7 diciembre 2018
Adecuado a informe de validación

Orden de <<dd>> de <<mmmm>> de <<yyyy>>, por la que se establece la Política de la Seguridad de las Tecnologías de la Información y las Comunicaciones de la Consejería de Turismo y Deporte.

Las leyes 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público configuran un escenario en el que la tramitación electrónica debe constituir la actuación habitual de las Administraciones tanto en el ámbito de su gestión interna como en el de las relaciones con la ciudadanía y entre ellas.

Concretamente, la Ley 39/2015, de 1 de octubre, establece el marco de relación entre las Administraciones Públicas y la ciudadanía a través de los medios electrónicos, determinando que, en sus relaciones con las Administraciones Públicas, las personas son titulares del derecho a la protección de datos de carácter personal y, en particular, a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas. Por su parte, la Ley 40/2015, de 1 de octubre, establece que las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas, garantizarán la protección de los datos de carácter personal y facilitarán preferentemente la prestación conjunta de servicios a los interesados.

El Estatuto de Autonomía para Andalucía, en su artículo 58.1.2.º, atribuye a la Comunidad Autónoma de Andalucía, en el marco de la legislación del Estado, competencias exclusivas sobre el régimen de las nuevas tecnologías relacionadas con la sociedad de la información y del conocimiento y, en su artículo 34, reconoce el derecho a acceder y usar las nuevas tecnologías y a participar activamente en la sociedad del conocimiento, la información y la comunicación, mediante los medios que la ley establezca. En este sentido, la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía, señala en su artículo 7.2 que los principios que rigen las relaciones que mantenga la Administración de la Junta de Andalucía con la ciudadanía y con otras Administraciones Públicas a través de redes abiertas de telecomunicación son los de simplificación y agilización de trámites, libre acceso, accesibilidad universal y confidencialidad en el tratamiento de la información, y de seguridad y autenticidad en orden a la identificación de las partes y el objeto de la comunicación.

Por otro lado, 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, modificado por el Real Decreto 951/2015, de 23 de octubre, determina los principios básicos y requisitos mínimos requeridos para una

protección adecuada de la información, estableciendo en su artículo 11 la obligación para los órganos superiores de las Administraciones Públicas de disponer de su Política de Seguridad, aprobada por el titular de dicho órgano. Dicha Política de Seguridad deberá ser coherente con lo establecido en 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 (en lo sucesivo Reglamento General de Protección de Datos) y en la legislación estatal vigente en materia de protección de datos personales.

En el ámbito de la Comunidad Autónoma de Andalucía, el cumplimiento de los requisitos y finalidades del ENS se ha configurado mediante el Decreto 1/2011, de 11 de enero, por el que se establece la Política de Seguridad de las TIC en la Administración de la Junta de Andalucía, modificado por el Decreto 70/2017, de 6 de junio, y la Orden de 9 de junio de 2016, por la que se efectúa el desarrollo de la Política de Seguridad TIC en la Administración de la Junta de Andalucía.

En la Consejería de Turismo y Deporte este marco de relación se cimenta sobre la consolidación del uso de las Tecnologías de la Información y las Comunicaciones (en adelante TIC), persiguiendo con ello la implantación de una administración electrónica, interconectada, transparente y confiable, capaz de agilizar procedimientos y reducir tiempos de tramitación. Para potenciar la confianza en dicha administración electrónica es necesario el establecimiento de un conjunto de actividades y procedimientos que permitan el tratamiento y gestión de los riesgos asociados a la seguridad de los medios tecnológicos que la conforman. Todo ello en el marco de las características técnicas y funcionales de la Red Corporativa de Telecomunicaciones de la Administración de la Junta de Andalucía, creada por el Acuerdo del Consejo de Gobierno de 2 de junio de 1998, y de los principales sistemas de información corporativos de las entidades que forman parte de la Administración de la Junta de Andalucía.

La aprobación de esta política implica el compromiso de la Consejería de Turismo y Deporte con la gestión de la seguridad TIC, definiendo con ella los principios y directrices del marco regulador que permita el tratamiento de la misma así como la estructura organizativa y de gestión que velará por su cumplimiento.

En la elaboración y tramitación de la presente Orden, se han tenido en cuenta los principios de buena regulación a los que se refiere el artículo 129.1 de la Ley 39/2015, de1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

En relación con los principios de necesidad y eficacia, la presente Orden se limita a desarrollar el mandato establecido en el artículo 10 del Decreto 1/2011, de 11 de enero; asimismo se cumple con el de proporcionalidad, no imponiendo más obligaciones a la ciudadanía ni a la Administración que las imprescindibles para asegurar una correcta aplicación de los principios de mejora regulatoria y regulando las figuras necesarias para el cumplimiento de la finalidad perseguida; sobre el de seguridad jurídica, se han tenido en cuenta todas las normas europeas, estatales y autonómicas de aplicación, estableciendo un marco regulador estable, predecible, integrado, claro y de certidumbre; acerca del de transparencia, podría

entenderse que este reglamento no se limita a estructurar y ordenar funcionalmente los órganos administrativos, no siendo un reglamento puramente organizativo, ya que no solo regula aspectos domésticos de la organización interna (STS 3754/2002, de 27 de mayo, haciéndose eco de una reiterada jurisprudencia). Por tanto, entendiendo que su carácter organizativo tiene un efecto hacia el exterior, se ha considerado facilitar la participación ciudadana a través del trámite de audiencia; y, por fin, es eficiente porque no sólo evita imponer cargas administrativas adicionales, sino que se limita a utilizar los recursos ya existentes para dar los servicios requeridos sin que suponga ningún incremento de gasto.

Como establece el artículo 5 de la Ley 12/2007, de 26 de noviembre, para la promoción de la igualdad de género en Andalucía, esta Orden integra el principio de igualdad de género de forma transversal en su elaboración para garantizar un impacto positivo en la igualdad de oportunidades entre mujeres y hombres.

En su virtud, en uso de las atribuciones conferidas por los artículos 44.2 de la¨Ley 6/2006 de 24 de octubre, del Gobierno de la Comunidad Autónoma de Andalucía, y 26.2 a) de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía, y conforme a lo establecido en el Decreto 212/2015, de 14 de julio, por el que se aprueba la estructura orgánica de la Consejería de Turismo y Deporte

DISPONGO

CAPÍTULO I

Disposiciones generales

Artículo 1. Objeto.

La presente Orden tiene como objeto definir y regular la Política de Seguridad Tecnologías de la Información y las Comunicaciones (en adelante TIC) de la Consejería de Turismo y Deporte que se ha de aplicar en el tratamiento de todos los activos TIC de su titularidad o cuya gestión tenga encomendada.

Artículo 2. Misión del organismo.

Corresponde a la Consejería de Turismo y Deporte las competencias atribuidas en el artículo 1 del Decreto 212/2015, de 14 de julio, por el que se aprueba la estructura orgánica de la Consejería de Turismo y Deporte.

Artículo 3. Definiciones.

A los efectos previstos en esta Orden las definiciones han de ser entendidas en el sentido indicado en el glosario de términos incluido como Anexo.

Artículo 4. Ámbito de aplicación.

1. La Política de Seguridad TIC regulada en la presente Orden será de aplicación en la Consejería de Turismo y Deporte, tanto a los órganos directivos centrales como a los periféricos de Turismo y Deporte, así como a sus entidades vinculadas o dependientes, y en todos los activos y sistemas que traten información de forma automatizada o no automatizada, tanto en soporte digital como en papel, de los que sea titular, tenga encomendada su gestión o sean usados para el ejercicio de las competencias que les son propias, obligando asimismo a todo el personal que acceda a los mismos y a la información tratada, con independencia de cuál sea su destino, adscripción o relación jurídica.

2. Sin perjuicio de lo anterior y de acuerdo con lo establecido por la regulación de la Política de Seguridad TIC de la Administración de la Junta de Andalucía, cada entidad vinculada o dependiente deberá contar con su propio documento de Política de Seguridad TIC aprobado por la persona titular de la entidad.

CAPÍTULO II

Objetivos, principios y marco regulador

Artículo 5. Objetivos y principios.

Se asumen los principios y objetivos establecidos en los artículos 4 y 5 del Decreto 1/2011, de 11 de enero, por el que se establece la Política de Seguridad de las TIC en la Administración de la Junta de Andalucía, circunscritos al ámbito competencial de los órganos contemplados en el ámbito de aplicación de esta norma.

Artículo 6. Marco regulador.

1. De conformidad con lo dispuesto por la disposición adicional primera del Decreto 1/2011, de 11 de enero, y sin perjuicio de cualquier otra normativa aplicable a esta Consejería en virtud de su naturaleza legal y sus competencias, el marco regulador de seguridad TIC se conformará por las siguientes disposiciones y documentos:

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

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

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

2. La Consejería de Turismo y Deporte podrá ampliar y desarrollar el marco regulador en los términos previstos en el artículo 21 de la presente Orden.

CAPÍTULO III

Organización de la Seguridad TIC

SECCIÓN 1.ª CUESTIONES GENERALES

Artículo 7. Cuestiones generales.

1. Un pilar básico en la gestión de la seguridad TIC es el establecimiento de una organización de seguridad que contemple las distintas funciones y responsabilidades existentes. La estructura organizativa que define la presente Orden contempla los siguientes bloques de responsabilidad:

a) Especificación de requisitos en materia de seguridad de la información.

b) Especificación de requisitos en materia de seguridad de los servicios.

c) Operación del sistema en base a las especificaciones de requisitos realizadas.

d) Supervisión del estado de la seguridad.

2. Se definirán una serie de perfiles que, respetando el principio básico de función diferenciada y con independencia de a qué persona o conjunto de personas se asignen, permitan cubrir las atribuciones que se derivan del conjunto de responsabilidades anterior.

3. Como proceso integral, la seguridad TIC ha de implicar a todas las áreas de la Consejería de Turismo y Deporte, debiendo estar presente en todos los ámbitos de su actividad.

SECCIÓN 2.ª ORGANIZACIÓN DE LA SEGURIDAD TIC EN LA CONSEJERÍA

Artículo 8. Estructura organizativa en la Consejería.

1. La organización para la gestión de la seguridad TIC en el ámbito de la Consejería de Turismo y Deporte se conforma mediante la siguiente estructura:

a) Comité de Seguridad TIC.

b) Unidad de Seguridad TIC.

c) Responsable de Seguridad y Responsable Delegado o Delegada de Seguridad.

d) Responsable de la Información y, en su caso, del Tratamiento.

e) Responsable del Servicio.

f) Responsable del Sistema.

g) Delegado o Delegada de Protección de Datos.

h) Otras responsabilidades.

2. En función de las necesidades y circunstancias de la organización, las funciones de algunas de estas figuras podrá recaer sobre una misma persona, unidad o departamento.

Artículo 9. Comité de Seguridad TIC.

1. Se crea el Comité de Seguridad TIC de la Consejería de Turismo y Deporte, en adelante Comité de Seguridad TIC, como órgano no colegiado, de dirección y seguimiento en materia de seguridad de los activos TIC de los que esta Consejería sea titular o cuya gestión tenga encomendada.

2. Conforme a lo expuesto en el artículo 3.3 de la Ley 12/2007, de 26 de noviembre, para la Promoción de la Igualdad de Género en Andalucía, la composición del Comité de Seguridad TIC deberá garantizar, en la medida de lo posible, la representación paritaria de mujeres y hombres, configurándose así:

a) Presidencia: La persona titular de la Viceconsejería, con voto de calidad en la toma de decisiones del Comité en caso de empate.

b) Vicepresidencia: La persona titular de la Secretaría General Técnica.

c) Vocalías:

1° La persona titular de cada órgano directivo central de la Consejería que tenga responsabilidad sobre algún sistema de información.

2° Una persona en representación de los órganos periféricos de Turismo y Deporte, designada por la persona titular de la Viceconsejería entre las distintas personas con el perfil Responsable Delegado de Seguridad en dicho órganos.

3° Las personas que ostenten los perfiles Responsable de Seguridad y Delegado o Delegada de Protección de Datos de la Consejería.

d) Secretaría: La persona titular de la jefatura del Servicio de Informática, con voz y voto, que convocará las reuniones y preparará el orden del día.

3. El Comité de Seguridad TIC podrá convocar a sus reuniones a las personas que en cada caso autorice

la Presidencia, por propia iniciativa o a propuesta de alguno de sus miembros. Asimismo, podrá recabar de personal técnico especializado, propio o externo, la información pertinente para la toma de decisiones.

4. Las funciones que le corresponden al Comité de Seguridad TIC son:

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

b) Velar por la disponibilidad de los recursos necesarios para desarrollar las iniciativas y planes estratégicos definidos, así como por los mecanismos para que todos los ámbitos de responsabilidad y actuación en relación a la gestión de la seguridad TIC queden perfectamente definidos y sean debidamente informados.

c) Nombrar los miembros de la Unidad de Seguridad TIC de la Consejería, así como a su responsable y proponer el nombramiento de la persona que ostentará el perfil de Delegado o Delegada de Protección de Datos de la Consejería.

d) Coordinar a alto nivel las actuaciones de seguridad TIC, velando para que la definición y el desarrollo de las mismas se adecuen en todo momento a las directrices marcadas por la Política de Seguridad TIC e involucrando a las diferentes áreas implicadas.

e) Elevar las propuestas de revisión de la Política de Seguridad TIC de la Consejería de Turismo y Deporte, o de revisión del marco regulador de seguridad TIC de la Junta de Andalucía, a los órganos competentes para su reglamentaria tramitación.

f) Aprobar la normativa de seguridad TIC de segundo nivel, según lo previsto en el artículo 21.

g) Establecer las directrices comunes y supervisar el cumplimiento de la normativa en materia de seguridad TIC en su ámbito.

h) Adoptar las medidas correctoras que correspondan derivadas de las conclusiones de las auditorías elaboradas por la Unidad de Seguridad TIC.

i) Promover la formación y concienciación en materia de seguridad TIC entre el personal de la Consejería de Turismo y Deporte.

j) Impulsar los preceptivos análisis de riesgos junto a la Unidad de Seguridad TIC y los perfiles Responsable de la Información, Responsable de Servicio y Delegado o Delegada de Protección de Datos. Para ello, se deberá impulsar la determinación de los niveles de seguridad de la información tratada, usando la valoración de los impactos que tendrían los incidentes que afectaran a la seguridad de la información.

k) Gestionar la aceptación, en su caso, de los riesgos residuales por sus responsables correspondientes respecto de la información y/o de los servicios de su competencia, obtenidos en el análisis de riesgos.

l) Monitorizar el desempeño del proceso de gestión de incidentes de seguridad TIC, así como la toma de decisiones en respuesta a incidentes de seguridad críticos.

m) Establecer los mecanismos necesarios para compartir la documentación del marco regulador con

el propósito de normalizarlo en todo el ámbito de aplicación y determinar los medios de difusión de la Política de Seguridad TIC.

n) Establecer los mecanismos necesarios de coordinación con los Comités de Seguridad TIC de las entidades vinculadas o dependientes de la Consejería de Turismo y Deporte.

o) Resolver los conflictos que puedan plantearse entre las diferentes personas responsables o entre diferentes áreas de la organización en materia de seguridad TIC.

p) Coordinar las medidas técnicas y organizativas establecidas en la normativa de protección de datos personales, de acuerdo con los correspondientes análisis de riesgos y, en su caso, las evaluaciones de impacto en la protección de datos, contando con el asesoramiento del Delegado o Delegada de Protección de Datos.

ñ) Realizar propuestas de necesidades de recursos que supongan la atención y dotación adecuada de los requerimientos de seguridad de los diferentes sistemas de información.

q) Cuantas otras le sean encomendadas.

Artículo 10. Funcionamiento y régimen jurídico del Comité de Seguridad TIC.

1. El Comité de Seguridad TIC se reunirá con carácter ordinario una vez al año y con carácter extraordinario cuando lo decida la Presidencia, por propia iniciativa o previa solicitud de alguno de sus miembros.

2. El Comité de Seguridad TIC se podrá constituir, convocar, celebrar sus sesiones, adoptar acuerdos y remitir actas, tanto de forma presencial como utilizando redes de comunicación a distancia, con las medidas adecuadas que garanticen la identidad de las personas comunicantes y la autenticidad de la información transmitida.

3. En caso de vacante, ausencia, enfermedad y en general cuando concurra una causa justificada, la persona titular de la Presidencia podrá ser sustituida por la titular de la Vicepresidencia. Tanto la Vicepresidencia como las Vocalías y la Secretaría podrán ser sustituidas por las personas suplentes que, al tiempo de su designación, se hayan determinado, debiendo recaer sobre personas que reúnan similares condiciones. En cualquier caso, se deberá contar con un régimen de suplencias para dar respuesta a estas situaciones.

4. El Comité de Seguridad TIC se regirá por esta Orden, por la normativa reguladora de la Política de Seguridad TIC en la Administración de la Junta de Andalucía, así como por el resto de normativa aplicable, como la reguladora del Esquema Nacional de Seguridad (en adelante ENS) y de la protección de datos de carácter personal.

Artículo 11. Unidad de Seguridad TIC.

1. La Unidad de Seguridad TIC, según lo establecido en el artículo 11.1 del Decreto 1/2011, de 11 de

enero, estará adscrita a la Secretaría General Técnica y deberá conformarse de acuerdo con el cumplimiento del principio de función diferenciada.

2. La Unidad de Seguridad TIC será nombrada o renovada por el Comité de Seguridad TIC, debiendo contar con una persona responsable.

3. Las funciones de la Unidad de Seguridad TIC serán:

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

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

c) Definición, implantación y mantenimiento de los controles de carácter organizativo para la protección de los datos, aplicaciones y sistemas, así como la realización, supervisión y mantenimiento de los análisis de riesgos de la Consejería y proponer las medidas necesarias para su tratamiento.

d) Revisión del análisis de riesgos de forma periódica, cuando existan cambios sustanciales en la información tratada y/o los servicios prestados, ocurra un incidente de seguridad grave o se reporten vulnerabilidades graves, elevando el correspondiente informe al Comité de Seguridad TIC.

e) Análisis de informes de auditorias, elevando al Comité de Seguridad TIC las conclusiones.

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

g) Definición y supervisión de los criterios y requisitos técnicos de seguridad aplicados en las distintas fases del ciclo de vida de los soportes, sistemas y aplicaciones de la Consejería por parte de los Servicios o Departamentos responsables de la prestación de los servicios TIC. Antes de la puesta en producción de nuevos sistemas de información o de evolutivos de los existentes, la Unidad de Seguridad TIC deberá evaluar los aspectos de seguridad y comunicar los posibles riesgos a las personas Responsables de la Información y Responsables de los Servicios correspondientes.

h) Elaboración de un informe cuando, en el marco de una relación establecida con un tercero, éste no pueda satisfacer algún aspecto de la Política, que precise los riesgos en que se incurre y la forma de tratarlos. Dicho informe requerirá la aceptación, en su caso, de las personas Responsables de la Información y Responsables de los Servicios afectados para continuar con la mencionada relación.

i) Definición y ejecución de los programas formativos y de concienciación relacionados con buenas prácticas de seguridad TIC en el ámbito de la Consejería, procurando promover la selección paritaria de mujeres y hombres entre las personas participantes.

j) Coordinación, dirección y seguimiento de la actividad en materia de seguridad TIC de las entidades vinculadas o dependientes de la Consejería, desde el momento que se tenga conocimiento de la aprobación de la Política de Seguridad TIC de dichas entidades.

k) Aplicación de los criterios y directrices de gestión de la seguridad TIC emanadas de la Unidad de

Seguridad TIC Corporativa.

l) Gestión de la documentación de seguridad TIC.

m) Y cuantas otras le sean encomendadas por el órgano directivo del que dependa funcional u orgánicamente.

4. La Unidad de Seguridad TIC elaborará y mantendrá un inventario de servicios y sistemas en el que se indiquen expresamente las personas u órganos que asumen las figuras de Responsable de la Información, Responsable del Servicio, Responsable del Sistema y Responsable de Seguridad.

Artículo 12. Responsable de Seguridad y Responsable Delegado o Delegada de Seguridad.

1. A tenor del artículo 11.3 del Decreto 1/2011, de 11 de enero, la persona responsable de la Unidad de Seguridad TIC de la Consejería ostentará la condición de Responsable de Seguridad con los deberes y responsabilidades que le asigna la normativa reguladora del ENS.

2. Cada órgano directivo periférico de Turismo y Deporte deberá contar con una persona Responsable Delegado o Delegada de Seguridad, designada por la persona titular de dicho órgano, contemplando el principio de función diferenciada.

3. La persona titular de la Viceconsejería nombrará de entre estas personas Responsable Delegado o Delegada de Seguridad un representante que formará parte como vocal del Comité de Seguridad TIC.

Artículo 13. Responsable de la Información y del Tratamiento. .

1. Será Responsable de la Información la persona con capacidad de decisión sobre la finalidad, contenido y uso de la información.

2. A los efectos previstos en el Reglamento General de Protección de Datos, el Responsable de la Información tendrá asimismo, respecto de los datos personales contenidos en la información incluida en su ámbito de actuación, la consideración de Responsable del Tratamiento.

3. Las funciones del Responsable de la Información serán:

a) Ayudar a determinar los requisitos de seguridad de la información, realizando una categorización de la información mediante la valoración del impacto de los incidentes que puedan producirse.

b) Proporcionar la información necesaria a la Unidad de Seguridad TIC para realizar los preceptivos análisis de riesgos, con la finalidad de establecer las salvaguardas a implantar. Para ello contará con la ayuda de los Responsables de los Servicios y de la persona Responsable del Sistema.

c) Aceptar, en su caso, los riesgos residuales de las informaciones tratadas que sean de su competencia identificados en el análisis de riesgos, y en particular los resultantes del informe al que se refiere el apartado 3.h) del artículo 11.

4. Cuando el Responsable de la Información ostente la condición de Responsable del Tratamiento, además de las funciones descritas en el apartado anterior, le corresponderá adoptar la decisión sobre la

creación del tratamiento, su finalidad, así como el contenido y uso de los datos tratados a lo largo de todo el ciclo de vida del tratamiento.

5. El nombramiento o renovación de esta responsabilidad recaerá en la persona titular del órgano directivo central o periférico, servicio administrativo con gestión diferenciada o, en su caso, órgano colegiado en cuyo ámbito de decisión se incluya la información tratada.

Artículo 14. Responsable del Servicio.

1. Será Responsable del Servicio la persona con capacidad de decisión sobre las características del servicio a prestar, teniendo en cuenta la categorización de la información usada por dicho servicio.

2. Las funciones del Responsable del Servicio serán:

a) Ayudar a determinar los requisitos de seguridad de los servicios, realizando una categorización de los servicios mediante la valoración del impacto de los incidentes que puedan producirse.

b) Proporcionar la información necesaria a la Unidad de Seguridad TIC para realizar los preceptivos análisis de riesgos, con la finalidad de establecer las salvaguardas a implantar. Para ello contará con la ayuda de los Responsables de la Información y de la persona Responsable del Sistema.

c) Aceptar, en su caso, los riesgos residuales de los servicios prestados que sean de su competencia identificados en el análisis de riesgos, y en particular los resultantes del informe al que se refiere el apartado 3.h) del artículo 11.

3. El nombramiento o renovación de esta responsabilidad recaerá en la persona titular del órgano directivo, central o periférico, o unidad organizativa en cuyo ámbito de decisión se incluya la determinación de las características del servicio a prestar.

Artículo 15. Responsable del Sistema.

1. Será Responsable del Sistema la persona con la responsabilidad de implantar, operar y mantener el sistema de información durante todo su ciclo de vida.

2. Las funciones del Responsable del Sistema serán:

a) Gestionar el sistema durante todo su ciclo de vida, desde la especificación del mismo a la instalación y seguimiento de su funcionamiento.

b) Velar porque la seguridad TIC esté presente en todas y cada una de las partes del ciclo de vida del sistema, contemplando que las directrices de seguridad establecidas de manera horizontal por la Junta de Andalucía se sigan en el desarrollo del sistema, de acuerdo con los criterios y requisitos técnicos de seguridad aplicables.

c) Asesorar en la definición de la topología y política de gestión del sistema, definiendo los criterios de uso y los servicios disponibles en el mismo.

d) Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.

e) Crear y gestionar la documentación de seguridad del sistema, con el asesoramiento de la Unidad de Seguridad TIC.

f) Aprobar la normativa de seguridad TIC de cuarto nivel, según lo previsto en el artículo 21.

g) Asesorar, en colaboración con la Unidad de Seguridad TIC, a los Responsables de la Información y a los Responsables de los Servicios en el proceso de análisis y la gestión de riesgos.

h) Investigar los incidentes de seguridad que afecten al sistema, y en su caso, comunicarlos al Responsable de Seguridad o a quién éste determine.

i) Suspender el tratamiento de cierta información o la prestación de un determinado servicio si detecta deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con la persona Responsable de la Unidad de Seguridad TIC y con las personas Responsable del Servicio y de la Información involucradas antes de ser ejecutada.

3. El nombramiento o renovación de esta responsabilidad recaerá sobre la persona titular de la jefatura del Servicio de Informática de la Consejería de Turismo y Deporte.

4. En caso de sistemas de información cuya implantación, operación y mantenimiento se lleve a cabo por terceras partes, la persona titular del órgano directivo bajo cuyo ámbito se establezca la relación con dichos terceros deberá comunicar los datos de la persona Responsable de Sistema correspondiente.

Artículo 16. Delegado o Delegada de Protección de Datos.

1. El Delegado o Delegada de Protección de Datos será el perfil garante, dentro de la Consejería de Turismo y Deporte, del cumplimiento de la normativa de protección de datos de carácter personal vigente en cada momento.

2. Este perfil de responsabilidad deberá asumirse por una persona funcionaria adscrita a la Consejería con un perfil especializado en derecho y de reconocida competencia en materia de protección de datos, de acuerdo con lo establecido en el Reglamento General de Protección de Datos.

3. El Delegado o Delegada de Protección de Datos desempeñará, además de las recogidas en la normativa reguladora de la materia, las siguientes funciones:

a) Informar y asesorar en la contratación, análisis, diseño, operación y mantenimiento de los tratamientos realizados sobre datos de carácter personal.

b) Velar por el cumplimiento de lo dispuesto en la normativa de protección de datos, contemplando aspectos como los siguientes:

1° Concienciar y formar al personal que participa en las operaciones de tratamiento.

2° Supervisar el deber de información y la gestión del Registro de Actividades de Tratamiento de la Consejería, debiendo facilitarle las diferentes personas Responsable del Tratamiento la información necesaria para ello.

3° Asesorar sobre la evaluación de impacto relativa a la protección de datos y supervisión de su

aplicación.

4º Establecer mecanismos de notificación a las partes interesadas de aquellos incidentes de seguridad que afecten a datos de carácter personal.

5º Cooperar con la autoridad de control correspondiente.

6º Supervisar las auditorías correspondientes.

4. El nombramiento o renovación de este perfil lo realizará la persona titular de la Viceconsejería a propuesta del Comité de Seguridad TIC.

Artículo 17. Otras responsabilidades.

1. La persona titular de la jefatura de servicio en materia de personal informará y notificará a todo el personal que ingrese en la Consejería de sus obligaciones respecto al cumplimiento del marco regulador de seguridad TIC. Deberá informar al Responsable de Seguridad sobre el grado de eficacia de implantación de esta medida y de los incidentes de seguridad que le competan en este ámbito.

2. Las personas titulares de las jefaturas de servicio, en el ámbito de sus competencias, verificarán y notificarán al Delegado o Delegada de Protección de Datos el cumplimiento normativo en relación a los datos de carácter personal que no se traten de forma automatizada y las medidas de seguridad física que correspondan.

3. Las personas titulares de las jefaturas de servicio responsables del área de contratación en los diferentes órganos directivos y unidades organizativas, deberán verificar y notificar a la persona Responsable de Seguridad TIC los aspectos de seguridad en relación a los contratos con terceras partes, velando por la inclusión de las clausulas necesarias para garantizar el cumplimiento de las medidas de seguridad implantadas.

4. La persona titular de la jefatura de servicio en materia jurídica, asesorará sobre las cuestiones legales que pudieran surgir durante el desarrollo regulador en el ámbito de la seguridad TIC, así como otras cuestiones relacionadas con las diferentes normativas que resulten de aplicación en cada momento.

Artículo 18. Resolución de conflictos.

1. En caso de conflicto entre las diferentes personas u órganos responsables de la estructura organizativa en el ámbito de la seguridad TIC, este será resuelto por el Comité de Seguridad TIC, debiendo contemplar siempre que prevalezca el mayor nivel de exigencia respecto a la seguridad.

2. En caso de conflicto entre los responsables de la estructura organizativa en el ámbito de la seguridad TIC y los responsables definidos en la normativa de protección de datos de carácter personal, este será resuelto por el Comité de Seguridad TIC, debiendo contemplar que prevalezca la decisión que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.

SECCIÓN 3.ª ORGANIZACIÓN DE LA SEGURIDAD TIC EN LAS ENTIDADES VINCULADAS O DEPENDIENTES

Artículo 19. Estructura organizativa en entidades vinculadas o dependientes.

1. De acuerdo con el artículo 6.2.c del Decreto 1/2011, de 11 de enero, la organización para la gestión de la seguridad TIC en las entidades vinculadas o dependientes de la Consejería de Turismo y Deporte se conforma mediante la siguiente estructura mínima:

a) Comité de Seguridad TIC.

b) Responsable de Seguridad TIC.

2. En función de las necesidades y circunstancias de la organización, las funciones de algunas de estas figuras podrá recaer sobre una misma persona, unidad o departamento.

3. La responsabilidad de la conformación y designación de estas figuras en las entidades vinculadas o dependientes recaerá sobre las propias entidades.

4. Las atribuciones del Comité de Seguridad TIC de las entidades vinculadas o dependientes podrán ser asumidas por el comité de dirección de la entidad.

5. Los nombramientos realizados para los distintos perfiles de la estructura organizativa de seguridad TIC en las entidades vinculadas o dependientes deberán comunicarse al Comité de Seguridad TIC de la Consejería de Turismo y Deporte.

CAPÍTULO IV

Gestión de la Seguridad TIC

Artículo 20. Directrices de seguridad.

Los principios básicos asumidos por la Política de Seguridad TIC de la Consejería de Turismo y Deporte se concretan en un conjunto de directrices particulares y responsabilidades específicas que se enmarcan en los siguientes ámbitos:

a) Tratamiento seguro de la información.

Los activos TIC de información deberán inventariarse asociando a cada uno de ellos los datos de la

persona responsable de los mismos y categorizarse de acuerdo a lo establecido por el ENS, en función de su sensibilidad y criticidad para el desarrollo de la actividad de la Consejería. Dicha categorización será la que determine el nivel de protección y las medidas a aplicar sobre el activo para garantizar la confidencialidad, la integridad y la disponibilidad de la información.

b) Tratamientos de datos de carácter personal.

Los tratamientos de datos de carácter personal que se efectúen en el marco de la actividad de los diferentes órganos directivos de la Consejería de Turismo y Deporte se ajustarán a lo dispuesto por el Reglamento General de Protección de Datos y la legislación relativa a esta materia vigente en cada momento.

La gestión de la seguridad de los datos de carácter personal se basará en la aplicación de las medidas técnicas y organizativas apropiadas teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines de los tratamientos realizados, los riesgos para los derechos y libertades de las personas físicas y el estado de la técnica y los costes de aplicación.

c) Acceso y uso de activos TIC.

Los criterios para un uso correcto, ordenado y seguro de los activos TIC que se ponen a disposición del personal que presta sus servicios bajo el ámbito de aplicación de esta Orden son de capital importancia para garantizar una óptima gestión de la seguridad. En el desarrollo de este ámbito se deberá contemplar lo dispuesto por las instrucciones y normas de carácter horizontal que regulen el comportamiento del personal empleado público en el uso de los sistemas informáticos y redes de comunicaciones de la Administración de la Junta de Andalucía.

d) Seguridad física y ambiental.

Los activos TIC se emplazarán en áreas seguras, protegidas mediante controles de acceso físicos acordes a su nivel de criticidad que impidan la interferencia humana, sea esta intencionada o accidental. Igualmente, se dispondrán medidas de protección contra factores externos y ambientales adversos.

e) Seguridad ligada al personal.

Todas las personas que presten servicios en la Consejería de Turismo y Deporte tendrán la obligación de conocer y cumplir la presente Política de Seguridad TIC y su normativa de desarrollo. Se implantarán los mecanismos necesarios para que cualquier persona que se incorpore a la Consejería o pueda acceder a alguno de sus activos TIC sea informado del marco regulador de seguridad aplicable y conozca sus responsabilidades, reduciendo de este modo el riesgo derivado de usos indebidos.

El incumplimiento manifiesto de la presente Política de Seguridad TIC o la normativa de seguridad derivada de ésta podrá acarrear el inicio de las medidas disciplinarias oportunas y, en su caso, las responsabilidades legales que correspondan.

Se dispondrán los medios necesarios para la articulación de iniciativas y actividades de formación y concienciación en seguridad TIC destinadas a lograr la adecuada capacitación de las personas empleadas

públicas de los órganos alcanzados por esta norma. Entre tales actividades se incluirán las de difusión de esta Política de Seguridad TIC y de su desarrollo regulador, las dirigidas a la prevención de amenazas o aquellas relativas a la protección de datos personales.

Las personas con responsabilidad en el uso, operación o administración de sistemas de información tendrán derecho a recibir formación para su uso seguro y a ser informados de sus deberes y obligaciones en materia de seguridad en la medida en que la necesiten para realizar su trabajo.

f) Control de acceso.

Se limitará el acceso lógico a los activos TIC de acuerdo a su criticidad, implantando para ello mecanismos de identificación, autenticación y autorización de usuarios en relación a las funciones que estos tengan permitidas, poniendo en práctica el principio de menor privilegio o de asignación solo de los privilegios de uso necesarios para el desempeño de las tareas encomendadas. Además, cuando sea necesario, se contemplará el registro de la utilización del sistema para asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la Consejería.

g) Seguridad en la gestión de comunicaciones y operaciones.

Se definirán los mecanismos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las TIC, supervisándose su estado y reportando incidencias. La información transmitida a través de redes de comunicaciones deberá protegerse de forma adecuada, teniendo en cuenta su nivel de sensibilidad y criticidad.

h) Planificación, desarrollo y mantenimiento de sistemas de información.

Los sistemas se diseñarán y configurarán de forma que la seguridad TIC se garantice por defecto y se contemple en todas las fases de su ciclo de vida, desde su planificación y diseño, pasando por las fases de desarrollo y mantenimiento y alcanzando hasta su retirada. Se contemplará la operativa que permita gestionar el conocimiento de la configuración de los sistemas así como las relaciones y conexiones entre ellos, lo que propiciará la planificación y gestión de su seguridad.

i) Gestión de incidentes de seguridad y de la continuidad.

Ante incidentes de seguridad TIC, el personal deberá actuar conforme a los mecanismos apropiados para su correcta identificación, registro y resolución, habilitando un sistema de gestión que permita la mejora continua de la seguridad del sistema.

En la gestión de los incidentes deberán integrarse aquellos procedimientos que establezca el órgano competente en materia de coordinación y ejecución de la Política de Seguridad TIC de la Administración de la Junta de Andalucía o el Comité de Seguridad TIC Corporativo de la Junta de Andalucía. Igualmente, la Consejería estará integrada en el grupo atendido por el Equipo de Respuesta a Incidentes de Seguridad Informática de la Junta de Andalucía, con el que coordinará su actuación ante incidentes.

Se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas y

mantener la continuidad de sus procesos, de acuerdo a las necesidades de nivel de servicio.

j) Relaciones con terceros.

Cuando la Consejería de Turismo y Deporte preste servicios a otros organismos o trate información de otros organismos, se les hará partícipes de esta Política de Seguridad TIC, estableciendo los mecanismos de coordinación entre las organizaciones y los procedimientos de actuación frente a incidentes de seguridad que procedan.

Cuando la Consejería de Turismo y Deporte utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad TIC y de la normativa de seguridad que aplique. Dicha tercera parte quedará sujeta, a través de cláusulas contractuales o acuerdos de nivel de servicio, a las obligaciones generales establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán mecanismos de comunicación y resolución de incidencias. Se deberá garantizar que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos, al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de esta Política de Seguridad TIC no pueda ser satisfecho por el tercero, la Unidad de Seguridad TIC realizará un informe que precise los riesgos en que se incurre y la forma de tratarlos, el cual deberá ser aprobado por los Responsables de la Información y de los Servicios afectados.

La Consejería podrá contar con la ayuda de terceros para mejorar sus sistemas de seguridad, mediante la contratación de auditorías, asistencias técnicas o desarrollos especializados.

Artículo 21. Desarrollo normativo de la seguridad TIC.

1. Las medidas contenidas en el cuerpo normativo de seguridad TIC son de obligado cumplimiento y se desarrollarán en cuatro niveles, según el ámbito de aplicación y nivel de detalle técnico, de manera que cada elemento de desarrollo se fundamente en el nivel superior. Todos los niveles deberán prestar especial atención a las exigencias derivadas del ENS, así como a la normativa de protección de datos de carácter personal vigente.

2. Los niveles de desarrollo normativo son los siguientes:

a) Primer nivel: Política de Seguridad TIC, aprobada mediante la presente Orden, y directrices y normas generales de seguridad TIC.

b) Segundo nivel: Normas de Seguridad TIC, que, centradas en un aspecto determinado, describen de forma general qué hay que proteger y en qué condiciones, estableciendo un conjunto de expectativas y requisitos de seguridad a concretar en niveles posteriores. El Comité de Seguridad TIC será quien apruebe las Normas de Seguridad TIC a propuesta de la Secretaría General Técnica.

c) Tercer nivel: Procedimientos de Seguridad, que describen explícitamente, paso a paso, cómo llevar a cabo un proceso definido en las normas de seguridad, asignando también las responsabilidades. La aprobación de los Procedimientos será realizada por la persona titular de la Secretaría General Técnica.

d) Cuarto nivel: Documentación Técnica, que incluye todo tipo de documentación especializada que se considere necesaria para completar y facilitar el desarrollo de las medidas de seguridad. La aprobación de la documentación de este nivel correrá a cargo de la persona Responsable del Sistema.

3. Además de los documentos que conforman los niveles anteriores, la documentación de seguridad TIC podrá contar con las guías e instrucciones que publiquen los centros expertos para la gestión de la seguridad de ámbito estatal y autonómico así como con otros documentos de carácter no vinculante, como pueden ser recomendaciones, informes, registros o evidencias electrónicas.

4. En virtud de los apartados 4 y 5 del artículo 2 de la Orden de 9 de junio de 2016, por la que se efectúa el desarrollo de la Política de Seguridad TIC en la Administración de la Junta de Andalucía, la Consejería podrá ampliar y desarrollar, sobre la base de los mínimos establecidos, su normativa de seguridad TIC.

5. La Unidad de Seguridad TIC será la encargada de la gestión de la documentación de seguridad TIC.

6. El Comité de Seguridad TIC establecerá los mecanismos necesarios para compartir la documentación del marco regulador con el propósito de normalizarlo, en la medida de lo posible, en todo el ámbito de aplicación.

Artículo 22. Gestión de riesgos.

1. La Consejería asume el compromiso de controlar los riesgos de seguridad y dar cumplimiento a la normativa vigente mediante un proceso continuo de gestión de riesgos. El establecimiento de dicho proceso seguirá las normas, guías y recomendaciones establecidas a tal efecto por el Centro Criptológico Nacional.

2. El proceso de gestión de riesgos comprende las fases de categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, que deberán ser proporcionales a los riesgos y estar justificadas.

3. Según lo dispuesto por el Reglamento General de Protección de Datos, en el análisis de riesgos también se deberán contemplar aquellos específicos de los tratamientos de datos de carácter personal.

4. Las personas encargadas de la categorización de los sistemas serán los Responsables de la Información y de los Servicios, siendo la Unidad de Seguridad TIC la responsable de supervisar los análisis de riesgos y proponer las medidas de seguridad necesarias para su tratamiento, pudiendo recabar para ello información y ayuda del Responsable del Sistema.

5. Los Responsables de la Información y de los Servicios son los responsables de aceptar los riesgos residuales calculados en el análisis y de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

6. La Unidad de Seguridad TIC revisará el análisis de riesgos con periodicidad anual o cuando existan cambios sustanciales en la información tratada y/o los servicios prestados, ocurra un incidente de seguridad grave o se reporten vulnerabilidades graves, elevando el correspondiente informe al Comité de Seguridad TIC.

Artículo 23. Auditorías de la seguridad.

1. Los sistemas de información serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos de la presente política, del ENS o de cualquier otra norma que así lo requiera. Con carácter extraordinario, se realizará dicha auditoría cuando existan cambios sustanciales en la información tratada y/o los servicios prestados, ocurra un incidente de seguridad grave o se reporten vulnerabilidades graves.

2. Los informes de auditoría quedarán a disposición del Comité de Seguridad TIC. Estos informes serán analizados por la Unidad de Seguridad TIC y elevará al Comité de Seguridad TIC las conclusiones que procedan para que éste adopte las medidas correctoras adecuadas.

Artículo 24. Cooperación con otros órganos y administraciones en materia de seguridad.

1. En atención a la mejora continua de la gestión de la seguridad TIC, se fomentará el establecimiento de mecanismos de comunicación con agentes especializados en esta materia, como pueden ser:

a) Comité de Seguridad TIC y Unidad de Seguridad TIC Corporativos de la Junta de Andalucía.

b) AndalucíaCERT: Equipo de Respuesta a Incidentes de Seguridad TIC de la Junta de Andalucía.

c) CCN-CERT: Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional.

d) INCIBE: Instituto Nacional de Ciberseguridad.

e) AEPD: Agencia Española de Protección de Datos.

f) Grupo de Delitos Informativos Informáticos y Telemáticos de la Guardia Civil y Brigada de Investigación Tecnológica del Cuerpo Nacional de Policía, para la investigación de acciones relacionadas con la delincuencia informática y los fraudes en el sector de las telecomunicaciones.

2. Adicionalmente, se mantendrán contactos con otros organismos de la Junta de Andalucía para compartir experiencias y ampliar conocimientos en esta materia.

Artículo 25. Actualización permanente y revisiones periódicas.

1. Esta Orden deberá mantenerse actualizada para adecuarla a la evolución tecnológica y al desarrollo de la sociedad de la información, así como a los estándares internacionales de seguridad.

2. Las revisiones de la Política de Seguridad TIC se harán a propuesta del Comité de Seguridad TIC.

Artículo 26. Difusión de la Política.

A los efectos de su mejor difusión entre el personal de la Consejería y de otras partes interesadas, la presente política de seguridad TIC se publicará y divulgará, además de en el Boletín Oficial de la Junta de Andalucía, a través de los medios que se establezcan por el Comité de Seguridad TIC.

Disposición adicional primera. Deber de colaboración de órganos y unidades de la Consejería.

Todos los órganos y unidades de la Consejería prestarán su colaboración en las actuaciones de implementación de la presente Política de Seguridad TIC.

Disposición adicional segunda. Habilitación para ejecución y desarrollo.

Se faculta a la persona titular de la Secretaría General Técnica de la Consejería para dictar cuantas instrucciones sean necesarias y adoptar cuantas medidas técnicas sean oportunas para la ejecución y desarrollo de la presente Orden.

Disposición derogatoria única. Derogación de normas.

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo establecido en la presente Orden y, en particular, la Orden de 26 de noviembre de 2014, de la Consejería de Turismo y Comercio, por la que se crea y regula la composición, atribuciones, funcionamiento y método de trabajo del Comité de Seguridad TIC.

Disposición final única. Entrada en vigor.

La presente Orden entrará en vigor el día de su publicación en el Boletín Oficial de la Junta de Andalucía.

ANEXO

Glosario de términos y abreviaturas.

Activo TIC: cualquier medio, de naturaleza física, lógica o humana, que interviene en los sistemas de información y en las redes de comunicaciones, incluyendo: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

Amenaza: circunstancia o evento con potencial para causar daño a un determinado activo TIC.

Autenticidad: propiedad que permite asegurar que quien accede y usa un activo es realmente quien afirma ser.

Confidencialidad: propiedad de un activo para no ponerse a disposición o ser revelado a usuarios no autorizados.

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

Disponibilidad: propiedad de un activo para estar accesible y utilizable en el momento que se requiera por los usuarios con autorización.

Gestión de riesgos: proceso para identificar, analizar y responder a los factores de riesgo que pueden afectar al correcto desarrollo de la actividad de una organización.

Impacto: daño causado por una amenaza que se ha materializado cobre un activo.

Incidente de seguridad TIC: suceso, accidental o intencionado, a consecuencia del cual se ve afectada la integridad, confidencialidad o disponibilidad de los activos sobre los que impacta.

Integridad: propiedad de un activo que permite asegurar que no se ha alterado de manera no autorizada.

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

Política de seguridad TIC: documento escrito que plasma el conjunto de directrices que han de regir la forma en que una organización gestiona y protege sus activos TIC.

Redes de comunicación: Infraestructura formada por medios, tecnologías y protocolos que facilita el intercambio de información entre los usuarios.

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

Seguridad TIC: capacidad de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes y las acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad de los datos almacenados o transmitidos y de los

servicios prestados.

Servicio: función desempeñada para cuidar intereses o satisfacer necesidades de la ciudadanía.

Sistema de información: conjunto organizado de activos TIC que, interactuando entre sí, permite el tratamiento de la información y la prestación de algún tipo de servicio.

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

Trazabilidad: propiedad que permite asociar de modo inequívoco a un usuario las acciones realizadas sobre un activo.

Usuario: todo proceso o persona física con acceso autorizado a los sistemas de información o redes de comunicaciones de la organización.

Vulnerabilidad: debilidad inherente de un activo que puede ser aprovechada por una amenaza para dañarlo.