I. Comunidad Autónoma

1. Disposiciones Generales

Consejo de Gobierno

2855 Decreto n.º 79/2025, de 5 de junio, por el 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.

Los equipos de ciberseguridad deben hacer frente al creciente volumen y sofisticación de las amenazas. La falta de visibilidad de la red, el volumen de datos a analizar, la escasez de personal y la necesidad de filtrado y rápida respuesta en forma de alertas, lleva consigo que para cualquier organización ya no es posible hacer este análisis de forma manual.

Los sistemas de información actuales tienen una consideración estratégica, por lo que son activos que hay que proteger de manera especial. El tamaño de los mismos, así como su altísima complejidad, hacen que ya no sea suficiente con las herramientas tradicionales que hasta ahora se han venido usando, sino que se requieren herramientas y profesionales de una capacitación muy alta, para poder hacer frente a las cada vez más sofisticadas amenazas, tanto internas como externas.

La cantidad de *malware* en la última década ha crecido de manera sostenida año tras año, situando a los equipos de seguridad ante un escenario con cada vez mayor cantidad de herramientas maliciosas e incidentes de seguridad.

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.

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. Por ello 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 la información o 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.

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, fijaba una serie de requisitos mínimos que debían concretarse en el correspondiente plan de adecuación. Entre tales requisitos estaban la aprobación formal de la política de seguridad y la organización de la seguridad. 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.

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, y detalla cómo debe desarrollarse el funcionamiento electrónico del sector público.

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.

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), fija un nuevo marco europeo en la protección de datos de carácter personal de aplicación en los Estados miembros de la Unión. Este marco regulatorio queda completado por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (Ley Orgánica de Protección de Datos), que prevé que el Esquema Nacional de Seguridad incluya las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios

de determinación del riesgo en el tratamiento de los datos a lo establecido en el Reglamento general de protección de datos.

En este contexto la Orden de 28 de marzo de 2017, del Consejero de Hacienda y Administración Pública por la que se establece la política de seguridad de la información en la Administración Regional vino a definir en nuestro ámbito territorial 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 pretendió de esta forma organizar el cumplimiento con las nuevas obligaciones normativas sobre protección de sistemas de información y de datos de carácter personal.

El Consejo de Gobierno, mediante Acuerdo de 1 de agosto de 2018, designa a la Inspección General de Servicios como Delegado de Protección de Datos de la Administración General de la Comunidad Autónoma de la Región de Murcia, sus Organismos y Entidades públicas y privadas, Fundaciones y Consorcios, excluidos los siguientes organismos y entidades: la Consejería de Familia e Igualdad de Oportunidades y el Instituto Murciano de Acción Social, los Centros Docentes de la Consejería de Educación, Juventud y Deportes y el Servicio Murciano de Salud, los cuales tienen sus propios Delegados de Protección de Datos.

Las normas europeas, como la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, y la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2); así como sus normas de transposición, a saber, el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información y el Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información que afectan a servicios esenciales e infraestructuras críticas, incorporan nuevos roles como el Responsable de la Seguridad de la Información con funciones no contempladas en la política de seguridad vigente.

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, deroga el Real Decreto 3/2010, e incorpora cambios que, entre otros aspectos, afectan a la valoración y categorización de los sistemas de información, y por tanto a los roles definidos en la Orden de 28 de marzo de 2017. Asimismo, indica expresamente que cuando un sistema de información trate datos personales, le será de aplicación lo dispuesto en el Reglamento general de protección de datos y en la Ley Orgánica de Protección de Datos.

El Decreto-ley 5/2022, de 20 de octubre, de dinamización de inversiones empresariales, libertad de mercado y eficiencia pública crea la Agencia de Transformación Digital de la Región de Murcia (Agencia de Transformación Digital), como un organismo autónomo dependiente de la Administración General de la Comunidad Autónoma de la Región de Murcia. Se trata de un organismo público con personalidad jurídica propia y plena capacidad pública y privada, que, a partir de la fecha en la que inicie su actividad, asume las funciones de la Dirección General competente en materia de informática.

La Agencia de Transformación Digital queda adscrita a la Consejería competente en materia de hacienda, teniendo entre sus fines los siguientes: «a) La detección de necesidades, planificación, ejecución y prestación de todos los servicios de informática, telecomunicaciones, comunicación audiovisual, ciberseguridad, gobierno del dato y estrategia digital de la Administración Regional y de los organismos y entidades de derecho público dependientes de ella, incorporando y fomentando la administración electrónica y la transformación digital en la Administración y la sociedad; así como la gestión de comunicación audiovisual de ámbito autonómico y local.»

Los cambios en el contexto técnico, legal y organizativo descrito motivan que la política de seguridad de la información establecida en la Orden de 28 de marzo de 2017, del Consejero de Hacienda y Administración Pública por la que se establece la política de seguridad de la información en la Administración Regional requiera, para cumplir sus fines, de adaptación al nuevo contexto.

El ejercicio de la potestad reglamentaria que supone este decreto, de acuerdo con el artículo 52 de la Ley 6/2004, de 28 de diciembre, del Estatuto del Presidente y del Consejo de Gobierno de la Región de Murcia, cumple los principios de buena regulación recogidos en el artículo 129 de la Ley 39/2015, de 1 de octubre. Así, en cumplimiento de los principios de necesidad y eficacia, la iniciativa normativa está justificada por el interés general y la finalidad de garantizar la existencia de una administración electrónica segura y confiable, y es el instrumento adecuado para desarrollar a nivel regional el Esquema Nacional de Seguridad. En virtud del principio de proporcionalidad, la norma contiene la regulación imprescindible para atender la necesidad que se pretende cubrir, sin establecer medidas restrictivas de derechos innecesarias. Con el fin de garantizar el principio de seguridad jurídica, la norma es coherente con el resto del ordenamiento jurídico, nacional y de la Unión Europea, tal y como se ha expuesto más arriba, para generar un marco normativo estable, predecible, integrado, claro y de certidumbre, que facilite su conocimiento y comprensión y, en consecuencia, la actuación y toma de decisiones de las personas y empresas. En aplicación del principio de transparencia, en la elaboración del decreto se han realizado todos los trámites que garantizan el acceso y la participación de los potenciales destinatarios, a través de la realización de consultas públicas y trámites de audiencia e información públicas. Finalmente, en garantía del principio de eficiencia la norma evita la imposición de cargas administrativas innecesarias y asegura la racionalización de la gestión de recursos públicos, posibilitando la atribución de las funciones requeridas por la política de seguridad de la información a órganos ya existentes en la Administración Regional.

El Decreto del Presidente n.º 19/2024, de 15 de julio, de reorganización de la Administración Regional establece que la Consejería de Economía, Hacienda, Fondos Europeos y Transformación Digital es el departamento de la Comunidad Autónoma de la Región de Murcia encargado de la propuesta, desarrollo y ejecución de las directrices generales del Consejo de Gobierno en lo relativo, entre otras materias, a sistemas de información y comunicaciones corporativas, incluida la planificación informática y la coordinación de redes corporativas; transformación digital interna de la administración y externa; comunicación audiovisual; sociedad de la información y telecomunicaciones; innovación tecnológica vinculada a las TICs de aplicación en la sociedad, administración

y sociedad del conocimiento. A dicha consejería le está adscrita la Agencia de Transformación Digital. Por su parte, el artículo 7 del Decreto n.º 179/2024, de 12 de septiembre, por el que se establecen los Órganos Directivos de la Consejería de Economía, Hacienda, Fondos Europeos y Transformación Digital, atribuye a la Dirección General de Transformación Digital, entre otras, las competencias relativas a los sistemas de información y la seguridad informática.

En virtud de lo expuesto, a propuesta del Consejero de Economía, Hacienda, Fondos Europeos y Transformación Digital, y de conformidad con lo dispuesto en el artículo 51 del Estatuto de Autonomía para la Región de Murcia, y en los artículos 22.12 y 52.1 de la Ley 6/2004, de 28 de diciembre, del Estatuto del Presidente y del Consejo de Gobierno de la Región de Murcia, de acuerdo con el Consejo Jurídico de la Región de Murcia, y tras la deliberación y acuerdo del Consejo de Gobierno, en sesión de fecha 5 de junio de 2025,

Dispongo:

Capítulo I

Disposiciones generales

Artículo 1. Objeto.

El presente decreto 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 General de la Comunidad Autónoma de la Región de Murcia y sus organismos públicos y entidades de derecho público y privado vinculadas y dependientes de ella, cuya misión conjunta es la realización de los intereses públicos regionales.

Forma parte, asimismo, del objeto de esta norma establecer el reparto de funciones y responsabilidades en materia de seguridad de la información.

Artículo 2. Ámbito de aplicación.

1. La política de seguridad y la organización de la seguridad de la información regulada en la presente norma deberá aplicarse a toda la información bajo la responsabilidad de la Administración General de la Comunidad Autónoma de la Región de Murcia y sus organismos públicos y entidades de derecho público y privado vinculadas y dependientes de ella a los 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 electrónico o en papel. Será de aplicación a todos los sistemas de información.

2. La política de seguridad de la información será de obligado cumplimiento para todos los órganos de la Administración General de la Comunidad Autónoma de la Región de Murcia y sus organismos públicos y entidades de derecho público y privado 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.

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

Artículo 3. 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 previsto en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, reconociendo como activos estratégicos la información y los sistemas que la soportan.

2. Junto con los principios básicos previstos en el Esquema Nacional de Seguridad y en el Esquema Nacional de Interoperabilidad, son aplicables los siguientes principios generales de protección en materia de seguridad de la información:

a) Seguridad global. 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 decisiones en materia de seguridad basadas en el análisis y la gestión de riesgos dentro de un ciclo de mejora continua.

c) Defensa proactiva. Se incorporarán, siempre que sea posible, mecanismos preventivos y de detección para evitar incidentes de seguridad o, al menos, para 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 con un enfoque de proporcionalidad entre los beneficios y los 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 norma deberá recibir la información y formación necesaria, de forma que sea consciente de los riesgos, de sus obligaciones y de sus 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 y propongan las correcciones a las deficiencias halladas, con la finalidad de lograr una mayor eficacia y eficiencia en la protección.

Artículo 4. Marco normativo.

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

a) Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

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

c) Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial).

d) Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

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

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

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

h) Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

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) Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

l) Ley 11/2022, de 28 de junio, General de Telecomunicaciones.

m) Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

n) Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

o) Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

p) Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

q) Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

r) 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.

s) Aquellas normas aplicables a la administración electrónica y seguridad de la información que complementen, desarrollen o sustituyan a las anteriores y que se encuentren dentro del ámbito de aplicación de la Política de Seguridad de la Información de la Administración Regional.

Artículo 5. Términos y definiciones.

1. Los términos empleados en esta norma tendrán el sentido que se establece en el Anexo IV del Real Decreto 311/2022, de 3 de mayo, en el Real Decreto-ley 12/2018, de 7 de septiembre y en el Anexo del Real Decreto 4/2010, de 8 de enero. También se asumen las definiciones recogidas en el Reglamento (UE) 2016/679 de 27 de abril, y en la Directiva (UE) 2022/2555 de 14 de diciembre.

2. Los estándares UNE-ISO/IEC 27001 y UNE-ISO/IEC 27002 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.

Artículo 6. Sistemas de información que traten datos personales y análisis de riesgos.

1. Se aplicarán a los datos de carácter personal que sean objeto de tratamiento por parte de la Agencia de Transformación Digital de la Región de Murcia las medidas de seguridad apropiadas derivadas del correspondiente análisis de riesgos, así como de la evaluación de impacto relativa a la protección de datos que se detalla en el Reglamento (UE) 2016/679 de 27 de abril y en la Ley Orgánica 3/2018, de 5 de diciembre.

2. Además, se aplicarán las medidas previstas en el Anexo II del Real Decreto 311/2022, de 3 de mayo. En el caso de que el análisis de riesgos determine medidas agravadas respecto a la normativa recogida en las medidas del citado Anexo, las medidas derivadas del análisis de riesgos serán las que se implementarán en la protección de datos de carácter personal.

3. Los servicios de la Agencia de Transformación Digital de la Región de Murcia podrán realizar tratamientos de datos personales como consecuencia de la implantación de medidas de seguridad que tengan un objeto distinto a la protección de datos personales, de acuerdo con lo dispuesto en el artículo 24 del Real Decreto 311/2022, de 3 de mayo. Dicho tratamiento tendrá en cuenta, entre otros, los principios de limitación de la finalidad; de prohibición del tratamiento de los datos personales para fines distintos; de minimización de datos, identificando los datos personales o las categorías de datos personales que pudieran ser tratados; y de limitación del plazo de conservación, identificando los plazos máximos de conservación de los datos personales.

Artículo 7. Requisitos mínimos de seguridad.

Los órganos y organismos que se encuentren en el ámbito de aplicación de esta norma aplicarán los requisitos mínimos de seguridad descritos en el capítulo III del Real Decreto 311/2022, de 3 de mayo, y en el Real Decreto 4/2010, de 8 de enero, conforme a lo establecido por la normativa en materia de seguridad de la información derivada de la aplicación de este decreto o, en su defecto, por lo establecido por la Agencia de Transformación Digital de la Región de Murcia.

Capítulo II

Organización de la política de seguridad de la información

Artículo 8. Organización de la Seguridad.

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) Responsable de la Información.

c) Responsable del Servicio.

d) Responsable de la Seguridad.

e) Responsable del Sistema.

f) Coordinador Operativo de la Seguridad.

g) Comités de Seguridad de la Información Delegados y Responsables de la Seguridad Delegados, en su caso.

Artículo 9. Comité de Seguridad de la Información.

1. El Comité de Seguridad de la Información se crea como órgano colegiado dependiente de la Consejería competente en materia informática,

2. Los objetivos del Comité de Seguridad de la Información son garantizar la coordinación de la seguridad de la información en la Administración regional, asegurar la eficacia en la aplicación de las medidas en esta materia y promover la adecuada inserción de la cultura de la seguridad de la información en todos los ámbitos competenciales de la Administración Regional, así como entre los empleados públicos y cualesquiera otras personas que desempeñen funciones o asuman responsabilidades públicas en el ámbito de las Administración regional.

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

a) Asesorar en materia de seguridad de la información.

b) Dar cuenta del estado de la seguridad de la información al Gobierno de la Comunidad Autónoma de la Región de Murcia.

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

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

e) Supervisar y revisar regularmente la política y organización de la seguridad de la información.

f) Ser informado, con carácter previo, de la aprobación de las normas de seguridad de la información.

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

h) Promover la elaboración de planes de mejora de la seguridad de la información de la organización.

i) Velar por que la seguridad de la información se tenga en cuenta en todos los sistemas de información, 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 de los mismos.

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

4. El Comité de Seguridad de la Información está compuesto por:

a) Presidencia: la persona titular de la Dirección General de la Agencia de Transformación Digital de la Región de Murcia.

b) Secretaría: la persona nombrada por quien sea titular de la Dirección General de la Agencia de Transformación Digital de la Región de Murcia, entre el personal de esta.

c) Vocales:

1.º La persona titular de la Vicesecretaría o equivalente de cada una de las Consejerías y Organismos Públicos de la Comunidad Autónoma de la Región de Murcia.

2.º Las personas responsables de Área o Subdirección General de la Agencia de Transformación Digital de la Región de Murcia.

3.º La persona Responsable de la Seguridad.

4.º Un funcionario de la Inspección General de Servicios, designado por la Dirección General competente en la materia.

A las sesiones del Comité podrán asistir en calidad de asesores, con voz pero sin voto, las personas que en cada caso acepte la Presidencia, a propuesta de los miembros del Comité.

En caso de vacante, ausencia o enfermedad, los suplentes serán designados por el órgano superior respectivo.

5. 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, dependientes funcionalmente del Comité de Seguridad de la Información, que serán responsables en su ámbito, de las actuaciones que se les deleguen. La composición y el régimen de funcionamiento de estos comités quedarán determinados en el acto de creación.

6. En lo no previsto en esta norma, el Comité de Seguridad de la Información se regirá por lo establecido para los órganos colegiados en la normativa básica recogida en la Sección 3.ª del Capítulo II del Título Preliminar de la Ley 40/2015, de 1 de octubre, así como en el artículo 19 de dicha ley.

Artículo 10. Responsable de la Información.

1. La persona Responsable de la Información determinará los requisitos de la información tratada, de conformidad con el artículo 13.2 del Real Decreto 311/2022, de 3 de mayo.

2. La persona Responsable de la Información será, para cada sistema de información, la persona titular del órgano administrativo, con rango inferior a Consejería, con competencia suficiente para decidir sobre la finalidad, el contenido, el uso y el tratamiento de la información contenida en aquél. Sus funciones serán las siguientes:

a) Determinará, junto con el Responsable del Servicio, las valoraciones de la información referidas en el artículo 40 del Real Decreto 311/2022, de 3 de mayo.

b) Realizará, junto con el Responsable de la Seguridad, los preceptivos análisis de riesgos, así como la evaluación de impacto relativa a la protección de datos, cuando sea precisa, con el asesoramiento, en su caso, del Delegado de Protección de Datos.

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

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

3. La persona Responsable de la Información para cada sistema de información, se corresponderá con el responsable de tratamiento, conforme a la definición del artículo 4.7 del Reglamento (UE) 2016/679 de 27 de abril.

Artículo 11. Responsable del Servicio.

1. La persona Responsable del Servicio determinará los requisitos de los servicios prestados, de conformidad con el artículo 13.2 del Real Decreto 311/2022, de 3 de mayo.

2. La persona Responsable del Servicio será, para cada sistema de información, la persona titular del órgano administrativo, con rango inferior a Consejería, con competencia suficiente para decidir sobre la finalidad y prestación del servicio que sustenta. Tendrá las siguientes funciones:

a) Determinará, junto con el Responsable de la Información, las valoraciones de la información referidas en el artículo 40 del Real Decreto 311/2022, de 3 de mayo.

b) Realizará, junto al Responsable de la Seguridad, los preceptivos análisis de riesgos.

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

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

e) En su caso, suspenderá 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 mínimos de seguridad establecidos.

Artículo 12. Responsable de la Seguridad.

1. La persona Responsable de la Seguridad será designada por quien sea titular de la Dirección General de la Agencia de Transformación Digital de la Región de Murcia entre personal adscrito a dicho organismo.

2. Conforme al principio de segregación de funciones, la persona Responsable de la Seguridad no abarcará funciones de administración o explotación de sistemas de información, o plataformas tecnológicas que los sustenten, concernidos por esta norma, limitándose a la gestión de los sistemas de información que requiera el desarrollo de sus funciones.

3. La persona Responsable de la Seguridad desarrollará las siguientes funciones:

a) Las recogidas en el Real Decreto 311/2022, de 3 de mayo, en relación con el Responsable de la Seguridad.

b) Las recogidas en el Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información para el Responsable de la seguridad de la información.

c) Determinar las decisiones para satisfacer los requisitos de seguridad de los sistemas de información.

d) Realizar auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información, promovidas por el Comité de Seguridad de la Información o por propia iniciativa.

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

f) Elaborar propuestas de normas, procedimientos e instrucciones técnicas de seguridad, así como Guías y Manuales de Seguridad conforme al artículo 14 de esta norma.

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, la persona titular de la Dirección General de la Agencia de Transformación Digital de la Región de Murcia podrá designar Responsables de la Seguridad Delegados que, bajo la dirección del Responsable de la Seguridad, ejercerán en su ámbito de actuación las funciones que aquel les delegue.

Artículo 13. Responsable del Sistema.

1. La persona Responsable del Sistema será designada para cada sistema de información por quien sea titular de la Dirección General de la Agencia de Transformación Digital de la Región de Murcia, entre personal adscrito a dicho organismo.

2. El Responsable del Sistema desarrollará las siguientes funciones:

a) Ejecutar las medidas de seguridad exigidas por la normativa vigente en materia de seguridad y las que determine el Responsable de la Seguridad.

b) Informar a las personas Responsables de la Información, del Servicio y de la Seguridad de cualquier cambio que conozca y pueda afectar a la seguridad del sistema de información.

c) En su caso, ejecutar, con el visto bueno de las personas Responsables de la Información, del Servicio y de la Seguridad, la suspensión del manejo de información o prestación de un servicio.

Artículo 14. Coordinador Operativo de la Seguridad.

1. La persona Coordinadora Operativa de la Seguridad será, para cada área de conocimiento o funcional, la persona designada entre su personal por quien sea titular de la Dirección General de la Agencia de Transformación Digital de la Región de Murcia.

2. La persona Coordinadora Operativa de la Seguridad asumirá, para su ámbito, las siguientes funciones:

a) Coordinar y supervisar, tanto en los servicios existentes como en los nuevos proyectos y contratos, la aplicación de las normas, procedimientos, instrucciones y guías de seguridad aplicables.

b) Ser punto de enlace para la resolución de incidencias y amenazas de seguridad.

c) Ser informado e informar a las personas Responsables de la Seguridad y del Sistema de cualquier cambio, anomalía, vulnerabilidad o compromiso relacionados con la seguridad.

Artículo 15. 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 la persona titular de la Dirección General de la Agencia de Transformación Digital de la Región de Murcia.

Capítulo III

Desarrollo, revisión y control del cumplimiento de la política de seguridad de la información

Artículo 16. Desarrollo de la política de seguridad de la información.

1. El cuerpo documental sobre seguridad de la información se desarrollará en niveles con diferente ámbito de aplicación y nivel de detalle técnico, de manera que cada documento de un determinado nivel de desarrollo se fundamente en los documentos de nivel superior. Dichos niveles de desarrollo, de mayor a menor nivel, son los siguientes:

a) Normas de seguridad. Definen qué hay que proteger y los requisitos de seguridad deseados. El conjunto de todas las normas de seguridad debe cubrir la protección de todos los entornos de los sistemas de información de la organización. Establecen un conjunto de expectativas y requisitos que deben ser alcanzados para poder satisfacer y cumplir cada uno de los objetivos de seguridad establecidos en la política.

b) Procedimientos de seguridad. Describen de forma concreta cómo proteger lo definido en las normas a las personas o grupos responsables de la implantación, mantenimiento y seguimiento de su nivel de cumplimiento. Son documentos que especifican, a alto nivel, cómo llevar a cabo las tareas habituales, quién debe hacer cada tarea y cómo identificar y reportar comportamientos anómalos.

c) Instrucciones técnicas de seguridad. Describen de forma detallada cómo abordar la implantación técnica por los distintos actores de lo definido en una parte de los procedimientos de seguridad.

d) Guías y Manuales de seguridad. Documentan aspectos de seguridad no contemplados en la normativa anterior.

2. Las normas de seguridad las aprueba la persona titular de la Dirección General de la Agencia de Transformación Digital de la Región de Murcia con el asesoramiento previo del Comité de Seguridad de la Información. Los procedimientos, instrucciones técnicas, guías y manuales los aprueba la persona titular de la Dirección General de la Agencia de Transformación Digital de la Región de Murcia.

3. La normativa de seguridad estará a disposición, según su perfil, de todos los miembros de la organización, y en particular, de aquellos que utilicen, operen o administren los sistemas de información. Adicionalmente, la normativa de seguridad de conocimiento general estará disponible en la intranet de la Administración Regional.

Artículo 17. Revisión de la política de seguridad de la información.

1. Las propuestas de modificación de la política de seguridad de la información, en su caso, serán aprobadas por la Consejería con competencia en materia informática.

2. La política de seguridad de la información deberá mantenerse actualizada permanentemente para adecuarla al progreso de los servicios de la administración electrónica, a la evolución tecnológica y a los estándares internacionales de seguridad.

Artículo 18. Concienciación y formación.

1. Los órganos competentes, en coordinación con el Comité de Seguridad de la Información, establecerán programas de concienciación con destino a los

empleados públicos y cualesquiera otras personas que desempeñen funciones o asuman responsabilidades públicas en el ámbito de la Administración regional, en particular a los de nueva incorporación.

2. Las personas con responsabilidad en el uso de los sistemas de información 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 como si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

Artículo 19. Obligaciones del personal.

1. Todos los empleados públicos y cualesquiera otras personas que desempeñen funciones o asuman responsabilidades públicas en el ámbito de la Administración Pública 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 informáticos aplicarán de forma inseparable a sus tareas y en el área de responsabilidad que les corresponda las normas de seguridad, los procedimientos y las instrucciones técnicas de seguridad vigentes en cada momento.

Artículo 20. Consecuencias del incumplimiento.

El incumplimiento de la política de seguridad o de su normativa de desarrollo, dará lugar al establecimiento por la Agencia de Transformación Digital de la Región de Murcia de las medidas preventivas y correctivas encaminadas a salvaguardar y proteger las redes y sistemas de información, sin perjuicio de la correspondiente exigencia, por el organismo competente, de responsabilidades disciplinarias.

Artículo 21. Terceras partes.

1. Cuando la Administración Regional preste servicios o ceda información a otras Administraciones Públicas, organismos o entidades del sector público, mediante los instrumentos jurídicos correspondientes, se les hará partícipes de esta política de seguridad de la información y de las normas que la desarrollan. Asimismo, se establecerán canales para el reporte y la coordinación entre la Administración Regional y terceros, así como procedimientos de actuación para la reacción ante ciberincidentes de seguridad.

2. Cuando la Administración utilice servicios de terceros o ceda información a terceros se les hará igualmente partícipes de esta política de seguridad de la información y de la normativa e instrucciones de seguridad que afecten a dichos servicios o información. Los terceros estarán sujetos a las obligaciones establecidas en la política de seguridad y en la normativa de seguridad que afecte 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 norma, que incluyan las cláusulas en las que se establezca la obligación de cumplir esta política y el sistema de verificación de su cumplimiento y de incluir un acuerdo de confidencialidad.

4. Cuando algún aspecto de la política de la seguridad de la información no pueda ser satisfecho por una tercera parte, se requerirá un informe vinculante del Responsable de la Seguridad que precise los riesgos en que se incurre y la forma

de tratarlos. Se requerirá la aprobación de este informe por los Responsables de la Información y de los Servicios afectados antes de seguir adelante.

Disposición transitoria única. Agencia de Transformación Digital de la Región de Murcia.

Hasta la puesta en funcionamiento efectivo de la Agencia de Transformación Digital de la Región de Murcia, las funciones atribuidas a esta serán desempeñadas por la Dirección General competente en materia informática.

Disposición derogatoria única. Derogación normativa.

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

Disposición final primera. Habilitación para la aplicación y la ejecución.

Se faculta al titular de la Dirección General de la Agencia de Transformación Digital de la Región de Murcia para adoptar las medidas que resulten necesarias para la aplicación y ejecución de esta norma.

Disposición final segunda. Entrada en vigor.

El presente decreto entrará en vigor a los veinte días de su publicación en el Boletín Oficial de la Región de Murcia.

Dado en Murcia, a 5 de junio de 2025.—El Presidente, Fernando López Miras.—El Consejero de Economía, Hacienda, Fondos Europeos y Transformación Digital, Luis Alberto Marín González.