JUNTA DE ANDALUCIA

CONSEJERÍA DE CONOCIMIENTO, INVESTIGACIÓN Y UNIVERSIDAD

Política de Seguridad

Versión:v01r01

Fecha:17/07/18

HOJA DE CONTROL

Título	Política de Seguridad		
Entregable			
Nombre del Fichero	1. Borrador Orden Politica de Seguridad CCIU v01r01.odt		
Autor	Servicio de Informática- SGT la Consejería de Conocimiento, Investigación y Universidad		
Versión/Revisión		**Fecha Versión**	25/06/18
Aprobado por		**Fecha Aprobación**	
Seguridad	Uso Interno	**Nº Total Páginas**	27

REGISTRO DE CAMBIOS

Versión	Causa del Cambio	Responsable del Cambio	Área	Fecha del Cambio
Borrador 1	Creación	Juan Gasch Illescas Rafael Delgado Lorente M.ª del Carmen Sánchez Escobar	Servicio de Informática. Área de Seguridad	25/06/18
Borrador 2	Modificaciones de escasa relevancia	Rafael Delgado Lorente M.ª del Carmen Sánchez Escobar	Servicio de Informática. Área de Seguridad	17/07/18

CONTROL DE DISTRIBUCIÓN

Nombre y Apellidos	Cargo	Área	Nº Copias

ÍNDICE

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 LA CONSEJERÍA DE CONOCIMIENTO, INVESTIGACIÓN Y UNIVERSIDAD

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 Ley 39/2015, de 1 de octubre, tiene como uno de sus objetivos centrales regular las relaciones entre las Administraciones la ciudadanía y las 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.º 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 a los mismos.

Para el desarrollo de esta Política de seguridad de las tecnologías de la información y las comunicaciones se ha seguido lo indicado 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 y por el que se deroga la Directiva 95/46/CE (en adelante, RGPD), así como en la legislación estatal vigente en materia de protección de datos personales; 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.

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 la Consejería de Conocimiento, Investigación y Universidad 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 Decreto 108/2018, de 19 de junio, por el que se regula la estructura orgánica de la Consejería de Conocimiento, Investigación y Universidad.

DISPONGO

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1. Objeto

De conformidad con lo establecido en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, la presente Orden tiene

por objeto definir y regular la política de seguridad de las tecnologías de la información y comunicaciones (en adelante TIC) de la Consejería de Conocimiento, Investigación y Universidad, que se ha de aplicar en el tratamiento de los activos TIC de su titularidad o cuya gestión tenga encomendada.

Artículo 2. Misión y objetivos del organismo.

Corresponde a la Consejería de Conocimiento, Investigación y Universidad las competencias atribuidas en el artículo 1 Decreto 108/2018, de 19 de junio, por el que se regula la estructura orgánica de la Consejería de Conocimiento, Investigación y Universidad.

Artículo 3. Ámbito de aplicación.

1. La presente política de seguridad TIC expresa el compromiso de la Consejería de Conocimiento, Investigación y Universidad con la gestión de la seguridad de la información en general y, particularmente, con la de los sistemas de información.

2. Pretende, en definitiva, dirigir y dar soporte a la gestión de la seguridad de la información mediante el establecimiento de una estructura organizativa en la que se apoyará el gobierno de la seguridad, así como dotarse de unas directrices básicas de acuerdo a los requisitos propios de seguridad y a la regulación aplicable, constituyéndose en el marco dentro del que se definirá el conjunto de normas reguladoras, procedimientos y prácticas que determinen el modo en que los activos son gestionados, protegidos y distribuidos.

3. De acuerdo con lo dispuesto en el artículo 10.3 del Decreto 70/2017, de 6 de junio, por el que se modifica 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, la política de seguridad TIC de la Consejería de Conocimiento, Investigación y Universidad y sus documentos complementarios serán de aplicación además de a sus servicios centrales y periféricos, a sus entidades vinculadas o dependientes. También serán de aplicación para todo el personal que acceda a los sistemas de información como a la propia información que sea gestionada por la Consejería de Conocimiento, Investigación y Universidad, con independencia de cuál sea su destino, adscripción o relación con la misma.

Artículo 4. 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 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. La Consejería de Conocimiento, Investigación y Universidad podrá ampliar y desarrollar el marco normativo en los términos previstos en el artículo 28 de esta Orden.

CAPÍTULO II

POLÍTICA DE SEGURIDAD TIC

Artículo 5. Contexto tecnológico y obligaciones generales.

1. La Consejería de Conocimiento, Investigación y Universidad, depende de los sistemas TIC para alcanzar sus objetivos en el ámbito de su competencia con la calidad necesaria. Por ello, estos sistemas deben ser administrados con diligencia, adoptando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o de los servicios prestados.

2. El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

3. Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para afectar a la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que las unidades organizativas deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (en lo sucesivo, ENS) y por la legislación de protección de datos de carácter personal, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

4. Las diferentes unidades organizativas deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Así, los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

5. Las unidades organizativas deben estar preparadas para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al artículo 7 del ENS.

6. Con carácter general, para el personal de la Consejería de Conocimiento, Investigación y Universidad, 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.

7. 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 la Consejería de Conocimiento, Investigación y Universidad.

Artículo 6. Objetivos, principios y definiciones.

Se asumen los principios, objetivos y definiciones 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 7. Prevención.

Las unidades organizativas deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. 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. Estos controles, y los perfiles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados. Para garantizar el cumplimiento de la política, las unidades organizativas deben:

- Autorizar la puesta en funcionamiento de los sistemas TIC de su competencia.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

Artículo 8. Detección.

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple ralentización hasta su detención, se deberán monitorizar de manera continua para detectar anomalías en los niveles de prestación de los mismos y actuar en consecuencia según lo establecido en el ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con lo establecido en el ENS. Así se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

Artículo 9. Respuesta.

Las unidades organizativas deben:

- Colaborar con el equipo de gestión de incidentes de seguridad de la Consejería.
- Designar un punto de contacto para las comunicaciones relativas a incidentes detectados en otras unidades organizativas o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

Artículo 10. Recuperación.

Para garantizar la disponibilidad de los servicios críticos, las unidades organizativas deben colaborar en el desarrollo de planes de continuidad de sus sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación liderados por el Comité de Seguridad TIC.

Artículo 11. Estructura organizativa de la seguridad TIC.

1. El mantenimiento y gestión de la seguridad de la información va íntimamente ligado al establecimiento de una organización de seguridad. Dicha organización se establece mediante la identificación y definición de las diferentes actividades y responsabilidades en materia de gestión de la seguridad y la implantación de una estructura que las soporte.

2. La estructura que se define en esta orden diferencia tres grandes bloques de responsabilidad: i) la especificación de las necesidades o requisitos en materia de seguridad de la información, ii) la operación del sistema de información que se atiene a dichos requisitos y iii) la función de supervisión de acuerdo al principio básico del ENS de "*La seguridad como función diferenciada*".

3. Siguiendo la terminología utilizada en el ENS, la especificación de los requisitos de seguridad corresponderá a los **responsables de la información y los servicios**, y al **responsable del tratamiento** si hubiera datos de carácter personal. La operación corresponderá al **responsable del sistema** y, por último, la supervisión corresponderá al **responsable de la seguridad**.

4. La seguridad de la información implica prácticamente a todas las áreas de la Consejería de Conocimiento, Investigación y Universidad, habida cuenta de que ha de estar presente en todos los ámbitos de su actividad y debe tener un carácter multidisciplinar, abarcando áreas como la informática y comunicaciones, gestión de personal y financiera, ejecución de proyectos, etc.

5. La estructura organizativa para la gestión de la seguridad TIC en el ámbito descrito está compuesta por los siguientes agentes en dos niveles:

a) En la Consejería de Conocimiento, Investigación y Universidad en concreto:

i. Comité de Seguridad TIC.

ii. Responsables de la información.

iii. Responsables de los servicios.

iv. Unidad de Seguridad TIC.

v. Delegado o Delegada de Protección de Datos.

vi. Responsable de Seguridad.

vii. Responsables de los Sistemas.

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. Delegado o Delegada de Protección de Datos.

v. Responsable de Seguridad.

vi. Responsable de Sistema.

6. 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.

7. 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 la Consejería de Conocimiento, Investigación y Universidad la responsabilidad de la conformación y designación de estas figuras, recaerá sobre las propias entidades vinculadas o dependientes.

8. La estructura organizativa será competente para mantener, actualizar y hacer cumplir, dentro del ámbito definido la Política de Seguridad de la Información

Artículo 12. Comité de Seguridad TIC de la Consejería de Conocimiento, Investigación y Universidad.

1. Se crea el Comité de Seguridad TIC de la Consejería de Conocimiento, Investigación y Universidad 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. Este Comité gestionará y coordinará todas las actividades relacionadas con la seguridad de los sistemas de información está compuesto por los siguientes miembros:

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

b) Vicepresidencia: Será ejercida por la persona titular de la Secretaría General Técnica.

c) Vocalías:

i. La persona titular de cada uno de los Centros Directivos de la Consejería de Conocimiento, Investigación y Universidad que tengan responsabilidad sobre algún sistema de información.

ii. La persona titular del Servicio de Informática de la SGT.

iii. La persona titular a la que se asignen las funciones de Delegado/a de Protección de Datos.

iv. La persona titular de la Unidad de Seguridad TIC, que ejercerá como Responsable de Seguridad.

v. Una persona representante de las Delegaciones Territoriales adscritas a la Consejería de Conocimiento, Investigación y Universidad designado por la Viceconsejería, elegido entre las personas Responsables de Seguridad de cada Delegación Territorial

d) Secretaría: Será designada por la persona titular de la Secretaría General Técnica, tendrá voz pero sin voto, convocará las reuniones del Comité y preparará el orden del día de las mismas.

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.

5. 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 persona titular de la Vicepresidencia. La Vicepresidencia, 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 las mismas condiciones. Serán designados por el mismo procedimiento que los titulares.

6. Este Comité tiene por objeto general actuar como órgano de dirección y seguimiento en materia de seguridad de los activos TIC titularidad de la Consejería de Conocimiento, Investigación y Universidad o cuya gestión tenga encomendada.

7. Al Comité de Seguridad TIC le corresponde velar por la aplicación en el ámbito de la Consejería de Conocimiento, Investigación y Universidad, de las previsiones contenidas en la normativa relativa a la seguridad TIC recogida en el artículo 4 de esta noma.

8. En particular, le corresponde:

a) Impulsar el cumplimiento de la Política de Seguridad de la Información y su desarrollo normativo, estableciendo las directrices comunes y de supervisión de seguridad TIC

b) Definición, aprobación y seguimiento de los objetivos, iniciativas y planes estratégicos en materia de seguridad TIC, velando en particular por la coordinación entre diferentes planes que puedan coexistir. Promover la mejora continua del sistema de gestión de la seguridad TIC.

c) Velar por la disponibilidad de los recursos necesarios para desarrollar las iniciativas y planes estratégicos definidos.

d) La creación de la Unidad de Seguridad TIC.

e) Nombrar al Responsable de Seguridad TIC.

f) Nombrar a los Responsables de los Sistemas.

g) Impulsar el cumplimiento de la Política de Seguridad de la Información

h) Atender las peticiones en materia de seguridad TIC de los centros directivos.

i) Informar regularmente a la persona titular de la Consejería de Conocimiento, Investigación y Universidad del estado de la seguridad de las tecnologías de la información y comunicaciones en su ámbito.

j) Elevación de propuestas de revisión de la política de seguridad TIC de la Consejería de Conocimiento, Investigación y Universidad, de directrices y sus normas de seguridad, o de revisión del marco normativo de seguridad TIC de la Junta de Andalucía, a los órganos competentes para su tramitación.

k) Aprobación de la normativa de seguridad TIC de segundo y tercer nivel de la Consejería de Conocimiento, Investigación y Universidad.

l) Coordinar los esfuerzos de todo el equipo humano con responsabilidad en materia de seguridad TIC para asegurar que son consistentes y están alineados con la estrategia decidida, evitando duplicidades.

m) Coordinación con los Comités de Seguridad TIC de las entidades instrumentales vinculadas o dependientes de la Consejería de Conocimiento, Investigación y Universidad.

n) Promoción de formación, entrenamiento y concienciación sobre las medidas legales y organizativas relativas a la Seguridad TIC entre el personal de Consejería de Conocimiento, Investigación y Universidad.

o) Elaborar y aprobar los requisitos de formación y cualificación de las personas administradoras, operadoras y usuarias desde el punto de vista de seguridad TIC de la Consejería de Conocimiento, Investigación y Universidad.

p) Coordinación y aprobación de los planes de continuidad de la Consejería de Conocimiento, Investigación y Universidad.

q) Promover auditorías periódicas para verificar el correcto cumplimento de la política, normativa y procedimientos de seguridad.

r) Monitorizar los principales riesgos residuales asumidos y recomendar posibles actuaciones respecto a ellos.

s) Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto a ellos, velando en particular por la coordinación en la gestión de incidentes de seguridad TIC.

t) Priorizar las actuaciones en materia de seguridad TIC cuando los recursos sean limitados.

u) Velar para que la seguridad TIC se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en producción, procurando la creación y utilización de servicios horizontales que reduzcan duplicidades y permitan un funcionamiento homogéneo de todos los sistemas.

v) Resolver los conflictos de competencia que se puedan suscitar entre los diferentes responsables de la gestión de la seguridad TIC o elevar propuesta para resolverlos, en su caso.

w) 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, de la Unidad Seguridad TIC y el Delegado o Delegada de protección de datos.

x) Impulsar los preceptivos análisis de riesgos, junto a los Responsables de las Informaciones que correspondan, contando con la participación de la Unidad de Seguridad TIC y el Delegado o Delegada de protección de datos.

y) Coordinar la aceptación de los riesgos residuales por sus responsables correspondientes respecto de la información y servicios de su competencia, obtenidos en los análisis de riesgos realizados.

Artículo 13. Comité: funcionamiento.

1. El Comité de Seguridad TIC se reunirá con carácter ordinario, al menos, tres veces al año y, con carácter extraordinario, cuando lo decida la persona titular de la Presidencia de oficio o a propuesta de alguno de sus miembros, y siempre que:

a) Se produzcan incidencias de seguridad graves que afecten a cualquier sistema.

b) Surjan nuevas necesidades de seguridad que requieran la participación del Comité.

2. El Comité de Seguridad TIC se podrá constituir, convocar, celebrar sus sesiones, adoptar acuerdos y remitir actas, tanto de forma presencial como a distancia, salvo que su reglamento interno recoja expresa y excepcionalmente lo contrario.

3. Los miembros del Comité de Seguridad TIC podrán proponer a la Presidencia, individual o colectivamente, la inclusión de asuntos en el orden del día. La propuesta deberá realizarse mediante medio electrónico, dirigido a la Presidencia con una antelación mínima de 48 horas a la fecha de la convocatoria.

4. A las sesiones del Comité de Seguridad TIC podrán asistir en calidad de asesoras, con voz pero sin voto, las personas que en cada caso estime pertinente la Presidencia, por iniciativa propia o a propuesta de sus miembros.

5. La persona que ostente la Secretaría del Comité levantará acta de cada reunión del mismo.

6. Cada entidad vinculada o dependiente deberá de 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.

Artículo 14. Delegaciones Territoriales.

1. Cada Delegación Territorial deberá contar con una persona Responsable de Seguridad, que será designada por la persona titular de la Delegación Territorial atendiendo al principio de función diferenciada indicado en el artículo 5. j) del citado Decreto 1/2011, de 11 de enero.

2. La persona que ostente la titularidad de la Viceconsejería nombrará de entre estos Responsables de Seguridad un representante que pasará a ser vocal del Comité de Seguridad.

Artículo 15. Entidades vinculadas o dependientes.

1. De acuerdo con lo dispuesto en el artículo 10 del Decreto 1/2011, de 11 de enero, en su actual redacción y su normativa de desarrollo, cada entidad deberá contar con un documento de Política de Seguridad TIC, que será aprobado por el titular de la entidad correspondiente y se plasmará en los términos descritos en el Real Decreto 3/2010, de 8 de enero. Sin perjuicio de lo establecido en el artículo 10.3 del citado Decreto 1/2011, en el que se indica que el documento de política de seguridad TIC de las Consejerías y sus documentos complementarios también serán de obligando cumplimiento para sus entidades vinculadas o dependientes.

2. El documento de política de seguridad TIC de las entidades vinculadas o dependientes, 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.

3. El Comité de Seguridad TIC de la Consejería de Conocimiento, Investigación y Universidad articulará los mecanismos de colaboración y coordinación necesarios con los de sus entidades vinculadas o dependientes.

4. Las atribuciones de los Comités de Seguridad TIC de las entidades vinculadas o dependientes podrán ser asumidas por los comités de dirección existentes en dichas entidades, lo cual deberá ser recogido expresamente en el correspondiente documento de política de seguridad TIC

Artículo 16. Perfiles de responsabilidad.

Las figuras o perfiles de Responsabilidad (de Seguridad, del Sistema, de Información, de Servicios) que se describen en los siguientes epígrafes deben entenderse como un conjunto de responsabilidades y atribuciones que deben quedar adecuadamente cubiertas dentro de la organización, con independencia de a qué persona concreta o conjunto de personas sean asignadas.

Artículo 17. Unidad de Seguridad TIC.

1. En virtud del artículo 11.1 del citado Decreto 1/2011, de 11 de enero, la Consejería de Conocimiento, Investigación y Universidad 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, esta Unidad estará adscrita a la Secretaría General Técnica.

2. La Unidad de Seguridad TIC de la Consejería de Conocimiento, Investigación y Universidad 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 la Consejería de Conocimiento, Investigación y Universidad tendrá las atribuciones que establece el artículo 11.1 del Decreto 1/2011, de 11 de enero, que se indican a continuación:

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

b) Diseño y ejecución de los programas de actuación propios, 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 y mantenimiento de los análisis de riesgos.

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

e) 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 por parte de los Servicios o Departamentos responsables de la prestación de los servicios de tecnologías de la información y comunicaciones. 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 al centro o centros directivos responsables de la información y del servicio.

f) Definición de los programas formativos y de concienciación relacionados con buenas prácticas de seguridad TIC, procurando promover, en el proceso de selección de las personas participantes en estos programas, la concurrencia de mujeres.

g) Coordinación, dirección y seguimiento de la actividad en materia de seguridad TIC de las entidades vinculadas o dependientes de la Consejería.

h) Aplicación de los criterios y directrices de gestión de la seguridad TIC emanadas de la Unidad de Seguridad TIC Corporativa.

4. La persona responsable de la Unidad de Seguridad TIC de la Consejería de Conocimiento, Investigación y Universidad tendrá la condición de Responsable de Seguridad.

5 La Unidad de Seguridad TIC de la Consejería de Conocimiento, Investigación y Universidad 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.

6. 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 18. Responsable de la Información.

1. El Responsable de la Información (propietario de la información), en lo relativo al ENS, es la figura que determinará los niveles de seguridad de la información dentro del marco establecido en el anexo I del Real Decreto 3/2010, por el que se regula el Esquema Nacional de Seguridad, siendo posible la presentación de una propuesta previa por parte del Comité de Seguridad TIC.

2. La persona en quien recaerá la figura de Responsable de Información y de acuerdo con la guía de seguridad CCN-STIC-801 que trata las Responsabilidades y Funciones en el ENS, será la persona titular del centro directivo que tiene la responsabilidad última del uso que se haga de la información y, por tanto, de su protección. Coincidirá con el Responsable del Tratamiento que se define en el artículo 4 del RGPD.

3. En virtud del artículo 10.4 del Decreto 1/2011, de 11 de enero, los deberes y responsabilidades principales de este perfil 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, identificando los niveles de seguridad de dicha información mediante la valoración del impacto sobre esta de los incidentes que pudieran 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 del Responsable del Sistema.

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

4. El nombramiento o renovación de la figura de Responsable de la Información 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 y a la adscripción a los mismos en cada momento de las distintas informaciones manejadas.

Artículo 19. Responsable del Servicio.

1. Los Responsables de los Servicios, en lo relativo al ENS, son los agentes que determinarán los niveles de seguridad de los servicios dentro del marco establecido en el anexo I del Real Decreto 3/2010, por el que se regula el ENS. La figura de Responsable de los Servicio corresponderá a las personas titulares de cada unidad administrativa, con rango igual o superior a Servicio.

2. En virtud del artículo 10.4 del Decreto 1/2011, de 11 de enero, los deberes y responsabilidades principales de este 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 los servicios a prestar, identificando los niveles de seguridad de los mismos mediante la valoración del impacto sobre estos de los incidentes que pudieran producirse.

b) En el ámbito de cada servicio, proporcionar la información necesaria a la Unidad Seguridad TIC 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.

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 las correspondientes unidades organizativas y a la adscripción a las mismas en cada momento de los distintos servicios prestados.

Artículo 20. Delegado o Delegada de Protección de Datos.

1. La figura del Delegado/a de Protección de Datos, en los términos establecidos en el RGPD, será asumida por una persona funcionaria del grupo A1 perteneciente a la Consejería de Conocimiento, Investigación y Universidad que deberá tener un perfil especializado en derecho, y reconocida competencia en materia de protección de datos. Deberá estar adscrita a una unidad organizativa con competencias y funciones de carácter horizontal a fin 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 la persona titular de la Viceconsejería.

3. Las funciones asociadas al perfil de Delegado de Protección de Datos serán las indicadas en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y demás disposiciones reguladoras de la materia.

4. La figura del Delegado de Protección de Datos de la Consejería de Conocimiento, Investigación y Universidad 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.

5. La dirección de cada entidad vinculada o dependiente deberá nombrar una persona Delegada de Protección de Datos que comunicará, además de a la Agencia Española de Protección de Datos, al Comité de Seguridad TIC de la Consejería de Conocimiento, Investigación y Universidad.

Artículo 21. Responsable de Seguridad TIC.

1. La persona Responsable de Seguridad será nombrada por el Comité de Seguridad y tendrá las siguientes funciones y responsabilidades:

a) Dirigirá la Unidad de Seguridad TIC de la Consejería de Conocimiento, Investigación y Universidad.

b) Será responsable de conocer los cambios tecnológicos que puedan afectar a los sistemas de información, pudiendo tener consecuencias para la organización. En este caso deberá alertar al Comité de Seguridad y proponer las medidas oportunas.

c) Elaborará la normativa de seguridad que se presentará al Comité de Seguridad TIC para su aprobación.

d) Será responsable de la correcta ejecución de las instrucciones emanadas del Comité de Seguridad TIC, transmitiendo dichas instrucciones directamente o a través de la Unidad de Seguridad TIC.

e) Será responsable de la presentación regular de informes sobre el estado de seguridad de los servicios TIC al Comité de Seguridad TIC.

f) Será responsable de la preparación de informes en caso de incidentes excepcionalmente graves y en caso de desastres.

g) Será responsable de la elaboración del Análisis de Riesgos de los sistemas, análisis que será presentado al Comité de Seguridad TIC para su aprobación. Este análisis deberá actualizarse regularmente dependiendo de la criticidad del sistema.

h) Será responsable de la inspección de las verificaciones regulares de seguridad aprobadas por el Comité. El resultado de estas inspecciones se presentará al Comité de Seguridad TIC para su conocimiento y aprobación. Si como resultado de la inspección aparecen incumplimientos, propondrá medidas correctoras que presentará el Comité de Seguridad TIC para su aprobación, responsabilizándose de que sean llevadas a cabo.

i) Será responsable de la elaboración y seguimiento del Plan de Seguridad que será presentado al Comité de Seguridad TIC para su aprobación.

j) Elaborará para su aprobación por el Comité de Seguridad TIC los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de la seguridad de las TIC.

Artículo 22. Responsable del Sistema.

1. 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 por decisión del Comité de Seguridad de la Consejería de Conocimiento, Investigación y Universidad y se comunicará, mediante acto documentado, a la persona o personas designadas.

2. 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 la Consejería de Conocimiento, Investigación y Universidad (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.

3. Corresponde a las personas responsables TIC de los SI, y será nombrado por el Comité de Seguridad TIC de la Consejería. Las atribuciones del Responsable del sistema en lo relativo al ENS serán las siguientes:

a) Gestionar el Sistema durante todo su ciclo de vida, desde la especificación, la instalación, hasta el seguimiento de su funcionamiento.

b) Definir los criterios de uso y los servicios disponibles en el Sistema.

c) Elaborar los procedimientos operativos de Seguridad para su aprobación el Responsable de Seguridad

d) Determinar la configuración autorizada de hardware y software a utilizar en el Sistema y aprobar las modificaciones importantes de dicha configuración.

e) Implantar y controlar las medidas específicas de seguridad del Sistema.

f) Elaborar junto con el Responsable de Seguridad los planes de mejora continua de la seguridad que deberá de aprobar el Comité de Seguridad

g) Elaborar planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.

h) Suspender el manejo de cierta información o la prestación de un cierto servicio si detecta deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el Responsable de la Seguridad, antes de ser ejecutada.

Artículo 23. Actualización de la política de seguridad de la información.

Será misión del Comité de Seguridad TIC la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. Las modificaciones en la Política de Seguridad serán aprobadas por la persona titular de la Consejería de Conocimiento, Investigación y Universidad entrando en vigor al día siguiente de su aprobación y difundida 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.

Artículo 24. 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. En concreto, se adoptarán las medidas técnicas y organizativas que corresponda implantar atendidos los riesgos generados por el tratamiento una vez llevada a cabo la evaluación exigida por el artículo 24.1 del Reglamento (UE) 2016/679.

Artículo 25. Gestión de Riesgos.

1. La Consejería de Conocimiento, Investigación y Universidad realizará una gestión de la seguridad basada en los riesgos, propiciando que tanto el análisis como la gestión de riesgos sean parte esencial del proceso de seguridad, que deberá ser lo más transversal posible al resto de procesos de la organización.

2. La gestión de riesgos deberá realizarse de manera continua sobre cada sistema de información, conforme a los principios de gestión de la seguridad basada en los riesgos y reevaluación periódica. Permitirá mantener un entorno controlado, minimizando los riesgos hasta niveles aceptables, reduciendo estos niveles mediante el despliegue de medidas de seguridad, proceso para el que se establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

3. En línea con lo anterior, los procesos de la organización sujetos a esta Política (y los sistemas asociados que les dan soporte) deberán someterse a un análisis de riesgos, evaluándose las amenazas y los riesgos a los que están expuestos.

4. Los responsables de la información y/o servicios serán 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.

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

6. La selección de las medidas de seguridad a aplicar será propuesta por la Unidad de Seguridad TIC al Comité de Seguridad TIC, así como el seguimiento de su aplicación.

7. 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.

8. Este análisis se repetirá por parte de la Unidad de Seguridad TIC:

a) Preferiblemente, una vez al año.

b) Cuando cambie la información manejada.

c) Cuando cambien los servicios prestados.

d) Cuando ocurra un incidente grave de seguridad.

e) Cuando se detecten vulnerabilidades graves.

9. La Unidad de Seguridad TIC elevará el informe correspondiente al análisis realizado al Comité de Seguridad TIC.

10. Para realizar el análisis de riesgos se utilizará las metodologías y las herramientas que apliquen, de acuerdo con lo establecido por los organismos competentes: el Consejo Superior de Administración Electrónica y el Centro Criptológico Nacional.

11. Para la armonización de los análisis de riesgos, el Comité de Seguridad TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad TIC propiciará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

Artículo 26. Categorización de los sistemas.

1. La determinación de la categoría de un sistema se basa en la valoración del impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas, con repercusión en la capacidad organizativa para:

a) Alcanzar sus objetivos.

b) Proteger los activos a su cargo.

c) Cumplir sus obligaciones diarias de servicio.

d) Respetar la legalidad vigente.

e) Respetar los derechos de las personas.

2. La determinación de la categoría de un sistema se realizará de acuerdo con lo establecido en el ENS, y será de aplicación a todos los sistemas empleados para la prestación de los servicios de la Administración electrónica y soporte del procedimiento administrativo general.

3. Se definen tres categorías: BÁSICA, MEDIA y ALTA.

a) Un sistema de información será de categoría ALTA si alguna de sus dimensiones de seguridad alcanza el nivel ALTO.

b) Un sistema de información será de categoría MEDIA si alguna de sus dimensiones de seguridad alcanza el nivel MEDIO, y ninguna alcanza un nivel superior.

c) Un sistema de información será de categoría BÁSICA si alguna de sus dimensiones de seguridad alcanza el nivel BAJO, y ninguna alcanza un nivel superior.

Artículo 27. Determinación del nivel requerido en una dimensión de seguridad.

1. De acuerdo a lo establecido en el ENS, se tendrán en cuenta las siguientes dimensiones de la seguridad:

a) Disponibilidad [D].

b) Autenticidad [A].

c) Integridad [I].

d) Confidencialidad [C].

e) Trazabilidad [T].

2. Cada dimensión de seguridad afectada se adscribirá a uno de los siguientes niveles: BAJO, MEDIO o ALTO. Si una dimensión de seguridad no se ve afectada, no se adscribirá a ningún nivel.

Artículo 28. Desarrollo de la política de seguridad de la información.

1. La Política de Seguridad de la Información complementa los documentos de seguridad de la Consejería de Conocimiento, Investigación y Universidad en materia de protección de datos de carácter personal, de sistemas de información y de seguridad física de las instalaciones

2. Esta Política se desarrollará por medio de una normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

3. 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, directrices y normas generales de seguridad TIC.

b) Segundo nivel normativo: Normas Específicas de Seguridad TIC, que desarrollan y detallan la Política de SeguridadTIC, 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.

4. Al amparo de la presente Orden, la Consejería de Conocimiento, Investigación y Universidad 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 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.

5. Además de los documentos citados en el anterior párrafo, la documentación de seguridad TIC de los órganos contemplados en el ámbito de aplicación de esta norma podrá contar, bajo criterio de la Unidad de Seguridad TIC, con otros documentos de carácter no vinculante: recomendaciones, buenas prácticas, informes, registros, evidencias electrónicas, etc.

6. La Unidad de Seguridad TIC, deberá mantener la documentación de seguridad actualizada y organizada, y gestionar los mecanismos de acceso a la misma.

7. El Comité de Seguridad TIC establecerá los mecanismos necesarios para publicar y 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 29. Gestión de incidentes de seguridad y de la continuidad.

1. La Consejería de Conocimiento, Investigación y Universidad 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 30. Obligaciones del personal. Concienciación y formación.

1. El objetivo es lograr la plena conciencia respecto a que la seguridad de la información afecta a todos los miembros de la Consejería de Conocimiento, Investigación y Universidad y a todas las actividades, de acuerdo al principio de seguridad integral recogido en el artículo 5 del ENS, así como la articulación de los medios necesarios para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren.

2. Todo el personal de la Consejería de Conocimiento, Investigación y Universidad tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue a los afectados.

3. Todo el personal de la Consejería de Conocimiento, Investigación y Universidad asistirá a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de la Consejería de Conocimiento, Investigación y Universidad en particular a los de nueva incorporación.

4. Las personas con responsabilidad en el uso, operación y administración de sistemas TIC recibirán formación en el manejo seguro de los sistemas en la medida en que la necesiten para realizar sus funciones.

Artículo 31. Terceras partes.

1. Cuando la Consejería de Conocimiento, Investigación y Universidad preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, estableciéndose canales para la comunicación y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

2. Cuando la Consejería de Conocimiento, Investigación y Universidad utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a estos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de comunicación y resolución de incidencias. Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

3. Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se establece en los párrafos anteriores, el Responsable de Seguridad requerirá un informe 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 los servicios afectados antes de continuar con las actuaciones.

Artículo 32. Auditorías y conformidad normativa.

1. La Consejería de Conocimiento, Investigación y Universidad 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 la Consejería de Conocimiento, Investigación y Universidad 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 coordinará, estas actividades de auditoría, y analizará y elevará al Comité de Seguridad TIC las conclusiones que procedan para que éste adopte las medidas correctoras adecuadas.

3. Con carácter extraordinario deberán realizarse auditorías siempre que se produzcan modificaciones sustanciales en el sistema de información con un potencial impacto en el cumplimiento de las medidas de seguridad.

4. Los informes de auditoría quedarán a disposición de la persona titular de la Consejería y del Comité de Seguridad TIC.

Artículo 33. 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 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 Informativos 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.

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 Secretaría General Técnica 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 10 de enero de 2017, por la que se regula la composición, atribuciones, funcionamiento y método de trabajo del Comité de Seguridad de las Tecnologías de la Información y Comunicaciones de la Consejería de Economía y Conocimiento, publicada en el BOJA núm. 11 de 18 de enero de 2018.

Disposición final segunda.

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

Sevilla, a XX de XXXX de 2018