad relacionada con la seguridad.

Artículo 18.- Resolución de conflictos.

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de la Política de Seguridad de la Información, éste será resuelto por el titular de la Consejería con competencias en materia informática.

Artículo 19.- Revisión de la Política de Seguridad de la Información.

Las propuestas de modificación de la Política de Seguridad de la Información, en su caso, serán aprobadas por la Consejería con competencias en materia informática.

Artículo 20.- Desarrollo de la Política de Seguridad de la Información.

1. El cuerpo documental sobre seguridad de la información se desarrollará en tres niveles con diferente ámbito de aplicación y nivel de detalle técnico, de manera que cada documento de un determinado nivel se fundamente en los documentos de nivel superior.

a) Las normas de seguridad. Establecen un conjunto de requisitos que deben ser alcanzados para poder satisfacer cada uno de los objetivos de seguridad establecidos por la aplicación de esta orden.

b) Los procedimientos e instrucciones técnicas de seguridad. Describirán de forma concreta cómo proteger lo definido por las normas de seguridad. Son documentos que especifican cómo llevar a cabo las tareas habituales, quién debe hacer cada tarea y cómo identificar y reportar comportamientos anómalos.

c) El manual de comportamiento en el uso de los medios electrónicos para el personal de la Función Pública Regional. Fija las reglas de comportamiento que deben cumplir los usuarios en el uso de los sistemas de información.

2. Las normas de seguridad las aprueba la Dirección General competente en materia informática previo informe del Comité de Seguridad de la Información. Los procedimientos e instrucciones técnicas las aprueba la Dirección General competente en materia informática.

3. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información. Adicionalmente, la normativa de seguridad estará disponible en la intranet en: https://rica.carm.es/

Artículo 21.- Concienciación y formación.

Se establecerá un programa de concienciación continua para atender a todos los miembros de la Administración Regional, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una nueva responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

Artículo 22.- Obligaciones del personal.

1. Todos los miembros de la Administración de la Región de Murcia tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad que la desarrolle.

2. Los técnicos con responsabilidad en las distintas fases del ciclo de vida de los sistemas de informáticos aplicarán de forma inseparable a sus tareas y en al área de responsabilidad que les corresponda las normas de seguridad, los procedimientos e instrucciones técnicas de seguridad vigentes en cada momento.

Artículo 23.- Consecuencias del incumplimiento.

El incumplimiento de la Política de Seguridad o su normativa de desarrollo, dará lugar al establecimiento por la Dirección general competente en materia informática de medidas preventivas y correctivas, encaminadas a salvaguardar y proteger las redes y sistemas de información, sin perjuicio de la correspondiente exigencia de responsabilidades disciplinarias.

Artículo 24.- Terceras partes.

1. Cuando la Administración Regional preste servicios o ceda información a otras Administraciones Públicas u organismos, mediante los instrumentos jurídicos correspondientes, se les hará partícipe de esta Política de Seguridad de la Información y de las normas que la desarrollan.

2. Cuando la Administración utilice servicios de terceros o ceda información a terceros se les hará igualmente partícipe de esta Política de Seguridad de la Información y de la normativa e instrucciones de seguridad que ataña a dichos servicios o información.

3. Cuando los servicios con terceros se formalicen mediante contratos o convenios, se requerirá a partir de la entrada en vigor de esta Orden, que incluyan una cláusula en la que se establezca la obligación de cumplir esta política y el sistema de verificación de su cumplimiento e incluir un acuerdo de confidencialidad.

Cuando algún aspecto de la Política de la Seguridad de la Información no pueda ser satisfecho por una tercera parte, se requerirá un informe del Responsable de Seguridad de la Información que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por el Responsable de la Información y de los Servicios afectados antes de seguir adelante.

Disposición final primera. Habilitación para el desarrollo posterior.

Se faculta al titular de la Dirección General competente en materia informática para adoptar las medidas que resulten necesarias para la aplicación, desarrollo y ejecución de esta norma.

Disposición final segunda. Entrada en vigor.

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

Murcia, 28 de marzo de 2017.—El Consejero de Hacienda y Administración Pública, Andrés Carrillo González.

Anexo

Glosario

Activo. Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

Análisis de riesgos. Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

Autenticidad. Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

Confidencialidad. Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

Disponibilidad. Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

Incidente de seguridad. Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.

Integridad. Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

Plan de continuidad (de negocio). Un plan de continuidad del negocio es un plan logístico para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcialmente o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.

Riesgo. Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

Riesgo residual. Es el riesgo que una institución puede asumir después de aplicar medidas o salvaguardias de seguridad.