Miólnir

· CIBERSEGURIDAD · CUMPLIMIENTO NORMATIVO
· FORMACIÓN · CONSULTORA TECNOLÓGICA

Política de Seguridad de la Información

Julio de 2024

HISTORIAL DE CAMBIOS

Nombre del fichero	Versión	Resumen de cambios producidos	Fecha
Política de seguridad_Miolnir.pdf	1.0	Primera versión	01-07-2024

CLASIFICACIÓN

USO INTERNO
La información contenida en este documento es USO INTERNO. Es responsabilidad del Área o Departamento receptor de este documento su distribución interna en base a la necesidad de conocer la información aquí contenida.

CONTROL DE DIFUSIÓN

AUTOR/ES: MIOLNIR CYBERSEC S.L.
DISTRIBUCIÓN: MIOLNIR CYBERSEC S.L.

Índice

1. Introducción

MIOLNIR CYBERSEC S.L., en adelante la Organización, como muestra de compromiso con la seguridad de la información de sus sistemas ha desarrollado la presente Política de Seguridad de la Información, en adelante Política de Seguridad, de conformidad con lo establecido en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

La Política de Seguridad es una declaración ética, responsable y de estricto cumplimiento en toda la Organización, la cual es desplegada a través de las diferentes Normativas y Procedimientos con los que se procura que los riesgos sean tratados adecuadamente.

El uso de los Activos de información debe estar en consonancia con las buenas prácticas y procedimientos de trabajo profesionales, así como con los requisitos legales, reglamentarios y contractuales, que deben garantizar la Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad de la información y los servicios.

2. Objetivo y ámbito de aplicación

Este documento constituye el establecimiento de un marco organizativo y tecnológico en la Organización.

Se entenderá la Seguridad como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información, quedando excluidas cualquier tipo de actuaciones puntuales o de tratamiento coyuntural.

Debe ser conocida y cumplida por todo el personal de la Organización, independientemente del puesto, cargo y responsabilidad dentro de la misma.

3. Legislación y normativa de referencia

El marco normativo de las actividades de la Organización en el ámbito de esta Política de Seguridad está integrado por las siguientes normas:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- 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).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).

4. Principios y directrices

Los principios que deben contemplarse a la hora de garantizar la seguridad de la información son la prevención, la detección, la respuesta y la recuperación, de manera que las amenazas existentes

no se materialicen o en caso de materializarse no afecten gravemente a la información que se maneja, o los servicios que se prestan.

4.1. Prevención

Se debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello deberán implementarse las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

4.2. Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple ralentización hasta su detención, se debe monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 8 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 9 del ENS.

Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

4.3. Respuesta

Se deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente.

4.4. Recuperación

Para garantizar la disponibilidad de los servicios críticos, se deben desarrollar planes de continuidad de los sistemas TIC y actividades de recuperación.

4.5. Otros principios generales:

- El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.
- La información debe ser protegida contra accesos y alteraciones no autorizados, manteniendo la confidencial e integridad.
- La información debe estar disponible, permitiendo su acceso autorizado, siempre que sea necesario.
- La Seguridad de la Información es responsabilidad de todos. Todas las personas que tienen acceso a la información de la Organización deben protegerla, por lo que deben estar adecuadamente formadas y concienciadas.
- La Seguridad de la Información no es algo estático, debe ser constantemente controlada y periódicamente revisada.
- Todos aquellos activos (infraestructura, soportes, sistemas, comunicaciones, etc.) donde reside la información, viaja o es procesada, deben estar adecuadamente protegidos.
- Las medidas de seguridad que se implanten deben estar en proporción a la criticidad de la información que protejan y a los daños o pérdidas que se pueden producir en ella. En todo momento se seguirá como mínimo las medidas de seguridad impuestas por el ENS, así como las guías CCN-STIC elaboradas por el Centro Criptológico Nacional del Centro Nacional de Inteligencia.
- El tratamiento de datos de carácter personal debe estar siempre de acuerdo con las leyes aplicables en cada momento, siendo especialmente importantes la Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y la Ley Orgánica de Protección de Datos.

5. Organización de la Seguridad de la Información

La estructura organizativa de la gestión de la seguridad de la información en el ámbito de la seguridad de la información de la Organización está compuesta por los siguientes agentes:

a) El Comité de Gestión de la Seguridad de la Información.
b) El Responsable de Seguridad.
c) Responsables de la Información y de los Servicios.
d) Responsables del Sistema de Información.
e) Delegado de Protección de Datos.
f) Responsable del Tratamiento.

5.1. Comité de Gestión de la Seguridad de la Información

Para la gestión de la Seguridad de la Información, se crea el Comité de Gestión de la Seguridad de la Información, en adelante el Comité de Seguridad, dentro del ámbito de la presente Política de Seguridad formado por un equipo multidisciplinar que coordinará las actividades y controles de seguridad establecidos en la Organización y que vela por el cumplimiento de la normativa vigente, interna y externa, en materia de protección de datos de carácter personal y seguridad.

Son funciones del Comité de Seguridad las siguientes:

a) Identificar los objetivos de la Organización en el ámbito de la Seguridad de la Información.

b) Elaborar la Política de Seguridad, establecer los criterios de revisión de la misma, revisarla, distribuirla y velar por su cumplimiento.

c) Promover y respaldar los planes de acción e iniciativas que garanticen la implantación de la Política de Seguridad en la Organización.

d) Establecer los requisitos de seguridad que deben cumplir a nivel organizativo, técnicos y de control, los sistemas y servicios de la Organización.

e) Garantizar que la seguridad forma parte del proceso de planificación de la gestión de la información y como proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información.

f) Comunicar a los terceros que colaboren en la explotación de los sistemas de información la realización de la misma conforme a los exigidos en el ENS.

g) Aprobar los nombramientos de responsables y responsabilidades en materia de seguridad de la información.

h) Valorar el grado de conformidad de los procedimientos implantados en la Organización con las normas definidas en la política, estableciendo planes de mejora para aquellos que requieran de una modificación para su conformidad.

i) Supervisar las normativas y procedimientos de seguridad que se definan para dar cumplimiento y desarrollo a la Política de Seguridad.

j) Acordar y aprobar metodologías y procesos específicos relativos a la Seguridad de la Información.

k) Verificar que todas las acciones llevadas a cabo en materia de Seguridad sean compatibles o se encuentren respaldadas por la Política de Seguridad.

l) Promover la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de las Administraciones en materia de Seguridad.

m) Promover la formación y concienciación en materia de Seguridad de la Información a todo el personal.

n) Mantener contactos periódicos con grupos, otras entidades, organismos, foros, etc. que resulten de interés en el ámbito de la Seguridad de la Información, compartiendo experiencias y conocimiento que ayuden a mejorar y mantener la seguridad de los sistemas de la Organización.

o) Valorar y evaluar los recursos necesarios para dar soporte al proceso de planificación e implantación de la seguridad en la Organización.

El Comité de Seguridad, se reunirá con carácter ordinario, al menos una vez al año, pudiéndose reunir de manera extraordinaria, por razones de urgencia y causa justificada, en periodos inferiores.

5.2. Responsable de Seguridad

Es el responsable de que los servicios y sistemas de información de la Organización se mantengan con el mayor grado de seguridad atendiendo a los principios de:

- **Confidencialidad:** la información asociada a los servicios electrónicos solo debe poder ser conocida por las personas autorizadas para ello.
- **Integridad:** la información asociada a los servicios electrónicos no debe ser alterada por personas no autorizadas.
- **Disponibilidad:** garantía de que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma siempre que lo requieran, así como garantía de que los servicios permanecerán disponibles.

Son funciones del Responsable de Seguridad:

- Supervisar el cumplimiento de la presente Política, de sus normas y procedimientos derivados.
- Coordinar la interacción con otros organismos especializados.
- Tomar conocimiento y supervisar la investigación y monitorización de los incidentes de seguridad.
- Establecer las medidas de seguridad, adecuadas y eficaces para cumplir los requisitos de seguridad establecidos por los Responsables de los Servicios y de la Información, siguiendo en todo momento lo exigido en el Anexo II del ENS.
- Asesorar, en colaboración con el Responsable del Sistema, los Responsables de los Servicios y de la Información en la realización de los análisis y gestión de riesgos, elevando el informe resultado al Comité de Seguridad.
- Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad, siguiendo las directrices del Comité de Seguridad.
- Preparar los temas a tratar en las reuniones del Comité de Seguridad, aportando información puntual para la toma de decisiones.

Respecto a la documentación, son funciones del Responsable de Seguridad:

- Aprobar y proponer al Comité de Seguridad la documentación de seguridad de segundo nivel (Normativas y Procedimientos de Seguridad) de obligado cumplimiento.
- Supervisar la documentación de tercer nivel (Procedimientos Técnicos de Seguridad) de obligado cumplimiento.
- Mantener la documentación organizada y actualizada, gestionando los mecanismos de acceso a la misma.

Respecto a la protección de datos de carácter personal, son funciones del Responsable de Seguridad:

- Garantizar la seguridad de los datos, implantando y haciendo cumplir las medidas, procedimientos, instrucciones y normativas establecidas en el Manual jurídico definido en la organización, así como sus anexos.
- Colaborar con el responsable del tratamiento en la difusión del Manual jurídico y de sus anexos.
- Mantener un listado actualizado del personal autorizado a acceder a los sistemas de información.

- Realizar los controles periódicos establecidos para verificar el cumplimiento del Manual jurídico y de sus anexos.
- Analizar los informes de auditoría y proponer al responsable del tratamiento las medidas correctoras oportunas.
- Cumplir con el procedimiento de ejercicio de derechos de los interesados según las solicitudes recibidas.
- Autorizar permisos de acceso a los usuarios sobre los recursos, (automatizados y no automatizados) que se encuentran bajo su responsabilidad y que sean estrictamente necesarios para el desarrollo de las funciones del trabajador.
- Realizar un inventario y un registro de entrada y salida de soportes.
- Autorizar la salida de soportes con datos personales que se encuentren bajo su responsabilidad.
- Autorizar la generación de copias o reproducción de documentos.
- Mantener un listado de personal autorizado a la información en soporte papel.
- Revisar los permisos y perfiles de acceso de la información que se encuentra bajo su gestión.
- Autorizar la recuperación de datos tratados.
- Habilitar y mantener un registro de incidencias para la información que esté bajo su responsabilidad. Este registro deberá estar disponible para cualquier revisión o auditoría.

En aquellos sistemas de información que, por su complejidad, distribución, separación física de elementos o números de usuarios se necesitara de personal adicional para llevar a cabo las funciones del Responsable de Seguridad, el Responsable de Seguridad podrá designar cuantos Responsables de Seguridad Delegados considere necesarios, incluyendo los Responsables de Seguridad relativos al RGPD. Los Responsables de Seguridad Delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable de Seguridad teniendo dependencias funcionales directas con él.

El Responsable de Seguridad será nombrado y cesado por el Comité de Seguridad.

5.3. Responsables de la Información y de los Servicios

Esta responsabilidad recaerá en el jefe de cada área o departamento de la organización, pudiendo una misma persona acumular las responsabilidades de la información de todos los servicios y procesos que gestione.

Son los responsables de clasificar la información conforme a los criterios y categorías establecidas en el ENS y en cada una de las dimensiones de seguridad conocidas y aplicables, dentro del marco establecido en el Anexo I del ENS.

Son los responsables de determinar los niveles de seguridad de los servicios en cada dimensión de seguridad dentro del marco establecido en el Anexo I del ENS y en cada una de las dimensiones de seguridad conocidas y aplicables (disponibilidad, autenticidad, trazabilidad, confidencialidad e integridad).

Son los encargados, contando con la participación y asesoramiento del Responsable de Seguridad y del Responsable del Sistema de Información, de realizar los preceptivos análisis de riesgos, y de seleccionar las salvaguardas a implantar.

Son los responsables de aceptar los riesgos residuales calculados en el análisis de riesgos, y de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

Los responsables de información y de los servicios son establecidos en el Plan Director de Seguridad, el cual contiene la planificación de actuaciones destinadas a subsanar las insuficiencias detectadas, para el cumplimiento del Esquema Nacional de Seguridad.

5.4. Responsable del Sistema de Información

Personal designado cuyas responsabilidades son:

- Desarrollo, operación y mantenimiento del sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Garantizar que las medidas de seguridad se integren adecuadamente dentro del marco general de la Seguridad de la Información.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.
- Elaborar procedimientos técnicos de seguridad de los sistemas de información.
- Elaborar planes de continuidad de los sistemas de información.

Podrá acordar la suspensión del manejo de determinada información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión deberá ser acordada con el Responsable de la Información y servicio afectados y el Responsable de Seguridad antes de ser ejecutada.

En aquellos sistemas que, por su complejidad, distribución, separación física de elementos o número de usuarios se necesite personal adicional para llevar a cabo las funciones de Responsable de Sistemas, se podrán designar cuantos Responsables de Sistemas Delegado que se consideren oportunos. La designación y delegación de funciones en los Responsables de Sistemas Delegados corresponde al Responsable del Sistema, sin perjuicio de que la responsabilidad final siga recayendo sobre el Responsable del Sistema. Los Responsable de Sistemas Delegados se harán cargo en su ámbito de todas aquellas acciones que delegue el Responsable del Sistema relacionadas con la operación, mantenimiento, instalación y verificación del correcto funcionamiento del Sistema de Información correspondiente, así como también tendrá dependencia funcional directa con el Responsable del Sistema que es a quién reporta.

Los responsables del Sistema de Información son establecidos en el Plan Director de Seguridad, el cual contiene la planificación de actuaciones destinadas a subsanar las insuficiencias detectadas, para el cumplimiento del Esquema Nacional de Seguridad. Por regla general será el departamento de Informática, pudiendo delegar en los responsables de cada uno de los sistemas afectados.

5.5. Delegado de Protección de Datos

El Delegado de Protección de Datos será único para todos los órganos y organismos de la Organización. Se informará de su nombramiento y cese a la Agencia Española de Protección de Datos, cuando aplique.

Son funciones del Delegado de Protección de Datos:

- Informar y asesorar a la Organización y a todos los empleados que se ocupen del tratamiento de datos personales, de las obligaciones que se deriven del Reglamento General de Protección de Datos y de otras disposiciones relacionadas con la protección de datos.
- Supervisar el cumplimiento del Reglamento General de Protección de Datos en la Organización.
- Asesorar 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.

Además, asesorará y supervisará en las siguientes áreas:

- Cumplimiento de principios relativos al tratamiento, como los de limitación en la finalidad, minimización o exactitud de los datos.
- Identificación de las bases jurídicas de los tratamientos.
- Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.
- Existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.
- Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.
- Establecimiento de mecanismos de recepción y gestión de solicitudes de ejercicio de derechos por parte de los interesados.
- Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.
- Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación Organización – encargado de tratamiento.
- Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la Organización y de las razones que justifiquen la transferencia.
- Diseño e implantación de políticas de protección de datos.
- Auditorías de protección de datos.
- Establecimiento y gestión de los registros de actividades de tratamiento.
- Análisis de riesgo de los tratamientos realizados.
- Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos.
- Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.
- Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados.
- Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos.
- Realización de evaluaciones de impacto sobre la protección de datos.
- Relaciones con las autoridades de supervisión.

- Implantación de programas de formación y sensibilización del personal de la Organización en materia de protección de datos.

5.6. Responsable del Tratamiento

El responsable del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determina los fines y medios del tratamiento, es decir, MIOLNIR CYBERSEC SL.

MIOLNIR CYBERSEC SL debe, entre otras cosas:

- Garantizar la observancia de los principios relativos al tratamiento y aprobar la política, normativa y procedimientos concernientes a la protección de datos personales.
- Designar a quien ejerza como Responsable de Seguridad, quien deberá coordinar y controlar las medidas definidas en el Manual jurídico.
- Designar al Delegado de Protección de Datos, cuando corresponda.
- 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 normativas aprobadas e implementadas en la organización.
- 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 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 adecuadas.

5.7. Resolución de conflictos

En caso de conflicto entre los diferentes responsables, éste será resuelto por el superior jerárquico de los mismos. En defecto de lo anterior, prevalecerá la decisión del Responsable de Seguridad.

5.8. Obligaciones del Personal

Todo el personal, interno y externo, de MIOLNIR CYBERSEC S.L. tiene la obligación de conocer y cumplir la presente Política de Seguridad, las normativas y procedimientos derivados de la misma, tales como las relativas a la protección de datos de carácter personal, siendo responsabilidad del Comité de Seguridad disponer de los mecanismos necesarios para que la información llegue a todo el personal indicado.

El incumplimiento manifiesto de la Política de Seguridad de la Información o la normativa y procedimientos derivados de ésta podrá acarrear el inicio de medidas disciplinarias oportunas y, en su caso, las responsabilidades legales correspondientes.

6. Asesoramiento Especializado en Materia de Seguridad

6.1. Asesoramiento especializado

El Responsable de Seguridad será el encargado de coordinar los conocimientos y las experiencias disponibles en la organización con el fin de proporcionar ayuda en la toma de decisiones en materia de seguridad.

6.2. Revisión independiente de la Seguridad de la Información

El Comité de Seguridad propondrá la realización de revisiones periódicas sobre la vigencia e implementación de la Política de Seguridad con el fin de garantizar que las prácticas en la Organización reflejan adecuadamente sus disposiciones.

7. Protección de Datos de Carácter Personal

Para el tratamiento de datos de carácter personal en los sistemas de información se seguirá en todo momento lo desarrollado en el documento de seguridad y su documentación asociada conforme a lo exigido 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), así como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).

8. Formación y concienciación

El objetivo es lograr la plena conciencia respecto a que la Seguridad de la Información afecta a todo el personal de la Organización y a todas las actividades de acuerdo al principio de seguridad integral recogido en el art. 6 del ENS. A estos efectos, la Organización, propondrá y organizará sesiones formativas y de concienciación para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren.

9. Análisis y gestión de riesgos

La Organización asume el compromiso de controlar los riesgos de seguridad, así como dar cumplimiento a la legislación y normas internas vigente bajo un proceso de mejora continua conforme a los marcos y metodologías existentes en la actualidad (MAGERIT, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información).

Para ello, con el objetivo de conocer el nivel de exposición de los activos de información a los riesgos y amenazas en materia de seguridad, los Responsables de los Sistemas de Información realizarán, con periodicidad al menos anual, análisis de riesgos cuyas consecuencias se plasmarán en actuaciones para tratar y mitigar el riesgo, o incluso, replantear la seguridad de los sistemas en caso necesario.

Se realizará un análisis de riesgos:

- Regularmente, una vez al año.

- Cuando haya cambios en los servicios esenciales prestados o cambios significativos en las infraestructuras que los soportan.
- Cuando ocurra un incidente de seguridad grave.
- Cuando se identifiquen amenazas severas que no hubieran sido tenidas en cuenta o vulnerabilidades graves que no estén contrarrestadas por las medidas de protección implantadas.

Las conclusiones de los análisis de riesgos serán elevadas al Responsable de Seguridad y éste al Comité de Seguridad.

10. Estructura normativa

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.
- Segundo nivel: Normativas y Procedimientos de Seguridad.
- Tercer nivel: Procedimientos Técnicos de Seguridad.
- Cuarto nivel: Informes, registros y evidencias electrónicas.

10.1. Primer nivel: Política de Seguridad

Documento de obligado cumplimiento por todo el personal, interno y externo de la Organización, recogido en el presente documento y aprobado internamente por la Organización.

10.2. Segundo Nivel: Normativas y Procedimientos de Seguridad

De obligado cumplimiento de acuerdo al ámbito organizativo, técnico o legal correspondiente.

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

10.3. Tercer Nivel: Procedimientos Técnicos de Seguridad

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.

La responsabilidad de aprobación de estos procedimientos técnicos es del Responsable del Sistema de Información correspondiente, bajo la supervisión del Responsable de Seguridad. En caso de que los procedimientos afectaran a varios sistemas de información será responsabilidad del Responsable de Seguridad el aprobarlos.

10.4. Cuarto Nivel: Informes, registros y evidencias electrónicas

Documentos de carácter técnico 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 de cada uno de los Responsables de los Sistemas de Información en su ámbito.

10.5. Otra documentación

Se podrá seguir en todo momento los procedimientos, normas e instrucciones técnicas STIC, así como las guías CCN-STIC de las series 400, 500 y 600.

11. Publicación de la política de seguridad

El presente documento, se publicará en la página web de la organización www.miolnir.es en su pie de página.

12. Entrada en vigor

La Política de Seguridad será aplicable a partir del día siguiente al de su publicación en la página web.

Linares, a 1 de julio de 2024.

53590059J ALVARO SOLAS (R: B56616469)

Firmado digitalmente por 53590059J ALVARO SOLAS (R: B56616469)
Fecha: 2024.08.02 10:35:59 +02'00'

Álvaro Solás Lara

CEO