PROYECTO DE ORDEN DE xx DE XXXXX DE XXX, DEL CONSEJERO DE ECONOMÍA, HACIENDA, Y EMPRESA 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.

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 en forma manual.

Los sistemas de información actuales, tienen una consideración estratégica, por lo que son activos a proteger de manera especial. El tamaño de los mismos, así como su altísima complejidad, hacen que ya no sean suficientes con las herramientas tradicionales que hasta ahora se han venido usando, sino que se requiere de 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. 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.

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, 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. 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.

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 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 viene a definir 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 organizar el cumplimiento con las nuevas obligaciones

normativas sobre protección de sistemas de información y de datos de carácter personal.

El acuerdo de Consejo de Gobierno mediante Acuerdo de 1 de agosto de 2018 designa a la Inspección General de Servicios 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 Directivas 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 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, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica e incorpora cambios que entre otros aspectos afectan a la valoración y categorización de los sistemas de información y por tanto a los roldes definidos en la Orden de 28 de marzo de 2017.

El Decreto-Ley n.º 5/2022, de 20 de octubre, de dinamización de inversiones empresariales, libertad de mercado y eficiencia pública se crea la Agencia de Transformación Digital de la Región de Murcia, 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.

La Agencia 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.

En virtud de lo expuesto,

Dispongo:

Artículo 1. *Objeto*.

El objeto de 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, establecer el reparto de funciones y responsabilidades en materia de seguridad de la información.

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 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 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 IV del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en el anexo del 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 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 y UNE-ISO/IEC 27002.

Artículo 4. *Sistemas de información que traten datos personales*

Cuando un sistema de información trate datos personales y estos sean competencia de la Agencia de Transformación Digital, esta desempeñará el rol de Encargado del Tratamiento recogido en el Reglamento General de Protección de Datos.

Artículo 5. *Principios básicos y requisitos mínimos*

Los organismos afectados por esta Orden aplicarán los Principios básicos y Requisitos mínimos descritos en el Capítulo II y III del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad conforme a lo establecido por la normativa en materia de seguridad de la información derivada de la aplicación de esta Orden o, en su defecto, por lo establecido por la Agencia de Transformación Digital.

Artículo 6. *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 y Servicio.
c) Responsable de Seguridad.
d) Responsables del Sistema.
e) Coordinador Operativo de la Seguridad.

Artículo 7. *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. Al Comité de Seguridad de la Información le corresponden las siguientes funciones:

a) Asesoramiento, consultoría y propuesta en materia de seguridad de la información.

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 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 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: La persona que ostente la dirección de la Agencia de Transformación Digital.

b) El/la Secretario/a será nombrado/a por el/la titular de la Agencia de Transformación Digital entre su personal.

c) Vocales:

i El/la Vicesecretario/a o equivalente de cada una de las Consejerías y Organismos Públicos de la Comunidad Autónoma de la Región de Murcia.

iii. Las personas responsables de Área de la Agencia de Transformación Digital.

vi. La persona Responsable de Seguridad de la Información.

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/las suplentes serán designados por el órgano superior respectivo.

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, dependientes funcionalmente del CSI, que serán responsables en su ámbito, de las actuaciones que se les deleguen.

Artículo 8. *Responsables de la Información y Servicio.*

1 La persona Responsable de la información y Servicio será, para cada sistema de información, la persona titular del órgano administrativo con competencia suficiente para decidir sobre la finalidad, contenido, uso y tratamiento de la información contenida en aquél, así como para decidir sobre la finalidad y prestación del servicio que sustenta.

2. A la persona Responsable de la Información y Servicio le corresponden las siguientes funciones:

a) Determinará las valoraciones de la información referidas en el artículo 40 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

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

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

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

e) En su caso, suspenderá, de acuerdo con el/la Responsable de la Información y el/la 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 9. *Responsable de Seguridad.*

1. La persona Responsable de Seguridad será designado por el/la titular de la Agencia de Transformación Digital entre personal adscrito a dicho órgano.

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

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

a) Las recogidas en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en relación con el Responsable de 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) Determinará las decisiones para satisfacer los requisitos de seguridad de los sistemas de información.

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

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 Orden.

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 10. *Responsable del Sistema.*

1. La persona Responsable del Sistema será designado para cada sistema de información por el/la titular de la Agencia de Transformación Digital entre personal adscrito a dicho órgano.

2. El Responsable del Sistema desarrollará las siguientes funciones:

a) La ejecución de las medidas de seguridad determinadas por la normativa que en materia de seguridad sean vigentes o, en su ausencia, las que determine el Responsable de Seguridad.

b) Informar a la persona Responsable de la Información y Servicio y de 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 la persona Responsable de la Información y Servicio y de Seguridad, la suspensión del manejo de información o prestación de un servicio.

Artículo 11 *Coordinador Operativo de la Seguridad*

1. La persona Coordinadora Operativa de la Seguridad será, para cada área de conocimiento y/o funcional la persona designada entre su personal por la Agencia de Transformación Digital.

2. La persona Coordinador/a Operativo/a 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) 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, compromiso o vulnerabilidad relacionada con la seguridad.

Artículo 12. *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 Agencia de Transformación Digital.

Artículo 13 *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 14. *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.

a) Las 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) Los procedimientos de seguridad. Describirán 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. Describirán de forma detallada cómo abordar la implantación técnica por los distintos actores 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 el/la Presidente/a del Comité de Seguridad de la información previo informe del Comité de Seguridad de la Información. Los procedimientos, instrucciones técnicas, guías y manuales las aprueba el/la Presidente/a del Comité de Seguridad de la información.

3. La normativa de seguridad estará a disposición, según su perfil, de todos los miembros de la organización, en particular para 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 CARM.

Artículo 15. *Concienciación y formación.*

Los órganos competentes, en coordinación con el Comité de Seguridad de la Información, establecerán programas de concienciación con destino a los miembros de la Administración Regional, en particular a los de nueva incorporación.

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 o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

Artículo 16. *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 17. *Consecuencias del incumplimiento.*

El incumplimiento de la Política de Seguridad o su normativa de desarrollo, dará lugar al establecimiento por Agencia de Transformación Digital 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 18. *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 las cláusulas 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 transitoria única. *Agencia de Transformación Digital.*

Hasta la entrada en funcionamiento efectivo de la Agencia de Transformación Digital 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 el desarrollo posterior.*

Se faculta al titular de la Agencia de Transformación Digital 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, a

EL CONSEJERO DE ECONOMÍA, HACIENDA Y EMPRESA

Fdo.

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.

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.

(Firmado y fechado electrónicamente al margen)

EL JEFE DE PLANIFICACIÓN INFORMÁTICA CORPORATIVA

Fdo. Manuel Frutos Mirete

EL SUBDIRECTOR GENERAL DE
INFRAESTRUCTURAS DIGITALES

Fdo.: Diego Pedro García García

EL DIRECTOR GENERAL DE INFORMÁTICA Y
TRANSFORMACIÓN DIGITAL

Fdo.: Javier Martínez Gilabert