SALIDA
JUNTA DE ANDALUCIA
CONSEJERÍA DE EMPLEO, EMPRESA Y COMERCIO
27 SET. 2018
7000 / 16242
Registro General 5.66
Dirección General de Telecomunicaciones y Sociedad de la Información
Fecha: la de firma

JUNTA DE ANDALUCIA

CONSEJERÍA DE EMPLEO, EMPRESA Y COMERCIO
Dirección General de Telecomunicaciones y Sociedad de la Información

CONSEJERÍA DE CONOCIMIENTO, INVESTIGACIÓN Y UNIVERSIDAD.

SECRETARÍA GENERAL TÉCNICA.

C/. Johannes Kepler, 1
Isla de la Cartuja
41092 - Sevilla

RECEPCIÓN
JUNTA DE ANDALUCIA
CONSEJERÍA DE CONOCIMIENTO, INVESTIGACIÓN Y UNIVERSIDAD
28 SEP. 2018
Registro General Servicios Centrales 3.4
707
Sevilla
Hora

N. ref: MOB /ATV

S. ref: SCR / FFG

Asunto: Respuesta a solicitud de informe (expte. 37/2018)

Tras recibir su escrito de fecha 10 de agosto de 2018 solicitando, en base a lo establecido en la Instrucción 2/2016, de 11 de febrero, de la Viceconsejería de Economía y Conocimiento (actualmente Conocimiento, Investigación y Universidad), por la que se establece el procedimiento para la elaboración de disposiciones de carácter general, acuerdos del Consejo de Gobierno, convenios de colaboración y otros procedimientos administrativos en el ámbito de esa Consejería, que se emita por este órgano directivo informe con carácter facultativo sobre el contenido del Proyecto de Orden por la que se establece la política de seguridad de las tecnologías de la información y comunicaciones de la Consejería de Conocimiento, Investigación y Universidad, este Centro Directivo le cabe indicar que:

El apartado 1.b) del artículo 45 de la Ley 6/2006, de 24 de octubre, del Gobierno de la Comunidad Autónoma de Andalucía, dicta que

> "b) A lo largo del proceso de elaboración deberán recabarse, además de los informes, dictámenes y aprobaciones preceptivos, cuantos estudios y consultas se estimen convenientes para garantizar el acierto y la legalidad de la disposición".

El Decreto 210/2015, de 14 de julio, por el que se regula la estructura orgánica de la Consejería de Empleo, Empresa y Comercio, establece entre las competencias de la Dirección General de Telecomunicaciones y Sociedad de la Información la coordinación y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones de la Administración de la Junta de Andalucía.

Por otra parte, el Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía (modificado por el Decreto 70/2017, de 6 de junio), establece que 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 contará con una Unidad de Seguridad TIC Corporativa, cuyas funciones se asignarán a una unidad administrativa con nivel orgánico mínimo de Servicio, y cuyas atribuciones son:

a) Labores de soporte, asesoramiento e información al Comité de Seguridad TIC de la Junta de Andalucía y su Grupo de Respuesta a Incidentes TIC, así como de ejecución de las decisiones y acuerdos adoptados.

Código Seguro de verificación:eY4xB2ynA5L3KOAoaov1Zg==. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: https://www.juntadeandalucia.es/economiainnovacionyciencia/verifirma2
Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMADO POR	MANUEL ORTIGOSA BRUN		FECHA	26/09/2018
ID. FIRMA	ws029.juntadeandalucia.es	eY4xB2ynA5L3KOAoaov1Zg==	PÁGINA	1/4

eY4xB2ynA5L3KOAoaov1Zg==

b) Diseño y ejecución de los programas de actuación de carácter horizontal, así como la dirección de los proyectos y servicios corporativos de seguridad TIC.

c) Desarrollo, mantenimiento y supervisión del marco regulador de seguridad TIC.

d) Generación y supervisión de criterios y directrices corporativas de gestión de la seguridad TIC.

e) Recogida sistemática de información y supervisión del estado de las principales variables de seguridad TIC de la Administración de la Junta de Andalucía, mediante el reflejo, cuando proceda, de los datos referidos a personas desagregados por sexo.

f) Coordinación y seguimiento de la actividad de las Unidades de Seguridad TIC de las Consejerías.

g) Realización de los procedimientos de compra centralizada de productos y servicios corporativos de seguridad TIC a propuesta del Comité de Seguridad TIC en aquellos supuestos en que se determine su conveniencia en razón a criterios de oportunidad, eficacia y de economías de escala.

h) Realización de auditorías técnicas y de cumplimiento normativo, en aquellos supuestos en que se determine su conveniencia en razón a criterios de oportunidad, eficacia, eficiencia y de economías de escala.

i) Representación de la Administración de la Junta de Andalucía ante los foros y agentes de relevancia del sector.

j) Coordinación del Grupo de Personas Expertas en Seguridad TIC.

k) Y cuantas otras le sean encomendadas por la Dirección General competente en materia de coordinación y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones.

El Decreto 1/2011, de 11 de enero también establece en su artículo 10, entre otros aspectos, que

1. Sin perjuicio de las directrices establecidas en el marco regulador de seguridad TIC de la Administración de la Junta de Andalucía, cada Consejería y entidad incluida en el ámbito de aplicación del presente Decreto deberá disponer formalmente de su propio documento de política de seguridad TIC, así como de las disposiciones de desarrollo que adecuen, en su caso, las directrices comunes de la Administración de la Junta de Andalucía a sus particularidades. Asimismo, cada Consejería y entidad deberá contar con un Comité de Seguridad TIC, que no tendrá carácter colegiado y que actuará como órgano de dirección y seguimiento en materia de seguridad de los activos TIC de su titularidad o cuya gestión tenga encomendada.

2. El documento de política de seguridad TIC será aprobado por la persona titular de la Consejería o entidad correspondiente y se plasmará en los términos descritos en el Real Decreto 3/2010, de 8 de enero, debiendo hacer referencia y ser coherente con lo establecido en el documento de

Código Seguro de verificación:eY4xB2ynA5L3KOAoaov1Zg==. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: https://www.juntadeandalucia.es/economiainnovacionyciencia/verifirma2
Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMADO POR	MANUEL ORTIGOSA BRUN		FECHA	26/09/2018
ID. FIRMA	ws029.juntadeandalucia.es	eY4xB2ynA5L3KOAoaov1Zg==	PÁGINA	2/4

eY4xB2ynA5L3KOAoaov1Zg==

seguridad que exige el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, aprobado por el Real Decreto 1720/2007, de 21 de diciembre.

3. El documento de política de seguridad TIC de las Consejerías y sus documentos complementarios también serán de obligado cumplimiento para sus entidades vinculadas o dependientes.

4. El documento de política de seguridad TIC deberá recoger la composición, atribuciones, y funcionamiento del Comité de Seguridad TIC y del resto de perfiles con responsabilidad en seguridad, incluyendo, en su caso, los recogidos en el Real Decreto 3/2010, de 8 de enero, definiendo para cada uno de ellos, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.

De los artículos citados y las atribuciones asignadas por los mismos se puede determinar que la aprobación del documento de política de seguridad no requiere de un informe preceptivo por parte de este Centro Directivo ni de la Unidad de Seguridad TIC Corporativa.

En base a lo anterior, y al inciso "cuantos estudios y consultas se estimen convenientes para garantizar el acierto y la legalidad de la disposición" del apartado 1.b) del citado artículo 45 de la Ley 6/2006, de 24 de octubre, se pueden apuntar desde este Centro Directivo las siguientes apreciaciones:

1. No se encuentran incompatibilidades entre el texto del Proyecto de Orden y lo establecido por, por una parte, 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 y, por otra, por el Decreto 1/2011, de 11 de enero, modificado por el Decreto 70/2017, de 6 de junio.
2. Con respecto al artículo 5.6, debe tenerse en cuenta que la Resolución de 27 de septiembre de 2004, de la Secretaría General para la Administración Pública, por la que se establece en manual de comportamiento de los empleados públicos en el uso de los sistemas de información y redes de comunicaciones de la Junta de Andalucía se encuentra en proceso de revisión.
3. Se recomienda incluir en el artículo 7 alguna referencia a la gestión de riesgos derivada de los tratamientos de datos de carácter personal:

   " ...Para ello, deben implementar las medidas mínimas de seguridad determinadas por el ENS así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos que cumpla los requisitos del ENS y del RGPD..."
4. Los artículos 26 y 27 son validos pero tienen el peligro de quedar anticuados ante cualquier cambio en los articulados del ENS por lo que se recomienda que estos artículos hagan referencia directa al contenido del ENS.

Código Seguro de verificación:eY4xB2ynA5L3KOAoaov1Zg==. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: https://www.juntadeandalucia.es/economiainnovacionyciencia/verifirma2
Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMADO POR	MANUEL ORTIGOSA BRUN		FECHA	26/09/2018
ID. FIRMA	ws029.juntadeandalucia.es	eY4xB2ynA5L3KOAoaov1Zg==	PÁGINA	3/4

eY4xB2ynA5L3KOAoaov1Zg==

5. Sería conveniente hacer que el artículo 30 incluya también en su alcance al personal externo de la consejería, posiblemente con una redacción como "Todas las personas que prestan servicios en la Consejería ...".
6. Sería conveniente añadir el contenido de los artículos 11 (Resolución de conflictos) y 21 (Difusión de la política de seguridad) incluidos en el borrador de política de seguridad TIC elaborado por la Oficina de Apoyo a la Seguridad TIC, que se adjunta a este escrito.

EL DIRECTOR GENERAL DE TELECOMUNICACIONES Y SOCIEDAD DE LA INFORMACIÓN

Código Seguro de verificación:eY4xB2ynA5L3KOAoaov1Zg==. Permite la verificación de la integridad de una copia de este documento electrónico en la dirección: https://www.juntadeandalucia.es/economiainnovacionyciencia/verifirma2
Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMADO POR	MANUEL ORTIGOSA BRUN		FECHA	26/09/2018
ID. FIRMA	ws029.juntadeandalucia.es	eY4xB2ynA5L3KOAoaov1Zg==	PÁGINA	4/4

eY4xB2ynA5L3KOAoaov1Zg==

PROTOTIPO DE POLÍTICA DE SEGURIDAD

(el contenido siguiente será adaptado por cada organización a sus necesidades especificas, modificando los aspectos que procedan en cada caso)

ORDEN DE XX DE XX DE 2018, POR LA QUE SE ESTABLECE LA POLÍTICA DE SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DE <ORGANISMO>.

(Preámbulo o introducción: elegir entre OPCIÓN 1 y OPCIÓN 2)

OPCIÓN 1. Añadir un texto que cubra, entre otros posibles, los siguientes aspectos:

- Situación de la Administración Pública ante el entorno de las TIC
- Trayectoria llevada hasta el momento en la gestión de la seguridad TIC
- Justificación de la necesidad del presente documento de política de seguridad TIC y la legislación aplicable
- Referencia a objetivos perseguidos, criterios básicos, etc., en relación con la legislación de referencia en materia de seguridad TIC
- Planteamiento para el cuerpo normativo en materia de seguridad emanado del documento de política
- En su caso, "Dispongo" por parte del titular del organismo, aludiendo al Decreto de estructura del mismo.

OPCIÓN 2: se indica un ejemplo de posible texto para este primer apartado

Los avances tecnológicos en los ámbitos de la informática, las telecomunicaciones y de la sociedad de la información son ya un hecho consolidado, que afecta no sólo a la sociedad sino también a los poderes públicos. Son los poderes públicos los responsables de generar confianza en el uso por parte de la ciudadanía de los medios tecnológicos en sus relaciones con la Administración Pública. Para conseguir esta confianza, los medios tecnológicos utilizados deben ser seguros y para ello se debe garantizar la confidencialidad, integridad y disponibilidad de los sistemas, de las comunicaciones y de los servicios telemáticos, permitiendo tanto a la ciudadanía, los profesionales y las empresas, como a las Administraciones Públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

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 vienen a configurar un escenario en el que la tramitación electrónica debe constituir la actuación habitual de las Administraciones en sus múltiples vertientes de gestión interna, de relación con los ciudadanos y de relación de aquellas entre sí.

En concreto, la La Ley 39/2015, de 1 de octubre, tiene como uno de sus objetivos centrales regular las relaciones entre las Administraciones y los ciudadanos y empresas, teniendo en cuenta el desarrollo de las tecnologías de la información y comunicación de los últimos años y cómo este afecta a las relaciones entre estos agentes. Pretende implantar una Administración totalmente electrónica, interconectada y transparente, mejorando la agilidad de los procedimientos administrativos y reduciendo los tiempos de

tramitación. Por su parte, la Ley 40/2015, de 1 de octubre, procura dotar a nuestro sistema legal de una norma comprensiva del régimen jurídico de las Administraciones Públicas, regulando el funcionamiento interno de cada Administración y de las relaciones entre ellas.

El Estatuto de Autonomía para Andalucía, en su artículo 34, reconoce el derecho a acceder y usar las nuevas tecnologías y a participar activamente en la sociedad del conocimiento, la información y la comunicación, mediante los medios y recursos que la ley establezca. Asimismo, el artículo 58.1.2.° atribuye a la Comunidad Autónoma de Andalucía competencias exclusivas sobre el régimen de las nuevas tecnologías relacionadas con la Sociedad de la Información y del Conocimiento, en el marco de la legislación del Estado.

Por otro lado, la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía, señala en su artículo 7.2 que los principios que rigen las relaciones que mantenga la Administración de la Junta de Andalucía con la ciudadanía y con otras Administraciones Públicas a través de redes abiertas de telecomunicación son los de simplificación y agilización de trámites, libre acceso, accesibilidad universal y confidencialidad en el tratamiento de la información, y de seguridad y autenticidad en orden a la identificación de las partes y el objeto de la comunicación. Para ello establece que estos sistemas deben cumplir con el requisito de existencia de medidas de seguridad que eviten la interceptación y alteración de las comunicaciones, así como los accesos no autorizados. En este mismo texto legal se abunda en materia de seguridad señalándose que los medios o soportes en que se almacenen los documentos electrónicos contarán con las medidas de seguridad que garanticen la integridad, protección y conservación de los documentos almacenados, así como la identificación de las personas usuarias y el control de acceso de los mismos.

Para el desarrollo de esta Política de seguridad de las tecnologías de la información y las comunicaciones se ha seguido lo dispuesto en: el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS) y su modificación mediante Real Decreto 951/2015, de 23 de octubre; el Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía y su modificación mediante el Decreto 70/2017, de 6 de junio; la Orden de 9 de junio de 2016, por la que se efectúa el desarrollo de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.

Adicionalmente, se tienen en cuenta en esta Política de Seguridad los aspectos de seguridad digital requeridos por 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 y en la legislación estatal vigente en materia de protección de datos personales (en adelante, RGPD).

[Opcional 1, si <ORGANISMO> es operador de infraestructuras críticas] Al estar <ORGANISMO> en el ámbito subjetivo de aplicación de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y de su correspondiente Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas, se han tenido en cuenta los preceptos requeridos por dichas normas.

[Opcional 2, si <ORGANISMO> está obligado como Organismo Pagador a implantar un sistema de gestión de seguridad de la información] Al estar <ORGANISMO> obligado por el Reglamento Delegado (UE) N°

907/2014 de la Comisión, de 11 de marzo de 2014, que completa el Reglamento (UE) n.° 1306/2013 del Parlamento Europeo y del Consejo en lo relativo a los organismos pagadores y otros órganos, la gestión financiera, la liquidación de cuentas, las garantías y el uso del euro, se ha tenido en cuenta en el desarrollo de esta Política de Seguridad lo dispuesto en el Anexo I, apartado 3.B de dicho Reglamento Delegado.

[Opcional 3, a fecha de redacción de este modelo de Política de Seguridad se está tramitando la norma de transposición de 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, que puede tener impacto sobre <ORGANISMO> si éste es operador de servicios esenciales]

En la elaboración de esta política de seguridad, asimismo, se han tenido en cuenta el contexto 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.

Esta política de seguridad establece el compromiso de <ORGANISMO> con la seguridad de los sistemas de información, define los objetivos y criterios básicos para el tratamiento de la misma, sienta los pilares del marco normativo de seguridad en este organismo y la estructura organizativa y de gestión que velará por su cumplimiento.

Por otra parte, de acuerdo con el artículo 5 de la Ley 12/2007, de 26 de noviembre, para la promoción de la igualdad de género en Andalucía, esta norma integra el principio de igualdad de género de forma transversal en su elaboración, garantizando con ello un impacto positivo en la igualdad de oportunidades entre mujeres y hombres.

En su virtud, conforme a lo establecido en <indicar norma que establece la estructura orgánica de ORGANISMO>

DISPONGO

Artículo 1. Objeto

La presente Orden tiene por objeto definir y regular la política de seguridad TIC de <ORGANISMO>, que se ha de aplicar en el tratamiento de los activos de tecnologías de la información y comunicaciones de su titularidad o cuya gestión tenga encomendada.

Artículo 2. Ámbito de aplicación

La Orden será de aplicación a <ORGANISMO>, tanto a sus servicios centrales como periféricos y a sus entidades vinculadas o dependientes. También será de aplicación para todo el personal que acceda a los sistemas

de información como a la propia información que sea gestionada por <ORGANISMO>, con independencia de cuál sea su destino, adscripción o relación con la misma.

Artículo 3. Objetivos, principios y definiciones

Se asumen los principios, objetivos y deficiones establecidos en los artículos 2, 4 y 5 del Decreto 1/2011, de 11 de enero, circunscritos al ámbito competencial de los órganos contemplados en el ámbito de aplicación de esta norma.

Artículo 4. Contexto tecnológico y responsabilidad general

1. <ORGANISMO> depende de forma significativa de las Tecnologías de la Información y las Comunicaciones (TIC) para alcanzar sus objetivos. En consecuencia, éstas deben ser administradas con diligencia, tomando las medidas adecuadas para protegerlas frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

2. La preservación de la seguridad TIC será considerada objetivo común de todas las personas al servicio de los órganos contemplados en el ámbito de aplicación de esta norma, siendo éstas responsables del uso correcto de los activos TIC puestos a su disposición.

3. Todas las personas que presten servicios a <ORGANISMO> tienen la obligación de conocer y cumplir, en sus respectivos ámbitos de actuación, la presente política de seguridad, así como la normativa de seguridad que emana de la misma, siendo responsabilidad del Comité de Seguridad de <ORGANISMO> de disponer los medios necesarios para que la información llegue a los interesados.

4. Con carácter general, para el personal de <ORGANISMO>, regirán las normas de uso de los recursos TIC previstas en la Resolución de 27 de septiembre de 2004, de la Secretaría General para la Administración Pública, por la que se establece el manual de comportamiento de los empleados públicos en el uso de los sistemas informáticos y redes de comunicaciones de la Administración de la Junta de Andalucía, o en la normativa de carácter horizontal vigente en cada momento.

5. Las normas de uso de los recursos TIC serán trasladadas convenientemente, en la medida en que pueda resultar necesario o recomendable, al clausulado de los contratos suscritos por <ORGANISMO>.

Artículo 5. Marco normativo

1. Se asume como marco normativo general el que en cada momento se defina, en virtud de la Disposición adicional primera del Decreto 1/2011, de enero, por la la Consejería competente en materia de coordinación y

ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones, a propuesta del Comité de Seguridad TIC de la Junta de Andalucía. Todo ello sin perjuicio de otra normativa aplicable a este organismo en virtud de su naturaleza legal y sus competencias.

2. <ORGANISMO> podrá ampliar y desarrollar el marco normativo en los términos previstos en el artículo 14 de esta Orden.

Artículo 6. Estructura organizativa de la seguridad TIC

1. La gestión de la seguridad de la información en un organismo va íntimamente ligada al establecimiento de una organización de seguridad. Dicha organización se establece mediante la identificación de las diferentes actividades y responsabilidades en materia de gestión de la seguridad y mediante su asignación formal a los agentes que correspondan, con arreglo al principio de básico de función diferenciada recogido tanto en el ENS como en la política de seguridad TIC de la Junta de Andalucía.

2. Atendiendo a dicho principio, la estructura que se define en este documento diferencia tres grandes bloques de responsabilidad: a) la especificación de las necesidades y requisitos en materia de seguridad de la información; b) el desarrollo y/o explotación del sistema de información y c) la función de supervisión de la seguridad del sistema de información. En este sentido, los distintos bloques de responsabilidad mencionados quedarán distribuidos convenientemente, conforme a lo estipulado en el articulado subsiguiente de esta Orden, sobre los distintos agentes integrantes de la siguiente ...

(elegir entre OPCIÓN 1 y OPCIÓN 2)

OPCIÓN 1: En caso de caso de Consejerías/SAS/SAE ...

... estructura organizativa a dos niveles:

a) En <ORGANISMO> propiamente:

i. Comité de Seguridad TIC.

ii. Responsables de la información

iii. Responsables de los servicios

iv. Unidad de Seguridad TIC

v. Responsable de Seguridad

vi. Responsable del Sistema

b) En cada una de las entidades vinculadas o dependientes:

i. Comité de Seguridad TIC.

ii. Responsables de la información

iii. Responsables de los servicios

iv. Responsable de Seguridad

v. Responsable del Sistema

OPCIÓN 2: En caso de entidades vinculadas o dependentes ...
... estructura organizativa:

i. Comité de Seguridad TIC.

ii. Responsables de la información

iii. Responsables de los servicios

iv. Responsable de Seguridad

v. Responsable del Sistema

3. Dependiendo de las necesidades y circunstancias de la organización, en ciertos casos, la función de algunos de estos agentes podrá recaer sobre una misma persona, unidad o departamento.

(añadir el punto 4 sólo en el caso de Consejerías/SAS/SAE ...)

4. Con sujeción al marco previsto por el ENS, por la normativa en materia de protección de datos, por la política de seguridad TIC de la Junta de Andalucía y por su normativa de desarrollo, en las entidades vinculadas o dependientes de <ORGANISMO> la responsabilidad de la conformación y designación de estas figuras, recaerá sobre las propias entidades vinculadas o dependientes.

Artículo 7. Comité de Seguridad TIC de <ORGANISMO>

1. Se crea el Comité de Seguridad TIC de <ORGANISMO> como órgano no colegiado de dirección y seguimiento en materia de seguridad de los activos TIC de los que <ORGANISMO> sea titular o cuya gestión tenga encomendada.

2. El Comité de Seguridad TIC de <ORGANISMO> estará formado por:

a) La persona titular de la <Viceconsejería o equivalente>, que ejercerá la presidencia del Comité.
b) La persona titular de <SGT, órgano directivo competente en la aplicación de las TI o equivalente>, que ejercerá la vicepresidencia del Comité.
c) La persona titular de cada uno de los <Centros Directivos de <ORGANISMO> o equivalentes> que tenga responsabilidad sobre algún sistema de información, que actuará como vocal.

d) La persona titular de <la Coordinación de Tecnologías y Comunicaciones de la SGT u órgano directivo competente en la aplicación de las TI o equivalente>, que actuará como vocal.

e) (elegir entre OPCIÓN 1 y OPCIÓN 2)

OPCIÓN 1: DPD asignado a una unidad/órgano de carácter horizontal en la organización

La persona titular de la unidad u órgano a la que se asignen las funciones de Delegado de Protección de Datos, que actuará como vocal.

OPCIÓN 2: DPD asignado a una persona

La persona a la que se asignen las funciones de Delegado de Protección de Datos, que actuará como vocal.

f) (elegir entre OPCIÓN 1 y OPCIÓN 2)

OPCIÓN 1: En caso de caso de Consejerías/SAS/SAE ...

La persona titular de la Unidad de Seguridad TIC, que ejercerá la secretaría del Comité.

OPCIÓN 2: En caso de entidades vinculadas o dependentes ...

La persona que haya sido designada como Responsable de Seguridad TIC, que ejercerá la secretaría del Comité.

g) [Opcional 1, si <ORGANISMO> es operador de infraestructuras críticas] Las personas designadas como Responsables de Seguridad y Enlace y Delegados de Seguridad en lo tocante a las infraestructuras críticas de las que <ORGANISMO> sea operador.

h) [Opcional 2, si <ORGANISMO> está obligado como Organismo Pagador a implantar un sistema de gestión de seguridad de la información] Las personas con responsabilidades de seguridad en el sistema de gestión de seguridad de la información implantado como requisito de autorización de <ORGANISMO> como organismo pagador.

3. Cuando el tratamiento de determinadas cuestiones lo requiera, se podrá convocar a las reuniones del Comité a personal técnico especializado, a los efectos de prestar asesoramiento experto.

4. Serán funciones propias del Comité de Seguridad TIC:

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.
c) Nombramiento de < la Unidad /Responsable de Seguridad TIC de <ORGANISMO>, indicar lo que proceda según el tipo de organismo...>.

d) Elevación de propuestas de revisión de la política de seguridad TIC de <ORGANISMO>, de directrices y normas de seguridad de <ORGANISMO>, o de revisión del marco normativo de seguridad TIC de la Junta de Andalucía, a los órganos competentes para su reglamentaria tramitación.
e) Aprobación de la normativa de seguridad TIC de segundo y tercer nivel de <ORGANISMO>.
f) Establecimiento de directrices comunes y supervisión del cumplimiento de la normativa en materia de seguridad TIC.
g) Supervisión del nivel de riesgo y toma de decisiones en la respuesta a incidentes de seguridad TIC que afecten a los activos TIC.
h) Coordinación con los Comités de Seguridad TIC de las entidades instrumentales vinculadas o dependientes de <ORGANISMO>.
i) Promoción de formación, entrenamiento y concienciación sobre las medidas legales y organizativas relativas a la Seguridad TIC entre el personal de <ORGANISMO>.
j) Impulsar la determinación de los niveles de seguridad de la información tratada, en la que se valorarán los impactos que tendrían los incidentes que afectaran a la seguridad de la información, todo ello con la participación de los Responsables de la Información correspondientes y de <la Unidad /Responsable de Seguridad TIC, indicar lo que corresponda ...>.
k) Impulsar los preceptivos análisis de riesgos, junto a los Responsables de las Informaciones / Servicios que correspondan, contando con la participación de <la Unidad /Responsable de Seguridad TIC, indicar lo que corresponda ...>.
l) Coordinar la aceptación de los riesgos residuales por sus responsables correspondientes respecto de la información / servicios de su competencia, obtenidos en el análisis de riesgos.

5. El Comité se reunirá al menos una vez al año, previa convocatoria y, de sus reuniones, se levantará acta.

6. El Comité de Seguridad contará con un esquema de suplencias en caso de que las personas titulares no puedan acudir a las reuniones del mismo.

Artículo 8. Responsables de la información y de los servicios de <ORGANISMO> y procedimiento de designación y renovación

(elegir entre OPCIÓN 1 y OPCIÓN 2)

OPCIÓN 1:

1. Los Responsables de la información y/o de los servicios serán las personas titulares de los centros directivos que decidan sobre la finalidad, contenido y uso de la información y/o sobre las características de los servicios a prestar, así como las que determinen los niveles de seguridad dentro del marco establecido en el anexo I del ENS.

2. En virtud del artículo 10.4 del Decreto 1/2011, de 11 de enero, los deberes y responsabilidades principales de estos perfiles de responsabilidad, dentro de su ámbito de actuación y sin perjuicio de otras previstas en el ENS y la guía CCN-STIC-801, son los siguientes:

a) Ayudar a determinar los requisitos de seguridad de la información y/o de los servicios a prestar, identificando los niveles de seguridad de la información y/o servicios mediante la valoración del impacto sobre los mismos de los incidentes que pudieran producirse.

b) Proporcionar la información necesaria a < la Unidad / Responsable de Seguridad TIC, dejar lo que proceda ...> para realizar los preceptivos análisis de riesgos, con la finalidad de establecer las salvaguardas a implantar. Para ello contará con la ayuda del Responsable del Sistema (o los responsables si hubiere varios).

c) En relación con los análisis de riesgos de los sistemas de información, aceptar los riesgos residuales de las informaciones manejadas y/o servicios prestados que sean de su competencia.

3. El nombramiento o renovación de estas figuras responsables se realiza en virtud de la presente política de seguridad TIC, estando aparejados automáticamente a la toma de posesión de la titularidad de los correspondientes centros directivos o unidades organizativas y a la adscripción a los mismos en cada momento de las distintas informaciones manejadas y servicios prestados.

OPCIÓN 2: Prevista para organizaciones complejas...

Se basa en el mismo esquema que para OPCIÓN 1, pero segregando la responsabilidad sobre los servicios y asignándola a una persona o unidad diferente de la correspondiente a la persona responsable de la información. En este caso, cada unidad administrativa, con rango igual o superior a Servicio, asumirá la figura de Responsable del servicio, con arreglo a lo previsto en el ENS, para aquellos servicios de los que determine sus requisitos. El nombramiento o renovación, en estos casos, será realizado y comunicado, mediante acto documentado, por los Responsables de la Información.

Artículo 9. <Unidad de seguridad TIC, borrar esta referencia a la USTIC si NO es preceptivo disponer de ella**>, Responsable de Seguridad TIC.**

(elegir entre OPCIÓN 1 u OPCIÓN 2)

OPCIÓN 1: En caso de caso de Consejerías/SAS/SAE ...

1. En virtud del artículo 11.1 del Decreto 1/2011, de 11 de enero, <ORGANISMO> contará con una Unidad de Seguridad TIC, garantizando el cumplimiento del principio de función diferenciada recogido en el artículo 5.j) de dicho Decreto. A estos efectos, estará adscrita a la <Viceconsejería de ORGANISMO / .... u otro órgano que permita cumplir con el mencionado principio>

2. La Unidad de Seguridad TIC de <ORGANISMO> será nombrada o renovada y se comunicará, mediante acto documentado, por el Comité de Seguridad TIC de este organismo, teniendo al frente a una persona responsable.
3. La Unidad de Seguridad TIC de <ORGANISMO> tendrá las atribuciones que establece el artículo 11.1 del Decreto 1/2011, de 11 de enero.
4. La persona responsable de la Unidad de Seguridad TIC de <ORGANISMO> tendrá la condición de Responsable de Seguridad y, en virtud del artículo 10.4 del Decreto 1/2011, de 11 de enero, la presente política establece que le corresponderán los deberes y responsabilidades en los términos recogidos en el ENS y la guía CCN-STIC-801.
[Opcional 1, si <ORGANISMO> es operador de infraestructuras críticas] Establecer funciones de la Unidad de Seguridad TIC relativas a los aspectos de seguridad digital de la protección de infraestructuras críticas.
[Opcional 2, si <ORGANISMO> está obligado como Organismo Pagador a implantar un sistema de gestión de seguridad de la información] Establecer funciones de la Unidad de Seguridad TIC relativas al SGSI implantado.
5. La Unidad de Seguridad TIC de <ORGANISMO> elaborará y mantendrá un inventario de servicios y sistemas, con indicación expresa de las personas u órganos que asumen, para cada uno de ellos, las figuras de responsable de la información, responsable del servicio, responsable del sistema y responsable de seguridad. Dicho listado se entregará, actualizado, al Comité de Seguridad TIC del organismo en cada una de sus reuniones, con indicación de aquellas deficiencias o faltas de información que se produzcan, de modo que el Comité disponga de información completa y pueda arbitrar los mecanismos necesarios para la subsanación de las deficiencias o faltas de información.

[Opcional] Artículo XXX. Delegado de Protección de Datos

1. La figura del Delegado de Protección de Datos, en los términos establecidos en el RGPD, será asumida por <una persona, unidad u órgano ...elegir la opción que mejor se adapte a la situación de cada organismo> de <ORGANISMO> que, al menos, contará con un perfil especializado en derecho y de reconocida competencia en materia de protección de datos, así como tener una adscripción dentro de la estructura de la organización a un órgano con competencias y funciones de carácter horizontal, a los efectos de poder relacionarse adecuadamente con la dirección de la organización y con las autoridades de control.
2. El nombramiento o renovación de la figura del Delegado de Protección de Datos se realizará y comunicará, mediante acto documentado, por decisión de <dirección de ORGANISMO / Comité de Seguridad de ORGANISMO (elegir una opción)>, teniendo al frente a una persona responsable.
3. La figura del Delegado de Protección de Datos de <ORGANISMO> velará por la elaboración y mantenimiento de un registro de tratamientos de datos de carácter personal, con indicación expresa de las personas u órganos que asumen las figuras de responsable del fichero o tratamiento, encargado del tratamiento y resto de requisitos exigidos por el art 30 del RGPD. Dicho listado se entregará, actualizado, al Comité de Seguridad TIC del organismo en cada una de sus reuniones, con indicación de aquellas deficiencias o faltas de información que se produzcan, de modo que el Comité disponga de información completa y pueda arbitrar los mecanismos necesarios para la subsanación de las deficiencias o faltas de información.

OPCIÓN 2: En caso de entidades vinculadas o dependientes ...

1. En virtud del artículo 11.2 del Decreto 1/2011, de 11 de enero, <ORGANISMO> contará con un Responsable de Seguridad TIC, garantizando el cumplimiento del principio de función diferenciada recogido en el artículo 5.j) de dicho Decreto. A estos efectos, estará adscrito a <Dpto u otro órgano que permita cumplir con el mencionado principio>.
2. La figura del Responsable de Seguridad TIC de <ORGANISMO> será nombrada o renovada y se comunicará, mediante acto documentado, por el Comité de Seguridad TIC de este organismo.
3. El Responsable de Seguridad TIC de <ORGANISMO> tendrá las atribuciones que establece el artículo 11.2 del Decreto 1/2011, de 11 de enero.
[Opcional 1, si <ORGANISMO> es operador de infraestructuras críticas] Establecer funciones de la persona Responsable Seguridad TIC relativas a los aspectos de seguridad digital de la protección de infraestructuras críticas.
[Opcional 2, si <ORGANISMO> está obligado como Organismo Pagador a implantar un sistema de gestión de seguridad de la información] Establecer funciones de de la persona Responsable de Seguridad TIC relativas al SGSI implantado.
4. El Responsable de Seguridad TIC de <ORGANISMO> elaborará y mantendrá un inventario de servicios y sistemas, con indicación expresa de las personas u órganos que asumen, para cada uno de ellos, las figuras de responsable de la información, responsable del servicio, responsable del sistema y responsable de seguridad. Dicho listado se entregará, actualizado, al Comité de Seguridad TIC del organismo en cada una de sus reuniones, con indicación de aquellas deficiencias o faltas de información que se produzcan, de modo que el Comité disponga de información completa y pueda arbitrar los mecanismos necesarios para la subsanación de las deficiencias o faltas de información.

[Opcional] Artículo XXX. Delegado de Protección de Datos

1. La figura del Delegado de Protección de Datos, en los términos establecidos en el RGPD, será asumida por <una persona, unidad u órgano ...elegir la opción que mejor se adapte a la situación de cada organismo> de <ORGANISMO> que, al menos, contará con un perfil especializado en derecho y de reconocida competencia en materia de protección de datos, así como tener una adscripción dentro de la estructura de la organización a un órgano con competencias y funciones de carácter horizontal, a los efectos de poder relacionarse adecuadamente con la dirección de la organización y con las autoridades de control.
2. El nombramiento o renovación de la figura del Delegado de Protección de Datos se realizará y comunicará, mediante acto documentado, por decisión de <dirección de ORGANISMO / Comité de Seguridad de ORGANISMO (elegir una opción)>, teniendo al frente a una persona responsable.
3. La figura del Delegado de Protección de Datos de <ORGANISMO> velará por la elaboración y mantenimiento de un registro de tratamientos de datos de carácter personal, con indicación expresa de las personas u órganos que asumen las figuras de responsable del fichero o tratamiento, encargado del tratamiento y resto de requisitos exigidos por el art 30 del RGPD. Dicho listado se entregará, actualizado, al Comité de Seguridad TIC del organismo en cada una de sus reuniones, con indicación de aquellas deficiencias o faltas de información que se produzcan, de modo que el Comité disponga de información completa y pueda arbitrar los mecanismos necesarios para la subsanación de las deficiencias o faltas de información.

Artículo 10. Responsable del Sistema y procedimiento de designación y renovación

1. La figura de Responsable del sistema, desde la perspectiva del ENS, de cada sistema de información que se encuentre albergado en los servidores corporativos de la misma será asumida por una persona adscrita a <la SGT, órgano directivo competente en la aplicación de las TI o equivalente, o una unidad administrativa con rango de Servicio dependiente del mismo (indicar lo que corresponda)>.

2. En virtud del artículo 10.4 del Decreto 1/2011, de 11 de enero, la presente política establece que los deberes y responsabilidades de este perfil de responsabilidad serán los previstos en el ENS y la guía CCN-STIC-801 para la figura del Responsable del Sistema y su designación y renovación ...[elegir OPCIÓN]

> [OPCIÓN 1: por decisión del Comité de Seguridad].
> ... se realizará por decisión del Comité de Seguridad de <ORGANISMO> y se comunicará, mediante acto documentado, a la persona o personas designadas.
>
> [OPCIÓN 2: por decisión del órgano directivo competente en la aplicación de las TI o equivalente].
> ... se realizará por decisión del órgano directivo competente en la aplicación de las TI de <ORGANISMO> y se comunicará, mediante acto documentado, a la persona o personas designadas.

3. La figura de Responsable del sistema, desde la perspectiva del ENS, de los sistemas de información cuya implantación, explotación y mantenimiento se haga fuera de <ORGANISMO> (en otros organismos de la Junta de Andalucía o en empresas externas) será nombrada o renovada por el responsable de la información o el responsable de servicio correspondiente y se comunicará mediante acto documentado.

Artículo 11. Resolución de conflictos

1. En caso de conflicto entre los diferentes responsables, éste será resuelto por el órgano superior jerárquico de los mismos. En defecto de lo anterior, prevalecerá la decisión del Comité de Seguridad TIC.

2. En los conflictos entre las personas responsables que componen la estructura organizativa de la política de seguridad TIC de <ORGANISMO> y las personas responsables definidas en virtud de la normativa de protección de datos de carácter personal prevalecerá la decisión que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.

Artículo 12. Datos de Carácter Personal

1. Para el tratamiento de datos de carácter personal en los sistemas de información se seguirá en todo momento 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, así como lo establecido en la legislación nacional y autonómica vigente en cada momento en relación con esta materia.

2. La seguridad de los datos de carácter personal se basará en criterios de reducción del riesgo dependiendo de la naturaleza y tratamientos de los mismos.

[OPCIONAL, si se ha incluido artículo sobre funciones del Delegado de Protección de Datos] 3. Para el cumplimiento de la obligación de disponer de un registro de tratamientos, se estará a lo indicado en el artículo XXX de esta Orden.

Artículo 13. Gestión de riesgos

1. La gestión de riesgos debe realizarse de manera continua sobre el sistema de información, conforme a los principios de gestión de la seguridad basada en los riesgos y reevaluación periódica.

2. Los responsables de la información y/o servicios son responsables de los riesgos sobre la información y / o los servicios y por tanto, de aceptar los riesgos residuales calculados en el análisis de riesgos, así como de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

3. El Comité de Seguridad TIC es responsable de realizar un seguimiento de los principales riesgos residuales asumidos por la organización y de recomendar posibles actuaciones respecto de ellos.

3. La selección de las medidas de seguridad a aplicar será propuesta por < la Unidad de Seguridad TIC / el Responsable de seguridad TIC, indicar lo que corresponda ...> al Comité de Seguridad TIC, así como el seguimiento de su aplicación.

4. El proceso de gestión de riesgos comprende las fases de identificación y valoración de informaciones y servicios esenciales prestados, categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, las cuales deberán ser proporcionales a los riesgos y estar justificadas. Este análisis deberá revisarse cada año por parte de < la Unidad de Seguridad TIC / el Responsable de seguridad TIC, indicar lo que corresponda ...>, que elevará el correspondiente informe al Comité de Seguridad TIC.

5. Para realizar el análisis de riesgos se utilizará la metodología MAGERIT, aprobada por el Consejo Superior de Administración Electrónica, y las herramientas que la apliquen, como PILAR, desarrollada por el Centro Criptológico Nacional.

Artículo 14. Desarrollo normativo de la seguridad TIC

1. El cuerpo normativo sobre seguridad TIC es de obligado cumplimiento y se desarrollará en tres niveles, según el ámbito de aplicación y nivel de detalle técnico, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Dichos niveles de desarrollo normativo son los siguientes:
a) Primer nivel normativo: Política de Seguridad TIC y directrices y normas generales de seguridad TIC.
b) Segundo nivel normativo: Normas Específicas de Seguridad TIC, que desarrollan y detallan la Política de Seguridad TIC, centrándose en un área o aspecto determinado.

c) Tercer nivel normativo: Procedimientos, Procesos, Guías e Instrucciones Técnicas de Seguridad TIC, que dan respuesta, incluyendo detalles de implementación y tecnológicos, a cómo se puede realizar una determinada tarea cumpliendo con lo expuesto en la Política.
2. Al amparo de la presente Orden, <ORGANISMO> podrá ampliar y desarrollar, sobre la base de los mínimos establecidos, sus propias normas en materia de seguridad TIC, en virtud del artículo 2.5 de la Orden de 9 de junio de 2016.
3. Además de los documentos citados en el apartado 1, la documentación de seguridad TIC de los órganos contemplados en el ámbito de aplicación de esta norma podrá contar, bajo criterio de <la Unidad / Responsable de Seguridad TIC, dejar lo que corresponda ...>, con otros documentos de carácter no vinculante: recomendaciones, buenas prácticas, informes, registros, evidencias electrónicas, etc.
4. <La Unidad / Responsable de Seguridad TIC, dejar lo que corresponda ...> deberá mantener la documentación de seguridad actualizada y organizada, y gestionar los mecanismos de acceso a la misma.
5. El Comité de Seguridad TIC establecerá los mecanismos necesarios para compartir la documentación derivada del desarrollo normativo con el propósito de normalizarlo, en la medida de lo posible, en todo el ámbito de aplicación de la Política.

Artículo 15. Gestión de incidentes de seguridad y de la continuidad

1. <ORGANISMO> deberá estar preparado para prevenir, detectar, reaccionar y recuperarse de incidentes, según los términos previstos en el artículo 7 del ENS.
2. El Comité de Seguridad deberá aprobar y revisar periódicamente un plan para mantener la continuidad de los procesos y sistemas críticos y garantizar su recuperación en caso de desastre. La finalidad de este plan es reducir el tiempo de indisponibilidad a niveles aceptables mediante la combinación de controles de carácter organizativo, tecnológico y procedimental tanto preventivos como de recuperación.
3. A los efectos de una mejor gestión de los incidentes, se actuará de forma coordinada con AndalucíaCERT.

Artículo 16.Formación y concienciación en seguridad TIC

Anualmente se desarrollarán actividades de formación y concienciación en seguridad TIC destinadas a las personas empleadas públicas de los órganos contemplados en el ámbito de aplicación de esta norma. Entre tales actividades se incluirán las de difusión de esta política de seguridad TIC y de su desarrollo normativo.

Artículo 17. Terceras partes

1 Cuando <ORGANISMO> preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta política de seguridad TIC, estableciéndose los canales que procedan para la comunicación y coordinación entre las respectivas organizaciones, en especial para una rápida y eficaz reacción ante incidentes de seguridad.

2.Cuando <algún Centro Directivo /Dpto de <ORGANISMO> / <ORGANISMO>, indicar lo que corresponda ...> 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 TIC que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta, a través de cláusulas contractuales o acuerdos de nivel servicio, a las obligaciones generales establecidas en dicha normativa, pudiendo disponer la tercera parte de sus propios procedimientos operativos para

satisfacerla. Se establecerán mecanismos de comunicación y resolución de incidencias. Se velará por que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos, al mismo nivel que el establecido en esta política de seguridad TIC.

3. Cuando algún aspecto de esta política de seguridad TIC no pueda ser satisfecho por una tercera parte según se requiere en el párrafo anterior, se requerirá un informe de < la Unidad de Seguridad TIC / el Responsable de seguridad TIC, indicar lo que corresponda ...> 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/o los servicios afectados antes de proseguir en la relación con la tercera parte.

Artículo 18. Auditorías y conformidad con la normativa

1 <ORGANISMO> manifiesta el compromiso de auditar los sistemas de información de forma periódica con objeto de revisar el cumplimiento normativo vigente.
2. Los sistemas de información de <ORGANISMO> serán objeto, al menos cada dos años, de una auditoría regular ordinaria interna o externa que verifique el cumplimiento de los requisitos del ENS y de cualquier otra norma que requiera la realización de auditorías periódicas. < La Unidad de Seguridad TIC / El Responsable de seguridad TIC, indicar lo que corresponda ...> realizará o, en su caso, coordinará, estas actividades de auditoría.
3. Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad requeridas.
3. Los informes de auditoría quedarán a disposición del <órgano de dirección> y del Comité de Seguridad TIC. Por otra parte, < la Unidad de Seguridad TIC / el Responsable de seguridad TIC, indicar lo que corresponda ...> deberá analizar dicho informe y elevar al Comité de Seguridad TIC las conclusiones que procedan para que éste adopte las medidas correctoras adecuadas.

Artículo 19. Cooperación con otros órganos y otras administraciones en materia de seguridad

A efectos de coordinación, obtención de asesoramiento e intercambio de experiencias para la mejora continua de la gestión de la seguridad de la información, se fomentará el establecimiento de mecanismos de comunicación con otros agentes especializados en esta materia. En especial, se contemplarán los siguientes:

- Comité de Seguridad TIC de la Junta de Andalucía
- Unidad de Seguridad TIC Corporativa de la Junta de Andalucía
- Consejo de Transparencia y Protección de Datos de Andalucía
- CCN-CERT: Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN), como soporte y coordinación para la resolución de incidentes que sufra la Administración General, Autonómica o Local.
- Agencia Española de Protección de Datos (AEPD)

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

Artículo 20. Actualización permanente y revisiones periódicas

1. Esta orden deberá mantenerse actualizada para adecuarla a la evolución de los servicios TIC y, en general, 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 de la información se harán a propuesta del Comité de Seguridad TIC.

Artículo 21. Difusión de la política de seguridad de la información

A los efectos de su mejor difusión entre el personal de la organización 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. Constitución del Comité de Seguridad TIC

La primera reunión del Comité de Seguridad TIC tendrá por objeto la constitución, renovación o confirmación del mismo y se celebrará en un plazo máximo de un mes a partir de la entrada en vigor de la presente orden.

Disposición final primera. Habilitación para ejecución y desarrollo

Se habilita a la persona titular de <órgano directivo competente en la aplicación de las TI o equivalente> para dictar cuantas actuaciones sean necesarias para la ejecución y desarrollo de lo establecido en 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 X de XXXX de XXXX, por la que se establece La Política de Seguridad TIC/Comité de Seguridad TIC de <ORGANISMO>, publicada en el BOJA núm. XX de X de XXXX de XXXX

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 Junta de Andalucía.

Sevilla, XX de xxxxxx de 201X