# Política de Seguridad de la Información del ENS

v3.3 – 16-06-2023

**PÚBLICO**

# INDICE


INDICE Y CONTROL DE EDICIONES ..... 3
INTRODUCCIÓN. ..... 4
OBJETO. ..... 4
ALCANCE. ..... 4
OBJETIVOS Y MISIÓN ..... 4
MARCO LEGAL Y REGULATORIO. ..... 6
ORGANIZACIÓN DE LA SEGURIDAD ..... 7
Mecanismos de coordinación y Comités ..... 7
Funciones y responsabilidades de seguridad ..... 7
Designación de funciones. ..... 8
Coordinación, nombramiento y resolución de conflictos ..... 8
FORMACIÓN Y CONCIENCIACIÓN ..... 9
GESTIÓN DE RIESGOS ..... 10
DATOS DE CARÁCTER PERSONAL ..... 11
Determinación de la categoría y del nivel de seguridad requerido para los sistemas. ..... 12
Establecimiento, implantación, mantenimiento y mejora del SGSI y directrices para la gestión de la documentación ..... 14
DOCUMENTACIÓN ..... 16
PROCESO DE APROBACIÓN Y REVISIÓN ..... 17

# INDICE Y CONTROL DE EDICIONES

| Versión | Fecha | Modificaciones realizadas respecto a la anterior edición |
|---|---|---|
| 1.0 | 22/10/2021 | Creación del documento |
| 2.0 | 18/03/2022 | Revisión de la Política para su adecuación con la GUÍA DE SEGURIDAD (CCN-STIC-805) ESQUEMA NACIONAL DE SEGURIDAD POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN |
| 3.0 | 16/09/2022 | Actualización de la política con las actividades incluidas en el nivel MEDIO |
| 3.1 | 04/11/2022 | Pequeños ajustes de redacción como consecuencia de la auditoría interna |
| 3.2 | 18/11/2022 | Pequeños ajustes asociados con el IOM de Auditoría de Certificación |
| 3.3 | 16/06/2023 | Cambio de formato y nombre de marca |

# INTRODUCCIÓN.

La Dirección de knowmad mood, en el marco de su competencia general e indelegable de determinar las políticas y estrategias generales de la organización, y siguiendo las directrices definidas en la Política de Seguridad de la Información (incluida en la Política de los Sistemas de Gestión), aprueba la siguiente Política de Seguridad de la Información del Esquema Nacional de Seguridad (en adelante, ENS). El objetivo de esta Política es definir y establecer los principios, criterios y objetivos de mejora que rigen las actuaciones en materia de seguridad de la información de los sistemas que se encuentran sujetos al ENS.

# OBJETO.

Establecer las directrices y principios que regirán el modo en que knowmad mood gestionará y protegerá su información y sus servicios, cumpliendo con los objetivos y directrices de la Política de Seguridad de la Información corporativa, a través de la implantación, mantenimiento y mejora de un SGSI y aplicando los requisitos y medidas de seguridad dentro del marco regulatorio del Esquema Nacional de Seguridad (ENS).

# ALCANCE.

Tomando en cuenta el contexto en el cual se determinan las cuestiones internas y externas de la organización, las partes interesadas que son relevantes y sus requisitos para la seguridad de la información, así como las interfaces y dependencias entre las actividades realizadas por la entidad y las que se llevan a cabo por otras organizaciones en el cumplimiento. Esta Política se circunscribe a los servicios y sistemas incluidos en el alcance del ENS que dan cobertura al cumplimiento de los requisitos y medidas de seguridad establecidas en el Esquema Nacional de Seguridad en lo relativo a:

- Diseño, desarrollo, mantenimiento y soporte de aplicaciones,
- Implantación, soporte y mantenimiento de sistemas de información,
- Comercialización de software
- Consultoría,
- Formación
- Gestión de puesto de trabajo

# OBJETIVOS Y MISIÓN

Mediante esta Política, knowmad mood asume y promueve los siguientes principios generales que deben guiar todas sus actividades:

a) Garantizar el cumplimiento con los objetivos y principios generales detallados en la Política de Seguridad de la Información aprobada y promovida por la Dirección de la empresa
b) Asegurar el establecimiento y cumplimiento de la presente política y los objetivos de la seguridad de la información, y que estos sean compatibles con la estrategia de la empresa.
c) Asegurar la integración y el cumplimiento de los requisitos aplicables del ENS en los servicios y procesos de la sociedad.
d) Asegurar que los recursos necesarios para el ENS estén disponibles.
e) Comunicar la importancia de una gestión de la seguridad eficaz y conforme con los requisitos del ENS.
f) Asegurar que el ENS consigue los resultados previstos.
g) Dirigir y apoyar a las personas para contribuir a la eficacia del ENS.
h) Promover la mejora continua.
i) Apoyar otros roles pertinentes de la Dirección, liderando a sus áreas de responsabilidad en seguridad de la información.

Los objetivos de seguridad de la información se establecerán en las funciones y niveles pertinentes, enfocados a la mejora y utilizando como marco de referencia:

a) Cambios en las necesidades de las partes interesadas que lleven a una mejora del alcance del sistema.
b) Requisitos de seguridad de la información aplicables y los resultados de la apreciación y del tratamiento de los riesgos para garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información, así como la protección de los datos personales.
c) Factores internos como la aplicación de técnicas organizativas que mejoren el seguimiento de la tramitación y resolución de incidentes de seguridad.
d) Factores externos como los avances tecnológicos, cuya aplicación mejoren la eficacia del tratamiento de los riesgos.
e) La mejora de la eficacia de la formación y concienciación del personal que trabaja en la entidad y afecta a su desempeño en seguridad de la información.

Así mismo, la planificación para la consecución de los objetivos de seguridad de la información establecidos se realizará tomando en cuenta lo que se va a hacer, los recursos necesarios, el responsable y el plazo de consecución.

# MARCO LEGAL Y REGULATORIO.

a) Real Decreto 3/2010, de 8 de enero que regula el Esquema Nacional de Seguridad (ENS) y su modificación por el Real Decreto 951/2015, de 23 de octubre.
b) 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.
c) 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.
d) 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.
e) 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).
f) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
g) Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.
h) Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
i) Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
j) Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público
k) Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

Adicionalmente, knowmad mood cuenta con un registro pormenorizado de toda la legislación que es aplicable a los servicios del Sistema de Gestión y del ENS.

# ORGANIZACIÓN DE LA SEGURIDAD

La Dirección de knowmad mood tiene como responsabilidad fundamental la de liderar y comprometerse con respecto al ENS.

## Mecanismos de coordinación y Comités

knowmad mood cuenta con un Comité de Seguridad de la Información que dispone de las siguientes funciones:

- Asegurarse de que se establecen, implementan y mantienen los procesos necesarios para el SGSI y el cumplimiento del ENS.
- Asegurarse de que se promueva la toma de conciencia de los requisitos del cliente y resto de Partes Interesadas en todos los niveles de la organización.

El Comité de Seguridad de la Información (CSI), estará compuesto por:

- Dirección representada por el Director Adjunto
- Responsable de Procesos, Calidad y Organización
- Responsable de SI e Infraestructuras
- Responsable de Infraestructuras
- Responsable de seguridad del SGSI y del ENS
- CISO

## Funciones y responsabilidades de seguridad

a) **Responsable de la Información:** Debe determinar los requisitos de seguridad de la información tratada y las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos

b) **Responsable del Servicio:** Debe incluir las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control y será responsable de la valoración de las consecuencias de un impacto negativo sobre la seguridad de los servicios, que se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.

c) **Responsable del Sistema:** que tendrá las siguientes funciones:
   - 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 topología 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.
   - Aprueba la valoración del Sistema

d) **Responsable de Seguridad (desempeñado por el RSGSI):** Determinar las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios. Además, será responsable de las siguientes funciones incluidas y descritas de manera más amplia en el Manual del Sistema de Gestión:

- Velar por el cumplimiento de las políticas de seguridad
- Gestionar y desarrollar los análisis de riesgos de seguridad de la información
- Desarrollar, impulsar, coordinar e implementar la Política de Seguridad de la Información
- Elaborar e implementar los procedimientos e instrucciones técnicas en materia de seguridad de la información.
- Recomendar los controles de seguridad aplicables a los sistemas de información para reducir el riesgo.
- Recomendar las actividades de diseño, evaluación, selección e implementación de soluciones de Seguridad de la Información.
- Promover la formación y concienciación en materia de seguridad de los sistemas de información y las redes de comunicaciones que los soportan, tanto en aspectos lógicos, físicos y organizativos.
- Investigar los incidentes de seguridad de la información.
- Notificar al CSI incidentes de seguridad que tengan impacto en la prestación de los servicios
- Dirigir la actividad de Seguridad de la Información, que dispondrá de los medios técnicos y humanos necesarios para asumir todas las funciones que tiene asignadas, tanto organizativas como técnicas. Cualesquiera otras funciones que se recojan en la legislación vigente en la materia.

e) **Responsable de Seguridad protección datos personales:** Velar por el cumplimiento de los requisitos en materia de protección de datos de carácter personal
f) **Administrador del sistema:** Cumplimiento de los procedimientos técnicos de seguridad de la información
g) **Administradores funcionales de aplicaciones**: Altas, bajas y gestión de privilegios en las aplicaciones

## Designación de funciones.

La Dirección asegura, con la colaboración del RSGSI, que el personal dispone de la necesaria formación teórica y práctica en materia de seguridad de la información para el desempeño eficiente de sus funciones.

Las funciones y responsabilidades inherentes a cada puesto de trabajo dentro del SGSI, así como los requisitos de formación y experiencia necesarios, están recogidas en los perfiles de puesto de trabajo y en el Manual de Organización, debiendo ser aprobadas las modificaciones por la dirección en el CSI.

El registro que designa a las personas que realizan las funciones descritas es el “PR-IR-006 R01 Listado Funciones vs Responsables”.

## Coordinación, nombramiento y resolución de conflictos

La coordinación se lleva a cabo en el seno de la Dirección que podrá delegar sus funciones en el Comité de Seguridad de la Información.

Tanto los nombramientos como la posible resolución de conflictos correrán a cargo de la Dirección.

# FORMACIÓN Y CONCIENCIACIÓN

Dentro de los planes de formación se incluirán acciones de concienciación orientadas al personal de forma que se realice una concienciación relativa, entre otros, a los siguientes aspectos:

- Política de seguridad de la información.
- Seguridad de la información.
- Riesgos, vulnerabilidades y amenazas de los sistemas de información.
- Necesidad del cumplimiento de la legislación vigente

# GESTIÓN DE RIESGOS

Las actividades objeto de esta política de seguridad incluidas en el ámbito del ENS tiene su correspondiente gestión de riesgos

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- regularmente, al menos una vez al año
- cuando cambie la información manejada
- cuando cambien los servicios prestados
- cuando ocurra un incidente grave de seguridad
- cuando se reporten vulnerabilidades graves
- cuando se realice cualquier cambio significativo del sistema o del SGSI

Para la armonización del análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. 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 a realizar.

knowmad mood dispone de una metodología documentada para la realización del análisis de riesgos recogida en el documento “PR-IT-001 Metodología de análisis de riesgos”.

# DATOS DE CARÁCTER PERSONAL.

El tratamiento de datos de carácter personal se basará en la “Política de Protección de Datos”, en la que se fijan las directrices que se deben seguir para garantizar la privacidad de los datos de los clientes, proveedores, empleados y, en general, de todos los colectivos de datos implicados, identificando la base de legitimación más adecuada para los tratamientos de datos personales llevados a cabo de acuerdo con la legislación vigente.

# Determinación de la categoría y del nivel de seguridad requerido para los sistemas.

La categoría en materia de seguridad de los sistemas de información incluidos dentro del alcance del Esquema Nacional de Seguridad, se determinará en función de la valoración del impacto que tendría un incidente que afecte a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad.

La valoración de las consecuencias del impacto se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.

La facultad para determinar la categoría de un sistema le corresponde al responsable del servicio, de la información y del sistema y será de aplicación a todos los sistemas empleados para la prestación de los servicios incluidos en el alcance del Esquema Nacional de Seguridad. El proceso de categorización de los sistemas se realizará a través de las siguientes actividades:

- Identificación del nivel correspondiente a cada servicio/información, en función de las dimensiones de seguridad.
- Determinación de la categoría del sistema, teniendo en cuenta que cuando un sistema maneja diferentes informaciones y presta diferentes servicios, el nivel del sistema en cada dimensión, será el mayor de los establecidos para cada información y servicios.

La identificación del nivel correspondiente a cada servicio/información en las dimensiones disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad se realizará considerando los siguientes criterios definidos en el Esquema Nacional de Seguridad:

- Nivel BAJO (B). Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
- Nivel MEDIO (M). Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
- Nivel ALTO (A). Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

La clasificación se realizará en base a las siguientes categorías: BÁSICA (B), MEDIA (M) y ALTA (A).

- Un sistema de información será de categoría ALTA (A) si alguna de sus dimensiones de seguridad alcanza el nivel ALTO (A).
- Un sistema de información será de categoría MEDIA (M) si alguna de sus dimensiones de seguridad alcanza el nivel MEDIO (M), y ninguna alcanza un nivel superior.
- Un sistema de información será de categoría BÁSICA (B) si alguna de sus dimensiones de seguridad alcanza el nivel BAJO (B), y ninguna alcanza un nivel superior.

La clasificación de la información será realizada por el Responsable de la Información considerando lo establecido legalmente sobre la naturaleza de la misma.

La valoración del sistema de información y la determinación de la categoría del sistema estará documentada en la Declaración de Aplicabilidad, siendo el Responsable de la Información, Responsable del Servicio y Responsable del Sistema los responsables de su documentación y aprobación formal. Además, en cada momento tendrá la potestad de modificar el nivel de seguridad requerido, de acuerdo con los criterios descritos en el presente documento.

Considerando la categoría del sistema y los niveles asociados a cada dimensión de seguridad, se determinarán las medidas que se deberán aplicar a dicho sistema.

# Establecimiento, implantación, mantenimiento y mejora del SGSI y directrices para la gestión de la documentación

Los controles de seguridad deberán implantarse, mantenerse y mejorarse continuamente, y estar disponibles como información documentada que deberá ser revisada y aprobada por la dirección.

En cumplimiento del artículo 11 del Real Decreto del ENS, la presente Política de Seguridad se desarrollará aplicando los siguientes requisitos mínimos que se encuentran incluidos en la documentación del sistema:

a) Organización e implantación del proceso de seguridad. Considerando las directrices desarrolladas en la Política del Sistema de Gestión, se desarrollará un conjunto de procedimientos operativos que permitan garantizar la implantación de dichas directrices y la consecución de los objetivos de la organización en materia de seguridad de la información.
b) Análisis y gestión de los riesgos. El proceso de análisis y gestión de los riesgos, recogido en la metodología de análisis de riesgos, se realizará de acuerdo con las siguientes actividades:
    - Identificación de activos.
    - Análisis y valoración.
    - Cálculo del riesgo.
    - Determinación del riesgo aceptable.
c) Gestión de personal. La Dirección se asegurará que el personal dispone de la formación necesaria teórica y práctica en materia de seguridad de la información para el desempeño eficiente de sus funciones. Para lograr los objetivos de seguridad de la información todo el personal debe estar involucrado en el tratamiento y saber de qué forma se puede contribuir a su consecución. Estas medidas se encuentran desarrolladas en el procedimiento de seguridad relativa a los recursos humanos.
d) Profesionalidad. La Dirección deberá garantizar que el personal dispone del conocimiento y habilidades necesarios para el adecuado desempeño de sus funciones. Además, deberá proporcionarla formación necesaria cuando se detecten carencias en el cumplimiento de las actividades.
e) Autorización y control de los accesos. Los sistemas de información deberán disponer de un mecanismo de control de accesos que limite su acceso a los usuarios y dispositivos que estén debidamente autorizados, restringiendo el acceso a las funciones que le son permitidas. Las medidas de seguridad aplicadas se encuentran descritas en el procedimiento de control de acceso.
f) Protección de las instalaciones. La organización deberá disponer de un conjunto de controles de acceso físico a las instalaciones, que permita limitar el acceso únicamente a las personas autorizadas a las zonas de almacenamiento y/o procesamiento de información confidencial. Las medidas de protección se encuentran descritas en el procedimiento de seguridad física y del entorno.
g) Adquisición de productos. La adquisición de productos deberá considerar y garantizar el cumplimiento con los requisitos de seguridad establecidos por la Dirección, tal y como se detalla en el procedimiento de adquisición, desarrollo y mantenimiento.
h) Seguridad por defecto. Los sistemas deberán configurarse según las políticas y procedimientos de seguridad definidos. El procedimiento de seguridad de las operaciones desarrolla las medidas de seguridad que se deben aplicar a los sistemas de información.
i) Integridad y actualización del sistema. Se deberán aplicar medidas que permitan conocer el estado de seguridad de los sistemas, y que permitan identificar y gestionar los riesgos de seguridad de estos. Estas medidas se encuentran desarrolladas en el procedimiento de seguridad de las operaciones.

j) Protección de la información almacenada y en tránsito. Se deberán aplicar medidas de seguridad que permitan garantizar un adecuado nivel de protección de la información almacenada y en tránsito. Estas medidas se encuentran detalladas en el procedimiento de gestión de activos.
k) Prevención ante otros sistemas de información interconectados. Se deberán analizar y gestionar los riesgos derivados de las conexiones de los sistemas de información con redes públicas, y aplicar las medidas necesarias de protección según el nivel de seguridad requerido por el sistema.
l) Registro de actividad. Los sistemas de información deberán contar con registros de actividad de los usuarios que permitan custodiar la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas. Estas medidas se encuentran detalladas en el procedimiento de seguridad de las operaciones.
m) Incidentes de seguridad. Los sistemas de información deberán contar con un sistema de detección y reacción frente a código dañino. Además, existirá un registro de incidentes de seguridad que permitirá realizar un seguimiento de la resolución de estos y aplicar mejoras a través de las lecciones aprendidas. Estas medidas se encuentran detalladas en el procedimiento de Gestión de Incidentes de Seguridad.
n) Continuidad de la actividad. Se deberán establecer, en la medida de lo posible y según el nivel de riesgo asociado, los mecanismos necesarios para garantizar la recuperación de la información y la continuidad de las operaciones.
o) Mejora continua del proceso de seguridad. La Dirección deberá llevar a cabo una revisión periódica del sistema para asegurarse de su conveniencia, adecuación y eficacia continua. Ante la ocurrencia de cualquier desviación respecto a los resultados esperados, se deberá iniciar el proceso de tratamiento de la misma mediante los procesos establecidos.

Esta Política se desarrollará por medio de normativa y procedimientos de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización dentro del alcance que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. Se deberá comunicar la información documentada de los controles de seguridad al personal que trabaja en la entidad (personal interno y externo), que tendrá la obligación de aplicarla en la realización de sus actividades.

La información documentada será clasificada en: información de uso público, información de uso interno e información confidencial, dando el uso adecuado de acuerdo con dicha clasificación y según el criterio que se establezca en la Política de Gestión de Activos.

# DOCUMENTACIÓN

La información documentada asociada al ENS se organiza, codifica y aprueba de acuerdo con los requisitos generales del Sistema Integrado de Gestión que se recogen en el documento “KNOWMAD MOOD-Manual del Sistema de Gestión”.

Toda la información documentada relativa al Sistema Integrado de Gestión se aloja en los Sistemas de Información de knowmad mood.

# PROCESO DE APROBACIÓN Y REVISIÓN

Esta Política de Seguridad del ENS será aprobada por la Dirección y revisada junto a la Política de los Sistemas de Gestión de forma periódica o cuando circunstancias técnicas u organizativas lo requieran para evitar que quede obsoleta.

31649683G JOSE MANUEL RUFINO (R: A80827694)

Firmado digitalmente por 31649683G JOSE MANUEL RUFINO (R: A80827694)
Fecha: 2023.06.30 09:10:19 +02'00'

*José Manuel Rufino*
*Consejero Delegado de Aplicaciones y Tratamiento de Sistemas, S.A.*
*30 de junio de 2023*