CONSEJERÍA DE SANIDAD

CVE-2023-2651 *Orden SAN/3/2023, de 23 de marzo, por la que se regulan las medidas de gestión integral y organización de la seguridad de la información y de la protección de datos en el ámbito del Sistema Sanitario Público de Cantabria.*

La Ley 39/2015 de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, recoge en el artículo 13 relativo a los derechos de las personas en sus relaciones con las Administraciones Públicas, en su letra h), el derecho "a la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas." Por otro lado, en su artículo 17.3, sobre el archivo de documentos, se indica que "los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad, de acuerdo con lo previsto en el Esquema Nacional de Seguridad, que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos, así como el cumplimiento de las garantías previstas en la legislación de protección de datos".

Por otra parte, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, contiene similares previsiones en el artículo 3, en materia de principios generales, el artículo 38, sobre la sede electrónica, el artículo 46, relativo al archivo electrónico de documentos, el artículo 155, sobre transmisiones de datos entre Administraciones Públicas y, finalmente, el artículo 156.2, sobre el Esquema Nacional de Seguridad.

En este sentido, el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, tiene por objeto el establecimiento de los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados. El artículo 12 del citado Real Decreto establece que cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente. Está política de seguridad se establecerá con base en los principios recogidos en el capítulo II de la propia norma (seguridad como proceso integral, gestión de seguridad basada en los riesgos, prevención, detección, respuesta y conservación, existencia de líneas de defensa, vigilancia continua, reevaluación periódica y diferenciación de responsabilidades).

Sentadas las anteriores premisas normativas, debe tenerse en cuenta que la información que gestiona el Sistema Sanitario Público de Cantabria constituye un activo esencial para el cumplimiento de sus funciones y objetivos. En este sentido, el funcionamiento correcto de los sistemas de información que albergan y gestionan datos sanitarios, así como el desarrollo de la salud digital resultan imprescindibles para el ejercicio adecuado, eficaz y eficiente de las competencias atribuidas en materia de asistencia y de gestión sanitaria. Por otra parte, la singularidad de los datos relativos a la salud y su carácter de categoría especial de datos personales, resulta del artículo 9.1 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 sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, y del artículo 9.2 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Dicho marco normativo exige al Sistema Sanitario Público asumir la responsabilidad asociada a la protección de esos datos frente a las amenazas que puedan afectar a su seguridad. Ello implica la necesidad de afrontar su gestión con diligencia, tomando las medidas normativas, organizativas y técnicas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, uso previsto y valor de la información tratada o los servicios prestados. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para ga-

CVE-2023-2651

rantizar la prestación continua de los servicios. Esto implica que se deban aplicar las medidas de seguridad exigidas por la normativa vigente en materia de seguridad de la información y protección de datos, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Así las cosas, el Decreto 79/2021, de 30 de septiembre, 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, si bien su artículo 1.5 excluye de su ámbito de aplicación el Sistema Sanitario Público de Cantabria. De otra parte, la Disposición Adicional Quinta prevé que 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.

Más adelante, su Disposición Adicional Octava prevé que 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.

Del juego conjunto de las citadas previsiones resultan afectados por la presente Orden la totalidad de órganos y entidades que integran el Sistema Sanitario Público de Cantabria (SSPC), esto es, la Consejería de Sanidad, el Servicio Cántabro de Salud, la Fundación Instituto de Investigación "Marques de Valdecilla" (IDIVAL), la Fundación Marqués de Valdecilla y la Sociedad mercantil "Hospital Virtual Valdecilla S.L". No obstante, mientras a las entidades del sector público institucional la presente Orden les resulta de aplicación plena, en el caso de la Consejería competente en materia de Sanidad la Orden solo le afecta en relación con la información sanitaria y los datos de salud. Es por ello que los sistemas de información transversales al conjunto de la Administración General se rigen por las disposiciones del Decreto 79/2021, de 30 de septiembre.

De acuerdo con las previsiones contenidas en las normas precitadas, la presente Orden regula las medidas de gestión integral y organización de la seguridad de la información y de la protección de datos en el ámbito del Sistema Sanitario Público de Cantabria, que integran su Política de Seguridad de la Información, adaptándolas al nuevo Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

En virtud de lo expuesto y de conformidad con las atribuciones conferidas por el artículo 35. f) de la Ley 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,

DISPONGO

CAPÍTULO PRIMERO

DISPOSICIONES GENERALES

Artículo 1. Objeto y ámbito de aplicación.

1. La presente Orden tiene por objeto regular las medidas de gestión integral y organización de la seguridad de la información y de la protección de datos en el ámbito del Sistema Sanitario Público de Cantabria (en adelante SSPC), que integran su Política de Seguridad de la Información.

CVE-2023-2651

2. La presente Orden resultará de aplicación a:

a) Los sistemas de información que incorporen información sanitaria y/o datos de salud para su utilización por la Consejería de Sanidad.

b) Los sistemas de información gestionados por el Servicio Cántabro de Salud, la Fundación "Instituto de investigación Sanitaria Valdecilla" (IDIVAL), la Fundación "Marqués de Valdecilla" y el Hospital Virtual Valdecilla S. L., con independencia de la naturaleza sanitaria o no de los datos.

Artículo 2. Misión y objetivos.

1. De acuerdo con el artículo 1.1 de la Ley 7/2002, de 10 de diciembre, de Ordenación Sanitaria de Cantabria, en relación con lo previsto en artículo 12.1.a) del Real Decreto 311/2022, de 3 de mayo, es misión del SSPC hacer efectivo el derecho a la protección de la salud previsto en el artículo 43 de la Constitución española, en el ámbito territorial de la Comunidad Autónoma de Cantabria.

2. A tal efecto, son objetivos del SSPC los consignados como principios rectores en el artículo 4 de la Ley 7/2002, de 10 de diciembre, de Ordenación Sanitaria de Cantabria.

Artículo 3. Marco regulatorio.

El marco regulatorio en el que se desarrollarán las actividades del SSPC estará integrado por:

a) La Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud, Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, Ley 44/2003 de 21 de noviembre, de ordenación de las profesiones sanitarias, Ley 55/2003 de 16 de diciembre, del Estatuto Marco del personal estatutario de los servicios de salud, Ley 33/2011, de 4 de octubre, General de Salud Pública, la Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública y así como la restante legislación sanitaria estatal que resulte de aplicación.

b) La Ley 7/2002, de 10 de diciembre, de Ordenación Sanitaria de Cantabria, la Ley 7/2006, de 15 de junio, de garantías de tiempos máximos de respuesta en atención sanitaria especializada en el sistema sanitario público de Cantabria, Ley 7/2001, de 19 de diciembre, de Ordenación Farmacéutica de Cantabria y las restantes normas reguladoras de la organización y funcionamiento aplicables a la Consejería de Sanidad, Servicio Cántabro de Salud, la Fundación "Instituto de investigación Sanitaria Valdecilla" (IDIVAL), la Fundación "Marqués de Valdecilla" y el Hospital Virtual Valdecilla S. L.

c) 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), la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y la restante normativa de aplicación en materia de seguridad de la información y protección de datos personales.

CAPÍTULO SEGUNDO

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Artículo 4. Estructura organizativa de la seguridad de la información.

La estructura organizativa de organización de la Seguridad de la Información en el SSPC se articula a través de las siguientes figuras:

CVE-2023-2651

a) El Comité de Seguridad de la Información del SSPC.

b) Los Responsables de la Información y los Responsables de los Servicios.

c) El Responsable de Seguridad.

d) El Responsable del Sistema.

Artículo 5. Comité de Seguridad de la Información del SSPC.

1.- Se crea el Comité de Seguridad de la Información del SSPC como órgano colegiado adscrito a la Consejería de Sanidad que gestionará y coordinará todas las actividades necesarias para velar e impulsar la seguridad de los sistemas de información y protección de los datos personales del SSPC.

2.- Son funciones del Comité las siguientes:

a) Elaborar las propuestas de modificación y actualización permanente de la PSI del Sistema Sanitario Público de Cantabria.

b) Promover y aprobar la normativa interna de seguridad de la información como desarrollo de la PSI, sin perjuicio de las otras normas aplicables al Servicio de Salud en conjunto.

c) Velar por la difusión de la PSI, promoviendo actividades de concienciación y formación en materia de seguridad para el personal de la organización.

d) Apoyar la coordinación, cooperación y colaboración con otras Administraciones Públicas en materia de Seguridad de la Información a través de los órganos que se creen al respecto en las Administraciones Públicas.

e) Promover la mejora continua en la gestión de la seguridad de la información.

f) Aprobar el Plan de Auditoría y el Plan de Formación.

g) Resolver los conflictos en materia de seguridad de la información.

h) Definir, dentro del marco establecido por la presente Política, la asignación de roles y los criterios para alcanzar las garantías que estime pertinentes en lo relativo a la segregación de tareas.

3. El Comité tendrá la siguiente composición:

a) Presidencia: la persona titular de la Consejería de Sanidad.

b) Vicepresidencia: el titular del órgano directivo que tenga la condición de Responsable del Sistema.

c) Vocalías:

—El Responsable de Seguridad.

—Los Responsables de la Información y del Servicio.

—El Presidente del Comité Delegado de Protección de Datos.

c) Secretario, con voz pero sin voto, un funcionario de la Dirección General de Transformación Digital y Relaciones con los Usuarios.

A las reuniones del Comité podrán acudir, con voz, pero sin voto, aquellas personas que, por razón de su actividad, tengan relación con los asuntos a tratar.

4.- El Comité se reunirá como mínimo una vez al año y de forma extraordinaria siempre que el Presidente lo considere pertinente.

CVE-2023-2651

5.- El funcionamiento del Comité se regirá por las disposiciones de la Ley 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 en materia de órganos colegiados.

Artículo 6. Responsables de la Información.

1. De conformidad con el artículo 13.2.a) del Real Decreto 311/2022, de 3 de mayo, el Responsable de la Información determinará los requisitos de la información tratada.

2. La condición de Responsables de la Información, en relación con su respectivo ámbito competencial, recaerá en las personas titulares de:

a) La Secretaría General y cada una de las Direcciones Generales de la Consejería de Sanidad.

b) La Dirección Gerencia del Servicio Cántabro de Salud

c) La Gerencia de la Fundación Marqués de Valdecilla.

d) La Dirección de Gestión del Instituto de investigación Sanitaria Valdecilla (IDIVAL).

e) La Dirección Gerencia del Hospital Virtual Valdecilla S. L.

3. En particular, son funciones del Responsable de la Información, dentro de su ámbito de actuación, las siguientes:

a) Determinar los requisitos y uso de la información tratada.

b) Determinar los niveles de seguridad de la información tratada, valorando los impactos de los incidentes que afecten a la seguridad de la información.

c) Realizar los preceptivos análisis de riesgos de la información y seleccionar las salvaguardas que se han de implantar.

d) Aceptar los riesgos residuales respecto de la información, calculados en el análisis de riesgos.

e) Solicitar informe no vinculante al Responsable de la Seguridad para la determinación de los niveles de seguridad de la información.

4. En el caso de información que contenga datos personales, el Responsable de la Información actuará como Responsable del Tratamiento a efectos de lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Artículo 7. Responsables del Servicio.

1. De conformidad con el artículo 13.2.b) del Real Decreto 311/2022, de 3 de mayo, el Responsable del Servicio determinará los requisitos de los servicios prestados.

2. La condición de Responsables del Servicio, en relación con su respectivo ámbito competencial, recaerá en las personas titulares de:

a) La Secretaría General y cada una de las Direcciones Generales de la Consejería de Sanidad

b) La Dirección Gerencia del Servicio Cántabro de Salud

c) La Dirección de Gestión del Instituto de investigación Sanitaria Valdecilla (IDIVAL)

d) La Gerencia de la Fundación Marqués de Valdecilla

CVE-2023-2651

e) La Dirección Gerencia del Hospital Virtual Valdecilla S. L.

3. Serán funciones del responsable del servicio:

a) Determinar los niveles de seguridad del servicio, valorando los impactos de los incidentes que afecten a la seguridad del servicio.

b) Realizar los preceptivos análisis de riesgos del servicio y seleccionar las salvaguardas que se han de implantar.

c) Aceptar los riesgos residuales respecto de los servicios calculados en el análisis de riesgos.

d) Solicitar informe al Responsable de la Seguridad para la determinación de los niveles de seguridad del servicio.

Artículo 8. Responsable de Seguridad.

1. De conformidad con el artículo 13.2.c) del Real Decreto 311/2022, de 3 de mayo, el Responsable de Seguridad determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.

2. La condición de Responsable de Seguridad recaerá en la persona titular de la Secretaría General de la Consejería de Sanidad. El Responsable de seguridad ejercerá sus funciones a asistido por el Servicio de Administración General, sin perjuicio de la posibilidad de contar con medios externos.

3. Serán funciones del Responsable de Seguridad:

a) Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.

b) Elaborar la normativa de seguridad de segundo nivel a través cuantos procedimientos y protocolos sean necesarios para garantizar un nivel adecuado de seguridad.

c) Velar e impulsar el cumplimiento de la normativa en materia de seguridad de la información.

d) Supervisar que la documentación de seguridad se mantenga organizada y actualizada, y de gestionar los mecanismos de acceso a la misma.

e) Promover la mejora continua en la gestión de la seguridad de la información.

f) Supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución y participar en la toma de decisiones en momentos de alerta.

g) Validar los Planes de Continuidad de Sistemas que elabore el Responsable del Sistema, que deberán ser aprobados por el Comité de Seguridad de la Información

h) Proponer la categoría del sistema según lo establecido en el anexo I del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

e) Emitir informe para la determinación de los niveles de seguridad de la información y del servicio a petición de los Responsables de la Información y Responsables del Servicio.

i) Implantar criterios comunes para la correcta gestión de los derechos de acceso, rectificación, supresión y oposición, y de limitación de tratamiento y portabilidad respecto a datos de salud, y la conservación y destrucción de documentos que contempla la Ley Orgánica 3/2018, de 5 de diciembre, en relación con sobre la Historia Clínica Electrónica y las actividades de tratamiento con datos personales, declarados responsabilidad del Servicio Cántabro de Salud.

CVE-2023-2651

j) Implantar criterios comunes para la correcta gestión del derecho de acceso a la información pública reconocido por la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, y Ley de Cantabria 1/2018, de 21 de marzo, de Transparencia de la Actividad Pública, en relación con los sistemas de información del SSPC.

Artículo 9. Responsable del Sistema.

1. De conformidad con el artículo 13.2.d) del Real Decreto 311/2022, de 3 de mayo, el Responsable del Sistema, por sí o a través de recursos propios o contratados, se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.

2. La condición de Responsable del Sistema corresponderá a la persona titular de la Dirección General competente en materia de Transformación Digital.

3. Son funciones del responsable del Sistema:

a) Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

b) Definir la tipología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.

c) Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

d) Acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada, siempre que las circunstancias lo permitan, con los Responsables de la Información, los Responsables del Servicio, y con el Responsable de la Seguridad antes de ser ejecutada.

e) Monitorizar el estado de la seguridad del Sistema de Información y reportarlo periódicamente o ante incidentes de seguridad relevantes al Responsable de Seguridad.

f) Informar sobre incidentes de seguridad, vulnerabilidades y anomalías en la gestión de la Seguridad de la Información al Responsable de Seguridad y cuando afecte al tratamiento de datos personales, adicionalmente a los Responsables del tratamiento de datos personales.

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

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

CAPÍTULO TERCERO

ORGANIZACIÓN DE LA GESTIÓN DE LA PROTECCIÓN DE DATOS PERSONALES

Artículo 10. Comité Delegado de Protección de Datos.

1. Se crea adscrito a la Consejería de Sanidad un Comité Delegado de Protección de Datos que ejercerá las funciones previstas en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

2. El Comité estará presidido por el Jefe del Servicio de Asesoramiento Jurídico de la Consejería de Sanidad y contará con tres vocales que serán asesores jurídicos de la Consejería de Sanidad, de los cuales uno de ellos intervendrá como secretario con voz y voto.

CVE-2023-2651

3. El Comité podrá contar con asistencia técnica externa para el desarrollo de sus funciones. Las personas que presten asistencia externa al Comité podrán asistir a las reuniones del Comité, estando obligados a mantener el debido secreto respecto de la información a la que tengan acceso, así como la confidencialidad de los datos personales que puedan conocer. Asimismo, el personal del SSPC estará obligado a prestar asistencia técnica al Comité cuando así se recabe.

4. El régimen de funcionamiento del Comité será el previsto en las normas reguladoras de los órganos colegiados en la Ley 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. El Comité contará con un reglamento de régimen interior, que podrá establecer un sistema de distribución de funciones, designando a miembros del mismo como responsables de la tramitación y resolución de materias concretas.

CAPÍTULO CUARTO

PERSONAL DEL SISTEMA SANITARIO PÚBLICO DE CANTABRIA Y DE ENTIDADES EXTERNAS

Artículo 11. Obligaciones del personal del SSPC.

1. Las medidas contenidas en la presente Orden resultan de obligado cumplimiento para todo el personal propio o adscrito a él que preste servicios en el mismo independientemente de la forma de contratación y vinculación con el mismo, de manera permanente o eventual, que en el desempeño de sus funciones o parte de ellas desarrolle su trabajo dentro o fuera de sus instalaciones, en adelante los usuarios.

2. Toda persona que tenga acceso a los sistemas de información del Sistema Sanitario Público de Cantabria tendrá las siguientes obligaciones:

a) Conocer y respetar la Política de Seguridad de la Información, así como las normas, procedimientos y pautas de seguridad que se aprueben por los comités o personas descritas en la presente Orden.

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

c) Utilizar los equipos informáticos con fines estrictamente laborales, quedando prohibido el uso de los mismos para fines particulares. Queda prohibido el almacenamiento de datos personales en local.

d) La utilización de internet y del correo electrónico corporativo queda limitado a usos profesionales, quedando prohibido su uso con fines ilegales. El uso de los sistemas de información, tales como internet o el correo electrónico corporativo, así como de los equipos informáticos y las carpetas de red, podrán ser auditados en los términos que autorice la legislación vigente, y, en cualquier caso, analizados a efectos de investigación de incidentes de seguridad y de infracciones de la presente Norma. El Sistema Sanitario Público de Cantabria se reserva el derecho de acceso a buzones de correo y a otros sistemas y recursos de almacenamiento de datos y adoptará las medidas técnicas correctoras necesarias a fin de garantizar la seguridad, la integridad y el correcto funcionamiento de los recursos y sistemas de información, teniendo en cuenta que contienen información corporativa y son propiedad del Sistema Sanitario Público de Cantabria, respetando los principios de proporcionalidad, necesidad e idoneidad.

e) Las credenciales de acceso a los sistemas de información son personales e intransferibles, salvo situaciones de urgente necesidad apreciadas por el Responsable del Seguridad.

CVE-2023-2651

f) Cuando un usuario se ausente de su puesto de trabajo, deberá activar el sistema de bloqueo del equipo, con el fin de que la información que consta en la pantalla no sea fácilmente accesible por terceros no autorizados.

g) La documentación en papel que contenga información confidencial, deberá estar custodiada en todo momento mientras se esté haciendo uso de la misma, y almacenarla en lugares con acceso restringido. En caso de que la documentación en papel deje de ser necesaria, debe ser destruida convenientemente.

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

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

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

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

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

m) Atender a las acciones de concienciación en materia de seguridad de la información y protección de datos personales que se realicen.

Artículo 12. Personal de entidades externas.

1. De conformidad con el artículo 13.5 del Real Decreto 311/2022, de 3 de mayo, en el caso de servicios externalizados, salvo por causa justificada y documentada, la organización prestataria de dichos servicios deberá designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo de los órganos de dirección, y que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

Dicho POC de seguridad será el propio Responsable de Seguridad de la organización contratada, formará parte de su área o tendrá comunicación directa con la misma. Todo ello sin perjuicio de que la responsabilidad última resida en la entidad pública destinataria de los citados servicios.

2. En el caso de personas vinculadas a entidades externas, el uso de los sistemas de información se limitará a las tareas o actividades circunscritas en los términos del contrato o acuerdo que regula la relación entre esa entidad y el Sistema Sanitario Público de Cantabria.

CAPÍTULO QUINTO

OTRAS DISPOSICIONES

Artículo 13. Resolución de conflictos

Los eventuales conflictos entre los diferentes responsables que componen la estructura organizativa de la Política de Seguridad de la Información se resolverán por la Comisión de Seguridad de la Información.

CVE-2023-2651

Artículo 14. Revisión de la política de Seguridad de la Información.

1. La Política de Seguridad de la Información deberá mantenerse actualizada permanentemente para adecuarla al progreso de los servicios de administración electrónica, a la evolución tecnológica y al desarrollo de la información.

2. La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, organización general, o de otro tipo.

3. Anualmente, o con menor periodicidad si existen circunstancias que así lo aconsejen, el Responsable de Seguridad revisará la presente Política y la someterá, de haber modificaciones, al Comité de Seguridad de la Información.

DISPOSICIÓN TRANSITORIA ÚNICA

Sistemas de información actualmente gestionados por la Dirección General competente en materia de tecnologías de la información

La presente Orden no resultará de aplicación en relación con los sistemas de información sanitaria y/o datos de salud actualmente gestionados por la Dirección General competente en materia de tecnologías de la información de la Consejería de Presidencia, Interior, Justicia y Acción Exterior, que se regirán por lo dispuesto en el Decreto 79/2021, de 30 de septiembre.

DISPOSICIÓN FINAL PRIMERA

Modificación de la Orden SAN/15/2020, de 31 de enero, por la que se crea y regula el Comité de Sistemas y Tecnologías de la Información del Sistema Sanitario Público de Cantabria

Se añade un apartado 4 al artículo 3 de la Orden SAN/15/2020, de 31 de enero, por la que se crea y regula el Comité de Sistemas y Tecnologías de la Información del Sistema Sanitario Público de Cantabria, con la siguiente redacción:

"4. El Comité de Sistemas y Tecnologías de la Información Sistema Sanitario Público de Cantabria desarrollará funciones de apoyo técnico y diseño de las actuaciones necesarias de adecuación del Sistema Sanitario Público de Cantabria a las obligaciones que recoge 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, a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y al Esquema Nacional de Seguridad, aprobado por Real Decreto 311/2022, de 3 de mayo.

En particular, en relación con sus funciones en materia de seguridad, corresponderá al Comité:

a) Conocer los principales riesgos residuales asumidos por el Sistema Sanitario Público de Cantabria y recomendar posibles actuaciones respecto de ellos.

b) Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.

c) Velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.

d) Promover la realización de las auditorías de cumplimiento normativo y auditorías técnicas de seguridad que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.

CVE-2023-2651

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

f) Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos de tecnologías de la información y las comunicaciones desde su especificación inicial hasta su puesta en operación.

g) Prestar asesoramiento técnico y apoyo a los órganos que integran la estructura organizativa de la seguridad de la información del Sistema Sanitario Público de Cantabria.

Para el cumplimiento de sus funciones en materia de seguridad, el Comité podrá invitar a sus reuniones a los responsables en materia de tecnologías de la información de las entidades del sector público sanitario de carácter fundacional o empresarial".

DISPOSICIÓN FINAL SEGUNDA

Entrada en vigor

La presente Orden entrará en vigor el día 1 de abril de 2023.

Santander, 23 de marzo de 2023.

El consejero de Sanidad,

Raúl Pesquera Cabezas.

2023/2651

CVE-2023-2651