I. Comunidad Autónoma

3. Otras disposiciones

Consejería de Salud

Servicio Murciano de Salud

4248 Resolución del Director Gerente del Servicio Murciano de Salud por la que se ordena la publicación del acuerdo del Consejo de Administración de dicho ente, por el que se aprueba la política de protección de datos y seguridad de la información del Servicio Murciano de Salud.

El 6 de febrero de 2020, el Consejo de Administración del Servicio Murciano de Salud, a propuesta del Director Gerente del Servicio Murciano de Salud, adoptó el Acuerdo de aprobar la Política de Protección de Datos y Seguridad de la Información del Servicio Murciano de Salud.

En su virtud y en uso de las competencias que me otorga el artículo 8.1.b del Decreto 148/2002, de 27 de diciembre, por el que se establece la estructura y funciones de los órganos de participación, administración y gestión del Servicio Murciano de Salud

Resuelvo:

Primero: Ordenar la publicación en el Boletín Oficial de la Región de Murcia del Acuerdo del Consejo de Administración del Servicio Murciano de Salud de fecha 6 de febrero de 2020, por el que se aprueba la Política de Protección de Datos y Seguridad de la Información del Servicio Murciano de Salud, que se inserta a continuación.

Segundo: La presente Resolución surtirá efectos desde el día de su publicación en el Boletín Oficial de la Región de Murcia.

Murcia, a 24 de julio de 2020.—El Director Gerente del Servicio Murciano de Salud, Asensio López Santiago.

Anexo

Política de Protección de Datos y Seguridad de la Información

Servicio Murciano de Salud

Índice

1. Introducción

El Servicio Murciano de Salud depende de los sistemas TIC (Tecnologías de la información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada.

Es por ello que, en el desarrollo de la Administración Electrónica, implica el tratamiento automatizado de grandes cantidades de información por los sistemas de tecnologías de la información y de las comunicaciones, que está sometida a diferentes tipos de amenazas y vulnerabilidades. En el contexto de la Administración Electrónica, se entiende por seguridad de la información la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes y acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad de los datos almacenados o transmitidos y de los servicios que dichas redes o sistemas ofrecen, o a través de los cuales se realiza el acceso.

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), en adelante RGPD, de plena aplicación a partir del 25 de mayo de 2018., establece en su artículo 24 dentro de las obligaciones generales del responsable del tratamiento de datos personales que, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el citado Reglamento. Igualmente, dispone que dichas medidas se revisarán y actualizarán cuando sea necesario y que, cuando sean proporcionadas en relación con las actividades de tratamiento, entre dichas medidas se incluirá la aplicación por parte del responsable del tratamiento, de las oportunas políticas de protección de datos. Asimismo, el considerando 78 establece que, a fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto.

En el mismo sentido, el artículo 28 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, en adelante LOPDGDD, referido a las obligaciones generales del responsable y encargado del tratamiento, establece que dichos responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del RGPD, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable.

Por su parte, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, contempla en su artículo 13 el derecho a la protección de datos personales y, en particular, a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público en su artículo 3.2 establece que las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas, garantizarán la protección de los datos de carácter personal, y facilitarán preferentemente la prestación conjunta de servicios a los interesados.

Asimismo, la redacción del Real Decreto-Ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones, da una nueva redacción al artículo 155 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, estableciendo que solo se permitirán cesiones de datos entre Administraciones Públicas cuando la finalidad ulterior sea compatible con la inicial, ofreciendo para ello las máximas garantías de seguridad, integridad y disponibilidad.

En este sentido, el artículo 156 de la citada Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, dispone que el Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

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

El artículo 11 del ENS, exige que todos los órganos superiores de las Administraciones Públicas dispongan formalmente de su política de seguridad, que se aprobará por el titular del órgano superior correspondiente. Esta política de seguridad se establecerá con base en los principios básicos recogidos en el capítulo II de la propia norma (seguridad integral, gestión de riesgos, prevención, reacción y recuperación, líneas de defensa, reevaluación periódica y función diferenciada) y desarrollará una serie de requisitos mínimos consignados en el ya mencionado artículo 11.1.

A su vez, la plena aplicación del Reglamento General de Protección de Datos a partir del 25 de mayo de 2018, exige que el Servicio Murciano de Salud adopte una Política de Protección de Datos a fin de garantizar y poder demostrar que los tratamientos que lleva a cabo son conformes al citado Reglamento.

Siendo obligaciones legales del Servicio Murciano de Salud tanto la aprobación de una Política de Seguridad de la Información como la de una Política de Protección de Datos, se considera conveniente adoptar una política conjunta de protección de datos y seguridad de la información, dada la íntima conexión entre ambas materias. Esta política común ha de permitir recoger y delimitar con claridad las responsabilidades y funciones tanto en materia de protección de datos como de seguridad de la información, de forma que se aborden tanto las cuestiones comunes a ambos ámbitos como aquellas que resultan propias de cada uno de ellos. Asimismo, ha de ser aplicable a todos los sistemas de información y a todas las unidades que integren el Servicio Murciano de Salud y

a todo el personal con acceso a la información, con independencia de su destino, condición laboral o relación por la que se acceda a la información.

Así pues, la presente política es el documento base mediante el cual se define el marco de referencia que permite la gestión de la protección de datos y de la seguridad de la información en el contexto de las actividades de tratamiento con datos personales y los sistemas de información del Servicio Murciano de Salud. En este marco general se delimitan las diferentes responsabilidades y roles necesarios para definirla, implantarla y gestionarla, roles que se integran en la estructura orgánica existente. La protección de datos y la seguridad de la información deben contar con el compromiso y apoyo de todos los niveles directivos de forma que pueda estar coordinada e integrada con el resto de iniciativas estratégicas del Servicio Murciano de Salud para conformar un todo coherente y eficaz.

2. Objeto y ámbito de aplicación

Constituye el objeto de la presente, la aprobación de la política de protección de datos y de seguridad de la información (en adelante PPDSI) en el marco de los sistemas de información y de las actividades de tratamiento con datos de carácter personal del Servicio Murciano de Salud (en adelante SMS).

La PPDSI será de aplicación a todos los sistemas de información y a todas las actividades de tratamiento de datos personales de los que sean responsables del SMS.

La PPDSI será de obligado cumplimiento para todas las unidades que conforman la estructura del SMS y para todo el personal con acceso a la información de la que es responsable aquella, con independencia de su destino, condición laboral o relación por la que se accede a la información.

Asimismo, se establece el reparto de funciones y responsabilidades en materia de seguridad de la información entre los distintos órganos que lo conforman.

En el ámbito de aplicación material del RGPD y ENS, la presente PPDSI afectará a la información tratada por cualquier medio con independencia del soporte, que gestiona el SMS en el ejercicio de sus competencias.

3. Misión del Servicio Murciano de Salud

El SMS como Entidad de Derecho Público, adscrito a la Conserjería de Sanidad, tiene la misión de ejercer las competencias de gestión y prestación de la asistencia sanitaria a la población, atribuidas por la Ley 4/1994, de 26 de julio, de Salud de la Región de Murcia y por las disposiciones que la desarrollan o complementan.

4. Marco normativo

Sin carácter exhaustivo, comprende la legislación en materia de protección de datos y seguridad de la información, así como la sectorial y específica que se detalla a continuación:

a) Reglamento (UE) 2016/679 del Parlamento Europeo y 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.

b) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

c) Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

d) Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

e) Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

f) Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

g) Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

h) Real Decreto-Ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

i) Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

j) Ley 59/2003, de 19 de diciembre, de firma electrónica.

k) Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

l) Ley 41/2002, de 14 noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

m) Ley 14/1986, de 25 de abril, General de Sanidad.

n) Ley 33/2011, de 4 de octubre, General de Salud Pública.

o) Ley 3/2009, de 11 de mayo, de los Derechos y Deberes de los Usuarios del Sistema Sanitario de la Región de Murcia.

p) Ley 4/1994, de 26 de julio, de Salud de la Región de Murcia.

El SMS, desarrollará sus funciones en el marco normativo de la protección de datos, de los procedimientos administrativos y sector público y de la administración electrónica que le resultan de aplicación.

5. Principios de protección de datos y seguridad de la información

El SMS tratará la información y los datos personales bajo su responsabilidad conforme a los siguientes principios de protección de datos y seguridad de la información:

a) Licitud, lealtad y transparencia: los datos de carácter personal serán tratados de manera lícita, leal y transparente en relación con el interesado;

b) Limitación de la finalidad: los datos de carácter personal serán tratados para el cumplimiento de fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines;

c) Minimización de datos: los datos de carácter personal serán adecuados, pertinentes y limitados a los necesario en relación con los fines para los que son tratados;

d) Exactitud: los datos de carácter personal serán exactos y, si fuera necesario, actualizados; se adoptarán todas las medias razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan;

e) Limitación del plazo de conservación: los datos de carácter personal serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines que justificaron su tratamiento;

f) Integridad y confidencialidad: los datos de carácter personal serán tratados de tal manera que se garantice su seguridad, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas. Quienes intervengan en el tratamiento de los datos estarán sujetos al deber de secreto incluso después de haber concluido aquel;

g) Responsabilidad proactiva: el SMS será responsable del cumplimiento de los principios anteriormente señalados y adoptará las medidas técnicas y organizativas que le permitan estar en condiciones de demostrar dicho cumplimiento;

h) Legitimación en el tratamiento de datos personales: solo se tratarán los datos de carácter personal cuando dicho tratamiento se encuentre amparado en alguna de las causas de legitimación establecidas en los artículos 6 y 9 del RGPD;

i) Atención de los derechos de los afectados: se adoptarán medidas en la organización que garanticen el adecuado ejercicio por los afectados, cuando proceda, de los derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad respecto de sus datos de carácter personal;

j) Alcance estratégico: la protección de datos y la seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de forma que pueda estar coordinada e integrada con el resto de iniciativas estratégicas del SMS para conformar un todo coherente y eficaz.

k) Responsabilidad diferenciada: en los sistemas de información responsabilidad del SMS se observa el principio de responsabilidad diferenciada de forma que se delimiten las diferentes responsabilidades y roles:

I. Responsable del Tratamiento: determina los fines y medios del tratamiento;

II. Encargado del Tratamiento: trata los datos personales por cuenta del responsable del tratamiento;

III. Delegado de protección de datos: realizará las tareas necesarias para el cumplimiento de la normativa de Protección de datos, así como, informar y asesorar al responsable del tratamiento de las obligaciones en materia de cumplimiento del RGPD;

IV. Responsable de la Información: determina los requisitos de seguridad de la información tratada;

V. Responsable del servicio: determina los requisitos de seguridad de los servicios prestados;

VI. Responsable del Sistema: tiene la responsabilidad sobre los requisitos no funcionales y de diseño, construcción, operación y soporte de los sistemas de información utilizados en la prestación de los servicios.

VII. Responsable de seguridad de la información: determina las decisiones para satisfacer los requisitos de seguridad.

l) Seguridad integral: la seguridad tenderá a la preservación de la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio. La seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, que participan de forma directa o indirecta en el ciclo de vida de los servicios de información que los sustentan.

m) Gestión de riesgos: la gestión de riesgos es el conjunto de actividades coordinadas que el SMS desarrolla para identificar los riesgos y el impacto sobre un activo, cuando una amenaza se materializa y puede afectar al tratamiento de los datos o de la información debido a la existencia de una debilidad o vulnerabilidad del sistema o como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de los datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos. El análisis y gestión de riesgos son parte esencial del proceso de protección de datos y de seguridad de la información, de forma que permita el mantenimiento de un entorno controlado, minimizando el riesgo hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo, el SMS tendrá en cuenta los riesgos que se derivan para los derechos de las personas con respecto al tratamiento de sus datos personales.

n) Defensa proactiva: incorporando siempre que sea posible, mecanismos preventivos y de detección para evitar la ocurrencia de incidentes de seguridad, o al menos, minimizar su impacto sobre los sistemas de información cuando estos sucedan.

o) Proporcionalidad: el SMS establecerá medidas de protección, detección y recuperación de forma que resulten proporcionales a los potenciales riesgos y a la criticidad y valor de la información, de los tratamientos de datos personales y de los servicios afectados.

p) Proceso de verificación: el SMS implantará un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad de los tratamientos.

q) Protección de datos y seguridad desde el diseño: el SMS promoverá la implantación del principio de protección de datos desde el diseño con el objetivo de cumplir los requisitos definidos en el RGDP y, por tanto, los derechos de los interesados de forma que la protección de datos se encuentre presente en las primeras fases de concepción de un proyecto. Asimismo, la seguridad de la información se aplicará desde el diseño inicial de los sistemas de información.

r) Protección de datos por defecto: el SMS promoverá que los sistemas de información de su titularidad se diseñen y configuren de forma que garanticen la protección de datos por defecto.

Las directrices fundamentales de protección de datos y seguridad de la información se concretan en un conjunto de principios particulares y responsabilidades específicas que se configuran como objetivos instrumentales que garantizan el cumplimiento de los principios básicos del PPDSI y que inspiran las actuaciones del SMS en dicha materia. Se establecen como mínimos los siguientes:

a) Registro de actividades de tratamiento: se mantendrá un registro de actividades de tratamiento, en los términos previstos en la presente política, analizando las bases jurídicas, que se hará público en la página web del SMS. Asimismo, los activos de información se encontrarán inventariados, categorizados y estarán asociados a un responsable.

b) Organización e implantación del proceso de seguridad: la seguridad debe comprometer a todos los miembros del SMS. Por ello, esta política

detalla según el anexo II la identificación de los responsables de velar por su cumplimiento y deberá darse a conocer por todos los miembros del SMS.

c) Análisis y gestión de riesgos: esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema y los datos de carácter personal en él contenidos, empleando una metodología reconocida internacionalmente.

d) Formación del personal: se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información y a los datos de carácter personal, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.

e) Profesionalidad: la seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento. Asimismo, el personal del SMS recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a sus sistemas y servicios.

f) Control de los accesos: se limitará el acceso a los activos de información por parte de los usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación y autorización acordes a la criticidad de cada activo. Además, se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

g) Seguridad física: los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y a los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

h) Seguridad en la gestión de comunicaciones y operaciones: se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las Tecnologías de la Información y Comunicaciones. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.

i) Adquisición, desarrollo y mantenimiento de los sistemas de información: se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.

j) Gestión de incidentes de seguridad: se implantarán los mecanismos apropiados para la correcta identificación, registro, resolución y notificación, en los términos previstos en la normativa de protección de datos y seguridad de la información de los incidentes de seguridad.

k) Gestión de la continuidad de la actividad: los sistemas dispondrán de copias de seguridad y se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio.

6. Análisis de riesgos, evaluación de impacto en la protección de datos y gestión de los riesgos de seguridad de la información

Cuando la información contenga datos personales se llevará a cabo, de forma periódica en los plazos legalmente establecidos, un análisis de riesgos

que permitirá identificar y gestionar los riesgos minimizándolos hasta los niveles que puedan considerarse aceptables. Esta evaluación incluirá un análisis de los riesgos para los derechos y libertades de las personas físicas respecto de las actividades de tratamiento con datos personales que lleven a cabo en el SMS, así como para los sistemas de información que sirven de soporte para dichas actividades de tratamiento.

Además, el SMS llevará a cabo una evaluación de impacto de las actividades de tratamiento en la protección de datos personales cuando del análisis realizado resulte probable que el tratamiento suponga un riesgo significativo para los derechos y libertades de las personas, conforme lo previsto en el artículo 35 del RGPD.

La gestión de riesgos de seguridad de la información debe realizarse de manera continua sobre el sistema de información, conforme a los principios de gestión de la seguridad basada en los riesgos y en la reevaluación periódica.

Será el Responsable de Seguridad de la Información el encargado de recomendar un marco de directrices básicas para armonizar los criterios a seguir para la valoración de riesgos.

El Responsable de la Información y los Responsables de los Servicios son los propietarios de los riesgos sobre la información y sobre los servicios, respectivamente, siendo responsables de su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

El Responsable del Sistema debe cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.

El SMS utilizará para el análisis y gestión de riesgos de los sistemas de información, la Metodología MAGERIT. El método MAGERIT, son las siglas de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administraciones, dicho método cubre la fase AGR (Análisis y Gestión de Riesgos). Si hablamos de Gestión global de la Seguridad de un Sistema de Seguridad de la Información basado en ISO 27001, MAGERIT, es el núcleo de toda actuación organizada en dicha materia, ya que influye en todas las fases que sean de tipo estratégico y se condiciona la profundidad de las fases de tipo logístico.

7. Notificación de violaciones de seguridad de los datos de carácter personal

El SMS adoptará las medidas necesarias para garantizar la notificación a la propia Agencia Española de Protección de Datos, como autoridad de control competente, de las violaciones de seguridad de los datos de carácter personal que pudieran producirse a través del procedimiento de notificación de brechas de seguridad establecido a tal efecto, de conformidad con lo dispuesto en el artículo 33 del RGPD.

Igualmente adoptará las medidas procedentes para la comunicación a los interesados que pudieran haberse visto afectados por la violación de seguridad de los datos de carácter personal, en los casos y conforme a lo dispuesto en el artículo 34 del RGPD.

8. Revisión y auditoría

El SMS llevará a cabo de forma periódica, y al menos cada dos años, una auditoría encaminada a la verificación, evaluación y valoración de la eficacia de las medidas técnicas y organizativas para garantizar loa seguridad de los tratamientos y sistemas de información.

En todo caso, se realizará una auditoría específica y extraordinaria cuando se lleven a cabo modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas.

Las auditorías serán supervisadas por el Responsable de Seguridad de la Información y por el Delegado de Protección de Datos cada uno en el ejercicio de sus competencias.

9. Organización de la seguridad

La estructura organizativa para la gestión de la seguridad de la información en el ámbito de la Política de Protección de Datos y Seguridad de la Información del SMS está compuesta por los siguientes agentes:

1. Comité de Protección de Datos y Seguridad de la Información
2. Responsable del Tratamiento
3. Responsable de la Información
4. Responsable del Servicio
5. Responsable de Seguridad de la Información
6. Responsable del Sistema
7. Delegado de Protección de Datos

10. Comité de Protección de Datos y Seguridad de la Información

El Comité de Protección de Datos y Seguridad de la Información (en adelante Comité), bajo la dirección del Director Gerente del Servicio Murciano de Salud, es un órgano colegiado de los previstos en el artículo 20.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que gestionará y coordinará todas las actividades relacionadas con la Política de Protección de Datos y la Seguridad de la información.

El Comité está compuesto por los siguientes miembros:

• **Responsable del Comité:** titular de la Subdirección General de Tecnologías de la información. Tendrá voto de calidad en la toma de decisiones del Comité.

• **Secretario**: será el Responsable de Seguridad de la información de la Subdirección General de Tecnologías de la Información, siendo el coordinador del Comité.

• **Vocales:** se propone a al menos a un representante de cada una de las Direcciones Generales y un miembro de la Secretaría General Técnica.

Delegado de protección de datos: Adicionalmente participará con voz, pero sin voto en las reuniones del Comité cuando en el mismo vayan a acordarse cuestiones relacionadas con el tratamiento de datos de carácter personal, así como siempre que se requiera su participación. En todo caso, si un asunto se sometiese a votación se hará constar siempre en el acta el parecer del DPD.

El Comité actuará en el ámbito de cumplimiento de la normativa de protección de datos y seguridad de la información vigente.

El Comité coordinará las actividades relacionadas con la seguridad de la información y los sistemas de información ejerciendo las siguientes funciones:

a) Atender las inquietudes de la Dirección de la Entidad, así como informar de forma regular sobre el estado de la seguridad de la información.

b) Elaborar propuestas de modificación y actualización permanente de la PPDSI del SMS y de su estructura organizativa.

c) Determinar los criterios para el procedimiento de análisis de riesgos y elaborar propuestas de niveles de riesgos aceptables para la seguridad de la información del SMS.

d) Aprobar las normas para garantizar la seguridad de la información.

e) Promover recursos y medios para la concienciación y formación en materia de seguridad de la información a todo el personal del SMS.

f) Velar por el cumplimiento de la PPDSI y su normativa de desarrollo.

g) Analizar los informes facilitados por el Responsable de Seguridad en lo relativo al resultado de los análisis de riesgos de las auditorías realizadas, de los proyectos y de las iniciativas y acciones de mejora de la seguridad requeridas.

h) Revisar la información facilitada por el Responsable de Seguridad de la Información relativa a los incidentes de seguridad.

i) Participar en la toma de decisiones que garanticen la seguridad de la información y los servicios del SMS.

11. Responsable del Tratamiento

Es Responsable del Tratamiento es el Director Gerente del Servicio Murciano de Salud en los términos establecidos en el artículo 4.7 del RGPD.

Serán funciones del Responsable del tratamiento:

a) Llevar a cabo un registro de las actividades de tratamiento efectuadas bajo su responsabilidad actualizado en los términos del artículo 30 del RGPD, así como determinar la base jurídica para su tratamiento.

b) Establecer y aplicar las medidas técnicas y organizativas de privacidad y seguridad necesarias para la protección de datos personales en los tratamientos que gestiona a fin de garantizar y poder demostrar que el tratamiento es conforme con el RGPD, revisándolas y actualizándolas cuando sea necesario.

c) Realizar las evaluaciones de impacto sobre la protección de datos (EIPD) necesarias cuando los tratamientos conlleven un alto riesgo para los derechos y libertades de los interesados. Recabará el asesoramiento del DPD al realizar la EIPD.

d) Garantizar el cumplimiento de los principios relativos al tratamiento en los términos del artículo 5 del RGPD.

e) Garantizar el cumplimiento de la obligación de informar adecuadamente y aplicando el principio de transparencia en la recogida de los datos personales.

f) Cumplir todas aquellas obligaciones y respetar los derechos de las personas interesadas, de acuerdo con lo previsto en el RGPD y en la LOPDGDD y demás normativa vigente.

g) Si el tratamiento o parte de él, fuera realizado por un encargado del tratamiento, el responsable del tratamiento elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas. Asimismo, realizará seguimiento de la correcta aplicación de estas medidas.

h) Realizar, en su caso, las preceptivas notificaciones de violaciones de seguridad a la autoridad de control, a las personas interesadas y al DPD.

i) En definitiva, velar por el efectivo cumplimiento del RGPD, de la LOPDGDD y demás normativa vigente en el tratamiento de datos personales.

12. Responsable de la Información

El Centro Criptológico Nacional establece que el Responsable de la Información es el responsable último de cualquier error o negligencia que conlleve

un incidente en la disponibilidad en materia de seguridad de la información y de confidencialidad e integridad en materia de protección de datos, concurriendo también en la figura del responsable del tratamiento, quien es el responsable último de la confidencialidad e integridad de los datos personales.

Es por ello que, la condición de Responsable de la información recae en el Director Gerente que tendrá asimismo la condición de responsable de los tratamientos llevados a cabo por el SMS.

En el marco del Esquema Nacional de Seguridad, son funciones del responsable de la información:

a) Establecer los requisitos o niveles de la información en materia de seguridad.

b) Aprobación formal de los niveles, pudiendo recabar una propuesta al Responsable de la Seguridad y la opinión del Responsable del Sistema.

La determinación de los niveles en cada dimensión de seguridad debe realizarse dentro del marco establecido en el anexo I del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica.

13. Responsables del Servicio

El Responsable del servicio es la persona que determina los requisitos de seguridad de los servicios prestados a partir de la información (a veces se dice "se heredan los requisitos") y los niveles de seguridad del mismo dentro del marco que establece el anexo I del Real Decreto 3/2010, pudiendo recabar para ello la propuesta del Responsable de Seguridad y la opinión del Responsable del Sistema.

Las funciones de Responsable del Servicio recaerán en la persona titular del órgano o unidad administrativa que gestione cada procedimiento administrativo y en cuyo ámbito se lleve a cabo el tratamiento de los datos de carácter personal en su caso. Un tratamiento de información puede abarcar diferentes servicios y, por tanto, la existencia de uno o varios responsables del servicio.

14. Responsable de Seguridad de la Información

La condición de Responsable de Seguridad recae en el Técnico Responsable del Departamento de Informática. Es la persona que decide las medidas organizativas y técnicas exigibles para garantizar la protección de datos y la seguridad de la información en los servicios prestados con base en los requisitos fijados por el responsable del tratamiento y el responsable de la información.

Son funciones del responsable de seguridad de la información del SMS las siguientes:

a) Mantenimiento y mejora continua de la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad.

b) Promover la formación y concienciación en materia de seguridad de la información entre el personal del SMS.

c) La elaboración y mantenimiento actualizado de procedimientos y normativas de seguridad que serán presentados al Comité de protección de datos y seguridad de la información para su revisión y aprobación.

d) Elaborar el documento de Declaración de Aplicabilidad vistas las medidas del anexo II del ENS y las exigencias derivadas de los datos de carácter personal

en cumplimiento de lo establecido en la Disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales que establece que el ENS establecerá las medidas que deban implantarse en caso de tratamiento de datos personales.

e) Promover la realización de auditorías periódicas internas o externas para verificar el cumplimiento de las obligaciones del SMS con relación a la seguridad de la información.

f) Constituir el punto de contacto para la coordinación con el equipo de respuesta ante incidencias de seguridad informáticas (CSIRT).

g) La coordinación con el Centro Criptológico Nacional en la utilización de servicios de respuesta a incidentes de seguridad de la información.

h) La coordinación y control del cumplimiento de las medidas de seguridad definidas en los documentos y normas que desarrollen la presente política.

i) La gestión de las incidencias de seguridad de la información que se produzcan informando de las más relevantes al Comité de Seguridad y a los responsables de las unidades del SMS afectadas por las incidencias.

j) Participar en el Comité de Protección de Datos y Seguridad de la Información como Secretario.

Habida cuenta la existencia de sistemas de información que, por su complejidad, distribución, separación física de sus elementos y números de usuarios, se hace necesario contar con Responsables de Seguridad Delegados para llevar a cabo las funciones de Responsable de Seguridad en cada una de las Gerencias.

Se asignará un Responsable de Seguridad Delegado para cada una de las 9 Gerencias de área de Salud más uno para cada una de las siguientes; Gerencia de Salud mental, Gerencia 061 y Gerencia de Hemodonación.

Los Responsables de Seguridad Delegados realizarán esas funciones bajo la supervisión, directrices y mandato del Responsable de Seguridad.

15. Responsable del Sistema

Será responsable del sistema el jefe/a del servicio, sistemas informáticos y comunicaciones. En calidad de responsable será el encargado de:

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

b) Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.

c) Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.

Para el desempeño de estas funciones, podrá contar con el personal técnico del SMS que sea necesario.

16. Delegado de Protección de Datos

El SMS cuenta con un Delegado de Protección de Datos a fin de dar cumplimiento a lo requerido en el artículo 37.1.a) del RGPD. Dicha designación fue comunicada a la Agencia Española de Protección de Datos de acuerdo con lo establecido en el artículo 34.2 de la LOPDGDD.

El Delegado de Protección además de las tareas establecidas en el artículo 39 del RGPD, llevará a cabo las tareas que deriven de la normativa española de

protección de datos de carácter personal, de los documentos de buenas prácticas que se adopten por la propia Agencia Española de Protección de Datos y de su esquema de certificación AEPD-DPD.

Se garantiza la independencia del Delegado de Protección de Datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses. En el desempeño de sus tareas, tendrá acceso a los datos personales y procesos de tratamiento.

17. Asignación de tareas

El Director Gerente podrá, asignar tareas relativas a la mejora de los principios recogidos en la presente política a personas o grupos de trabajo. En la asignación de tareas se tendrá en cuenta a todo el personal que presta sus servicios en el SMS y a especialistas externos cuando sea necesario.

18. Resolución de conflictos

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de esta política, le corresponderá en última instancia, a la Dirección, asistida por el Comité de Protección de Datos y Seguridad de la Información y al Delegado de Protección de Datos en su caso. Los datos personales constituyen un objeto protegido de mayor rango y marcarán las pautas a seguir.

19. Obligaciones del personal

Todos los órganos y unidades del SMS prestarán su colaboración en las actuaciones de implementación de la Política de Protección de Datos y Seguridad de la Información, debiendo colaborar en la mejora de los principios y requisitos en materia de protección de datos y seguridad de la información evitando y aminorando los riesgos a los que se encuentra expuesta la información y los datos personales de los que es titular el SMS. A tal efecto, comunicarán a los integrantes de la estructura organizativa de este Política cualquier propuesta o sugerencia que ayude a preservar la confidencialidad, la integridad y la disponibilidad de la información.

Todas las personas que presten servicio al SMS tienen la obligación de conocer y cumplir lo previsto en la presente Política, así como las normas y procedimientos que la desarrollen.

Cuando el SMS utilice servicios de terceros o les ceda información, se les hará partícipes de esta Política y normas y procedimientos que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

20. Concienciación y formación

Se desarrollarán actividades formativas específicas orientadas a la concienciación y formación del personal que presta sus servicios en el SMS, así como la difusión entre los mismos de esta Política y de su desarrollo normativo.

El SMS dispondrá los medios necesarios para que todas las personas con acceso a la información sean informadas acerca de sus deberes y obligaciones, así como de los riesgos existentes en el tratamiento de la información.

El Delegado de protección de datos se encargará de impartir la formación y concienciación al personal que participa en las operaciones de tratamiento con datos personales, y el Responsable de la Seguridad sobre la seguridad de la información, así como de su supervisión en el caso de delegar dicha función, a fin de garantizar el cumplimiento de la presente Política.

21. Desarrollo normativo de la PPDSI

El cuerpo normativo sobre Protección de Datos y Seguridad de la información se desarrollará en cinco niveles con diferente ámbito de aplicación, nivel de detalle técnico y obligatoriedad de cumplimiento, pero de manera que cada elemento normativo se fundamente en las normas de nivel superior y por encima de todas, la presente Política.

1) **Primer nivel**: está constituido por la presente Política de Protección de Datos y Seguridad de la Información, aprobada por la Dirección del SMS.

2) **Segundo nivel:** formado por la distinta normativa de seguridad y, constituye la reglamentación que debe seguirse, o a la que deben ajustarse las conductas, tareas o actividades de las personas en relación con la protección de la información. Serán aprobadas por el Comité de Protección de Datos y Seguridad de la Información.

3) **Tercer nivel**: constituido por los procedimientos generales que describen las acciones a realizar en un proceso relacionado con la seguridad de la información, responsabilidad de varias unidades organizativas. Dichos procedimientos serán aprobados por el Responsable de Seguridad de la Información.

4) **Cuarto nivel**: los procedimientos específicos, son los mismos que los procedimientos genéricos con la diferencia de que estos están orientados a una unidad organizativa concreta. Serán aprobados por el Responsable de Seguridad y creados por la unidad implicada.

5) **Quinto nivel**: compuesto por informes, registros y evidencias electrónicas. Los informes son documentos de carácter técnico que recogen el resultado y las conclusiones de un estudio o de una evaluación. Los registros de actividad o alertas de seguridad son documentos de carácter técnico que recogen amenazas y vulnerabilidades. Las evidencias electrónicas se generan durante todo el ciclo de vida de los sistemas de información, pudiendo abarcar uno o más sistemas en función del aspecto tratado.

22. Consecuencias del incumplimiento

El incumplimiento de la Política de Protección de datos y Seguridad de la Información o su normativa de desarrollo, dará lugar al establecimiento por la Dirección del SMS de medidas correctivas, encaminadas a salvaguardar y proteger las redes y sistemas de información, sin perjuicio de la correspondiente exigencia de responsabilidades disciplinarias.