POLITICA DE SEGURIDAD DE LA INFORMACIÓN

Sistema de Gestión de Seguridad de la Información basado en ENS

Nombre:	NS-SGSI-01 Política de seguridad de la información ASSAP AUDITORES
Título:	Política de seguridad de la información (v.r.) A. Auditores
Edición:	V.1.0
Clasificación:	Interno
Estado:	Publicado
Fecha:	10/05/2024
Páginas:	18
Editado por:	Responsable de Seguridad
Revisado por:	Comité de Seguridad de la Información
Aprobado por:	Direccion

[X] **Copia controlada**	[ ] **Copia no controlada**	**Nº 01**

HOJA DE CONTROL			
Título	Política de seguridad de la información		
Entregable	NS-SGSI-01 Política de seguridad de la información ASSAP AUDITORES		
Nombre del Fichero	NS-SGSI-01 Política de seguridad de la información ASSAP AUDITORES		
Autor	Responsable de Seguridad de la Información		
Versión/Edición	V.1.0	**Fecha Versión**	10/05/2024
Aprobado por	Dirección	**Fecha Aprobación**	10/05/2024
		Nº Total Páginas	18

REGISTRO DE CAMBIOS				
Versión	**Cambio**	**Responsable del Cambio**	**Área**	**Fecha del Cambio**
V.1.0	Creación del documento	Responsable de Seguridad de la Información	ENS	10/05/2024

ÍNDICE

1. INTRODUCCIÓN

El presente documento constituye la Política de Seguridad de la Información de ASSAP AUDITORES, S.L. (en adelante ASSAP) y da cumplimiento al artículo 12 del Real Decreto 311/2022, de 3 de mayo por el que se regula por el que se regula el Esquema Nacional de Seguridad, y a la medida de seguridad org.1 contemplada en el Anexo II de dicho Real Decreto.

La estructura de este documento sigue las pautas establecidas por las guías del Centro Criptológico Nacional, para la redacción de la Política de Seguridad de la Información en el ámbito del Esquema Nacional de Seguridad y recoge la postura de ASSAP en cuanto a la seguridad de la información y establece los criterios de obligado cumplimiento que deben regir nuestra actividad de auditoría en cuanto a la seguridad.

Los sistemas de información deben estar protegidos contra amenazas con potencial para incidir en la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios de auditoría.

Este documento se compromete a cumplir escrupulosamente con las garantías exigidas por el Esquema Nacional de Seguridad, RGPD, LOPDGDD y con el resto de legislación vigente aplicable en esta materia.

Con ocasión de ello, esta Política de Seguridad de la Información se desarrollará a través de un Sistema de Gestión de Seguridad de la Información (SGSI) documentado y con procedimientos regulados de aprobación, revisión y actualización constante.

Esta Política de seguridad de ASSAP AUDITORES S.L., al entrar en vigor, sustituye cualquier otra que existiera a nivel de los diferentes departamentos o áreas de la organización.

2. ALCANCE Y AMBITO DE APLICACIÓN

La presente Política de Seguridad de la Información define el marco y organización de la gestión y protección de la información y servicios de ASSAP AUDITORES, S.L., incluyendo **todos los sistemas información que dan soporte a la prestación de servicios de auditoría a clientes según la declaración de aplicabilidad vigente**. En concreto, además de a dichos sistemas, aplica a todas las TIC y activos que resultan necesarios para la prestación de servicios de gestión y auditoría.

Para responder a su misión de ofrecer a sus clientes servicios de auditoría adecuados, protegidos de la destrucción, indisponibilidad, manipulación o revelación no autorizada de la información, ASSAP reconoce expresamente la importancia de diseñar e implementar controles de seguridad para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad, y conservación de los datos, informaciones y servicios utilizados que se gestionen en **el** ejercicio de sus competencias. La presente Política pretende describir y formalizar la posición y las directrices principales de la seguridad de la información.

Esta Política debe ser conocida y cumplida por todo el personal, independientemente del puesto, cargo y responsabilidad dentro de ASSAP.

Todas las personas que intervengan en cualquier fase del tratamiento de datos están sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del RGPD y 5 de la LOPDgdd, y podrán responder del tratamiento que se realice sobre los datos que manejen.

3. MARCO NORMATIVO

3.1 PRINCIPAL LEGISLACION

Se toma como marco normativo de referencia, a título ejemplificativo y sin carácter exhaustivo, la siguiente legislación:

- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
- 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.
- Ley 11/2022, de 28 de junio, General de Telecomunicaciones.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- 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 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.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Asimismo, resultarán de aplicación cuantas otras normas regulen la actividad de ASSAP AUDITORES S.L. en el ámbito de la prestación de sus servicios y aquellas otras dirigidas a asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en los medios electrónicos gestionados de sus clientes empresas, entidades y administraciones públicas en el ejercicio de su actividad y competencias. En especial, la Ley 22/2015, de 20 de julio, de Auditoría de Cuentas.

3.2 OTRAS NORMAS DE REFERENCIA.

A mayor abundamiento, para la elaboración de esta Política de Seguridad se han tenido en cuenta las Guías de Seguridad del Centro Criptológico Nacional (CCN-STIC); en especial, la Guía 805 relativa a la Política de Seguridad de la Información en el Esquema Nacional de Seguridad (CCN-STIC-805) y la Guía 801 relativa a las Responsabilidades y Funciones en el Esquema Nacional de Seguridad (CCN-STIC-801).

4. GLOSARIO DE TÉRMINOS Y ABREVIATURAS

4.1. TÉRMINOS

- DATOS DE CARÁCTER PERSONAL. Toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.
- SISTEMA DE INFORMACIÓN. Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.
- POLÍTICA DE SEGURIDAD. Conjunto de directrices plasmadas en un documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que considera críticos.
- PRINCIPIOS BÁSICOS DE SEGURIDAD. Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.
- INCIDENTE DE SEGURIDAD. Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.
- GESTIÓN DE INCIDENTES. Plan de acción para atender a las incidencias que se den. Además de resolverlas debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.
- ANÁLISIS DE RIESGOS. Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.
- GESTIÓN DE RIESGOS. Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.
- RESPONSABLE DE LA INFORMACIÓN. Persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.
- RESPONSABLE DEL SERVICIO. Persona que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.
- RESPONSABLE DEL SISTEMA. Persona que se encarga de la explotación del sistema de información.

4.2. ACRONIMOS

- ENS. Esquema Nacional de Seguridad.
- LOPDGDD. Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.
- RGPD. Reglamento General de Protección de Datos.
- CCN. Centro Criptológico Nacional.
- TIC. Tecnologías de la Información y las Comunicaciones.
- STIC. Seguridad de las Tecnologías de la Información y las Comunicaciones.
- CSI. Comité de Seguridad de la Información.
- PSI. Política de Seguridad de la Información.
- RD. Real Decreto.

5. DESCRIPCIÓN DE LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN

5.1. MISIÓN Y OBJETIVOS DE LA ORGANIZACIÓN

ASSAP AUDITORES S.L. ha establecido un marco de gestión de la seguridad de la información según lo establecido por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en adelante ENS, reconociendo como activos estratégicos la información y los servicios prestados y los sistemas que los soportan.

ASSAP depende de los sistemas TIC para prestar sus servicios y para alcanzar sus objetivos, por lo que la adopción de las medidas necesarias para garantizar la disponibilidad, trazabilidad, integridad, autenticidad o confidencialidad de la información tratada es un elemento y objetivo crucial en nuestra actividad. Los objetivos de seguridad de la información de ASSAP son:

1. Garantizar la garantizar la integridad, confidencialidad, autenticidad, trazabilidad y protección de la información de ASSAP y de nuestros clientes
2. Garantizar la prestación continuada de los servicios, actuando preventivamente, supervisando la y reaccionando ante incidentes.
3. Asegurar el cumplimiento eficiente del ENS y de cualquier obligación legal en materia de seguridad
4. Incorporar las mejores prácticas y la mejora del sistema de gestión de seguridad de la información

La Política de Seguridad de la Información protege la información derivada de los servicios de auditoría prestados (tanto propia, como de clientes), así como la continuidad de los servicios, de las amenazas a los que éstos pueden verse sometidos, garantizando la continuidad de los sistemas de información, minimizando los riesgos de daño y asegurando el eficiente cumplimiento de los objetivos y servicios de ASSAP AUDITORES S.L.

5.2. PRINCIPIOS RECTORES Y REQUISITOS MÍNIMOS

Nuestra política cumple los principios básicos señalados en el capítulo II del ENS y se desarrolla en base a los siguientes requisitos mínimos:
a) Organización e implantación del proceso de seguridad: La seguridad comprometerá a todos los miembros de ASSAP, sin excepción.
b) Análisis y gestión de los riesgos: Conforme al apartado 9.
c) Gestión de personal: En las políticas de uso interno, se detallarán la obligatoriedad de conocimiento y concienciación en materia de seguridad según sus responsabilidades.
d) Profesionalidad: Periódicamente se diseñará un plan de formación específico en el que se tiene en cuenta las necesidades de profesionalización del sistema de seguridad.
e) Autorización y control de acceso: 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.
f) Protección de las instalaciones: Los sistemas de información se ubicarán en zonas protegidas, con acceso restringido, habilitado únicamente al personal autorizado.
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 específicos de selección de proveedores y productos
h) Mínimo privilegio. Los sistemas y aplicaciones se diseñarán y construirán ofreciendo la funcionalidad mínima necesaria, y ninguna adicional.
i) Integridad y actualización del sistema: Se seguirán en todo momento las informaciones acerca de las vulnerabilidades que afectan a los sistemas de información y las recomendaciones de los fabricantes de equipos y software.
j**) Protección de la información almacenada y en tránsito:** Se protegerán los entornos que contienen información almacenada y en tránsito entre entornos inseguros, en especial los equipos portátiles y soportes extraíbles.
k) Prevención ante otros sistemas de información interconectados: Se desplegarán las protecciones necesarias para proteger el perímetro de la red corporativa.
l) Registro de la actividad y detección de código dañino: 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: ASSAP ha definido un procedimiento de gestión de incidentes de seguridad que aseguran la correcta gestión y respuesta efectiva., incluyendo las obligaciones exigidas por el RGPD y la LOPDGDD cuando afectan a datos personales.
n) Continuidad de la actividad: Para asegurar la disponibilidad de los servicios y sistemas de información se establecerán medidas que permitan, ante una contingencia, la reanudación de los servicios y sistemas de información a los niveles adecuados de operatividad.
o) Gestión de la seguridad y mejora continua: Se deberá establecerán indicadores que permitan tomar las decisiones informadas pertinentes para cumplir los requisitos de seguridad establecidos y se realizará un análisis de la situación para mejorar el sistema de gestión de seguridad de la información

5.3. GESTION DE INCIDENTES DE SEGURIDAD

A través de este documento ASSAP AUDITORES S.L. se prepara para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Artículo 8 del ENS.

5.3.1. Prevención.

Uno de los objetivos fundamentales es esquivar los riesgos que pueden perjudicar la información y/o los servicios por los incidentes de seguridad evitables; y reducir al mínimo la exposición a los riesgos que no resultan evitables. Para ello, ASSAP AUDITORES S.L. se propone disponer de todas las medidas de seguridad necesarias para el cumplimiento de las exigencias del ENS y de la normativa relativa a protección de datos, junto a los controles adicionales identificados a través de una evaluación de amenazas y riesgos.

5.3.2. Detección.

En previsión de la posibilidad de degradación de la información y/o servicios, ASSAP AUDITORES S.L. establece el objetivo de monitorizar las operaciones y procedimientos para detectar anomalías y actuar en consecuencia desarrollando planes de mejora continua conforme al Artículo 10 del ENS.

5.3.3. Reacción.

En aras de asegurar el acceso, integridad, confidencialidad, disponibilidad, autenticidad, trazabilidad de la información y la prestación continuada de los servicios ASSAP AUDITORES S.L. se propone establecer los mecanismos para responder eficazmente a los incidentes de seguridad. Esto es, incluyendo la designación de puntos de contacto en cada departamento para las comunicaciones respecto a incidentes ocurridos en el seno de cada una de éstos; así como el establecimiento de las medidas necesarias para un adecuado intercambio de información relacionada con el incidente en cuestión.

5.3.4. Recuperación.

Para la garantía de la disponibilidad de la información y de los servicios, ASSAP AUDITORES S.L. también establece como objetivo el desarrollo de planes de continuidad de los sistemas TIC como parte de su misión de implementar el valor de la Seguridad de la Información en el conjunto de la Organización y su respuesta frente a incidentes de seguridad.

6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN ASSAP

6.1. ROLES: FUNCIONES Y RESPONSABILIDADES

6.1.1. Responsable de la Información

Le corresponde la potestad de establecer los requisitos de la información en materia de seguridad, es decir, la potestad de determinar los niveles de seguridad de la información. Será quien determinará los requisitos de seguridad aplicables a la información bajo su responsabilidad y su nivel correspondiente.

Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, conviene que se escuche la opinión del Responsable del Sistema. Es el responsable último de cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad (en materia de protección de datos) y de disponibilidad (en materia de seguridad de la información).

6.1.2. Responsables de los servicios

Son los roles que deben establecer los requisitos de seguridad aplicables a los servicios bajo su responsabilidad. Ostentarán las siguientes responsabilidades específicas:

- Determinar los niveles de seguridad de los servicios. Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, se puede recabar una propuesta al Responsable de la Seguridad y conviene que se escuche la opinión del Responsable del Sistema.
- Velar por la inclusión de cláusulas de seguridad en los contratos con terceras partes y por su cumplimiento.
- Colaborar en el análisis de impacto de los incidentes que se puedan producir y plantear las estrategias y salvaguardas ante los mismos.
- Cualquier otra función que pueda ser encomendada por los órganos correspondientes.

6.1.3. Responsable del tratamiento

De acuerdo con lo especificado en el RGPD y la LOPDGDD, la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento. Este rol, que recae sobre ASSAP AUDITORES S.L., representada por la figura del Administrador de la entidad.

6.1.4. Delegado de Protección de Datos

Tiene asignadas las funciones contempladas en el art. 39 del Reglamento General de Protección de Datos.

6.1.5. Responsable de Seguridad de la Información

El Responsable de la Seguridad de la Información tomará las decisiones necesarias para satisfacer los requisitos de seguridad establecidos por el responsable y de los servicios. Este rol asume las siguientes responsabilidades específicas:

- Determinar la categoría del sistema y las medidas de seguridad que deben aplicarse (declaración de aplicabilidad)
- Informar al Responsable de la Información y a los Responsables de los Servicios de las incidencias de seguridad.
- Llevar a cabo el seguimiento de la Política de Seguridad de la Información de manera operativa, así como desarrollar las normativas y procedimientos derivados del sistema de seguridad de la información tanto relativos a la seguridad física y lógica de los recursos. y su supervisión.
- Determinar las medidas de seguridad necesarias para la protección de la información manejada y los servicios prestados y verificar que las establecidas son adecuadas en todo momento.
- Constituirse como punto de contacto con las autoridades competentes de referencia.
- Reportar el estado de la seguridad al Comité de Seguridad de la Información.
- Impulsar o instar la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones en materia de seguridad de la información.
- Cualquier otra función que pueda ser encomendada por los órganos correspondientes.

6.1.6. Responsable del sistema

El responsable de los sistemas de información será el encargado de aplicar las medidas de seguridad de índole tecnológica determinadas por el Responsable de la seguridad. Asumirá las siguientes responsabilidades específicas:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la tipología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.
- Cualquier otra función que pueda ser encomendada por los órganos correspondientes.
- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.
- La gestión de las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- La aplicación de los Procedimientos Operativos de Seguridad (POS).
- Asegurar que los controles de seguridad establecidos son adecuadamente observados.
- Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
- Supervisar las instalaciones de hardware y software, sus 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 del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- 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.

6.1.7. Responsable de RRHH

Cumplirá la función de implicar a todo el personal de la organización en el conocimiento y cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan, así como de los cambios que en aquellas se produzcan. Igualmente, se responsabilizará de la implementación de los compromisos de confidencialidad que deban suscribir los empleados y colaboradores y de la capacitación continua de los mismos en materia de seguridad.

6.2. COMITÉS: FUNCIONES Y RESPONSABILIDADES

6.2.1. Dirección de ASSAP AUDITORES S.L.

Tiene las siguientes funciones:

- Aprobar, como parte del Comité de Seguridad, la Política de Seguridad de la Información de LAS ENTIDADES ASSAP y cualquier otra política sectorial complementaria de la anterior que permita el cumplimiento del ENS y el Reglamento General de Protección de Datos y normativa aplicable en materia de protección de datos.
- Aprobar el desarrollo organizativo propuesto por el Comité de Seguridad de la Información (Comité SI).
- Participación en el nombramiento y cese de los integrantes del Comité SI.
- Adoptar las medidas pertinentes, en materia de seguridad de la información, a propuesta del Comité SI.

- Nombrar al Delegado de Protección de Datos, a propuesta del Presidente del Comité SI, previo informe del Responsable de Seguridad.

6.2.2. Comité de Seguridad de la Información

El comité CSI tiene las siguientes funciones:

- Elaborar y proponer la política de seguridad de la organización de ASSAP AUDITORES S.L., para su posterior aprobación por la Dirección.
- Velar porque la seguridad de la información sea parte del proceso de planificación de ASSAP AUDITORES S.L.
- Velar por el cumplimiento de la normativa de aplicación legal, regulatoria y sectorial referente a la seguridad de la información y a la protección de datos de carácter personal.
- Elaborar y proponer a la Dirección el desarrollo organizativo que permita el cumplimiento del ENS, así como del Reglamento General de Protección de Datos y normativa complementaria.
- Recabar informes regulares del estado de seguridad de la información de la organización y de los posibles incidentes referentes a Tecnologías de Información y Comunicación (TIC); trasladando sus conclusiones a Dirección.
- Coordinar las actuaciones de seguridad y dar respuesta a las inquietudes de seguridad transmitidas a través de los responsables de los distintos departamentos.
- Promover la difusión y apoyo a la seguridad de la información dentro de la estructura orgánica de ASSAP AUDITORES S.L.
- Llevar a cabo acciones de concienciación, formación y motivación del personal afectado por esta Política, sobre la importancia de lo establecido en el marco de gestión de seguridad de la información y sobre su implicación en el cumplimiento de las expectativas de los departamentos, usuarios y la protección de su información.

6.2.3. Procedimiento de designación y delegación de funciones en ASSAP

El Responsable de Seguridad y el Responsable del Sistema se designan por la durante un período anual, renovable automáticamente. El resto de los responsables y directores serán asignados en función de las necesidades operativas y organizativas de la organización.

El sistema de delegación de funciones está previsto en el documento de Funciones y responsabilidades en materia de seguridad de la información

6.3. Revisión de la Política de Seguridad de la Información.

El CSI se reunirá al menos cada 6 meses para verificar el cumplimiento de la presente Política de Seguridad y hacer cumplir las directrices generales y actuaciones correspondientes contenidas en ésta y para plantear acciones correctivas y preventivas necesarias para cumplir los objetivos del plan de tratamiento de riesgos y la mejora continua de la seguridad de la información.

7. ESTRUCTURA DE LA DOCUMENTACION DE SEGURIDAD

La Política de Seguridad de la Información es de obligado cumplimiento y se estructura en los siguientes niveles relacionados jerárquicamente:

1) Primer nivel: Política de Seguridad de la Información.

2) Segundo nivel: Políticas de Seguridad de la Información y de protección de datos

3) Tercer nivel: Procedimientos e Instrucciones Técnicas de Seguridad de la Información.

4) Cuarto nivel: Informes, registros y evidencias electrónicas.

La estructura jerárquica permite adaptar con eficiencia los niveles inferiores a los cambios en los entornos operativos de ASSAP, sin necesidad de revisar su estrategia de seguridad.

El personal de ASSAP tiene la obligación de conocer y cumplir, además de la Política de Seguridad de la Información, todas las Políticas, los Procedimientos e Instrucciones Técnicas de Seguridad de la Información que puedan afectar a sus funciones.

La Política de Seguridad de la Información, las Políticas de Seguridad, los Procedimientos e Instrucciones Técnicas de Seguridad de la Información estarán disponibles, siempre que se considere que su difusión es necesaria, para todos los empleados en la Intranet de ASSAP según su necesidad de distribución a los puntos de uso.

1) Primer nivel: Política de Seguridad de la Información Este documento es de obligado cumplimiento por todo el personal, interno y externo, de ASSAP, revisado por el Comité de Seguridad de la Información y aprobado por la Dirección.

2) Segundo nivel: Políticas de Seguridad de la Información De obligado cumplimiento de acuerdo con el ámbito organizativo, técnico o legal correspondiente. La responsabilidad de aprobación de los documentos redactados en este nivel será competencia del Comité de Seguridad de la Información a propuesta del Responsable de Seguridad.

3) Tercer nivel: Procedimientos e Instrucciones Técnicas de Seguridad de la Información Documentos técnicos orientados a resolver las tareas, consideradas críticas por el perjuicio que causaría una actuación inadecuada, de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información. Son especialmente importantes para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

4) Cuarto Nivel: Informes, registros y evidencias electrónicas que recogen el resultado y las conclusiones de un estudio o una valoración; documentos de carácter técnico que recogen amenazas y vulnerabilidades de los sistemas de información, así como también evidencias electrónicas generadas durante todas las fases del ciclo de vida del sistema de información. La responsabilidad de que existan este tipo de documentos es del Responsable del Sistema.

5) Otra documentación.

8. TRATAMIENTOS DE DATOS DE CARÁCTER PERSONAL

Dentro de este ámbito se recogen las directrices de ASSAP AUDITORES S.L. relacionadas con la protección de la información, relativas tanto a la protección específica de los datos de carácter personal de acuerdo con las exigencias del RGPD, así como a la protección general de toda la información gestionada por ASSAP AUDITORES S.L. de terceros que contenga datos personales en el ejercicio de sus funciones.

ASSAP AUDITORES S.L. cumple de forma escrupulosa las exigencias legales vigentes en materia de protección de datos de carácter personal, aplicando de manera global a esta información las medidas de protección preceptivas por dicha regulación, sin perjuicio de cumplir, además, otras medidas de seguridad adicionales en caso de que se consideren necesarias.

ASSAP AUDITORES S.L. clasifica la información en virtud de su naturaleza, identificando responsables de la información de acuerdo con lo establecido en la presente Política. Los criterios de clasificación y designación de responsables están identificados en el procedimiento correspondiente, en base a los cuales estos responsables podrán modificar dicha clasificación.

Las políticas, procedimientos y medidas aplicables al tratamiento de datos de carácter personal se encuentran recogidos en el sistema de gestión de protección de datos.

9. ANÁLISIS Y GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán ser sometidos a un análisis y gestión de riesgos, evaluando los activos, amenazas y vulnerabilidades a los que están expuestos y proponiendo las contramedidas adecuadas para mitigar los riesgos. Aunque se precisa un control continuo de los cambios realizados en los sistemas, este análisis se repetirá:

- Al menos una vez al año (mediante revisión y aprobación formal).
- Cuando sw
- Cuando ocurra un incidente grave o se comunique una vulnerabilidad grave de seguridad.

Para el análisis y gestión de riesgos se usará la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), elaborada por el Consejo Superior de Administración Electrónica y enfocada a las Administraciones Públicas.

El nivel de riesgo máximo aceptable se establecerá en base a la metodología elegida, MAGERIT, que se utilizará como objetivo de mejora en los planes de mitigación de riesgo que se desarrollen.

10. SERVICIOS EXTERNOS

ASSAP AUDITORES S.L. exige, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con unos niveles idóneos de gestión y madurez en los servicios prestados. ASSAP AUDITORES S.L. regula contractualmente la utilización de recursos externos a la organización, estableciendo en dichos contratos las características del servicio, las responsabilidades de cada parte, la calidad mínima exigible y las consecuencias del incumplimiento del contrato. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad de la Información 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, así como del responsable del tratamiento previsto en el RGPD y LOPDGDD, antes de seguir adelante.

Cuando ASSAP AUDITORES S.L. preste servicios a organismos o maneje información de organismos o AAPP, se les hará partícipe de esta Política de Seguridad de la Información y se establecerán canales para el reporte y coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

11. COMPROMISO Y RESPONSABILIDAD DEL PERSONAL

Todos los usuarios de los sistemas de información de ASSAP AUDITORES S.L. son responsables de la seguridad de los activos de información.

ASSAP AUDITORES S.L. establece las funciones y obligaciones que en materia de seguridad son aplicables a cada puesto de trabajo, identificando las condiciones de confidencialidad a cumplir y las medidas disciplinarias asociadas en caso de incumplimiento.

Asimismo, ASSAP AUDITORES S.L. tiene un programa de formación y concienciación que garantiza que periódicamente todo el personal recibe la información necesaria para saber cómo realizar su trabajo de manera segura y cómo debe participar en la gestión de la seguridad de los sistemas de información y los incidentes que puedan producirse, con el fin de que ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas sean fuentes de riesgo para la seguridad.

El personal debe velar porque el puesto de trabajo esté despejado, de modo que no haya más material sobre su mesa que el requerido para la actividad que se esté realizando en cada momento. Ese material se deberá guardar en un lugar cerrado, como armarios o cajones, cuando no se esté utilizando.

Los equipos portátiles, al tener la consideración de entornos inseguros, deberán contar con medidas de seguridad adicionales. Por una parte, estos equipos estarán equipados con un firewall personal, que limite su visibilidad y controle el acceso al equipo cuando se conecte a redes públicas. Por otra se habilitarán normativas para controlar los equipos portátiles que posee la organización, su responsable y su ubicación y para reportar incidentes relacionados con pérdidas o sustracciones de dichos equipos. Asimismo, sus usuarios también deberán limitar la información que contienen estos equipos, evitando, en la medida de lo posible, que contengan claves de acceso remoto a la red de ASSAP AUDITORES S.L..

12. APROBACIÓN

La presente Política de Seguridad de la Información fue aprobada por la Dirección de ASSAP AUDITORES, S.L. el día 10 de mayo de 2024.

Fdo. Dirección de Assap Auditores S.L.

V..0