3. Otras disposiciones

CONSEJERÍA DE SALUD Y FAMILIAS

Resolución de 8 de abril de 2021, de la Dirección Gerencia del Servicio Andaluz de Salud, por la que se aprueba la Política de Seguridad de las Tecnologías de la información y la comunicación del Servicio Andaluz de Salud.

El Servicio Andaluz de Salud (SAS), creado mediante la Ley 8/1986, de 6 de mayo, del Servicio Andaluz de Salud, es una agencia administrativa de las previstas en el artículo 65 de la Ley 9/2007, de 22 de octubre. Está adscrito a la Consejería de Salud y Familias, desarrollando sus funciones bajo la supervisión y control de la misma, dependiendo específicamente de la Viceconsejería, conforme al Decreto 105/2019, de 12 de febrero, por el que se establece la estructura orgánica de la Consejería de Salud y Familias y del Servicio Andaluz de Salud.

El SAS forma parte esencial del Sistema Sanitario Público de Andalucía conforme al artículo 45, apartado 1, punto a) de la Ley 2/1998, de 15 de junio, de Salud de Andalucía. Entre sus funciones, destacan por su relevancia la gestión del conjunto de prestaciones sanitarias en el terreno de la promoción y protección de la salud, prevención de la enfermedad, asistencia sanitaria y rehabilitación que le corresponda en el territorio de la Comunidad Autónoma de Andalucía, la administración y gestión de las instituciones, centros y servicios sanitarios que actúan bajo su dependencia orgánica y funcional y la gestión de los recursos humanos, materiales y financieros que se le asignen para el desarrollo de sus funciones.

El ofrecimiento de servicios sanitarios públicos de calidad, buscando la eficiencia, el aprovechamiento óptimo de los recursos, la accesibilidad, la equidad y satisfacción de los usuarios, requiere indiscutiblemente gestionar de forma segura la información como uno de los activos más importantes. Este hecho, y el uso extensivo de las tecnologías de la información y comunicaciones, ponen de manifiesto la necesidad de definir la Política de Seguridad TIC del SAS, con el objetivo de establecer directrices básicas y duraderas para una protección eficaz de los sistemas gestionados por el organismo y de la información almacenada en los mismos.

La presente Política de Seguridad TIC responde a las directrices marcadas por el artículo 11 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS) en el ámbito de la Administración Electrónica, donde se expresa el deber de disponer de un documento de Política de Seguridad que deberá ser aprobado por el titular del órgano superior correspondiente, tomando en consideración los principios básicos y requisitos mínimos señalados en el ENS.

Del mismo modo, esta política se dicta en desarrollo y respuesta concreta al artículo 10 del Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía (modificado por el Decreto 70/2017, de 6 de junio, con los cambios introducidos por el Decreto 171/2020, de 13 de octubre, por el que se establece la Política de Seguridad Interior en la Administración de la Junta de Andalucía.

La aprobación de esta política manifiesta el interés de los órganos de gobierno del SAS en la gestión de la seguridad TIC. Con ella se establecen los objetivos y las responsabilidades necesarias para proteger los activos de información y los medios que se usen para su proceso, garantizando la integridad, disponibilidad y confidencialidad de estos, cumpliendo con el marco legal vigente y respetando las directrices, normas y procedimientos que oportunamente se establezcan.

Para ello, el SAS establecerá las medidas técnicas, organizativas y de control que garanticen la consecución de estos objetivos.

00190161

Sobre estos fundamentos y en ejercicio de las competencias atribuidas por el artículo 69 de la Ley 2/1998, de 15 de junio, de Salud de Andalucía, en relación con el Decreto 105/2019, de 12 de febrero, por el que se establece la estructura orgánica de la Consejería de Salud y Familias y del Servicio Andaluz de Salud (en adelante SAS),

R E S U E L V O

Primero. Aprobar el Documento de Política de Seguridad de las Tecnologías de la Información y la Comunicación (TIC) del Servicio Andaluz de Salud que se especifica en el Anexo único a esta Resolución.

Segundo. La presente resolución producirá efectos desde el día siguiente a su publicación en el Boletín Oficial de la Junta de Andalucía.

Sevilla, 8 de abril de 2021.- El Director Gerente, Miguel Ángel Guzmán Ruiz.

A N E X O

DOCUMENTO DE POLÍTICA DE SEGURIDAD DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DEL SERVICIO ANDALUZ DE SALUD

1. Objeto.

El presente documento tiene por objeto definir y regular la política de Seguridad de las tecnologías de la información y las comunicaciones (en adelante TIC) del Servicio Andaluz de Salud, que se debe aplicar en el tratamiento de los activos TIC de su titularidad o cuya gestión tenga encomendada.

2. Ámbito de aplicación.

La política de Seguridad TIC contenida en el presente documento será de aplicación al Servicio Andaluz de Salud, tanto a sus Servicios Centrales como en sus diferentes órganos, centros e Instituciones sanitarias desplegadas en el territorio e integradas administrativamente en el mismo. También será de aplicación para todas las personas que accedan a los Sistemas de Información como a la propia información que sea gestionada por el Servicio Andaluz de Salud, con independencia de cuál sea su destino, adscripción o relación con la misma.

Con carácter meramente enunciativo, la política de seguridad contenida en el presente documento será de aplicación a los servicios centrales; a los servicios de atención primaria y hospitalaria prestados por Instituciones dependientes o vinculadas y a las organizaciones específicas como son las áreas de gestión sanitaria y la red andaluza de medicina transfusional, tejidos y células trasplantes.

Esta política de Seguridad TIC se hará extensiva a los centros y servicios de terceros concertados con el SAS o Consorcios que compartan información con el mismo, en los términos previstos en el presente documento.

Así mismo, podrá ser aplicable a cualesquiera otros centros, servicios y establecimientos sanitarios que formen parte del Sistema Sanitario Público de Andalucía y que no encuentren cobertura en la política de seguridad TIC de la Consejería de Salud y Familias.

3. Misión.

La política de seguridad TIC tiene como misión disminuir de manera significativa los riesgos a los que están sometidos los activos de información que dan soporte a los procesos de protección de la salud de la ciudadanía.

00190161

En sentido amplio, satisfacer esta misión consiste en lograr niveles adecuados de disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad, como dimensiones de la seguridad, para toda la información institucional relevante, con el objeto de asegurar la continuidad operacional de los procesos y servicios; y también de privacidad, para salvaguardar los derechos y libertades de las personas físicas.

Todo ello a través de un sistema de gestión de seguridad de la información.

4. Definiciones.

1. Se asumen las definiciones y estándares establecidos en el artículo 2 del Decreto 1/20011, de 11 de enero, circunscritos al ámbito competencial del SAS en política de seguridad TIC y a su ámbito de aplicación.

2. Además, a los efectos previstos en este Documento, han de entenderse las siguientes definiciones:

a) Activo de información: información con valor para la organización incluyendo los soportes, sistemas, servicios, infraestructuras e instalaciones donde se trata. En todo momento se entenderá incluido en este concepto al activo TIC.

b) Seguridad TIC: entendida en sentido amplio, comprende las dimensiones de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de la información, así como la protección de datos personales.

c) Servicio: función o prestación desempeñada por el SAS destinada a cuidar intereses o satisfacer necesidades de los ciudadanos, en el contexto de los sistemas de información.

d) Marco normativo de seguridad TIC: política, normas y planes de seguridad, procedimientos técnicos, recomendaciones, y buenas prácticas definidas por la organización para dar cumplimiento a la presente política.

e) Instituciones: comprende a los hospitales; áreas de gestión sanitaria; distritos sanitarios; centros de transfusión, tejidos y células; así como los órganos dependientes del SAS.

f) Red pública de comunicaciones: una red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público y que soporta la transferencia de señales entre puntos de terminación de la red.

5. Objetivos.

La presente Política de Seguridad TIC expresa el compromiso del SAS con la gestión de la seguridad TIC para dar respuesta a la obligación recogida en el artículo 10 del Decreto 1/2011, modificado por el Decreto 70/2017. Así mismo da cumplimiento a las obligaciones establecidas en el ENS.

Por tanto, los objetivos de la Política de Seguridad del SAS son:

a) Dirigir y dar soporte al gobierno y gestión de la seguridad TIC, entendida como un proceso de mejora continua.

b) Establecer el marco normativo de seguridad TIC, considerando especialmente la continuidad de los servicios y la gestión de incidencias.

c) Impulsar la formación y concienciación en materia de seguridad TIC del personal, garantizando el conocimiento del marco normativo de seguridad.

d) Definir la estructura organizativa en la que se apoyará el gobierno de la seguridad TIC, indicando comités, unidades, roles y figuras necesarias, así como sus funciones y responsabilidades.

e) Garantizar la ejecución de los análisis y planes de tratamiento del riesgo de los activos de información.

f) Garantizar la eficacia de las medidas de seguridad implantadas por medio de evaluaciones, auditorías y certificaciones.

00190161

6. Contexto y obligaciones generales.

Las instituciones y entidades del SAS incluidas en el ámbito de aplicación de la Política de Seguridad TIC dependen de forma significativa de las Tecnologías de la Información y las Comunicaciones (TIC) para alcanzar sus objetivos. En consecuencia, éstas deben ser administradas con diligencia, tomando las medidas adecuadas para protegerlas frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo último de la Política de Seguridad TIC es garantizar la calidad de la información y la prestación continuada de los servicios para que el SAS pueda cumplir sus objetivos. Para ello, y según el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad, en las decisiones en materia de seguridad deberán tenerse en cuenta los siguientes principios básicos:

I. Seguridad integral, entendida como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el Sistema.

II. Gestión de riesgos, donde el análisis de estos será parte esencial del proceso de seguridad, y cuya gestión dará lugar al mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables.

III. Prevención, reacción y recuperación, para evitar que las amenazas sobre el mismo no se materialicen y no afecten gravemente a la información que maneja o a los servicios que se prestan.

IV. Líneas de defensa, estableciendo una estrategia de protección constituida por múltiples capas de seguridad;

V. Reevaluación periódica de las medidas de seguridad y actualización permanente de las mismas.

VI. Función diferenciada, donde la responsabilidad de la seguridad TIC estará diferenciada de la responsabilidad del sistema y por tanto de la responsabilidad sobre la prestación de los servicios.

Asimismo, la información en general y los sistemas TIC en particular deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los centros directivos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes centros directivos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en los pliegos de licitación, especialmente para proyectos TIC.

7. Marco normativo.

El diseño, operación, uso y administración de la información, los sistemas y los servicios del SAS deben cumplir las siguientes normas y cualesquiera otras que resulten de aplicación:

a) El marco normativo general de carácter autonómico definido en virtud de la disposición adicional primera del Decreto 1/2011, por la Consejería competente en materia de coordinación y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones, a propuesta del Comité de Seguridad TIC de la Junta de Andalucía.

b) El marco normativo autonómico para la seguridad interior definido por el Decreto 171/2020, de 13 de octubre.

00190161

c) El marco normativo general de carácter nacional e internacional, vigente en cada momento, que en materia de seguridad TIC genere responsabilidades en el SAS en virtud de su naturaleza legal. A estos efectos y con carácter enunciativo, pero no limitativo, se consideran las siguientes normas:

1. 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.
2. 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.
3. Reglamento (UE) 2016/679 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 (Reglamento general de protección de datos o RGPD).
4. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
5. Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
6. Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
7. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
8. Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

d) El marco normativo sectorial, vigente en cada momento, que genere responsabilidades en el SAS en virtud de su naturaleza legal, con repercusión en la seguridad TIC. A estos efectos y con carácter enunciativo, pero no limitativo, se consideran las siguientes normas:

1. Ley 2/1998, de 15 de junio, de Salud de Andalucía.
2. Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.
3. Decreto 105/2019, de 12 de febrero, por el que se establece la estructura orgánica básica de la Consejería de Salud y Familias y del SAS, modificado por Decreto 118/2020, de 8 de septiembre.
4. Decreto 662/2019, de 27 de diciembre de administración electrónica, simplificación de procedimientos y racionalización organizativa de la Junta de Andalucía.

e) Las obligaciones contraídas con terceros con repercusión en la seguridad TIC.

El SAS podrá ampliar y desarrollar este marco normativo en los términos previstos en el apartado 12 de este documento.

8. Organización de la seguridad TIC

El mantenimiento y gestión de la seguridad TIC va íntimamente ligado al establecimiento de una organización de seguridad. Dicha organización se establece mediante la identificación y definición de las diferentes actividades y responsabilidades en materia de gestión de la seguridad y la implantación de una estructura que las soporte.

La organización de la Seguridad TIC del SAS que se define en este documento consta de los siguientes elementos:

a) Una estructura jerárquica de Comités competentes en materia de Seguridad TIC, los cuales se constituyen como órganos de decisión y gobierno, donde el nivel central coordinará a los Comités de carácter territorial o de Institución

b) La definición de los diferentes roles y responsabilidades en el gobierno y la gestión de la Seguridad TIC;

c) La definición de la Unidad de Seguridad TIC del SAS.

8.1. Comités: funciones y responsabilidades

La estructura organizativa para la gestión de la seguridad TIC en el SAS se compone de los siguientes órganos:

a) El Comité de Seguridad Interior y Seguridad TIC del SAS.

00190161

b) Los Comités de Seguridad interior y Seguridad TIC de las Instituciones que componen el SAS.

8.1.1. El Comité de Seguridad Interior y Seguridad TIC del SAS.

El Comité de Seguridad Interior y Seguridad TIC del SAS (en adelante CSISTIC-SAS) creado por Resolución de 26 de marzo de 2021 del Director Gerente del Servicio Andaluz de Salud por el que se crea el Comité de Seguridad interior y Seguridad de las tecnologías de la información y comunicaciones del SAS y se determinan su composición, funciones y bases de funcionamiento (BOJA núm. 65, de 08 de abril), es el órgano de dirección para la Política de Seguridad TIC de la Agencia.

El CSISTIC-SAS tendrá la composición, funciones y régimen funcional básicos que se establecen en su norma de creación.

8.1.2 Comités de Seguridad interior y Seguridad TIC de las Instituciones

Las Instituciones deberán contar con Comités de Seguridad interior y Seguridad TIC de las Instituciones y al menos, con una persona Responsable de Seguridad interior y una persona responsable de Seguridad TIC, de acuerdo con los criterios organizativos que establezca el CSISTIC-SAS.

Estos criterios garantizarán como mínimo las siguientes atribuciones a los Comités en materia de Seguridad TIC:

- Actuar como órgano no colegiado de dirección y seguimiento en materia de seguridad de los activos de información de su titularidad o cuya gestión tenga encomendada.

- Nombrar a la persona Responsable de Seguridad TIC de la Institución, que tendrá como mínimo las atribuciones establecidas en el artículo 11.2 del Decreto 1/2011 modificado por el Decreto 70/2017.

Las atribuciones de los Comités de Seguridad interior y Seguridad TIC de las Instituciones podrán ser asumidas por los comités de dirección existentes en las mismas.

En otro caso, su composición habrá de garantizar, en la medida de lo posible, la representación paritaria de mujeres y hombres, contando, al menos, con:

a) La persona titular de la Dirección-Gerencia de la institución, que ocupa su Presidencia.

b) Las personas responsables de las áreas Asistencial, Económica y de Personal, en calidad de responsables delegadas de los activos de información / tratamiento de datos de la entidad o institución.

c) La persona responsable de los Sistemas y Tecnologías de la institución.

d) La persona responsable de la Seguridad TIC de la institución.

e) La persona responsable de seguridad interior de la Institución.

f) La persona responsable de las Unidades de Atención de la Ciudadanía.

g) La persona responsable de Documentación Clínica.

Los Comités de Seguridad interior y Seguridad TIC de cada Institución dan respuesta al artículo 10 y la disposición adicional segunda del Decreto 1/2011, modificado por el Decreto 70/2017.

Para su efectiva constitución, se requerirá la aprobación previa del CSISTIC-SAS.

Los Comités de Seguridad TIC de las Instituciones podrán elevar al CSISTIC-SAS las cuestiones, actividades o necesidades relacionadas con la seguridad TIC en su ámbito de responsabilidad que consideren oportunas.

8.2. Perfiles: funciones y responsabilidades.

Se definen los siguientes roles para la gestión de la seguridad TIC en el SAS de acuerdo con el Esquema Nacional de Seguridad y el Reglamento General de Protección de Datos:

1. Responsables de la información
2. Responsables de los Servicios.
3. Responsables de los Sistemas y Tecnologías del SAS.
4. Delegado de Protección de Datos del SAS.
5. Responsable de Seguridad TIC del SAS.

00190161

6. Responsables de Seguridad TIC de las instituciones.

8.2.1. Responsables de la Información.

En el Servicio Andaluz de Salud, la superior responsabilidad de la información del mismo la ostenta el Director Gerente del organismo o persona (con nombramiento de alto cargo) en quien delegue.

La persona responsable de los activos de información (propietaria de la información) tendrá la responsabilidad última del uso que se haga de la información y de protegerla. Asumirá las funciones y tareas especificadas en el ENS para este rol, y en particular:

a) Establecer los requisitos de seguridad TIC, para lo que podrá solicitar la propuesta previa del CSISTIC-SAS.

b) Comunicar los requisitos de seguridad TIC a las personas responsables de la seguridad TIC competentes.

c) Asumir la responsabilidad final de implantar las medidas de protección de la información como responsables últimos de la misma.

d) Asumir la propiedad de los riesgos sobre la información, monitorizarlos y aceptar el riesgo residual.

e) Determinar y aprobar los niveles de seguridad requeridos en cada dimensión junto con la persona Responsable de los Servicios o con el Comité de Coordinación de la Seguridad TIC del SAS.

f) Aceptar el riesgo residual junto con la persona Responsable de los Servicios.

Esta figura también será, según dicta el Reglamento General de Protección de Datos y demás normativa relacionada, designada como Responsable de los Tratamientos, la cual queda definida como «la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento». Sus funciones específicas en esta materia constan en el apartado 9 titulado «Datos de Carácter Personal».

8.2.2. Responsables de los Servicios.

La/s persona/s responsable/s de los servicios tiene la responsabilidad última del uso que se haga de ellos y de protegerlos. Asumirá las funciones y tareas especificadas en el ENS para este rol y en particular:

a) Establecer los requisitos de seguridad de los servicios, para lo que podrá solicitar la propuesta previa del CSISTIC-SAS.

b) Comunicar los requisitos de seguridad de los servicios a las personas responsables de la seguridad TIC competentes.

c) Asumir la responsabilidad final de implantar las medidas de protección de los servicios como responsables últimos de los mismos.

d) Asumir la propiedad de los riesgos sobre los servicios, monitorizarlos y aceptar el riesgo residual.

e) Determinar y aprobar formalmente los niveles de seguridad de los servicios en cada dimensión.

f) Aceptar el riesgo residual sobre los servicios que le competen.

Las personas responsables de los servicios en el Servicio Andaluz de Salud serán las personas titulares de cada una de las Direcciones Generales del Organismo, cada una en su ámbito de competencias.

Las personas Responsables delos Servicios reportan a la Dirección Gerencia del SAS.

8.2.3. Responsables de los sistemas y tecnologías del SAS.

La Responsabilidad de los sistemas y tecnologías del SAS a efectos de esta Resolución recaerá en la persona que en cada momento tenga asignada la citada responsabilidad por designación del Director Gerente del organismo.

De acuerdo con la figura de responsable del sistema del ENS, las atribuciones del responsable de los sistemas y tecnologías del SAS serán las siguientes funciones y tareas:

00190161

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

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

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

d) Acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el responsable de la seguridad TIC, antes de ser ejecutada.

e) Elaborar procedimientos operativos de seguridad.

f) Junto al Responsable de Seguridad TIC del SAS, elaboran planes de mejora de la seguridad.

g) Elaborar planes de continuidad. Ejercicios.

h) Suspensión temporal del servicio si se produce una desviación elevada de los niveles aceptables de riesgos.

i) Elaborar el ciclo de vida: especificación, arquitectura, desarrollo, operación, cambios.

j) Planificar la implantación de las salvaguardas en el sistema.

Reportes:

- La persona Responsable de los sistemas y tecnologías del SAS informa a la persona Responsable de la Información de las incidencias funcionales relativa a la información que le compete.

- La persona Responsable de los sistemas y tecnologías del SAS informa a la persona Responsable del Servicio de las incidencias funcionales relativas al servicio que le compete.

- La persona Responsable de los sistemas y tecnologías del SAS reporta al CSISTIC-SAS de las actuaciones en materia de seguridad, en particular en lo relativo a decisiones de arquitectura del sistema, de la eficacia de las medidas de protección que se deben implantar, además de un resumen consolidado de los incidentes de seguridad.

El artículo 10 del ENS recoge el principio de «La seguridad como función diferenciada». Este principio exige que la persona Responsable de los sistemas y tecnologías del SAS sea independiente de la persona Responsable de Seguridad TIC del SAS.

8.2.4. Delegado de Protección de Datos del SAS.

El RGPD establece la figura del delegado de protección de datos (DPD) y su carácter obligatorio para las autoridades u organismos públicos, y por tanto plenamente aplicable en el marco del SAS.

Su nombramiento se realizará por la persona titular de la Viceconsejería con competencias en materia de Salud, conforme a los criterios establecidos por la Junta de Andalucía.

Su posición y funciones habrán de atenerse, al menos, a las descritas en la normativa y, respecto de estas últimas, en particular a las siguientes:

a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;

b) supervisar el cumplimiento de lo dispuesto en el RGPD, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35 del RGPD;

00190161

d) cooperar con la autoridad de control;

e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36 del RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto.

f) Asesorar al Comité de Ética de la Investigación en su ámbito, en calidad de experto en materia de protección de datos personales, conforme al apartado 2.h de la disposición adicional decimoséptima de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Estas funciones serán desempeñadas por el delegado de protección de datos del SAS prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

El delegado de protección de datos del SAS dará cobertura y actuará como referencia de las instituciones incluidas en el ámbito de aplicación de la presente política de seguridad TIC del SAS.

En consideración a la estructura organizativa y el tamaño del SAS, el delegado de protección de datos del SAS contará con el soporte de los distintos responsables de seguridad TIC.

8.2.5. Responsable de Seguridad TIC del SAS.

El CSISTIC-SAS nombrará a la persona Responsable de Seguridad TIC del SAS que tendrá la condición de Responsable de Seguridad en los términos establecidos en el ENS. Para ello se garantizará el principio de función diferenciada recogido en el artículo 10 del ENS y en el artículo 5.j del Decreto 1/2011.

De acuerdo con el artículo 11 del Decreto 1/2011, modificado por el Decreto 70/2017, la persona Responsable de la Seguridad TIC tendrá las siguientes funciones:

a) Labores de soporte, asesoramiento e información al CSISTIC-SAS.

b) La dirección de la Unidad de la Seguridad TIC del SAS.

c) Diseño y ejecución de los programas de actuación, incluyendo, entre otros, planes directores de seguridad, proyectos de desarrollo normativo, auditorías técnicas y de cumplimiento y planes de adecuación legal.

d) Definición, implantación y mantenimiento de los controles de carácter organizativo para la protección de la información, aplicaciones y sistemas, así como la realización y mantenimiento de los análisis de riesgos.

e) Definición y ejecución de los programas formativos y de concienciación relacionadas con buenas prácticas de seguridad TIC, procurando promover, en el proceso de selección de las personas participantes en estos programas, la concurrencia de mujeres.

f) Aplicación de los criterios y directrices de gestión de la seguridad emanadas del CSISTIC-SAS

g) Aplicación de los criterios y directrices de protección de datos emanadas del Delegado de Protección de Datos.

Tendrá atribuciones de coordinación y dirección de la labor desempeñada por el resto de las personas responsables de seguridad designadas.

8.2.6. El Responsable de Seguridad TICs de la Instituciones.

En cumplimiento del artículo 6.2.c.2.º del Decreto 1/2011 de 11 de enero, modificado por el Decreto 70/2017 de 6 de junio y el apartado tercero de la disposición adicional única del Decreto 70/2017 de 6 de junio, en cada Institución del SAS existirá un Responsable de Seguridad TIC de la misma, que será designado por el CSISTIC-SAS.

Dependerá funcionalmente del Responsable de Seguridad TIC del SAS y por tanto podrá actuar como Responsable de Seguridad Delegado en su ámbito competencial si así se determina.

El Responsable de Seguridad TIC de la Institución tendrá las siguientes atribuciones:

a) Formar parte como vocal del Comité de Seguridad interior y Seguridad TIC de la Institución.

00190161

b) Labores de soporte, asesoramiento e información al Comité de Seguridad Interior y Seguridad TIC de la institución correspondiente, así como de ejecución de las decisiones y acuerdos adoptados por éste.

c) Diseño y ejecución de los programas de actuación propios de la institución, incluyendo, entre otros, planes directores de seguridad, proyectos de desarrollo normativo, auditorías técnicas y de cumplimiento y planes de adecuación legal.

d) Definición, implantación y mantenimiento de los controles de carácter organizativo para la protección de la información, los datos de carácter personal, aplicaciones y sistemas, así como la realización y mantenimiento de los análisis de riesgos de la entidad o institución.

e) Definición y ejecución de los programas formativos y de concienciación relacionados con buenas prácticas de seguridad TIC, en el ámbito de institución.

f) Aplicación de los criterios y directrices de gestión de la seguridad TIC emanadas del Comité de Seguridad Interior y Seguridad TIC de la Institución, del CSISTIC-SAS, de la Unidad de Seguridad TIC del SAS, del Responsable de Seguridad TIC del SAS y del Delegado de Protección de Datos del SAS.

El CSISTIC-SAS, a propuesta del Responsable de Seguridad TIC del SAS, podrá designar a una de las personas Responsables de Seguridad TIC de las Instituciones, como responsable de dos o más instituciones en el ámbito territorial de la provincia donde desempeña su labor, adoptando el carácter de Responsable de Seguridad TIC en el ámbito territorial para el que sea designado.

Sus funciones y responsabilidades serán las establecidas en este apartado, para las Instituciones de su ámbito territorial y dependerá funcionalmente a todos los efectos del Responsable de Seguridad TIC del SAS.

Al menos, deberá existir un Responsable de Seguridad TIC de las Instituciones del SAS por cada una de las Áreas de Salud de la Comunidad Autónoma.

8.3. Unidad de Seguridad TIC del SAS.

La Unidad de Unidad de Seguridad TIC del SAS se desarrolla de acuerdo con el artículo 11 del Decreto 1/2011, modificado por el Decreto 70/2017, y de la disposición adicional segunda de este último.

A ella se le atribuyen las siguientes funciones:

a) Labores de soporte, asesoramiento e información al CSISTIC-SAS, así como de ejecución de las decisiones y acuerdos adoptados por éste.

b) Diseño y ejecución de los programas de actuación propios del SAS, incluyendo, entre otros, planes directores de seguridad, proyectos de desarrollo normativo, auditorías técnicas y de cumplimiento y planes de adecuación legal.

c) Definición, implantación y mantenimiento de los controles de carácter organizativo para la protección de la información, aplicaciones y sistemas, así como la realización y mantenimiento de los análisis de riesgos del SAS.

d) Supervisión sistemática de los controles de carácter procedimental, operacional y medidas técnicas de protección de la información, aplicaciones y sistemas del SAS.

e) Definición y supervisión de los criterios y requisitos técnicos de seguridad aplicados en las distintas fases del ciclo de vida de los soportes, sistemas y aplicaciones del SAS por parte de los Servicios o Departamentos responsables de la prestación de los servicios de tecnologías de la información y comunicaciones. Antes de la puesta en producción de nuevos sistemas de información o de evolutivos de los existentes, la Unidad de Seguridad TIC del SAS deberá evaluar los aspectos de seguridad y comunicar los posibles riesgos al centro o centros directivos responsables de la información y del servicio.

f) Definición y ejecución de los programas formativos y de concienciación relacionados con buenas prácticas de seguridad TIC en el ámbito del SAS.

g) Coordinación, dirección y seguimiento de la actividad en materia de seguridad TIC de las entidades vinculadas o dependientes del SAS.

00190161

h) Aplicación de los criterios y directrices de gestión de la seguridad TIC emanadas de la Unidad de Seguridad TIC Corporativa de la Junta de Andalucía.

i) Y cuantas otras le sean encomendadas por CSISTIC-SAS.

Al frente de la Unidad de Seguridad TIC del SAS estará la persona designada como Responsable de Seguridad TiC del SAS.

En cumplimiento del apartado 3 de la disposición adicional única del Decreto 70/2017, de 6 de junio, deberá procederse, en su caso, a realizar las reorganizaciones y reasignaciones de puestos que sean necesarias para que la Unidad de Seguridad TIC del SAS y la persona Responsable de Seguridad TIC del SAS dispongan de los perfiles profesionales necesarios y cumplan el principio de función diferenciada.

9. Datos de carácter personal.

Todo tratamiento de datos de carácter personal estará sometido al cumplimiento del Reglamento General de Protección de Datos y demás normativa de aplicación.

El responsable del tratamiento estará obligado al cumplimiento del principio de responsabilidad proactiva o de rendición de cuentas, entre otros, lo que supone cumplir con los requisitos de protección de datos más allá del estricto cumplimiento de la letra de la ley. Para ello proveerá de recursos al Delegado de Protección de Datos del SAS y a la Unidad de Seguridad TIC a fin de garantizar la «licitud, equidad y transparencia», «limitación de finalidad», «minimización de datos», «precisión», «limitación de almacenamiento» y «seguridad (disponibilidad, integridad y confidencialidad)».

El responsable del tratamiento ha de garantizar la definición, implantación, cumplimiento y monitorización, como mínimo, de las siguientes medidas:

a) El registro de actividades de tratamiento.

b) La protección de datos desde el diseño.

c) La protección de datos por defecto.

d) Las medidas de seguridad adecuadas al riesgo evaluado.

e) En su caso, las evaluaciones de impacto.

f) Las autorizaciones y/o consultas previas pertinentes a la autoridad de protección de datos.

g) En su caso, la designación formal del Delegado Protección de Datos (DPD).

h) El registro documental de las quiebras de seguridad TIC y en su caso, la notificación de éstas a quienes corresponda.

i) La suscripción a códigos de conducta y la solicitud de esquemas de certificación cuando proceda.

10. Conformidad con el Esquema Nacional de Seguridad.

De acuerdo con los capítulos II y III del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad, donde se recogen los principios básicos y los requisitos mínimos de seguridad, el Servicio Andaluz de Salud, implementará las medidas de seguridad proporcionalmente a la naturaleza de la información y a los servicios a proteger y teniendo en cuenta la categoría de los sistemas afectados.

El Servicio Andaluz de Salud, para lograr el cumplimiento de los artículos 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, que recogen los principios básicos y de los requisitos mínimos, implementará diversas medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger y teniendo en cuenta la categoría de los sistemas afectados.

10.1. Seguridad como un proceso integral y seguridad por defecto.

La seguridad constituye un proceso integrado por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad al Servicio Andaluz de Salud estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

00190161

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuente de riesgo para la seguridad.

Los sistemas se diseñarán de forma que garanticen la seguridad por defecto, del siguiente modo:

a) El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos.

b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.

c) En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés, sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.

d) El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

10.2. Evaluación periódica, integridad y actualización del sistema.

El Servicio Andaluz de Salud, implementará los controles y evaluaciones regulares de la seguridad, (incluyendo evaluaciones de los cambios de configuración de forma rutinaria), para conocer en todo momento el estado de la seguridad de los sistemas con relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos. Antes de la entrada de nuevos elementos, ya sean físicos o lógicos, estos requerirán de una autorización formal.

Así mismo, solicitará la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

10.3. Gestión de personal y profesionalidad.

Todo el personal del Servicio Andaluz de Salud y las Instituciones que se comprenden en el ámbito de aplicación de esta política, tiene la obligación de conocer y cumplir la presente Política de Seguridad TIC, así como la normativa de seguridad que emana de la misma siendo responsabilidad del Comité de CSISTIC-SA disponer los medios necesarios para su difusión.

Todo el personal relacionado con la información y los sistemas deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad. Sus actuaciones serán supervisadas para verificar que se siguen los procedimientos establecidos. Así mismo, ejercitará y aplicará los principios de seguridad en el desempeño de su cometido.

Por otra parte, y con carácter general, son de obligado cumplimiento las directrices recogidas en las políticas de seguridad TIC, normas, procedimientos y manuales de comportamiento elaborados por la Administración de la Junta de Andalucía o cualquiera de sus Consejerías con competencias al respecto. Estas normas de seguridad establecen y concretan el significado y alcance del uso seguro de los sistemas.

Para corregir, o exigir responsabilidades en su caso, cada usuario que acceda a la información del sistema debe estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado determinada actividad.

El incumplimiento de esta política de seguridad TIC podrá suponer el inicio de las medidas disciplinarias que procedan, sin perjuicio de las responsabilidades legales que correspondan.

La seguridad de los sistemas del Servicio Andaluz de Salud 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.

00190161

El Servicio Andaluz de Salud exigirá, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con unos niveles idóneos de gestión y madurez en los servicios prestados.

10.4. Gestión de la seguridad basada en los riesgos y análisis y gestión de riesgos.

Todos los activos serán objeto de un análisis de riesgos, con revisión y aprobación anual. Para su desarrollo se aplicarán los criterios, metodologías y herramientas definidas para las administraciones públicas, de acuerdo con el ENS y los requerimientos de análisis de impacto de privacidad recogidos en el Reglamento 679/2016 de la Unión Europea y las recomendaciones realizadas por la autoridad de control.

Los análisis de riesgos se actualizarán en caso de que se identifiquen nuevos activos, o cambien los existentes, o sus requisitos de seguridad, se identifiquen cambios en relación con los servicios prestados u ocurra un incidente grave de seguridad, o se identifiquen o reporten vulnerabilidades de seguridad graves en los sistemas existentes.

Por otra parte, se llevará a cabo una adecuada gestión de los riesgos, por lo que las decisiones sobre las medidas, proyectos e iniciativas de seguridad a realizar contemplarán los resultados de la evaluación de los riesgos existentes en relación con la seguridad TIC sobre los sistemas utilizados.

Los resultados de los análisis de riesgos serán elevados al correspondiente Comité por la persona que ejerza labores de Responsable de Seguridad TIC con competencias sobre los activos afectados.

10.5. Incidentes de seguridad, prevención, reacción y recuperación.

Se establecerá un sistema de detección y reacción frente a código dañino y se registrarán los incidentes de seguridad que se produzcan y las acciones de tratamiento que se sigan. Estos registros se emplearán para la mejora continua de la seguridad del sistema.

Debe evitarse, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. El Reglamento General de Protección de Datos, en su artículo 32, establece medidas de seguridad relacionadas con la gestión de incidentes con el objeto de disponer de la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida. Igualmente, el artículo 7 del ENS recoge la necesidad de prevenir, detectar, reaccionar y recuperarse de incidentes:

1. Prevención: se deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Dichos controles, los perfiles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados. Por otra parte, para garantizar el cumplimiento de la política, es necesaria la autorización de los sistemas antes de entrar en operación y la evaluación y revisión periódica de la seguridad.

2. Detección: La operación de los servicios debe ser monitorizada de forma continua para detectar anomalías en los niveles de prestación de los mismos y poder actuar en consecuencia según lo establecido en el artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

3. Respuesta: Se deben establecer mecanismos para responder eficazmente a los incidentes de seguridad, así como designar un punto de contacto. Igualmente, deben establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con otros equipos de respuesta a incidente.

4. Recuperación: Para garantizar la disponibilidad de los servicios críticos, los servicios deben desarrollar planes de continuidad de los sistemas como parte de su plan general de continuidad de negocio y actividades de recuperación.

00190161

En caso de violación de la seguridad de los datos personales, las notificaciones a la autoridad de control y las comunicaciones al interesado se llevarán a cabo conforme a los artículos 33 y 34 del Reglamento General de Protección de Datos.

A estos efectos, la Unidad de Seguridad TIC del SAS realizará las auditorías periódicas de seguridad (prevención), el seguimiento y control del estado de seguridad de los sistemas y servicios (detección), la coordinación de la respuesta eficaz a los incidentes de seguridad desde su notificación hasta su resolución (respuesta) y el desarrollo de los planes de continuidad de los sistemas de información (recuperación).

10.6. Líneas de defensa y prevención ante otros sistemas interconectados.

El Servicio Andaluz de Salud implementará una estrategia de protección basada en múltiples capas, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una de las capas falle, el sistema implementado permita:

- Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.
- Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
- Minimizar el impacto final sobre el mismo.

Esta estrategia de protección ha de proteger el perímetro, en particular, si se conecta a redes públicas. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

10.7. Función diferenciada y organización e implantación del proceso de seguridad

El Servicio Andaluz de Salud, ha organizado su seguridad comprometiendo a todos los miembros de la organización mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en el apartado de «Organización de la Seguridad TIC» del presente documento.

10.8. Autorización y control de los accesos.

El acceso a los sistemas de información del Servicio Andaluz de Salud será controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.

10.9. Protección de las Instalaciones.

Los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas. Como mínimo, las salas estarán cerradas y se dispondrá de un control de llaves.

10.10. Adquisición de productos de seguridad y contratación de servicios de seguridad.

Para la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones que vayan a ser utilizados por el Servicio Andaluz de Salud se valorarán positivamente aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen, a juicio del responsable de Seguridad. Las mencionadas certificaciones deberán estar de acuerdo con las normas y estándares de mayor reconocimiento internacional, en el ámbito de la seguridad funcional.

10.11. Protección de la información almacenada y en tránsito y continuidad de la actividad

El Servicio Andaluz de Salud implementará los mecanismos para proteger la información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los equipos portátiles, asistentes personales (PDA), dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.

00190161

Forman parte de la seguridad los procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos por el Servicio Andaluz de Salud en el ámbito de sus competencias.

Se desarrollarán procedimientos para asegurar la recuperación y conservación a largo plazo de los documentos electrónicos producidos en el ámbito de las competencias del Servicio Andaluz de Salud. De igual modo, se implementarán los mecanismos de seguridad en base a la naturaleza del soporte en el que se encuentren los documentos, para garantizar que toda información relacionada en soporte no electrónico esté protegida con el mismo grado de seguridad que la electrónica.

Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

Se dispondrá de un plan para mantener la continuidad de los procesos y sistemas críticos y garantizar su recuperación en caso de desastre. La finalidad de este plan es reducir el tiempo de indisponibilidad a niveles aceptables mediante la combinación de controles de carácter organizativo, tecnológico y procedimental tanto preventivos como de recuperación.

10.12. Registros de actividad.

El Servicio Andaluz de Salud habilitará los registros de la actividad 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. Todo ello con la finalidad exclusiva de lograr el cumplimiento del objeto del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional seguridad en el ámbito de la Administración Electrónica, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación.

10.13. 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 gestión de las tecnologías de la información.

11. Categorización de los sistemas de información e inventariado de activos.

La categorización de los sistemas de información y el inventario de activos se hará de conformidad con el capítulo X del ENS.

Los activos se encontrarán inventariados, con un responsable asociado y se encontrarán actualizados para asegurar su validez.

El CSISTIC-SAS, en base a las funciones de la organización, su capacidad para cumplir los fines encomendados, sus activos y las personas afectadas, elaborará unos criterios de valoración a fin de facilitar esta labor a los responsables correspondientes.

12. Desarrollo normativo de la seguridad TIC.

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos y estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

El marco normativo sobre seguridad TIC es de obligado cumplimiento y se desarrollará en niveles, según el ámbito de aplicación y nivel de detalle técnico, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Dichos niveles de desarrollo son los siguientes:

1. Primer nivel normativo: política de seguridad TIC y las estrategias de seguridad del SAS y las propias de las entidades o instituciones. La política de seguridad está constituida por la presente norma, siendo de obligado cumplimiento. Las estrategias de

00190161

seguridad TIC serán aprobadas por los Comités competentes en materia de Seguridad TIC.

2. Segundo nivel normativo: normas y planes de seguridad TIC. Está constituido por el conjunto de normas y planes que desarrollan la política de seguridad y que regulan qué se puede hacer y qué no, en relación con un cierto tema, desde el punto de vista de la seguridad sin entrar en detalles de implementación ni tecnológicos. Los documentos relativos a este segundo nivel normativo los propone el Responsable de Seguridad TIC del SAS y los aprueba el CSISTIC-SAS.

3. Tercer nivel normativo: procedimientos técnicos. Está constituido por el conjunto de procedimientos técnicos que dan respuesta, incluyendo detalles de implementación y tecnológicos, a cómo se puede realizar una determinada tarea respetando los principios de seguridad de la organización y los procesos internos en ella establecidos. La responsabilidad de aprobación de estos procedimientos técnicos dependerá de su ámbito de aplicación, que podrá ser en un ámbito específico o en un sistema de información determinado.

Aparte de los documentos citados, la documentación de seguridad podrá contar, con otros documentos como recomendaciones, buenas prácticas, informes, registros, evidencias electrónicas, etc.

El CSISTIC-SAS establecerá los mecanismos necesarios para normalizar y compartir la documentación derivada del desarrollo normativo.

13. Concienciación y formación.

Uno de los objetivos de la Seguridad TIC en el SAS es lograr la plena conciencia de que la seguridad TIC afecta a todo el personal y a todas las actividades, de acuerdo con el principio de Seguridad Integral recogido en el artículo 5 del ENS. Por tanto, se deberán articular los medios necesarios para que todas las personas que intervienen en los procesos y sus responsables jerárquicos tengan sensibilidad hacia los riesgos existentes.

En el marco de la responsabilidad proactiva del responsable del tratamiento se encuentra la obligación de dar a conocer las políticas y procedimientos existentes sobre protección de datos a todo el personal involucrado en los procesos relevantes. Esto puede garantizarse a través de propuestas de formación obligatoria, provisión de material informativo o capacitación recurrente, coordinadas por el Delegado de Protección de Datos del SAS.

Por tanto, se establecerá un programa de concienciación y formación continua en materia de seguridad TIC, con actividades anuales, destinado a los profesionales del SAS, y en particular a los de nueva incorporación.

Las personas que realicen actividades especialmente relacionadas con la gestión y operación de la seguridad TIC tienen que recibir las acciones formativas necesarias en esta materia.

14. Cooperación con otros órganos y otras administraciones en materia de seguridad TIC.

A efectos de coordinación, obtención de asesoramiento e intercambio de experiencias para la mejora continua de la gestión de la seguridad TIC, se fomentará el establecimiento de mecanismos de comunicación con otros agentes especializados en esta materia. En especial, se contemplarán los siguientes:

a) Comité de Seguridad TIC de la Junta de Andalucía.

b) Unidad de Seguridad TIC de la Junta de Andalucía.

c) Andalucía-CERT: Centro experto para la gestión de la seguridad TIC de la Junta de Andalucía.

d) Consejo de Transparencia y Protección de Datos de Andalucía

00190161

e) CCN-CERT: Capacidad de Respuesta a Incidentes de Seguridad TIC del Centro Criptológico Nacional (CCN), como soporte y coordinación para la resolución de incidentes que sufran las entidades e instituciones que conforman el SAS.

f) Agencia Española de Protección de Datos (AEPD).

15. Resolución de conflictos.

En caso de conflicto entre los responsables que componen la estructura organizativa definida para la gestión de la seguridad TIC, lo resolverá su superior jerárquico; en su ausencia, prevalece la decisión del CSISTIC-SAS.

En todo caso ha de prevalecer la decisión que implique el nivel más alto de protección.

16. Terceras partes.

Cuando se empleen servicios de terceros o se ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información para su cumplimiento. Dicha tercera parte podrá desarrollar sus propios procedimientos operativos para satisfacer el marco normativo. Se establecerán procedimientos específicos de comunicación y resolución de incidencias. La tercera parte garantizará que su personal esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en el párrafo anterior, se solicitará un informe a la persona Responsable de Seguridad TIC del tercero que precise los riesgos en que se incurre y la forma de tratarlos. Dependiendo del alcance, el informe será valorado por la persona Responsable de Seguridad TIC del SAS o de las instituciones, previo a su remisión a los responsables de la información y los servicios afectados para su aprobación.

Las contrataciones y acuerdos de nivel de servicio que se establezcan con terceros incluirán cláusulas y garantías de cumplimiento de los requisitos de seguridad.

Cuando se presten servicios a terceros o actúe como cesionario manejando información de terceros, se les hará partícipe de esta Política de Seguridad TIC, estableciéndose canales para la comunicación y coordinación de los respectivos Comités de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

17. Auditoría.

Los sistemas de información se auditarán de forma periódica. Los sistemas de información corporativos, así como los sistemas de información propios de las entidades e instituciones, serán objeto, al menos cada dos años, de una auditoría regular ordinaria interna o externa que verifique el cumplimiento de los requerimientos del ENS, del RGPD y cualquier otra norma que requiera la realización de auditorías periódicas. Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad requeridas.

La persona Responsable de Seguridad TIC con competencias sobre los activos auditados deberá analizar dicho informe y elevarlo junto con sus conclusiones a la persona Responsable de los Sistemas y Tecnologías del SAS, a las personas Responsables de la Información / Tratamientos de datos y a los Comités de Seguridad TIC correspondientes, para que se adopten las medidas correctoras adecuadas.

Los contratos de prestación de servicios establecidos con terceros contendrán la posibilidad de verificación de su cumplimiento a través de auditorías de seguridad TIC.

18. Actualización de la política de seguridad TIC.

El CSISTIC_SAS revisará bianualmente esta Política de Seguridad TIC y realizará la propuesta de revisión o mantenimiento de esta. La Política será aprobada por el Director Gerente del SAS y difundida para que la conozcan todas las partes afectadas.

00190161