Sección III. Otras disposiciones y actos administrativos

CONSEJO INSULAR DE MALLORCA
PLENO, COMISIÓN DE GOBIERNO, CONSEJO EJECUTIVO Y PRESIDENCIA

10837 ***Aprobación del documento de Política de Seguridad de la Información***

El Consejo Ejecutivo del Consejo Insular de Mallorca, día 26 de septiembre de 2018, ha aprobado el documento de Política de Seguridad de la Información que seguidamente se transcribe

«**Política de Seguridad de la Información del Consejo Insular de Mallorca**

Índice

1. Aprobación y entrada en vigor

Texto aprobado el 26 de septiembre de 2018 por elConsejo Ejecutivo delConsejo Insular de Mallorca.

Esta política de seguridad de la información es efectiva desde la fecha mencionada y hasta que sea reemplazada por una política nueva.

2. Introducción

El Consejo Insular de Mallorca, en adelante el Consejo, depende de los sistemas de las tecnologías de la información y la comunicación

(TIC) para alcanzar sus objetivos.

Estos sistemas tienen que ser administrados con diligencia, tomando las medidas adecuadas para protegerlos de daños accidentales o deliberados que puedan afectar a la disponibilidad, la integridad o la confidencialidad de la información tratada o los servicios prestados.

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 rapidez a los incidentes.

Los sistemas de las TIC tienen que estar protegidos contra amenazas de evolución rápida con potencial para incidir en la confidencialidad, en la integridad, en la disponibilidad, en el uso previsto y en el valor de la información y en 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. Eso implica que los agentes implicados se tienen que aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como hacer un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes agentes implicados tienen que garantizar que la seguridad de las TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde la concepción del servicio hasta la retirada, pasando por las decisiones desarrollo o de adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación se han de identificar e incluir en la planificación y ejecución de los proyectos de las TIC, tanto si se hacen con recursos propios como externos.

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece que las administraciones públicas se tienen que relacionar entre sí y con sus órganos, organismos públicos y entidades vinculadas o dependientes a través de medios electrónicos. Estos medios tienen que asegurar la interoperatividad y seguridad de los sistemas y de las soluciones adoptadas, tienen que garantizar la protección de los datos de carácter personal y tienen que facilitar preferentemente la prestación conjunta de servicios a las personas interesadas. En este sentido, el artículo 156 de la mencionada Ley 40/2015, de 1 de octubre, regula el Esquema Nacional de Seguridad.

Por otra parte, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en el artículo 13 reconoce una serie de derechos de las personas en sus relaciones con las administraciones públicas. Entre estos derechos, se reconoce el derecho relativo a la protección de datos de carácter personal y, en particular, a la seguridad y confidencialidad de los datos que figuren en los ficheros, en los sistemas y en las aplicaciones de las administraciones públicas.

El Real Decreto 3/2010, de 8 de enero, por el cual se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, modificado parcialmente por el Real Decreto 951/2015, de 23 de octubre, tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en el ámbito de aplicación, los principios básicos y los requisitos mínimos que permitan una protección adecuada de la información.

El artículo 11 del mencionado Real Decreto 3/2010, de 8 de enero, exige que todos los órganos superiores de las administraciones públicas dispongan formalmente de su política de seguridad, que tiene que aprobar el titular del órgano superior correspondiente. Esta política de seguridad se tiene que establecer sobre la base de los principios básicos recogidos en el capítulo II de la misma norma (seguridad integral, gestión de riesgos, prevención, reacción y recuperación, líneas de defensa, re-evaluación periódica y función diferenciada) y tiene que desplegar una serie de requisitos mínimos consignados en el artículo 11.1, que ya hemos mencionado.

Los principios básicos son directrices fundamentales de seguridad que se tienen que tener siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes:

a. Alcance estratégico: la seguridad de la información tiene que contar con el compromiso y apoyo de todos los niveles directivos, de manera que pueda estar coordinada e integrada con el resto de iniciativas estratégicas del organismo para conformar un todo coherente y eficaz.
b. Responsabilidad diferenciada: en los sistemas de información se tiene que diferenciar la persona responsable de la información, que determina los requisitos de seguridad de la información tratada; la persona responsable del servicio, que determina los requisitos de seguridad de los servicios prestados; la persona responsable del sistema, que tiene la responsabilidad sobre la prestación de los servicios y la persona responsable de la seguridad, que determina las decisiones para satisfacer los requisitos de seguridad.
c. Seguridad integral: la seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema, para evitar, salvo los casos de urgencia o de necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información se tiene que considerar una parte de la operativa habitual, tiene que estar presente y se tiene que aplicar desde el diseño inicial de los sistemas de información.
d. Gestión de riesgos: el análisis y la gestión de riesgos es una parte esencial del proceso de seguridad. La gestión de riesgos permite mantener un entorno controlado y minimizar los riesgos hasta niveles aceptables. La reducción de estos niveles se hace mediante el despliegue de medidas de seguridad y se establece un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos en que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos se tienen que tener en cuenta los riesgos que se deriven del tratamiento de los datos personales.
e. Proporcionalidad: el establecimiento de medidas de protección, detección y recuperación tiene que ser proporcional a los riesgos

potenciales, a la criticidad y al valor de la información i de los servicios afectados.

f. Mejora continua: las medidas de seguridad se tienen que reevaluar y actualizar periódicamente para adecuar la eficacia a la evolución constante de los riesgos y de los sistemas de protección. La seguridad de la información tiene que ser atendida, revisada y auditada por personal cualificado, instruido y dedicado.
g. Seguridad por defecto: los sistemas se tienen que diseñar y configurar de manera que garanticen un grado suficiente de seguridad por defecto.

3. Ámbito de aplicación

Esta política de seguridad se tiene que aplicar a toda la información del Consejo Insular de Mallorca.

4. Misión y objetivos

El Consejo reconoce como activos estratégicos la información y los sistemas que la gestionan.

Uno de los objetivos fundamentales de la implantación de esta política de seguridad es establecer las bases para que tanto los empleados públicos como la ciudadanía puedan acceder a los servicios públicos en un entorno seguro y de confianza.

La política de seguridad de la información define el marco global para gestionar la seguridad de la información, proteger todos los activos de información y garantizar la continuidad en el funcionamiento de los sistemas. Se pretende así minimizar los riesgos derivados de un posible fallo en la seguridad y asegurar el cumplimiento de los objetivos del Consejo ante un hipotético incidente de seguridad de la información.

Para eso, se establecen los objetivos generales en materia de seguridad de la información:

a. Contribuir desde la gestión de la seguridad a cumplir la misión y los objetivos del Consejo.
b. Disponer de las medidas de control necesarias para garantizar que se cumplen los requisitos legales que sean aplicables como consecuencia de la actividad desarrollada, especialmente con respecto a la protección de datos de carácter personal y a la prestación de servicios a través de medios electrónicos o telemáticos.
c. Garantizar la implantación de las medidas y de los mecanismos de seguridad apropiados para proteger los servicios prestados, los sistemas de información empleados para prestarlos y la información procesada, almacenada o transmitida por estos, de manera coherente con los riesgos afrontados.
d. Garantizar la eficacia de las medidas de seguridad implantadas por medio de evaluaciones y auditorías.
e. Establecer una estructura organizativa adecuada para gestionar la seguridad de la información y definir los roles y los comités necesarios, además de las funciones y las responsabilidades respectivas.
f. Garantizar la operación continuada y adecuada de los servicios y de los sistemas, y actuar para prevenir, detectar, reaccionar y operar de manera oportuna ante los incidentes de seguridad que se produzcan, además de velar para que se implanten los mecanismos necesarios para asegurar la continuidad de las actividades críticas y permitir que se recuperen en un período de tiempo aceptable.
g. Impulsar y fomentar la formación, la concienciación y el cumplimiento de las obligaciones en materia de seguridad de la información del personal al servicio de la organización, a fin de garantizar el conocimiento de las políticas y de las normativas aprobadas, y de las prácticas recomendadas, con el objetivo último de conseguir que la seguridad de la información se convierta en un factor inherente al desarrollo de las funciones y de las operativas cotidianas.
h. Promover que las actividades destinadas a conseguir los niveles de seguridad requeridos se estructuren y se conciban como un proceso de mejora continua, y no como acciones o esfuerzos puntuales, y sustentarlo en el análisis y la gestión sistematizados de los riesgos.
i. Proteger los activos de información de la administración del Consejo y la tecnología que los gestionan ante cualquier amenaza, intencionada o accidental, interna o externa, para asegurar la confidencialidad, la integridad, la disponibilidad, la autenticidad y la trazabilidad.

Esta política de seguridad asegura un compromiso continuo y manifiesto del Consejo para difundir y consolidar la cultura de la seguridad.

5. Marco normativo

El diseño, la operación, el uso y la administración de la información, de los sistemas de información y de los servicios del Consejo tienen que cumplir las normas siguientes, las cuales se mencionan con carácter enunciativo y no limitador:

a. Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal
b. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de les Administraciones Públicas
c. Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público
d. Ley 59/2003, de 19 de diciembre, de Firma Electrónica
e. Real Decreto 3/2010, de 8 de enero, por el cual se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica

f. Real Decreto 4/2010, de 8 de enero, por el cual se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica
g. Real Decreto 1720/2007, de 21 de diciembre, por el cual se aprueba el Reglamento de despliegue de la Ley Orgánica 15/1999
h. Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de les personas físicas con respecto al tratamiento de datos personales y a la libre circulación de estos datos y por el cual se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
i. Ordenanza por la cual se regula la Administración electrónica del Consejo Insular de Mallorca y los organismos que dependen (BOIB núm. 69, de 16 de mayo de 2013)

6. Organización de la seguridad

La estructura organizativa para gestionar la seguridad de la información en el ámbito descrito por esta política de seguridad de la información está formada por los agentes siguientes:

a. Comité de Seguridad de la Información
b. Responsables de la información
c. Responsables del servicio
d. Responsable de la seguridad
e. Responsables del sistema
f. Delegado o delegada de la protección de datos de carácter personal

La estructura organizativa es competente para mantener, actualizar y hacer cumplir, dentro del ámbito definido, la política de seguridad de la información.

6.1 Comité de Seguridad de la Información

Composición y funcionamiento

Integran el Comité de Seguridad de la Información:

a) Presidencia: el consejero ejecutivo o la consejera ejecutiva competente en materia de tecnologías y sistemas de información

b) Vocalías:

- Las personas titulares de las Secretarias Técnicas de todos los departamentos del Consejo de Mallorca
- La persona titular de la Secretaría General
- La persona responsable de la seguridad
- El delegado o la delegada de la protección de datos de carácter personal

Asimismo, forman parte del Comité como vocales con voz, pero sin voto:

- Las personas responsables del sistema.
- Las personas que, en cada caso, proponga la Presidencia, en calidad de asesores.

El Comité de Seguridad de la Información puede consultar al personal técnico, propio o externo, la información pertinente para tomar decisiones

El Comité se tiene que reunir con carácter ordinario al menos una vez al año y, con carácter extraordinario, en los supuestos siguientes:

a. A instancia de la Presidencia.
b. Cuando haya incidencias de seguridad graves o surjan necesidades de seguridad nuevas que requieran la participación de los componentes del Comité.

Para que el Pleno del Comité se pueda constituir de manera válida y hacer sesiones, deliberar y tomar acuerdos se requerirá, en primera convocatoria, la presencia del presidente o presidenta, del secretario o secretaria y de la mitad más uno de los miembros.

El Pleno tiene que adoptar los acuerdos por mayoría de los miembros presentes con derecho a voto.

El funcionamiento del Comité se tiene que ajustar a lo que prevé la Ley 40/2015.

Funciones

Al Comité de Seguridad de la Información le corresponden funciones de asesoramiento, de consultoría y de propuesta en materia de seguridad de la información.

En particular, le corresponde:

a. Informar regularmente del estado de la seguridad de la información a los órganos superiores correspondientes.
b. Promover la mejora continua del sistema de gestión de la seguridad de la información.
c. Elaborar i revisar la política de seguridad de la información para que los órganos superiores correspondientes lo aprueben.
d. Impulsar el cumplimiento de la política de seguridad de la información y su despliegue normativo.
e. Aprobar la normativa de seguridad de la información a propuesta de la persona responsable de la seguridad.
f. Aprobar los procedimientos de actuación en relación con la seguridad de los servicios de las TIC.
g. Aprobar el plan de auditoría y el plan de formación propuestos por la persona responsable de la seguridad.
h. Proponer planes de mejora de la seguridad de la información de la organización.
i. Velar para que la seguridad de la información se tenga en cuenta en todos los proyectos de tecnologías de la información en todas les fases: a la hora de redactar la especificación inicial, en el momento de la puesta en marcha y en el mantenimiento posterior, así como a la hora de preservar la información que sea requerida una vez se ha dejado de utilizar. En particular, tiene que velar para crear y utilizar servicios horizontales que reduzcan duplicados y den soporte a un funcionamiento homogéneo de todos los sistemas de las TIC.
j. Divulgar la política de seguridad de la información y las normativas e instrucciones de seguridad de la información aprobadas, con la promoción de actividades de concienciación y formación en materia de seguridad para el personal.
k. Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones sobre estos riesgos.
l. Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.

6.2 Responsables de la información

La persona responsable de la información es la que tiene la competencia suficiente para decidir sobre la finalidad, el contenido y el uso de esta información, y de determinar dentro del marco establecido en el Anexo I del Real Decreto 3/2010, de 8 de enero, por el cual se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, los requisitos de seguridad de la información tratada.

La persona designada tiene que figurar en la documentación de seguridad del sistema de información.

Funciones

a. Establecer los requisitos, en materia de seguridad, de la información que manejan. Si esta información incluye datos de carácter personal, además se tienen que tener en cuenta las medidas de seguridad que corresponda implantar, vistos los riesgos generados por el tratamiento de acuerdo en lo que exige el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.
b. Hacer, juntamente con las personas responsables del servicio y de la responsable de la seguridad, los análisis de riesgos preceptivos y seleccionar las salvaguardias que se tienen que implantar.
c. Aceptar los riesgos residuales respecto de la información calculados en el análisis de riesgos.
d. Hacer el seguimiento y control de los riesgos, con la participación de la persona responsable de la seguridad.
e. Suspender, de acuerdo con la persona responsable del servicio y con la responsable de seguridad, la prestación de un servicio electrónico o el manejo de una determinada información, si es informado de deficiencias graves de seguridad.

6.3 Responsables del servicio

La persona responsable del servicio es la persona con competencia suficiente para decidir sobre la finalidad y prestación de este servicio y tiene que determinar dentro del marco establecido en el Anexo I del Real Decreto 3/2010, de 8 de enero, por el cual se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, los requisitos de seguridad de los servicios prestados.

La persona designada tiene que figurar en la documentación de seguridad del sistema de información.

Funciones

a. Establecer los requisitos, en materia de seguridad, de los servicios. Si estos servicios incluyen datos de carácter personal, además, se tienen que tener en cuenta las medidas de seguridad que corresponda implantar, dados los riesgos generados por el tratamiento de acuerdo a lo que exige el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.
b. Hacer, juntamente con los responsables de la información y de la seguridad, los análisis de riesgos preceptivos.
c. Aceptar los riesgos residuales respecto de la información calculados en el análisis de riesgos.
d. Hacer el seguimiento y control de los riesgos, con la participación de la persona responsable de la seguridad.
e. Suspender, de acuerdo con la persona responsable de la información y con la de la seguridad, la prestación de un servicio electrónico o el manejo de una determinada información, si es informado de deficiencias graves de seguridad.

6.4 Responsable de la seguridad

La persona responsable de la seguridad la tiene que designar la persona titular del departamento con competencias en materia de seguridad de las tecnologías de la información y la comunicación entre el personal adscrito a este departamento.

La persona designada tiene que figurar en la documentación de seguridad del sistema de información.

Funciones

Son funciones de la persona responsable de la seguridad:

a. Actuar como un secretario o secretaria del Comité de Seguridad de la Información.
b. Estar al corriente de los cambios de la tecnología y del entorno en la cual vive la organización, informarse de las consecuencias para las actividades de seguridad de la información, alertar al Comité de Seguridad de la Información y proponer las medidas oportunas de adecuación.
c. Presentar regularmente informes sobre el estado de seguridad de los servicios de las TIC al Comité de Seguridad de la Información.
d. Elaborar el análisis de riesgos de los sistemas de las TIC y presentarla al Comité de Seguridad de la Información para que la apruebe. Este análisis se tiene que actualizar regularmente.
e. Ejecutar regularmente verificaciones de seguridad según un plan que el Comité de Seguridad de la Información ha predeterminado y aprobado. Los resultados de estas inspecciones se tienen que presentar al Comité de Seguridad de la Información para que los conozca y los apruebe. Si, como resultado de la inspección, aparecen incumplimientos, la persona responsable de la seguridad tiene que proponer medidas correctoras que tiene que presentar al Comité de Seguridad de la Información para que las apruebe.
f. Elaborar el plan de seguridad y hacer el seguimiento. Este plan se tiene que presentar al Comité de Seguridad de la Información para que lo apruebe.
g. Promover el despliegue del marco normativo en materia de seguridad.
h. Elaborar para que el Comité de Seguridad de la Información les apruebe los requisitos de formación y cualificación de administradores, operadores y usuarios desde el punto de vista de seguridad de las TIC.
i. Preparar los informes pertinentes en caso de incidentes excepcionalmente graves y en caso de desastres. Se tiene que presentar un informe detallado al Comité de Seguridad de la Información.
j. Coordinar la respuesta en caso de incidentes que desborden los casos previstos y procedimentados. Es la persona responsable de coordinar la investigación forense relacionada con incidentes que se consideren relevantes.
k. Proponer a las personas responsables de la información la determinación de los niveles de seguridad en cada dimensión de seguridad siempre que se le solicite.
l. Proponer a las personas responsables del servicio la determinación de los niveles de seguridad en cada dimensión de seguridad siempre que se le solicite.
m. Mantener la documentación de seguridad organizada y actualizada y gestionar los mecanismos para acceder.
n. Promover la mejora continua en la gestión de la seguridad de la información.
o. Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de acontecimientos de la seguridad y por los mecanismos de auditoría implementados en el sistema.
p. Proponer la categoría del sistema según el procedimiento descrito en el anexo I del Real Decreto 3/2010, de 8 de enero, y las medidas de seguridad que se tienen que aplicar de acuerdo con lo que prevé el anexo II del mismo Real Decreto.
q. Asumir las funciones explícitamente atribuidas a la figura de responsable de seguridad en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad.

6.5 Responsables del sistema

Las personas responsables del sistema las tiene que designar la persona titular del departamento con competencias en materia de las tecnologías de la información y la comunicación entre el personal adscrito a este departamento.

Las personas designadas tienen que figurar en la documentación de seguridad del sistema de información.

Funciones

a. Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, así como encargarse de las especificaciones, de la instalación y de la verificación que funciona correctamente.
b. Definir la topología y el sistema de gestión del sistema de información, y establecer los criterios de uso y los servicios disponibles.
c. Asegurar que les medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
d. Acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio, si la persona responsable del sistema es informada de deficiencias graves de seguridad que puedan afectar a la satisfacción de los requisitos establecidos. Esta decisión se tiene que acordar con las personas responsables de la información afectada, del servicio afectado y con la persona responsable de la seguridad, antes de ejecutarla.
e. Elaborar los planes de mejora de la seguridad junto con la persona responsable de la información.
f. Planificar la implantación de salvaguardas en los sistemas.
g. Ejecutar los planes de seguridad aprobados.

6.6 Delegado o delegada de protección de datos

El delegado o la delegada de protección de datos es único para todos los órganos y organismos del Consejo Insular de Mallorca y se tiene que informar del nombramiento y cese a la Agencia Española de Protección de Datos.

Les funciones del delegado o de la delegada de protección de datos son las que se indican en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en otras disposiciones reguladoras de la materia.

La persona designada tiene que figurar en la documentación de seguridad del sistema de información.

6.7 Resolución de conflictos

En caso de conflicto entre las diferentes personas responsables que componen la estructura organizativa de la política de seguridad de la información, la Presidencia del Comité es la encargada de resolverlo y tienen que prevalecer las exigencias más altas derivadas de la protección de datos de carácter personal. Los casos en qué no tenga bastante autoridad para decidir, los tiene que elevar.

7. Datos de carácter personal

Con respecto a los datos de carácter personal que trata el Consejo, se tienen que adoptar les medidas técnicas y organizativas que corresponda implantar, vistos los riesgos generados por el tratamiento una vez hecha la evaluación exigida por el artículo 24.1 del Reglamento (UE) 2016/679.

En caso de conflicto entre las diferentes personas responsables tienen que prevalecer las exigencias más altas derivadas de la protección de datos de carácter personal.

8. Gestión de riesgos

La gestión de riesgos se tiene que hacer de manera continua sobre los sistemas de información, de acuerdo con los principios de gestión de la seguridad basada en los riesgos y en la evaluación periódica. La persona responsable del servicio se tiene que encargar de que se haga el análisis preceptivo de riesgos y que se proponga el tratamiento adecuado, calculando los riesgos residuales.

La persona responsable de la seguridad, dentro de su ámbito de actuación, es la encargada de recomendar un marco de directrices básicas para armonizar los criterios a seguir para valorar los riesgos.

Las personas responsables de la información y del servicio son las propietarias de los riesgos sobre la información y sobre los servicios, respectivamente, y son responsables del seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

El proceso de gestión de riesgos, que comprende las fases de categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, que tienen que ser proporcionales a los riesgos y tienen que estar justificadas; se tiene que revisar y se tiene que aprobar cada año por la persona titular del órgano o de la unidad administrativa o, en su caso, del organismo autónomo, a través de un plan de adecuación al Esquema Nacional de Seguridad.

Les fases indicadas del proceso de gestión de riesgos se tienen que hacer según lo que disponen los anexos I y II del Real Decreto 3/2010, de 8 de enero, y siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones para la aplicación elaboradas por el Centro Criptológico Nacional, así como toda la información referente al análisis de riesgo y de impacto en la protección de datos especificada en el mencionado Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril del 2016.

Aunque se necesita un control continuo de los cambios hechos en los sistemas, este análisis se tiene que repetir:

a. Al menos una vez al año (mediante una revisión y una aprobación formal).
b. Cuando cambie la información manejada.
c. Cuando cambien los servicios prestados.
d. Cuando haya un incidente grave de seguridad.
e. Cuando se reporten vulnerabilidades graves.

9. Despliegue de la política de seguridad de la información

El marco normativo de la política de seguridad de la información se tiene que estructurar en los niveles siguientes:

a. Esta política de seguridad de la información tiene que establecer los requisitos y criterios de protección de carácter global.
b. Les normas de seguridad tienen que definir qué hay que proteger y los requisitos de seguridad deseados.
    - El conjunto de todas las normas de seguridad tiene que abarcar la protección de todos los entornos de los sistemas de información de la organización.

- Estas normas tienen que establecer un conjunto de expectativas y de requisitos que se tienen que alcanzar para poder satisfacer y cumplir cada uno de los objetivos de seguridad establecidos en la política.
- Las tiene que proponer la persona responsable de la seguridad y las tiene que aprobar el Comité de Seguridad de la Información.

c. Los procedimientos de seguridad tienen que describir, de forma concreta, cómo proteger todo lo que se establece en las normas, y también las personas o los grupos que tienen que ser responsables de implantarlos, mantenerlos y hacer el seguimiento del nivel de cumplimiento.

- Son documentos que tienen que especificar cómo llevar a cabo las tareas habituales, quien tiene que hacer cada tarea y como identificar y reportar comportamientos anómalos.
- La aprobación depende del ámbito de aplicación, que puede ser en un ámbito específico o en un sistema de información determinado.

Además, se pueden establecer guías con recomendaciones y buenas prácticas.

10. Revisión de la política

El Comité de Seguridad de la Información tiene que revisar y proponer las actualizaciones necesarias de la política de seguridad de la información cuando:

a. Se hagan cambios en el marco legal que puedan cuestionar la validez de esta política.
b. Se detecten incidencias de seguridad que supongan un incremento significativo del nivel de riesgo actual o que hayan causado un impacto en los sistemas de información del Consejo.
c. Lo considere oportuno para mejorar la seguridad de la información del Consejo.

La revisión de la política de seguridad de la información tiene que garantizar la alineación con la estrategia, la misión y la visión del Consejo en materia de seguridad de la información y tiene que asegurar que se cumplen los objetivos de control establecidos.

Para cumplir este objetivo, el Comité de Seguridad de la Información puede proponer cualquier modificación que considere necesaria.

11. Obligaciones del personal

Todo el personal con responsabilidad en el uso, operación o administración de sistemas de tecnologías de la información y las comunicaciones tiene la obligación de conocer y cumplir esta política de seguridad de la información y la normativa de seguridad derivada, independientemente del tipo de relación jurídica que le vincule con el Consejo.

Todas las personas recibirán formación para el manejo seguro de los sistemas en la medida que la necesiten para llevar a cabo su trabajo.

La política de seguridad tiene que ser accesible para todo el personal que preste los servicios en el Consejo Insular de Mallorca.

Con el objetivo de fomentar la cultura de la seguridad, el Comité de Seguridad de la Información promoverá un programa de concienciación continua para formar a todo el personal.

Si se incumple la política de seguridad y la normativa de despliegue, se establecerán medidas preventivas y correctoras encaminadas a salvaguardar y proteger las redes y los sistemas de información, sin perjuicio de exigir la responsabilidad disciplinaria correspondiente.

12. Relaciones con terceros

Cuando la Administración del Consejo preste servicios o ceda información a otras administraciones públicas u organismos, se les tiene que hacer partícipes de esta política de seguridad de la información y de las normas e instrucciones derivadas.

Asimismo, cuando la Administración utilice servicios de terceros o ceda información a terceros, se les tiene que hacer igualmente partícipes de esta política de seguridad de la información, de la normativa y de las instrucciones de seguridad que corresponda a estos servicios o información. Los terceros quedan sujetos a las obligaciones y medidas de seguridad que establece la normativa y las instrucciones, y pueden desarrollar sus procedimientos operativos propios para satisfacerla. Se tienen que establecer procedimientos específicos de detección y resolución de incidencias. Se tiene que garantizar que el personal de terceros esta concienciado adecuadamente en materia de seguridad de la información, al menos al mismo nivel que el que se establece en esta política de seguridad de la información.

En concreto, los terceros tienen que garantizar que se cumple la política de seguridad de la información basándose en estándares auditables que permitan verificar que estas políticas se cumplen. Asimismo, se tienen que garantizar, mediante una auditoría o un certificado de destrucción o de borrado, que el tercero cancela y elimina los datos pertenecientes a la Administración del Consejo al acabar el contrato.

Cuando algún aspecto de la política de seguridad de la información no pueda ser satisfecho por una tercera parte, se requerirá un informe de la persona responsable de seguridad de la información que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá que la persona responsable de la información y de los servicios afectados apruebe este informe antes de seguir adelante.»

Palma, 11 d'octubre de 2018

El SecretarioGeneral por delegación del presidente
(Decreto de día 20 de julio de 2015, BOIBnúm. 114, de 28 de julio)
Jeroni M. Mas Rigo