SERVICIO EXTREMEÑO DE SALUD

RESOLUCIÓN de 14 de junio de 2021, de la Dirección Gerencia, por la que se aprueba la política de privacidad y seguridad de la información del Servicio Extremeño de Salud. (2021061888)

La Junta de Extremadura tiene como misión servir con objetividad a los intereses generales y procurar satisfacer, con eficacia y eficiencia, las necesidades públicas, de conformidad con los principios constitucionales y estatutarios, para beneficio de la ciudadanía.

En el Estatuto de la Comunidad Autónoma de Extremadura, en la redacción dada por la Ley Orgánica 1/2011, de 28 de enero, se impone, entre otros, "facilitar el acceso a las nuevas tecnologías de la información y comunicación a los ciudadanos y empresas" (artículo 7), ajustar su actuación a "los principios de buena fe, confianza legítima, transparencia, calidad en el servicio a los ciudadanos" (artículo 37.2) y como medida de buena administración "regular los procedimientos administrativos propios y adaptar los procedimientos generales para dar celeridad y transparencia a la tramitación administrativa, para extender las relaciones interadministrativas y con los ciudadanos por medios telemáticos y para la simplificación de trámites"(artículo 39.2).

De acuerdo con ello, la Ley 4/2013, de 21 de mayo, de Gobierno Abierto de Extremadura, previene que la buena administración y el buen gobierno administrativo deberán ser informados por los principios previstos en la normativa básica del estado y otros tales como la modernización, accesibilidad y prevención dirigidos a impulsar el proceso de transformación digital de la Administración pública.

Dichas previsiones deben ser contextualizadas en el nuevo marco de actuación del sector público definido por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que imponen el funcionamiento de las Administraciones Públicas por medios electrónicos, para satisfacción de la ciudadanía preservando la protección de datos de carácter personal y, en particular, la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones que dispongan para prestar servicios públicos.

En relación con este ámbito, el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica, modificado parcialmente por el Real Decreto 951/2015, de 23 de octubre, establece la necesidad que todos los órganos superiores de las Administraciones Públicas dispongan formalmente de una política de seguridad que cumpla los principios básicos y requisitos mínimos que precisa para procurar una protección adecuada de la información y requiere así como la necesidad de que se apruebe por el titular del órgano superior.

A nivel autonómico, el Decreto 225/2014, de 14 de octubre, de régimen jurídico de administración electrónica de la Comunidad Autónoma de Extremadura, cuyo ámbito de aplicación se extiende a la Administración de la Comunidad Autónoma, los organismos públicos vinculados o dependientes de la misma sujetos a derecho público y los restantes organismos cuando ejerzan potestades públicas, a la ciudadanía y a las relaciones con otras Administraciones Públicas establece en su disposición adicional séptima que el Consejo de Gobierno establecerá una Política de Seguridad de la Información, "donde se marcarán las directrices de la Administración para garantizar el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias". "La Política de Privacidad y Seguridad de la Información será reglamentariamente desarrollada por la Consejería competente en materia de administración electrónica, a través del órgano directivo competente conforme al apartado tercero de la disposición adicional séptima del Decreto 225/2014".

En su virtud, con fecha 26 de junio de 2018 se adoptó Acuerdo del Consejo de Gobierno de la Junta de Extremadura por el que se establece la política de privacidad y seguridad de la información de la Administración de la Comunidad Autónoma de Extremadura (DOE n.º 132, 9 de julio de 2018) que en su alcance señala que "Los Organismos Públicos estarán sujetos a la Política en todos sus términos y condiciones de acuerdo con las instrucciones, indicaciones de los órganos superiores de las Consejerías a las que están adscritas a excepción del Servicio Extremeño de Salud, que en atención a sus especiales funciones y singularidades respecto a su organización y funcionamiento, deberá establecer su propia Política de Privacidad y Seguridad de la Información alineados con los principios y requisitos mínimos de esta política"

En este sentido nace la obligación de establecer la Política de Privacidad y Seguridad de la Información del Servicio Extremeño de Salud que define las directrices para garantizar la integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad de los datos que dispone, conserva y obtiene en la prestación de los servicios de interés público para preservar e incrementar la confianza de la ciudadanía.

Dicha Política debe ser coherente con la Estrategia de Ciberseguridad de la Unión Europea, con las exigencias del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), que sienta las bases de una normativa de privacidad, en el auge de la economía digital, para garantía de los derechos de la ciudadanía y con las de las Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Así, el Real Decreto 3/2010 regulador del Esquema Nacional de Seguridad, en su anexo II, sección 3.1 precisa que "la política de seguridad se plasmará en un documento escrito, en el

que, de forma clara, se precise, al menos, lo siguiente: a) Los objetivos o misión de la organización; b) El marco legal y regulatorio en el que se desarrollarán las actividades; c) Los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación; d) La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización; y e) Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso".

La disposición adicional séptima del Decreto 225/2014 indica en su apartado segundo "la Política de Seguridad de la Información de la Comunidad Autónoma de Extremadura cumplirá los principios básicos y los requerimientos mínimos recogidos en Real Decreto 3/2010, de 8 de enero, por el que se regula el esquema nacional de seguridad".

Con estas premisas, la Política que sea de aplicación necesariamente tiene que cumplir con el contenido prescrito en el Esquema Nacional de Seguridad, que además de lo indicado en el anexo II ya enunciado, en su artículo 10 configura la seguridad como función diferenciada en la que se contemplan varios roles posibles, debiendo detallar la correspondiente política de la seguridad las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos, exigiendo el artículo 11 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.

Por todo ello, el documento ha sido elaborado cumpliendo dichos requerimientos sin incorporar al ordenamiento organizativo otras funciones o responsabilidades de las definidas por la Ley 1/2002, de Gobierno de la Comunidad Autónoma de Extremadura y por el Decreto 221 /2008, de 24 de octubre, por el que se aprueban los estatutos del Organismo Autónomo Servicio extremeño de Salud (DOE n.º 210, de 30 de octubre).

El alcance de la política se extiende de las previsiones y requisitos del Esquema Nacional de Seguridad a la normativa de protección de datos bajo la consideración que esta última forma parte de la seguridad de la información, lo que se desprende de la inclusión de ambas materias en el derecho de la ciudadanía a que refiere el artículo 13 h) de la Ley 39/2015, de 1 de octubre.

De acuerdo con ello, los principios, requisitos mínimos y otras referencias contenidas en la Política de Privacidad y Seguridad de la información se han elaborado considerando el conjunto de normas de dichos ámbitos normativos. En particular se han considerado las Guías CCN-STIC de Seguridad, que constituyen un cuerpo de normas, instrucciones, guías y recomendaciones desarrolladas por el Centro Criptológico Nacional, perteneciente al Centro Nacional de Inteligencia, con el fin de mejorar el grado de ciberseguridad de las organizaciones (CCN-STIC-805 Política de Seguridad de la Información, CCN-STIC-830 Ámbito de aplicación

del Esquema Nacional de Seguridad, CNN-STIC-800 Glosario de términos y abreviaturas del ENS, CCN-STIC-801 Responsabilidades y Funciones en el ENS).

En este sentido, se ha propuesto describir las directrices con un lenguaje sencillo y simplificado evitando en la medida de lo posible los tecnicismos para facilitar su entendimiento por toda la organización. Por todo ello, se estima que el contenido de la Política cumple sobradamente con el contenido legalmente impuesto.

De acuerdo con ello, la propuesta organizativa incluida en la política se realiza de conformidad con los mandatos de la normativa superior (sometida a los trámites de información) consistiendo en una simple contextualización de dichas previsiones en la estructura organizativa del Servicio Extremeño de Salud considerando lo que se precisa en los Estatutos del Organismo Autónomo, Servicio Extremeño de Salud, aprobados por el Decreto 221/2008, de 24 de octubre (DOE n.º 210, de 30 de octubre) respecto a las funciones y responsabilidades que deben asumir los respectivos órganos.

El Real Decreto 3/2010 regulador del Esquema Nacional de Seguridad, en su anexo II, sección 3.1 precisa que "la política de Seguridad será aprobada por el órgano superior competente que corresponda".

En su virtud, esta Dirección Gerencia en uso de las atribuciones conferidas en el artículo 4, apartado v), de los Estatutos del Organismo Autónomo, Servicio Extremeño de Salud, aprobados por el Decreto 221/2008, de 24 de octubre (DOE n.º 210, de 30 de octubre),

RESUELVE:

Primero. Establecer la Política de privacidad y seguridad de la información del Servicio Extremeño de Salud, que se incorpora como anexo.

Segundo. Disponer su publicación en el Diario Oficial de Extremadura.

Mérida, 14 de junio de 2021.

El Director Gerente,

CECILIANO FRANCO RUBIO

SERVICIO EXTREMEÑO DE SALUD

CONSEJERÍA DE SANIDAD Y SERVICIOS SOCIALES

POLÍTICA DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN DEL SERVICIO EXTREMEÑO DE SALUD

ADMINISTRACIÓN DE LA COMUNIDAD AUTÓNOMA DE EXTREMADURA

Política de Privacidad y Seguridad de la Información del Servicio Extremeño de Salud

El Servicio Extremeño de Salud es un ente público de carácter autónomo, adscrito a la Consejería de Sanidad y Servicios Sociales de la Junta de Extremadura, dotado de personalidad jurídica y patrimonio propios, con plena capacidad de obrar para el cumplimiento de sus fines, al que se confía la gestión de los servicios públicos sanitarios de carácter asistencial.

De conformidad con la Ley 10/2001, de 28 de junio, de Salud de Extremadura los objetivos fundamentales del Servicio de Extremeño de Salud consisten en participar en la definición de las prioridades de la atención sanitaria a partir de las necesidades de salud de la población y dar efectividad al catálogo de prestaciones y servicios que se pone al servicio de la población con la finalidad de proteger la salud; distribuir de manera óptima los medios económicos asignados a la financiación de los servicios y de las prestaciones sanitarias; garantizar que las prestaciones se gestionen de manera eficiente; garantizar, evaluar y mejorar la calidad del servicio al ciudadano, tanto en la asistencia como en el trato; promover la participación de los profesionales en la gestión del sistema sanitario extremeño y fomentar la motivación profesional, y promover la formación, la docencia y la investigación en el ámbito de la salud.

Hay que considerar que la información que recaba y gestiona el Servicio Extremeño de Salud en el ejercicio de sus competencias constituye un activo esencial para cumplir adecuadamente los objetivos reseñados, y que el funcionamiento correcto de los sistemas de información que albergan y gestionan dichos datos es imprescindible para el ejercicio adecuado, eficaz y

eficiente de las obligaciones atribuidas en materia de asistencia y de gestión sanitaria. Por tanto, asume la responsabilidad asociada a la protección de esos datos frente a las amenazas que puedan afectar a su seguridad.

Los beneficios de la implantación de las tecnologías de la información en los entornos sanitarios son más que evidentes, pues facilitan la prestación de servicios sanitarios con coherencia y cohesión desde los distintos niveles asistenciales, en especial en un ámbito geográfico caracterizado por su dispersión, lo cual no hace sino potenciar aún más los beneficios de estas tecnologías. No obstante, en este entorno la seguridad de la información es claramente un imperativo, pues la información gestionada en este ámbito está sometida a unos requisitos de seguridad muy exigentes.

En relación con este ámbito, el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica, modificado parcialmente por el Real Decreto 951/2015, de 23 de octubre, establece la necesidad de que todos los órganos superiores de las Administraciones Públicas dispongan formalmente de una política de seguridad que cumpla los principios básicos y requisitos mínimos que precisa para procurar una protección adecuada de la información y requiere la necesidad de que se apruebe por el titular del órgano superior.

En desarrollo de lo anterior, el anexo II precisa que "la política de seguridad se plasmará en un documento escrito, en el que, de forma clara, se precise, al menos, lo siguiente:

— Los objetivos o misión de la organización;

— El marco legal y regulatorio en el que se desarrollarán las actividades;

— Los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.

— La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización.

— Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso".

A nivel autonómico, el Decreto 225/2014, de 14 de octubre, de régimen jurídico de administración electrónica de la Comunidad Autónoma de Extremadura, cuyo ámbito de aplicación se extiende a la Administración de la Comunidad Autónoma, los organismos públicos vinculados o dependientes de la misma sujeto a derecho público y los restantes organismos cuando

ejerzan potestades públicas, a la ciudadanía y a las relaciones con otras Administraciones Públicas establece en su Disposición Adicional Séptima que "el Consejo de Gobierno establecerá una Política de Seguridad de la Información, "donde se marcarán las directrices de la Administración para garantizar el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias".

Dicha Política debe ser coherente con la Estrategia de Ciberseguridad de la Unión Europea y las exigencias del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), que sienta las bases de una normativa de privacidad, en el auge de la economía digital, para garantía de los derechos de la ciudadanía y que se transponen en la Ley 3/2018.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Sustituye a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. BOE de 14 de diciembre de 1999 y a su Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. BOE de 19 de enero de 2008.

Adicionalmente la Política de Privacidad y Seguridad de la Información del Servicio Extremeño de Salud está alineada con la Política de Privacidad y Seguridad de la Información de la Comunidad Autónoma de Extremadura, publicada en el DOE n.º 132 del 9 de Julio de 2018 (Resolución de 3 de julio de 2018, de la Vicepresidenta y Consejera, por la que se ordena la publicación en el Diario Oficial de Extremadura del Acuerdo del Consejo de Gobierno de la Junta de Extremadura de 26 de junio de 2018 por el que se establece la política de privacidad y seguridad de la información de la Administración de la Comunidad Autónoma de Extremadura), que define las directrices de la Administración para garantizar la integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad de los datos que dispone, conserva y obtiene en la prestación de los servicios de interés público para preservar e incrementar la confianza de la ciudadanía.

1. Misión, Objetivos, Objeto y Alcance

1.1. Misión

1.2. Objetivos

1.3. Objeto

7. Protección de datos de carácter personal

7.1. Registro de actividades de tratamiento

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

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

8. Análisis de Riesgos de Seguridad de la Información

9. Revisión y auditoría

10. Medidas de Seguridad

11. Revisión de la Política

12. Relación con Terceras Partes

13. Resolución de Conflictos

14. Personal del Servicio Extremeño de Salud

1. Misión, Objetivos, Objeto y Alcance

1.1. Misión

El Servicio Extremeño de Salud, en adelante SES, tiene como misión servir con objetividad a los intereses generales y procurar satisfacer, con eficacia y eficiencia, las necesidades sanitarias, públicas, de conformidad con los principios constitucionales y estatutarios, respetando los principios de buena fe, confianza legítima, transparencia, seguridad y calidad en el servicio a los ciudadanos y a las organizaciones.

A efectos de esta Política, el Servicio Extremeño de Salud tiene por misión mantener unos adecuados niveles de seguridad y protección frente a amenazas a la información que gestiona, que es el activo fundamental para cumplir sus objetivos.

1.2. Objetivos

El Servicio Extremeño de Salud asume los siguientes objetivos en materia de seguridad de la información:

1) Establecer las pautas necesarias para garantizar en todo momento la seguridad de la información a través de directrices con objeto de preservar, proteger y consolidar la seguridad de los servicios y los activos de información con el objetivo de mejorar la calidad de los servicios que se prestan a los ciudadanos.

2) Garantizar la implantación de las medidas y de los mecanismos de seguridad apropiados para proteger los servicios prestados, los sistemas de información utilizados para prestarlos y la información procesada, almacenada o transmitida por éstos, de manera coherente con los riesgos afrontados.

3) Asegurar que se cumpla la normativa vigente en materia de seguridad y protección de datos a las que el Servicio Extremeño de Salud deba someterse.

4) Garantizar la eficacia de las medidas de seguridad implantadas por medio de evaluaciones y auditorías.

5) Establecer una estructura organizativa adecuada para la gestión de la seguridad de la información definiendo los roles y los comités necesarios, además de las funciones y las respectivas responsabilidades.

6) Garantizar la operación continuada y adecuada de los servicios y de los sistemas actuando para prevenir, detectar, reaccionar y operar de manera oportuna ante los incidentes de seguridad que se produzcan, y velar por la implantación de los mecanismos

necesarios que aseguren la continuidad de las actividades críticas permitiendo que éstas se recuperen en un periodo de tiempo aceptable.

7) Impulsar y fomentar la formación, la concienciación y el cumplimento de las obligaciones en materia de seguridad de la información del personal al servicio de la organización, a fin de garantizar el conocimiento de las políticas y las normativas aprobadas y de las prácticas recomendadas, con el objetivo último de lograr que la seguridad de la información se convierta en un factor inherente al desarrollo de las funciones y de las operativas cotidianas.

8) Promover que las actividades destinadas a lograr los niveles de seguridad requeridos se estructuren y se conciban como un proceso de mejora continua, y no como acciones o esfuerzos puntuales, sustentándolo en el análisis y la gestión sistematizados de los riesgos.

1.3. Objeto

La Política de Privacidad y Seguridad de la Información, en adelante PPSI, establece el marco de referencia y las directrices para asegurar la integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones utilizadas y servicios prestados, en especial cuando se traten datos de carácter personal, que gestiona el SES en el ejercicio de sus competencias.

1.4. Alcance

La PPSI se aplicará a los órganos del SES y a los organismos y entes públicos que utilicen los sistemas de información y/o de comunicaciones dependientes del SES.

La PPSI del Servicio Extremeño de Salud es aplicable con carácter obligatorio a todas las unidades administrativas y a todos los órganos del Servicio Extremeño de Salud, y también a los entes que —en su caso— estén adscritos a éste, por lo que debe observarla todo el personal que preste servicio en ellos.

Asimismo, es aplicable a los centros privados que estén incorporados al sistema sanitario público de Extremadura por medio de acuerdos, convenios u otras fórmulas de gestión integrada o compartida y debe ser observada por su personal.

Deberá de ser observada por todo el personal de los órganos y organismos citados. La política de privacidad y seguridad de la información también es aplicable y de obligado cumplimiento para las personas que, aunque no presten servicio directamente en el Servicio Extremeño de Salud o en algún ente adscrito a éste, tengan acceso a la información o a los sistemas que gestionan dicha información.

Será de aplicación sobre todos aquellos sistemas de información y a todas las actividades de tratamiento de datos de carácter personal de los que sea responsable, en especial aquellos relacionados con el ejercicio de derechos por medios electrónicos de la ciudadanía o empleados públicos, con el cumplimiento de deberes por medios electrónicos o con el acceso a la información o al procedimiento administrativo.

Los Organismos Públicos dependientes y/o órganos del SES estarán sujetos a la PPSI en todos sus términos y condiciones de acuerdo con las instrucciones e indicaciones de los órganos superiores a los que estén adscritos.

La PPSI se aplicará a todos los sistemas de información y a todas las actividades de tratamiento de datos de carácter personal de los que sea responsable en el ámbito descrito.

2. Definiciones

A los efectos de la política de privacidad y seguridad de la información del Servicio Extremeño de Salud, son aplicables las definiciones que establece el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica. Asimismo, se definen los siguientes conceptos como más destacados:

a) Responsable de la información: persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.

b) Responsable de la seguridad de la información: persona que determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

c) Responsable del servicio: persona que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.

d) Responsable del sistema: persona que se encarga de la explotación del sistema de información.

3. Acrónimos

— SES: Servicio Extremeño de Salud

— ACAEx: Administración de la Comunidad Autónoma de Extremadura.

— CGCSI: Comité de Gestión y Coordinación de la Seguridad de la Información.

— USIPD: Unidad de Seguridad de la Información y Protección de Datos

— OTSI: Oficina Técnica de Seguridad de la Información

— ENS: Esquema Nacional de Seguridad (Real Decreto: 3/2010).

— PPSI: Política de Privacidad y Seguridad de la Información.

— RGPD: Reglamento General de Protección de Datos (Reglamento (UE) 2016/679).

— RJAE: Régimen Jurídico de Administración Electrónica. (Decreto 225/2014).

— TIC: Tecnologías de la Información y las Comunicaciones.

— SGSI: Sistema de Gestión de Seguridad de la Información.

— CCN: Centro Criptológico Nacional

— CERT: Computer Emergency Reaction Team

— STIC: Seguridad TIC

— LGACAEX: Ley de Gobierno y Administración de la Comunidad Autónoma de Extremadura.

— ENS: Esquema Nacional de Seguridad (Real Decreto 3/2010)

4. Marco Regulador de la Seguridad de la Información

Dada la diversidad de las competencias y funciones del SES, la amplitud de los temas que afectan a la Seguridad de la Información y su rápida evolución, se debe desarrollar un Marco Regulador de la Seguridad de la Información, que se compondrá de:

a) Marco Normativo - Legislativo aplicable en materia de Seguridad de la Información.

b) La estrategia y la Política de Privacidad y Seguridad de la Información.

c) Documentos técnicos de desarrollo de la Política de Privacidad y Seguridad de la Información.

d) Disposiciones y resoluciones de los órganos competentes del presente acuerdo, cuyo ámbito afecte a la Privacidad y Seguridad de la Información.

4.1. Marco Legal y Normativo

4.1.1. Legislación

De forma general forman parte del marco normativo las normas de ámbito autonómico, estatal y europeo que afecte a la gestión de la Privacidad y Seguridad de la Información.

De forma específica, se toma como marco normativo de referencia, para el desarrollo de la PPSI, la siguiente normativa legal:

A nivel europeo:

Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de Julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión. (Directiva NIS)

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), que es aplicable a partir del 25 de mayo de 2018.

Reglamento Delegado (UE) núm.907/2014 de la Comisión de 11 de marzo de 2014 que completa el Reglamento (UE) núm.1306/2013 del Parlamento Europeo y del Consejo en lo relativo a los organismos pagadores y otros órganos, la gestión financiera, la liquidación de cuentas, las garantías y el uso del euro, en el anexo I apartado 3 B) ii) dice textualmente "A partir del 16 de octubre de 2016, la seguridad de los sistemas de información deberá estar certificada de conformidad con la norma ISO/IEC 27001: Information Security management systems Requeriments (ISO) (Sistema de gestión de la Seguridad de la Información-Requisitos) (ISO)".

A nivel estatal:

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

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 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Real Decreto-ley 12/2018, de 7 de septiembre, de Seguridad de las Redes y Sistemas de Información (Ley NIS)

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. (Reglamento NIS)

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

Real Decreto 951/2015, de 23 de octubre, de modificación 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.

A nivel autonómico:

Ley 1/2002, de 28 de febrero, del Gobierno y de la Administración de la Comunidad Autónoma de Extremadura, en adelante LGACAEx.

Ley 4/2013, de 21 de mayo, de Gobierno Abierto de Extremadura.

Decreto 225/2014, de 14 de octubre, de régimen jurídico de Administración Electrónica de la Comunidad Autónoma de Extremadura, en adelante RJAE.

A nivel sanitario:

Ley 10/2001, de 28 de junio, de Salud de Extremadura.

Ley 1/2005, de 24 de junio, de tiempos de respuesta en la atención sanitaria especializada del Sistema Sanitario Público de Extremadura.

Ley 3/2005, de 8 de julio, de información sanitaria y autonomía del paciente

Ley 6/2006, de 9 de noviembre, de Farmacia de Extremadura.

Ley 7/2011, de 23 de marzo, de Salud Pública de Extremadura.

Aparte de estas disposiciones legales y, en cualquier caso, el Servicio Extremeño de Salud —en materia de política de privacidad y seguridad de la información— actuará con estricto cumplimiento de la legalidad vigente.

4.2. Estrategia de Privacidad y Seguridad de la Información

La dirección del Servicio Extremeño de Salud, su Consejo de Gobierno, establecerá, la estrategia de Privacidad y Seguridad de la Información del Organismo, estableciendo las condiciones necesarias de confianza en la ciudadanía para el ejercicio de sus derechos y cumplimiento de las obligaciones.

4.3. Política de Privacidad y Seguridad de la Información

El presente documento define la Política de Privacidad y Seguridad de la Información que será aprobada conforme a los criterios del punto "6 Organización de la Seguridad

de la Información en el Servicio Extremeño de Salud" y revisada conforme al punto "10. Revisión de la política".

4.4. Documentos Técnicos de Desarrollo

La documentación técnica de desarrollo se estructura jerárquicamente en los siguientes niveles:

a) Nivel 1: Políticas y planes específicos

b) Nivel 2: Normativas de Privacidad y Seguridad de la Información

c) Nivel 3: Procedimientos y guías técnicas

Cada documento técnico, de un nivel determinado, debe estar fundamentado en documentación de nivel superior.

Nivel 1: Políticas y planes específicos

A Nivel estratégico, en el que se incluyen las directrices emitidas por la normativa vigente y por la presente política de privacidad y seguridad de la información.

Las políticas específicas deben ser entendidas como un conjunto de directrices que rigen la forma en la que esta Entidad gestiona la Privacidad y Seguridad de la información.

Los planes específicos definen las actuaciones a llevar a cabo para el desarrollo de las acciones derivadas del Marco Regulador.

Las políticas y planes específicos serán aprobados por el comité correspondiente y/o el titular del área con competencia en administración electrónica a propuesta del órgano directivo competente, previa consulta al referido comité.

Nivel 2: Normativas de Privacidad y Seguridad de la Información

A Nivel táctico, en el que se establecen las normas que definen las pautas para cada una de las áreas de conocimiento y seguridad del Servicio de Salud de conformidad con los objetivos establecidos por la política de seguridad de la información.

El segundo nivel normativo desarrolla la PPSI mediante normas específicas que abarcan un área o aspecto determinado de la Privacidad y Seguridad de la Información.

Las Normativas de Privacidad y Seguridad de la Información específicas serán aprobados por el comité correspondiente o el titular del área con competencia en administración electrónica a propuesta del órgano directivo competente en la materia sobre la que se desarrolla el documento, previa consulta al referido comité.

Nivel 3: Procedimientos y guías técnicas

A Nivel operativo, en el que se desarrollan los procedimientos y las instrucciones técnicas que detallen las actividades que se deberán realizar para gestionar la seguridad de la información definiendo los detalles concretos y los aspectos prácticos sobre la manera de realizarlas para ejecutar la tarea especificada y cumplir las responsabilidades asignadas.

Los procedimientos indican el método de ejecución, paso a paso, en tareas o actividades concretas relacionadas con la Privacidad y Seguridad de la Información.

Las guías técnicas tienen un carácter formativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de Privacidad y Seguridad de la Información.

Los procedimientos y guías técnicas deben ser aprobados por el órgano o unidad administrativa con competencias en la materia sobre la que se desarrolla el documento, previa validación del Responsable de Privacidad y Seguridad de la Información.

Este marco documental estará a disposición del personal que trabaje para el Servicio de Salud y que necesite conocerlo, en particular para quien use o administre los sistemas de información y las comunicaciones.

En cuanto al tratamiento de los datos de carácter personal, hay que actuar según lo que disponen los correspondientes documentos de seguridad exigidos en la legislación vigente.

5. Principios Básicos y Requisitos Mínimos de Privacidad y Seguridad de la Información

5.1. Principios Básicos

El SES 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) 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.

c) 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.

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

e) Exactitud: Los datos de carácter personal serán exactos y, si fuera necesario, actualizarlos; se adoptarán todas las medidas 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.

f) 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.

g) 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.

h) Responsabilidad proactiva: El SES 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.

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

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

k) Seguridad integral: La seguridad tenderá a la preservación de la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio. La seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural.

l) Gestión de riesgos: La gestión del riesgo es el conjunto de actividades coordinadas que el SES desarrolla para dirigir y controlar el riesgo, entendiendo como riesgo el efecto de la incertidumbre sobre la consecución de los objetivos El análisis y gestión

de riesgos son parte esencial del proceso de protección de datos y de seguridad de la información del SES, de forma que perita el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos, la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo el SES tendrá en cuenta aquellos riesgos que se deriven para los derechos de las personas con respecto al tratamiento de sus datos personales.

m) Proceso de verificación: El SES implantará un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la privacidad y seguridad de la información.

n) Protección de datos y seguridad desde el diseño: El SES promoverá la implantación del principio de protección de datos desde el diseño con el objetivo de cumplir los requisitos definidos en el RGPD 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.

o) Prevención, reacción y recuperación: La privacidad y la seguridad de la información deben contemplar los aspectos de prevención, reacción y recuperación sobre los activos, para conseguir que las amenazas sobre los mismos no se materialicen, no afecten gravemente a la información que maneja, o los servicios que se prestan.

p) Líneas de defensa: Los sistemas de información han de disponer de una estrategia de protección constituida por múltiples capas de seguridad.

q) Reevaluación periódica: La gestión de la Privacidad y Seguridad de la Información se revisará, evaluará y actualizará periódicamente para mantener su eficacia de forma continuada, con la finalidad de hacer frente a la constante evolución de los riesgos y las medidas de seguridad.

r) Responsabilidad diferenciada: En los sistemas de información del SES se observará el principio de responsabilidad diferenciada de forma que se delimiten las diferentes responsabilidades y roles.

s) Servicio a la ciudadanía: La Privacidad y la Seguridad de la Información estará orientada a la prestación de servicios de confianza a la ciudadanía en sus relaciones con la Administración.

5.2. Requisitos Mínimos

El SES establece los siguientes requisitos mínimos, que han de regir su Marco Regulador:

a) Organización e implantación del proceso de seguridad: La seguridad compromete a todo el personal dentro del alcance definido en este documento.

b) Análisis y gestión de los riesgos: El SES debe analizar y tratar sus riesgos empleando metodologías reconocidas. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos, en especial cuando se traten datos de carácter personal.

c) Evaluación de impacto en la privacidad: Cuando se traten datos de carácter personal que, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas, debe realizarse, antes del tratamiento, una evaluación del impacto en la privacidad.

d) Gestión de Personal: El personal de las entidades incluidas en el alcance serán informados de sus deberes y obligaciones en materia de seguridad.

e) Profesionalidad: El personal de las entidades incluidas en el alcance que desarrollen funciones en el ámbito de la Privacidad y Seguridad de la Información dispondrán de la capacitación adecuada para la ejecución de las tareas encomendadas.

f) Autorización y control de los accesos: El acceso a los sistemas de información estarán controlados y limitados. Cada usuario, proceso, dispositivo y otros sistemas de información que accedan a la información de los sistemas del SES 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.

g) Protección de las instalaciones: Las instalaciones del SES contarán con medidas de seguridad física adecuadas a la información que tratan en su interior.

h) Adquisición de productos: En la adquisición de productos de seguridad, se atenderá, de manera proporcionada, a la categoría y el nivel de seguridad determinados para los sistemas de información para los que sus funcionalidades son requeridas, las cuales deberán estar certificadas, salvo en aquellos casos en que las exigencias de proporcionalidad en cuando a los riesgos asumidos no lo justifiquen a juicio del Responsable de Seguridad.

i) Seguridad por defecto: Los sistemas de información deben diseñarse y configurarse de forma que proporcionen las mínimas funcionalidades requeridas, incluidas aque-

llas relacionadas con la operación, administración y registro de actividad, asegurando su disponibilidad y de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

j) Integridad y actualización del sistema: Se mantendrá actualizado el estado de seguridad de los sistemas de información, con relación a las especificaciones de los fabricantes, las vulnerabilidades y las actualizaciones que les afecten, de forma que dicho estado sirva como entrada a las actividades de gestión de riesgos. Cualquier elemento de los sistemas de información, para los que se considere necesaria su instalación, deberá tener la autorización previa por parte del Responsable de Privacidad y Seguridad de la Información.

k) Protección de la información almacenada y en tránsito: Se prestará especial atención a la información, en cualquier soporte, almacenada o en tránsito a través de entornos inseguros. Aplicándose las medidas de seguridad que correspondan a la naturaleza del soporte en que se encuentren, de conformidad con las normas de aplicación a la seguridad de los mismos.

l) Prevención ante otros sistemas de información interconectados: Se protegerán adecuadamente tanto las comunicaciones entre los sistemas de información y otros sistemas externos y en particular los puntos de interconexión entre las redes que soporten dichas comunicaciones, especialmente aquellas que se realicen a través de redes públicas.

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

n) Incidentes de seguridad: Se implantarán los mecanismos apropiados para la correcta identificación, registro, resolución y notificación, en los términos previstos en el RGPD y el ENS, de los incidentes de seguridad.

o) Continuidad de la actividad: Se desarrollarán planes de continuidad de negocio y actividades de recuperación para garantizar la disponibilidad de los servicios.

p) Mejora continua del proceso de seguridad: La gestión de la Privacidad y la Seguridad de la Información estará sometida a un ciclo de mejora continua como resultado de la aplicación del principio de reevaluación periódica.

6. Organización de la Seguridad de la Información en el Servicio Extremeño de Salud

6.1. Estructura de la Organización de la Seguridad de la Información

El Servicio Extremeño de Salud, en su adecuación al cumplimiento del Esquema Nacional de Seguridad, creará los siguientes órganos específicos para estructurar la gestión de la seguridad de la información y de la protección de datos.

Para cumplir las medidas de seguridad del ENS, en los marcos organizativo, operacional y de protección, debe ser la organización, en este caso el SES, a través de los órganos definidos, quien dirija y oriente a la dirección de la Entidad en la forma de conseguirlo. Estos órganos se estructuran en tres niveles: Gobierno, Supervisión y Operacional.

Se describe a continuación cada uno de estos órganos:

Comité de Gestión y Coordinación de Seguridad de la Información

Tiene como objetivo alinear todas las actividades de la organización referentes a seguridad de la información. El Comité de Gestión y Coordinación de la Seguridad de la Información coordina la seguridad de la información en la entidad y establece la estrategia; estará formado por un representante de la dirección de la entidad, el Responsable de la Seguridad de la Información y por representantes de otras áreas de la organización afectadas (Responsables de Servicios y Responsables de la Información).

Se convocarán reuniones ordinarias del Pleno del Comité con una periodicidad mínima semestral. Además, cualquiera de sus miembros podrá solicitar una convocatoria extraordinaria si concurren causas que lo aconsejen. A este respecto los miembros del Comité tendrán las siguientes funciones:

— Proponer que se incluyan en el orden del día las cuestiones que estimen oportunas con relación a la seguridad de la información.

— Asistir a las reuniones del Comité, participar en sus debates, formular ruegos y preguntas y ejercer el derecho a voto.

El Comité podrá acordar la creación de cuantos grupos de trabajo considere necesarios para preparar, estudiar y desarrollar las cuestiones sometidas a su conocimiento. Dichos grupos ejercerán por razones de urgencia y operatividad las funciones que el Pleno les delegue. El Comité conocerá en las sesiones del Pleno los resultados de las actuaciones de los grupos de trabajo.

De cada sesión se extenderá un acta, en la que constarán las circunstancias de lugar y tiempo, las personas asistentes, el orden del día, un resumen de las deliberaciones, las

decisiones acordadas y cualquier otro tema que los miembros del Comité soliciten expresamente que conste en ella.

El Comité de Gestión y Coordinación de Seguridad de la Información contará con los siguientes perfiles:

Perfiles a nivel de Gobierno:

— Responsable de la Dirección.

— Responsable de Tratamiento de Datos (RGPD- Nueva LOPDGDD).

— Responsable de la Información.

— Responsable del Servicio.

— Otros responsables de diferentes áreas del Servicio Extremeño de Salud que se considere necesario.

Perfiles a nivel de Supervisión:

— Responsable de Seguridad: Ejercerá las funciones de Secretario del Comité de Gestión y Coordinación de Seguridad de la Información y será el enlace con la Unidad de Seguridad de la Información y Protección de Datos.

— Delegado de Protección de Datos (RGPD- Nueva LOPDGDD).

Funciones:

— Atender las inquietudes de la Dirección de la entidad y de los diferentes departamentos.

— Informar regularmente del estado de la seguridad de la información a la Dirección.

— Promover la mejora continua del sistema de gestión de la seguridad de la información.

— Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.

— Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, que están alineados con la estrategia decidida en la materia, evitando duplicidades.

— Elaborar (y revisar regularmente) la Política de Privacidad y Seguridad de la Información para su aprobación por la Dirección.

— Aprobar la Normativa de Seguridad de la información.

— Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios, desde el punto de vista de seguridad de la información.

— Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones.

— Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de tales incidentes.

— Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.

— Aprobar planes de mejora de la seguridad de la información de la organización. En particular velará por la coordinación de distintos planes que puedan realizarse en diferentes áreas.

— Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.

— Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.

— Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

Unidad de Seguridad de la Información y Protección de Datos

Tiene como objetivo impulsar, promover y fomentar la seguridad de la información en su ámbito de responsabilidad y actuación. La Unidad de Seguridad de la Información y Protección de Datos desarrollara, entre otras, labores de soporte, asesoramiento e información al Comité de Gestión y Coordinación de Seguridad de la Información del Servicio Extremeño de Salud.

La Unidad de Seguridad de la Información y Protección de Datos contará con los siguientes perfiles:

Perfiles a nivel Operativo:

— Responsable del Sistema.

— Administrador de Seguridad.

— Encargado de Tratamiento (RGPD- Nueva LOPDGDD).

Perfiles a nivel de Supervisión:

— Responsable de Seguridad.

— Coordinador de la Oficina Técnica.

— Delegado de Protección de Datos (RGPD- Nueva LOPDGDD).

Funciones:

— Labores de soporte, asesoramiento e información al Comité de Gestión y Coordinación de Seguridad de la Información y a su Grupo de Respuesta a Incidentes TIC, sí lo hubiera, así como de ejecución de las decisiones y acuerdos adoptados.

— Coordinar los esfuerzos de las distintas gerencias, de los órganos y los organismos pertenecientes al Servicio Extremeño de Salud o adscritos a este y, en general, de todos los grupos internos con responsabilidades sobre la seguridad de la información, con el fin de asegurar que las iniciativas en esta materia sean homogéneas y de evitar duplicidades.

— Diseño y ejecución de los programas de actuación de carácter horizontal, así como la dirección de los proyectos y servicios corporativos de seguridad TIC.

— Desarrollo, mantenimiento y supervisión del marco regulador de seguridad TIC.

— Generación y supervisión de criterios y directrices corporativas de gestión de la seguridad TIC.

— Recogida sistemática de información y supervisión del estado de las principales variables de seguridad TIC.

— Coordinación y seguimiento de la actividad de las diferentes Unidades de Seguridad TIC.

— Realización de los procedimientos de compra centralizada de productos y servicios corporativos de seguridad TIC a propuesta del Comité de Seguridad de la Información, en aquellos supuestos en que se determine su conveniencia en razón a criterios de oportunidad, eficacia y de economías de escala.

— Realización de auditorías técnicas y de cumplimiento normativo, en aquellos supuestos en que se determine su conveniencia en razón a criterios de oportunidad, eficacia, eficiencia y de economías de escala.

— Representación ante los foros y agentes de relevancia del sector.

— Coordinación del Grupo de Personas Expertas en Seguridad TIC.

— Y cuantas otras le sean encomendadas por la Subdirección de Sistemas de Información en materia de coordinación y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones.

Oficina Técnica de Seguridad de la Información

Tiene como objetivo la gestión técnica de la Seguridad de la Información en la organización, implantar las normativas y políticas de seguridad, auditar y realizar el seguimiento y mejora de las políticas y normativas, detección y seguimiento de los incidentes de seguridad.

La Oficina Técnica de Seguridad TIC contará con los siguientes perfiles:

— Perfiles a nivel Operativo:

• Administrador de Seguridad

— Perfiles a nivel de Supervisión:

• Coordinador de la Oficina Técnica

Funciones Destacadas:

— Informar al Responsable de Seguridad de incidentes.

— Análisis Forense de incidentes.

— Monitorización del sistema.

— Administración del equipamiento de seguridad.

— Análisis de requisitos de nuevas necesidades de seguridad.

— Concienciación en materia de seguridad de la información.

— Realizar auditorías internas de seguridad.

— Monitorización y Correlación de eventos de seguridad.

— Mejora y evaluación continua de la seguridad.

— Implantar las Normativas y Políticas de Seguridad.

— Desarrollar nuevas Políticas y Normativas de Seguridad en función de las necesidades detectadas.

— Formación y Concienciación de los usuarios.

6.2. Perfiles: Funciones y Responsabilidades

Responsable de la Dirección. La responsabilidad de la actividad de una entidad del sector Público se sitúa, en última instancia, en su Titular.

Las competencias o funciones de la entidad están recogidas en su norma de creación o en las sucesivas normas de desarrollo de su estructura, el Titular de la Entidad, en este caso el Titular de la Gerencia del SES, es responsable de fijar los objetivos estratégicos, organizar adecuadamente sus elementos constituyentes, sus relaciones internas y externas, y dirigir su actividad, incluyendo la aprobación de la Política de Seguridad de la Información del organismo, así como, en su caso, la Política de Protección de Datos, facilitando los recursos adecuados para alcanzar los objetivos de seguridad propuestos, velando por su cumplimiento.

La figura de la Dirección de la entidad (personificada en su Titular) cobra una importancia capital: de la Dirección depende la estrategia y el compromiso de la entidad con la seguridad y su adecuada implantación, gestión y mantenimiento.

La Política de Privacidad y Seguridad de la Información deberá identificar claramente a quién corresponden las funciones de Responsable de la Información, del Servicio, de Seguridad, del Sistema y Delegado de Protección de Datos, pudiendo determinar, además, aquellos puestos que serían compatibles e incompatibles para el desempeño de estas funciones. Con las salvedades definidas en el ENS, es posible que una misma persona pueda aunar varias responsabilidades o formar éstas parte de un órgano colegiado.

La información es la materia prima de la que se nutre la actividad de las entidades del Sector Público y puede tener su origen en la propia entidad, los ciudadanos y en terceras entidades (públicas o privadas).

El Responsable de la Información es una persona situada en el nivel Directivo de la organización. Esta figura tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.

El ENS asigna al Responsable de la Información la potestad de establecer los requisitos de la información en materia de seguridad. O, en terminología del ENS, la potestad de determinar los niveles de seguridad de la información, pudiendo ser una persona física concreta o un órgano colegiado.

La aprobación formal de los niveles de seguridad corresponde al Responsable de la Información, que recibirá la propuesta del Responsable de la Seguridad y del Responsable del Sistema, dentro de la estructura creada en el comité o unidad correspondiente.

Los Responsables de la Información ejercerán las siguientes funciones en su ámbito de actuación y competencia:

a) Evaluar los niveles de Seguridad de la Información tratada.

b) Asegurar el cumplimiento del Marco Regulador de la Privacidad y Seguridad de la Información.

c) Proporcionar los recursos y medios adecuados para el cumplimiento de los principios básicos, requisitos mínimos y Marco regulador en materia de Privacidad y Seguridad de la Información.

d) Asumir las funciones explícitamente atribuidas a la figura del Responsable de la Información en el ENS.

e) Informar al Responsable de Privacidad y Seguridad de la Información sobre el cumplimiento de los niveles de seguridad y resto de requerimientos que se definan.

El Responsable del Servicio tiene la potestad de establecer los requisitos del servicio en materia de seguridad. O, en terminología del ENS, la potestad de determinar los niveles de seguridad de los servicios, pudiendo ser una persona física concreta o tratarse en el Comité de Gestión y Coordinación de la Seguridad de la Información del SES.

La aprobación formal de los niveles de seguridad corresponde al Responsable del Servicio, que recibirá la propuesta del Responsable de la Seguridad y del Responsable del Sistema, dentro de la estructura creada en el comité o unidad correspondiente.

La determinación de los niveles en cada dimensión de seguridad debe realizarse dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad.

La prestación de un servicio siempre debe atender a los requisitos de seguridad de la información que maneja, en el caso del SES información sanitaria entre otras, a los que se suele añadir requisitos de disponibilidad, accesibilidad, interoperabilidad, etc.

Los Responsables de los Servicios ejercerán las siguientes funciones en su ámbito de actuación y competencia:

a) Evaluar los niveles de seguridad de los servicios prestados.

b) Establecer requisitos de Seguridad.

c) Proporcionar los recursos y medios adecuados para el cumplimiento de los principios básicos, requisitos mínimos y Marco Regulador de la Privacidad y Seguridad de la Información.

d) Como responsables últimos de los servicios, asumir la responsabilidad final de implantar las medidas de protección de aquellos.

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

f) Asumir las funciones explícitamente atribuidas a la figura del Responsable de los Servicios en el ENS.

En el ámbito del Servicio Extremeño de Salud existirá al menos un responsable operativo para cada uno de los servicios prestados por dicho ente.

Responsable de Privacidad y Seguridad de la Información es un perfil designado por la Dirección de la entidad teniendo en cuenta sus cualidades profesionales, en particular sus conocimientos especializados en legislación y las prácticas en materia de seguridad de la información y protección de datos de carácter personal.

El ENS señala que el Responsable de la Seguridad determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Las dos funciones esenciales del Responsable de la Seguridad son:

— Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la Política de Privacidad y Seguridad de la Información de la organización.

— Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

Adicionalmente el Responsable de Seguridad y Privacidad ejercerá como Secretario del Comité de Gestión y Coordinación de la Seguridad de la Información, y como tal:

— Convocará las reuniones del Comité de Gestión y Coordinación Seguridad de la Información.

— Preparará los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.

— Elaborará el acta de las reuniones.

— Convocará otros perfiles consultivos a las reuniones del comité sí fuera necesario.

— Es responsable de la ejecución directa o delegada de las decisiones del Comité.

El Responsable de Privacidad y Seguridad de la Información ejerce las siguientes funciones:

a) Colaborar, cooperar y asistir a los Responsables de la Información / Servicios en el desarrollo de sus funciones con la asistencia técnica del órgano competente de los sistemas de información que soporten los servicios.

b) Convocar reuniones del Comité de Gestión y Coordinación de Seguridad de la Información, así como de la Unidad de Seguridad de la Información y Protección de Datos para evitar redundancia de acciones, asegurar la reutilización de recursos y unificar criterios en materia de Privacidad y Seguridad de la Información y protección de datos, tales como clausulado, directrices, procedimientos comunes, etc.…

c) Desarrollar, operar y mantener el Sistema de Gestión de la Seguridad de la Información, en adelante SGSI, apoyado por todos los responsables.

d) Proponer el desarrollo de documentos técnicos del Marco Regulador y elevarlas a la persona titular competente en materia de administración electrónica para su aprobación. Proponer los planes de Privacidad y Seguridad de la Información, auditorías, continuidad de los servicios, formación y concienciación y observar su ejecución, así como su seguimiento.

e) Mantener informado al Delegado de Protección de Datos de cuantas decisiones tengan relación con la protección de datos que afecten de forma genérica al ámbito del SES. Difundir la PPSI y el resto del Marco Regulador en las entidades incluidas en su alcance. Velar por el cumplimiento y observancia del Marco Regulador de Privacidad y Seguridad de la Información.

f) Velar por que la Privacidad y Seguridad de la Información se incorpore en todos los proyectos de los sistemas de información, desde su especificación inicial hasta su puesta en operación y posterior mantenimiento, así como en la preservación de la información que sea requerida tras el cese de sus actividades.

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

h) Gestionar los incidentes de seguridad, con el apoyo de la Oficina Técnica de Seguridad de la Información desde su notificación hasta su resolución y participar en la toma de decisiones en momentos asistido por el órgano directivo competente en materia tecnologías de la información y comunicación.

i) A intervalos planificados, recibir y revisar información sobre el desempeño y cumplimiento del sistema de gestión de la Seguridad de la Información.

j) Representar al Servicio Extremeño de Salud en foros sectoriales o ante agentes externos en asuntos relacionados con la seguridad de la información.

k) Reportar información resumida de las actuaciones en materia de seguridad y de los incidentes, al Comité para la Gestión y la Coordinación de la Seguridad de la Información.

l) Asumir las funciones explícitamente atribuidas a la figura del Responsable Seguridad de la Información en el ENS.

El Responsable del Sistema será designado por la dirección de la entidad.

Tiene las siguientes funciones:

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 tipología 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.

d) El Responsable del Sistema puede proponer la suspensión del tratamiento de una cierta información o la prestación de un determinado servicio si aprecia deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. La decisión final, que será tomada por la dirección de la entidad, debe ser acordada con los responsables de la información y los servicios afectados y el Responsable de Privacidad y Seguridad.

e) Elaborar los planes de mejora de la seguridad junto con los responsables de la seguridad de la información.

f) Planificar la implantación de salvaguardas en los sistemas.

g) Ejecutar los planes de seguridad aprobados.

En el ámbito del Servicio Extremeño de Salud, todo sistema de información tendrá un responsable operativo, que será el titular de la unidad competente en su gestión y operación.

Administrador de Seguridad. Sus funciones más significativas serían 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.

El Delegado de Protección de Datos, es quien debe informar, asesorar y supervisar el cumplimiento en materia de protección de datos y actuar como punto de contacto con las autoridades de control. Tendrá como mínimo las siguientes funciones:

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 Reglamento (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 Reglamento (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.

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.

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

6.3. Procedimiento de Designación de Perfiles

Es función de la Dirección de la entidad, en este caso de la Gerencia del SES, designar los siguientes perfiles que se integraran en la estructura definida para la seguridad de la información en la organización:

— Al Responsable de la Información, que puede ser un cargo unipersonal o un órgano colegiado.

— Al Responsable del Servicio, que, pudiendo ser el mismo que el Responsable de la Información, también puede ser un cargo unipersonal o un órgano colegiado.

— Al Responsable de Privacidad y Seguridad de la Información, que debe reportar directamente a la Dirección o a los órganos de gobierno de la entidad y a los Comités de Seguridad constituidos.

— Al Responsable del Sistema, que, en materia de seguridad, reportará al Responsable de la Seguridad.

Es función del Responsable de Seguridad nombrar:

— Al Administrador de Seguridad.

El Comité de Coordinación y Gestión de la Seguridad de la Información analizará los candidatos propuestos para los diferentes perfiles y realizará una propuesta final a la dirección para que esta lleve a cabo los nombramientos.

La Unidad de Seguridad de la Información y Privacidad podrá elevar candidaturas a los diferentes perfiles para su estudio en el Comité de Gestión y Coordinación.

6.4. Nombramientos

El Responsable de la Dirección será el titular de la Gerencia del Servicio Extremeño de Salud, o en su defecto la persona en la que este delegue de manera formal.

Adicionalmente la persona titular de la Gerencia del Servicio Extremeño de Salud, o aquella en la que esta delegue de manera formal, ejercerá como Responsable de Tratamiento en representación de su entidad, en este caso el SES, que lo es como persona jurídica.

El Delegado de Protección de Datos será nombrado por la persona titular de la Gerencia del Servicio Extremeño de Salud con competencias en administración electrónica a fin de dar cumplimiento a lo requerido en el artículo 37 del RGPD, que llevará a cabo las tareas establecidas en el artículo 39 del citado RGPD, así como las que se deriven de la normativa española de protección de datos de carácter personal y de los documentos de buenas prácticas que se adopten por la propia entidad.

El titular de la Subdirección de Sistemas de Información del SES ejercerá como Responsable Privacidad y Seguridad de la Información, así como de Delegado de Protección de Datos, en su ámbito de actuación y competencias.

Los titulares de los Órganos Directivos que se designen en las diferentes áreas de actividad ejercerán como Responsables de los Servicios y/o Responsables de la Información.

El Responsable del Sistema será seleccionado entre el personal técnico, con los conocimientos adecuados, de la Subdirección de Sistemas de Información del SES.

Los Administradores de Seguridad serán seleccionados entre personal técnico que presta servicio en la Subdirección de Sistemas de Información del SES, con los conocimientos adecuados.

El Coordinador de la Oficina Técnica de Seguridad del SES será seleccionado entre los administradores de Seguridad.

El Comité de Coordinación y Gestión de la Seguridad de la Información analizará los candidatos propuestos para los diferentes perfiles y realizará una propuesta final a la dirección para que esta lleve a cabo los nombramientos.

La Unidad de Seguridad de la Información y Privacidad podrá elevar candidaturas a los diferentes perfiles para su estudio en el Comité de Gestión y Coordinación.

7. Datos de Carácter Personal

El Servicio Extremeño de Salud trata datos de carácter personal, entre otros datos sanitarios de carácter especialmente protegidos.

7.1. Registro de Actividades de Tratamiento

El SES mantendrá actualizado el registro de las actividades de tratamiento con datos de carácter personal de las que sea responsable, que incluirá toda la información a la que

se refiere el artículo 30 del RGPD. El listado de actividades de tratamiento se mantendrá actualizado y podrá consultarse en el Portal de Transparencia y Participación Ciudadana de la ACAEx así como en el portal Salud Extremadura del SES.

7.2. Análisis y Gestión de Riesgos. Evaluación de Impacto (EIPD)

Cuando la información contenga datos de carácter personal, se llevará a cabo, de forma periódica y al menos cada 2 años, un análisis de riesgos que permita 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 lleve a cabo el SES, así como los sistemas de información que sirven de soporte para dichas actividades de tratamiento.

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

7.3. Notificación Violaciones de Seguridad

El SES adoptará las medidas necesarias para garantizar la notificación de las violaciones de seguridad de los datos de carácter personal que pudieran producirse a través del procedimiento establecido al 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, conforme a lo dispuesto en el artículo 34 del RGPD.

8. Análisis de Riesgos de Seguridad de la Información

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

Todos los sistemas de información del Servicio Extremeño de Salud serán objeto de un análisis de los riesgos a cargo de los responsables de seguridad de la información, que se repetirá con una periodicidad mínima anual.

Los análisis de los riesgos, además, se actualizarán en cualquiera de estos casos:

a) Si se identifican nuevos activos de información o si cambian los existentes o sus requisitos de seguridad.

b) Si se identifican cambios con relación a los servicios prestados.

c) Si ocurre un incidente grave en la seguridad o se identifican o reportan graves vulnerabilidades en la seguridad de los sistemas existentes.

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

Para el análisis y gestión de riesgos se utilizarán las herramientas facilitadas por el Centro Criptológico Nacional (CCN), en particular: la metodología MAGERIT, las herramientas PILAR o las que se desarrollasen en el futuro, así como las guías, recomendaciones y herramientas elaboradas por el SES en lo que respecta al tratamiento de datos de carácter personal.

Las decisiones sobre las medidas, proyectos e iniciativas de seguridad que deban tomarse en el ámbito del Servicio Extremeño de Salud han de prever los resultados de la evaluación de los riesgos existentes en relación con la seguridad de la información sobre los sistemas utilizados.

El responsable de la seguridad de la información elevará al comité correspondiente los resultados de los análisis de los riesgos

9. Revisión y Auditoría

El SES 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 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 Privacidad y Seguridad de la Información y por el Delegado de Protección de Datos.

10. Medidas de Seguridad

Las medidas de seguridad implantadas se corresponderán con las previstas en el Anexo II (Medidas de Seguridad) 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.

11. Revisión de la Política

El Responsable de Privacidad y Seguridad de la Información y el Delegado de Protección de Datos asegurarán la revisión de la PPSI cuando se produzcan cambios significativos en el con-

texto y/o la organización del SES o bien con la periodicidad que se determine en el desarrollo del SGSI, la cual se elevará, para su revisión y aprobación, al Comité de Gestión y Coordinación de la Seguridad de la Información.

Su revisión debe garantizar que ésta se encuentra alineada con la estrategia, la misión y visión del organismo en materia de Privacidad y Seguridad de la Información.

En último término la Política de Privacidad y Seguridad de la Información, y sus revisiones, será aprobada formalmente por la Alta Dirección de la Organización y tendrá carácter imperativo sobre toda la organización.

Así mismo está sujeta a un proceso de revisión regular que la adapte a nuevas circunstancias, técnicas u organizativas, y evite que quede obsoleta.

Por ello se establece un proceso organizativo que asegura que regularmente se revisa la oportunidad, idoneidad, completitud y precisión de lo que la Política establezca y sea sometida a aprobación formal por la Alta Dirección.

12. Relación con Terceras Partes

Cuando un tercero preste servicio al Servicio Extremeño de Salud en el que deba acceder a datos personales de los que el SES es Responsable del Tratamiento, o se cedan activos de información a éstos, se le debe hacer partícipe del Marco Regulador de Privacidad y Seguridad de la Información que ataña a dichos servicios o activos.

Las terceras partes quedan sujetas a las obligaciones establecidas en dicho Marco.

Los contratos, encargos o convenios que se suscriban a partir de la entrada en vigor de este acuerdo deben incluir la obligación de cumplir esta Política y el sistema de verificación de su cumplimiento. Las subcontrataciones requerirán el consentimiento expreso del Responsable de la Información para el acceso a los activos de la información.

Cualquier tercero adjudicatario de un contrato, encargo o convenio que conlleve el tratamiento de datos de carácter personal en nombre del SES deberá ser constituido como Encargado de Tratamiento y firmar el correspondiente Encargo de Tratamiento como anexo a los contratos suscritos para la prestación de los servicios contratados.

Cuando el Servicio Extremeño de Salud preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de las respectivas unidades de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando el Servicio Extremeño de Salud utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Privacidad y Seguridad y de la Normativa de Seguridad 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 formado y concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando dicho tercero sea una administración pública o un organismo del sector público, aplicará sus propias normas de seguridad de la información una vez que se le haya cedido la información.

Si un tercero no puede cumplir algún aspecto de la política de seguridad de la información según lo que se requiere en los párrafos anteriores, será preciso obtener un informe del responsable de seguridad competente que precise los riesgos en que se incurre y la manera de tratarlos. Con anterioridad a su continuación, también será necesario que los responsables de la información y los responsables de los servicios afectados aprueben dicho informe antes de seguir adelante.

13. Resolución de Conflictos

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa definida para la gestión de la seguridad de la información, lo resolverá su superior jerárquico; en su ausencia, prevalece la decisión del Comité para la Gestión y la Coordinación de la Seguridad de la Información.

En caso de conflicto entre los responsables que componen la estructura organizativa para la gestión de la seguridad de la información y los definidos en la normativa de protección de datos de carácter personal, prevalece la decisión que implique el nivel más alto de protección.

14. Personal del Servicio Extremeño de Salud

El Servicio Extremeño de Salud garantizará la definición y la ejecución de las acciones necesarias para concienciar y fomentar el cumplimiento de las obligaciones por parte del personal con relación a los riesgos y las amenazas relativos a la seguridad de la información.

Las personas que realicen actividades especialmente relacionadas con la seguridad de la información —en particular el personal técnico a cargo de la gestión, operación y administración de los sistemas de información— tienen que recibir las acciones formativas necesarias en materia de seguridad.

Todo el personal que preste servicio en el ámbito del Servicio Extremeño de Salud conocerá y respetará el contenido de esta política de seguridad de la información y el marco normativo que la desarrolla.

La gestión y preservación de la seguridad de la información y el cumplimiento de los objetivos citados en esta Política deben ser el fin común de todas las personas que presten servicio directa o indirectamente en el Servicio Extremeño de Salud, de tal manera que son responsables del uso correcto de los activos de tecnologías de la información y de las comunicaciones y de los activos de información puestos a su disposición en el desempeño de sus funciones profesionales.

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

• • •