3. Otras disposiciones

OFICINA ANDALUZA CONTRA EL FRAUDE Y LA CORRUPCIÓN

Resolución de 16 de abril de 2025, de la Oficina Andaluza contra el Fraude y la Corrupción, por la que se da publicidad a las normas que regulan la política de seguridad de la información en la institución, prevista por el Esquema Nacional de Seguridad.

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en su artículo 3.2, dispone la obligación de las Administraciones Públicas de relacionarse entre sí «a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas», así como la de garantizar la protección de los datos de carácter personal. Posteriormente, en su artículo 156, se establece que el Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de dicha norma, estando constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

Esta previsión legal ha sido desarrollada a través del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS), que deroga al anterior Real Decreto 3/2010, de 8 de enero, que regulaba el ENS.

El Esquema Nacional de Seguridad está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información y debe ser aplicado por las Administraciones Públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

La administración digital debe ser confiable para que la ciudadanía realice los trámites administrativos correspondientes con total seguridad y fiabilidad. Para ello, el ENS persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones, y sin que la información pueda llegar a conocimiento de personas no autorizadas.

Por su parte, la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, recoge en su artículo 13, sobre derechos de las personas en sus relaciones con las administraciones públicas, el relativo a la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las administraciones públicas.

En el ámbito específico de esta institución, la Ley 2/2021, de 18 de junio, de lucha contra el fraude y la corrupción en Andalucía y protección de la persona denunciante asegura, en su artículo 15, la protección de los datos de carácter personal y el sometimiento de la Oficina a las previsiones del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, así como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

La información, por tanto, constituye un activo de primer orden para la Oficina Andaluza contra el Fraude y la Corrupción, desde el momento en que resulta esencial para la prestación de gran parte de los servicios, y para la gestión de la seguridad de la información, el ENS establece una serie de medidas específicas para proteger tanto la información como los servicios que dependan de ella y minimizar los riesgos hasta un nivel que resulte aceptable.

El artículo 12 del Real Decreto 311/2022, de 3 de mayo, establece que cada Administración Pública contará con una política de seguridad formalmente aprobada por el órgano competente; y define a la política de seguridad de la información (en adelante,

00319334

PSI) como el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta. Específicamente, en su apartado 1.c), establece que la PSI debe incluir «los roles o funciones de seguridad, definiendo para cada uno, sus deberes y responsabilidades, así como el procedimiento para su designación y renovación», y en su apartado 1.d), recoge la necesidad de incluir «la estructura y composición del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad y la relación con otros elementos de la organización».

Por otra parte, el artículo 13 del ENS, establece los roles y funciones de los responsables de velar por el cumplimiento de la PSI, admitiendo la posibilidad de externalizar algunas de éstas por razones organizativas y de escasez de recursos humanos.

Como consecuencia de lo expuesto, esta Dirección de conformidad con las atribuciones legalmente atribuidas, con fecha 15 de abril de 2025, dictó resolución designando a las personas responsables en materia de gestión de la seguridad de la información que constituirán el Comité de Seguridad; aprobando y ordenando la publicación de la Política de la Seguridad de la Información en la institución que se contiene en el anexo de la presente, para su general conocimiento.

Sevilla, 16 de abril de 2025.- La persona titular de la Dirección, P.S. (ex art. 28 Ley 2/2021 y art. 16 RRIF), la Directora Adjunta, Marta Blázquez Expósito.

A N E X O

NORMAS POR LAS QUE SE REGULA LA POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN EN LA OFICINA ANDALUZA CONTRA EL FRAUDE Y LA CORRUPCIÓN

1. Aprobación y entrada en vigor.

El texto que se expone a continuación constituye la Política de la Seguridad de la Información de la Oficina Andaluza contra el Fraude y la Corrupción (en adelante, la Oficina o la OAAF), aprobada por Resolución de 15 de abril de 2025, de la persona titular de la Dirección en virtud las facultades que le otorgan los artículos 26 de la Ley 2/2021, de 18 de junio, de lucha contra el fraude y la corrupción en Andalucía y protección de la persona denunciante, y 14 del Reglamento de Régimen Interior y Funcionamiento de la Oficina, aprobado por Acuerdo de la Mesa del Parlamento de Andalucía de 20 de abril de 2022.

Esta «Política de Seguridad de la Información» (en adelante, PSI), será efectiva desde su fecha de aprobación y hasta que sea reemplazada por una nueva Política de Seguridad de la Información que la sustituya.

2. Introducción.

La creciente digitalización de las administraciones públicas, han convertido a éstas en un objetivo prioritario para los agentes de las amenazas de ciberseguridad, que persiguen tanto la indisponibilidad de los sistemas atacados, como el acceso a toda la información tratada, así como los servicios asociados a sistemas y redes de comunicaciones.

Como muestra con su compromiso con la seguridad de la información y con el cumplimiento normativo, la Oficina ha desarrollado la presente PSI, de conformidad con lo establecido en artículo 12 el Real Decreto 311/20222, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) y de la medida de seguridad org.1 contemplada en el Anexo II de dicho real decreto.

En este sentido, en el apartado segundo del artículo anteriormente mencionado, se establece que «Cada administración pública contará con una política de seguridad

00319334

formalmente aprobada por el órgano competente. Asimismo, cada órgano o entidad con personalidad jurídica propia comprendido en el ámbito subjetivo del artículo 2 deberá contar con una política de seguridad formalmente aprobada por el órgano competente».

La presente PSI recoge la postura de la OAAF en cuanto a la seguridad de la información, estableciendo los criterios generales que deben regir la actividad del organismo en cuanto a la seguridad. Su objetivo es garantizar la calidad la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza ante cualquier incidente de seguridad.

En todo caso, los sistemas de información deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad, así como sobre el uso previsto y valor de la información y los servicios. Para hacer frente a estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios, así como para garantizar la aplicación de medidas para proteger la privacidad de todo usuario al que se le preste servicios desde la OAAF.

Por ello, los diferentes departamentos de la OAAF deben garantizar que la seguridad TIC debe ser una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta la retirada del servicio, pasando por el desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y la valoración de sus costes deberán identificarse e incluirse en la planificación, en la solicitud de ofertas y en los pliegos de licitación para cualquier proyecto TIC, especialmente cuando los proveedores que formen parte de sus servicios. Del mismo modo, el uso de activos de información deberá estar en consonancia con las buenas prácticas y procedimientos de trabajo profesional, así como con los requisitos legales y reglamentarios.

3. Principios básicos de seguridad.

La OAAF es consciente de que la transformación digital de los servicios y de la información asociada a dicha prestación de servicios, implica necesariamente actividades relacionadas con la seguridad de la información. Es por ello por lo que deben integrarse dentro de la Organización actividades que garanticen la proactividad, vigilancia y reactividad. Las directrices fundamentales en materia de seguridad de la información deberán estar presentes en cualquier actividad de los sistemas de información que se encuentran dentro del alcance la presente política. En cumplimiento de los dispuesto en el ENS, la OAAF se guiará por los siguientes principios:

3.1. Seguridad integral. La seguridad se deberá entender como un proceso integral, constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información. Además, se deberá prestar especial atención respecto a la concienciación de todo el personal que intervengan en procesos y en los responsables jerárquicos para evitar aquellos riesgos potenciales derivados del desconocimiento, falta de organización o coordinación en materia de seguridad.

3.2. Gestión basada en los riesgos. El análisis y gestión de riesgos será parte esencial del proceso de seguridad, siendo una actividad continua, permanentemente actualizada dentro de la entidad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la información tratada, los servicios a prestar y los riesgos a los que se está expuesto.

3.3. Prevención, detección, respuesta y conservación. Para minimizar las vulnerabilidades técnicas y evitar que las amenazas se materialicen, o que de hacerlo, no afecten gravemente a la información que se gestiona o a los servicios que se prestan, se deberán implementar:

○ Medidas de prevención. Para disuadir o reducir la superficie de exposición a vulnerabilidades. La OAAF implementará las medidas de seguridad de aplicación a nivel

00319334

básico establecidas por el Anexo II del ENS, así como otras medidas adicionales que pudiesen ser necesarias tras realizar el análisis de riesgos.

○ Medidas de detección. Se establecerán mecanismos de detección, comunicación y gestión de incidentes de seguridad, de manera que cualquier incidente pudiese ser detectado y tratado en el menor tiempo posible, estableciendo elementos de monitorización y detección de anomalías y poniendo en marcha procedimientos específicos de respuestas ante incidentes de seguridad, así como pautas para la comunicación por parte de los usuarios de posibles incidentes de seguridad.

○ Medidas de respuesta. Se establecerán medidas de respuesta ante eventos que pudiesen afectar a los servicios y/o la información, permitiendo:

- Responder eficazmente a los incidentes de seguridad.

- Desarrollar una reacción adecuada frente a los incidentes, reduciendo al máximo la probabilidad de que el sistema sea comprometido en su conjunto.

- Designar un punto de contacto para comunicaciones si se detectan incidentes en otras áreas o departamentos.

- Establecer protocolos para la coordinación e intercambio de información relacionada con el incidente, incluyendo comunicaciones con las autoridades competentes.

3.4. Conservación. El sistema deberá garantizar, sin perjuicio de los principios básicos o requisitos mínimos que se establecen a través de la presente PSI, la conservación de los datos e información en soporte electrónico que se encuentre dentro del alcance del ENS. Esta medida ayudará a garantizar también la disponibilidad de los servicios durante todo el ciclo de vida de la información.

3.5. Existencia de líneas de defensa. Se debe establecer una estrategia de seguridad robusta, los sistemas deben disponer de una protección basada en líneas de defensa, creando múltiples capas de seguridad que interactuen y operen desde distintas esferas para permitir el desarrollo continuo y cíclico de medidas de seguridad para evitar que un incidente de seguridad afecte al sistema de información. De esta manera, cuando una capa se viese comprometida, existirán más capas permitiendo poder reaccionar ante aquellos incidentes que no pudiesen evitarse, reduciendo la probabilidad de que el sistema se comprometa en su totalidad, minimizando el impacto final sobre el mismo. Dichas líneas de defensa estarán constituídas por medidas de naturaleza organizativa, física y lógica.

3.6. Vigilancia continua y reevaluación periódica. Existirán procesos de vigilancia continua, de manera que se puedan detectar actividades o comportamientos anómalo para darles respuesta rápidamente. Además, deberá existir una evaluación permanente del estado de seguridad de los activos que permita medir su evolución, de manera que se detecte vulnerabilidades y se puedan identificar posibles deficiencias de configuración, de manera que también se reevalúen y actualicen las medidas de seguridad periódicamente para adecuarlas tanto a la evolución de riesgos como de los sistemas de protección.

3.7. Diferenciación de responsabilidades. En los sistemas de información se establecerán una separación de funciones y responsabilidades en la gestión de seguridad de la información, de manera que se asegure la calidad del sistema de información y se eviten posibles conflictos de intereses, asegurando la estabilidad de la seguridad, mediante actuaciones coordinadas entre todos los roles implicados.

4. Objetivos de seguridad de la información.

Se establecen como objetivos de seguridad de la información los siguientes:

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

II. Lograr la plena concienciación de los usuarios respecto a la seguridad de la información.

III. Gestionar los activos de información, bajo un inventario, clasificación y asignación de un responsable.

00319334

IV. Implementar medidas de seguridad ligadas a las personas, incluyendo aquellos mecanismos que fuesen necesarios para que cualquier persona que acceda o pudiese acceder a los activos de información, conozca sus responsabilidades, y reduzcan el riesgo derivado de usos indebidos, logrando la plena concienciación.

V. Desplegar y controlar la seguridad física logrando que los activos de información se encuentren en áreas seguras, protegidos por controles de acceso físicos adecuados a su nivel de criticidad y frente a amenazas físicas o ambientales.

VI. Establecer la seguridad en la gestión de comunicaciones y operaciones mediante los procedimientos necesarios, logrando que la información que se transmita a través de redes de comunicaciones esté adecuadamente protegida.

VII. Limitar el acceso a los activos mediante controles de acceso a usuarios, procesos y servicios, por medios de mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo, asegurando la trazabilidad del acceso y auditando su uso.

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

IX. Mantener el control y la seguridad en la adquisición e incorporación de nuevos componentes del sistema.

X. Gestionar incidentes de seguridad para la correcta identificación, registro y resolución de éstos.

XI. Proteger la información personal, adoptado las medidas técnicas y organizativas en atención a los riesgos derivados del tratamiento conforme a la legislación de seguridad y privacidad.

XII. Adoptar las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

5. Misión de la OAAF.

La Oficina tiene como misión, el impulso de la integridad y la ética pública, la protección de los denunciantes, así como la prevención del fraude, la corrupción, los conflictos de intereses o cualquier otra actividad ilegal que vaya en detrimento de intereses públicos o financieros del sector público andaluz del sector público andaluz y las demás instituciones, órganos y entidades públicas incluidos en el artículo 3, párrafos a), b), c) y d) de la Ley 2/2021, de 18 de junio, de lucha contra el fraude y la corrupción en Andalucía y protección de la persona denunciante. Debe promover una cultura de buenas prácticas y de rechazo del fraude y la corrupción en el diseño, ejecución y evaluación de las políticas públicas, así como en la gestión de los recursos públicos, a través de la creación de un código ético o de buenas conductas.

Mediante el establecimiento de una política de seguridad de la información, la Oficina se dota de un marco de gestión de los servicios electrónicos puestos a disposición para poder hacer frente a su misión, conforme a las funciones y competencias atribuidas por diferentes normas y, en concreto, de acuerdo con lo dispuesto por el artículo 7 y concordantes de la Ley 2/2021, de 18 de junio.

6. Alcance.

Esta PSI es de obligado cumplimiento para todas las unidades que conforman la estructura de la OAAF, y para todo el personal con acceso a la información de la que es responsable aquélla, independientemente de su destino, condición laboral o relación con la Oficina por la que se accede a la información.

La PSI se aplicará a los sistemas de información de la OAAF, que están relacionados con el sistema de recepción de denuncias a través de los diversos canales de denuncia habilitados y de cualquiera de las vías previstas en el art. 17.2 de la Ley 2/2023, con la gestión posterior de las mismas mediante el gestor de expedientes y con el ejercicio de derechos por medios electrónicos, por el cumplimiento de deberes por medios

00319334

electrónicos o con el acceso a la información o al procedimiento administrativo y que se encuentren dentro del alcance del ENS.

La presente PSI se aplicará también a la información en soporte no electrónico que sea causa o consecuencia directa de la información electrónica gestionada por la OAAF, en el ámbito de sus competencias, aplicándose las medidas de seguridad correspondientes a la naturaleza del soporte, de acuerdo con el artículo 22.3 del Real Decreto 311/2022, de 3 de mayo.

7. Marco regulatorio.

La base normativa que afecta al desarrollo de las actividades y competencias de la OAAF y que implica la implantación de forma explícita de medidas de seguridad en los sistemas de información, está constituida por la siguiente legislación:

Normas con rango de ley:

• Ley 2/2021, de 18 de junio, de lucha contra el fraude y la corrupción en Andalucía y protección de la persona denunciante.

• Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

• Reglamento UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

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

• Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

• Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

• Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía.

• Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

• Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

• Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.

• Ley 5/2023, de 7 de junio, de la Función Pública de Andalucía.

• Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

• Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

• Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

Disposiciones de carácter general con rango inferior a ley:

• Acuerdo de Parlamento de Andalucía, de 20 abril 2022, por el que se aprueba el Reglamento de Régimen Interior y Funcionamiento de la Oficina Andaluza contra el Fraude y la Corrupción.

• Resolución de 20 de marzo de 2023, de la Oficina Andaluza contra el Fraude y la Corrupción, por la que se crea y ordena la puesta en funcionamiento del canal externo de información (Canal de Denuncias).

• Resolución de 7 de junio de 2023, de la Oficina Andaluza contra el Fraude y la Corrupción, por la que se crea y se ordena la puesta en funcionamiento del canal interno de información de la OAAF.

00319334

• Resolución de 12 de junio de 2023, de la Oficina Andaluza contra el Fraude y la Corrupción, por la que se crea el Registro de Responsables del Sistema Interno de Información y se regula su funcionamiento.

• Resolución de 4 de diciembre de 2023, de la Oficina Andaluza contra el Fraude y la Corrupción, por la que se crea y se regula la sede electrónica.

• Resolución de 20 de diciembre de 2023, de la Oficina Andaluza contra el Fraude y la Corrupción, por la que se crea y se regula el registro electrónico de la institución.

• Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.

• Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

• Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.

• Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.

• Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.

• Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

• Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.

En todo caso, la anterior relación normativa debe ser entendida como una referencia «dinámica», comprendiendo no sólo las expresamente mencionadas, sino las que modifiquen, sustituyan o desarrollen a las anteriores y que se encuentren dentro del ámbito de aplicación de la Política de Seguridad de la Información de la OAAF.

Igualmente se consideran las restantes normas aplicables a los servicios bajo el objeto de aplicación del ENS, y comprendidos dentro del ámbito de aplicación de la presente PSI, incluyendo las instrucciones técnicas de seguridad de obligado cumplimiento, publicadas mediante resolución de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación digital, a propuesta de la Comisión Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional (CCN) tal y como se establece en la Disposición adicional segunda del ENS.

Así mismo, la OAAF también será responsable de identificar las guías de seguridad del CCN, que serán de aplicación para mejorar el cumplimiento de lo establecido en el ENS.

8. Requisitos mínimos de seguridad.

La OAAF, para lograr el correcto cumplimiento de los requisitos mínimos establecidos en el ENS, implementará diversas medidas de seguridad proporcionales a la naturaleza de la información y de los servicios a proteger, teniendo en cuenta en todo caso la categoría de los sistemas afectados. Para ello, el sistema de gestión generado de la aplicación de la presente PSI se desarrollará aplicando los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad. La seguridad de los sistemas deberá comprometer a todos los miembros de la organización. Por otro lado, se aplicará el principio de diferenciación de responsabilidades, de acuerdo con las especificaciones realizadas en el apartado específico de «Organización de seguridad de la información» y sus subapartados.

b) Análisis y gestión de riesgos. Los servicios e infraestructuras bajo el alcance de la presente PSI, estarán sometidos a un análisis de riesgos conforme a los marcos y

00319334

metodologías existentes en la actualidad (Magerit) para orientar las medidas de protección y minimizar los mismos. Este análisis se repetirá:

- Al menos una vez al año.
- Cuando cambien la información y/o los servicios manejados de manera significativa.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

Las conclusiones de los análisis de riesgos serán elevadas al Responsable de Seguridad y éste al Comité de Seguridad. El Comité de Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

El análisis de riesgos se realizará igualmente cuando se vaya a iniciar o a modificar un tratamiento de datos de carácter personal, en línea a lo establecido en el Reglamento General de Protección de Datos. En estos casos se contemplarán en el alcance del análisis todos aquellos activos que intervengan en el tratamiento, considerando tanto activos relacionados con los sistemas de información, como humanos, locales o terceros.

A raíz de los resultados obtenidos en los mencionados análisis de riesgos de los servicios y de los tratamientos de datos personales, se determinarán las medidas necesarias para proteger dichos datos.

c) Gestión de personal. Todo el personal, propio o ajeno, que utilice o acceda a los sistemas de información sometidos a la presente PSI, tendrá la obligación de conocer y respetar su contenido, así como el marco normativo de desarrollo que se apruebe para el cumplimiento directo de la misma. Las personas con responsabilidad en el uso, operación o administración de sistemas de información, serán informados sobre sus deberes, obligaciones y responsabilidades y 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 una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades.

d) Profesionalidad. La seguridad de los sistemas de información deberá ser revisada y auditada por personal cualificado, dedicado e instruido. Se exigirá, de manera objetiva y no discriminatoria, respecto a aquellas organizaciones que, en su caso, presten servicios de seguridad, cuenten con profesionales cualificados y con niveles idóneors de gestión de los servicios prestados. Se determinará los requisitos de formación y experiencia necesaria del personal para el desarrollo de los puestos de trabajo.

e) Autorización y control de accesos. El acceso a los sistemas de información estará restringido y limitado a aquellos usuarios o procesos que lo necesiten para el desarrollo de su actividad y estén previamente autorizados. El acceso a la información seguirá el principio de «necesidad de conocer», de forma que los privilegios otorgados a cada identidad sean los mínimos imprescindibles para el desarrollo de su actividad.

La identificación de los usuarios será tal que se pueda conocer en todo momento quién recibe derechos de accesos y quién ha realizado alguna actividad, por lo que los identificadores deberán ser personales, no compartidos, e intransferibles.

Los lugares con acceso restringido igualmente deberán estar controlados y previamente autorizados por los responsables asignados.

f) Protección de las instalaciones. Los sistemas de información y su infraestructura de comunicaciones asociada deberán permanecer en áreas controladas y disponer de los mecanismos de acceso adecuados y proporcionales en función del análisis de riesgos.

g) Adquisición de productos de seguridad y contratación de servicios de seguridad. Para el proceso de adquisición de nuevos productos, sistemas o servicios se establecerán protocolos de análisis de riesgos con proveedores y se mantendrán actualizados los listados de proveedores habituales. Las adquisiciones deben ser autorizadas por los responsables del área implicada y el Servicio de Contratación cumpliendo la normativa vigente de contratación. Cuando proceda, se suscribirán los correspondientes contratos con los encargados de tratamiento, conforme a lo dispuesto en el art. 28 del RGPD.

00319334

h) Mínimo privilegio. Los sistemas y aplicaciones se diseñarán y construirán otorgando los mínimos privilegios necesarios para el correcto desempeño de funciones del usuario: Seguridad por defecto, de tal forma que:

○ El sistema ofrecerá la funcionalidad imprescindible para que la organización alcance sus objetivos. Cualquier función que no sea de interés o innecesaria será deshabilitada o no implementada.

○ La operación, administración y registros de actividad serán las mínimas necesarias, asegurando que solo serán desarrolladas por personas autorizadas y desde equipos y emplazamientos autorizados, pudiendo incluir restricciones de horario y puntos de acceso facultados, en su caso.

○ Cualquier función que no sea de interés o innecesaria será deshabilitada o no implementada. El uso del sistema ha de ser sencillo y seguro, de tal forma que el uso inseguro requiera de actos conscientes por parte del usuario.

La seguridad estará presente desde la concepción de un sistema o aplicación y permanecerá presente durante todo su ciclo de vida. En la concepción de un nuevo sistema o aplicación, o modificación sustancial de un sistema o aplicación existente, se contará siempre, y desde el inicio, con la participación del Responsable de la Información y del Servicio, del Responsable de Seguridad de la Información y del Delegado o Delegada de Protección de Datos.

i) Integridad y actualización del Sistema. La inclusiones o modificaciones de elementos físicos o lógicos en el registro de activos del sistema requerían de autorización previa. Del mismo modo, se evaluará y monitorizará, permanentemente los sistemas para que, atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones, se adecue el estado de seguridad y se puedan detectar tempranamente posibles incidentes de seguridad.

j) Protección de la información almacenada y en tránsito. Se protegerán los entornos que contienen información almacenada y en tránsito entre entornos inseguros. En este sentido se protegerán convenientemente los equipos portátiles que puedan contener información, así como los soportes extraíbles (pendrives, discos duros extraíbles, etc.).

En el caso de la existencia de una normativa de protección de la información, más restrictiva, se dará cumplimiento a la misma. Esta normativa puede ser interna o externa.

k) Prevención ante otros sistemas de información interconectados. Se desplegarán las protecciones necesarias para proteger el perímetro de la red corporativa de la OAAF, de forma que se neutralicen las posibles intrusiones procedentes del exterior, ya sea iniciadas malintencionadamente por terceros o como consecuencia de la interconexión con sistemas de terceros.

l) Registro de actividad. Los sistemas y aplicaciones generarán los registros de actividad necesarios para conocer la actividad en los sistemas, de forma que se pueda determinar en todo momento qué persona actúa, sobre qué datos, con qué operaciones y sus privilegios de acceso.

m) Incidentes de seguridad. La OAAF definirá e implantará procedimiento de gestión de incidentes de seguridad que asegure la correcta gestión y respuesta para mitigar o minimizar el impacto del incidente. procedimiento de comunicación, gestión y respuesta a incidentes de seguridad contemplará la comunicación y notificación de los incidentes a las correspondientes autoridades de control, en su caso, de acuerdo con la legislación vigente.

n) Continuidad de la actividad. Los sistemas dispondrán de copias de seguridad y se establecerán los mecanismos que fuesen necesarios para garantizar que la Organización pudiese continuar con las operaciones.

o) Mejora continua del proceso de seguridad. Se deberá establecer un Sistema de Gestión de la Seguridad que permita conocer en cada momento el estado de la seguridad, mediante la definición y medida de indicadores, y permita tomar las decisiones informadas pertinentes para cumplir los requisitos de seguridad establecidos.

00319334

Se establecerá un proceso de mejora continua mediante el análisis de la situación, la implantación de nuevas medidas de seguridad, la mejora de las existentes y la aportación de mejoras sugeridas por el Comité de Seguridad de la Información o personal de la OAAF.

9. Organización de la seguridad de la información.

Conforme a los establecido en el ENS, así como las pautas establecidas en las Guías CCN-STIC, la OAAF se soportará sobre la estructura y roles que se describen a continuación:

- Estructura de especificación. Es la que se encarga de establecer los requisitos de seguridad asociados a los servicios prestados y a garantizar el cumplimiento normativo asociado que le es de aplicación, específicamente, respecto del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Estructura de supervisión. Es la que se encarga de verificar el cumplimiento de los requisitos de seguridad y el alineamiento continuo con los objetivos de la organización.
- Estructura operativa. Se encarga de implantar las medidas de seguridad identificadas.

9.1. Estructura de especificación.

Esta estructura es la encargada de determinar los requisitos de seguridad que serán de aplicación a los servicios prestados por la Organización y a garantizar el cumplimiento normativo asociado a la aplicación del ENS. Forman parte de la Estructura de Especificación:

- Comité de Seguridad de la información.
- Responsable de la Información.
- Responsable de los Servicios.
- Responsable del Tratamiento.

9.1.1. Comité de seguridad de la Información.

Coordinará la seguridad de la información en la Organización. El Comité de Seguridad de la Información, (en adelante, CSI) tiene como funciones:

- Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por la persona titular de la Dirección de la Oficina, en los términos establecidos en el ENS.
- Aprobar la normativa interna en el ámbito de la seguridad de la información que fuese necesario.
- Verificar los procedimientos de seguridad de la información y demás documentación para su posterior aprobación por el Responsable de Seguridad.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos de Tecnología de la Información (TI), desde su especificación inicial hasta su puesta en operación siempre que se traten de sistemas de información que se encuentren dentro del alcance de la PSI.
- Promover la realización de las auditorías periódicas, que permitan verificar el cumplimiento de las obligaciones en materia de seguridad que establezca la Política de Seguridad y la normativa vigente.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables, pudiendo elevar a la Dirección de la OAAF aquellos casos en los que no tenga suficiente autoridad para decidir.
- Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
- Elaborar y aprobar los requisitos de formación y calificación de los administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.
- Realizar un seguimiento de los principales riesgos residuales asumidos por la Organización y recomendar posibles actuaciones respecto de ellos.
- Atender las inquietudes de la Dirección de la OAAF e informarla regularmente sobre el estado de la seguridad.
- Promover la mejora continua del sistema de gestión de la seguridad.

00319334

- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Elaborar la estrategia de la organización en materia de seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas para evitar duplicidades y asegurar la consistencia con la estrategia de seguridad.

Este Comité estará integrado por aquellas personas con responsabilidad en la toma de decisión en seguridad de la información y aquellas que sean designadas por representación. Serán miembros del Comité de Seguridad de la Información:

- Responsable de los Servicios. Que ostentará la Presidencia del órgano.
- Responsable de Seguridad. Que ostentará la Secretaría del órgano.
- Responsable del Sistema. Que osentará la suplencia de la Presidencia en caso de ausencia de su titutar.
- Responsable o Responsables de la Información. Entre los cuales se designará a la suplencia de la Secretaría en caso de ausencia de la persona titular.

Los Responsables de la Información y de los Servicios serán convocados en función de los asuntos a tratar.

El Delegado o la Delegada de Protección de Datos participará con voz, pero sin voto en las reuniones del Comité de seguridad de la información cuando en el mismo vayan a abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal, así como siempre que se requiera su participación. En todo caso, si un asunto se sometiese a votación, se hará constar siempre en acta la opinión del Delegado o Delegada de Protección de Datos.

La Persona titular de la Dirección o persona en quién delegue podrá asistir, con voz, pero sin voto, a petición propia y/o cuando la naturaleza de los temas a tratar así lo requiera.

Con carácter opcional, podrán asistir al Comité de Seguridad de la Información personal técnico, propio o externo, para asesoramiento en materia de seguridad de la información.

El CSI se reunirá periódicamente al menos cuatrimestralmente ocuando existan propuestas o eventos que lo justifiquen, previa convocatoria al efecto realizada con 48 horas de antelación. En la convocatoria se incluirán los asuntos del orden del día a tratar.

Se podrán realizar reuniones con carácter extraordinario, siendo la convocatoria con un plazo de 24 horas. En la misma se referenciará el carácter extraordinario y urgente de la convocatoria, así como los asuntos del orden del día a tratar. En las sesiones extraordinarias no se incluirá el apartado de ruegos y preguntas.

La Presidencia del Comité tendrá la facultad de suspender la celebración de las sesiones del CSI como consecuencia de los periodos vacacionales, cuando ello no suponga un menoscabo a la seguridad, así como para posponer o adelantar la celebración de las sesiones ordinarias del Comité, dentro de la misma semana de su celebración, cuando el día fijado sea festivo.

Para la válida constitución del CSI, a efectos de la celebración de sesiones, deliberaciones y toma de acuerdos, se requerirá la asistencia, presencial o a distancia, de la persona que ostente la Presidente y de la persona que ostente la Secretaría o, en su caso, de quienes les suplan, y la de la mitad, al menos, de sus miembros.

Las reuniones del CSI no serán retribuidas, a excepción de los gastos por desplazamiento que, en su caso, puedan producirse.

En lo no previsto por la presente PSI, el funcionamiento del Comité se regirá por lo dispuesto en la sección 3.ª del capítulo II del título preliminar de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

9.1.2. Responsable del Servicio.

Determina los requisitos (de seguridad) de los servicios prestados. En el caso de la OAAF será una persona física, con una visión general y horizontal sobre los servicios prestados, ya que en éstos intervienen varios departamentos específicos.

00319334

Serán funciones del Responsable del Servicio:

- Determinar la valoración de los servicios conforme los criterios establecidos en la normativa en vigor.
- Determinar los requisitos de seguridad de los servicios.
- Emitir dictámen, no vinculante, para elevar al Responsable de Seguridad, cuando se restrinja el derecho de acceso a los servicios por parte de denunciantes, denunciados e interesados en procedimientos.
- Aceptar los niveles de riesgo residual que afectan a los servicios.
- La aprobación formal de los niveles de seguridad de los servicios, pudiendo recabar la propuesta del Responsable de la Seguridad y la opinión del Responsable del Sistema.
- Poner en comunicación del Responsable de la Seguridad cualquier variación respecto a los Servicios de los que es responsable, especialmente la incorporación de nuevos Servicios.
- Determinar el impacto de una indisponibilidad de estos servicios en las actividades de los servicios.
- Determinar los fines y medios del correspondiente tratamiento de datos personales, a los efectos previstos en el RGPD.

9.1.3. Responsable de la Información.

Determina los requisitos (de seguridad) de la información tratada. En el caso de la OAAF serán dos personas de perfil técnico, uno de cada una de las Subdirecciones que intervienen en la gestión y tratamiento de datos de una denuncia (Subdirección de Investigación, Inspección y Régimen Sancionador y Subdirección de Asuntos Jurídicos Prevención y Protección al Denunciante).

- Determinar la valoración de la información conforme los criterios establecidos en la normativa en vigor.
- Determinar los requisitos de seguridad de la información.
- Aceptar los niveles de riesgo residual que afectan a la información
- Poner en comunicación del Responsable de la Seguridad cualquier variación respecto a la información de la que es responsable, especialmente la incorporación de Información a su cargo.
- Determinar los fines y medios del correspondiente tratamiento de datos personales, a los efectos previstos en el RGPD.

9.1.4. Responsable del Tratamiento.

El Responsable de Tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento. El Responsable del Tratamiento es la propia Organización. Las funciones del Responsable del Tratamiento son:

- Garantizar la observancia de los principios relativos al tratamiento y aprobar la política, normativa y procedimientos concernientes a la protección de datos personales.
- Designar al Delegado o Delegada de Protección de Datos.
- Adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales y evitar su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. En particular, difundirá entre el personal las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudieran incurrir en caso de incumplimiento.
- Garantizar el cumplimiento de las políticas y procedimientos aprobados e implementados en la OAAF en materia de protección de datos.
- Realizar evaluaciones del impacto en la protección de datos personales, cuando corresponda.
- Asegurar que la realización de tratamientos por cuenta de terceras partes esté regulada en un contrato, que deberá constar por escrito o en alguna otra forma que permita

00319334

acreditar su celebración y contenido, estableciéndose expresamente que la persona encargada del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará (ni siquiera para su conservación) a otras personas.

- Adoptar las medidas correctoras que fuesen necesarias y pertinentes cuando se detecten deficiencias respecto al cumplimiento de la normativa vigente aplicable en materia de protección de datos o se detecten anomalías que pudiesen comprometer los datos personales objeto de tratamiento.

9.2. Estructura de supervisión.

Esta estructura se encarga de verificar la correcta implantación y operación de los requistios de seguridad que se hayan establecido, de cara a mantener la alineación con los objetivos y de cumplir con la normativa y legislación aplicable.

En la supervisión global de todas las actividades relativas a la seguridad de la información, se encuentra el Responsable de Seguridad de la información.

En el ámbito de supervisión, también se encuadra la figura del Delegado o Delegada de Protección de Datos. Las funciones y responsabilidades de cada una de las figuras mencionadas, se describen en los siguientes apartados.

9.2.1. Responsable de Seguridad.

Determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones. Por tanto, son funciones derivadas de este rol, aquellas relacionadas con el liderazgo de la seguridad y aquellas relacionadas con las operaciones de seguridad. Será distinto del Responsable del Sistema, no debiendo existir dependencia jerárquica entre ambos. Excepcionalmente podrá ser autorizado por el máximo órgano de seguridad, que, en ausencia de recursos, obligue a que ambas funciones recaigan en la misma persona o en distintas personas entre las que exista relación jerárquica, siempre que se desplieguen medidas compensatorias para garantizar la diferenciación de responsabilidades. Serán funciones del Responsable de la Seguridad:

- Desarrollar las funciones de supervisión de la seguridad, en colaboración con el Responsable del Sistema.
- Determinar las decisiones y acciones necesarias, para cumplir con los requisitos de seguridad de la información y los servicios.
- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los Servicios prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Designar responsables de la ejecución de los procesos de análisis de riesgos, desarrollar, documentar y aprobar formalmente la Declaración de Aplicabilidad, identificación de las medidas de seguridad necesarias, determinar las configuraciones de seguridad necesarias, y encargarse de que el personal responsable elabore la documentación del sistema y en su caso, custodiarlo debidamente.
- Considerar medidas adicionales a las requeridas por el ENS, o en su caso, reemplazar las requeridas por otras compensatorias, habida cuenta del estado de la tecnología, la naturaleza de la información tratada o los servicios prestados y los riesgos a que están expuestos los sistemas de información afectados.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad, procediendo a su validación.
- Colaborar con las auditorías externas/internas en materia de seguridad de la información, revisarlas y encargar a los responsables de los sistemas la implantación de las correcciones que se deriven.
- Gestionar los procesos de certificación.
- Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.

00319334

- Coordinar con el CSIRT y/o la Autoridad de Control correspondiente, cualquier «incidente» que tenga un impacto significativo en la prestación de sus servicios. En su caso, notificar a las personas destinatarios de los servicios, información relacionada con el incidente, las medidas o soluciones frente a la ciberamenaza o cualquier información que se considere relevante.

- Aprobar los procedimientos de seguridad que forman parte del Mapa Normativo (y no son competencia expresa de otros roles) y poner en conocimiento del CSI las modificaciones que se hayan realizado a lo largo del periodo en curso entre reuniones.

- Convocar las reuniones del Comité de Seguridad.

Para el desarrollo de las funciones se pueden considerar un único Responsable de la Seguridad o varios, diferenciando claramente sus funciones y responsabilidades y el ámbito de actuación asignado.

El Responsable de la Seguridad podrá delegar funciones en otras personas u órganos o entidades, pero no podrá delegar la responsabilidad de las siguientes:

- Funciones relacionadas con la normativa, identificación de las tendencias de seguridad seguidas por el sistema, y el seguimiento de la mejora y eficiencia del sistema.
- Supervisión y conformidad del sistema.
- Operativas de la seguridad del sistema.
- Medidas de seguridad generales, salvo su aprobación.
- Medidas de seguridad complementarias o fuentes añadidas, salvo su aprobación.
- Medidas compensatorias o complementarias, salvo su aprobación.
- Ejecución del análisis de riesgos y desarrollo de propuesta de tratamiento de riesgos.
- Procedimientos operativos de seguridad.
- Propuestas de formaciones y acciones de sensibilización.
- Desarrollo de análisis de continuidad y propuestas de estrategias de resiliencia.
- Análisis del ciclo de vida de los componentes del sistema.

9.2.2. Delegado o Delegada de Protección de Datos.

Las funciones del Delegado o Delegada de Protección de Datos son:

- Velar para que la Organización cumpla con la normativa de protección de datos y respete los derechos de los interesados.

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben de conformidad con el RGPD y de otras disposiciones de protección de datos de la Unión Europea o de los Estados miembros.

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

- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.

- Cooperar con la autoridad de control.

- Actuar como punto de contacto de la autoridad de control.

9.3. Estructura de operación.

La estructura de operación de la seguridad debe asumir la administración operativa de la seguridad de los sistemas de información, implantando en dichos sistemas las medidas necesarias para satisfacer los requisitos establecidos por la estructura de especificación. Formará parte de esta estructura el responsable del Sistema.

9.3.1. Responsable del Sistema.

Se encargará de implementar la seguridad en el sistema y supervisar la operación diaria del mismo, pudiendo delegar en administradores algunas funciones.

00319334

Podrá apoyarse en áreas o servicios propios o de terceros con funciones en ciberseguridad para el desarrollo de funciones específicas proactivas y tácticas, como vigilancia, monitorización y respuesta. Serán funciones del Responsable del Sistema:

• Desarrollar, operar y mantener los sistemas de información afectados por el ENS durante todo su ciclo de vida: especificaciones, instalación y verificación de su correcto funcionamiento.

• Definir la topología y sistema de gestión de dichos sistemas de información estableciendo los criterios de uso y los servicios disponibles en los mismos.

• Elaborar los procedimientos operativos de seguridad que deberán ser aprobados por el Responsable de Seguridad.

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

• Elaborar junto con el Responsable de Seguridad los planes de mejora de la seguridad.

• Detener el acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad, debiendo recabar el previo acuerdo de los Responsables de la información afectada, del servicio afectado y del Responsable de Seguridad, antes de ser ejecutada.

• Garantizará que los dispositivos que abandonen las instalaciones mantienen la seguridad necesaria conforme a las necesidades de la información que manejan.

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

Además, para llevar a cabo, en su caso, las funciones del administrador de la seguridad del sistema:

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

• La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.

• Aprobar los cambios en la configuración vigente del Sistema de Información.

• Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.

• Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.

• Supervisar las instalaciones de componentes, su mantenimiento, modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.

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

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

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

9.4. Procedimiento de designación.

La creación del Comité de Seguridad de la Información, el nombramiento de sus integrantes y la designación de los responsables identificados en esta política se realizará por la persona titular de la Dirección de la OAAF, a propuesta de la Dirección adjunta.

Los miembros del Comité, así como los roles de seguridad serán revisados cada dos años o con ocasión de vacante.

9.5. Resolución de conflictos.

Los conflictos entre las diferentes personas, unidades u órganos responsables que componen la estructura organizativa de la política de seguridad serán resueltos por el superior jerárquico común. En su defecto, prevalecerá la decisión del CSI (Comité de Seguridad de la Información), elevando a la Dirección de la OAAF aquellos casos en los que no tenga suficiente autoridad para decidir.

00319334

10. Desarrollo de la Política de Seguridad de la Información.

La documentación relativa a la Seguridad de la Información estará clasificada en cuatro niveles, de manera que cada documento de un nivel se fundamenta en los de nivel superior:

Primer nivel: Política de Seguridad de la Información. Documento de obligado cumplimiento por todo el personal, interno y externo de la Organización, recogido en el presente documento y aprobado por la Dirección de la OAAF.

Segundo nivel: Procedimientos de Seguridad. De obligado cumplimiento de acuerdo con el ámbito organizativo, técnico o legal correspondiente. Describirán de forma general los principios y normas de seguridad que serán concretados en los niveles posteriores. Se podrá seguir en todo momento los procedimientos, normas e instrucciones técnicas STIC, así como las guías CCN-STIC.

La responsabilidad de aprobación de los documentos redactados en este nivel será competencia del Responsable de Seguridad bajo la supervisión del CSI.

Tercer nivel: Normas Técnicas. Estos documentos completarán los procedimientos y recogerán instrucciones concretas sobre el modo en que deben llevarse a cabo determinadas actuaciones.

Cuarto Nivel: Informes, registros y evidencias electrónicas. Documentos a través de los cuales quedará evidencia de la puesta en práctica de las directrices marcadas por el propio Sistema de Gestión.

11. Protección de datos personales.

La OAAF trata datos de carácter personal en el ejercicio de sus competencias y de acuerdo con la normativa vigente. El tratamiento de datos se ajustará a las obligaciones y principios recogidos 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 y por el que se deroga la Directiva 95/46/CE (RGPD); a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales; la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción; y la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

Todos los sistemas de información de la Organización que traten datos de carácter personal se ajustarán a la normativa y asignarán las medidas técnicas y organizativas que fuesen necesarias para proteger los datos personales, en base al riesgo que aplique a cada tratamiento.

Adicionalmente, la OAAF ha nombrado un Delegado de Protección de Datos, que estará a disposición de los interesados para atender cualquier cuestión relacionada con la aplicación de la normativa de protección de datos.

12. Terceras partes.

Cuando se presten servicios o se gestione información de otras organizaciones, se les hará participe de esta PSI.

Cuando se utilicen servicios de terceros o se ceda información a terceros, se les hará participe de esta PSI y de la normativa de seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, sin perjuicio de que pueda desarrollar sus propios procedimientos operativos para satisfacerla.

Las entidades terceras deberán seleccionarse atendiendo a los principios de idoneidad y cumplimiento de los marcos normativos exigibles, además del resto de

00319334

criterios aplicables de contratación. También se debedrán garantizar que el personal de terceros está adecuadamente formado y concienciado en materia de seguridad.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según serequiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

13. Incumplimiento.

El incumplimiento de la presente PSI, podrá tener como resultado el inicio de aplicación de medidas disciplinarias que procediesen, sin perjuicio de posibles responsabilidades legales que fuesen de aplicación.

14. Revisión.

De acuerdo con el principio de reevaluación periódica, la presente PSI será objeto de revisión anual, a fin de adaptarse a las circunstancias técnicas u organizativas y evitar su obsolescencia.

00319334