DOCUMENTO DE POLÍTICA DE SEGURIDAD INTERIOR Y SEGURIDAD TIC DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DE LA CONSEJERÍA DE SALUD Y FAMILIAS

1.-Introducción.

Los avances tecnológicos en los ámbitos de la informática, las telecomunicaciones y de la sociedad de la información son ya un hecho consolidado, que afecta no sólo a la sociedad sino también a los poderes públicos. Son los poderes públicos los responsables de generar confianza en el uso por parte de la ciudadanía de los medios tecnológicos en sus relaciones con la Administración Pública. Para conseguir esta confianza, los medios tecnológicos utilizados deben ser seguros y para ello se debe garantizar la confidencialidad, integridad y disponibilidad de los sistemas, de las comunicaciones y de los servicios telemáticos, permitiendo tanto a la ciudadanía, profesionales y empresas, como a las Administraciones Públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

Las leyes 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, vienen a configurar un escenario en el que la tramitación electrónica debe constituir la actuación habitual de las Administraciones en sus múltiples vertientes de gestión interna, de relación con la ciudadanía y de relación de aquellas entre sí.

En concreto, la Ley 39/2015, de 1 de octubre, tiene como uno de sus objetivos centrales regular las relaciones entre las Administraciones y la ciudadanía y empresas, teniendo en cuenta el desarrollo de las tecnologías de la información y comunicación de los últimos años y cómo este afecta a las relaciones entre estos agentes. Pretende implantar una Administración totalmente electrónica, interconectada y transparente, mejorando la agilidad de los procedimientos administrativos y reduciendo los tiempos de tramitación. Por su parte, la Ley 40/2015, de 1 de octubre, procura dotar a nuestro sistema legal de una norma comprensiva del régimen jurídico de las Administraciones Públicas, regulando el funcionamiento interno de cada Administración y de las relaciones entre ellas.

El Estatuto de Autonomía para Andalucía, en su artículo 34, reconoce el derecho a acceder y usar las nuevas tecnologías y a participar activamente en la sociedad del conocimiento, la información y la comunicación, mediante los medios y recursos que la ley establezca. Asimismo, el artículo 58.1.2.o atribuye a la Comunidad Autónoma de Andalucía competencias exclusivas sobre el régimen de las nuevas tecnologías relacionadas con la Sociedad de la Información y del Conocimiento, en el marco de la legislación del Estado.

Por otro lado, la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía, señala en su artículo 7.2 que los principios que rigen las relaciones que mantenga la Administración de la Junta de Andalucía con la ciudadanía y con otras Administraciones Públicas a través de redes abiertas de telecomunicación, son los de simplificación y agilización de trámites, libre acceso, accesibilidad universal y confidencialidad en el tratamiento de la información, y de seguridad y autenticidad en orden a la identificación de las partes y el objeto de la comunicación. Para ello establece que estos sistemas deben cumplir con el requisito de existencia de medidas de seguridad que eviten la interceptación y alteración de las comunicaciones, así como los accesos no autorizados. En este mismo texto legal se abunda en materia de seguridad señalándose que los medios o soportes en que se almacenen los documentos electrónicos contarán con las medidas de seguridad que garanticen la integridad, protección y conservación de los documentos almacenados, así como la identificación de las personas usuarias y el control de acceso de las mismas.

Para el desarrollo de esta Política de Seguridad de las tecnologías de la información y las comunicaciones se ha seguido lo dispuesto en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS) y su modificación mediante Real Decreto 951/2015, de 23 de octubre; el Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía, y su modificación mediante el Decreto 70/2017, de 6 de junio; la Orden de la Consejería de Empleo, Empresa y Comercio, de 9 de junio de 2016, por la que se efectúa el desarrollo de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.

Adicionalmente, se tienen en cuenta en esta Política de Seguridad los aspectos de seguridad digital requeridos por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante RGPD) y en la legislación estatal vigente en materia de protección de datos de carácter personal.

En la elaboración de esta Política de Seguridad, asimismo, se han tenido en cuenta el contexto de la Red Corporativa de Telecomunicaciones de la Administración de la Junta de Andalucía, creada por el Acuerdo del Consejo de Gobierno de 2 de junio de 1998, y de los principales sistemas de información corporativos de las entidades que forman parte de la Administración de la Junta de Andalucía.

Del mismo modo, se ha tenido en cuenta el actual Decreto 171/2020, de 13 de octubre, cuyo objeto es establecer una política de seguridad interior en la Administración de la Junta de Andalucía que defina un completo sistema para la prevención y reacción ante daños intencionadamente provocados por agentes externos, personal propio o personas usuarias, contra sus propias personas usuarias, su personal, sus activos y la continuidad de su funcionamiento y servicios. En el decreto se prevé la implementación de una compleja estructura para la coordinación, dirección y ejecución de la política de seguridad interior, tanto en el eje funcional, a lo largo de los distintos niveles de la administración autonómica, como en eje territorial, teniendo en cuenta el despliegue provincial de la Junta de Andalucía. Así mismo, el decreto también prevé un importante desarrollo e implementación de planes de seguridad interior contra riesgos intencionales, que se desplegarán a todos los niveles de la Junta de Andalucía.

Esta Política de Seguridad establece el compromiso de la Consejería de Salud y Familias con la seguridad de los sistemas de información, define los objetivos y criterios básicos para el tratamiento de la misma, sienta los pilares del marco normativo de seguridad en este organismo y la estructura organizativa y de gestión que velará por su cumplimiento.

Por otra parte, de acuerdo con el artículo 5 de la Ley 12/2007, de 26 de noviembre, para la promoción de la igualdad de género en Andalucía, esta norma integra el principio de igualdad de género de forma transversal en su elaboración, garantizando con ello un impacto positivo en la igualdad de oportunidades entre mujeres y hombres.

2.-Objeto.

El presente documento tiene por objeto definir y regular la Política de Seguridad Interior y Seguridad TIC de la Consejería de Salud y Familias, que se ha de aplicar en el tratamiento de los activos de tecnologías de la información y comunicaciones de su titularidad o cuya gestión tenga encomendada, así como definir y regular un completo sistema para la prevención y reacción ante daños intencionadamente provocados por agentes externos, personal propio o personas usuarias, contra sus propias personas usuarias, su personal, sus activos y la continuidad de su funcionamiento y servicios.

3.-Ámbito de aplicación.

La Política de Seguridad Interior y Seguridad TIC contenida en el presente documento será de aplicación a la Consejería de Salud y Familias, tanto a sus servicios centrales como periféricos y a sus entidades vinculadas o dependientes establecidas en el Anexo I, excepto a las que estén integradas en el Sistema Sanitario Público de Andalucía, de acuerdo con lo previsto en el artículo 43 de la Ley 2/1998, de 15 de junio, de Salud de Andalucía, a las que será de aplicación el documento de Política de Seguridad del Sistema Sanitario Público de Andalucía. También será de aplicación para todas las personas que accedan a los sistemas de información como a la propia información que sea gestionada por la Consejería de Salud y Familias, con independencia de cuál sea su destino, adscripción o relación con la misma.

4.-Objetivos, principios y definiciones.

1. Se asumen los objetivos, principios y definiciones establecidos en los artículos 3, 4 y 5 del Decreto 171/2020, de 13 de Octubre, por el que se establece la Política de Seguridad Interior en la Administración de la Junta de Andalucía.

2. Se asumen los principios, objetivos y definiciones establecidos en los artículos 2, 4 y 5 del Decreto 1/2011, de 11 de enero, por el que se establece la Política de Seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía, circunscritos al ámbito competencial de los órganos contemplados en el ámbito de aplicación de esta norma.

5.-Contexto tecnológico y responsabilidad general.

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

2. La preservación de la seguridad TIC será considerada objetivo común de todas las personas al servicio de los órganos contemplados en el ámbito de aplicación de la Política de Seguridad, siendo éstas responsables del uso correcto de los activos TIC puestos a su disposición.

3. Todas las personas que presten servicios a la Consejería de Salud y Familias y en las entidades incluidas en el ámbito de aplicación de su Política de Seguridad, tienen la obligación de conocer y cumplir, en sus respectivos ámbitos de actuación, la misma, así como la normativa de seguridad que emana de ella, siendo responsabilidad del Comité de Seguridad Interior y Seguridad TIC de la Consejería de Salud y Familias disponer los medios necesarios para que la información llegue a las personas afectadas.

4. Con carácter general, para las personas trabajadoras incluidas en el ámbito de aplicación de la presente Política de Seguridad, regirán las normas de uso de los recursos TIC previstas en la Resolución de 27 de septiembre de 2004, de la Secretaría General para la Administración Pública, por la que se establece el manual de comportamiento de los empleados públicos en el uso de los sistemas informáticos y redes de comunicaciones de la Administración de la Junta de Andalucía, o en la normativa de carácter horizontal vigente en cada momento.

5. Las normas de uso de los recursos TIC serán trasladadas convenientemente, en la medida en que pueda resultar necesario o recomendable, al clausulado de los contratos suscritos por la Consejería de Salud y Familias.

6.-Marco normativo.

1. Se asume como marco normativo general el que en cada momento se defina, en virtud de la disposición adicional primera del Decreto 1/2011, de 11 enero, por la Consejería competente en materia de coordinación y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones, a propuesta del Comité de Seguridad Interior y Seguridad TIC de la Junta de Andalucía. Todo ello sin perjuicio de otra normativa aplicable a este organismo en virtud de su naturaleza legal y sus competencias.

2. La Consejería de Salud y Familias podrá ampliar y desarrollar el marco normativo en los términos previstos en el apartado 18, Desarrollo normativo de la seguridad TIC, del presente documento de Política de Seguridad.

7.-Estructura organizativa de la Seguridad Interior y Seguridad TIC.

1. La gestión de la seguridad de la información en un organismo va íntimamente ligada al establecimiento de una organización de seguridad. Dicha organización se establece mediante la identificación de las diferentes actividades y responsabilidades en materia de gestión de la seguridad y mediante su asignación formal a los agentes que correspondan, con arreglo al principio básico de función diferenciada recogido tanto en el ENS como en la política de seguridad TIC de la Junta de Andalucía.

2. Atendiendo a dicho principio, la estructura que se define en este documento diferencia tres grandes bloques de responsabilidad:

a) La especificación de las necesidades y requisitos en materia de seguridad de la información.

b) El desarrollo y/o explotación del sistema de información.

c) La función de supervisión de la seguridad del sistema de información.

En este sentido, los distintos bloques de responsabilidad mencionados quedarán distribuidos convenientemente, conforme a lo estipulado en el apartado subsiguiente, sobre los distintos agentes integrantes de la siguiente estructura organizativa a dos niveles:

a) En la Consejería de Salud y Familias:

En relación con el Esquema Nacional de Seguridad en el ámbito de la administración electrónica:
i. Comité de Seguridad Interior y Seguridad TIC.
ii. Responsables de la información.
iii. Responsables de los servicios.
iv. Unidad de Seguridad TIC.
v. Responsable de Seguridad TIC.
vi. Responsables de los sistemas.

En relación con la normativa de protección de datos de carácter personal:
i. Responsables de los tratamientos de datos de carácter personal
ii. Encargados de los tratamientos de datos de carácter personal
iii. Delegado de Protección de Datos.

En relación con la Política de Seguridad Interior en la Administración de la Junta de Andalucía:
i. Unidad de Seguridad Interior.

b) En cada una de las entidades incluidas en el ámbito de aplicación de la Política de Seguridad TIC:

En relación con el Esquema Nacional de Seguridad en el ámbito de la administración electrónica:
i. Comité de Seguridad Interior y Seguridad TIC.
ii. Responsables de la información
iii. Responsables de los servicios
iv. Responsable de Seguridad Interior y Seguridad TIC

v. Responsables de los sistemas

En relación con la normativa de protección de datos de carácter personal:
i. Responsables de los tratamientos de datos de carácter personal
ii. Encargados de los tratamientos de datos de carácter personal
iii. Delegado de Protección de Datos

En relación con la Política de Seguridad Interior en la Administración de la Junta de Andalucía:
i. Unidad de Seguridad Interior.

3. Dependiendo de las necesidades y circunstancias de la organización, en ciertos casos, la función de algunos de estos agentes podrá recaer sobre una misma persona, unidad o departamento, siempre que no exista conflicto de intereses.

4. Con sujeción al marco previsto por el ENS, por la normativa en materia de protección de datos, por la Política de Seguridad Interior y Seguridad TIC de la Junta de Andalucía y por su normativa de desarrollo, en las entidades vinculadas o dependientes de la Consejería de Salud y Familias incluidas en el ámbito de aplicación de la presente Política de Seguridad, la responsabilidad de la conformación y designación de estas figuras, recaerá sobre las propias entidades.

8.-Comité de Seguridad Interior y Seguridad TIC.

A) Comité de Seguridad Interior y Seguridad TIC de la Consejería de Salud y Familias.

1. Se crea el Comité de Seguridad Interior y Seguridad TIC de la Consejería de Salud y Familias como órgano de dirección y seguimiento en materia de seguridad de los activos de los que la Consejería de Salud y Familias sea titular o cuya gestión tenga encomendada.

2. El Comité de Seguridad Interior y Seguridad TIC de la Consejería de Salud y Familias estará formado por:

a) La persona titular de la Viceconsejería, que ejercerá la presidencia del Comité.
b) La persona titular de Secretaría General Técnica, que ejercerá la vicepresidencia del Comité.
c) La persona titular de cada una de las Secretarías Generales y Centros Directivos de la Consejería de Salud y Familias o equivalentes que tenga responsabilidad sobre algún sistema o tratamiento de información, que actuarán como vocales.
d) El Delegado de Protección de Datos de la Consejería de Salud y Familias, que actuará como vocal.
e) La persona titular del Servicio de Informática de la Consejería de Salud y Familias, que actuará como vocal.
f) La persona titular de la Unidad de Seguridad Interior de la Consejería de Salud y Familias, que actuará como vocal.
g) Las personas titulares de los Puntos Coordinadores de Seguridad Interior, que actuará como vocal.
h) La persona titular de la Unidad de Seguridad Seguridad TIC de la Consejería de Salud y Familias, que ejercerá la secretaría del Comité y actuará como vocal.

3. Asimismo, el Comité de Seguridad Interior y Seguridad TIC podrá convocar a sus reuniones a las personas que en cada caso autorice la presidencia, por propia iniciativa o a propuesta de alguno de sus miembros.

4. El Comité de Seguridad Interior y Seguridad TIC podrá recabar de personal técnico especializado, propio o externo, la información pertinente para la toma de decisiones.

5. En caso de vacante, ausencia o enfermedad u otras causas legales, la persona titular de la Presidencia será sustituida por la persona titular de la Vicepresidencia. Tanto la Vicepresidencia como las Vocalías podrán designar una persona que les sustituya en estas circunstancias entre personal funcionario que ocupen puestos de trabajo de nivel 28 o superior.

6. Serán funciones propias del Comité de Seguridad Interior y Seguridad TIC:

a) La definición, aprobación y seguimiento de los objetivos, iniciativas y planes estratégicos en materia de seguridad TIC.
b) Velar por la disponibilidad de los recursos necesarios para desarrollar las iniciativas y planes estratégicos definidos.
c) El nombramiento del responsable de la Unidad de Seguridad Interior y Seguridad TIC de la Consejería de Salud y Familias.
d) La elevación de propuestas de revisión de la Política de Seguridad Interior y Seguridad TIC de la Consejería, de directrices y normas de seguridad de la Consejería, o de revisión del marco normativo de seguridad TIC de la Junta de Andalucía, a los órganos competentes para su reglamentaria tramitación.
e) La aprobación de la normativa de seguridad TIC de segundo y tercer nivel de la Consejería, de acuerdo con lo establecido en el apartado 18, Desarrollo normativo de la seguridad TIC, del presente documento.
f) El establecimiento de directrices comunes y supervisión del cumplimiento de la normativa en materia de seguridad TIC.
g) La supervisión del nivel de riesgo y toma de decisiones en la respuesta a incidentes de seguridad TIC que afecten a los activos TIC.
h) La coordinación con los Comités de Seguridad Interior y Seguridad TIC de las entidades instrumentales vinculadas o dependientes de la Consejería de Salud y Familias, incluidas en el ámbito aplicación de estas normas.
i) La promoción de la formación, entrenamiento y concienciación sobre las medidas legales y organizativas relativas a la Seguridad TIC entre el personal de la Consejería de Salud y Familias.
j) Impulsar la determinación de los niveles de seguridad de la información tratada, en la que se valorarán los impactos que tendrían los incidentes que afectaran a la seguridad de la información, todo ello con la participación de los Responsables de la Información y de los Tratamientos correspondientes y de la Unidad de Seguridad TIC.
k) Impulsar los preceptivos análisis de riesgos, junto a los Responsables de la Información / Servicios / Tratamientos que correspondan, contando con la participación de la Unidad de Seguridad TIC.
l) Coordinar la aceptación de los riesgos residuales por sus personas responsables correspondientes respecto de la información / servicios / tratamientos de su competencia, obtenidos en el análisis de riesgos.

m) Definición, aprobación y seguimiento de los objetivos, iniciativas y planes estratégicos para la seguridad interior, incluido el Plan de Seguridad Interior.
n) Velar por la disponibilidad de los recursos necesarios para desarrollar las iniciativas y planes estratégicos definidos.
o) El establecimiento de directrices comunes y la supervisión del cumplimiento de la normativa de seguridad interior.
p) La aprobación del modelo de relación con los Puntos Coordinadores de Seguridad Interior.
q) La promoción de la educación, el entrenamiento y la concienciación sobre las medidas relativas a la seguridad interior entre el personal.
r) El análisis y la adopción de decisiones en la respuesta a incidentes susceptibles de generar una crisis de seguridad.
s) Las previsiones para la designación de los Puntos Coordinadores de Seguridad Interior.

7. El Comité se reunirá al menos una vez al año, previa convocatoria y, de sus reuniones, se levantará acta por el Secretario, que será aprobada en la misma o en la próxima reunión del mismo.

B) Comité de Seguridad Interior y Seguridad TIC de las entidad vinculadas del Anexo I.

1. La composición del Comité de Seguridad Interior y Seguridad TIC se decidirá por el órgano directivo del máximo nivel de cada entidad. En todo caso, formará parte del Comité de Seguridad Interior y Seguridad TIC, el Delegado de Protección de Datos, el Responsable de Seguridad TIC, la persona responsable del Servicio de Informática de la entidad y en su caso, el Coordinador de Seguridad Interior.

2. Será de aplicación a este Comité los subapartados 3, 4, 6 y 7 del apartado A) anterior.

9.-Responsables de la información y de los servicios y procedimiento de designación y renovación.

1. Los Responsables de la información y/o de los servicios serán las personas titulares de los centros directivos que decidan sobre la finalidad, contenido y uso de la información y/o sobre las características de los servicios a prestar, así como las que determinen los niveles de seguridad dentro del marco establecido en el anexo I del ENS.

2. En virtud del artículo 10.4 del Decreto 1/2011, de 11 de enero, los deberes y responsabilidades principales de estos perfiles de responsabilidad, dentro de su ámbito de actuación y sin perjuicio de otras previstas en el ENS y la guía CCN-STIC-801, son los siguientes:

a) Ayudar a determinar los requisitos de seguridad de la información y/o de los servicios a prestar, identificando los niveles de seguridad de la información y/o servicios mediante la valoración del impacto sobre los mismos de los incidentes que pudieran producirse.
b) Proporcionar la información necesaria a la Unidad de Seguridad Interior y Seguridad TIC, para realizar los preceptivos análisis de riesgos, con la finalidad de establecer las salvaguardas a implantar. Para ello contará con la ayuda del Responsable del sistema (o los responsables si hubiere varios).

c) En relación con los análisis de riesgos de los sistemas de información, aceptar los riesgos residuales de las informaciones manejadas y/o servicios prestados que sean de su competencia.

3. El nombramiento o renovación de estas figuras responsables se realiza en virtud de la presente Política de Seguridad, estando aparejados automáticamente a la toma de posesión de la titularidad de los correspondientes centros directivos o unidades organizativas y a la adscripción a los mismos en cada momento de las distintas informaciones manejadas y servicios prestados.

10.-Responsables de los Tratamientos de datos de carácter personal.

1. Los Responsables de los Tratamientos de datos de carácter personal en el ámbito de aplicación de este documento de Política de Seguridad son las autoridades públicas que determinen los fines y medios de los tratamientos, de conformidad con el artículo 4.7 del Reglamento General de Protección de Datos.

2. En el ámbito de la Política de Seguridad de esta Consejería, los Responsables de la Información, es decir, los órganos directivos, tendrán la condición de Responsables del Tratamiento respecto a los tratamientos sobre los que determinen sus fines y medios, salvo que las normas aplicables sobre asignación de atribuciones en materia de protección de datos de carácter personal dispongan otra cosa.

11. Encargados de los Tratamientos de datos de carácter personal.

1. Si los Responsables de los Tratamientos designaran a un Encargado del Tratamiento lo harán únicamente por cada tratamiento a un Encargado de Tratamiento que ofrezca garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas para que el tratamiento sea conforme al Reglamento General de Protección de Datos y garantice la protección de los derechos de las personas interesadas, de conformidad con el artículo 28 del Reglamento General de Protección de Datos.

2. Las principales funciones y responsabilidades, dentro de su ámbito de actuación, son las establecidas en el artículo 28 del Reglamento General de Protección de Datos y demás normativa de aplicación.

3. Tanto el Responsable como el Encargado del Tratamiento deberá determinar claramente cuándo el tratamiento se realiza bajo su autoridad, conforme a lo establecido en el artículo 29 del Reglamento General de Protección de Datos y cuándo se realiza mediante un Encargado de Tratamiento sujeto a lo establecido en el artículo 28 de dicho Reglamento General de Protección de Datos.

12.-Unidad de Seguridad TIC, Responsable de Seguridad TIC.

1. En virtud del artículo 11.1 del Decreto 1/2011, de 11 de enero, la Consejería de Salud y Familias contará con una Unidad de Seguridad Interior y Seguridad TIC, garantizando el cumplimiento del principio de función diferenciada recogido en el artículo 5.j) de dicho Decreto, que ejerza las funciones de Responsabilidad de Seguridad TIC de la Consejería, debiendo ser designada la persona responsable de la citada Unidad entre las personas funcionarias adscritas a la Consejería.

2. La Unidad de Seguridad TIC de de la Consejería de Salud y Familias será nombrada o renovada y se comunicará, mediante acto documentado, por el Comité de Seguridad Interior y Seguridad TIC de este organismo, teniendo al frente a una persona responsable.

3. La Unidad de Seguridad TIC de la Consejería de Salud y Familias tendrá las atribuciones que establece el artículo 11.1 del Decreto 1/2011, de 11 de enero.

4. La persona responsable de la Unidad de Seguridad TIC de la Consejería de Salud y Familias tendrá la condición de Responsable de seguridad y, en virtud del artículo 10.4 del Decreto 1/2011, de 11 de enero, la presente Política establece que le corresponderán los deberes y responsabilidades en los términos recogidos en el ENS y la guía CCN-STIC-801.

5. La Unidad de Seguridad TIC de la Consejería de Salud y Familias elaborará y mantendrá un inventario de servicios y sistemas, con indicación expresa de las personas u órganos que asumen, para cada uno de ellos, las figuras de Responsable de la información, Responsable del servicio, Responsable del sistema y Responsable de seguridad.

Dicho inventario se entregará, actualizado, al Comité de Seguridad Interior y Seguridad TIC del organismo en cada una de sus reuniones, con indicación de aquellas deficiencias o faltas de información que se produzcan, de modo que el Comité disponga de información completa y pueda arbitrar los mecanismos necesarios para la subsanación de las deficiencias o faltas de información.

13.-Unidad de Seguridad Interior.

1. En virtud del artículo 10 del Decreto 171/2020, de 13 de octubre, por el que se establece la Política de Seguridad Interior en la Administración de la Junta de Andalucía, la Consejería de Salud y Familias contará con una Unidad de Seguridad Interior que ejerza la responsabilidad ejecutiva para la seguridad interior del conjunto de los activos en su ámbito, debiendo ser designada por el Comité de Seguridad Interior y Seguridad TIC.

2. La Unidad de Seguridad Interior de la Consejería de Salud y Familias tendrá las atribuciones que establece el artículo 10.2 del Decreto 171/2020, de 13 de octubre.

14.-Delegado de Protección de Datos.

1. La figura del Delegado de Protección de Datos, en los términos establecidos en el RGPD, será asumida por una persona entre las personas funcionarias al servicio de la Consejería de Salud y Familias, con una adscripción dentro de la estructura de la organización a un órgano con competencias y funciones de carácter horizontal, a los efectos de poder relacionarse adecuadamente con la dirección de la organización y con las autoridades de control.

2. El nombramiento o renovación de la figura del Delegado de Protección de Datos se realizará y comunicará, mediante acto documentado, por decisión de la persona titular de la Viceconsejería, no pudiendo ser removida ni sancionada por desempeñar sus funciones, salvo que incurriera en dolo o negligencia grave en su ejercicio.

3. La figura del Delegado de Protección de Datos de la Consejería de Salud y Familias y de las entidades comprendidas en el Anexo I, velará por la elaboración y mantenimiento de un registro de tratamientos de datos de carácter personal, con indicación expresa de las personas u órganos que asumen las figuras de Responsable del tratamiento, Encargado del tratamiento y resto de requisitos exigidos por el art 30 del RGPD. Dicho registro se entregará, actualizado, al Comité de Seguridad Interior y Seguridad TIC del organismo en cada una de sus reuniones, con indicación de aquellas deficiencias o faltas de información que se produzcan, de modo que el Comité disponga de información completa y pueda arbitrar los mecanismos necesarios para la subsanación de las deficiencias o faltas de información.

15.-Responsable del sistema y procedimiento de designación y renovación.

1. En virtud del artículo 10.4 del Decreto 1/2011, de 11 de enero, la presente política establece que los deberes y responsabilidades de este perfil serán los previstos en el ENS y la guía CCN-STIC-801. La figura de Responsable del sistema, desde la perspectiva del ENS, de cada sistema de información que se encuentre albergado en los servidores corporativos de la misma, será asumida por una persona adscrita al Servicio con competencia en sistemas de información, designada al efecto por la persona titular de la jefatura de Servicio y figurará en la documentación de seguridad de los sistemas de información. Para cada sistema de información deberá existir una persona Responsable de sistema, siendo posible que una misma persona sea responsable de varios sistemas.

2. La figura de Responsable del sistema, desde la perspectiva del ENS, de los sistemas de información cuya implantación, explotación y mantenimiento se haga fuera de la Consejería (en otros organismos de la Junta de Andalucía o en empresas externas) será designada o renovada por el Responsable de la información o el Responsable de servicio correspondiente y se comunicará mediante acto documentado.

16.-Resolución de conflictos.

1. En caso de conflicto entre los diferentes responsables, éste será resuelto por el órgano superior jerárquico común de los mismos. En defecto de lo anterior, prevalecerá la decisión del Comité de Seguridad Interior y Seguridad TIC.

2. En los conflictos entre las personas responsables que componen la estructura organizativa de la Política de seguridad de la Consejería de Salud y Familias y las entidades que figuran en el Anexo I, y las personas responsables definidas en virtud de la normativa de protección de datos de carácter personal, prevalecerá la decisión que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.

17.-Datos de Carácter Personal.

1. Para el tratamiento de datos de carácter personal en los sistemas de información se seguirá en todo momento lo establecido en 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, así como lo establecido en la legislación nacional y autonómica vigente en cada momento en relación con esta materia.

2. La seguridad de los datos de carácter personal se basará en criterios de reducción del riesgo dependiendo de la naturaleza y tratamientos de los mismos.

3. Para el cumplimiento de la obligación de disponer de un registro de tratamientos, se estará a lo indicado en el apartado 13.3, Delegado de Protección de Datos, del presente documento.

18.-Gestión de riesgos.

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

2. Las personas encargadas de la categorización de los sistemas, serán los Responsables de la información y/o servicios, siendo la Unidad de Seguridad Interior y Unidad de Seguridad TIC las encargadas de supervisar los análisis de riesgos y proponer las medidas de seguridad a aplicar.

3. Los Responsables de la información y/o servicios son responsables de los riesgos sobre la información y/o los servicios y por tanto, de aceptar los riesgos residuales calculados en el análisis de riesgos, así como de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea. Se entiende por Riesgo Residual el riesgo remanente que existe después de que se hayan tomado las medidas de seguridad.

4. El Comité de Seguridad Interior y Seguridad TIC es responsable de realizar un seguimiento de los principales riesgos residuales asumidos por la organización y de recomendar posibles actuaciones respecto de ellos.

5. La selección de las medidas de seguridad a aplicar será propuesta por la Unidad de Seguridad Interior y la Unidad de Seguridad TIC al Comité de Seguridad Interior y Seguridad TIC, así como el seguimiento de su aplicación.

6. El proceso de gestión de riesgos comprende las fases de identificación y valoración de informaciones y servicios esenciales prestados, categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, las cuales deberán ser proporcionales a los riesgos y estar justificadas. Este análisis deberá revisarse cada año por parte de la Unidad de Seguridad Interior y Unidad de Seguridad TIC, que elevará el correspondiente informe al Comité de Seguridad Interior y Seguridad TIC.

7. Para realizar el análisis de riesgos se utilizará la metodología MAGERIT, aprobada por el Consejo Superior de Administración Electrónica, y las herramientas que la apliquen, como PILAR, desarrollada por el

Centro Criptológico Nacional; así como cualquier otra metodología de evaluación del riesgo que la sustituya por ser mayor su efectividad.

19.-Desarrollo normativo de la Seguridad Interior y Seguridad TIC.

1. El cuerpo normativo sobre Seguridad Interior y Seguridad TIC es de obligado cumplimiento y se desarrollará en tres niveles, según el ámbito de aplicación y nivel de detalle técnico, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior.

Dichos niveles de desarrollo normativo son los siguientes:

a) Primer nivel normativo: Política de Seguridad y directrices y normas generales de seguridad.
b) Segundo nivel normativo: Normas Específicas de Seguridad, que desarrollan y detallan la Política de Seguridad Interior y TIC, centrándose en un área o aspecto determinado.
c) Tercer nivel normativo: Procedimientos, Procesos, Guías e Instrucciones Técnicas de Seguridad Interior y TIC, que dan respuesta, incluyendo detalles de implementación y tecnológicos, a cómo se puede realizar una determinada tarea cumpliendo con lo expuesto en la Política.

2. Al amparo de la presente Política de Seguridad Interior y Seguridad TIC, la Consejería de Salud y Familias podrá ampliar y desarrollar, sobre la base de los mínimos establecidos, sus propias normas en materia de seguridad Interior y TIC, en virtud del Decreto 171/2020 de 13 octubre; así como el artículo 2.5 de la Orden de 9 de junio de 2016.

3. Además de los documentos citados en el punto 1 de este apartado, la documentación de seguridad Interior y TIC de los órganos contemplados en el ámbito de aplicación de esta norma podrá contar, bajo criterio de la Unidad de Seguridad Interior y Unidad de Seguridad TIC, con otros documentos de carácter no vinculante: recomendaciones, buenas prácticas, informes, registros, evidencias electrónicas, etc.

4. La Unidad de Seguridad Interior y la Unidad de Seguridad TIC deberá mantener la documentación de seguridad actualizada y organizada, y gestionar los mecanismos de acceso a la misma.

5. El Comité de Seguridad Interior y Seguridad TIC establecerá los mecanismos necesarios para compartir la documentación derivada del desarrollo normativo con el propósito de normalizarlo, en la medida de lo posible, en todo el ámbito de aplicación de la Política.

20.-Gestión de incidentes de seguridad y de la continuidad.

1. La Consejería de Salud y Familias y sus entidades incluidas en el ámbito de aplicación de la presente Política de Seguridad, deberán estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, según los términos previstos en el artículo 7 del ENS y la Resolución de 13 de julio de 2018, de la Dirección General de Telecomunicaciones y Sociedad de la Información, por la que se establecen normas sobre gestión de incidentes de seguridad TIC.

2. El Comité de Seguridad Interior y Seguridad TIC deberá aprobar y revisar periódicamente un plan para mantener la continuidad de los procesos y sistemas críticos y garantizar su recuperación en caso de

desastre. La finalidad de este plan es reducir el tiempo de indisponibilidad a niveles aceptables mediante la combinación de controles de carácter organizativo, tecnológico y procedimental tanto preventivos como de recuperación.

3. A los efectos de una mejor gestión de los incidentes, se actuará de forma coordinada con AndalucíaCERT.

21.-Formación y concienciación en Seguridad Interior y TIC.

Anualmente se desarrollarán actividades de formación y concienciación en seguridad Interior y TIC destinadas a las personas empleadas públicas de los órganos contemplados en el ámbito de aplicación del documento. Entre tales actividades se incluirán las de difusión de esta Política de Seguridad y de su desarrollo normativo.

22.-Terceras partes.

1. Cuando la Consejería de Salud y Familias y las entidades comprendidas en el Anexo I, presten servicios a otros organismos o manejen información de otros organismos, se les hará partícipes de esta Política de Seguridad, estableciéndose los canales que procedan para la comunicación y coordinación entre las respectivas organizaciones, y se establecerán procedimientos de actuación en especial para una rápida y eficaz reacción ante incidentes de seguridad.

2. Cuando algún Centro Directivo de la Consejería de Salud y Familias y las entidades comprendidas en el Anexo I, utilicen servicios de terceros o cedan información a terceros, se les hará partícipes de esta Política de Seguridad y de la normativa de seguridad Interior y seguridad TIC que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta, a través de cláusulas contractuales o acuerdos de nivel servicio, a las obligaciones generales establecidas en dicha normativa, pudiendo disponer la tercera parte de sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de comunicación y resolución de incidencias, así como se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos, al mismo nivel que el establecido en esta Política de Seguridad.

23.-Auditorías y conformidad con la normativa.

1. La Consejería de Salud y Familias y las entidades comprendidas en el Anexo I, manifiestan el compromiso de auditar los sistemas de información de forma periódica con objeto de revisar el cumplimiento normativo vigente.

2. Los sistemas de información de la Consejería de Salud y Familias y las entidades comprendidas en el Anexo I, serán objeto, al menos cada dos años, de una auditoría regular ordinaria interna o externa que verifique el cumplimiento de los requisitos del ENS y de cualquier otra norma que requiera la realización de auditorías periódicas. La Unidad de Seguridad Interior y la Unidad de Seguridad TIC realizarán o, en su caso, coordinarán, estas actividades de auditoría.

3. Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad requeridas.

4. Los informes de auditoría quedarán a disposición del Responsable de la información y/o servicio, del Responsable del sistema, del Delegado de Protección de Datos y del Comité de Seguridad Interior y Seguridad TIC. Por otra parte, la Unidad de Seguridad Interior y la Unidad de Seguridad TIC deberá analizar dicho informe y elevar al Comité de Seguridad Interior y Seguridad TIC las conclusiones que procedan para que éste adopte las medidas correctoras adecuadas.

24.-Cooperación con otros órganos y otras administraciones en materia de seguridad.

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

- Comité de Seguridad Interior y Seguridad TIC de la Junta de Andalucía
- Unidad de Seguridad Interior y Seguridad TIC Corporativa de la Junta de Andalucía
- Consejo de Transparencia y Protección de Datos de Andalucía
- CCN-CERT: Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN), como soporte y coordinación para la resolución de incidentes que sufra la Administración General, Autonómica o Local.
- Agencia Española de Protección de Datos (AEPD)
- Instituto Nacional de Ciberseguridad (INCIBE)
- Grupo de Delitos Telemáticos de la Guardia Civil y Brigada de Investigación Tecnológica (BIT) del Cuerpo Nacional de Policía, para la investigación de acciones relacionadas con la delincuencia informática y los fraudes en el sector de las telecomunicaciones.

25.-Actualización permanente y revisiones periódicas.

1. Este documento de Política de Seguridad Interior y Seguridad TIC deberá mantenerse actualizado para adecuarlo a la evolución de los servicios y, en general, a la evolución tecnológica y al desarrollo de la sociedad de la información, así como a los estándares internacionales de seguridad.

2. Las revisiones de la Política de Seguridad se harán a propuesta de la Unidad de Seguridad Interior y la Unidad de Seguridad TIC, a la que podrán dirigirse los Comités de Seguridad Interior y Seguridad TIC de las entidades que figuran en el Anexo I, siendo aprobadas las mismas por el Comité de Seguridad Interior y Seguridad TIC de la Consejería de Salud y Familias.

26.-Difusión de la política de seguridad de la información.

A los efectos de su mejor difusión entre el personal de la organización y de otras partes interesadas, la presente Política de Seguridad se publicará y divulgará, a través de los medios que se establezcan por el Comité de Seguridad Interior y Seguridad TIC y, en todo caso, figurará en la página web de la Consejería y de las entidades comprendidas en el Anexo I.

27.-Constitución del Comité de Seguridad Interior y Seguridad TIC.

La primera reunión del Comité de Seguridad Interior y Seguridad TIC, tanto de la Consejería de Salud y Familias como de las entidades incluidas en el ámbito de aplicación de la presente Política de Seguridad, tendrá por objeto la constitución, renovación o confirmación del mismo y se celebrará en el plazo máximo de un mes a partir de la entrada en vigor del presente documento.

28.-Entrada en vigor.

El presente documento de Política de Seguridad Interior y Seguridad TIC entrará en vigor al mes de su aprobación por la persona titular de la Consejería con competencia en materia de salud y familias.

APROBACIÓN: El presente documento de Política de Seguridad TIC queda aprobado.

El CONSEJERO DE SALUD Y FAMILIAS,

Fdo.: Jesús Ramón Aguirre Muñoz

ANEXO I

Escuela Andaluza de Salud Pública (EASP)
Fundación Pública Andaluza para la Investigación de Málaga en Biomedicina y Salud (FIMABIS)
Fundación para la Investigación Biosanitaria de Andalucía Oriental (FIBAO)
Fundación Pública Andaluza para la Integración Social de Personas con Enfermedad Mental (FAISEM)
Fundación Pública Andaluza Progreso y Salud (FpyS)
Fundación Pública Andaluza para la Gestión de la Investigación en Salud de Sevilla (FISEVI)