1.DISPOSICIONES GENERALES

CONSEJO DE GOBIERNO

CVE-2021-8273 *Decreto 79/2021, de 30 de septiembre, por el que se aprueba la Política Integral de Seguridad de la Información y la Organización competencial para la Protección de Datos Personales de la Administración de la Comunidad Autónoma de Cantabria.*

La Administración de la Comunidad Autónoma de Cantabria, desde hace tiempo ha sido consciente de la importancia de las tecnologías informáticas y de su utilidad para mejorar los servicios que se prestan a la ciudadanía. También de la importancia de la seguridad de la información y de la necesidad de establecer un marco legal para regularla y garantizarla.

Las indudables ventajas que conlleva la generalizada presencia de las herramientas y servicios informáticos 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 grupos de delincuentes y otras organizaciones criminales que practican el tráfico de información, el espionaje masivo o dirigido y que en ocasiones realizan sabotajes que afectan a los sistemas de información de organizaciones públicas o privadas.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, supuso el reconocimiento del 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. Posteriormente, con la entrada en vigor de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, se produce un impulso definitivo a la implantación generalizada en todo el sector público administrativo del expediente íntegramente electrónico y de las relaciones telemáticas entre las Administraciones Públicas y de estas con la ciudadanía.

Entre los fines de actual legislación, 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,

CVE-2021-8273

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 información. 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.

El 26 de mayo de 2015, entró en vigor el 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 el cual se procede a regular todos estos aspectos por primera vez en el ámbito de nuestra Administración.

Posteriormente, el 7 de diciembre de 2018 entró en vigor la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales que desarrolla en el ámbito de nuestro país el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Por ello, es necesario regular en el ámbito de nuestra Administración la organización competencial para la Protección de Datos Personales y dentro de ello, resulta imprescindible determinar las condiciones jurídicas que configure el estatuto jurídico funcional del puesto de trabajo singularizado del Delegado de Protección de Datos, que ostenta por imperativo normativo europeo de unas especiales condiciones legales de garantías legales para su desempeño, además de desarrollar una función de supervisión en la gestión de la protección de datos por parte de cualquier órgano incluidos los directivos y también todas las unidades administrativas, finalmente se detallan también el resto de las funciones que el ordenamiento básico atribuye al mismo. Asimismo, se establecen las bases de los puestos de trabajo que pueden resultar necesarios en nuestra organización interna para el adecuado cumplimiento del referido RGP y de la LOPD, en concreto, la incorporación de los puestos singularizados de los "delegados adjuntos" bajo la supervisión funcional del Delegado de Protección de Datos.

Finalmente, se ha procedido a la modificación al mismo tiempo ciertos aspectos de la vigente Política Integral de Seguridad de la Información de la Administración de la Comunidad Autónoma de Cantabria, con la finalidad de mejorar la implementación y gestión de esta área, tanto en las cuestiones organizativas como en el de diseño de puestos de trabajo de responsables sectoriales de seguridad, delimitando sus tareas y funciones con relación a la nueva organización.

Esta nueva Política Integral de Seguridad contribuirá a garantizar el ejercicio del derecho al autogobierno reconocido a la Comunidad Autónoma de Cantabria, que es la misión de la organización, cumpliendo con el Estatuto de Autonomía de Cantabria y el resto de normativa que le afecta, que constituye el marco legal en el que desarrolla sus actividades, en unas condiciones de seguridad y confianza adecuadas.

En su virtud, a propuesta de la Consejera de Presidencia, Interior, Justicia y Acción Exterior, y previa deliberación del Consejo de Gobierno, en su reunión del día 30 de septiembre de 2021,

CVE-2021-8273

DISPONGO

TÍTULO 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 integral de la Seguridad de la Información y la organización competencial para la Protección de Datos Personales, garantizando el cumplimiento de la normativa vigente en ambas materias, contribuyendo así a la misión de la organización: ejercer el derecho al autogobierno reconocido constitucionalmente a la Comunidad Autónoma de Cantabria.

2. La Seguridad de la Información tendrá como finalidad garantizar de forma integral una adecuada salvaguarda de cualquier tipo de información de valor utilizada por la Administración, incluidos los tratamientos de datos personales de los que sean responsables órganos directivos, organismos públicos y entidades de derecho público vinculadas o dependientes de la Administración de la Comunidad Autónoma de Cantabria en el ejercicio de sus competencias, así como de los servicios que se presten en base a esa información.

3. El presente Decreto también es de aplicación en el ámbito de la prestación de medios materiales y personales a la Administración de Justicia en Cantabria para el cumplimiento del Esquema Judicial de Interoperabilidad y Seguridad (EJIS), en todos aquellos aspectos en que sean coincidentes con el Esquema Nacional de Seguridad (ENS), pudiéndose complementar con normas de Seguridad de la Información o procedimientos de Seguridad de la Información que recojan aspectos del EJIS o de la Política de Seguridad de la Información de la Administración de Justicia, no contemplados por la presente Política o por el Esquema Nacional de Seguridad.

4. Las previsiones de este Decreto serán de aplicación 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, cuando en el ejercicio de sus competencias:

a) Utilicen sistemas de información implantados en las infraestructuras tecnológicas de la Administración de la Comunidad Autónoma de Cantabria.

b) Utilicen servicios tecnológicos en la nube.

c) Traten información, en particular datos personales.

d) Realicen contratos, convenios o encomiendas con terceros cuyo objeto incluya el tratamiento de información o la prestación de un servicio empleando sistemas de información.

5. Quedan excluidos del ámbito de aplicación del presente Decreto, el Sistema sanitario público de Cantabria y el sector público empresarial y fundacional.

6. Además de las exclusiones previstas en el apartado anterior, con relación a la protección de datos personales y su régimen competencial y organizativo de gestión, quedan también excluidos del ámbito de aplicación de este Decreto:

a) Los Centros docentes gestionados por la Consejería competente en materia de Educación.

b) La Administración de Justicia en Cantabria, en todas sus actuaciones con fines jurisdiccionales o vinculadas directamente a los mismas, que estarán sometidas al marco legal y organizativo que en esta materia establezca el Consejo General del Poder Judicial.

CVE-2021-8273

TÍTULO II
Seguridad de la Información

CAPÍTULO I
Objetivos, directrices básicas y principios

Artículo 2. Objetivos y directrices básicas de la Seguridad de la Información.

1. Los objetivos 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 de la Seguridad de la Información son las siguientes:

a) Gestión formal y racionalizada de la Seguridad de la Información.

b) Responsabilidades determinadas de todos los órganos y personas implicadas en la Seguridad de la Información.

c) Adecuada coordinación y/o colaboración en la implementación de 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 3. Principios de la Política de Seguridad de la Información.

La Seguridad de la Información 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.

También se regirá por estos principios básicos el Sistema de Gestión de la Seguridad de la Información (SGSI), entendiendo por tal el sistema de gestión que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la Seguridad de la Información. El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.

CAPÍTULO II
Estructura organizativa y asignación de funciones de la Seguridad de la Información

Artículo 4. Estructura organizativa.

La estructura organizativa de la Seguridad de la Información será la siguiente:

1. Nivel de coordinación y gestión global:

a) Comisión General de Seguridad de la Información.

b) Responsable de Seguridad de la Información de la Administración de la Comunidad Autónoma de Cantabria.

CVE-2021-8273

c) Comité Técnico de Ciberseguridad.

d) Órgano directivo con rango de Dirección General con competencias en materia de informática.

Al cual le corresponderá proponer a la Comisión General de Seguridad de la Información la estrategia de Seguridad de Seguridad de la Información a aprobar, así como las demás funciones que se recojan en este Decreto.

2. Nivel de coordinación y gestión sectorial:

a) Comisiones y Comités Sectoriales de Seguridad de la Información.

b) Responsables Sectoriales de Seguridad de la Información.

c) Coordinadores Sectoriales de Seguridad de la Información.

3. Nivel de implementación de las medidas de seguridad:

a) Responsables de la Información y Responsables del Servicio.

b) Gestores Responsables de Seguridad de la Información.

c) Responsables de los Sistemas de Información.

d) Administradores de Ciberseguridad de los Sistemas de Información.

e) Responsables del Tratamiento.

f) Encargados del Tratamiento.

Artículo 5. Creación, composición y régimen de funcionamiento de la Comisión General de Seguridad de la Información.

1. Adscrita a la Consejería con competencias en materia informática estará la Comisión General de Seguridad de la Información, como órgano colegiado que establecerá la estrategia de seguridad de la información en el ámbito de aplicación de la presente política. La cual estará constituida por los siguientes miembros:

a) Presidente: La persona titular de la Consejería con competencias en materia de informática.

b) Secretario: La persona que tenga asignada la función de Responsable de Seguridad de la Información de la Administración de la Comunidad Autónoma de Cantabria, y como miembro de la Comisión, tendrá así mismo derecho a voto.

c) Vocales: Las personas titulares de las Secretarías Generales de cada Consejería, la persona titular del órgano directivo con rango de Dirección General con competencias en materia de informática, así como la persona que tenga asignada la función de Responsable de Seguridad de la Información de la Administración de la Comunidad Autónoma de Cantabria.

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

3. El Delegado de Protección de Datos de la Administración de la Comunidad Autónoma de Cantabria participará con voz, pero sin voto, en las reuniones de la Comisión General de Seguridad de la Información cuando en el mismo vayan a abordarse cuestiones relacionadas con la protección de datos personales, para lo que será convocado formalmente.

4. La Comisión se reunirá a propuesta de su presidente o en cualquier momento a propuesta de un tercio de los vocales que la integran.

5. Esta Comisión se regirá por el presente Decreto, y por las normas sobre los órganos colegiados de sección 5ª del Capítulo II del Título II de la Ley de Cantabria 5/2018, de 22 de noviembre, de Régimen Jurídico del Gobierno, de la Administración y del Sector Público Institucional de la Comunidad Autónoma de Cantabria y, en lo que resulte de aplicación conforme las previsiones del Capítulo II de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

CVE-2021-8273

Artículo 6. Funciones de la Comisión General de Seguridad de la Información.

A la Comisión General de Seguridad de la Información le corresponden las siguientes funciones en el ámbito de aplicación de la presente política:

a) Asegurar el compromiso de la Administración de la Comunidad Autónoma de Cantabria con una efectiva gestión de la Seguridad de la Información y su mejora continua.

b) Conocer el estado de la Seguridad de la Información en la Administración de la Comunidad de Cantabria.

c) Supervisar la gestión de riesgos.

d) Aprobar la estrategia de Seguridad de la Información, propuesta por el órgano directivo con rango de Dirección General con competencias en materia de informática y supervisar su cumplimiento.

e) Proponer cambios o actualizaciones en la Política de Seguridad de la Información, incluidos los datos personales, en posesión de la Comunidad Autónoma de Cantabria en el ejercicio de sus competencias, así como de los servicios que se presten en base a esa información, así como en su normativa de desarrollo.

f) Coordinar esfuerzos e iniciativas relacionadas con la Seguridad de la Información de las diferentes Consejerías y organismos públicos y entidades de derecho público vinculadas o dependientes.

g) Resolver conflictos de funciones.

h) Informar al Consejo de Gobierno sobre el estado de la Seguridad de la Información, los incidentes relevantes y la estrategia en la materia.

i) Y las demás funciones que se recojan en este Decreto.

Artículo 7. Responsable de Seguridad de la Información de la Administración de la Comunidad Autónoma de Cantabria.

1. El Responsable de Seguridad de la Información de la Administración de la Comunidad Autónoma de Cantabria se corresponde con la persona que ocupe el puesto de trabajo adscrito al órgano directivo con rango de Dirección General con competencias en materia de informática que tenga atribuida la función de Responsable de Seguridad de la Información.

2. El Responsable de Seguridad de la Información de la Administración de la Comunidad Autónoma de Cantabria determinará las decisiones para satisfacer los requisitos de seguridad de la información y los servicios. La responsabilidad sobre la seguridad de los sistemas de información estará diferenciada de la responsabilidad en la prestación de los servicios.

Artículo 8. Funciones de los Responsables de Seguridad de la Información.

1. Al Responsable de Seguridad de la Información de la Administración de la Comunidad Autónoma de Cantabria le corresponden las siguientes funciones:

a) Coordinar el Sistema de Gestión de la Seguridad de la Información en su conjunto e impulsar su continuo y efectivo funcionamiento.

b) Redactar propuestas de normativa de Seguridad de la Información.

c) Diseñar procedimientos de gestión en la materia, así como redactar manuales, estándares y guías de referencia.

d) Informar preceptivamente sobre la validez técnica, en materia de seguridad de la información, de los proyectos de nuevas normas que afecten a la Seguridad de la Información y la Protección de Datos Personales, así como su adecuación al sistema de gestión de la seguridad de la información de la Administración de la Comunidad Autónoma de Cantabria.

e) Establecer las pautas metodológicas y criterios comunes para la realización de categorizaciones de sistemas de información, selección de medidas de seguridad y declaraciones de aplicabilidad, evaluaciones de impacto, análisis de riesgos, procesos de gestión del riesgo y planes de continuidad.

CVE-2021-8273

f) Supervisar, y coordinar en su caso, los proyectos de adecuación al Esquema Nacional de Seguridad y a otras disposiciones legales en materia de Seguridad de la Información, incluida la seguridad de la protección de datos personales, para garantizar la coherencia del Sistema de Gestión de la Seguridad de la Información en la Administración de la Comunidad Autónoma de Cantabria.

g) Ejercer de interlocutor con otras organizaciones en materia de Seguridad de la Información, salvo en lo que corresponda al Delegado de Protección de Datos de la Administración de la Comunidad Autónoma de Cantabria.

h) Coordinación y apoyo para el cumplimiento de las obligaciones en materia de protección de datos personales.

i) Realizar, coordinar y/o supervisar, según proceda en cada caso, las acciones formativas en materia de Seguridad de la Información.

j) Asesorar en materia de Seguridad de la Información.

k) Coordinar a los Responsables Sectoriales de Seguridad de la Información.

l) Colaborar con el Delegado de Protección de Datos de la Administración de la Comunidad Autónoma de Cantabria y sus Delegados adjuntos, para procurar una coherente gestión de Seguridad de la Información de manera integral.

m) Y las demás funciones que se recojan en este Decreto.

2. Al Responsable de Seguridad de la Información de la Administración de la Comunidad Autónoma de Cantabria, así como a los Responsables Sectoriales de Seguridad de la Información, cada uno en su ámbito de actuación, les corresponden:

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 y la legislación vigente en la materia.

b) Promover una adecuada gestión de la Seguridad de la Información y la efectiva implantación de las medidas de seguridad que correspondan.

c) Diseñar y proponer acciones para la mejora de la Seguridad de la Información.

d) Impulsar y coordinar la creación de planes de continuidad.

e) Promover la formación y concienciación en materia de Seguridad de la Información.

f) Realizar análisis de riesgos, evaluaciones de impacto, selección de medidas de seguridad y declaraciones de aplicabilidad.

g) Coordinar los procesos de gestión del riesgo o asesorar sobre ellos.

h) Asesorar en la realización de categorizaciones de sistemas de información.

i) Coordinar los incidentes de Seguridad de la Información que desborden los casos previstos y regulados mediante procedimientos de Seguridad de la Información.

j) Asesorar en materia de Seguridad de la Información, en particular sobre medidas de seguridad, normativa, metodologías de gestión y evolución tecnológica.

k) Elaborar informes sobre el estado de la Seguridad de la Información.

l) Promover auditorías periódicas y velar por que se realicen las que la normativa vigente fije como obligatorias.

m) Gestionar y mantener el Sistema de Gestión de Seguridad de la Información en su ámbito de actuación, procurando la consistencia de los procesos que se diseñen, las actuaciones que se realicen, la documentación generada y los catálogos de activos relevantes para la seguridad de información, incluidos los aspectos técnicos de los registros de actividades de tratamientos. Así como procurar su progresiva mejora.

n) Supervisar a los Coordinadores Sectoriales de Seguridad de la Información existentes en su ámbito de actuación.

o) Colaborar con los órganos colegiados y aquellos funcionarios que desempeñen puestos de trabajo que formen parte de la gestión de Seguridad de la Información de la Administración

CVE-2021-8273

de la Comunidad de Cantabria. Y en particular, con el Delegado de Protección de Datos y sus adjuntos.

p) Aquellas funciones que asigne la legislación básica en materia de Seguridad de la Información.

q) Y las demás funciones que se recojan en este Decreto.

Artículo 9. Medios materiales y recursos humanos del Responsable de Seguridad de la Información de la Administración de la Comunidad Autónoma de Cantabria.

1. El desarrollo de las funciones asignadas al Responsable de Seguridad de la Información de la Comunidad Autónoma de Cantabria, corresponderá al funcionario que desempeñe el puesto de Jefe Servicio de Seguridad de la Información. Este puesto, así como los Responsables Sectoriales de Seguridad de la Información estarán adscritos al órgano directivo, con rango Dirección General, con competencias en materia informática y comunicaciones de esta Administración.

2. A la unidad administrativa Servicio de Seguridad de la Información se le asignarán los recursos necesarios para posibilitar el adecuado cumplimiento de sus funciones en el ámbito de actuación asignado, dotándole del personal de apoyo administrativo y personal experto que resulte necesario para el adecuado desarrollo de sus funciones. Los puestos de trabajo serán incorporados a la correspondiente relación de puestos de trabajo de la Consejería que tenga atribuidas las competencias en materia informática. Asimismo, también podrá acudirse a contrataciones de prestación de servicios externos cuando sea necesario.

Artículo 10. Creación, composición y régimen de funcionamiento del Comité Técnico de Ciberseguridad.

1. Adscrito al órgano directivo con rango de Dirección General con competencias en materia informática estará el Comité Técnico de Ciberseguridad, como órgano colegiado para coordinar actuaciones destinadas al cumplimiento de los requisitos técnicos y operativos de la normativa de Seguridad de la Información y Protección de Datos Personales, y de la estrategia de seguridad de la información aprobada por la Comisión General de Seguridad de la Información, en relación a los sistemas de información y servicios tecnológicos dependientes del citado órgano directivo. El cual estará constituido por los siguientes miembros:

a) Presidente: La persona titular del órgano directivo con rango de Dirección General con competencias en materia de informática.

b) Secretario: La persona que tenga asignada la función de Responsable de Seguridad de la Información de la Administración de la Comunidad Autónoma de Cantabria, que, como miembro del comité, tendrá así mismo derecho a voto.

c) Vocales: Las personas titulares de las jefaturas de las unidades Centro de Proceso de Datos, Servicio de Informática y Centro de Tecnologías INET, la persona titular de la Subdirección General de Informática, así como la persona que tenga asignada la función de Responsable de Seguridad de la Información de la Administración de la Comunidad Autónoma de Cantabria.

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 una vez al año y con carácter extraordinario a propuesta de su presidente o de un tercio de los vocales que la integran.

4. El órgano directivo con rango de Dirección General con competencias en materia de informática podrá designar, mediante resolución, a nuevos vocales que formen parte del Comité Técnico de Ciberseguridad, entre el personal de dicho órgano directivo.

5. 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 5/2018, de 22 de noviembre, de Régimen Jurídico del Gobierno, de la Administración y del Sector Público Insti-

CVE-2021-8273

tucional de la Comunidad Autónoma de Cantabria y, en lo que resulte de aplicación conforme las previsiones del Capítulo II de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Artículo 11. Funciones del Comité Técnico de Ciberseguridad.

Al Comité Técnico de Ciberseguridad, respecto a los sistemas de información gestionados por el órgano directivo con rango de Dirección General con competencias en materia de informática, le corresponden las siguientes funciones:

a) Conocer el estado global de la Seguridad de la Información, así como emitir informes, relativos a:

1º. El grado de cumplimiento efectivo de las normas de Seguridad de la Información y procedimientos de Seguridad de la Información.

2º. El grado de implantación de las medidas de seguridad en los sistemas de información.

3º. La respuesta a los incidentes de seguridad acontecidos.

4º. Las necesidades de formación del personal informático.

5º. Las necesidades normativas y procedimentales.

6º. Las necesidades de medios materiales o personales.

b) Adoptar medidas de coordinación de actividades que afecten a varias unidades y, en particular, en lo relativo a planes de mejora o adecuación en materia de Seguridad de la Información.

c) Velar por la correcta gestión de los incidentes de seguridad, especialmente cuando vinculen a personal de varias unidades.

d) Velar por que la Seguridad de la Información se tenga en cuenta en todos los proyectos de tecnologías de la información y las telecomunicaciones, así como durante el ciclo de vida completo de los sistemas de información.

e) Promover la creación y utilización de soluciones horizontales que reduzcan duplicidades y contribuyan al funcionamiento homogéneos de todos los sistemas de información.

f) Y las demás funciones que se recojan en este Decreto.

Artículo 12. Creación, composición y régimen de funcionamiento de las estructuras sectoriales de gestión de Seguridad de la Información.

1. Por orden del Consejero/a con competencias en materia de informática, a petición de un órgano directivo, organismo o entidad de derecho público vinculada o dependiente, pueden crearse estructuras sectoriales de gestión de la Seguridad de la Información, que podrán incluir órganos colegiados de Seguridad de la Información, Responsables Sectoriales de Seguridad de la Información, y Coordinadores Sectoriales de Seguridad de la Información.

2. El ámbito de actuación de esta estructura corresponderá a una Consejería, organismo público o entidad de derecho público vinculada o dependiente o bien a un sector de la Administración de la Comunidad Autónoma de Cantabria que se determine.

3. Estas estructuras sectoriales deberán coordinar sus actuaciones con el conjunto de la estructura de Gestión de la Seguridad de la Información y, en particular, con el Responsable de Seguridad de la Información de la Administración de la Comunidad Autónoma de Cantabria.

4. Las Comisiones y Comités Sectoriales de Seguridad de la Información podrán designar uno o varios Coordinadores Sectoriales de Seguridad de la Información para los órganos directivos u organismos públicos y entidades de derecho público vinculadas o dependientes que estén en su ámbito de actuación. Sus funciones se asignarán a puestos de coordinadores, jefes de servicio o subdirectores o puestos de trabajo con funciones de coordinación.

CVE-2021-8273

Artículo 13. Funciones de las Comisiones o Comités Sectoriales.

1. En su ámbito de actuación, las funciones serán:

a) Asegurar el compromiso con una efectiva gestión de la Seguridad de la Información y su mejora continua.

b) Conocer el estado de la Seguridad de la Información.

c) Supervisar la gestión de riesgos.

d) Aprobar la estrategia de Seguridad de la Información.

e) Elevar a la Comisión General de Seguridad de la Información propuestas de mejora de la gestión de la Seguridad de la Información, incluyendo propuestas en el ámbito normativo.

f) Aquellas otras funciones que se establezcan en la normativa de creación de cada estructura sectorial.

2. Además, podrán establecerse funciones adicionales a las Comisiones o Comités, mediante Orden del Consejero/a con competencias en materia de informática.

Artículo 14. Responsables Sectoriales de Seguridad de la Información.

1. Los Responsables Sectoriales de Seguridad de la Información se corresponden con las personas que ocupen puestos, existentes o de nueva creación, que tengan asignada la función de Responsable Sectorial de Seguridad de la Información para el ámbito de una Consejería, organismo público o entidad de derecho público vinculada o dependiente o sector de la Administración de la Comunidad Autónoma que se determine.

2. En particular, se deberán nombrar Responsables Sectoriales de Seguridad de la Información para los servicios prestados a la Administración de Justicia en Cantabria, la Consejería con competencia en materia de servicios sociales y para los Centros Educativos de Cantabria. Sin perjuicio de que puedan nombrar otros Responsables Sectoriales de Seguridad para otros ámbitos que así lo requieran.

3. Les corresponderán las funciones que se recojan en el artículo 8.2 y en el resto de este Decreto.

Artículo 15. Funciones de los Coordinadores Sectoriales de Seguridad de la Información.

1. Para los órganos directivos, organismos públicos y entidades de derecho público vinculadas o dependientes para los que se haya determinado su ámbito actuación, las funciones de los Coordinadores Sectoriales de Seguridad de la Información son:

a) Coordinar y/o supervisar actuaciones en materia de Seguridad de la Información, en particular la revisión de accesos vigentes y registros de actividad, la elaboración de catálogos de activos y servicios, planes de continuidad y pruebas de verificación, así como la realización de auditorías o consultorías.

b) Promover la formación, información y concienciación del personal en su ámbito sectorial.

c) Ser el interlocutor en la materia, para su ámbito de actuación, con el resto de participantes en la gestión de la Seguridad de la Información, coordinándose debidamente con los Responsables de Seguridad.

d) Realizar, coordinar o supervisar las tareas que le sean asignadas en la orden de creación de la estructura de Seguridad de la Información sectorial de la que forma parte.

e) Coordinar y/o supervisar actuaciones aprobadas por el órgano colegiado de la Información al que esté vinculado y realizar aquellas otras que le sean asignadas por ese órgano.

f) Supervisión del cumplimiento de las obligaciones en materia de protección de datos personales, en todos los aspectos ligados a la Seguridad de la Información, con las siguientes funciones para sus respectivos ámbitos de actuación:

1.º Colaborar con el Delegado de Protección de Datos o Delegados adjuntos que corresponda en la supervisión de los tratamientos de datos personales.

CVE-2021-8273

2.º Estar a disposición de los Responsables del Tratamiento para coordinar actuaciones relacionadas con tratamientos de datos personales no automatizados y realizar las tareas de supervisión o seguimiento que correspondan.

3.º Colaborar con los Responsables del Tratamiento en las obligaciones derivadas en materia de protección de datos personales relacionadas con seguridad de la información. En particular en la realización de los Registros de Actividad del Tratamiento.

2. Sus actividades estarán coordinadas y supervisadas con el Responsable de Seguridad de la Información que corresponda a su ámbito de actuación.

3. Para el desempeño de sus funciones estarán apoyadas por otro personal del órgano u órganos directivos correspondientes a su ámbito de actuación, experto o con capacidad de decisión en las materias afectadas por las actuaciones a realizar.

Artículo 16. Responsables de la Información y Responsables del Servicio.

1. Los Responsables de la Información y los Responsables del Servicio son los órganos directivos, con rango de Dirección General o Secretaría General, y los directores de los organismos autónomos y el máximo directivo de las entidades de derecho público vinculadas o dependientes, en el ámbito de sus competencias. Tendrán así mismo la condición de Responsables del Tratamiento de Datos Personales en los términos establecidos en el artículo 41 de este mismo Decreto.

2. Para aquellos sistemas de información que contengan información o se utilicen para prestar servicios de varios órganos directivos, en aquellas partes diferenciadas las funciones corresponderán a cada uno de ellos.

3. En aquellos aspectos de decisión superpuestos entre varios órganos directivos, las funciones recaerán en la Secretaría General de la Consejería correspondiente, sin perjuicio de lo dispuesto en el artículo 26 de este Decreto.

Artículo 17. Funciones de los Responsables de la Información y Responsables del Servicio.

A los Responsables de la Información y Responsables del Servicio, en el ámbito de sus competencias, sin perjuicio de las obligaciones que establece el Esquema Nacional de Seguridad para tales figuras, 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 de la información en materia de seguridad, determinando los niveles de seguridad y la categoría de los sistemas de información que se utilicen para tratarla, en los términos que legalmente se determinen.

d) Establecer los requisitos de los servicios en materia de seguridad, determinando los niveles de seguridad y la categoría de los sistemas de información que se utilicen para prestarlos, en los términos que legalmente se determinen.

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

g) Autorizar accesos a la información y servicios de los que son responsables, así como decidir la modificación o cancelación de esos accesos.

h) Establecer los criterios para las autorizaciones a realizar por los Gestores Responsables del organismo u órgano directivo del que es titular, que en todo caso respetarán el contenido del artículo 24.1 de este Decreto.

i) Podrán establecer criterios para la asignación de accesos de oficio sin que se requiera, por lo tanto, una autorización explícita para cada caso particular, respetando el contenido del artículo 24.2 de este Decreto.

CVE-2021-8273

j) Velar por la implementación efectiva de las medidas de seguridad y el cumplimiento de las obligaciones que correspondan, vinculadas a la información o los servicios de los que son responsables, tanto si se realizan tratamientos automatizados o no automatizados, se emplean elementos tecnológicos o se utiliza cualquier otro medio o instrumento para tratar esa información o prestar esos servicios.

Artículo 18. Gestores Responsables de Seguridad de la Información.

Los Gestores Responsables de Seguridad de la Información serán los órganos directivos con rango de subdirección, o bien, las unidades con rango de servicio o equivalentes, que, en el ámbito de sus competencias o funciones, respectivamente, traten información o presten servicios a través de sistemas de información, con independencia del tipo de tratamiento o del medio empleado para tratar esa información o prestar esos servicios.

Artículo 19. Funciones de los Gestores Responsables de Seguridad de la Información.

A los Gestores Responsables les corresponden las siguientes funciones:

a) Velar por la adecuada gestión y cumplimiento de las previsiones establecidas al respecto por la Política de Seguridad y demás normativa de desarrollo para la adecuada implementación de la Seguridad de la Información en el ámbito de las competencias de su órgano directivo o las funciones de su unidad.

a) Solicitar y, en su caso, autorizar, si se les ha encomendado esta función por el responsable de la información o del servicio del que dependa jerárquicamente, los accesos, así como su modificación o cancelación, a información, servicios o sistemas de información, para el personal de su unidad o el personal correspondiente a contratos de prestación de servicios vinculados a su unidad.

b) Colaborar con los demás componentes de la estructura organizativa de la Seguridad de la Información.

c) Informar sobre activos relevantes para el tratamiento de información o la prestación del servicio empleados en su unidad.

d) Informar sobre situaciones y amenazas que afecten o puedan afectar al funcionamiento de sus unidades, así como al tratamiento de información que realicen o los servicios que presten.

e) Asesorar a su órgano directivo con rango de Dirección General o Secretaría General, organismos públicos y entidades de derecho público vinculadas o dependientes, respecto a los requisitos en materia de seguridad convenientes para la información y servicios de los que estos sean responsables.

f) Informar sobre incidentes de seguridad.

g) Atender a las auditorías que se realicen.

h) Proporcionar la información que le sea requerida para la adecuada gestión de la Seguridad de la Información.

i) Participar en la elaboración de planes de continuidad, evaluaciones de impacto o análisis de riesgos.

Artículo 20. Responsables de los Sistemas de Información.

1. Los responsables de los sistemas de información serán los empleados públicos adscritos al órgano directivo con rango de Dirección General con competencias en materia de informática, que desempeñen puestos de trabajo, reservados a los cuerpos facultativo superior y/o diplomados y técnicos medios y que tengan asignadas funciones específicas en materia informática, y que se corresponden, con:

a) Las personas titulares de subdirecciones o unidades con rango de servicio o equivalente, para los sistemas de información bajo su responsabilidad.

CVE-2021-8273

b) Las personas titulares de las unidades con rango de sección, cuando tengan responsabilidad sobre sistemas de información y no dependa de una unidad con rango de servicio. O bien, cuando su inmediato superior le asigne esa función sobre un conjunto de sistemas de información.

c) Cualquier otra persona designada como tal por el órgano directivo con rango de Dirección General con competencias en materia de informática, para determinados sistemas de información.

2. La coordinación de los Responsables de los Sistemas de Información corresponde al titular del órgano directivo con rango de Dirección General con competencias en materia de informática, que velará por el efectivo cumplimiento de las funciones establecidas en esta Política de Seguridad de la Información.

Artículo 21. Funciones de los Responsables de los Sistemas de Información.

1. Las funciones de los Responsables de los Sistemas de Información son:

a) Velar por la efectiva gestión de la Seguridad de la Información y la efectiva implementación de las medidas de seguridad que correspondan en los sistemas de información bajo su responsabilidad durante todo el ciclo de vida de los mismos.

b) Informar sobre incidentes de seguridad, vulnerabilidades y anomalías en la gestión de la Seguridad de la Información:

1.º En todos los casos: A la persona titular del órgano directivo con rango de Dirección General con competencias en materia de informática y al Responsable de Seguridad de la Información de la Administración de la Comunidad Autónoma de Cantabria, y en su caso a los Responsables Sectoriales de Seguridad de la Información que correspondan y al titular de la unidad de gestión con rango de servicio a la que su puesto estuviera adscrito.

2.º Cuando afecte al tratamiento de datos personales, adicionalmente a los anteriores, deberá informar al Responsable del Tratamiento de datos personales.

c) Coordinar la respuesta a incidentes de seguridad y la eliminación de vulnerabilidades en los sistemas de información bajo su responsabilidad.

d) Velar por la existencia de planes de contingencia y recuperación de los sistemas de información bajo su responsabilidad.

e) Colaborar en la elaboración de catálogos de activos y servicios, análisis de riesgos, evaluaciones de impacto, planes de continuidad y sus pruebas de verificación correspondientes, en la realización de auditorías, en acciones de asesoramiento y en cualquier otra actividad relacionada con la Seguridad de la Información en que sea necesaria su participación.

f) Coordinar a los Administradores de Ciberseguridad de los Sistemas de Información de su unidad.

g) Suspender el acceso a información, servicios o sistemas de información en situaciones en la que existan deficiencias graves o el riesgo de daños de difícil reparación, bajo las condiciones que se establecen en este mismo Decreto.

Artículo 22. Administradores de Ciberseguridad de los Sistemas.

Los Administradores de Ciberseguridad de los Sistemas de Información serán los empleados públicos adscritos al órgano directivo con rango de Dirección General con competencias en materia de informática, que desempeñen puestos de trabajo, reservados a los cuerpos facultativo superior y/o diplomados y técnicos medios con responsabilidad técnica directa sobre los sistemas de información. Estarán coordinados en sus tareas por el Responsable del Sistema de Información que corresponda para cada sistema de información.

CVE-2021-8273

Artículo 23. Funciones de los Administradores de Ciberseguridad de los Sistemas de Información.

1. Las funciones de los Administradores de Ciberseguridad de los Sistemas de Información, para los sistemas de información que tengan asignados, son las siguientes:

a) Integrar los requisitos en materia de Seguridad de la Información con el resto de requisitos funcionales, operativos, técnicos, regulatorios o de cualquier otro tipo que tengan que satisfacer los sistemas de información durante todo su ciclo de vida.

b) Velar por que esos requisitos se cumplen y aplicar los procedimientos y controles que se establezcan.

c) Atender a las vulnerabilidades y a los incidentes de seguridad que se produzcan y de los que tenga conocimiento o sea notificado, informando al Responsable del Sistema y al Responsable de Seguridad de la Información de la Administración de la Comunidad Autónoma de Cantabria de la situación, efectos y solución.

d) Realizar las labores técnicas que correspondan para la gestión de accesos de usuarios debidamente autorizados.

e) Colaborar con el resto de componentes de la estructura organizativa de la Seguridad de la Información en las actividades en que se le requieran y en particular, por parte del Responsable de Seguridad de la Información de la Administración de la Comunidad Autónoma de Cantabria, y especialmente en labores de asesoramiento y en la elaboración de catálogos de activos y servicios, categorizaciones de sistemas de información, declaraciones de aplicabilidad, análisis de riesgos, evaluaciones de impacto y planes de continuidad.

2. Estas funciones podrán ser desarrolladas directamente por los Administradores de Ciberseguridad de los Sistemas de Información, o bien coordinando a otros empleados públicos asignados para realizar las tareas que correspondan o mediante la supervisión y control de contratos de prestación de servicios.

CAPÍTULO III

Criterios para la autorización de accesos, la suspensión de los servicios y la gestión de conflictos

Artículo 24. Autorización de accesos.

1. Las reglas para conceder autorizaciones de acceso a la información, servicios o sistemas de información son:

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

b) El alcance de los accesos se limitará a lo estrictamente necesario para el adecuado desempeño de las funciones y tareas encomendadas. En el caso de personal de adjudicatarios de contratos de servicios, se limitará a lo estrictamente necesario ajustado a las tareas a realizar dentro del objeto del contrato.

c) Los accesos deberán suspenderse cuando dejen de ser necesarios.

d) En las autorizaciones de 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 de la Información y procedimientos de Seguridad de la Información que la desarrollen, así como el resto de normativa en la materia.

2. Los Responsables de la Información o Responsables del Servicio podrán encomendar la función de autorizar accesos a información, a los servicios o los sistemas de información vinculados, así como cancelar o modificar esas autorizaciones, exclusivamente a los órganos directivos con rango de subdirección, o bien, a las unidades con rango de servicio o equivalentes.

3. Los criterios para la asignación de accesos de oficio que pueden establecer los Responsables de la Información o Responsables del Servicio sin que se requiera, por lo tanto, que realizar una autorización explícita para cada caso particular, se regirá por las siguientes reglas:

CVE-2021-8273

a) La asignación de accesos de oficio estará basada en el puesto de trabajo asignado o a las funciones desempeñadas, debiendo corresponder exclusivamente a información, servicios o sistemas de información vinculados a las competencias del propio órgano directivo u organismo.

b) La asignación de oficio deberá ser técnica y procedimentalmente viable.

c) La asignación de oficio de accesos, junto con los criterios a seguir para su aplicación, serán comunicados y propuestos formalmente al órgano directivo con rango de Dirección General con competencias en materia de informática, quien valorará la viabilidad de la propuesta.

d) Si la propuesta es considerada viable, el Responsable de la Información o Responsable del Servicio correspondiente deberá velar por que sea correctamente aplicada, así como gestionar las modificaciones que sean oportunas en cada momento.

4. Las Secretarías Generales podrán establecer y proponer criterios para la asignación de accesos de oficio para sus empleados públicos.

5. El órgano directivo con rango de Dirección General con competencias en materia de informática, podrá establecer criterios para la asignación de accesos de oficio a usuarios dados de alta en la red corporativa.

Artículo 25. Suspensión del acceso a información, servicios o sistemas de información.

Los Responsables de los Sistemas de Información, así como la persona titular del órgano directivo con rango de Dirección General con competencias en materia informática, podrán proceder a la suspensión del acceso a cierta información o la prestación de cierto servicio, cuando sea conocedor de deficiencias graves en la seguridad y exista un riesgo razonable de que puedan suceder daños de difícil reparación o que afecten gravemente a los derechos fundamentales y libertades de las personas físicas. Esta suspensión deberá realizarse bajo los siguientes condicionantes:

a) Debe informarse en el menor plazo posible, a poder ser antes de proceder a la suspensión, a:

1.º Los Responsable de la Información afectados.

2.º Los Responsables del Servicio afectados.

3.º Los Responsables de Tratamiento de datos personales afectados.

4.º A la persona titular del órgano directivo con rango de Dirección General con competencia en materia de informática. Y, en su caso, a la persona titular de la unidad de gestión con rango de servicio a la que su puesto esté adscrito.

5.º Al Responsable de Seguridad de la Información de la Administración de la Comunidad Autónoma de Cantabria. Y, en su caso, a los Responsables Sectoriales de Seguridad que correspondan.

b) La suspensión se mantendrá el tiempo mínimo imprescindible para eliminar el riesgo que ha provocado tal suspensión.

c) La persona titular del órgano directivo con rango de Dirección General con competencias en materia de informática, podrá determinar en cualquier momento el cese de la suspensión, teniendo siempre en consideración las consecuencias posibles si el riesgo aún no ha sido eliminado.

Artículo 26. Resolución de conflictos en la Gestión de la Seguridad de la Información.

En caso de conflictos en la gestión de la Seguridad de la Información, se resolverán atendiendo a las siguientes reglas de atribución:

a) Si el conflicto es entre Gestores Responsables de un mismo órgano directivo u organismo público o entidad de derecho público vinculada o dependiente, decidirá el Responsable de la Información o Responsable del Servicio superior a las partes.

CVE-2021-8273

b) Si el conflicto es entre Gestores Responsables o bien entre Responsables de la Información o Responsables del Servicio de órganos directivos, u organismos públicos y entidades de derecho público vinculadas o dependientes, de una misma Consejería, decidirá la Secretaría General de la Consejería correspondiente, en el caso de que este último órgano directivo sea parte en el conflicto, decidirá el Consejero/a.

c) Si el conflicto es entre Gestores Responsables o bien entre Responsables de la Información o Responsables del Servicio de órganos directivos, organismos públicos o entidades de derecho público vinculadas o dependientes, de diferentes Consejerías, decidirá la Secretaría General de la Consejería con competencias en Informática.

d) Si el conflicto es entre Administradores de Ciberseguridad de los Sistemas de Información, decidirá el Responsable de los Sistema de Información del que dependan.

e) Si el conflicto es entre Responsables del Sistema de Información, decidirá el órgano directivo con rango de Dirección General con competencias en materia de informática, asesorado por el Responsable de Seguridad de la Información de la Administración de la Comunidad Autónoma de Cantabria.

f) Si el conflicto es entre Responsables Sectoriales de Seguridad de la Información, decidirá el Responsable de Seguridad de la Información de la Administración de la Comunidad Autónoma de Cantabria.

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

TÍTULO III

Implementación de la gestión integral de la seguridad de la información

Artículo 27. Gestión basada en riesgos.

1. La gestión de riesgos es un factor esencial para una exitosa gestión de la Seguridad de la Información. En ella deberán colaborar todos los participantes en la gestión de la Seguridad de la Información, debiendo participar o bien colaborar en su caso los miembros de la estructura organizativa de gestión de la protección de datos personales, según sus competencias y funciones.

2. En el establecimiento de pautas metodológicas y criterios comunes para la realización de categorizaciones de sistemas de información, análisis de riesgos y evaluaciones de impacto, se tendrán en consideración, cuando se realicen tratamientos de datos personales, el riesgo para los derechos y libertades de las personas físicas.

3. Los órganos colegiados con competencia sobre la gestión de Seguridad de la Información serán informados de los análisis de riegos que les correspondan.

4. Los Responsables del Tratamiento de datos personales podrán solicitar el asesoramiento en la realización de análisis de riesgos y evaluaciones de impacto de tratamientos de datos personales a los Responsables de Seguridad, o bien, al Delegado de Protección de Datos o sus adjuntos, dentro de los límites competenciales que legalmente corresponde a cada uno, y ello, sin perjuicio de sus responsabilidades respecto a disponer de esos análisis de riesgos o evaluaciones de impacto de tratamientos de datos personales.

Artículo 28. 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.

a) Las Normas de Seguridad de la Información desarrollan la Política de Seguridad de la Información.

b) Las Normas de Seguridad de la Información, aprobadas mediante Orden del Consejero/a con competencias en materia de informática, regularán aspectos necesarios para garantizar la implantación de la Política de Seguridad y uniformizar su aplicación y gestión. Se desarrollarán

CVE-2021-8273

aquellas normas que sean obligatorias por la legislación en materia de Seguridad de la Información o Protección de Datos Personales y aquellas otras que se consideren convenientes para garantizar esa aplicación y gestión uniforme.

2. Los Procedimientos de Seguridad de la Información son aquellos que incorporan criterios o instrucciones para la correcta aplicación de la Política de Seguridad o de las Normas de Seguridad de la Información y 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. También se pueden establecer actuaciones o métodos a aplicar en el tratamiento de información de manera automatizada o no automatizada.

Serán aprobados mediante instrucción del órgano directivo con rango de Dirección General con competencias en materia de informática, pudiendo recabarse el previo informe del Comité Técnico de Ciberseguridad en los casos que dicho órgano directivo lo considere conveniente.

3. La Política de Seguridad de la Información, Normas de Seguridad de la Información y Procedimientos de Seguridad de la Información, 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 29. Seguridad en la Protección de Datos Personales.

Todos los tratamientos de datos personales, ya sean realizados de manera automatizada, no automatiza o mixta, así como los sistemas de información empleados para el tratamiento de datos personales, se ajustarán a los requisitos de seguridad requeridos por la normativa en materia de Protección de Datos Personales.

Los realizados de manera automatizada, deberán también cumplir con los requisitos de seguridad establecidos por el Esquema Nacional de Seguridad.

Toda información en soporte no electrónico, que haya sido causa o consecuencia directa de la información electrónica, y por lo tanto afectada por el Esquema Nacional de Seguridad, deberá estar protegida con el mismo grado de seguridad que ésta.

Artículo 30. Formación, concienciación e información.

1. La Administración de la Comunidad Autónoma de Cantabria deberá adoptar las medidas necesarias para que su personal reciba la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios de la Administración

2. El órgano directivo con rango de Dirección General con competencias en materia de informática:

a) Desarrollará acciones de formación, concienciación e información 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.

3. Los órganos colegiados de Seguridad de la Información promoverán la formación y concienciación del personal en estas materias dentro de su ámbito de actuación.

4. La supervisión y coordinación de las acciones formativas e informativas que realicen los Responsables Sectoriales de Seguridad de la Información corresponderá al Responsable de Seguridad de la Información de la Administración de la Comunidad de Cantabria.

CVE-2021-8273

5. El Responsable de Seguridad de la Información de la Administración de la Comunidad de Cantabria y el Delegado de Protección de Datos de la Administración de la Comunidad de Cantabria colaborarán en el diseño y planificación de las acciones formativas e informativas que afecten a la materia de protección de datos de carácter personal, para garantizar la coherencia, evitar redundancias y adecuarlas a las necesidades reales de la organización.

Artículo 31. Obligaciones del personal.

1. Todas las personas que traten información de la Administración de la Comunidad Autónoma de Cantabria, de manera automatizada o no automatizada, o tengan acceso a sus sistemas de información, tienen las siguientes obligaciones:

a) Conocer y respetar la Política de Seguridad de la Información, así como las normas de Seguridad de la Información y procedimientos de Seguridad de la Información que la desarrollen y que le afecten, y en particular, las normas de Seguridad de la Información sobre utilización de los recursos y sistemas tecnológicos y de información.

b) Atender a las acciones de concienciación o formación en materia de Seguridad de la Información y Protección de Datos Personales que se realicen.

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

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

e) Colaborar, en su caso, en la resolución de incidentes de seguridad y en la realización de acciones preventivas.

f) Participar en la gestión de la Seguridad de la Información cuando corresponda según las funciones de su puesto de trabajo.

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

h) Colaborar y participar en las auditorías sobre Seguridad de la Información y Protección de Datos Personales cuando sea requerido.

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

Artículo 32. Obligaciones de personas externas a la Administración de la Comunidad Autónoma de Cantabria.

1. 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.

2. 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 33. Terceras partes.

1. Cuando la Administración de la Comunidad Autónoma de Cantabria preste servicios a otras entidades de derecho público o ceda información a terceros:

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

CVE-2021-8273

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

2. 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, así como el tratamiento de información, se deberán tener en cuenta las medidas y consideraciones de Seguridad de la Información que resulten de aplicación, según la normativa vigente en la materia y especialmente lo señalado en el Decreto 60/2018, de 12 de julio, por el que se regula el Régimen Jurídico de la Administración de la Comunidad Autónoma de Cantabria en el uso de medios electrónicos en la actividad administrativa y sus relaciones con los ciudadanos. 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.

3. Cuando la Administración de la Comunidad Autónoma de Cantabria: implante o utilice sistemas de información cedidos por otras Administraciones u organismos públicos de ellas dependientes, deberá:

a) Tener en consideración las obligaciones que sean oportunas en materia de Seguridad de la Información y Protección de Datos Personales.

b) Así mismo deberán establecerse canales de información y coordinación en materia de Seguridad de la Información y Protección de Datos Personales.

4. Cuando algún aspecto de la Política de Seguridad de la Información no pueda ser satisfecho por una tercera parte, el Responsable de Seguridad de la Información de la Administración de la Comunidad Autónoma de Cantabria emitirá informe sobre los riesgos en que se puede incurrir y la forma de tratarlos, a petición expresa del responsable del servicio o responsable de la información beneficiario de la cesión.

5. 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 las medidas que se adoptarán para reducir los riesgos y el nivel de los mismos que asumen.

Artículo 34. Colaboración con otras entidades públicas.

Se promoverán convenios de colaboración con otras entidades públicas con competencias en materia de Seguridad de la Información, especialmente con el Centro Criptológico Nacional (CCN), el Instituto Nacional de Ciberseguridad (INCIBE) y la Agencia Española de Protección de Datos [AEPD].

Artículo 35. Categorización de los Sistemas de Información.

1. Corresponde a los Responsables de la Información y los Responsables del Servicio la determinación de los requisitos de seguridad de los sistemas de información vinculados a su ámbito competencial, determinando los niveles de seguridad y su categoría, según lo establecido en el artículo 17 del presente Decreto. Sin perjuicio de lo anterior, se establecen a continuación unos criterios para fijar unos niveles y una categoría por defecto, a aplicar cuando los Responsables de la Información y los Responsables del Servicio no se hayan pronunciado explícitamente al respecto, de forma que solo sea necesario que lo hagan cuando consideren que los requisitos de un determinado sistema de información deban ser diferentes:

a) Aquellos sistemas de información que ofrezcan información pública, tales como las páginas web informativas, tendrán asignada por defecto la Categoría Básica, con los niveles de las dimensiones Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad, en Nivel Bajo.

b) Los sistemas de información utilizados para la gestión administrativa, destinados fundamentalmente a ser utilizados por los empleados públicos, tendrán asignada por defecto la Categoría Media, con los niveles de las dimensiones Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad, en Nivel Medio.

CVE-2021-8273

c) Los módulos que permitan realizar gestiones por parte de los ciudadanos o terceros y que estén técnicamente segregados de los sistemas de información utilizados por los empleados públicos, se considerarán sistemas de información autónomos y tendrán asignada por defecto la Categoría Básica, con los niveles de las dimensiones Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad, en Nivel Bajo, siempre y cuando permitan exclusivamente el acceso a datos de un único ciudadano o tercero, tras un proceso de autenticación y no se manejen datos personales que supongan un alto riesgo para los derechos y libertades de las personas físicas.

2. Cuando concurra cualquier circunstancia por la que no resulte adecuado aplicar estos criterios por defecto, se deberá procederá a realizar la determinación de los requisitos de seguridad que precisa el sistema de información por parte del Responsable de Seguridad o del Responsable del Servicio, determinando la categoría y niveles de seguridad que correspondan.

3. Los criterios por defecto aquí establecidos podrán desarrollarse de forma más detallada o modificarse mediante una norma de seguridad de la información, aprobada por la persona titular de la Consejería con competencias en materia informática.

TÍTULO IV

De la organización y gestión competencial para la Protección de Datos Personales de la Administración de la Comunidad Autónoma de Cantabria

CAPÍTULO I

Objetivos, directrices y principios de la Protección de Datos Personales

Artículo 36. Objetivos y directrices básicas de la Protección de Datos Personales.

1. Los objetivos de la Protección de Datos Personales son los siguientes:

a) Garantizar y poder demostrar que el tratamiento de datos personales es conforme a la normativa vigente en materia de protección de datos.

b) Garantizar los datos personales contra el tratamiento no autorizado o ilícito, su pérdida, destrucción o acceso accidental.

c) Garantizar el ejercicio de derechos por parte de los interesados.

d) Garantizar la adecuada gestión de incidentes de seguridad en los aspectos que afecten a datos personales.

e) Garantizar la libre circulación de los datos personales en los términos que fija le legislación vigente en la materia.

2. Las directrices básicas de la Protección de Datos Personales son las siguientes:

Aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo asociado a cada tratamiento de datos personales y para cumplir con el resto de obligaciones de la legislación en materia de protección de datos personales.

a) La coordinación con otras normas que afecten a la Protección de Datos Personales en el ámbito de la Administración de la Comunidad Autónoma de Cantabria.

b) Responsabilidades definidas y delimitadas en materia de Protección de Datos Personales de todos los órganos y personas implicadas.

Artículo 37. Principios de la Protección de Datos Personales.

El tratamiento de datos personales se realizará conforme a los principios recogidos en el Capítulo II del Reglamento General de Protección de Datos y en el Título II de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

CVE-2021-8273

CAPÍTULO II

Organización de la gestión de la Protección de Datos Personales

Artículo 38. Estructura organizativa de la Protección de Datos Personales.

La organización para la gestión de la Protección de Datos Personales en la Administración de la Comunidad Autónoma de Cantabria se estructura en:

1. Nivel de coordinación de la Protección de Datos Personales:

a) Comisión General de Protección de Datos.

b) Órgano directivo, de rango Dirección General, con competencias en la coordinación de las actuaciones relativas al cumplimiento de las obligaciones legales en materia de protección de datos personales en la Administración de la Comunidad Autónoma de Cantabria.

2. Nivel de implementación de la protección de datos personales:

a) Responsables del tratamiento de datos personales.

b) Encargados del tratamiento de datos personales.

3. Nivel de supervisión de la Protección de Datos Personales:

a) Gestores responsables de Protección de Datos.

b) Delegado de Protección de Datos de la Administración de la Comunidad Autónoma de Cantabria.

c) Delegados Adjuntos de Protección de Datos.

d) Referentes de Protección de Datos.

Artículo 39. Creación, composición y régimen de funcionamiento de la Comisión General de Protección de Datos.

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

a) Presidente: El Delegado de Protección de Datos de la Administración de la Comunidad Autónoma de Cantabria.

b) Vocales:

- Los Delegados Adjuntos de Protección de Datos.
- Los empleados públicos que ejerzan las funciones de referentes de protección de datos.

c) Secretario: Un funcionario adscrito a la Oficina de asistencia técnica para la protección de datos personales.

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

3. La Comisión General de protección de datos se convocará a petición del Delegado de Protección de Datos cuando lo estime oportuno, y en todo caso, como mínimo dos veces al año.

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 5/2018, de 22 de noviembre, de Régimen Jurídico del Gobierno, de la Administración y del Sector Público Institucional de la Comunidad Autónoma de Cantabria y, en lo que resulte de aplicación conforme las previsiones del Capítulo II de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Artículo 40. Funciones de la Comisión General de Protección de Datos.

A la Comisión General de Protección de Datos le corresponden las siguientes funciones en el ámbito de aplicación de la presente política:

a) Coordinarse con el Delegado de Protección de Datos en las políticas de protección de datos y su aplicación legal.

CVE-2021-8273

b) Comunicar las instrucciones del Delegado de Protección de Datos para que los empleados públicos referentes de protección de datos puedan realizar sus actividades de manera coordinada eficaz y eficiente.

c) Exponer, ante los demás integrantes de la Comisión General de protección de datos, cuestiones planteadas por las personas Responsables de tratamiento de cada organización a los efectos de unificar doctrina, cuando sea solicitado por el Delegado de Protección de Datos.

d) Analizar las informaciones relevantes que se hayan producido en materia de protección de datos.

e) Examinar los últimos avances y/o interpretaciones efectuadas por las instituciones de control y otras administraciones públicas en relación con la protección de datos personales.

f) Conocer el estado de la gestión desarrollada en la implementación de la Política de Seguridad de la Información, y en su caso, acordar medidas de colaboración con los responsables de la seguridad de la información.

Artículo 41. Responsables del Tratamiento de Datos Personales.

1. Los Responsables del Tratamiento de Datos Personales serán los órganos directivos, con rango de dirección general o secretaría general, y los directores de los organismos autónomos y el máximo directivo de las entidades de derecho público vinculadas o dependientes, en el ámbito de sus competencias, cuando determinen los fines y medios del tratamiento de datos personales.

2. En el caso de que dos o más responsables de Tratamientos de Datos Personales determinen conjuntamente los objetivos y los medios para el tratamiento, serán considerados corresponsables.

3. A los Responsables del Tratamiento les corresponden las obligaciones que establece la legislación en materia de Protección de Datos Personales para esta figura.

Artículo 42. Gestores Responsables de Protección de Datos Personales.

Los Gestores Responsables de Protección de Datos Personales serán los órganos directivos con rango de subdirección, o bien, las unidades con rango de servicio o equivalentes, que, en el ámbito de sus competencias o funciones, respectivamente, ejecuten operaciones con datos personales, velando por el adecuado cumplimiento de las obligaciones legales en este ámbito.

Artículo 43. Encargados del Tratamiento.

1. Los Encargados del Tratamiento serán los órganos directivos, organismos públicos y entidades de derecho público vinculadas o dependientes, cuando traten datos personales de los que no son responsables, de forma que estos actúan por cuenta del correspondiente responsable de tratamiento de datos.

2. Estos tratamientos deberán realizarse dentro del ámbito de competencias de cada órgano directivo, organismo público y entidad de derecho público vinculada o dependiente, y deberán estar atribuidas por decretos de estructura orgánica o por acuerdos que vinculen a las partes y de los que se derive la función de cada una de ellas en lo relativo a los tratamientos de datos personales.

3. Deberán cumplir con las obligaciones establecidas por la legislación en materia de Protección de Datos Personales para los Encargados del Tratamiento, incluyendo el registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable del tratamiento.

4. Cuando un órgano directivo realice operaciones con datos personales correspondiente a tratamientos de los que es Responsable del Tratamiento otro órgano directivo, organismo público y entidad de derecho público vinculada o dependiente, tendrá la función de Encargado del Tratamiento en los términos establecidos en el presente Decreto, y además, se deberán cumplir las condiciones establecidas en el artículo 28.3 del Reglamento General de Protección

CVE-2021-8273

de Datos. Así mismo, en cumplimiento de lo previsto en el artículo 28.2 del Reglamento General de Protección de Datos, el órgano directivo competente en materia de informática cuando actúe como encargado de tratamiento, cuenta con la autorización de todos los responsables de tratamiento de datos personales afectados, salvo manifestación expresa en sentido contrario y que deberá comunicarse oficialmente al órgano directivo competente en materia de informática, para acudir a otro encargado de tratamiento diferente.

5. El responsable del tratamiento podrá exigir de forma motivada al encargado del tratamiento la emisión de un compromiso sobre el cumplimiento de ciertas condiciones en las operaciones de tratamiento que realice.

Artículo 44. Notificación de violaciones de seguridad que afecten a datos personales.

1. Los Encargados del Tratamiento, informarán sin dilación indebida al Responsable del Tratamiento correspondiente las violaciones de la seguridad de los datos personales de las que tengan conocimiento.

2. Los Responsables del Tratamiento de Datos Personales informarán sobre violaciones de la seguridad de datos personales al Delegado de Protección de Datos Personales, a los Delegados Adjuntos de Protección de Datos personales si corresponde a su ámbito de actuación, al Responsable de Seguridad de la Información, y a los Responsables Sectoriales de Seguridad de la Información si corresponde a su ámbito de actuación.

3. Además, deberán notificar a la autoridad de control y a los interesados en aquellos casos establecidos por la legislación en materia de protección de datos.

Artículo 45. Independencia, autonomía y adscripción organizativa del Delegado de Protección de Datos.

1. El Delegado de Protección Datos ejercerá sus funciones con plena independencia y autonomía jerárquica y funcional, en los términos establecidos en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), y el artículo 36 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

2. El Delegado de Protección de Datos se adscribe orgánicamente de forma directa al Consejero/a que tenga atribuidas las competencias generales sobre tecnología y protección de datos, pero por exigencia legal, sin integrarse funcionalmente ni jerárquicamente en su estructura. El puesto de trabajo de Delegado de Protección de Datos tendrá la consideración de puesto de trabajo singularizado.

3. El Delegado de Protección de Datos elaborara un informe anual sobre la actividad desarrollada que se remitirá al Consejero/a que tenga atribuidas las competencias generales sobre protección de datos.

4. El portal web institucional del Gobierno de Cantabria recogerá en lugar visible los datos de contacto de la persona designada como Delegado de Protección de Datos y de sus adjuntos.

Artículo 46. Requisitos y procedimiento para su nombramiento y cese.

1. El puesto de trabajo de Delegado de Protección de Datos se encuentra reservado su desempeño a funcionario/a de carrera del Subgrupo A1, y, como requisitos de desempeño deberá estar en posesión de titulación académica superior en Derecho y pertenecer a cualquier de los siguientes cuerpos: al Cuerpo Técnico Superior, Cuerpo Facultativo Superior, Cuerpo Superior de Inspectores de Finanzas y Cuerpo de Letrados.

2. El Procedimiento de provisión del puesto de trabajo de Delegado de Protección de Datos será mediante la convocatoria pública del procedimiento de provisión de concurso de méritos específico, de acuerdo con la legislación de empleo público que resulte de aplicación en la Administración de la Comunidad Autónoma de Cantabria.

CVE-2021-8273

3. El Delegado de Protección de Datos se mantendrá inamovible salvo renuncia o que incurriera en dolo o negligencia grave en el ejercicio de sus funciones, lo que originaría el correspondiente expediente de remoción de su puesto de trabajo conforme lo establecido por la legislación sobre empleo público para el procedimiento de provisión utilizado para su nombramiento.

Artículo 47. Funciones del Delegado de Protección de Datos.

1. En el ejercicio de las funciones que le son propias, el Delegado de Protección de Datos tendrá las funciones principales siguientes:

a) La colaboración y apoyo a los órganos responsables del Sistema de Gestión de la Seguridad de la información de la Administración de la Comunidad Autónoma de Cantabria, en el desarrollo y mantenimiento de dicho sistema y en la elaboración de la normativa que resulte necesaria sobre protección de datos.

b) Informar y asesorar a los referentes de protección de datos, responsables o encargados del tratamiento y a sus empleados de las obligaciones que les incumben en aplicación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y demás normativa en materia de protección de datos que resulte de aplicación.

c) Supervisar el cumplimiento del reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), del resto de disposiciones normativas aplicables y de las políticas por los responsables o los encargados en materia de protección de datos personales, incluidas la asignación de responsabilidades, la concienciación, formación del personal así como la realización de las auditorias correspondientes.

d) La interlocución de los órganos responsables o encargados del tratamiento ante las diversas Autoridades de Protección de Datos.

e) Actuar como punto de contacto de la autoridad de control en cuestiones relacionadas con los tratamientos, incluyendo la consulta previa a que se refiere el artículo 36 del RGPD.

f) Realizar consultas a la autoridad de control, en su caso, sobre cualquier otro asunto.

g) Emitir recomendaciones a las personas responsables o encargadas del tratamiento en materia de protección de datos.

h) Supervisar, según proceda en cada caso, las acciones formativas en materia de Protección de Datos personales con el Responsable de Seguridad de la información.

i) La comunicación inmediata al Consejero/a que tenga atribuidas las competencias generales sobre protección de datos, a los órganos directivos afectados y a la persona responsable o encargada del tratamiento cuando sea conocedor de la existencia de una vulneración relevante en materia de protección de datos personales.

j) Las resoluciones que le sean atribuidas por el ordenamiento jurídico en relación con las reclamaciones sobre protección de datos.

k) Las demás funciones que le atribuyan las normas en materia de protección de datos.

2. El Delegado de Protección de Datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Artículo 48. Gestión sectorial de la Protección de Datos Personales: Delegados adjuntos.

1. A propuesta de la Consejería con competencias en materia de protección de datos personales, podrán crearse puestos de trabajo de Delegados Adjuntos de Protección de Datos, con-

CVE-2021-8273

forme los trámites legalmente establecidos, que estarán también reservados a funcionarios de carrera del Subgrupo A1, y como requisito de desempeño deberá estar en posesión de titulación académica superior en Derecho y pertenecer a cualquiera de los siguientes cuerpos: al Cuerpo Técnico Superior, Cuerpo Facultativo Superior, Cuerpo Superior de Inspectores de Finanzas y Cuerpo de Letrados. Estos estarán adscritos orgánicamente de forma directa al Consejero/a que tenga atribuidas las competencias generales sobre tecnología y protección de datos, correspondiendo al Delegado de Protección de Datos la supervisión funcional de sus actuaciones.

2. El Procedimiento de provisión del puesto de trabajo de Delegado Adjunto de Protección de Datos será mediante la convocatoria pública del procedimiento de provisión de concurso de méritos específico, de acuerdo con la legislación de empleo público que resulte de aplicación en la Administración de la Comunidad Autónoma de Cantabria.

3. El ámbito de actuación de los Delegados Adjuntos de Protección de Datos puede corresponder a una Consejería, organismo público o entidad de derecho público vinculada o dependiente, o también al área general o una específica de la actividad administrativa de la Administración de la Comunidad Autónoma de Cantabria, según se determine en el momento de su creación.

4. A los Delegados adjuntos les corresponde en su respectivo ámbito de actuación, entre otras, las siguientes funciones:

a) Pedir información sobre las actividades de tratamiento de datos en colaboración con las personas responsables o encargadas del tratamiento y los empleados que lleven a cabo el tratamiento.

b) Analizar y comprobar la conformidad con la normativa de las actividades de tratamiento.

c) Asesorar y supervisar, a los referentes de protección de datos, responsables o encargados del tratamiento y a sus empleados de las obligaciones que les incumben en aplicación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y demás normativa en materia de protección de datos personales que resulte de aplicación.

d) La comunicación inmediata al Delegado de Protección de datos, a los órganos directivos afectados y a la persona responsable o encargada del tratamiento de la existencia de una vulneración relevante en materia de protección de datos personales.

e) La colaboración y apoyo a los órganos responsables del sistema de seguridad de la información de la Administración de la Comunidad Autónoma de Cantabria, a fin de desarrollar, operar y mantener dicho sistema.

f) Cualquier otra que se les encomiende por el Delegado de Protección de Datos en relación con las materias que les son propias.

Artículo 49. Medios materiales y recursos humanos.

1. Para el desarrollo de las funciones asignadas al Delegado de Protección de Datos este contará con la colaboración de la Oficina de asistencia técnica para la protección de datos personales que contará con el personal administrativo y de apoyo técnico que se estimen necesarios para una adecuada prestación de sus funciones, así, al menos, está contará con un jefe de oficina y un asesor jurídico. Esta unidad estará adscrita orgánicamente de forma directa al Consejero/a que tenga atribuidas las competencias generales sobre tecnología y protección de datos personales. Asimismo, por la Dirección General competente en materia de informática se prestará el apoyo para asesoramiento técnico cuando así se le requiera por el Delegado de Protección de Datos, bien de forma continua o temporal. También podrá acudirse a contrataciones de prestación de servicios externos cuando sea necesario.

2. El Gobierno de Cantabria deberá adoptar todas las medidas necesarias para la implementación del derecho y deber de formación del Delegado de Protección de Datos y de los Delegados Adjuntos.

CVE-2021-8273

Artículo 50. Referentes de protección de datos

1. Por las Secretarias Generales de cada Consejería u órgano directivo de los organismos objeto de este Decreto, se deberá nombrar formalmente a una o varias personas a su cargo, dentro del ámbito de su organización, que desarrollen las funciones de Referente de protección de datos.

2. Las funciones de los empleados públicos que ejerzan el cargo de Referentes de protección de datos será la de asistir al Delegado de Protección de Datos y sus adjuntos en el ámbito de la actividad de la organización a la que pertenezcan.

3. Las funciones de quienes ejerzan el cargo de Referentes de protección de datos serán las siguientes:

a) Coordinar y atender en la organización en la que presta sus servicios el cumplimiento del RGPD y normativa de desarrollo dando cuenta al Delegado de Protección de Datos y sus adjuntos de cualquier disfunción detectada.

b) Hacer el seguimiento de los tratamientos de datos que se realizan en su organización, cotejando los mismos con el registro de tratamientos y dando cuenta de ello al Delegado/a de protección de datos y sus adjuntos.

c) Acudir a las reuniones de coordinación a las que sea citado por el Delegado/a de protección de datos, debiendo aportar a las mismas la documentación o información que el Delegado de Protección de Datos y sus adjuntos le soliciten.

d) Prestar su colaboración al Delegado de Protección de Datos y sus adjuntos en todas las tareas que se le encomienden.

CAPÍTULO III

Otras cuestiones sobre la gestión procedimental de la protección de datos personales

Artículo 51. Registro de Actividades del Tratamiento Centralizado.

A los efectos de cumplir con la obligación de llevar un Registro de Actividades de Tratamiento efectuadas por los Responsables del Tratamiento bajo su responsabilidad, se podrá crear por el órgano directivo con competencias en materia de informática, un Registro Centralizado de Actividades del Tratamiento de la Administración de la Comunidad Autónoma de Cantabria, que podrán utilizar los Responsables del Tratamiento para ejercitar su obligación de contar con un Registro de las Actividades del Tratamiento efectuadas bajo su responsabilidad.

Este sistema de información también servirá como registro centralizado de todas las categorías de actividades de tratamiento efectuadas por Encargados del Tratamiento, por cuenta de un Responsable del Tratamiento.

Para la creación de este sistema de información y su posterior gestión contará con el asesoramiento del Delegado de Protección de Datos de la Administración de la Comunidad Autónoma de Cantabria.

La implantación y gestión de este sistema de información será dirigida por el Responsable de Seguridad de la Información de la Administración de la Comunidad Autónoma de Cantabria, que velará por que su estructura y contenido sea útil para la gestión de la Protección de Datos Personales y la gestión de la Seguridad de la Información, particularmente en lo relativo a inventario de activos, análisis de riesgos y evaluaciones de impacto.

Desde el momento de su puesta en producción, los Responsables del Tratamiento, y en su caso los Encargados del Tratamiento, podrán emplear este Registro de Actividades del Tratamiento centralizado, volcando en él la información preexistente.

Artículo 52. Resolución de conflictos en la gestión de la seguridad de la información de la Protección de Datos Personales.

En caso de conflictos en la gestión de la seguridad de la información de la Protección de Datos Personales, estas se resolverán según las reglas establecidas en el artículo 26 de este Decreto.

CVE-2021-8273

Artículo 53. Colaboración sobre actuaciones en materia de Seguridad de la Información y la gestión de la Protección de Datos Personales.

Debido a que estas dos áreas de actividad están fuertemente interrelacionadas, con implicaciones tecnológicas y organizativas, y en su gestión completa concurren dos tipos de actores, en concreto, los denominados "Responsable de Seguridad de la información" y el "Delegado de Protección de Datos", se establece como criterio de relación entre los mismos, el principio de cooperación y colaboración en todas aquellas actuaciones que afecten a los campos de actuación de ambas partes, de forma que se consensuarán las decisiones a tomar, con pleno respeto al reparto competencial legalmente establecido, a la legislación vigente y el contenido de la presente Política de Seguridad de la Información.

DISPOSICIONES ADICIONALES

Disposición adicional primera.

Incoación de expediente para la modificación de la Relación de Puestos de Trabajo de la Consejería de Presidencia, Interior, Justicia y Acción Exterior.

Por la Consejería de Presidencia, Interior, Justicia y Acción Exterior, con carácter de urgencia, y en el plazo máximo de tres meses, se procederá a iniciar la tramitación de un expediente para la aprobación de una modificación de la Relación de Puestos de Trabajo de esa Consejería, que incorporará al mismo una propuesta de creación de los siguientes puestos de trabajo:

a) De acuerdo con lo establecido en el artículo 14 de este Decreto, se procederá a la creación inicial de los puestos de trabajo de Responsables Sectoriales de Seguridad de la Información, en concreto:

1. Responsable Sectorial de Seguridad de la Información de la Administración de Justicia en Cantabria.

2. Responsable Sectorial de Seguridad de la Información para los servicios prestados a la Consejería con competencias en materia de Asuntos Sociales.

3. Responsable Sectorial de Seguridad de la Información para los servicios prestados a la consejería con competencias sobre los Centros Educativos de Cantabria.

b) De acuerdo con lo establecido en el artículo 46 de este Decreto, se procederá a la creación del puesto de trabajo de Delegado de Protección de Datos del Gobierno de Cantabria.

c) De acuerdo con lo establecido en el artículo 48 de este Decreto, se procederá a la creación de los puestos de trabajo de Delegados Adjuntos de protección de datos, para el ámbito de:

1. La Consejería con competencia en materia de empleo y políticas sociales.

2. General para la Administración de la Comunidad Autónoma de Cantabria.

Disposición adicional segunda. Expediente para la modificación de la Estructura Orgánica y la Relación de Puestos de Trabajo de la Consejería de Presidencia, Interior, Justicia y Acción Exterior con relación a la Oficina de Asistencia Técnica.

1. Con posterioridad a la creación de los puestos de trabajo prevista en la disposición adicional primera de este Decreto se iniciará el correspondiente expediente para la creación de los siguientes puestos de trabajo:

a) Un puesto de trabajo de Jefe de la Oficina de Asistencia Técnica para la protección de datos personales.

b) Un puesto de trabajo de Asesor jurídico adscrito a la oficina de asistencia técnica para la protección de datos personales.

Disposición adicional tercera. Medidas presupuestarias.

Por la Consejería de Economía y Hacienda se procederá a realizar cuantas actuaciones presupuestarias sean necesarias para la financiación, ejecución y desarrollo del presente Decreto,

CVE-2021-8273

como asimismo de las modificaciones de la Estructura Orgánica y Relación de Puestos de Trabajo de la Consejería de Presidencia, Interior, Justicia y Acción Exterior.

Disposición adicional cuarta. Plazo para convocatoria de concursos específicos.

En el plazo máximo de 3 meses desde la aprobación de la creación de los puestos de trabajo previstos en este Decreto, se procederá a la publicación en el Boletín Oficial de Cantabria de la convocatoria del procedimiento de concurso de méritos específico para la provisión de los puestos de trabajo de Responsables Sectoriales de Seguridad de la Información, Delegado de Protección de Datos y Delegados adjuntos.

Disposición adicional quinta. Adhesiones a la Política Integral 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 estén en el ámbito de aplicación de la presente Política de Seguridad de la Información, podrán adherirse a ella, estableciendo su propia gestión de la Seguridad de la Información, y especificando los mecanismos de desarrollo y adaptación que sean precisos para atender a sus necesidades específicas. Así mismo, deberán dotarse de los medios humanos y materiales necesarios para su efectiva implantación.

Disposición adicional sexta. Coordinadores Sectoriales de Seguridad de la Información del Organismo Pagador y del Servicio Cántabro de Empleo.

Para adecuar a la presente Política Integral de Seguridad la "Orden PRE/49/2016, de 22 de julio, por la que regula la estructura de gestión de seguridad de la información y de la continuidad de los servicios del Organismo Pagador" y la "Orden PRE/50/2016, de 22 de julio, por la que regula la estructura de gestión de seguridad de la información y de la continuidad de los servicios del Servicio Cántabro de Empleo", las figuras creadas con estas órdenes denominadas "Responsable Sectorial de Seguridad de la Información del Organismo Pagador" y "Responsable Sectorial de Seguridad de la Información del Servicio Cántabro de Empleo", pasarán a denominarse "Coordinador Sectorial de Seguridad de la Información del Organismo Pagador" y "Coordinador Sectorial de Seguridad de la Información del Servicio Cántabro de Empleo". Conservarán las mismas funciones especificadas en ambas órdenes, además de tener asignadas las funciones correspondientes a la figura de Coordinador Sectorial de Seguridad que se establecen en el presente Decreto.

Disposición adicional séptima. La Protección de Datos personales relativos a los Centros docentes gestionados por la Consejería competente en materia de Educación.

Mediante Orden de la Consejera de Educación y Formación Profesional se establecerán las medidas de gestión integral y organización de la protección de datos de los Centros docentes gestionados por la Consejería.

Disposición adicional octava. La seguridad de la información y los datos personales relativos a la salud.

Mediante Orden del Consejero competente en materia de sanidad se establecerán las medidas de gestión integral y organización de la seguridad de la información sanitaria y de la protección de datos de salud en el ámbito del sistema sanitario público de Cantabria.

DISPOSICIONES TRANSITORIAS

Disposición transitoria primera. Del ejercicio del cargo de Delegado de Protección de Datos hasta el nombramiento definitivo conforme las previsiones del presente Decreto.

CVE-2021-8273

El ejercicio del cargo de Delegado de Protección de Datos hasta el momento del nombramiento legal conforme las previsiones del presente Decreto de un nuevo Delegado de Protección de Datos, continuarán siendo desempeñadas por el funcionario de carrera que tenga otorgado el nombramiento para el desempeño de este cargo, o bien, por la persona jurídica a la que se le hubiera podido contratar estos servicios.

Disposición transitoria segunda. Desempeño temporal de las funciones asignadas 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 de entrada en vigor del presente Decreto.

Disposición transitoria tercera. Desempeño transitorio del cargo de Delegados Adjuntos de Protección de Datos.

Hasta la creación y posterior provisión definitiva de los puestos de trabajo de Delegados Adjuntos de Protección de Datos, en el plazo máximo de tres meses desde la publicación de este Decreto, se deberá proceder al nombramiento por resolución de la Secretaria General de la Consejería con competencia en materia de empleo y políticas sociales para los tratamientos vinculados a la misma y, por la Secretaria General de la Consejería de Presidencia, Interior, Justicia y Acción Exterior, a funcionarios públicos adscritos a cada una de ellas, que ostenten, al menos, la cualificación de titulación exigida por este Decreto para esta clase de puestos.

Disposición transitoria cuarta. Desempeño del cargo de Responsable de Seguridad de la Información de la Administración de la Comunidad Autónoma de Cantabria.

El cargo de Responsable de Seguridad de la Información de la Comunidad Autónoma de Cantabria, será desempeñado por la persona adscrita al órgano directivo con competencias en materia que informática que ocupe el puesto de Jefe de Servicio de Seguridad de la Información adscrito a este órgano o en su defecto por la persona a la que se le haya encomendado dicha función mediante el correspondiente nombramiento por resolución de la Secretaria General.

Disposición transitoria quinta. Desempeño del cargo de Responsables Sectoriales de Seguridad de la Información.

El cargo de Responsables Sectoriales de Seguridad de la Información, será desempeñado por las personas adscritas al órgano directivo con competencias en materia que informática a puestos que incluyan esas funciones o en su defecto por la persona a la que se le haya encomendado dicho cargo función mediante el correspondiente nombramiento por resolución de la Secretaria General.

DISPOSICIONES DEROGATORIAS

Disposición derogatoria única. Derogación Normativa.

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

2. En particular, quedan derogados el 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 y el Decreto 48/1994, de 18 de octubre, por el que se regulan los ficheros informatizados con datos personales dependientes de los órganos de la Administración de la Comunidad Autónoma de Cantabria y sus organismos autónomos.

CVE-2021-8273

DISPOSICIONES FINALES

Disposición final primera. Desarrollo normativo.

Se faculta a la persona titular de la Consejería de Presidencia, Interior, Justicia y Acción Exterior para dictar cuantas disposiciones sean precisas para la aplicación y desarrollo del presente Decreto.

Disposición final segunda. Cláusula de Género.

Todas las referencias contenidas en este Decreto expresadas en masculino gramatical, cuando se refieran a personas físicas deben entenderse referidas indistintamente a hombres y mujeres y a sus correspondientes adjetivaciones masculinas o femeninas.

Disposición final tercera. Entrada en vigor.

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

Santander, 30 de septiembre de 2021.

El presidente del Gobierno,

Miguel Ángel Revilla Roiz.

La consejera de Presidencia, Interior, Justicia y Acción Exterior,

Paula Fernández Viaña.

2021/8273

CVE-2021-8273