1.DISPOSICIONES GENERALES

CONSEJO DE GOBIERNO

CVE-2015-6977 *Decreto 31/2015, de 14 de mayo, por el que se aprueba la Política de Seguridad de la Información de la Administración de la Comunidad Autónoma de Cantabria.*

En las sociedades de los países desarrollados, el uso de las nuevas tecnologías se ha hecho cotidiano, transformando la vida diaria de los ciudadanos y suponiendo una revolución para el funcionamiento interno de las organizaciones públicas y privadas. También ha introducido cambios profundos en la relación entre estas organizaciones y su entorno: agilizando los intercambios de información entre entidades y permitiendo ofrecer servicios accesibles a las personas en cualquier momento y lugar.

La indudables ventajas que conlleva esta masiva presencia de las nuevas tecnologías, también ha supuesto afrontar importantes desafíos para que su utilización sea compatible con los derechos y deberes de la ciudadanía en los países democráticos.

Entre estos desafíos ha cobrado en los últimos años una excepcional importancia la seguridad de las infraestructuras tecnológicas y de la información que se almacena o se trata con ellas. Existen bandas mafiosas, grupos terroristas y otras organizaciones criminales que practican el tráfico de información privada, el espionaje masivo o dirigido y que en ocasiones realizan sabotajes que afectan a los sistemas de información de organizaciones públicas o privadas.

En el ámbito de las Administraciones Públicas de nuestro país, el Gobierno de España ha sido consciente de la importancia de las nuevas tecnologías y de su utilidad para mejorar los servicios que éstas prestan a los ciudadanos. También de la importancia de la seguridad de la información y de la necesidad de establecer un marco legal para regularla y garantizarla.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, reconoce el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos, regulando los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa, en las relaciones entre las Administraciones Públicas, así como en las relaciones de los ciudadanos con las mismas con la finalidad de garantizar sus derechos, un tratamiento común ante ellas y la validez y eficacia de la actividad administrativa en condiciones de seguridad jurídica.

Entre los fines de esa ley, se señala la necesidad de crear unas condiciones de confianza en el uso de los medios electrónicos, estableciendo las medidas necesarias para la preservación de la integridad y los derechos fundamentales, y en especial, los relacionados con la intimidad y la protección de datos de carácter personal.

El Esquema Nacional de Seguridad aprobado por el Real Decreto 3/2010, de 8 de enero, tiene como meta precisamente atender a esa necesidad, para permitir a los ciudadanos y a las Administraciones Públicas el ejercicio de derechos y el cumplimiento de deberes a través de estos medios. Así, se busca garantizar la calidad de la información y la adecuada prestación de los servicios sin interrupciones, mediante una estrategia de gestión de la seguridad de la información que combine medidas preventivas y de supervisión de la actividad diaria, con procedimientos específicos de respuesta ante los incidentes que pudieran presentarse y con la capacidad de adaptación a los cambios en las condiciones del entorno.

Esta gestión de la seguridad de la información debe entenderse como un proceso integral, constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas de información, descartándose cualquier actuación puntual o tratamiento coyuntural. Esta gestión implica directamente tanto al personal especialista en tecnología, como a los gestores con capacidad de decisión sobre la información o los servicios prestados, así como al resto de personas que usan o acceden de algún modo a los sistemas de informa-

CVE-2015-6977

ción. Por ello se debe prestar la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad.

El Esquema Nacional de Seguridad establece la obligación para las administraciones públicas de poner en marcha un conjunto de medidas de seguridad concretas, de tipo organizativo, operacional y de protección.

Entre las medidas de tipo organizativo incluye la obligación de formalizar una Política de Seguridad de la Información para la organización, en la que se definen, entre otros aspectos, la estructura para la gestión de la seguridad de la información y la asignación de funciones y roles.

Así, el presente decreto, fija esa Política de Seguridad de la Información, estableciendo los objetivos, principios básicos y la estructura organizativa para la gestión de la seguridad de la información en nuestra Administración.

Este decreto es una muestra del firme compromiso de la Administración de la Comunidad Autónoma de Cantabria con la necesidad de realizar una adecuada gestión de la seguridad de la información y con el cumplimiento del Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

En su virtud, a propuesta de la Consejera de Presidencia y Justicia y previa deliberación del Consejo de Gobierno, en su reunión del día 14 de mayo de 2015.

DISPONGO

CAPÍTULO I

Disposiciones generales

Artículo 1. Objeto y ámbito de aplicación

1. El presente decreto tiene por objeto establecer el marco común, las directrices básicas y el régimen organizativo para la gestión de la Seguridad de la Información. Tal y como define el anexo IV del Real Decreto 3/2010, "Seguridad de las redes y de la información, es la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles".

2. Sus previsiones serán de aplicación:

a) A la Administración de la Comunidad Autónoma de Cantabria, comprendiendo ésta, a estos efectos, a la Administración General y los organismos públicos y entidades de derecho público vinculadas o dependientes de la misma, cuando ejerzan funciones administrativas y utilicen sistemas de información gestionados por el órgano directivo con competencias en materia informática. Quedan excluidos del ámbito de aplicación del presente decreto el Servicio Cántabro de Salud y el sector público empresarial y fundacional.

b) A las personas físicas, jurídicas y entes sin personalidad en sus relaciones con las entidades anteriores cuándo procedan al uso de sistemas de información gestionados por el órgano directivo con competencias en materia informática.

Artículo 2. Misión de la organización

La Administración de la Comunidad Autónoma desarrolla funciones ejecutivas de carácter administrativo según lo establecido en el artículo 42 de la Ley de Cantabria 6/2002, de 10 de diciembre, de Régimen Jurídico del Gobierno y de la Administración de la Comunidad Autónoma de Cantabria.

CVE-2015-6977

Artículo 3. Objetivos y directrices básicas de la gestión de la seguridad de la información.

1. Los objetivos de la gestión de la seguridad de la información son los siguientes:

a) La protección de la información frente a accesos y modificaciones no autorizadas.

b) La protección de la información y de los servicios frente a fallos en la disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad.

c) El adecuado tratamiento de los incidentes de seguridad.

d) El cumplimiento de requisitos legales.

2. Las directrices básicas para la gestión de la seguridad de la información son las siguientes:

a) Una gestión formal y racionalizada de la seguridad de la información.

b) La determinación de las responsabilidades en materia de seguridad de la información de todos los órganos y personas implicadas.

c) La coordinación con otras normas en materia de seguridad, aunque no estén relacionadas directamente con la Seguridad de la Información, que puedan existir en el ámbito de la Administración de la Comunidad Autónoma de Cantabria.

Artículo 4. Principios de la política de seguridad de la información.

La gestión de la seguridad de la información, y por tanto el funcionamiento del Sistema de Gestión de la Seguridad de la Información (SGSI), se regirá por los siguientes principios básicos:

a) Seguridad integral.

b) Gestión de riesgos.

c) Prevención, reacción y recuperación.

d) Líneas de defensa.

e) Reevaluación periódica.

f) Función diferenciada.

CAPÍTULO II

Organización de la gestión de la seguridad de la información

Artículo 5. Estructura organizativa.

La organización para la gestión de la seguridad de la información en la Administración de la Comunidad Autónoma de Cantabria se estructura en:

a) Comisión General de Seguridad de la Información.

b) Comité Técnico de Ciberseguridad.

c) Responsables de la información y responsables del servicio.

d) Gestores responsables.

e) Responsable de Seguridad de la Información.

f) Responsables de los Sistemas.

g) Administradores de Ciberseguridad de los Sistemas.

h) Responsables de los ficheros que contengan datos de carácter personal.

i) Comisiones, comités y responsables sectoriales de Seguridad de la Información.

Artículo 6. Creación, composición y régimen de funcionamiento de la Comisión General de Seguridad de la Información.

1. Se crea la Comisión General de Seguridad de la Información, que estará constituida por los siguientes miembros:

CVE-2015-6977

a) Presidente: El Consejero con competencias en materia informática.

b) Secretario: El Responsable de Seguridad de la Información.

c) Vocales: Los Secretarios Generales de cada Consejería y el titular del órgano directivo con competencias en materia informática.

2. El presidente podrá convocar, con voz pero sin voto, a otras personas especializadas en los temas a tratar.

3. La Comisión se reunirá con carácter ordinario una vez al año y con carácter extraordinario a propuesta de su presidente o de un tercio de los vocales que la integran.

4. Esta Comisión se regirá por el presente decreto, por las normas sobre los órganos colegiados de sección 5ª del Capítulo II del Título II de la Ley de Cantabria 6/2002, de 10 de diciembre, de Régimen Jurídico del Gobierno de Cantabria y de la Administración de la Comunidad Autónoma de Cantabria, y en lo que resulte de aplicación, conforme las previsiones del Capítulo II del Título II de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Artículo 7. Funciones de la Comisión General de Seguridad de la Información.

A la Comisión General de Seguridad de la Información le corresponden las siguientes funciones:

a) Informar del estado de la seguridad de la información en la Administración de la Comunidad Autónoma de Cantabria al Consejo de Gobierno.

b) Elaborar la estrategia de seguridad de la información de la Administración de la Comunidad Autónoma de Cantabria.

c) Promover los proyectos de seguridad de la información y proponer la dotación de recursos a estos.

d) Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.

e) Coordinar los esfuerzos de las diferentes Consejerías, así como de otras entidades dependientes o vinculadas a la Administración de la Comunidad Autónoma de Cantabria, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia y evitar duplicidades.

f) Elaborar, y revisar regularmente, la Política de Seguridad de la Información para ser aprobada por el Consejo de Gobierno.

g) Emitir informes proponiendo la aprobación de las normas de seguridad de carácter general.

h) Emitir informes sobre el grado de cumplimiento de las normas de seguridad de carácter general.

i) Definir la estrategia a seguir para la gestión de los riegos residuales.

j) Supervisar los resultados de las auditorías e impulsar la realización de acciones correctivas.

k) Aprobar planes de mejora de la seguridad de la información.

l) Aprobar planes de continuidad de la prestación de los servicios.

m) Aprobar los análisis de riesgos.

n) Establecer prioridades para las actuaciones en materia de seguridad de la información cuando los recursos sean limitados.

o) Resolver los conflictos de responsabilidad que competencialmente le correspondan.

Artículo 8. Creación, composición y régimen de funcionamiento del Comité Técnico de Ciberseguridad.

1. Se crea el Comité Técnico de Ciberseguridad, que estará formado por:

a) Presidente: El titular del órgano directivo con competencias en materia informática.

CVE-2015-6977

b) Secretario: El Responsable de Seguridad de la Información.

c) Vocales: Jefe de Centro de Proceso de Datos, Jefe del Servicio de Informática, Jefe de Centro de Tecnologías INET y Responsable de Seguridad de la Información.

2. El presidente podrá convocar, con voz pero sin voto, a otras personas especializadas en los temas a tratar.

3. El comité se reunirá con carácter ordinario dos veces al año y con carácter extraordinario a propuesta de su presidente o de un tercio de los vocales que la integran.

4. Este Comité se regirá por el presente decreto, por las normas sobre los órganos colegiados de sección 5ª del Capítulo II del Título II de la Ley de Cantabria 6/2002, de 10 de diciembre, de Régimen Jurídico del Gobierno de Cantabria y de la Administración de la Comunidad Autónoma de Cantabria, y en lo que resulte de aplicación, conforme las previsiones del Capítulo II del Título II de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Artículo 9. Objetivos y funciones del Comité Técnico de Ciberseguridad.

1. El Comité Técnico de Ciberseguridad tiene como objetivos fundamentales desarrollar los aspectos técnicos y procedimentales de la seguridad de la información.

2. Al Comité Técnico de Ciberseguridad le corresponden las siguientes funciones:

a) Emitir informes proponiendo la aprobación de las normas de seguridad y procedimientos de seguridad de carácter técnico.

b) Emitir informes proponiendo la aprobación de procedimientos de seguridad que desarrollen las normas de seguridad de carácter general.

c) Emitir informes sobre el grado de cumplimiento de las normas de seguridad de carácter técnico, así como del grado de cumplimiento de los procedimientos que desarrollen normas de seguridad técnicas o de carácter general.

d) Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.

e) Monitorizar los principales riesgos residuales asumidos por la Administración de la Comunidad Autónoma de Cantabria y recomendar posibles actuaciones respecto de ellos.

f) Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.

g) Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.

h) Velar por la coordinación de los planes de mejora de la seguridad de la información que afecten a varias áreas.

i) Velar por la coordinación de los planes que puedan realizarse en diferentes áreas.

j) Proponer y desarrollar los planes de mejora de la seguridad de la información.

k) Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.

l) Preparar informes del estado de la seguridad de la información para la Comisión General de Seguridad de la Información.

Artículo 10. Responsables de la Información y Responsables del Servicio.

Las funciones de los Responsables de la Información y de los Responsables del Servicio que establece el Esquema Nacional de Seguridad serán desempeñadas por los Directores Generales o equivalentes en el ámbito de sus competencias.

CVE-2015-6977

Para aquellos sistemas de información vinculados a la gestión propia de las Secretarías Generales, o bien aquellos que atañan a varias Direcciones Generales, las funciones de Responsable de la Información y Responsable del Servicio serán desempeñadas por los Secretarios Generales o equivalentes, y en las entidades de derecho público por los órganos equivalentes.

Artículo 11. Funciones de los Responsables de la Información y Responsables de los Servicios.

A los Responsables de la Información y Responsables de los Servicios, en el ámbito de sus competencias, les corresponden las siguientes funciones:

a) Establecer el uso que se hará de la información.

b) Establecer las características de los servicios prestados.

c) Establecer los requisitos en materia de seguridad y determinar los niveles de seguridad de la información.

d) Establecer los requisitos en materia de seguridad y determinar los niveles de seguridad de los servicios.

e) Decidir sobre la aceptación del riesgo residual de los sistemas de información relacionados con la información o los servicios de los que son responsables.

f) Establecer las directrices sobre la asignación de accesos a las personas a la información o los servicios, partiendo de los siguientes principios básicos:

1º. Los accesos se concederán exclusivamente a las personas que lo requieran para el desempeño de sus funciones.

2º. El alcance de los accesos se limitará a lo estrictamente necesario para el adecuado desempeño de las funciones y tareas encomendadas.

3º. Los accesos deberán suspenderse cuando dejen de ser necesarios.

4º. En la asignación de los accesos se deberá tener en consideración el cumplimiento de la Política de Seguridad de la Información contenida en este Decreto y las normas de seguridad y procedimientos de seguridad que la desarrollen.

g) Procurar la existencia de planes de continuidad cuando sean necesarios.

h) Velar por una adecuada gestión de la seguridad de la información en el ámbito de su Secretaría General o Dirección General.

i) Colaborar en la gestión global de la seguridad de la información.

Para desarrollar estas funciones, contarán con la colaboración de los Gestores Responsables, que se corresponderán con los titulares de aquellas unidades a su cargo con rango de Servicio o equivalentes.

Artículo 12. Gestores Responsables.

Los Gestores Responsables serán los responsables de unidades con rango de Servicio o equivalentes que utilicen servicios o sistemas tecnológicos, aplicaciones o activos informáticos en general (carpetas de red, buzones departamentales, listas de distribución o recursos informáticos similares), para el desarrollo de sus competencias.

También los Subdirectores para aquellos servicios o sistemas tecnológicos, aplicaciones o activos informáticos en general sobre los que tengan capacidad de decisión y responsabilidad directa.

Artículo 13. Funciones de los Gestores Responsables.

1. A los Gestores Responsables les corresponden las siguientes funciones:

a) Velar por la adecuada gestión de la seguridad en el ámbito de sus competencias y colaborar con los Responsables de la Información o Responsables de los Servicios.

b) Establecer las personas que debe tener acceso en cada momento a los sistemas de información y a los activos que estén vinculados a su ámbito competencial, según las directrices

CVE-2015-6977

que le marque el Responsable de la Información o Responsable de los Servicios correspondiente o en su defecto, los principios básicos señalados en el artículo 11 apartado f).

c) Solicitar los accesos que necesiten las personas dependientes del mismo, o el personal de entidades externas vinculadas a sus contratos de prestación de servicios, procurando que se cumplan los requisitos de seguridad y confidencialidad que se requieran.

d) Identificar procesos y elementos clave en su ámbito competencial, así como sus riesgos asociados, para la clasificación de los servicios, sistemas, aplicaciones o activos.

e) Colaborar en la realización de auditorías de seguridad de la información.

f) Proporcionar la información que sea necesaria para una adecuada gestión de la seguridad de la información.

g) Informar sobre incidentes que puedan afectar a la seguridad de la información.

h) Colaborar en la elaboración de planes de continuidad.

i) Proponer a los Responsables de la Información o Responsables de los Servicios la valoración de las dimensiones de la seguridad de la información o de los servicios.

2. Se podrán aprobar normas de seguridad o procedimientos de seguridad que regulen el funcionamiento operativo de los "Gestores Responsables".

Artículo 14. Responsable de Seguridad de la Información.

1. El Responsable de Seguridad de la Información se corresponde con la persona que ocupe el puesto, adscrito al órgano directivo competente en materia de informática, que tenga encomendadas las funciones de dirección, coordinación y supervisión de la seguridad en la tecnología de la información.

2. Al Responsable de Seguridad de la Información le corresponde coordinar de manera continua el desarrollo de la seguridad de la información en el ámbito de aplicación del presente decreto y ejercer de interlocutor entre los distintos órganos, unidades o entidades de derecho público que componen la organización de gestión de la seguridad de la información.

3. Para el desarrollo de sus funciones, el Responsable de Seguridad de la Información podrá contar con un equipo compuesto por personal del órgano directivo con competencias en materia informática que le prestará apoyo y asesoramiento especializado. También podrá ayudarse de contratos de prestación de servicios cuando sea necesario.

Artículo 15. Funciones del Responsable de Seguridad de la Información.

Al Responsable de Seguridad de la Información le corresponde las siguientes funciones:

a) Procurar el mantenimiento de la seguridad de la información tratada y de los servicios prestados, de acuerdo a lo establecido en la Política de Seguridad de la Información.

b) Impulsar la elaboración de normas y procedimientos de seguridad de la información.

c) Promover una adecuada gestión de la seguridad de la información.

d) Diseñar y proponer acciones para la mejora de la seguridad de la información.

e) Impulsar la creación de planes de continuidad.

f) Promover la formación y concienciación en materia de seguridad de la información.

g) Realizar análisis de riesgos, seleccionar salvaguardas y medidas de seguridad, proponer y supervisar su implantación, así como revisar el proceso de gestión del riesgo.

h) Establecer pautas para la determinación de la categoría de los sistemas.

i) Supervisar y coordinar los proyectos de adecuación al Esquema Nacional de Seguridad.

j) Elaborar la declaración de aplicabilidad.

k) Coordinar los incidentes de seguridad de la información que desborden los casos previstos y regulados mediante procedimientos de seguridad de la información.

l) Asesorar a la organización que compone la estructura de seguridad de la información en lo relativo a la evolución tecnológica y metodológica en materia de seguridad de la información.

CVE-2015-6977

m) Elaborar informes sobre el estado de la seguridad de la información.

n) Promover auditorías periódicas para verificar el cumplimiento de obligaciones en materia de seguridad de la información.

o) Ejercer de interlocutor con otras organizaciones en materia de seguridad de la información.

p) Gestionar y mantener el Sistema de Gestión de Seguridad de la Información en su ámbito de actuación, procurando la consistencia de su documentación y su mejora continua.

Artículo 16. Responsables de los Sistemas.

1. Se trata del personal que ocupe las jefaturas de las unidades administrativas de la Dirección General con competencia en materia informática, y que desarrollen funciones estratégicas. Estas unidades serán determinadas en cada momento por el titular del órgano directivo con competencia en materia informática.

2. Son los responsables de la implementación efectiva de las medidas de seguridad y de la correcta gestión de la seguridad de la información en los sistemas de tecnológicos y de información a cargo de su unidad administrativa.

Artículo 17. Funciones de los Responsables de los Sistemas.

Las funciones de los Responsables de los Sistemas en materia de seguridad de la información son:

a) Coordinar a los Administradores de la Ciberseguridad de los Sistemas de su unidad administrativa.

b) Impulsar, coordinar y garantizar el desarrollo, operación y mantenimiento de los Sistemas de Información a cargo de su unidad, durante todo su ciclo de vida, de sus especificaciones, instalaciones y verificación de su correcto funcionamiento.

c) Definir, en colaboración con el personal de su unidad, la arquitectura, los criterios de uso y las características de los servicios a prestar con los sistemas de su ámbito de competencias.

d) Organizar la implementación, gestión y mantenimiento de las medidas de seguridad aplicables a los sistemas de información.

e) Supervisión de la correcta aplicación de las medidas de seguridad que correspondan en los distintos sistemas de información, asegurándose de su correcta integración dentro del marco general de la seguridad.

f) Supervisar la correcta aplicación de las normas y procedimientos de seguridad en los trabajos técnicos que se realizan sobre los sistemas de información.

g) Informar al Responsable de Seguridad de la Información sobre anomalías en la aplicación de las normas y procedimientos de seguridad.

h) Monitorizar el estado de la seguridad de los sistemas y notificar incidentes de seguridad.

i) Coordinar el tratamiento de los incidentes de seguridad y las vulnerabilidades de los sistemas de información a su cargo.

j) Impulsar la creación de planes de contingencia y recuperación, así como participar en la elaboración de planes de continuidad. Coordinar la realización de las pruebas de verificación que correspondan en cada caso.

k) Colaborar en auditorías y en, general, colaborar en la mejora continua de la gestión de la seguridad.

l) Elaborar procedimientos operativos de seguridad.

m) Elaborar planes de mejora de la seguridad en colaboración con el Responsable de Seguridad de la Información.

n) Podrá acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la

CVE-2015-6977

satisfacción de los requisitos establecidos en materia de seguridad y existe riesgo razonable de daños de difícil reparación. De la adopción de esta decisión se informará a los responsables de la información afectada, del servicio afectado y el Responsable de la Seguridad de la Información.

Artículo 18. Administradores de la Ciberseguridad de los Sistemas.

Se trata del personal técnico especializado que se encarga de dirigir las líneas tecnológicas estratégicas de la Administración de la Comunidad Autónoma de Cantabria y que serán los responsables de implementación y gestión la seguridad de la información en cada una de esas líneas, dentro del marco de la Política de Seguridad de los Sistemas de Información y de las normas de seguridad y procedimientos de seguridad que la desarrollen.

Artículo 19. Funciones de los Administradores de la Ciberseguridad de los Sistemas.

1. Las funciones de los Administradores de la Ciberseguridad de los Sistemas son:

a) Implementar, gestionar y mantener las medidas de seguridad aplicables al Sistema de Información.

b) Gestionar, configurar y actualizar, en su caso, el hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.

c) Gestionar las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.

d) Aplicar los procedimientos operativos de seguridad de la información.

e) Aprobar los cambios en la configuración vigente del Sistema de Información.

f) Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.

g) Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.

h) Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.

i) Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.

j) Informar a los Responsables de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.

k) Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

l) Participar en el diseño de los aspectos técnicos de los planes de contingencia, recuperación o continuidad.

m) Realizar pruebas de verificación de los planes de contingencia, recuperación o continuidad.

n) Asesorar en materia de seguridad de la información en lo relativo a su campo de actuación a la Comisión General de Seguridad de la Información, al Comité Técnico de Ciberseguridad, a las comisiones o comités sectoriales que pudiera existir, a los Responsables de los Sistemas o al Responsable de Seguridad de la Información.

2. Estas funciones podrán ser desarrollarlas directamente por los Administradores de Ciberseguridad, también coordinando éstos a otros empleados públicos o mediante la supervisión y control de contratos de prestación de servicios.

Artículo 20. Responsables de los ficheros que contengan datos de carácter personal.

Los responsables de ficheros que contengan datos de carácter personal deberán cumplir con lo dispuesto en la normativa sobre protección de datos de carácter personal y el resto de disposiciones legales de aplicación. También deberán aplicar la Política de Seguridad establecida en este decreto y las normas de seguridad o procedimientos de seguridad que la desarrollen.

CVE-2015-6977

Artículo 21. Comisiones, comités y responsables de la Seguridad de la Información sectoriales.

1. Por orden del Consejero competente en materia informática pueden crearse otras Comisiones o Comités para el estudio, informe y propuesta sobre seguridad de la información en materias sectoriales concretas.

2. Podrán crearse Responsables de Seguridad de la Información sectoriales en aquellos organismos públicos o entidades de derecho público vinculadas o dependientes de la Administración de la Comunidad Autónoma de Cantabria, así como en aquellos sectores de la Administración que necesiten un tratamiento particularizado.

3. Los Responsables de Seguridad de la Información sectoriales deberán respetar en sus actuaciones la Política de Seguridad de la Información y las normas de seguridad de la información o procedimientos de seguridad de la información que correspondan, así como estar coordinados con el Responsable de Seguridad de la Información al que se refiere el artículo 14 del presente decreto.

CAPÍTULO III

Gestión de la seguridad de la información

Artículo 22. Protección de datos personales.

Todos los sistemas de información se ajustarán a los niveles de seguridad requeridos por la normativa de protección de datos de carácter personal.

Artículo 23. Gestión de riesgos.

1. La gestión de riesgos es un factor esencial para una exitosa gestión de la seguridad de la información. En ella deberán colaborar los Responsables de la Información, Responsables de los Servicios, Gestores Responsables, Responsables de los Sistemas y Administradores de Ciberseguridad, según sus competencias y funciones.

2. El Responsable de Seguridad de la Información impulsarán la realización de análisis de riesgos en su ámbito de competencias y establecerán las pautas para la categorización de los sistemas.

3. Por parte del Responsable de Seguridad se realizará un análisis de riesgos de los sistemas de información gestionados por la Dirección General con competencias en material informática, que será revisado y aprobado por la Comisión General de Seguridad de la Información, con carácter anual.

Artículo 24. Desarrollo de la Política de Seguridad de la Información.

1. La Política de Seguridad de la Información que establece este decreto se desarrollará por medio de las Normas de Seguridad de la Información y los Procedimientos de Seguridad de la Información específicos, en aquellos ámbitos en que sea conveniente para su correcta gestión.

2. Las Normas de Seguridad de la Información desarrollan la Política de Seguridad de la Información.

a) Regularán con carácter general los siguientes aspectos:

1º. Usos correctos, e indebidos, de los equipos, servicios e instalaciones.

2º. Responsabilidad respecto al cumplimiento o violación de la Política de Seguridad de la Información y las normas o procedimientos que la desarrollen.

3º. Clasificación y tratamiento de la información.

4º. Criterios para la asignación de accesos, su control y seguimiento.

5º. Continuidad en la prestación de los servicios.

6º. Seguridad física.

CVE-2015-6977

7º. Contratación de sistemas o servicios tecnológicos.

8º. Funciones y responsabilidades de seguridad.

9º. Otras materias de similares características.

b) Serán aprobadas mediante orden de la Consejería con competencias en materia informática, previo informe preceptivo de la Comisión General de Seguridad de la Información.

3. Los Procedimientos de Seguridad de la Información son aquellos que, o bien regulan los detalles operativos o técnicos; o bien definen aspectos tecnológicos o metodológicos relacionados con la seguridad de la información, aplicados al desarrollo, implantación o gestión de sistemas, aplicaciones o servicios. Serán aprobados mediante instrucción del titular del órgano directivo con competencias en materia informática, previo informe preceptivo del Comité Técnico de Ciberseguridad.

4. La Política de Seguridad, Normas de Seguridad y Procedimientos de Seguridad, se complementarán con la documentación técnica, metodológica u operativa que resulte necesaria para la adecuación gestión de la seguridad de la información y la implantación de las medidas de seguridad que sean oportunas.

Artículo 25. Formación, concienciación e información.

La Dirección General con competencias en materia informática:

a) Desarrollará acciones de formación y concienciación en materia de seguridad de la información.

b) Procurará que las personas que utilicen los sistemas de información gestionados en al ámbito de sus competencias, o que accedan a la información en ellos contenidos, reciban de forma efectiva información sobre las obligaciones que suponen ese uso o acceso.

c) Dispondrá los medios necesarios para que las personas con responsabilidad en la administración u operación tecnológica de los sistemas de información reciban la formación necesaria para desarrollar su actividad acorde a los requisitos y necesidades de una correcta gestión de la seguridad de la información y una efectiva aplicación de las medidas de protección que correspondan.

Artículo 26. Obligaciones del personal.

1. Todas las personas que utilicen o tengan acceso a los sistemas tecnológicos o de información de la Administración de la Comunidad Autónoma de Cantabria, así como a la información en ellos contenida, tienen las siguientes obligaciones:

a) Conocer y respetar la Política de Seguridad de la Información, así como las normas de seguridad y procedimientos de seguridad que la desarrollen y que le afecten.

b) Atender a las acciones de concienciación en materia de seguridad de la información que se realicen.

c) Utilizar los servicios y sistemas de información, así como la información en ellos contenida y a la que tengan acceso, con una finalidad profesional acorde a las tareas encomendadas en función de su puesto de trabajo y a los fines y propósitos que motivaron la concesión del acceso.

d) Velar por la confidencialidad de la información a la que tenga acceso según la clasificación y características de la misma.

e) Notificar eventos que puedan suponer un incidente de seguridad o evidencien una debilidad que pueda implicar posteriores incidentes.

f) Colaborar en la resolución de incidentes de seguridad y en la realización de acciones preventivas cuando sea necesaria su participación.

g) Participar en la estructura de gestión de la seguridad de la información cuando corresponda según las competencias y funciones de su puesto de trabajo.

h) No realizar acciones intencionadas que perjudiquen la seguridad de los sistemas tecnológicos o de información, ni la información que contienen.

CVE-2015-6977

2. El incumplimiento de estas obligaciones podrá ser sancionado de conformidad con la normativa disciplinaria correspondiente.

3. En el caso de personas vinculadas a entidades externas, el uso se limitará a las tareas o actividades circunscritas en los términos del contrato o acuerdo que regula la relación entre esa entidad y la Administración de la Comunidad Autónoma de Cantabria.

4. Los ciudadanos que realicen trámites utilizando los servicios de Administración Electrónica, o que accedan a páginas web o sistemas públicos de la Administración de la Comunidad Autónoma de Cantabria, no están afectados por las obligaciones señaladas en el apartado 1 de este artículo, si bien, podrán aprobarse normas o recomendaciones específicas para el uso o acceso a esos servicios o sistemas que les pudieran afectar, en cuyo caso serían debidamente informados en el acceso a los mismos.

Artículo 27. Terceras partes.

1. Cuando se presten servicios a otros organismos o se ceda información a terceros:

a) Se les hará partícipes de la Política de Seguridad de la Información establecida en el presente decreto y de las normas de seguridad o procedimientos de seguridad relacionados con el servicio o la información afectados.

b) Se establecerán canales de información y coordinación entre los respectivos responsables de gestión de la seguridad de la información y se establecerán procedimientos de seguridad para la reacción ante incidentes.

2. Cuando se utilicen servicios o se maneje información de otros organismos o entidades, se procurarán canales de información y coordinación en materia de seguridad de la información.

3. En los contratos de adquisición de sistemas o aplicaciones informáticas, de prestación de servicios tecnológicos, y también en el caso de contratos de prestación de servicios de otro tipo que implique el uso de servicios, aplicaciones o sistemas informáticos internos, se deberán tener en cuenta las medidas y consideraciones de seguridad de la información que resulten de aplicación, según la legislación vigente en la materia y especialmente lo señalado en el artículo 9 del Decreto 74/2014, de 27 de noviembre, de Régimen Jurídico de la Administración Electrónica de la Comunidad Autónoma de Cantabria. También se deberán tener en cuenta las medidas y consideraciones de seguridad de la información que resulten de aplicación legal, en caso de acuerdos de cesión de sistemas, aplicaciones o acceso a servicios de otros organismos o entidades.

4. Cuando algún aspecto de la Política de Seguridad de la Información no pueda ser satisfecho por una tercera parte, se requerirá del Responsable de Seguridad de la Información un informe sobre los riesgos en que se puede incurrir y la forma de tratarlos. A la vista de dicho informe y antes de que se haga efectiva la prestación uso, acceso o cesión de que se trate, los responsables de la información o de los servicios decidirán sobre la aceptación o no del riesgo residual de los sistemas de información relacionados con la información o los servicios de los que son responsables.

Artículo 28. Colaboración con otras entidades públicas.

Se promoverán acuerdos de colaboración con otras entidades públicas con competencias en materia de seguridad de la información, especialmente con el Centro Tecnológico Nacional (CCN) y el Instituto Nacional de Ciberseguridad (INCIBE).

Artículo 29. Resolución de conflictos.

En el caso de conflicto sobre alguna decisión relacionada con la seguridad de la información, ésta se resolverá conforme a la siguiente atribución:

a) Si el conflicto es entre Gestores Responsables de una misma Dirección General, decidirá el Responsable de la Información o Responsable del Servicio superior a las partes.

b) Si el conflicto es entre Gestores Responsables o bien entre Responsable de la Información o Responsable del Servicio de dos Direcciones Generales distintas, decidirá el Secretario General de la Consejería correspondiente.

CVE-2015-6977

c) Si el conflicto entre Administradores de Ciberseguridad, decidirá el Responsable del Sistema correspondiente.

d) Si el conflicto es entre Responsables del Sistemas, decidirá el Responsable de Seguridad de la Información.

e) Ante otro tipo de conflictos, decidirá la Comisión General de Seguridad de la Información.

DISPOSICIONES ADICIONALES

Disposición adicional primera. Adecuación de las relaciones de puestos de trabajo.

La Consejería de Presidencia y Justicia procederá a las modificaciones y adaptaciones necesarias de los puestos de trabajo afectados por la asignación de nuevas funciones y tareas previstas en el presente decreto, estableciéndose para su ejecución un plazo de 12 meses a partir de su entrada en vigor. Así mismo, en este plazo, esa Consejería adoptará las actuaciones necesarias para la creación de la unidad de Responsable de Seguridad de la Información, y la adscripción orgánica de los puestos de trabajo necesarios para la correcta prestación del servicio.

Disposición adicional segunda. Adhesiones a la Política de Seguridad de la Información de la Administración de la Comunidad Autónoma de Cantabria.

El Servicio Cántabro de Salud, las entidades del sector público empresarial y fundacional, y otros organismos públicos y entidades de derecho público vinculadas o dependientes de la Administración de la Comunidad Autónoma de Cantabria que no utilicen sistemas de información gestionados por el órgano directivo con competencias en materia informática, podrán adherirse a esta Política de Seguridad, estableciendo su propia estructura de gestión de la Seguridad de la Información y especificando los mecanismos de desarrollo y adaptación que sean precisos para atender a sus necesidades específicas.

DISPOSICIONES TRANSITORIAS

Disposición transitoria primera. Desempeño temporal de las funciones de Responsable de Seguridad de la Información.

Hasta que se proceda a la creación de la unidad de Responsable de Seguridad de la Información, sus funciones serán realizadas por la persona que tenga encomendadas las tareas de dirección, coordinación y supervisión de la seguridad en tecnologías de la información de la Dirección General de Organización y Tecnología.

Disposición transitoria segunda. Desempeño temporal de las funciones asignadas a los titulares de otras unidades u órganos.

Hasta que se proceda a las adaptaciones y modificaciones legales necesarias de los órganos y puestos de trabajo afectados por la asignación de las nuevas funciones y tareas previstas en el presente decreto, éstas deberán ser prestadas por los actuales titulares de los mismos, desde el momento la entrada en vigor del presente decreto.

DISPOSICIONES DEROGATORIAS

Disposición derogatoria única. Derogación Normativa.

Quedan derogadas cuantas disposiciones de igual o inferior rango que se opongan o contradigan lo dispuesto en este decreto.

CVE-2015-6977

DISPOSICIONES FINALES

Disposición final primera. Desarrollo normativo.

Se faculta a la Consejera de Presidencia y Justicia para dictar cuantas disposiciones sean precisas para la aplicación y desarrollo del presente decreto.

Disposición final segunda. Entrada en vigor.

El presente decreto entrará en vigor el día siguiente de su publicación en el Boletín Oficial de Cantabria.

Santander, 14 de mayo de 2015.
El presidente del Gobierno,
Juan Ignacio Diego Palacios.

La consejera de Presidencia y Justicia,
Leticia Díaz Rodríguez.

2015/6977

CVE-2015-6977