SERVICIO EXTREMEÑO DE SALUD

RESOLUCIÓN de 9 de noviembre de 2026, de la Dirección Gerencia, por la que se aprueba la Política de Privacidad y Seguridad de la Información del Servicio Extremeño de Salud. (2026062911)

La transformación digital de los servicios públicos sanitarios y la creciente dependencia de los sistemas de información hacen necesario disponer de un marco actualizado de privacidad y seguridad que garantice la adecuada protección de la información, los datos personales, los servicios y los sistemas del Servicio Extremeño de Salud, así como la continuidad de la actividad asistencial y administrativa.

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, establece los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y de los servicios prestados por las entidades de su ámbito de aplicación. Su artículo 12 exige que cada Administración pública disponga formalmente de una política de seguridad, aprobada por el órgano competente, y su artículo 11 establece la necesaria diferenciación de las responsabilidades relativas a la información, los servicios, la seguridad y los sistemas, así como el detalle de las atribuciones de cada responsable y de los mecanismos de coordinación y resolución de conflictos.

La política de seguridad debe precisar, asimismo, los objetivos o misión de la organización, el marco legal y regulatorio aplicable, los roles y funciones de seguridad, los deberes y responsabilidades asociados, los procedimientos de designación y renovación, la estructura de los órganos de gestión y coordinación y las directrices para la estructuración, gestión y acceso a la documentación de seguridad.

Asimismo, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, imponen al responsable del tratamiento la adopción de medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, así como la capacidad de acreditar su cumplimiento, materias que se integran en la presente Política por constituir la seguridad de la información y la protección de datos personales un ámbito indisociable en la prestación de los servicios sanitarios.

En el ámbito autonómico, mediante Resolución de 15 de julio de 2025, del Consejero de Economía, Empleo y Transformación Digital, se ordenó la publicación en el Diario Oficial de Extremadura del Acuerdo del Consejo de Gobierno de la Junta de Extremadura, de 1 de julio

de 2025, por el que se establece una nueva Política de Privacidad y Seguridad de la Información de la Administración de la Comunidad Autónoma de Extremadura. Dicha política dispone que los organismos públicos quedan sujetos a sus términos y condiciones, a excepción del Servicio Extremeño de Salud que, en atención a sus especiales funciones y singularidades respecto de su organización y funcionamiento, debe establecer su propia Política de Privacidad y Seguridad de la Información, alineada con los principios y requisitos mínimos de la política autonómica.

La Política de Privacidad y Seguridad de la Información del Servicio Extremeño de Salud actualmente vigente fue aprobada mediante Resolución de 14 de junio de 2021, de la Dirección Gerencia, publicada en el Diario Oficial de Extremadura número 121, de 25 de junio de 2021. Su aprobación fue anterior a la entrada en vigor del Real Decreto 311/2022, por lo que resulta necesario adecuarla al vigente Esquema Nacional de Seguridad, a la evolución del marco normativo y técnico y a la actual estructura organizativa del Servicio Extremeño de Salud.

El Decreto 109/2026, de 26 de mayo, por el que se establece la estructura orgánica de la Consejería de Salud y Atención a la Dependencia y se modifican los Estatutos del Organismo Autónomo Servicio Extremeño de Salud, ha introducido cambios relevantes en sus órganos de dirección y gestión, entre ellos la creación de la Dirección General de Salud Digital, a la que se adscribe la Subdirección de Sistemas de Información y a la que se atribuyen competencias relacionadas con los sistemas y tecnologías de la información, las aplicaciones, las comunicaciones, la seguridad TIC, el acceso seguro, la identificación y autenticación, las infraestructuras y equipamientos y el gobierno del dato.

Asimismo, la Resolución de 12 de junio de 2026, de la Dirección Gerencia, desarrolla la estructura de los órganos de los Servicios Centrales del organismo y aprueba la relación de puestos de carácter directivo de los mismos, de acuerdo con la estructura orgánica vigente.

La nueva política incorpora un modelo actualizado de gobernanza de la privacidad y seguridad de la información, define los órganos, roles, funciones y responsabilidades, establece los mecanismos de coordinación, reporte, escalado y resolución de conflictos y ordena jerárquicamente el marco documental de desarrollo, atendiendo a la naturaleza asistencial, la distribución territorial y la criticidad de los servicios prestados por el Servicio Extremeño de Salud.

El Comité de Gestión y Coordinación de Seguridad de la Información del Servicio Extremeño de Salud, en sesión de 4 de noviembre de 2026, acordó elevar a la Dirección Gerencia la propuesta de aprobación de la Política de Privacidad y Seguridad de la Información que se incorpora como anexo a la presente resolución.

En su virtud, a propuesta del Comité de Gestión y Coordinación de Seguridad de la Información, y en uso de las atribuciones conferidas por el artículo 4, letras g) e y), de los Estatutos

del Servicio Extremeño de Salud, aprobados por Decreto 221/2008, de 24 de octubre, en la redacción dada por el Decreto 109/2026, de 26 de mayo, así como en cumplimiento de lo dispuesto en el artículo 12 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad,

RESUELVE:

Primero. Aprobar la Política de Privacidad y Seguridad de la Información del Servicio Extremeño de Salud, que se incorpora como anexo a la presente resolución.

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

Tercero. Dejar sin efecto la 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, sin perjuicio de la validez de los actos, disposiciones y actuaciones adoptados durante su vigencia que no se opongan a la Política aprobada mediante la presente resolución.

Cuarto. Las normas, procedimientos, instrucciones técnicas, guías, planes y demás documentación aprobada con anterioridad mantendrán su vigencia en cuanto no contradigan la Política aprobada mediante la presente resolución, hasta que sean revisados, sustituidos o dejados sin efecto por el órgano o rol competente.

Quinto. Los órganos, roles y designaciones regulados en la Política de Privacidad y Seguridad de la Información deberán adaptar sus actos de constitución, composición y nombramiento en el plazo máximo de un mes desde la entrada en vigor de la presente resolución. Cuando la adaptación dependa de nombramientos pendientes, el plazo se computará desde la toma de posesión de la persona titular del puesto afectado.

Sexto. La implantación, aplicación y desarrollo de la Política se atenderán con los medios personales, técnicos y presupuestarios disponibles, sin perjuicio de que los órganos competentes deban identificar, priorizar y promover la dotación de los recursos que resulten necesarios para garantizar el cumplimiento normativo, la gestión adecuada de los riesgos y la continuidad y seguridad de los servicios.

Séptimo. La presente resolución entrará en vigor el día siguiente al de su publicación en el Diario Oficial de Extremadura.

Mérida, 9 de noviembre de 2026.

La Directora Gerente,

ENCARNACIÓN SOLÍS PÉREZ

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

1. INTRODUCCIÓN.

Acrónimos.

Términos y definiciones.

2. MISIÓN, OBJETO Y ALCANCE.

2.1. Misión.

2.2. Objeto.

2.3. Alcance.

3. MARCO NORMATIVO Y ESTRATEGIA.

3.1. Marco normativo aplicable.

3.2. Estrategia de Privacidad y Seguridad de la Información.

4. PRINCIPIOS BÁSICOS, OBJETIVOS Y REQUISITOS MÍNIMOS.

4.1. Principios básicos en el ámbito de la protección de datos personales.

4.2. Principios básicos en el ámbito de la seguridad de la información.

4.3. Objetivos.

4.4. Requisitos mínimos.

5. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

5.1. Criterios de organización.

5.2. Modelo de gobernanza.

5.3. Roles de seguridad.

5.3.1. Responsable de la Información.

5.3.2. Responsable del Servicio.

5.3.3. Responsable de la Seguridad.

5.3.4. Responsable del Sistema.

5.3.5. Responsable del Tratamiento.

5.3.6. Delegado o Delegada de Protección de Datos.

5.4. Órganos de la seguridad de la información.

5.4.1. Comité de Gestión y Coordinación de Seguridad de la Información.

5.4.2. Unidad de Gobernanza y Cumplimiento Normativo de la Ciberseguridad.

5.4.3. Oficina de Ciberseguridad.

5.4.4. Centro de Operaciones de Ciberseguridad.

5.4.5. Órgano de Auditoría Técnica.

5.5. Otros roles.

5.6. Procedimientos de designación y renovación.

5.7. Diferenciación de responsabilidades y resolución de conflictos.

5.8. Obligaciones del personal.

6. SISTEMA DE GESTIÓN DE LA PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN.

6.1. Protección de datos personales.

6.1.1. Responsabilidad proactiva.

6.1.2. Privacidad desde el diseño y por defecto.

6.1.3. Gestión de brechas de seguridad de los datos personales.

6.1.4. Relaciones con terceros en el ámbito de la privacidad.

6.2. Seguridad de la información.

6.2.1. Gobernanza.

6.2.2. Gestión del riesgo.

6.2.3. Modelo de operación: prevención, detección, respuesta y recuperación.

6.2.4. Gestión y notificación de incidentes.

6.2.5. Cumplimiento y mejora continua.

6.3. Protección de infraestructuras críticas y servicios esenciales.

7. DESARROLLO DE LA POLÍTICA Y MARCO DOCUMENTAL.

7.1. Estructura del marco documental.

7.1.1. Nivel 1. Política de Privacidad y Seguridad de la Información.

7.1.2. Nivel 2. Normativa de Privacidad y Seguridad de la Información.

7.1.3. Nivel 3. Procedimientos, instrucciones técnicas y guías.

7.2. Coherencia y trazabilidad documental.

7.3. Norma para la gestión de la documentación.

7.4. Perfiles de cumplimiento específicos.

7.5. Planes y documentos específicos.

7.6. Revisión del marco documental y de la Política.

7.7. Publicación, difusión y cumplimiento.

8. RELACIÓN CON TERCERAS PARTES.

1. INTRODUCCIÓN.

El Servicio Extremeño de Salud (en adelante, SES) es un organismo autónomo de carácter administrativo, adscrito a la Consejería competente en materia sanitaria, dotado de personalidad jurídica propia y plena capacidad de obrar para el cumplimiento de sus fines, al que corresponde la gestión de los servicios públicos sanitarios de carácter asistencial.

La información que el SES recaba y gestiona en el ejercicio de sus competencias constituye un activo esencial para el cumplimiento de sus fines, y el funcionamiento correcto de los sistemas de información que la albergan y tratan resulta imprescindible para el ejercicio adecuado y eficiente de las obligaciones atribuidas en materia asistencial y de gestión sanitaria. El SES asume, en consecuencia, la responsabilidad asociada a la protección de esa información frente a las amenazas que puedan afectar a su seguridad.

La asistencia sanitaria es objetivo declarado de los actores de amenazas de ciberseguridad, que persiguen tanto la indisponibilidad de los sistemas atacados como el acceso a la información tratada, muy especialmente la historia clínica y los registros electrónicos asociados. La ciudadanía, como destinataria de los servicios, debe ser considerada el centro de la seguridad de los sistemas de información asistenciales, focalizando las medidas en los datos y en los derechos asociados, y de manera singular en la seudonimización y medidas equivalentes capaces de proteger la privacidad frente a los ataques que pudieran presentarse.

Hacer frente a estas amenazas requiere una estrategia que se adapte a la evolución del entorno para garantizar la prestación continua de los servicios. Ello implica aplicar las medidas de seguridad exigidas por el Esquema Nacional de Seguridad, realizar un seguimiento continuo de los niveles de prestación, monitorizar y analizar las vulnerabilidades reportadas y proporcionar una respuesta efectiva a los ciberincidentes que garantice la continuidad de los servicios. Este esfuerzo debe alcanzar a todos los niveles de la organización, desde el estratégico hasta el operativo, e interactuar con la cadena de suministro y con los proveedores.

Tanto los Servicios Centrales como las Gerencias de las Áreas de Salud deben asegurar que la ciberseguridad es parte integral de cada etapa del ciclo de vida de los sistemas, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y por las actividades de explotación. Los requisitos de seguridad y la valoración de su coste deben identificarse e incluirse en la planificación, en la solicitud de ofertas y en los pliegos de licitación. Los proveedores del sector sanitario presentan características específicas que esta Política debe considerar, en particular la reducida competencia y la exclusividad de determinadas soluciones, así como su condición de objetivo prioritario para los ciberatacantes.

Para la asistencia sanitaria, el objetivo prioritario de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando proactiva y preventivamente, supervisando la actividad diaria para detectar cualquier anomalía o incidente y reaccionando con presteza para recuperar los servicios en el menor tiempo posible.

El alcance de esta Política se extiende a las previsiones y requisitos del Esquema Nacional de Seguridad y a la normativa de protección de datos personales, bajo la consideración de que esta última forma parte de la seguridad de la información, tal como se desprende de la inclusión de ambas materias en el derecho reconocido a la ciudadanía por el artículo 13.h) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Las directrices que siguen se han redactado con un lenguaje deliberadamente sencillo, evitando los tecnicismos innecesarios, para facilitar su comprensión por el conjunto de la organización, y se limitan al contenido propio de una política de seguridad, remitiendo el desarrollo operativo al marco documental previsto en el capítulo 7.

Acrónimos.

— ACAEx: Administración de la Comunidad Autónoma de Extremadura.

— CCN: Centro Criptológico Nacional.

— CSIRT: Equipos de respuesta ante incidentes de seguridad.

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

— COC: Centro de Operaciones de Ciberseguridad.

— DGSD: Dirección General de Salud Digital.

— DPD: Delegado o Delegada de Protección de Datos.

— ENS: Esquema Nacional de Seguridad, regulado por el Real Decreto 311/2022, de 3 de mayo.

— LOPDGDD: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

— OAT: Órgano de Auditoría Técnica.

— OC: Oficina de Ciberseguridad.

— PCE Salud: Perfil de Cumplimiento Específico para el sector salud.

— PIC: Protección de Infraestructuras Críticas.

— PoC: Punto de contacto.

— PPSI SES: Política de Privacidad y Seguridad de la Información del Servicio Extremeño de Salud.

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

— SES: Servicio Extremeño de Salud.

— TIC: Tecnologías de la información y las comunicaciones.

— UGCNC: Unidad de Gobernanza y Cumplimiento Normativo de la Ciberseguridad.

Términos y definiciones.

Los términos empleados en esta Política se entenderán conforme a las definiciones contenidas en el Anexo IV del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, así como en la guía CCN-STIC 800 (Glosario de términos y abreviaturas del ENS), y en el artículo 4 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (Reglamento General de Protección de Datos), sin perjuicio de las precisiones que, en su caso, establezca la normativa de desarrollo de la presente Política.

2. MISIÓN, OBJETO Y ALCANCE.

2.1. Misión.

El Servicio Extremeño de Salud es un organismo autónomo de carácter administrativo, adscrito a la Consejería competente en materia sanitaria. Tiene como objeto la prestación de la atención sanitaria, incluyendo la planificación, organización, dirección y gestión de los centros sanitarios adscritos, así como la planificación, organización, dirección y gestión de sus recursos humanos, materiales y financieros. Todo ello de conformidad con los principios constitucionales y estatutarios, respetando los principios de buena fe, confianza legítima, transparencia, seguridad y calidad en el servicio a la ciudadanía y a las organizaciones.

2.2. Objeto.

La PPSI SES establece el marco de referencia y las directrices para asegurar la integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, in-

formaciones utilizadas y servicios prestados, en especial cuando se traten datos personales, que gestiona el SES en el ejercicio de sus competencias.

2.3. Alcance.

La PPSI SES será de aplicación a todos los sistemas de información y a todas las actividades de tratamiento de datos personales de los que el SES actúe como Responsable de Tratamiento, en especial aquellos relacionados con el ejercicio de derechos por medios electrónicos por todas las personas usuarias con acceso autorizado a dichos sistemas e información, sean o no personal propio del SES o personal público.

Quedan asimismo sometidas a esta Política todas las personas usuarias con acceso autorizado a dichos sistemas e información, sean o no personal público, y con independencia de la naturaleza de su relación jurídica, estando todas ellas obligadas a conocer y cumplir la PPSI SES y su normativa de desarrollo. Corresponde al Comité de Gestión y Coordinación de Seguridad de la Información promover la dotación de los recursos y medios necesarios para su cumplimiento.

La condición de responsable no requerirá, necesariamente, que las plataformas o sistemas que soportan los servicios sean gestionados directamente por el SES. Tales elementos se recogerán en la correspondiente declaración de alcance, distinguiendo la responsabilidad sobre cada uno de ellos en los procesos de análisis y gestión de riesgos que se lleven a cabo.

3. MARCO NORMATIVO Y ESTRATEGIA.

3.1. Marco normativo aplicable.

El marco normativo de la privacidad y seguridad de la información del SES está integrado por las normas de ámbito europeo, estatal y autonómico que afecten a estas materias y, en particular, por las siguientes:

— El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

— La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y el Real Decreto 1720/2007, de 21 de diciembre, en lo que no contradiga a la normativa anterior.

— El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, cuyo artículo 12 exige que las Administraciones Públicas dispongan formal-

mente de su política de seguridad, aprobada por el órgano competente, y cuyo artículo 11 configura la seguridad como función diferenciada, con detalle de las atribuciones de cada responsable y de los mecanismos de coordinación y resolución de conflictos.

— 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.

— La Ley 10/2001, de 28 de junio, de Salud de Extremadura, y las disposiciones que la desarrollan.

— El Decreto 225/2014, de 14 de octubre, de régimen jurídico de administración electrónica de la Comunidad Autónoma de Extremadura.

— La Política de Privacidad y Seguridad de la Información de la Administración de la Comunidad Autónoma de Extremadura, con cuyos principios y requisitos mínimos se alinea la presente Política.

— Las guías CCN-STIC de seguridad elaboradas por el Centro Criptológico Nacional, y en particular las relativas a la política de seguridad de la información, al ámbito de aplicación del ENS, al glosario de términos y a las responsabilidades y funciones en el ENS.

— La normativa sectorial que resulte aplicable al SES en materia de protección de infraestructuras críticas, servicios esenciales y ciberseguridad, así como las instrucciones técnicas de seguridad dictadas en desarrollo del ENS.

La relación actualizada de la normativa aplicable se mantendrá publicada y accesible a través del gestor documental y del portal del conocimiento del SES.

3.2. Estrategia de Privacidad y Seguridad de la Información.

De manera periódica, el SES establecerá las líneas de actuación y los objetivos en materia de privacidad y seguridad de la información para un contexto y un período determinados, con el fin de garantizar la confianza de la ciudadanía en los servicios públicos digitales.

La Estrategia de Privacidad y Seguridad de la Información del SES estará alineada con la estrategia global de la Administración de la Comunidad Autónoma de Extremadura en materia digital y será aprobada por resolución de la persona titular de la Dirección Gerencia, a propuesta del Comité de Gestión y Coordinación de Seguridad de la Información.

4. PRINCIPIOS BÁSICOS, OBJETIVOS Y REQUISITOS MÍNIMOS.

El Esquema Nacional de Seguridad se estructura en principios, requisitos y medidas de seguridad, aportando un enfoque que va de lo más general a lo más concreto. Los principios son las premisas que permiten a la organización cumplir sus objetivos y ejercer sus competencias mediante sistemas de información; se concretan en requisitos mínimos, que son las especificaciones para una protección adecuada de la información y los servicios; y estos descienden a un conjunto de medidas de seguridad.

4.1. Principios básicos en el ámbito de la protección de datos personales.

— Licitud, lealtad y transparencia: los datos personales se tratarán de manera lícita, leal y transparente en relación con la persona interesada.

— Legitimación del tratamiento: solo se llevará a cabo el tratamiento cuando esté legitimado en la normativa aplicable.

— Limitación de la finalidad: los datos se tratarán únicamente para el cumplimiento de fines determinados, explícitos y legítimos, y no ulteriormente de manera incompatible con dichos fines.

— Minimización de datos: serán adecuados, pertinentes y limitados a los fines para los que son tratados.

— Exactitud: serán exactos y, si fuera necesario, actualizados, adoptándose las medidas razonables para que se supriman o rectifiquen sin dilación cuando sean inexactos.

— Limitación del plazo de conservación: se mantendrán de forma que se permita la identificación de las personas interesadas durante no más tiempo del necesario para los fines que justificaron su tratamiento.

— Integridad y confidencialidad: se garantizará su seguridad, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante medidas técnicas y organizativas apropiadas. Quienes intervengan en el tratamiento estarán sujetos al deber de secreto incluso después de haber concluido aquel.

— Responsabilidad proactiva: el SES será responsable del cumplimiento de los principios anteriores y adoptará las medidas que le permitan estar en condiciones de demostrarlo.

— Atención de los derechos de las personas afectadas: se adoptarán las medidas organizativas que garanticen el adecuado ejercicio de los derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad.

— Protección de datos y seguridad desde el diseño y por defecto: la protección de datos estará presente desde las primeras fases de concepción de cualquier proyecto, y la seguridad de la información se aplicará desde el diseño inicial de los sistemas.

4.2. Principios básicos en el ámbito de la seguridad de la información.

— Alcance estratégico: la seguridad de la información cuenta con el compromiso y el apoyo de todos los niveles directivos, concierne a todos los miembros de la organización y debe estar coordinada e integrada con el resto de iniciativas estratégicas.

— Seguridad integral: la seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas, evitando actuaciones puntuales o tratamientos coyunturales.

— Gestión de riesgos: la gestión del riesgo es la piedra angular del proceso de seguridad, por permitir el mantenimiento de un entorno controlado con los riesgos en niveles aceptables. Al evaluar el riesgo se tendrán en cuenta los riesgos para los derechos y libertades de las personas derivados del tratamiento de sus datos personales.

— Proporcionalidad: las medidas adoptadas para gestionar los riesgos deberán estar justificadas y ser proporcionadas a estos.

— Prevención, detección, respuesta y recuperación: la seguridad del sistema contemplará acciones relativas a todos estos aspectos, orientadas a minimizar las vulnerabilidades, reducir la probabilidad de materialización de las amenazas y controlar su impacto, sin perjuicio de que las medidas desplegadas garanticen la conservación de los datos y la información.

— Líneas de defensa: los sistemas dispondrán de una estrategia de protección constituida por múltiples capas de seguridad que permitan una respuesta proporcionada, conforme a un esquema de contención, mitigación y recuperación.

— Reevaluación periódica: la gestión de la privacidad y seguridad de la información se revisará, evaluará y actualizará periódicamente para mantener su efectividad frente a la evolución de los riesgos.

— Responsabilidad determinada: se determinarán las personas responsables de la información, del servicio, del sistema y de la seguridad, con las atribuciones que esta Política establece.

— Servicio a la ciudadanía: la privacidad y seguridad de la información estará orientada a la prestación de servicios de confianza a la ciudadanía en sus relaciones con el SES.

— Vigilancia continua: se establecerán mecanismos jurídicos, técnicos y organizativos para la detección de actividades o comportamientos anómalos y su oportuna respuesta.

— Mejora continua: existirá un proceso permanente de revisión y actualización de las medidas de seguridad conforme a su efectividad y a la evolución de los riesgos.

— Cultura de la privacidad y la seguridad: se promoverán los conocimientos, percepciones, actitudes y madurez en esta materia de los diversos actores que intervienen en el ámbito del SES.

— Seguridad por defecto y desde el diseño: los sistemas se diseñarán y configurarán para garantizar la seguridad por defecto, proporcionando la funcionalidad mínima necesaria para prestar el servicio para el que fueron concebidos.

— Cumplimiento de las obligaciones profesionales de secreto: se establecerán medidas, normas y procedimientos internos que garanticen el cumplimiento de las obligaciones profesionales de secreto de las personas con acceso a datos personales, principalmente, de aquellos que tengan acceso a categorías especiales de datos.

4.3. Objetivos.

Constituyen objetivos de la privacidad y seguridad de la información del SES:

— Garantizar la calidad y protección de la información y de los servicios.

— Lograr la plena concienciación de las personas usuarias respecto de la seguridad de la información y la protección de datos personales.

— Gestionar los activos de información bajo un inventario, una clasificación y una asignación a una persona responsable.

— Implementar medidas de seguridad ligadas a las personas, de modo que quien acceda o pueda acceder a los activos de información conozca sus responsabilidades y se reduzca el riesgo derivado de un uso indebido.

— Desplegar y controlar la seguridad física, de forma que los activos de información se encuentren en áreas seguras, protegidas por controles de acceso adecuados a su criticidad y frente a amenazas físicas o ambientales.

— Establecer la seguridad en la gestión de las comunicaciones y operaciones, protegiendo la información transmitida conforme a su nivel de sensibilidad y criticidad.

— Limitar el acceso a los activos mediante mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo, asegurando la trazabilidad del acceso y auditando su uso.

— Controlar la adquisición, desarrollo y mantenimiento de los sistemas de información en todas las fases de su ciclo de vida, garantizando su seguridad por defecto.

— Mantener el control y la seguridad en la incorporación de nuevos componentes y tecnologías, en particular en los servicios de telemedicina y de información electrónica.

— Gestionar los incidentes de seguridad y las brechas de datos personales para su correcta identificación, registro, resolución y notificación.

— Garantizar la prestación continuada de los servicios de acuerdo con las necesidades de nivel de cada uno de ellos.

— Proteger la información personal mediante las medidas técnicas y organizativas apropiadas a los riesgos derivados del tratamiento, y facilitar el ejercicio de los derechos de las personas interesadas.

— Mejorar los procesos de identidad digital de las personas implicadas en los procesos sanitarios.

— Adoptar las medidas necesarias para el cumplimiento de la normativa vigente en materia de seguridad de la información y protección de datos personales, y acreditar dicho cumplimiento.

4.4. Requisitos mínimos.

El SES establece los siguientes requisitos mínimos, que han de guiar su marco regulador:

— Organización e implantación del proceso de seguridad: la seguridad compromete a todo el personal dentro del alcance definido, diferenciando roles y responsabilidades conforme a esta Política.

— Análisis y gestión de los riesgos: el SES gestionará sus riesgos empleando metodologías reconocidas. Las medidas adoptadas para mitigarlos o suprimirlos deberán estar justificadas y ser proporcionadas, considerando asimismo el tratamiento de datos personales.

— Evaluación de impacto en la privacidad: cuando se traten datos personales que, por su naturaleza, alcance, contexto o fines, entrañen un alto riesgo para los derechos y libertades de las personas, se realizará, antes del tratamiento, una evaluación de impacto relativa a la protección de datos.

— Gestión de personal: el personal comprendido en el alcance será informado de sus deberes y obligaciones en materia de seguridad y protección de datos.

— Profesionalidad: el personal dispondrá de la capacitación o información necesaria para el desarrollo de su puesto en condiciones de seguridad. Quienes desarrollen funciones en el ámbito de la privacidad y seguridad de la información dispondrán de la capacitación adecuada, exigible igualmente al personal de terceros que preste servicios en este ámbito.

— Autorización y control de los accesos: el acceso a los sistemas estará controlado y limitado. Cada usuario, proceso, dispositivo, aplicación u otro sistema que acceda a la información estará identificado y debidamente autorizado para el acceso exclusivo a las funciones permitidas.

— Protección de las instalaciones: las instalaciones contarán con medidas de seguridad física adecuadas a la información que tratan y a los servicios que prestan, y las infraestructuras críticas con los instrumentos de protección específicos previstos en la normativa vigente.

— Adquisición de productos y contratación de servicios: se atenderá de manera proporcionada a la categoría y al nivel de seguridad determinados para los sistemas afectados, exigiendo en consecuencia la conformidad con el ENS y, en su caso, otras certificaciones, salvo que las exigencias de proporcionalidad no lo justifiquen a juicio del Responsable de Seguridad. Serán objeto de especial estudio las soluciones de ciberseguridad, la interconexión con entidades externas y la prestación de servicios en la nube.

— Seguridad por defecto y mínimo privilegio: los sistemas se diseñarán y configurarán de forma que proporcionen la funcionalidad e información mínimas requeridas, asegurando que una utilización insegura requiera un acto consciente por parte de la persona usuaria.

— Integridad y actualización del sistema: el estado de seguridad de los sistemas se mantendrá actualizado conforme a las especificaciones de los fabricantes y a las vulnerabilidades que les afecten, sirviendo dicho estado como entrada a las actividades de gestión de riesgos. Las actualizaciones que afecten al estado de seguridad se ejecutarán conforme al proceso de autorización aprobado.

— 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, aplicando las medidas que correspondan a la naturaleza del soporte.

— Interconexión de sistemas: se protegerán las comunicaciones entre sistemas de información y con sistemas externos, en particular los puntos de interconexión y, especialmente, las comunicaciones que se realicen a través de redes públicas.

— Registro de actividad: con plenas garantías de los derechos al honor, a la intimidad personal y familiar y a la propia imagen, y conforme a la normativa de protección de datos, de función pública o laboral y demás disposiciones aplicables, se registrarán las actividades de las personas usuarias, 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.

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

— Continuidad de la actividad: la continuidad de las operaciones se basará en la formalización y prueba de los procesos técnicos que la soportan.

— Mejora continua del proceso de seguridad: la gestión de la privacidad y seguridad de la información estará sometida a un ciclo de mejora continua, coherente con el principio de reevaluación periódica.

5. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

5.1. Criterios de organización.

Conforme a lo establecido en el Esquema Nacional de Seguridad y a las pautas de las guías CCN-STIC, la organización de la seguridad de los sistemas de información del SES responde a los siguientes criterios:

— La seguridad de los sistemas de información compromete a todos los miembros de la organización.

— Se designarán los roles de seguridad previstos en el artículo 11 del ENS: Responsable de la Información, Responsable del Servicio, Responsable de la Seguridad y Responsable del Sistema, sin perjuicio de otros que resulten necesarios.

— Los roles se ejercerán bajo el principio de diferenciación de responsabilidades y pleno respeto a la atribución de cada uno de ellos, disponiéndose de mecanismos adecuados de coordinación y, en su caso, de resolución de conflictos.

— La responsabilidad de la seguridad de los sistemas estará diferenciada de la responsabilidad sobre su explotación.

— El Comité de Gestión y Coordinación de Seguridad de la Información constituye la estructura organizativa de carácter estratégico para la toma de decisiones en materia de privacidad y seguridad de la información, y ostenta la función de dirección de la seguridad en la organización.

— Podrán crearse órganos, subórganos y grupos de trabajo con funciones delegadas, entre los que distribuir aquellas funciones estratégicas, organizativas y tácticas que sus titulares consideren.

— La presidencia del Comité de Gestión y Coordinación de Seguridad de la Información será ejercida por la persona titular de la Dirección Gerencia, con la asunción formal de la responsabilidad de los actos.

5.2. Modelo de gobernanza.

La PPSI SES establece un modelo de gobernanza centralizado, adaptado a la naturaleza asistencial, la distribución territorial y la criticidad de los servicios del SES, estructurado en tres niveles:

— Nivel de gobierno y dirección estratégica: el Comité de Gestión y Coordinación de Seguridad de la Información (CGCSI).

— Nivel de coordinación, supervisión y cumplimiento: la Unidad de Gobernanza y Cumplimiento Normativo de la Ciberseguridad (UGCNC).

— Nivel operativo especializado: la Oficina de Ciberseguridad (OC), con el apoyo del Centro de Operaciones de Ciberseguridad (COC) y de las restantes capacidades técnicas que se determinen.

La Dirección General de Salud Digital, a la que corresponde el establecimiento, desarrollo y supervisión de las medidas de seguridad en materia de tecnologías de la información y comunicaciones, actúa como nexo directivo del modelo. La Oficina de Ciberseguridad se configura como unidad diferenciada de las unidades responsables del desarrollo, explotación, operación y mantenimiento de los sistemas de información, y ejerce sus funciones con autonomía funcional y de criterio respecto de aquellas, en los términos previstos en el apartado 5.7.

La estructura organizativa asigna facultades y competencias diferenciadas y establece los mecanismos de coordinación, reporte, escalado y resolución de conflictos. El despliegue

territorial podrá requerir puntos locales de seguridad y responsables delegados, que se formalizarán en los correspondientes instrumentos de designación. Las dependencias, interconexiones y flujos con otras entidades públicas, proveedores y organizaciones territoriales se documentarán y gestionarán conforme a esta Política y a su marco de desarrollo.

Los órganos y unidades previstos en esta Política tienen carácter interno y ejercen funciones de gobierno, coordinación, supervisión y ejecución en materia de privacidad y seguridad de la información, sin que se les atribuyan competencias resolutorias con efectos frente a terceros. Su constitución, composición y régimen de designación se formalizarán mediante resolución de la Dirección Gerencia, conforme al artículo 4, letra s), de los Estatutos del Servicio Extremeño de Salud

5.3. Roles de seguridad.

Los roles de seguridad se desplegarán en todos los niveles jerárquicos del SES, desde la dirección hasta los niveles operativos, mediante la designación formal de las personas responsables descritas en esta Política. Las personas designadas asumirán las funciones correspondientes a su rol en relación con la gestión de la seguridad de la información, la gestión de la seguridad operativa, la gestión de riesgos, la gestión de incidentes y la resiliencia del sistema, la mejora continua y la concienciación y formación.

5.3.1. Responsable de la Información.

Determina los requisitos de seguridad de la información tratada. Este rol será ejercido por la persona titular de la Dirección Gerencia del SES.

Serán funciones del Responsable de la Información:

— Determinar la valoración de la información conforme a los criterios establecidos en la normativa en vigor.

— Determinar los requisitos de seguridad de la información.

— Dictaminar sobre los derechos de acceso a la información.

— Aceptar los niveles de riesgo residual que afectan a la información.

— Comunicar al Responsable de la Seguridad cualquier variación respecto de la información de la que es responsable, especialmente la incorporación de nueva información a su cargo.

5.3.2. Responsable del Servicio.

Determina los requisitos de seguridad de los servicios prestados. Las personas titulares de las Direcciones Generales del SES ejercerán este rol respecto de los servicios comprendidos en sus competencias. La persona titular de la Dirección General de Salud Digital lo ejercerá respecto de los servicios digitales, tecnológicos e instrumentales incluidos en su ámbito competencial.

Serán funciones del Responsable del Servicio:

— Determinar la valoración de los servicios conforme a los criterios establecidos en la normativa en vigor.

— Determinar los requisitos de seguridad de los servicios.

— Dictaminar sobre los derechos de acceso a los servicios.

— Aceptar los niveles de riesgo residual que afectan a los servicios.

— Determinar el impacto de una indisponibilidad de los servicios en las actividades del SES.

— Comunicar al Responsable de la Seguridad cualquier variación respecto de los servicios de los que es responsable, especialmente la incorporación de nuevos servicios a su cargo.

5.3.3. Responsable de la Seguridad.

Determina las decisiones necesarias para satisfacer los requisitos de seguridad de la información y de los servicios, supervisa la implantación de las medidas precisas para garantizar que dichos requisitos se satisfacen y reporta sobre estas cuestiones. Este rol será ejercido por la persona que dirija la Oficina de Ciberseguridad.

El Responsable de la Seguridad será distinto del Responsable del Sistema, sin que exista dependencia jerárquica entre ambos. La responsabilidad de la seguridad estará diferenciada de la responsabilidad sobre la explotación de los sistemas, y aquel ejercerá sus funciones con autonomía funcional y de criterio respecto de las funciones de desarrollo, explotación, operación y mantenimiento de los sistemas de información.

Cuando corresponda, podrá declararse a la persona física que ostente este rol como responsable o representante del SES en la aplicación de las medidas destinadas a gestionar los riesgos de ciberseguridad derivados de la normativa europea y nacional en la materia.

Serán funciones del Responsable de la Seguridad:

— Desarrollar las funciones de supervisión de la seguridad, en colaboración con el Responsable del Sistema.

— Dirigir la Oficina de Ciberseguridad y remitir reportes al Comité de Gestión y Coordinación de Seguridad de la Información a través de la Unidad de Gobernanza y Cumplimiento Normativo de la Ciberseguridad.

— Determinar las decisiones y acciones necesarias para cumplir con los requisitos de seguridad de la información y de los servicios.

— Mantener y verificar el nivel adecuado de seguridad de la información manejada y de los servicios prestados.

— Identificar las medidas de seguridad y determinar las configuraciones de seguridad, considerando en su caso medidas adicionales a las requeridas por el ENS o compensatorias de estas, habida cuenta del estado de la tecnología, la naturaleza de la información tratada, los servicios prestados y los riesgos a que están expuestos los sistemas.

— Desarrollar, documentar y aprobar formalmente la Declaración de Aplicabilidad.

— Designar a las personas responsables de la ejecución de los procesos de análisis de riesgos y elevar las propuestas de tratamiento del riesgo.

— Proporcionar asesoramiento para la determinación de la valoración y categorización del sistema, en colaboración con el Responsable del Sistema.

— Participar en la elaboración e implantación de los planes de mejora de la seguridad y, en su caso, de los planes de continuidad, procediendo a su validación.

— Asegurar que el personal responsable elabora la documentación del sistema y, en su caso, custodiarla debidamente.

— Gestionar las revisiones internas y externas del sistema y los procesos de certificación, presentando las conclusiones al Comité de Gestión y Coordinación de Seguridad de la Información a través de la Unidad de Gobernanza y Cumplimiento Normativo de la Ciberseguridad y al Responsable del Sistema.

— Elevar a dicho Comité, a través de la citada Unidad, la aprobación de cambios y otros requisitos del sistema.

— Aprobar los documentos técnicos y operativos de seguridad en los términos previstos en el capítulo 7 de esta Política.

— Promover la formación y la concienciación en materia de privacidad y seguridad de la información.

— Garantizar la notificación y coordinación con el CSIRT competente y, cuando proceda, con la autoridad de control correspondiente, ante cualquier incidente que afecte o pueda afectar de forma significativa a la seguridad de la información o a la continuidad de los servicios esenciales, de acuerdo con los plazos y requisitos establecidos en la normativa aplicable. En su caso, informar a las personas destinatarias de los servicios sanitarios sobre el incidente, las medidas adoptadas o cualquier información que se considere relevante.

Con carácter general, los informes, propuestas y reportes del Responsable de la Seguridad se canalizarán a través de la UGCNC, sin que puedan ser modificados ni demorados en su tramitación. No obstante, podrá elevar directamente a la persona titular de la Dirección General de Salud Digital las cuestiones que, por su gravedad, urgencia, impacto potencial, afectación a servicios esenciales, posible incumplimiento normativo, conflicto de responsabilidades o necesidad de decisión directiva inmediata, no deban demorarse, y proponer, cuando proceda, su elevación al CGCSI o a su Presidencia.

El Responsable de la Seguridad podrá encomendar a otras personas, órganos o entidades la ejecución material de las funciones que tiene atribuidas, incluida su prestación mediante servicios externos, sin que ello suponga en ningún caso delegación ni transferencia de la responsabilidad inherente al rol. En particular, no serán delegables la aprobación de las medidas de seguridad generales, complementarias o compensatorias, la aprobación de la Declaración de Aplicabilidad, la validación de las propuestas de tratamiento del riesgo, la conformidad sobre la supervisión del sistema, la aprobación de los procedimientos operativos de seguridad y la valoración de los resultados de los análisis y auditorías técnicas de seguridad.

El Responsable de la Seguridad podrá designar personas con funciones de administración de la seguridad, a las que corresponderá:

— La ciberinteligencia y la vigilancia activa.

— La gestión, configuración y actualización del hardware y software en los que se basan los mecanismos y servicios de seguridad.

— Asegurar que los controles de seguridad establecidos se cumplen estrictamente.

— Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos y por los mecanismos de auditoría técnica.

— Informar al Responsable de la Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.

— Colaborar con los administradores del sistema en la investigación y resolución de los incidentes de seguridad, desde su detección hasta su cierre.

En los aspectos relativos a la seguridad lógica que le correspondan, el Responsable de la Seguridad podrá integrar las funciones de seguridad de otros roles que resulten necesarios por imperativo legal o por normativas sectoriales que contemplen obligaciones específicas para los órganos, organismos o unidades del sector público implicados en los servicios sanitarios, pudiendo asumir asimismo las funciones de coordinación con el CSIRT correspondiente.

5.3.4. Responsable del Sistema.

Se encarga de implantar la seguridad en el sistema y de supervisar su operación diaria. Este rol será ejercido por la persona titular de la Subdirección de Sistemas de Información.

Serán funciones del Responsable del Sistema:

— Desarrollar las funciones operativas de la seguridad, en colaboración con el Responsable de la Seguridad.

— Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluidas sus especificaciones, instalación y verificación de su correcto funcionamiento, elaborando los procedimientos operativos necesarios.

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

— Implantar las medidas técnicas de seguridad aprobadas en los planes de tratamiento de riesgos.

— Cerciorarse de que las medidas específicas de seguridad se integran adecuadamente en el marco general de seguridad.

— Colaborar en el desarrollo de la normativa para el uso de las tecnologías de la información y las comunicaciones y en la redacción de los planes de contingencia, realizando las comprobaciones necesarias para verificar su efectividad.

— Suspender el acceso a la información o la prestación del servicio cuando tenga conocimiento de deficiencias graves de seguridad, informando de inmediato al Responsable de la Seguridad.

— Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el Responsable de la Seguridad.

— Garantizar que los dispositivos que abandonen las instalaciones mantienen la seguridad necesaria conforme a la información que manejan.

— Analizar las conclusiones de las auditorías, revisiones internas y autoevaluaciones elevadas por el Responsable de la Seguridad, y proponer las medidas correspondientes.

Cuando la complejidad del sistema lo justifique, el Responsable del Sistema podrá designar responsables del sistema delegados, con dependencia funcional directa de aquel, responsables en su ámbito de las acciones que les delegue, en particular: medidas de identificación, autenticación y asignación de accesos; monitorización y seguimiento de actividades; interconexiones y seguimiento de autorizaciones de flujos; gestión de bastionados; parcheados y actualizaciones no críticas; cambios menores o preautorizados; y entradas en producción de servicios no críticos o previamente desplegados en entornos de preproducción.

Asimismo, podrá designar administradores del sistema, a los que corresponderá:

— La gestión de las autorizaciones concedidas a las personas usuarias, en particular los privilegios, incluyendo la monitorización de la actividad desarrollada y su correspondencia con lo autorizado.

— Aprobar los cambios en la configuración vigente del sistema de información.

— Asegurar que se aplican los procedimientos aprobados para manejar el sistema.

— Supervisar las instalaciones de componentes, su mantenimiento, modificaciones y mejoras, para asegurar que la seguridad no se compromete y que se ajustan a las autorizaciones pertinentes.

— Informar al Responsable del Sistema de cualquier anomalía.

— Colaborar con las personas con funciones de administración de la seguridad en la investigación y resolución de incidentes.

5.3.5. Responsable del Tratamiento.

El SES, como organismo autónomo dotado de personalidad jurídica propia, tendrá la condición de responsable del tratamiento, en los términos establecidos en el artículo 4.7 del Reglamento (UE) 2016/679, respecto de aquellos tratamientos cuyos fines y medios determine en el ejercicio de las competencias que tiene legalmente atribuidas. La persona titular de la Dirección Gerencia ejercerá las competencias de dirección y representación del organismo que le atribuyan sus Estatutos y las restantes normas organizativas aplicables, incluidas las relacionadas con el cumplimiento de las obligaciones que corresponden al organismo como responsable del tratamiento, sin perjuicio de la distribución interna de funciones y competencias que se realizará mediante normas organizativas internas, resoluciones de atribución o delegación u otros procedimientos internos.

La Dirección General de Salud Digital ejercerá, dentro de la organización del SES, las funciones que los Estatutos del organismo le atribuyen en materia de tratamiento de datos personales, sin perjuicio de la condición del SES como responsable del tratamiento, de las funciones independientes del Delegado o Delegada de Protección de Datos y del régimen aplicable a los encargados del tratamiento conforme al RGPD. El alcance y articulación de estas funciones se desarrollarán conforme al marco normativo aplicable y a los criterios de los órganos competentes en materia jurídica y de protección de datos.

5.3.6. Delegado o Delegada de Protección de Datos.

Corresponde al delegado o delegada de protección de datos informar y asesorar al Servicio Extremeño de Salud, a sus órganos directivos y al personal que participe en operaciones de tratamiento sobre las obligaciones que les incumben en materia de protección de datos personales, así como supervisar el cumplimiento del Reglamento General de Protección de Datos, de la Ley Orgánica 3/2018 y de las políticas, normas y procedimientos internos adoptados en esta materia. Asimismo, le corresponderá asesorar, cuando le sea solicitado, acerca de las evaluaciones de impacto relativas a la protección de datos y supervisar su realización; cooperar con la autoridad de control competente y actuar como punto de contacto con esta; y atender las consultas y reclamaciones que le dirijan las personas interesadas en relación con el tratamiento de sus datos personales y el ejercicio de sus derechos. Una normativa interna regulará su funciones y obligaciones de acuerdo a lo establecido en el RGPD.

El delegado o delegada de protección de datos será designado mediante el procedimiento establecido al efecto, atendiendo a sus cualidades profesionales y, en particular,

a sus conocimientos especializados en Derecho y en la práctica de la protección de datos. Sus funciones podrán ser desempeñadas por personal del SES o por una persona física o jurídica externa, mediante el correspondiente contrato de servicios.

El delegado o delegada de protección de datos quedará integrado en la UGCNC en los términos establecidos en la normativa organizativa del SES. Esta integración no afectará a su independencia funcional ni podrá suponer la recepción de instrucciones respecto del desempeño de sus funciones. Reportará directamente al nivel jerárquico superior del SES y no podrá ser removido, sancionado ni sufrir perjuicio alguno por el correcto desempeño de sus tareas, sin perjuicio de las responsabilidades que pudieran derivarse de dolo o negligencia grave.

5.4. Órganos de la seguridad de la información.

5.4.1. Comité de Gestión y Coordinación de Seguridad de la Información.

El CGCSI es el máximo órgano especializado de gobierno y dirección estratégica de la privacidad y seguridad de la información del SES. Coordina los restantes órganos del modelo y adopta las decisiones que le correspondan conforme a esta Política.

Composición.

— Presidencia: la persona titular de la Dirección Gerencia.

— Secretaría: la persona titular de la Dirección General de Salud Digital.

— Vocalías permanentes: las personas titulares de las Direcciones Generales del SES.

El Responsable de la Seguridad y el Delegado o Delegada de Protección de Datos serán convocados a todas las sesiones y asistirán a ellas con voz y sin voto, pudiendo solicitar la inclusión de asuntos en el orden del día. Su inasistencia no afectará a la válida constitución del órgano ni a la adopción de acuerdos.

Podrán asimismo asistir, con voz y sin voto, el Responsable del Sistema, las personas responsables de proyectos o servicios, personas expertas y representantes de otras entidades o terceros, cuando sean convocadas por la Presidencia, por iniciativa propia o a propuesta de cualquier miembro.

Funciones.

— Promover e impulsar la dotación de los recursos y medios necesarios para el cumplimiento de la PPSI SES.

— Proponer a la Dirección Gerencia la aprobación de la Estrategia, de la PPSI SES y de los planes que requieran decisión superior.

— Aprobar las normas de segundo nivel del marco documental, los planes corporativos de mejora y los criterios transversales en materia de privacidad y seguridad.

— Coordinar los esfuerzos de las distintas áreas y asegurar su alineamiento con la Estrategia.

— Recibir los reportes de la UGCNC y conocer el estado general de riesgos, incidentes, auditorías, cumplimiento y mejora continua.

— Priorizar actuaciones cuando los recursos sean limitados y resolver los conflictos de responsabilidad que se le eleven.

— Promover auditorías periódicas y velar por la seguridad y la protección de datos desde el diseño y por defecto.

Ordenar la publicación y difusión del marco regulador cuando corresponda.

Régimen de funcionamiento.

El CGCSI se reunirá, al menos, una vez al año y cuantas veces lo exijan sus fines. Los acuerdos se adoptarán por consenso de sus miembros permanentes y, de no alcanzarse, decidirá la Presidencia, haciéndose constar en acta las posiciones discrepantes. Podrá crear grupos de trabajo y convocar sesiones extraordinarias. De cada sesión se extenderá acta con indicación de lugar, fecha, asistentes, orden del día, síntesis de las deliberaciones, acuerdos adoptados y asuntos cuya constancia sea solicitada.

5.4.2. Unidad de Gobernanza y Cumplimiento Normativo de la Ciberseguridad.

La UGCNC es el órgano de coordinación, supervisión y cumplimiento del modelo de gobernanza. Presta soporte, asesoramiento e información al CGCSI y coordina la ejecución de sus decisiones.

Composición.

— Presidencia: la persona titular de la Dirección General de Salud Digital.

— Secretaría: el Responsable de la Seguridad, que actuará además como enlace con la Oficina de Ciberseguridad.

— Vocalías permanentes: la persona titular de la Subdirección de Sistemas de Información, el Delegado o Delegada de Protección de Datos y las personas formalmente designadas como responsables del sistema delegados.

Podrán asistir puntos de contacto con proveedores, responsables de proyectos, personal experto, consultores y otros perfiles cuya participación resulte necesaria.

Funciones.

— Dar soporte y asesoramiento al CGCSI y coordinar la ejecución de sus acuerdos.

— Desarrollar, mantener, supervisar y proponer la actualización del marco regulador.

— Elaborar o actualizar la documentación de primer y segundo nivel y elevarla al CGCSI cuando corresponda.

— Aprobar los documentos de tercer nivel de alcance general o transversal, en los términos previstos en el capítulo 7.

— Recibir y analizar los reportes sobre riesgos, incidentes, auditorías, cumplimiento y planes de mejora, elevando al CGCSI las cuestiones de naturaleza estratégica.

— Diseñar y coordinar programas horizontales y proyectos corporativos de seguridad TIC.

— Aprobar la creación, modificación o extinción de grupos de trabajo.

— Coordinar la formación y cualificación de administradores, operadores y personas usuarias.

Régimen de funcionamiento.

La UGCNC se reunirá, al menos, trimestralmente y cuantas veces lo exijan sus fines. Los acuerdos se adoptarán por consenso de sus miembros permanentes y, de no alcanzarse, decidirá la Presidencia, haciéndose constar en acta las posiciones discrepantes; cuando la discrepancia afecte a la aceptación de riesgos o a la atribución de responsabilidades, el asunto se elevará al CGCSI. Podrá crear grupos de trabajo y convocar sesiones extraordinarias. De cada sesión se extenderá acta.

5.4.3. Oficina de Ciberseguridad.

La Oficina de Ciberseguridad es la unidad operativa especializada que apoya al Responsable de la Seguridad y ejecuta las funciones de seguridad, cumplimiento, gestión de riesgos, monitorización, respuesta y mejora continua.

La Oficina de Ciberseguridad se configura como unidad diferenciada respecto de las unidades encargadas del desarrollo, explotación, operación y mantenimiento de los sistemas de información, y ejerce sus funciones con autonomía funcional y de criterio, en los términos y con las garantías previstas en el apartado 5.7. Su adscripción se determinará en la resolución de constitución de los órganos.

Composición.

— Dirección: la persona designada como Responsable de la Seguridad, que actuará como enlace con la UGCNC.

— Integrantes: las personas designadas para ejercer funciones de administración de la seguridad mediante recursos internos y, cuando proceda, servicios externos.

La participación de personal externo no supondrá delegación de la responsabilidad atribuida al Responsable de la Seguridad ni conferirá capacidad de decisión reservada a los roles previstos en el ENS.

Funciones.

— Gestionar y coordinar los incidentes de seguridad conforme al procedimiento vigente.

— Ejecutar la adecuación, implantación y gestión de la conformidad con el ENS.

— Analizar y gestionar los riesgos y proponer los planes de tratamiento y mejora.

— Elaborar y mantener la documentación de seguridad y elevarla para su aprobación cuando corresponda.

— Monitorizar el estado de seguridad, los riesgos residuales, las vulnerabilidades y el desempeño de los procesos de gestión de incidentes.

— Desarrollar acciones de ciberinteligencia, cibervigilancia, formación y concienciación.

— Coordinar operativamente el COC y supervisar los servicios de seguridad prestados al SES.

Régimen de funcionamiento.

La Oficina desarrollará sus funciones de forma continuada, en pleno o mediante grupos de trabajo, dejando constancia documental de sus actuaciones y acuerdos.

5.4.4. Centro de Operaciones de Ciberseguridad.

El COC constituye una capacidad operativa especializada del SES, que podrá prestarse mediante recursos propios, compartidos o externalizados, destinada a la vigilancia, detección, prevención, análisis y respuesta frente a amenazas e incidentes.

Serán funciones del COC:

— Vigilancia, monitorización y correlación de eventos de seguridad.

— Inteligencia de amenazas, búsqueda proactiva de amenazas y cibervigilancia.

— Gestión de vulnerabilidades y análisis de la superficie de exposición.

— Apoyo a la respuesta ante incidentes, análisis forense y alerta temprana.

— Supervisión de dispositivos y servicios de defensa y apoyo a las medidas de seguridad.

— Cualesquiera otras que se le asignen en la normativa o procedimientos específicos.

La dirección estratégica del COC corresponde a la Dirección General de Salud Digital. El seguimiento contractual corresponde a la Subdirección de Sistemas de Información, que verificará los niveles de servicio, recursos, hitos y obligaciones contractuales. La dirección operativa y técnica de los servicios prestados al SES corresponde al Responsable de la Seguridad, con el apoyo de la Oficina de Ciberseguridad, a quien compete determinar las prioridades operativas, coordinar la gestión de alertas e incidentes, supervisar la prestación y elevar indicadores, riesgos y propuestas de mejora.

Las unidades y servicios implicados en la prestación de servicios deberán coordinarse con la Oficina de Ciberseguridad en la definición y aplicación de las medidas y colaborar con el COC en su operativa diaria.

5.4.5. Órgano de Auditoría Técnica.

Podrá constituirse un Órgano de Auditoría Técnica independiente para la realización de auditorías de conformidad de los sistemas, que podrá asumir las supervisiones relativas a las medidas desplegadas para gestionar los riesgos de ciberseguridad de los sistemas de redes y de información utilizados para prestar los servicios.

Deberá preservar su independencia respecto del resto de la estructura técnica y de seguridad, así como la ausencia de conflicto de intereses entre los elementos auditor

y auditado. Cuando sea constituido, se procederá a su acreditación conforme a las normas establecidas por la autoridad competente y realizará las auditorías periódicas según los criterios y el modelo que se establezcan.

La constitución del Órgano de Auditoría Técnica no exime del cumplimiento del régimen de auditoría de la seguridad y de determinación de la conformidad previsto en el Esquema Nacional de Seguridad y en sus instrucciones técnicas de seguridad.

5.5. Otros roles.

Podrán considerarse otros roles de seguridad que resulten necesarios por imperativo legal o por normas particulares que detallen obligaciones específicas para los órganos y entidades del sector público implicados en los servicios sanitarios.

En particular, podrá designarse una persona responsable de proveedores sanitarios, con atribuciones en los procesos de homologación, seguimiento, control y contacto con los proveedores de servicios asistenciales con criticidad en la cadena de suministro. Este perfil será designado, en su caso, de entre los miembros de la UGCNC.

5.6. Procedimientos de designación y renovación.

Los roles y la pertenencia a los órganos descritos en esta Política se formalizarán mediante acta o instrumento de designación aprobado por el órgano competente. Cuando un rol se atribuya por razón del cargo, esta Política identificará el cargo y el acta identificará además a la persona titular.

Los nombramientos se revisarán, al menos, cada dos años y siempre que concurra alguna circunstancia que pueda afectar al adecuado ejercicio de las funciones, tales como la vacante del puesto, cambios organizativos, modificación de funciones o competencias, cambios normativos, situaciones de incompatibilidad o conflicto de intereses, o cualquier otra causa debidamente justificada.

En caso de vacante, cese, ausencia prolongada o incapacidad temporal se formalizará de manera inmediata un régimen de suplencia o sustitución que garantice la continuidad de las funciones de seguridad. El nuevo nombramiento se formalizará sin dilación indebida.

El cambio de la persona titular de un cargo no exigirá modificar esta Política cuando el rol esté atribuido por razón de dicho cargo, sin perjuicio de la actualización del acta o instrumento de designación.

5.7. Diferenciación de responsabilidades y resolución de conflictos.

Se diferenciarán las figuras de Responsable de la Información, Responsable del Servicio, Responsable de la Seguridad y Responsable del Sistema. La responsabilidad de la seguridad estará diferenciada de la responsabilidad sobre la explotación, y el Responsable de la Seguridad será distinto del Responsable del Sistema.

Quien ejerza el rol de Responsable de la Seguridad no podrá ser designado responsable del sistema delegado ni administrador del sistema, ni asumir funciones de desarrollo, explotación, operación o mantenimiento de los sistemas de información. Ningún puesto integrado en la Oficina de Ciberseguridad podrá tener atribuidas simultáneamente funciones de administración, explotación u operación de los sistemas sobre los que aquella ejerza funciones de supervisión.

Los mecanismos ordinarios de coordinación se articularán a través de la UGCNC. Los conflictos que no puedan resolverse en ese nivel se elevarán al CGCSI. Las cuestiones urgentes o graves podrán escalarse conforme al procedimiento previsto para el Responsable de la Seguridad.

Cuando el Responsable de la Seguridad discrepe de una decisión que afecte al estado de seguridad de la información o de los servicios, hará constar su discrepancia de forma motivada y documentada. La asunción del riesgo derivado corresponderá al Responsable de la Información o al Responsable del Servicio afectado, según su ámbito, mediante aceptación expresa del riesgo residual, que quedará debidamente registrada.

5.8. Obligaciones del personal.

Todas las personas que utilicen la información, los servicios o los sistemas de tratamiento sometidos a esta Política tienen la obligación de conocer y respetar su contenido y el marco normativo de desarrollo.

Todo el personal del SES comprendido dentro del ámbito del ENS atenderá a las sesiones de concienciación en materia de seguridad y protección de datos cuando le sea requerido. Se establecerá un programa de concienciación continua para atender a todo el personal, en particular al de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas de información recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir la responsabilidad, tanto si se trata de la primera asignación como de un cambio de puesto de trabajo o de responsabilidades.

6. SISTEMA DE GESTIÓN DE LA PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN.

El SES dispondrá de un sistema de gestión que incluya la planificación, la organización y el control de los recursos de privacidad y seguridad de la información, sometido a mejora continua y a actualización y aprobación periódicas.

6.1. Protección de datos personales.

6.1.1. Responsabilidad proactiva.

El responsable del tratamiento deberá garantizar el cumplimiento de la normativa de protección de datos personales y tener la capacidad de demostrarlo. A tal fin resultará necesaria la concienciación y formación del personal que realice tratamientos, de manera que conozca sus obligaciones y colabore en la recopilación y almacenamiento de evidencias de cumplimiento.

— Detección de la necesidad: la realización de un tratamiento de datos personales estará precedida de un análisis de necesidad, idoneidad y proporcionalidad, cuya conclusión debe ser que el tratamiento resulta imprescindible para cumplir con las funciones específicas atribuidas.

— Identificación y caracterización de las actividades de tratamiento: una vez detectada la necesidad, la actividad será determinada y caracterizada con precisión, conforme a los principios de protección de datos.

— Registro de Actividades de Tratamiento: el SES mantendrá actualizado el Registro de Actividades de Tratamiento, con toda la información exigida por la normativa vigente, y será accesible al público de forma clara, permanente y fácilmente localizable a través del apartado de protección de datos del portal web corporativo del SES.

— Información del tratamiento: se cumplirá con el deber de información facilitando el acceso a la misma de forma fácil e intuitiva, salvo en los supuestos exceptuados por la normativa reguladora.

— Ejercicio de derechos: el SES mantendrá canales habilitados para el ejercicio de los derechos de las personas interesadas y para proporcionar la información que proceda de manera concisa, transparente, inteligible y de fácil acceso en los plazos previstos, informando del resto de canales habilitados y de la posibilidad de acudir a la tutela de la autoridad de control.

— Transferencias internacionales: solo podrán realizarse transferencias internacionales a terceros países cuando concurran las garantías previstas normativamente. El SES velará por que el tratamiento de datos personales en su ámbito de responsabilidad se produzca cumpliendo dichas garantías.

6.1.2. Privacidad desde el diseño y por defecto.

El principio de privacidad desde el diseño y por defecto obliga a considerar la protección de datos desde la concepción y el diseño de los procesos y procedimientos.

El SES determinará e implementará las medidas técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo sobre las actividades de tratamiento, incluyendo, entre otras y en función del grado de control necesario:

— El mínimo privilegio en el acceso a los datos personales, garantizando el acceso únicamente a la información imprescindible para el puesto de trabajo concreto.

— La seudonimización y el cifrado de los datos personales.

— La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia de manera continua en los sistemas y servicios de tratamiento.

— La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.

— Un proceso de verificación, evaluación y valoración regulares de la efectividad de las medidas técnicas y organizativas.

6.1.3. Gestión de brechas de seguridad de los datos personales.

El SES habilitará mecanismos que posibiliten la detección temprana y proactiva de las situaciones que puedan suponer una brecha de seguridad de los datos personales, y establecerá procedimientos ágiles para su investigación, análisis, identificación y adopción de medidas de contención y mitigación, así como para la eliminación de sus causas.

El SES no demorará el proceso de decisión relativo a la notificación a la autoridad de control ni, en su caso, a la comunicación a las personas interesadas, adoptando las medidas necesarias para garantizar ambas conforme a los procedimientos establecidos por la autoridad de control.

6.1.4. Relaciones con terceros en el ámbito de la privacidad.

El SES velará por que el tratamiento de datos personales en el marco de la colaboración con entidades públicas o privadas se produzca en cumplimiento de los principios y garantías previstos en la normativa aplicable y, especialmente, bajo las premisas de mínimo privilegio y necesidad de conocer.

Los accesos estarán precedidos del análisis del supuesto concreto que determine la responsabilidad o corresponsabilidad de cada interviniente, la existencia de acuerdos que regulen el tratamiento conforme al modelo de colaboración, las características y finalidades del tratamiento y las medidas de seguridad apropiadas. El acceso a datos por cuenta de terceros se articulará mediante encargo de tratamiento, acuerdo de cesión o de corresponsabilidad, según corresponda, estando el SES habilitado para establecer los procedimientos técnicos necesarios para supervisar su cumplimiento.

6.2. Seguridad de la información.

6.2.1. Gobernanza.

El SES ha implantado un sistema orientado al riesgo mediante el cual se dirigen y controlan las actividades de seguridad de la información para cumplir con los objetivos establecidos frente a las amenazas a las que están expuestos sus procesos y los activos de información que los soportan.

El gobierno de la seguridad de la información se soporta en la distribución orgánica de funciones descrita en el capítulo 5, que asegura la segregación de funciones y la independencia de los roles en la definición, la implementación y la supervisión del cumplimiento de las medidas de control derivadas de los riesgos observados y del nivel de riesgo aceptable determinado.

6.2.2. Gestión del riesgo.

Las medidas de seguridad se definen mediante un enfoque sistemático basado en la gestión del riesgo. Todos los sistemas y actividades de tratamiento comprendidos en el alcance de esta Política están sujetos a análisis y gestión de riesgos.

El SES empleará metodologías reconocidas, preferentemente las alineadas con el ENS y recogidas en la serie CCN-STIC 800, y aplicará, cuando proceda, las metodologías de evaluación de impacto exigidas por el RGPD para los tratamientos de datos personales. El proceso comprenderá tanto el análisis de los riesgos tecnológicos sobre los sistemas de información como el análisis de los riesgos para los derechos y libertades de las personas.

La gestión del riesgo se aborda desde el diseño y por defecto y se lleva a cabo mediante un proceso sistemático que recoge la identificación y protección, la detección, respuesta y recuperación, y el control y la mejora.

Los análisis de riesgos y, en su caso, las evaluaciones de impacto se revisarán de manera periódica y siempre que se produzcan cambios sustanciales, con el objetivo de identificar nuevos riesgos y minimizar los existentes hasta niveles aceptables. El Responsable de la Información y los Responsables del Servicio son los propietarios de los riesgos sobre la información y sobre los servicios, respectivamente, y responsables de su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

6.2.3. Modelo de operación: prevención, detección, respuesta y recuperación.

Los sistemas de información del SES disponen de una protección basada en líneas de defensa, constituida por múltiples capas de seguridad que interactúan y operan desde diferentes esferas, y desarrollan de forma continua y cíclica las medidas correspondientes a los cuatro momentos del modelo de operación:

— Prevención: medidas dirigidas a la disuasión y a la reducción de la superficie de exposición, mediante el análisis de la exposición y el riesgo de los sistemas, el conocimiento de las tendencias de ataque al sector salud, el análisis de los ciberincidentes del entorno sanitario y el aprendizaje de las lecciones extraídas, considerando las motivaciones de los atacantes y los impactos potenciales. Con carácter general se establece el principio de autorización y control de los sistemas con carácter previo a su entrada en operación.

— Detección: controles de operación orientados a detectar anomalías en la prestación de los servicios y a actuar en consecuencia, incluyendo la identificación de patrones de ataque a partir de los cuales desarrollar reglas de detección de indicadores específicos de actividades maliciosas o de actores conocidos en el sector sanitario.

— Respuesta: medidas que permitan responder eficazmente a los incidentes, reducir al máximo la probabilidad de compromiso del conjunto del sistema, designar un punto de contacto para las comunicaciones relativas a incidentes y establecer protocolos de intercambio de información y coordinación, incluidas las comunicaciones en ambos sentidos con los CSIRT competentes.

— Recuperación: protocolos dirigidos a garantizar la disponibilidad de los servicios y, en su caso, la estrategia de gestión de los medios y técnicas que permitan la recuperación de los servicios más críticos, pudiendo extenderse a la cadena de suministro.

6.2.4. Gestión y notificación de incidentes.

El SES dispondrá de procedimientos de gestión de incidentes de seguridad de acuerdo con lo previsto en el Esquema Nacional de Seguridad, en la instrucción técnica de seguridad correspondiente y, cuando resulte de aplicación por su condición de operador de servicios esenciales, en la normativa sectorial vigente.

Dispondrá igualmente de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, cauces de comunicación a las partes interesadas y registro de las actuaciones. Se desplegarán las medidas necesarias para notificar al Centro Criptológico Nacional los incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados, en relación con la categorización de los sistemas, y se interactuará con los CSIRT correspondientes.

Cuando un incidente de seguridad constituya además una brecha de seguridad de los datos personales, se aplicará de forma coordinada lo previsto en el apartado 6.1.3.

6.2.5. Cumplimiento y mejora continua.

El SES define revisiones planificadas para evaluar la gestión de los riesgos de seguridad de la información, que contemplarán la reevaluación y actualización periódicas de los riesgos a los que está expuesto y la evaluación de la efectividad de las medidas implantadas.

Las medidas identificadas estarán alineadas con la legislación y regulación aplicables. Los incumplimientos detectados formarán parte de las acciones de mejora recogidas en el plan de mejora de la seguridad, sin perjuicio de las acciones inmediatas que deban llevarse a cabo para la contención o mitigación del riesgo derivado y para la identificación de responsabilidades.

El proceso permanente de mejora continua comportará, entre otras acciones, la revisión de esta Política, la revisión de los servicios y de la información y de su categorización, la ejecución y revisión periódica de los análisis de riesgos, la realización de auditorías internas y, cuando procedan, externas, y la revisión de las medidas de seguridad.

6.3. Protección de infraestructuras críticas y servicios esenciales.

El SES tiene la condición de operador de servicios esenciales y de operador crítico respecto de las infraestructuras de su titularidad o gestión que soportan la prestación de dichos servicios.

En el ámbito de la protección de infraestructuras críticas, la presente Política constituye el marco de referencia de la seguridad integral del conjunto de instalaciones y sistemas del SES que tengan tal consideración, y como tal será invocada en los instrumentos de planificación exigidos por la normativa sectorial aplicable.

Los aspectos desarrollados en esta Política con mayor impacto en la protección de infraestructuras críticas, que deberán considerarse en dichos instrumentos, son la organización para la seguridad de la información, la protección de instalaciones, comunicaciones e infraestructuras, la gestión de incidentes de seguridad, la continuidad de los servicios y la explotación y monitorización de los sistemas y servicios.

La identificación de las infraestructuras y servicios afectados, la designación de los roles exigidos por la normativa sectorial, la elaboración y actualización de los instrumentos de planificación y los mecanismos de coordinación con las autoridades competentes se desarrollarán mediante la normativa de segundo nivel prevista en el capítulo 7, en coordinación con las unidades competentes en materia de seguridad física e infraestructuras.

7. DESARROLLO DE LA POLÍTICA Y MARCO DOCUMENTAL.

La presente Política se desarrollará y complementará mediante un marco documental jerarquizado, coherente y sometido a un proceso de revisión y mejora continua, integrado por normas, procedimientos, instrucciones técnicas, guías, planes y demás documentos, registros y evidencias necesarios para garantizar el cumplimiento del Esquema Nacional de Seguridad, de la normativa de protección de datos personales y del resto del marco normativo aplicable.

El marco documental se desarrolla en coherencia con la Estrategia de Privacidad y Seguridad de la Información a que se refiere el apartado 3.2, que fija las líneas de actuación y los objetivos de la organización para un contexto y un período determinados y orienta la planificación de las actuaciones previstas en los documentos que lo integran.

La documentación será proporcional a la naturaleza, alcance y finalidad de la información tratada y de los servicios prestados, así como a la categoría de seguridad, los riesgos identificados y las responsabilidades atribuidas.

7.1. Estructura del marco documental.

7.1.1. Nivel 1. Política de Privacidad y Seguridad de la Información.

La PPSI SES constituye el documento de máximo nivel del marco documental interno en estas materias y establece los principios y objetivos generales; su objeto, misión y

ámbito de aplicación; el marco normativo y sectorial aplicable; el modelo de gobernanza; los órganos, roles, funciones y responsabilidades; los mecanismos de coordinación, reporte, escalado y resolución de conflictos; los criterios generales para la gestión de riesgos, incidentes, continuidad, cumplimiento, terceros y mejora continua; y las directrices para la estructuración, aprobación, gestión, acceso, revisión y difusión de la documentación.

La PPSI SES será aprobada mediante resolución de la persona titular de la Dirección Gerencia, a propuesta del Comité de Gestión y Coordinación de Seguridad de la Información, y será publicada en el Diario Oficial de Extremadura.

7.1.2. Nivel 2. Normativa de Privacidad y Seguridad de la Información.

El segundo nivel está constituido por las normas corporativas que desarrollan los principios, objetivos, requisitos y directrices establecidos en esta Política para ámbitos específicos, y que establecen requisitos, obligaciones y criterios de carácter general o transversal aplicables a los órganos, unidades, centros, servicios, sistemas de información, personas usuarias y terceros comprendidos en su ámbito de aplicación.

Formarán parte igualmente de este nivel las disposiciones y resoluciones de los órganos de gobierno del SES cuyo ámbito afecte a la privacidad y seguridad de la información.

La Normativa de Privacidad y Seguridad de la Información podrá regular, entre otras, las siguientes materias:

— Organización y gobierno de la privacidad y seguridad de la información.

— Análisis y gestión de riesgos.

— Clasificación y tratamiento de la información y gestión de activos.

— Identidad, autenticación, autorización y control de acceso, y gestión de usuarios y privilegios.

— Uso adecuado de los medios electrónicos.

— Seguridad desde el diseño y por defecto.

— Adquisición, desarrollo, implantación y mantenimiento de sistemas de información.

— Gestión de vulnerabilidades, configuraciones, cambios y actualizaciones.

— Registro de actividad, monitorización y supervisión.

— Gestión y notificación de incidentes.

— Continuidad de la actividad y recuperación.

— Seguridad de las comunicaciones, de las interconexiones y de los servicios en la nube.

— Gestión de proveedores y de la cadena de suministro.

— Protección de datos personales.

— Protección de infraestructuras críticas y servicios esenciales.

— Formación y concienciación.

— Auditoría, cumplimiento y mejora continua.

Las normas de Nivel 2 serán aprobadas por el Comité de Gestión y Coordinación de Seguridad de la Información, a propuesta de la Unidad de Gobernanza y Cumplimiento Normativo de la Ciberseguridad.

7.1.3. Nivel 3. Procedimientos, instrucciones técnicas y guías.

El tercer nivel está constituido por los documentos que definen los procesos, actividades, criterios técnicos y actuaciones necesarios para aplicar esta Política y las normas de Nivel 2. Podrá integrarse, entre otros, por procedimientos corporativos, procedimientos operativos y técnicos, instrucciones técnicas, protocolos de actuación, guías de configuración y bastionado, guías dirigidas a las personas usuarias, manuales operativos, modelos y formularios, listas de comprobación, documentación de apoyo y registros y evidencias de ejecución y cumplimiento.

El régimen de aprobación de este nivel es el siguiente:

— Los procedimientos corporativos, instrucciones técnicas y guías de alcance general o transversal serán aprobados por la Unidad de Gobernanza y Cumplimiento Normativo de la Ciberseguridad, a propuesta de la Oficina de Ciberseguridad o de la unidad competente, previo informe de los roles y unidades afectados por razón de la materia.

— El Responsable de la Seguridad podrá aprobar criterios, configuraciones, instrucciones y procedimientos técnicos de seguridad de carácter estrictamente operativo dentro de su ámbito de responsabilidad, siempre que no establezcan obligaciones generales para órganos o unidades ajenos a la Oficina de Ciberseguridad, no

modifiquen ni contradigan documentos de nivel superior, no afecten a las atribuciones reservadas a otros responsables u órganos, no impliquen la aceptación de riesgos que corresponda al Responsable de la Información o a los Responsables del Servicio y no requieran una decisión de carácter estratégico, corporativo o presupuestario. Cuando concurra alguna de estas circunstancias, el documento se elevará a la UGCNC para su aprobación.

— El Responsable del Sistema aprobará y mantendrá actualizados los procedimientos operativos relativos al desarrollo, implantación, explotación, mantenimiento y retirada de los sistemas comprendidos en su ámbito, sin perjuicio de las acciones que delegue conforme al apartado 5.3.4. Estos documentos contarán con informe del Responsable de la Seguridad cuando puedan afectar al estado de seguridad del sistema, a las medidas o configuraciones de seguridad implantadas, a la gestión de riesgos o al cumplimiento normativo.

7.2. Coherencia y trazabilidad documental.

Cada documento deberá fundamentarse en los documentos de nivel superior y mantener coherencia con esta Política, el marco normativo aplicable, la categoría de los sistemas afectados, los resultados de los análisis de riesgos y las correspondientes declaraciones de aplicabilidad.

Los documentos que integren el marco identificarán, al menos: su objeto y finalidad; su ámbito de aplicación; la unidad o rol responsable de su elaboración y mantenimiento; el órgano o rol competente para su aprobación; las personas, órganos, unidades o entidades destinatarias; su clasificación y condiciones de acceso; su versión y fecha de aprobación; su periodo de vigencia, cuando proceda; su periodicidad o causas de revisión; los documentos de nivel superior de los que derivan; y los registros o evidencias asociados a su aplicación.

La aprobación de un documento de nivel inferior no podrá modificar, contradecir o dejar sin efecto lo establecido en un documento de nivel superior. Cuando se detecte una contradicción prevalecerá el documento de nivel superior y se promoverá la revisión del documento afectado.

Las excepciones a lo previsto en el marco documental deberán estar justificadas, documentadas, sometidas a análisis de riesgos y autorizadas por el órgano o rol competente. Cuando la excepción implique la aceptación de riesgos sobre la información o los servicios, deberá ser aprobada por el Responsable de la Información o por el Responsable del Servicio afectado, según corresponda, previa valoración e informe del Responsable de la Seguridad.

7.3. Norma para la gestión de la documentación.

Los criterios de elaboración, identificación, clasificación, aprobación, publicación, distribución, modificación, revisión, conservación, archivo y retirada de la documentación se desarrollarán mediante una Norma para la Gestión de la Documentación de Privacidad y Seguridad de la Información, que deberá garantizar el control de versiones y cambios, la identificación inequívoca de los documentos vigentes, la retirada o identificación de los obsoletos, la trazabilidad de las aprobaciones y revisiones, la conservación de las evidencias de cumplimiento, la protección de la información contenida en la documentación, la asignación de permisos de acceso conforme a los principios de necesidad de conocer y mínimo privilegio, la disponibilidad de la documentación para quienes deban conocerla, su conservación durante los plazos aplicables y su revisión extraordinaria cuando se produzcan cambios relevantes.

7.4. Perfiles de cumplimiento específicos.

Los perfiles de cumplimiento específicos comprenden el conjunto de medidas de seguridad que, derivadas del preceptivo análisis de riesgos, resultan idóneas para una determinada entidad o sector de actividad y para una categoría de seguridad concreta, en aplicación del principio de proporcionalidad.

El SES podrá aplicar el Perfil de Cumplimiento Específico para el sector salud, así como cualesquiera otros perfiles validados y publicados por el Centro Criptológico Nacional que resulten aplicables, atendiendo al alcance, naturaleza, finalidad, categoría y riesgos de cada sistema de información. Su aplicación no sustituirá la determinación del alcance, la categorización de los sistemas, el análisis y gestión de riesgos, la Declaración de Aplicabilidad, la gestión de riesgos sobre los derechos y libertades de las personas, la adopción de medidas adicionales cuando resulten necesarias, la auditoría o evaluación de la conformidad, la vigilancia continua y reevaluación periódica, la gestión de incidentes ni la mejora continua.

Las medidas y criterios derivados de los perfiles aplicados se incorporarán, cuando corresponda, a las declaraciones de aplicabilidad, a los planes de tratamiento de riesgos y a la documentación normativa, procedimental y técnica de los sistemas afectados. La Oficina de Ciberseguridad y el Responsable del Sistema analizarán las nuevas versiones o actualizaciones que se publiquen y elevarán las propuestas correspondientes a la UGCNC y, cuando proceda por su alcance estratégico, organizativo o presupuestario, al CGCSI.

7.5. Planes y documentos específicos.

Los planes de seguridad y cumplimiento no constituyen, por su mera denominación, un nivel documental independiente. Su ubicación, aprobación y régimen de revisión se deter-

minarán en función de su naturaleza, finalidad, alcance y destinatarios. En particular, podrán considerarse planes estratégicos o corporativos, planes de adecuación o mejora, planes de tratamiento de riesgos, planes de continuidad y recuperación, planes de formación y concienciación y planes asociados a sistemas, proyectos, servicios o ámbitos concretos.

Los planes de carácter estratégico o corporativo serán aprobados por el órgano competente atendiendo a su alcance. Los planes asociados a un sistema concreto serán aprobados por los roles que deban asumir los riesgos, ejecutar las medidas o proporcionar los recursos, de acuerdo con las atribuciones establecidas en esta Política y en su normativa de desarrollo.

7.6. Revisión del marco documental y de la Política.

La Unidad de Gobernanza y Cumplimiento Normativo de la Ciberseguridad revisará periódicamente la vigencia, coherencia, adecuación y grado de desarrollo del marco documental.

Sin perjuicio de la revisión periódica, los documentos se revisarán cuando concurra alguna de las siguientes circunstancias:

— Cambios en la legislación o en el marco regulador aplicable.

— Modificaciones en la estructura orgánica, en los roles o en las responsabilidades.

— Incorporación o modificación sustancial de sistemas, servicios, procesos o tratamientos.

— Cambios en la categoría de seguridad de los sistemas.

— Variaciones relevantes en los riesgos o amenazas.

— Incidentes de seguridad de impacto significativo.

— Resultados de auditorías, revisiones o evaluaciones de conformidad.

— Cambios en los perfiles de cumplimiento específicos u otras guías de aplicación.

— Deficiencias detectadas en la aplicación de los documentos.

— Necesidades derivadas del proceso de mejora continua.

Las propuestas de modificación se tramitarán ante el órgano o rol competente para aprobar el documento afectado. Cuando la revisión afecte a la presente Política, la propuesta se elevará al Comité de Gestión y Coordinación de Seguridad de la Información para su elevación a la Dirección Gerencia.

7.7. Publicación, difusión y cumplimiento.

La PPSI SES será objeto de publicación en el Diario Oficial de Extremadura y estará disponible a través de los canales corporativos que se determinen.

La documentación que desarrolle esta Política será difundida entre las personas, órganos, unidades, centros y entidades afectadas, atendiendo a su contenido, ámbito de aplicación y clasificación de seguridad. El acceso a la documentación se realizará conforme a los principios de necesidad de conocer, mínimo privilegio y protección de la información. La documentación de carácter público podrá ponerse a disposición de la ciudadanía a través de los correspondientes portales institucionales.

Las personas comprendidas en el ámbito de aplicación deberán conocer y cumplir los documentos que resulten aplicables al ejercicio de sus funciones. Las obligaciones contenidas en el marco documental se trasladarán a los contratos, encargos, convenios y demás instrumentos jurídicos que regulen la relación con terceras partes cuando estas participen en la prestación de servicios, utilicen activos del SES, accedan a sus sistemas o traten información bajo su responsabilidad.

La UGCNC y la Oficina de Ciberseguridad promoverán las actuaciones de comunicación, formación, concienciación y supervisión necesarias para garantizar la aplicación efectiva del marco documental.

8. RELACIÓN CON TERCERAS PARTES.

Cuando un tercero lleve a cabo un suministro, preste un servicio, utilice activos de información del SES o se le cedan estos, deberá cumplir con la presente Política y con su desarrollo en lo que respecta al ámbito de la colaboración.

Los contratos, encargos o convenios que se suscriban con terceros incluirán la obligación de cumplir esta Política, el sistema de verificación de su cumplimiento y la designación de una persona o punto de contacto para la seguridad de la información tratada o del servicio prestado, que canalice y supervise el cumplimiento de los requisitos aplicables y la gestión de incidentes de privacidad y seguridad de la información en el ámbito de la colaboración.

Las obligaciones asumidas por los terceros se extenderán igualmente a sus subcontratistas, proveedores y demás colaboradores que intervengan en la cadena de provisión necesaria para la prestación del servicio o suministro. Dichas obligaciones se definirán y exigirán de forma proporcional a la criticidad del servicio, del tratamiento o de los activos afectados, pudiendo incluir, entre otros aspectos, compromisos específicos sobre niveles de servicio y seguridad, plazos de notificación de incidentes y brechas, derechos de supervisión y audi-

toría, requisitos de registro y conservación de evidencias, gestión de vulnerabilidades y actualizaciones, continuidad del servicio, así como planes de salida, reversibilidad y devolución o borrado seguro de la información y de los activos al finalizar la relación contractual.

El personal del SES responsable de los contratos, encargos o convenios suscritos con terceras partes será responsable de la verificación, a lo largo de la vida de dichos instrumentos, de los requisitos de privacidad y seguridad establecidos en ellos.

El artículo 2.3 del Esquema Nacional de Seguridad establece que los pliegos de prescripciones administrativas o técnicas de los contratos que celebren las entidades comprendidas en su ámbito de aplicación contemplarán todos los requisitos necesarios para asegurar la conformidad con el Esquema de los sistemas de información en los que se sustenten los servicios prestados por los contratistas, tales como la presentación de las correspondientes Declaraciones o Certificaciones de Conformidad. Esta cautela se extenderá igualmente a la cadena de suministro de dichos contratistas, en la medida en que resulte necesario y de acuerdo con los resultados del correspondiente análisis de riesgos.

A tal efecto, conforme a los procedimientos de determinación de la conformidad previstos en el artículo 38 del Esquema Nacional de Seguridad y en la instrucción técnica de seguridad dictada en su desarrollo, se exigirá Certificación de Conformidad respecto de los sistemas de información de categoría Media o Alta, sin que resulte suficiente en tales casos la Declaración de Conformidad.

No obstante, se atenderá a las especialidades del sector y, específicamente, a las situaciones de dependencia o exclusividad que pudieran presentarse. En caso de no disponer de proveedores que cuenten con las conformidades requeridas, deberán exigirse medidas de seguridad acordes a la valoración del riesgo, tanto para la información como para el servicio que vaya a prestarse, requiriéndose informe del Responsable de la Seguridad que precise los riesgos en que se incurre y la forma de tratarlos.

• • •