I. Comunidad Autónoma

3. Otras disposiciones

Consejería de Salud

Servicio Murciano de Salud

6702 Resolución de la Directora 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 30 de octubre de 2023, el Consejo de Administración del Servicio Murciano de Salud, a propuesta de la Directora 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 30 de octubre de 2023, 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 siguiente de su publicación en el Boletín Oficial de la Región de Murcia.

Murcia, 12 de noviembre de 2023.—La Directora Gerente, Servicio Murciano de Salud, Isabel Ayala Vigueras.

ANEXO

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 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en adelante ENS, 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 12 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, detección, respuesta y conservación, líneas de defensa, vigilancia continua y reevaluación periódica y diferenciación de responsabilidades) y desarrollará una serie de requisitos mínimos de seguridad establecidos en el Capítulo III.

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 la Política) 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 Política 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 Política 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 Política 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.

Por ello, es misión del SMS el cumplimiento de toda la normativa en materia de seguridad de la información que le sea de aplicación para la protección de la confidencialidad, integridad y disponibilidad de los servicios activos de la información del SMS.

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 de manera separada en el Excel Marco Normativo de la Política de Protección de Datos y Seguridad de la Información, garantizando la vigencia normativa aplicable.

El SMS, desarrollará sus funciones de acuerdo con el marco normativo detallado, las normativas, procedimientos y procesos internos desarrollados para el cumplimiento del Esquema Nacional de Seguridad.

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

Los principios y requisitos que deben de contemplarse a la hora de garantizar la seguridad de la información y asegurar que el SMS cumpla sus objetivos utilizando sistemas de información, están dirigidos por el marco normativo indicado y se desarrollan en este apartado.

5.1. Principios de Protección de datos

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) 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;

5.2. Principios de Seguridad de la Información

a) Seguridad integral: 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;

b) Gestión de riesgos: El análisis y la gestión de los riesgos es parte esencial del proceso de seguridad, debiendo constituir una actividad continua y permanentemente actualizada. La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables. La reducción a estos niveles se realizará mediante una apropiada

aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a los que estén expuestos;

c) Prevención, reacción y recuperación: La seguridad del sistema debe contemplar aspectos de prevención, detección, respuesta y recuperación, de manera que las amenazas existentes no se materialicen, o en caso de materializarse no afecten gravemente a la información que maneja, o los servicios que se prestan;

d) Líneas de defensa: El sistema ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas falle, permita, ganar tiempo para una reacción adecuada, reducir la probabilidad de que el sistema sea comprometido en su conjunto y minimizar el impacto final;

e) Reevaluación periódica: Las medidas de seguridad se reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario;

f) La seguridad como función 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.

5.3. Requisitos mínimos

Asimismo, la presente política se desarrolla aplicando los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad: la seguridad debe comprometer a todos los miembros del SMS. Por ello, esta política detalla la identificación de los responsables de velar por su cumplimiento y deberá darse a conocer por todos los miembros del SMS.

b) 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. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

c) Gestión 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. El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad que serán aprobadas por la dirección o el órgano superior correspondiente.

d) 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: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento. Asimismo, el SMS exigirá que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y niveles idóneos de gestión y madurez en los servicios prestado.

e) Autorización y control de los accesos: El acceso controlado a los sistemas de información estará limitado a los usuarios, procesos, dispositivos u otros

sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

f) Protección de las instalaciones: Los sistemas de información y su infraestructura de comunicaciones asociada deberán permanecer en áreas controladas y disponer de los mecanismos de acceso adecuados y proporcionales en función del análisis de riesgos, sin perjuicio de lo establecido en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y en el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

g) Adquisición de productos de seguridad y contratación de servicios de seguridad: se utilizarán, de forma proporcionada a la categoría del sistema y el nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición. Se atenderá a lo establecido por el CCN en cuanto a los requisitos y certificaciones de seguridad que se requieran.

h) Mínimo privilegio: Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño.

i) Integridad y actualización del sistema: La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa. La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

j) Protección de la información almacenada y en tránsito: a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección. Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información. oda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a la que se refiere este real decreto, deberá estar protegida con el mismo grado de seguridad que ésta.

k) Prevención ante otros sistemas de información interconectados: Se protegerá el perímetro del sistema de información, especialmente, si se conecta a redes públicas.

l) Registro de actividad y detección de código dañino: se registrarán las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

m) Incidentes de seguridad: se dispone de mecanismos para la detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

n) Continuidad de la actividad: los sistemas dispondrán de copias de seguridad y se implantarán los mecanismos apropiados para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

o) Mejora continua del proceso de seguridad: El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información.

6.- Directrices para la estructuración de la documentación

El cuerpo normativo sobre seguridad de la información es de obligado cumplimiento y se desarrollará en los cuatro niveles indicados a continuación, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior:

a) Primer nivel: Política de Seguridad de la Información.

b) Segundo nivel: Normativas de Seguridad de la Información.

c) Tercer nivel: Procedimientos de Seguridad de la Información.

d) Cuarto nivel: Registros del Sistema de Gestión de Seguridad de Información (SGSI)

El personal del SMS tendrá la obligación de conocer y cumplir, además de la Política de Seguridad de la Información, todas las normativas y procedimientos de seguridad de la información que puedan afectar a sus funciones.

La política, las normativas y los procedimientos de seguridad de la información estarán disponibles en la Intranet del SMS.

Constituye el primer nivel la Política de Seguridad de la Información, recogida en el presente texto, aprobada por el Comité de Protección de Datos y Seguridad de la información y el Consejo de Administración del SMS a propuesta del Director Gerente del SMS.

El segundo nivel desarrolla la Política de Seguridad de la Información mediante normativas específicas que abarcan un área o aspecto determinado de la seguridad de la información. De acuerdo con la presente Política, serán aprobadas por el Comité de Protección de Datos y Seguridad de la información.

Dichas normativas versaran sobre cada uno de los controles de seguridad establecidos en el ENS, en especial respecto al uso correcto de los equipos, servicios e instalaciones, así como lo que se considera uso indebido, la responsabilidad del personal con respecto al cumplimiento o violación de la normativa, derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

El tercer nivel está constituido por directrices de carácter técnico o procedimental que se deben observar en tareas o actividades relacionadas con la seguridad de la información y la protección de la información y de los servicios, y que serán aprobadas por el responsable de la seguridad o por el responsable de sistemas o servicios según su ámbito de competencia.

El cuarto nivel está constituido por diferentes informes, registros y evidencias electrónicas que permiten comprobar el efectivo cumplimiento de las medidas de seguridad acordadas por el SMS.

7.- 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. Subcomité de seguridad TI

3. Responsable del Tratamiento

4. Responsable de la Información

5. Responsable del Servicio

6. Responsable de Seguridad de la Información

7. Responsable del Sistema

8. Delegado de Protección de Datos

9. Administrador de seguridad

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

El Comité de Protección de Datos y Seguridad de la Información (en adelante Comité), 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 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.

7.2. Subcomité de Seguridad TI

Se trata de un grupo eminentemente técnico encargado de analizar las medidas de seguridad a implantar en la organización para garantizar la seguridad TI, establecer planes para la ejecución de dichas medidas y coordinar su adecuada ejecución. Se reunirán con carácter periódico, tantas veces como sea necesario para la consecución de los citados fines.

Estará formado, al menos por:

· Responsable de seguridad

· Responsable del sistema

· Responsable del servicio

· Administrador de Seguridad

7.3. 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.

7.4. Responsable de la Información

Son responsables de la información los titulares de las unidades organizativas dependientes del SMS, responsables de la información afectada por la Política de Seguridad de la Información, en sus respectivos ámbitos de competencias.

Corresponde al responsable de la información establecer los requisitos de la información en materia de seguridad, y en particular:

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

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

c) Aceptar los riesgos residuales respecto de la información calculada en el análisis de riesgos.

7.5. Responsables del Servicio

Es Responsable del servicio la persona titular del Servicio de Coordinación y Aplicaciones Informáticas (en adelante SCAI). El Responsable de dicho servicio coordina la actuación de su equipo, quienes tienen repartido la gestión de los diferentes aplicativos necesarios para dar continuidad a los servicios que tiene encomendados el SMS.

Será el Responsable quien, llegado el caso, designará y delegará en la persona/as competentes las funciones de responsable del servicio en función del servicio en cuestión.

Corresponde al responsable del servicio establecer los requisitos del servicio en materia de seguridad, y en particular:

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

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

c) Aceptar los riesgos residuales respecto de la información calculada en el análisis de riesgos.

7.6. Responsable de Seguridad

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, el Responsable de seguridad podrá designar Responsables de Seguridad Delegados para llevar a cabo las funciones de Responsable de Seguridad en cada una de las Áreas.

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

7.7. Responsable del Sistema

Será responsable del sistema el Subdirector General de Tecnologías de la información. 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 y/o delegar en el personal técnico del SMS que sea necesario.

7.8. 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.

7.9. Administrador de seguridad

Atendiendo a la estructura organizativa del SMS, el rol de Administrador de seguridad puede ser ejercido por diferentes personas dado que la seguridad es trasversal a toda la organización y la implantación, gestión y mantenimiento de las diferentes medidas de seguridad aplicables a un sistema de información puede depender de diferentes esferas de conocimiento.

Dado que se trata de un rol operacional, sus funciones serán llevadas a cabo por la persona titular del Servicio de Sistemas Informáticos y Comunicaciones (SSIC), quien podrá delegar dichas funciones en su personal y soporte técnico.

Dichas funciones son las siguientes:

a) La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información,

b) La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información,

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

d) La aplicación de los Procedimientos Operativos de Seguridad (POS).

e) Asegurar que los controles de seguridad establecidos son adecuadamente observados.

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

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

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

i) Informar al Responsable de la Seguridad o al Responsable del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.

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

8.- Procedimiento para la designación y renovación de los roles

Será el Comité de Protección de Datos y Seguridad de la Información el encargado de aprobar en acta la designación de cada uno de los roles asociados a un cargo, de tal manera que dicho rol será siempre ostentado por la persona titular del cargo en el SMS.

9.- Datos personales

El SMS realiza tratamientos de datos de carácter personal. La relación de actividades de tratamiento se encuentra publicada en el Registro de Actividades de Tratamiento del SMS, que está disponible para su consulta en la web Murciasalud.

10.- 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 y al menos una vez al año sobre el sistema de información, conforme a los principios de gestión de la seguridad basada en los riesgos y en la reevaluación periódica.

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.

Asimismo, se tendrán en cuenta para la evaluación de los riesgos que se deriven del tratamiento de datos, el catálogo de amenazas de la Comisión Europea respecto al ejercicio de derechos de los ciudadanos.

11.- 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.

12.- 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.

13.- Obligaciones del personal propio y terceros

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.

14.- Revisión y auditoría

El Comité de Protección de Datos y Seguridad de la Información revisará anualmente la presente Política o cuando exista un cambio significativo que obligue a ello.

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 la 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.

15.- 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.

16.- Derogación

Queda derogada la Política de Protección de datos y Seguridad de la Información del servicio Murciano de Salud, aprobada por Acuerdo del Consejo de Administración del Servicio Murciano de Salud de fecha 6 de febrero de 2020 (BORM n.º 180, de 5-8-2020).

MARCO NORMATIVO

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad
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
Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digital
Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
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.
Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de
Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras
Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las
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.
Ley 14/1986, de 25 de abril, General de Sanidad.

MARCO NORMATIVO

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

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

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

NORMATIVA SMS

N1	Normativa de buen uso de los sistemas
N2	Normativa de buen uso del correo electrónico
N3	Normativa de buen uso del servicio de internet
N4	Normativa de clasificación de la información
N5	Normativa de protección de los equipos portátiles corporativos
N6	Normativa de protección de puesto de trabajo
N7	Normativa Control de Acceso
N8	Normativa de adquisición, desarrollo y mantenimiento de los sistemas de información
N9	Normativa Plan de Continuidad del Servicio
N10	Normativa Protección de los soportes de información
N11	Normativa Gestión, monitorización y registro de la actividad
N12	Normativa Protección de la información
N13	Normativa Gestión del Personal
N14	Normativa Gestión de las comunicaciones
N15	Normativa Protección física y de los equipos
N16	Normativa Relación con proveedores
N17	Normativa Gestión de Incidentes

OTROS DOCUMENTOS SMS

D1	Arquitectura de comunicaciones - SSCC
D2	Herramientas de seguridad
D3	Documento: Instalaciones e infraestructuras. Áreas separadas y medidas de control

Guías CCN-STIC ESQUEMA NACIONAL DE SEGURIDAD

800 Glosario de términos y abreviaturas del ENS
801 Responsables y funciones en el ENS
802 Auditoría de la seguridad en el ENS
803 Valoración de sistemas en el ENS
804 Medidas de implantación del ENS
805 Política de seguridad de la información
806 Plan de adecuación del ENS
807 Criptografía de empleo en el ENS
808 Verificación del cumplimiento de las medidas en el ENS
809 Declaración de conformidad del ENS
810 Creación de un CERT/CSIRT
811 Interconexión en el ENS
812 Seguridad en entornos y aplicaciones Web
813 Componentes certificados en el ENS
814 Seguridad en el correo electrónico
815 Métricas e indicadores en el ENS
816 Seguridad en Redes inalambricas en el ENS
817 Criterios comunes para la gestión de incidentes de seguridad
818 Herramientas de seguridad en el ENS
819 Medidas compensatorias
820 Protección contra denegación del servicio
821 Normas de seguridad ENS
822 Procedimientos de seguridad
823 Utilización de servicios en la nube
824 Información del Estado de Seguridad
825 Esquema Nacional de Seguridad. Certificaciones 27001
826 Implementación de Seguridad Nextcloud
827 Gestión y uso de dispositivos móviles
830 Ámbito de aplicación del Esquema Nacional de Seguridad
831 Registro de la actividad de los usuarios
834 Protección ante Código Dañino en el ENS
835 Borrado de metadatos en el marco del ENS
836 Seguridad en VPN
844 Manual de usuario de INES

OTROS DOCUMENTOS

Magerit – v.3 Metodologías de Análisis y Gestión de Riesgos de los Sistemas de Información
- Libro I: Método
- Libro II: Catálogo de elementos
- Libro III: Guía de técnicas

Catálogo de amenazas de la Comisión Europea respecto al ejercicio de derechos de los ciudadanos