I. Principado de Asturias

• Otras Disposiciones

CONSEJERÍA DE ECONOMÍA Y EMPLEO

RESOLUCIÓN de 19 de septiembre de 2014, de la Consejería de Economía y Empleo, por la que se acuerda la aprobación de la política de seguridad de los sistemas de información en la Administración del Principado de Asturias.

La Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos consagra el derecho de los ciudadanos a comunicarse electrónicamente con la Administración Pública y señala, en su exposición de motivos, "que el principal reto que tiene la implantación de las Tecnologías de la Información y las Comunicaciones en la sociedad en general, y en la Administración en particular, es la generación de confianza suficiente que elimine o minimice los riesgos asociados a su utilización".

Asimismo, el artículo 3 de la mencionada ley, manifiesta la necesidad de "crear las condiciones de confianza en el uso de los medios electrónicos, estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos".

A esta necesidad, le da respuesta la propia Ley 11/2007 en su artículo 42.2, mediante la creación del Esquema Nacional de Seguridad, que obliga a las Administraciones Públicas a adoptar cuantas medidas de seguridad técnicas y organizativas sean precisas para hacer efectivas estas condiciones de seguridad.

El Esquema Nacional de Seguridad, regulado por el Real Decreto 3/2010, de 8 de enero, establece el marco regulatorio de la Política de Seguridad de la Información, y obliga a los órganos superiores de las Administraciones Públicas a dotarse formalmente de una Política de Seguridad que permita la adecuada protección de la información.

En este sentido, el artículo 11 del Real Decreto 3/2010 señala que todos los órganos superiores de las Administraciones Públicas deberán disponer formalmente de su Política de Seguridad aprobada por el titular del órgano superior correspondiente y que dicha política deberá establecerse conforme a los principios básicos y requisitos mínimos que se relacionan en los capítulos II y III del mencionado Real Decreto.

Además, la Política de Seguridad de la Información debe ser coherente con las exigencias del Real Decreto 1720/2007, de 21 de diciembre por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

En cuanto a la aprobación de la Política de Seguridad de la Información por parte del titular del órgano superior correspondiente, el artículo 11.2 del Real Decreto 3/2010 considera que son órganos superiores, los responsables directos de la ejecución de la acción del gobierno, central, autonómico o local, en un sector de actividad especifico de acuerdo con lo establecido en sus propias normas de organización.

A este respecto y conforme a la asignación de competencias efectuadas por el Decreto 73/2012, de 14 de junio, por el que se establece la estructura orgánica básica de la Consejería de Economía y Empleo, modificado por Decreto 228/2012 de 26 de diciembre y por Decreto 23/2013 de 30 de abril, le corresponden a la Consejería de Economía y Empleo las competencias en materia de gestión centralizada de los servicios informáticos y de comunicación de la Administración del Principado.

Por todo lo anterior y de conformidad con lo establecido en el artículo 38 de la Ley 6/1984, de 5 de julio, del Presidente y del Consejo de Gobierno del Principado de Asturias y los artículos 21, 32, 33 y 34 de la Ley 2/1995, de 13 de marzo, sobre Régimen Jurídico de la Administración del Principado de Asturias, por la presente,

D I S P O N G O

Artículo 1.—*Objeto.*

El objeto de la presente resolución es aprobar la Política de Seguridad de los sistemas de información de la Administración del Principado de Asturias, que se incorpora como anexo.

Artículo 2.—*-Ámbito de aplicación.*

1. Esta Resolución será de aplicación a los órganos de la Administración del Principado de Asturias y a los organismos públicos y entes públicos que utilicen los sistemas de información y/o de comunicaciones de la Administración del Principado de Asturias.

2. Deberá de ser observada por todo el personal de los órganos y organismos citados, y por cualquier persona que no perteneciendo a los anteriores tenga acceso a los sistemas de información y/o de comunicaciones de la Administración del Principado de Asturias.

Cód. 2014-15986

Artículo 3.—*Desarrollo técnico.*

Por resolución de la Consejería competente se procederá al desarrollo técnico de la presente disposición.

Disposición derogatoria

Queda derogada la Resolución de 17 de junio de 2011 de la Consejería de Administraciones Públicas y Portavoz del Gobierno que aprueba la política de seguridad de los sistemas de información en la Administración del Principado de Asturias.

Disposición final

La presente resolución entrará en vigor al día siguiente al de su publicación en el *Boletín Oficial del Principado de Asturias*.

En Oviedo, a 19 de septiembre de 2014.—El Consejero de Economía y Empleo, Graciano Torre González.—Cód. 2014-15986.

Anexo

Índice

1. Alcance.

La presente política aplica a todos los sistemas TIC (Tecnologías de la Información y las Comunicaciones) dentro del ámbito de gestión de la Dirección General de Tecnologías de la Información y las Comunicaciones, y a todos los usuarios con acceso autorizado a los mismos, sean o no empleados públicos y con independencia de la naturaleza de su relación jurídica con la Administración del Principado.

2. Misión del organismo.

La Administración del Principado de Asturias, bajo la dirección del Consejo de Gobierno, desarrolla su actuación para alcanzar los objetivos establecidos por las leyes y el resto del ordenamiento jurídico, sirviendo con objetividad a los intereses generales y actuando de acuerdo con los principios de eficacia, jerarquía, descentralización, desconcentración y coordinación, con sometimiento pleno a la Constitución, a la Ley y al Derecho.

Las competencias que corresponden a la Comunidad Autónoma del Principado de Asturias serán ejercidas por los órganos superiores de la Administración del Principado, conforme a lo establecido en el Estatuto de Autonomía para Asturias.

3. Objetivos en materia de seguridad de la información.

La Administración del Principado de Asturias considera esencial que en el tratamiento de la información, en su almacenamiento y procesamiento se garanticen los mayores niveles de seguridad y el máximo compromiso en su veracidad, disponibilidad y confidencialidad.

Igualmente el uso seguro y responsable de unos recursos que son corporativos, y en muchos casos compartidos, obliga a valorar la aplicación de medidas que contribuyan al mejor aprovechamiento tecnológico de los equipos, redes de comunicaciones, y aplicaciones y al desarrollo, cara al ciudadano, de una Administración electrónica eficaz y confiable.

Las medidas a tomar no pueden ser intuitivas o sobrevenidas sino bien calculadas, adaptadas a los niveles de riesgo asumidos, y correctamente procedimentadas, documentadas y aplicadas.

En materia de seguridad de la información se pretenden lograr los siguientes objetivos:

a. Establecer las bases de un modelo integral de gestión de la seguridad y los riesgos, que cubra en un ciclo de mejora continuo los aspectos técnicos, organizativos y procedimentales.

Cód. 2014-15986

b. Implantar las más adecuadas medidas de seguridad física y lógica, desde una óptica técnica, normativa y organizativa para asegurar la integridad, confidencialidad y disponibilidad de los datos en el entorno específico de la Administración del Principado de Asturias.

c. Garantizar a los usuarios de los sistemas informáticos de la Administración del Principado de Asturias que sus equipos, recursos y datos están adecuadamente protegidos frente a cualquier tipo de acceso indebido o sustracción/manipulación de la información.

d. Concienciar a los niveles más elevados de decisión en la Organización, sobre la importancia de cumplir y hacer cumplir las normas relativas a la seguridad informática, tanto las emanadas desde esta Política de Seguridad como las generadas por normas y leyes de carácter estatal o supranacional.

e. Fomentar el conocimiento de la Política de Seguridad y de sus normas entre todos los usuarios, reiterando con la mayor frecuencia y de la forma más efectiva su contenido, sus implicaciones, y las causas que las justifican.

f. Convertir la seguridad en un eje transversal para la Organización y para sus sistemas de información de manera que junto al rendimiento y operatividad se valore la necesidad de aplicar y respetar restricciones de seguridad, especialmente cuando afecte a las garantías y derechos de trabajadores y usuarios.

g. Concienciar al conjunto de usuarios de la importancia de su participación y comportamiento para lograr la mejor protección y uso de la información y de los recursos corporativos, así como de la obligatoriedad en el cumplimiento de las normativas de seguridad.

h. Entender que la gestión de los riesgos y la imposición de una Política de Seguridad debe de hacerse desde una normativa clara, bien difundida, revisable periódicamente y estricta, pero a la par flexible ante circunstancias específicas y modelos tecnológicos y sociales cambiantes.

i. Incrementar comités y grupos de trabajo específicos de seguridad, con participación de los diferentes servicios, direcciones y Consejerías, y con capacidad para cooperar en el diseño de procedimientos operativos de seguridad y en la mayor difusión de tales procedimientos en toda la Administración.

j. Analizar internamente pero también de manera externa, vía auditoria, la calidad de la seguridad de los sistemas de información, fomentando la consecución de normas estándares de excelencia.

4. Marco legal y regulatorio.

Normativa de ámbito estatal:

- Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
- Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre de protección de datos de carácter personal.
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- 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.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

Normativa autonómica:

- Decreto 111/2005, de 3 de noviembre, sobre registro telemático.
- Decreto 115/2008, de 20 de noviembre, de modificación del Decreto 111/2005, de 3 de noviembre, sobre registro telemático.

También forman parte del marco legal y regulatorio, las Normas derivadas del desarrollo de la presente Política de Seguridad de la Información, que detallan aspectos particulares de la gestión de la seguridad de los sistemas de información.

5. Organización de la seguridad: Funciones y responsabilidades.

La información constituye un activo de primer orden para la Administración desde el momento en que resulta esencial para la prestación de gran parte de sus servicios. La Administración del Principado de Asturias considera fundamental mantener la información manejada y los servicios prestados por sus sistemas de información con un nivel de protección adecuado. Para lograr dicho propósito, resulta imprescindible la creación de un marco de referencia para establecer las responsabilidades generales en la gestión de la seguridad de los sistemas de información, y asignar funciones específicas sobre la seguridad de la información.

Dentro del marco organizativo, le corresponde a la Dirección General de Tecnologías de la Información y las Comunicaciones (según el Decreto 73/2012, de 14 de junio, por el que se establece la estructura orgánica básica de la Consejería de Economía y Empleo) ejercer las funciones de dirección, diseño, desarrollo, implantación y mantenimiento de los programas y políticas de seguridad en materia de sistemas de información para todos los ámbitos de la Administración del Principado de Asturias.

Cód. 2014-15986

La Dirección General de Tecnologías de la Información y las Comunicaciones en el ejercicio de sus competencias y al objeto de alinear la Política de Seguridad de la Información con los requerimientos del Esquema Nacional de Seguridad (regulado por el Real Decreto 3/2010, de 8 enero), priorizará las siguientes actuaciones:

a. Promover la mejora continua en la gestión de la Seguridad de la Información.
b. Revisar regularmente la Política de Seguridad de la Información para que sea aprobada por el titular de la Consejería con competencias en materia de Seguridad de la Información.
c. Aprobar la Normativa de Seguridad de la Información.
d. Promover la realización de las auditorias periódicas que permitan verificar el cumplimiento de las obligaciones de la Administración del Principado de Asturias en materia de seguridad de la información.
e. Supervisar, controlar y coordinar los esfuerzos en materia de seguridad de la información de las diferentes áreas, tanto las específicamente destinadas a labores técnicas informáticas como a las que en cada momento requieran una respuesta TIC a sus necesidades funcionales; de tal forma se pretende asegurar que dichos esfuerzos sean consistentes y alineados con la normativa y la legislación vigente en materia de seguridad de la información.

5.1. Responsabilidad general.

El artículo 12 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS), establece que la seguridad deberá comprometer a todos los miembros de la organización. En este sentido, la preservación de la seguridad TIC y el seguimiento de las normas específicas que desarrollan esta Política, serán considerados objetivos comunes para todos los empleados de la Administración del Principado de Asturias, especialmente para aquellos que participen en cualquier fase del tratamiento de la información o tengan acceso a los locales donde se custodie o se realice dicho tratamiento.

Las responsabilidades generales de los usuarios de los sistemas de información incluyen el uso correcto y coherente de los activos de tecnologías de la información y comunicaciones puestos a su disposición por la Administración del Principado de Asturias para el desarrollo de sus funciones, y la notificación de cualquier incidencia de seguridad de la que tengan conocimiento.

5.2. Responsabilidades particulares.

Adicionalmente a las funciones especificas competencia de la Dirección General de Tecnologías de la Información y las Comunicaciones (según Decreto 73/2012, de 14 de junio, por el que se establece la estructura orgánica básica de la Consejería de Economía y Empleo) y a la responsabilidad general de todos los miembros de la organización, el Esquema Nacional de Seguridad y el Reglamento de desarrollo de la LOPD identifican una serie de roles, a los cuales asignan unas responsabilidades particulares en materia de seguridad de la información. Estos roles son:

El Responsable de la información: en el marco del Esquema Nacional de Seguridad, es la persona, órgano o unidad administrativa que tiene la responsabilidad última del uso que se haga de la información y, por tanto, de su protección. Es el propietario de los riesgos sobre la información y por consiguiente el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.

El Responsable de la información, al objeto de protegerla, tiene la potestad de determinar el nivel de seguridad requerido por la información de la cuál es responsable atendiendo especialmente a los requisitos de integridad y confidencialidad.

En la Administración del Principado de Asturias las funciones que el Esquema Nacional de Seguridad le atribuye al Responsable de la Información son competencia de la Secretaría General Técnica de cada una de las Consejerías.

El Responsable del Fichero: Rol identificado en la LOPD como la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decide sobre la finalidad, contenido y uso del tratamiento de los sistemas de información que contienen datos de carácter personal.

En la Administración del Principado de Asturias está responsabilidad recaerá en el órgano o unidad administrativa que decide sobre la finalidad, contenido y uso del tratamiento.

El Responsable del Servicio: según el Esquema Nacional de Seguridad, es la persona, órgano o unidad administrativa que tiene la potestad de establecer los requisitos del servicio en materia de seguridad.

Para determinar el nivel de seguridad del servicio electrónico, se atenderá especialmente a los requisitos de disponibilidad y trazabilidad, ya que los requisitos de integridad y confidencialidad vienen heredados de la información que maneja el servicio.

En la Administración del Principado de Asturias las funciones que el Esquema Nacional de Seguridad le atribuye al Responsable del Servicio son competencia de la Secretaría General Técnica de cada una de las Consejerías.

El Responsable de Seguridad: Este rol aparece tanto en el Esquema Nacional de Seguridad como en la LOPD.

En el ámbito de la LOPD, el Responsable de Seguridad es la persona o personas a las que el Responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables al citado fichero.

En el marco del Esquema Nacional de Seguridad, el Responsable de Seguridad es la persona, órgano o unidad administrativa que define las medidas necesarias para garantizar la seguridad del sistema de información durante todo su ciclo de vida y vela porque los sistemas de información efectivamente responden a los requisitos de seguridad establecidos.

En la Administración del Principado de Asturias las funciones que el Esquema Nacional de Seguridad le atribuye al Responsable del Seguridad son competencia de la Dirección General de Tecnologías de la Información y las Comunicaciones.

Cód. 2014-15986

El Responsable del Sistema: en el marco del Esquema Nacional de Seguridad, es la persona, órgano o unidad administrativa encargada de implantar las medidas necesarias para garantizar la seguridad del sistema de información durante todo su ciclo de vida, siguiendo las recomendaciones del Responsable de Seguridad y notificando a éste cualquier cambio en el sistema que pueda suponer una alteración previsible en los riesgos que afectan a dicho sistema.

En la Administración del Principado de Asturias las funciones que el Esquema Nacional de Seguridad le atribuye al Responsable del Sistema son competencia de la Dirección General de Tecnologías de la Información y las Comunicaciones.

5.3. Responsabilidades unificadas.

Con carácter general, los roles de Responsable de la Información y de Responsable del Servicio recaerán en el mismo órgano o unidad administrativa. Únicamente se diferenciarán: cuando el servicio maneje información de diferentes procedencias, no necesariamente del mismo órgano o unidad administrativa que presta el servicio o cuando la prestación del servicio no dependa de la misma unidad que el Responsable de la información.

En los Sistemas de información que tienen datos de carácter personal, coincidirán en el mismo órgano o unidad administrativa los roles de Responsable del Fichero y de Responsable de la Información, ya que ambos tienen la responsabilidad última del uso que se haga de la información.

5.4. Resolución de conflictos.

No cabe esperar que se produzcan conflictos entre las funciones de los distintos Responsables, pues las obligaciones respecto a los sistemas de información, vienen derivadas de la normativa aplicable: Esquema Nacional de Seguridad, LOPD, y cualquier otra normativa que resulte de aplicación en función de la información tratada o de los servicios prestados. Con carácter general, siempre deberá cumplirse la normativa de mayor exigencia.

En caso de discrepancia, los datos de carácter personal constituyen un objeto protegido de mayor rango y marcarán la pauta a seguir.

6. Protección de datos de carácter personal.

Los datos de carácter personal que sean objeto de tratamiento por parte de la Administración del Principado de Asturias, se protegerán mediante la implantación de las medidas de seguridad correspondientes, según lo dispuesto en:

- El Título VIII del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre.
- El anexo II del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad.

Para las gestiones derivadas del cumplimiento de la LOPD en los ficheros que contienen datos de carácter personal se utilizará, por parte de los responsables de tales ficheros, la aplicación de "Gestión LOPD", desarrollada a tal efecto por la Administración del Principado de Asturias. En la citada aplicación quedan registrados los ficheros afectados y sus correspondientes documentos de seguridad.

7. Concienciación y formación.

La Administración del Principado de Asturias desarrollará actividades específicas en materia de seguridad de la información, encaminadas a la concienciación y formación de los empleados, así como a la difusión entre los mismos de la Política de Seguridad de la Información y su desarrollo normativo.

De acuerdo al principio de Seguridad Integral recogido en el Esquema Nacional de Seguridad, se impulsarán líneas de actuación al objeto de lograr la plena conciencia respecto a que la seguridad de la información afecta a todos los miembros de la Administración y a todas las actividades desarrolladas. En tal sentido se articularán los medios necesarios para sensibilizar a todo el personal respecto a los riesgos a los que están expuestos los sistemas de información.

La seguridad de la información es el resultado de un proceso que depende tanto de factores técnicos como humanos. Por tanto, se pretende que todos los usuarios con acceso a los sistemas de información de la Administración del Principado de Asturias, conozcan y entiendan sus responsabilidades en materia de seguridad de la información. Quienes participen en cualquier fase del tratamiento de la información deberán responder, en la medida de sus responsabilidades, de la seguridad y buen uso de dicha información, colaborando de esta forma en reducir los riesgos a los que están expuestos los sistemas de información.

La Administración del Principado de Asturias dispondrá los medios para publicar, dar a conocer y facilitar el cumplimiento de esta Política de Seguridad de la Información y de los documentos que la desarrollan, así como para verificar su aplicación y efectividad.

8. Gestión de riesgos.

Los sistemas de información sujetos a esta Política de Seguridad serán sometidos de forma continua a un análisis y gestión de riesgos conforme a los principios de gestión de la seguridad basada en los riesgos (artículo 6 del Real Decreto 3/2010, de 8 de enero) y reevaluación periódica (artículo 9 del Real Decreto 3/2010, de 8 de enero).

El objetivo en este sentido, y en línea con lo que expresa la metodología MAGERIT, es llevar a cabo una gestión de riesgos que permita minimizar o eliminar, a un costo aceptable, los riesgos de seguridad a los que están expuestos los sistemas de información, posibilitando el mantenimiento de un entorno controlado, mediante el despliegue de las oportunas medidas de seguridad.

a. Los Responsables de la Información y del Servicio se encargarán, contando en el proceso con el asesoramiento del Responsable de Seguridad, de determinar los niveles de seguridad de la información para cada dimensión (disponibilidad, integridad, confidencialidad y trazabilidad).

Cód. 2014-15986

Asimismo, una vez realizado el análisis de riesgos, como responsables de los riesgos sobre la información y sobre los servicios, respectivamente, serán los encargados de aceptar los riesgos residuales calculados en el correspondiente análisis.

b. El Responsable de Seguridad, se encargará de categorizar los sistemas de información, realizar los preceptivos análisis de riesgos, y seleccionar las salvaguardas a implantar para minimizar los riesgos hasta niveles aceptables.

c. Los Responsables de la Información, del Servicio y del Sistema se encargarán de implantar las salvaguardas resultantes del análisis de riesgos, dentro de sus competencias.

Para homogenizar los distintos análisis de riesgos, se establecerá por parte de la Dirección General de Tecnologías de la Información y las Comunicaciones una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

En la realización de los análisis de riesgos formales se propone la utilización de la herramienta "Pilar" o "PilarMicro" que facilitan la realización de un seguimiento de la aplicación que se hace de las medidas de seguridad seleccionadas y proporcionan un valor de riesgo residual estabilizado y comparable entre diferentes sistemas de información.

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 deberán ser proporcionales a los riesgos y estar justificadas, se revisarán anualmente por parte del Responsable de Seguridad, siendo pertinente la realización de un informe con el Plan de Gestión del Riesgo, disponible para su consulta por los responsables implicados en el proceso.

9. Desarrollo normativo. Documentación de seguridad.

El cuerpo normativo sobre seguridad de la información se desarrollará en tres niveles, según el grado de concreción en la expresión del 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:

— Primer nivel: Política de Seguridad de la información (constituida por el presente documento).

Marca las directrices generales en materia de seguridad de la información. Se revisará anualmente, siendo aprobada por la Consejería con competencias en la materia y publicada en el BOPA.

Es de obligado cumplimiento para todo el personal con acceso a los sistemas de información de la Administración del Principado de Asturias y se puede consultar en el *Boletín Oficial del Principado de Asturias* y en la intranet https://intranet.asturias.es

— Segundo nivel: Normativa de Seguridad.

Normas de seguridad que tomando como base la Política de Seguridad de la Información, dan respuesta, sin entrar en detalles de implementación ni de tecnologías, a qué se puede hacer y qué no, en relación a un cierto tema desde el punto de vista de la seguridad de la información y a qué se considera un uso apropiado o inapropiado.

Estas normas son de obligado cumplimiento para todo el personal con acceso a los sistemas de información de la Administración del Principado de Asturias y se pueden consultar en https://intranet.asturias.es

— Tercer nivel: Procedimientos operativos e Instrucciones técnicas.

Son documentos que incluyen detalles técnicos y de implementación para dar respuesta a cómo se puede realizar una determinada tarea respetando los principios de seguridad de la información, y los procedimientos operativos internos establecidos en la organización.

Esta documentación es de obligado cumplimiento para el personal que gestiona y opera los sistemas de información de la Administración del Principado de Asturias y estará actualizada y almacenada en el repositorio que establezca la Dirección General de Tecnologías de la Información y las Comunicaciones para su manejo por el personal debidamente autorizado.

Aparte de los anteriores niveles de documentación de seguridad se podrá contar, bajo criterio del Responsable de Seguridad, con otros documentos de carácter no vinculante: recomendaciones de seguridad, informes y buenas prácticas, registros y evidencias electrónicas.

10. Actualización de la Política de Seguridad de la Información.

Anualmente, la Dirección General de Tecnologías de la Información y las Comunicaciones realizará la revisión de la Política de Seguridad de la Información para asegurar que sigue cumpliendo con los requisitos del marco normativo de referencia y que mantiene su idoneidad y eficacia. En caso de considerarse necesario se publicarán renovadas versiones de la misma, de cuya existencia habrá de darse la máxima difusión posible.

La Política de Seguridad de la Información será aprobada por el titular de la Consejería con competencias en materia de Seguridad de la Información.

La Normativa de Seguridad se mantendrá adecuadamente actualizada como marco de referencia base para la explicitación operativa y técnica de las instrucciones concretas que favorecen y posibilitan la seguridad en los distintos procedimientos operativos. La normativa se ajustará a los criterios generales que marca la Política de Seguridad, y estará planteada de manera realista de acuerdo a las necesidades concretas de la organización de la Administración del Principado de Asturias, a los cambiantes desarrollos de las Tecnologías de la Información y a las buenas prácticas y estándares de seguridad.

Cód. 2014-15986

Los procedimientos operativos e instrucciones técnicas se reevaluarán y actualizarán periódicamente; se pretende de esa manera adecuar su eficacia a la constante evolución de los riesgos a los que están expuestos los Sistemas de Información.

11. Incumplimiento.

En caso de conocimiento por parte de la Dirección General de Tecnologías de la Información y las Comunicaciones de incumplimiento de esta Política o de las normas y procedimientos derivados de ella, y en el ejercicio de su competencia y responsabilidad se gestionará el análisis de la situación intentando en primer lugar contrarrestar los riesgos o problemas que tales incumplimientos hayan podido generar, en segundo lugar y en función de cada caso informar, y en ocasiones formar, al usuario que incumple y a sus responsables.

Es fundamental un análisis de los incumplimientos detectados para discernir si son producto de ignorancia técnica, de desconocimiento de las normas o de mal entendimiento de las mismas, o por el contrario de actuaciones premeditadas y con fines malintencionados. La Dirección General Competente en materia TIC, podrá realizar los informes pertinentes sobre los casos de incumplimiento a fin de que se tomen, por quien corresponda, las medidas que correspondan en cada caso.

Cód. 2014-15986