

Política de Seguridad de la Información

Sistema de Gestión de Seguridad de la Información
Esquema Nacional de Seguridad

29 de mayo de 2026

Código: NOR.SGSI-001
Versión: 1.0
Nivel: Público

Control de versiones

Versión	Fecha	Descripción de las Modificaciones
1.0	29/05/2026	Edición inicial

Propiedad del documento

Este documento se acoge al amparo del Derecho a la Propiedad Intelectual, siendo de uso interno y exclusivo de NEMERGENT SOLUTIONS S.L. Quedan reservados todos los derechos inherentes a que ampara la Ley, así como los de traducción, reimpresión, transmisión por cualquier medio, reproducción en forma fotomecánica o en cualquier otra forma y almacenamiento en instalaciones de procesamiento de datos, aun cuando no se utilice más que parcialmente sin la autorización del autor de la obra (NEMERGENT SOLUTIONS S.L.).

Índice

1	INTRODUCCIÓN	4
2	OBJETO	5
3	ALCANCE	5
4	MISIÓN	6
5	MARCO NORMATIVO	6
6	PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN	8
7	ORGANIZACIÓN DE LA SEGURIDAD.....	14
7.1	Comité de Seguridad.....	14
7.2	Roles de Seguridad asociados al ENS.....	15
7.2.1	Responsable de la Información y de los Servicios	16
7.2.2	Responsable de la Seguridad de la Información.....	16
7.2.3	Responsable del Sistema	17
7.3	Procedimiento de Designación y Renovación.....	18
8	DATOS DE CARÁCTER PERSONAL	18
9	OBLIGACIONES DEL PERSONAL	19
10	VIGENCIA Y REVISIÓN DE LA POLÍTICA.....	19
11	DESARROLLO DE LA POLÍTICA DE SEGURIDAD	19
12	RELACIÓN CON TERCERAS PARTES	20

1 INTRODUCCIÓN

En un entorno empresarial cada vez más digitalizado e interconectado, la seguridad de la información se ha consolidado como un elemento estratégico y esencial para garantizar la continuidad del negocio y preservar la reputación de las organizaciones, especialmente en el ámbito de las empresas de servicios. La protección adecuada de los datos internos, la información de clientes y los activos digitales no solo permite cumplir con las obligaciones legales y normativas, sino que además refuerza la confianza de los clientes y socios, al tiempo que incrementa la competitividad en un mercado cada vez más exigente.

Las amenazas a la seguridad de la información, tales como accesos no autorizados, fugas de datos, ataques cibernéticos o fallos en los sistemas, pueden comprometer gravemente la operatividad de la organización. Estas situaciones pueden derivar en interrupciones del servicio, pérdida de información crítica, impactos económicos y deterioro de la imagen corporativa. Por ello, resulta imprescindible establecer un marco sólido de protección basado en medidas de control, prevención y gestión de riesgos que garanticen los principios fundamentales de la seguridad de la información: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

En este contexto, NEMERGENT SOLUTIONS asume como objetivo prioritario asegurar la calidad, fiabilidad y disponibilidad de la información, así como la prestación continua de sus servicios. Para ello, adopta un enfoque proactivo basado en la prevención de incidentes, la supervisión constante de la actividad y la capacidad de respuesta ágil y eficaz ante cualquier evento que pueda afectar a la seguridad. Todo ello en consonancia con los requisitos establecidos por el Esquema Nacional de Seguridad (ENS) e ISO 27001 Sistema de Gestión de la Seguridad de la Información (SGSI), que actúan como marcos de referencia para la implantación de controles y buenas prácticas en materia de seguridad.

Los sistemas de información de la organización deben estar protegidos frente a un entorno de amenazas en constante evolución, lo que requiere el desarrollo e implementación de una estrategia de seguridad dinámica y adaptable. Dicha estrategia debe permitir responder a los cambios tecnológicos, regulatorios y operativos, garantizando en todo momento la continuidad de los servicios. En este sentido, los distintos departamentos de la organización deben aplicar las medidas mínimas de seguridad exigidas por el ENS, además de llevar a cabo un seguimiento continuo del

nivel de prestación de los servicios, identificar y analizar vulnerabilidades, y mantener planes de respuesta ante incidentes que permitan actuar con rapidez y eficacia.

Asimismo, la organización debe fomentar una cultura de seguridad entre todos sus miembros, promoviendo la concienciación y formación continua en materia de protección de la información, dado que el factor humano constituye uno de los elementos más críticos en la gestión de la seguridad.

La presente Política de Seguridad de la Información se establece como el marco de referencia para la implantación y mejora continua del SGSI. Esta política define los principios, objetivos y directrices que guían la actuación de la organización en materia de seguridad, teniendo en cuenta su actividad, estructura organizativa, ubicación, activos de información y tecnológicos, así como el contexto interno y externo en el que opera.

Del mismo modo, esta política considera el entorno actual y previsible de amenazas, el cumplimiento de la legislación vigente, las normativas aplicables y los compromisos contractuales adquiridos, integrando todo ello en una estrategia de gestión de riesgos coherente. Este enfoque permite establecer objetivos claros, medibles y alineados con la estrategia global de la organización, garantizando así la protección efectiva de la información y el soporte a la consecución de los objetivos empresariales.

2 OBJETO

Esta Política tiene como finalidad definir y establecer los principios y compromisos fundamentales de NEMERGENT SOLUTIONS en materia de Seguridad de la Información. Asimismo, sirve como marco de referencia para todo el personal propio y colaboradores externos, así como para los sistemas de información que soportan los servicios y los procesos necesarios para alcanzar y cumplir los objetivos del negocio.

3 ALCANCE

Esta Política será comunicada a todas las personas de la organización que tengan acceso a la información de NEMERGENT SOLUTIONS, quienes están obligadas a conocerla y cumplirla, así como a respetar la normativa de seguridad. Corresponde al Comité de Seguridad garantizar que existan los medios necesarios para que dicha información se difunda adecuadamente entre el personal afectado.

4 MISIÓN

Nuestra misión es ser el aliado estratégico de nuestros clientes en la transformación digital de las comunicaciones críticas, proporcionando soluciones de software seguras, innovadoras y de alta disponibilidad sobre redes de banda ancha (4G/5G). Nos comprometemos a guiar a las organizaciones en la transición hacia el estándar internacional MCX mediante un servicio personalizado basado en la lealtad, la independencia y el compromiso. Nos esforzamos por cumplir cada acuerdo con responsabilidad y eficiencia, garantizando la fiabilidad tecnológica necesaria para fortalecer la confianza y el éxito de quienes nos eligen.

Los pilares clave en que se basa nuestra misión son:

- **Innovación en Seguridad Pública:** Facilitar que los cuerpos de seguridad, emergencias y sectores de infraestructura crítica dispongan de herramientas de comunicación fiables.
- **Adopción de Estándares Internacionales:** Garantizar la interoperabilidad total mediante el cumplimiento estricto de los estándares del 3GPP.
- **Digitalización del Sector:** Ayudar a las organizaciones a dar el salto tecnológico desde los canales de voz tradicionales hacia soluciones multimedia ricas en datos (vídeo en tiempo real, localización precisa y analítica).

5 MARCO NORMATIVO

NEMERGENT SOLUTIONS respeta la legislación vigente y exige a los destinatarios igual cumplimiento escrupuloso de la normativa en vigor en cada momento. El marco normativo en que se desarrollan las actividades de la empresa está integrado por las siguientes normas principales:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- 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 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.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal y Garantía de los Derechos Digitales (LOPDGDD).
- Reglamento (UE) 679/2016 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 2/2019, de 1 de marzo, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Real Decreto de 24 de julio de 1889, texto de la edición del Código Civil.
- Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.
- Decreto 2414/1961 de 30 de noviembre, Reglamento de actividades molestas, insalubres, nocivas y peligrosas y correcciones (BOE 292) y correcciones (BOE).
- Decreto 165/1999, de 9 de marzo, por el que se establece la relación de actividades exentas de obligación de la licencia de actividad prevista en la Ley 3/1998, de 27 de febrero, General de Protección del Medio Ambiente del País Vasco (B.O.P.V núm. 59, de 26 de marzo de 1999).
- Ley 3/1998, de 27 de febrero, General de Protección del Medio Ambiente del País Vasco (B.O.P.V núm. 59, de 27 de marzo de 1998).
- Ley 22/2011, de 28 julio, de Residuos y suelos contaminados.
- Ley 7/2022, de 8 de abril, de residuos y suelos contaminados para una economía circular.

El mantenimiento del marco normativo aplicable será responsabilidad del Comité de Seguridad, conforme a lo dispuesto en la Disposición adicional segunda relativa al desarrollo del Esquema Nacional de Seguridad, establecida en el Real Decreto 311/2022.

Asimismo, el Comité será responsable de identificar las guías de seguridad del Centro Criptológico Nacional (CCN) mencionadas en dicha disposición, que resulten aplicables con el fin de reforzar el cumplimiento de los requisitos establecidos en el ENS.

6 PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

NEMERGENT SOLUTIONS establece como el marco general para la definición del SGSI aquellas medidas y controles aplicables contenidos en el Real Decreto 311/2022 que regula el Esquema Nacional de Seguridad.

En tal sentido, los principios básicos para la Seguridad de la Información se recogen a continuación:

- Seguridad como proceso integral.
- Seguridad basada en la gestión de riesgos.
- Prevención, detección, respuesta y conservación.
- Existencia de líneas de defensa.
- Vigilancia continua.
- Reevaluación periódica
- Diferenciación de responsabilidades.

Basándonos en estos principios y para dar cumplimiento a los artículos del ENS se establece lo siguiente:

- **Seguridad como un proceso integral (artículo 6) y mínimo privilegio (artículo 20)**

La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales, técnicos, jurídicos y organizativos, relacionados con el sistema de información. Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y la de los responsables jerárquicos.

Los sistemas se diseñarán y configurarán de forma que garanticen el mínimo privilegio necesario para su correcto desempeño, del siguiente modo:

- El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.
 - Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos autorizados, pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.
 - Se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.
 - Se aplicarán las guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema.
- **Gestión de la seguridad basada en los riesgos (artículo 7) y análisis y gestión de riesgos (artículo 14)**

Como elemento esencial del proceso de seguridad, todos los sistemas están sometidos a un análisis de riesgos continuo y permanentemente actualizado, cuya finalidad es evaluar las amenazas y los riesgos a los que se encuentran expuestos. Este análisis se llevará a cabo de la siguiente manera:

- Al menos una vez al año.
- Cuando cambien los servicios prestados y/o información manejada.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité de Seguridad establecerá criterios de valoración de referencia para los distintos tipos de información gestionada y los servicios prestados. Asimismo, impulsará la disponibilidad de recursos necesarios para atender las necesidades de

seguridad de los diferentes sistemas, promoviendo inversiones de carácter transversal.

El Responsable de Seguridad de la Información será el encargado de garantizar la realización del análisis de riesgos, así como de identificar posibles carencias y debilidades, informando de ellas al Comité de Seguridad.

NEMERGENT SOLUTIONS contará con un proceso de gestión de riesgos que se desarrollará conforme a lo dispuesto en los anexos I y II del Real Decreto 311/2022, así como a las normas, instrucciones, guías CCN-STIC y recomendaciones elaboradas por el Centro Criptológico Nacional (CCN) para su correcta aplicación.

- **Vigilancia y reevaluación periódica (artículo 10) e integridad y actualización del sistema (Artículo 21)**

Se han implantado controles de supervisión continua y evaluaciones periódicas de la seguridad, con el objetivo de conocer en todo momento el estado de los sistemas en relación con las especificaciones de los fabricantes, las vulnerabilidades y las actualizaciones que puedan afectarles, actuando de forma diligente para gestionar los riesgos identificados. Asimismo, la incorporación de nuevos elementos, tanto físicos como lógicos, estará sujeta a una autorización formal previa.

De igual modo, se promoverán revisiones periódicas por parte de terceros, con el fin de obtener una evaluación independiente del estado de la seguridad.

- **Gestión de personal (artículo 15) y profesionalidad (artículo 16)**

Todo el personal de NEMERGENT SOLUTIONS participará, al menos una vez al año, en sesiones de concienciación en materia de seguridad de la información, con el objetivo de conocer y comprender sus deberes, obligaciones y responsabilidades en este ámbito. Además, se establecerá un programa continuo de concienciación dirigido a todos los miembros de la organización, prestando especial atención a las nuevas incorporaciones.

El personal con responsabilidades en el uso, operación o administración de los sistemas TIC recibirá la formación necesaria para garantizar un uso seguro de los mismos, en función de las exigencias de su puesto. Esta formación será obligatoria antes de asumir dichas responsabilidades, ya sea en una primera asignación o como consecuencia de un cambio de funciones o de puesto de trabajo.

- **Incidentes de seguridad (artículo 25), prevención, detección, respuesta y conservación (artículo 8)**

Se cuenta con procedimientos de gestión de incidentes de seguridad que incluyen mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como canales de comunicación con las partes interesadas y el registro de todas las actuaciones. Este registro se utilizará como base para la mejora continua de la seguridad del sistema.

Con el fin de evitar que la información y/o los servicios se vean afectados por incidentes de seguridad, se implementan las medidas de seguridad establecidas por el ENS, así como aquellos controles adicionales que se hayan identificado como necesarios a partir de la evaluación de amenazas y riesgos. Estos controles, junto con los roles y responsabilidades en materia de seguridad de todo el personal, se encuentran claramente definidos y documentados.

Asimismo, NEMERGENT SOLUTIONS establecerá las siguientes medidas de respuesta ante incidentes de seguridad para garantizar la disponibilidad, recuperación y conservación de sus servicios más críticos:

- Mecanismos de respuesta eficaz ante cualquier brecha o evento de seguridad.
 - Un punto de contacto centralizado para coordinar y canalizar las comunicaciones sobre incidentes detectados en otros departamentos.
 - Protocolos de intercambio bidireccional de información, facilitando la comunicación constante y directa con los Equipos de Respuesta a Emergencias (CERT).
- **Existencia de Líneas de defensa (artículo 9) y prevención ante otros sistemas interconectados (artículo 23)**

Se implementa una estrategia de defensa en profundidad basada en múltiples capas de seguridad (organizativas, físicas y lógicas). De este modo, ante el fallo de cualquiera de ellas, el sistema garantiza la capacidad de:

- Optimizar el tiempo de respuesta ante incidentes que no hayan podido evitarse.
- Mitigar el riesgo de un compromiso sistémico o global de la infraestructura.
- Minimizar el impacto residual sobre el sistema.

Este enfoque prioriza la protección del perímetro, especialmente en conexiones a redes públicas. Asimismo, se evaluarán de forma continua los riesgos derivados de la interconexión con sistemas externos, aplicando un control estricto sobre cada punto de unión.

- **Diferenciación de responsabilidades (artículo 11) y organización e implantación del proceso de seguridad (artículo 13)**

NEMERGENT SOLUTIONS articula su estrategia de seguridad mediante el compromiso activo de todo su personal. Para ello, define roles con responsabilidades claramente delimitadas, así como mecanismos específicos de coordinación y resolución de conflictos, detallados en el apartado de “Organización de la Seguridad” de esta Política. Asimismo, para los servicios externalizados, se exigirá que la entidad proveedora designe un punto o persona de contacto (POC) responsable de la seguridad de la información tratada y del servicio prestado.

- **Autorización y control de los accesos (artículo 17)**

Se implementan mecanismos de control de acceso a los sistemas de información, restringiéndolos exclusivamente al personal debidamente autorizado y bajo el principio de necesidad de conocer.

- **Protección de las instalaciones (artículo 18)**

Se implementan mecanismos de control de acceso físico para prevenir intrusiones no autorizadas, así como daños a la información y a los activos. Para ello, se establecen perímetros de seguridad, barreras físicas y medidas de protección general en todas las áreas restringidas.

- **Adquisición de productos de seguridad y contratación de servicios de seguridad (artículo 19)**

NEMERGENT SOLUTIONS priorizará la adquisición de productos y la contratación de servicios de seguridad TIC que cuenten con certificaciones de seguridad acreditadas y alineadas con su propósito de uso. Asimismo, se observarán estrictamente los criterios y directrices establecidos por el Organismo de Certificación del Centro Criptológico Nacional (CCN), promoviendo la selección de soluciones incluidas en su catálogo de productos y servicios certificados.

- **Protección de la información almacenada y en tránsito (artículo 22) y continuidad de la actividad (artículo 26)**

Se implementan mecanismos avanzados para proteger la información tanto almacenada como en tránsito, con especial rigor en entornos de alto riesgo (como dispositivos móviles, soportes portátiles o redes abiertas). Para asegurar la resiliencia operativa, los sistemas cuentan con copias de seguridad y mecanismos necesarios para garantizar la continuidad de las operaciones que garantizan la actividad ante cualquier interrupción de los medios habituales de trabajo. Asimismo, se dispone de procedimientos para la recuperación y conservación a largo plazo de los documentos electrónicos, asegurando mediante controles específicos que la información en soporte físico reciba el mismo grado de protección y confidencialidad que la digital.

- **Registros de actividad y detección de código dañino (artículo 24)**

Se han habilitado registros de actividad (logs) que retienen la información necesaria para monitorizar, analizar, investigar y documentar accesos o acciones no autorizadas, garantizando la trazabilidad e identificación inequívoca de cada usuario. La recopilación de estos datos se realiza con la finalidad exclusiva de dar cumplimiento al Real Decreto 311/2022 (ENS), asegurando el pleno respeto a los derechos al honor, a la intimidad personal y familiar, y a la propia imagen, de estricto acuerdo con la normativa de protección de datos personales, legislación laboral y de función pública aplicable.

Asimismo, con el único objetivo de salvaguardar la seguridad de la información, se analizará el tráfico de comunicaciones entrantes y salientes para prevenir accesos no autorizados, mitigar ataques de denegación de servicio (DoS/DDoS) y bloquear la propagación de código malicioso (malware).

- **Mejora continua del proceso de seguridad (artículo 27)**

El Sistema de Gestión de la Seguridad de la Información (SGSI) implementado promoverá la mejora continua de todos los procesos de seguridad. Para ello, se aplicarán metodologías y marcos de referencia de reconocido prestigio nacional e internacional que garanticen la madurez y la excelencia en la gestión de las tecnologías de la información.

7 ORGANIZACIÓN DE LA SEGURIDAD

NEMERGENT SOLUTIONS provee los recursos necesarios para salvaguardar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de sus sistemas de información. De este modo, se garantiza tanto el correcto desarrollo de la actividad laboral de sus profesionales como la excelencia y seguridad en los servicios prestados a los clientes.

7.1 Comité de Seguridad

NEMERGENT SOLUTIONS ha constituido un Comité de Seguridad, como órgano colegiado y está formado por los siguientes miembros:

- *Chief Executive Officer (CEO)* / Presidente del Comité.
- *Chief Operating Officer (COO)* / Responsable de Seguridad de la Información y Representante de los Responsables de Servicio/información.
- *System Engineer Manager* / Responsable del Sistema.
- *Human Resources Manager* / Responsable de Recursos Humanos y Datos Personales y *Chief Financial Officer (CFO)*.

El Comité de Seguridad de la Información estará presidido por el *Chief Executive Officer (CEO)*, en su calidad de máxima responsabilidad de las actividades, procesos y servicios de la organización. Su composición garantizará la representación de todas las áreas de negocio significativas, mientras que la secretaría será ejercida por Responsable de Seguridad de la Información.

El Comité se reunirá ordinariamente con una periodicidad anual, mediante convocatoria previa que incluirá un orden del día definido. No obstante, la frecuencia de las sesiones podrá ser alterada con carácter extraordinario cuando las circunstancias operativas lo justifiquen. Asimismo, y con carácter opcional, se podrá convocar a profesionales internos, asesores externos o perfiles mixtos según los requerimientos de la sesión.

Las competencias y responsabilidades clave del Comité en materia de seguridad de la información son:

- **Estrategia y Coordinación:** Definir, supervisar y coordinar la ejecución de los planes estratégicos de seguridad, actuando como órgano asesor y resolviendo conflictos de responsabilidad interna.

- **Cultura y Concienciación:** Difundir la política y normativa de seguridad, promoviendo la formación continua y una cultura de concienciación en toda la plantilla (interna y externa) mediante la asignación de los recursos necesarios.
- **Supervisión y Control:** Evaluar la eficacia de la gestión de la seguridad y el cumplimiento normativo a través de métricas o cuadros de mando, realizando el seguimiento de los acuerdos adoptados en sesiones anteriores.
- **Gobernanza del SGSI y Mejora Continua:** Impulsar la evolución del Sistema de Gestión de la Seguridad de la Información, asumiendo las siguientes atribuciones directas:
 - Monitorizar los riesgos residuales asumidos y recomendar acciones de mitigación.
 - Supervisar la gestión de incidentes de seguridad y proponer medidas correctoras.
 - Elaborar y actualizar periódicamente la Política de Seguridad para su aprobación definitiva.
 - Desarrollar la normativa técnica de seguridad en coordinación con la Gerencia.
 - Validar los procedimientos operativos y el resto de documentación del sistema.
 - Impulsar auditorías periódicas (ENS, LOPDGDD/RGPD) para verificar el cumplimiento legal.
 - Diseñar programas de sensibilización enfocados en la seguridad y la protección de datos personales.

7.2 Roles de Seguridad asociados al ENS

La gobernanza de la seguridad de la información en la organización se articula en torno a tres figuras organizativas diferenciadas, conforme a lo estipulado por el Esquema Nacional de Seguridad (ENS). Las competencias y funciones asignadas a cada rol se detallan a continuación:

7.2.1 Responsable de la Información y de los Servicios

Este rol es asumido de forma coordinada por los Responsables de Área de un Servicio en particular y dentro de sus respectivos ámbitos competenciales:

- **Establecimiento de requisitos:** Definir y proponer los requisitos de seguridad aplicables a la información y los servicios bajo su gestión, de acuerdo con el marco del Anexo I del Real Decreto 311/2022, elevándolos al Responsable de Seguridad o al Comité de Seguridad para su aprobación.
- **Clasificación y valoración de activos:** Determinar los niveles de seguridad requeridos mediante la participación en el Análisis de Riesgos y la valoración de los activos a su cargo en todas las dimensiones de seguridad aplicables.
- **Gestión de accesos:** Definir y autorizar los perfiles y derechos de acceso específicos a la información y los servicios de su competencia.
- **Aceptación de riesgos:** Validar y asumir formalmente los niveles de riesgo residual que afecten directamente a sus servicios y activos de información.
- **Gestión del cambio operacional:** Comunicar de inmediato al Responsable de Seguridad cualquier modificación sustancial en los servicios o la información bajo su cargo, especialmente la integración de nuevos flujos o plataformas.

7.2.2 Responsable de la Seguridad de la Información

Este rol es asumido por el *Chief Operating Officer (COO)*, actuando como el garante principal de la protección del sistema:

- **Garantía de cumplimiento:** Mantener, verificar y supervisar que el nivel de seguridad de la información gestionada y de los servicios electrónicos prestados sea el adecuado.
- **Cultura de seguridad:** Impulsar y promover planes de formación, concienciación y sensibilización en materia de ciberseguridad para todo el personal.
- **Categorización del sistema:** Asesorar y liderar la determinación de la Categoría del Sistema en coordinación con el Responsable del Sistema y el Comité de Seguridad.

- **Gobernanza del riesgo:** Designar a los encargados de ejecutar el análisis de riesgos, confeccionar la Declaración de Aplicabilidad (SoA), identificar las salvaguardas y determinar las configuraciones de seguridad necesarias.
- **Gestión documental y auditoría:** Elaborar, actualizar y mantener la documentación marco de seguridad, coordinando las auditorías y revisiones tanto internas como externas.
- **Resiliencia y continuidad:** Participar activamente en el diseño, implantación y validación de los planes de mejora de la seguridad y de los Planes de Continuidad de Negocio (BCP).
- **Certificación:** Coordinar la gobernanza del Sistema de Gestión y liderar los procesos de auditoría para la obtención y mantenimiento de la certificación ENS.
- **Evolución del sistema:** Elevar al Comité de Seguridad las propuestas de cambios estructurales y los nuevos requisitos normativos para su aprobación.

7.2.3 Responsable del Sistema

Este rol es asumido por el *System Engineer Manager*, encargado de la implantación operativa de las salvaguardas:

- **Ciclo de vida del sistema:** Desarrollar, operar, explotar y mantener los sistemas de información a lo largo de todo su ciclo de vida.
- **Integración de salvaguardas:** Garantizar que las medidas específicas de seguridad tecnológica se integren de forma alineada dentro del marco general de la organización.
- **Arquitectura y uso:** Diseñar la topología del Sistema de Información, estableciendo los criterios técnicos de uso y regulando los servicios disponibles en la infraestructura.
- **Normalización técnica:** Redactar, actualizar y mantener los procedimientos operativos, normas técnicas e instrucciones de trabajo del sistema.
- **Colaboración técnica:** Participar juntamente con el Responsable de Seguridad en la categorización del sistema y en el despliegue de los planes de mejora y de continuidad tecnológica.

- **Cláusula de salvaguarda operacional:** Suspender de manera inmediata el acceso a la información o la prestación de un servicio si se detectan deficiencias graves o vulnerabilidades críticas que comprometan la seguridad de la organización.
- **Administración de la Seguridad:** Ejercer las funciones propias de la administración de seguridad del sistema, encargándose específicamente de:
 - Gestionar, configurar y actualizar el hardware y software que sustentan las herramientas y los servicios de seguridad.
 - Aprobar los cambios en la línea base de configuración de los sistemas, garantizando la eficacia de los controles establecidos.
 - Supervisar las modificaciones, despliegues y mejoras de la infraestructura para asegurar que no se debilite el perímetro de seguridad y que se ajusten a las autorizaciones vigentes.
 - Asegurar la aplicación rigurosa de los procedimientos operativos aprobados.
 - Administrar el ciclo de vida de las identidades y los privilegios de los usuarios, monitorizando activamente que su actividad se ciña estrictamente a los permisos concedidos.
 - Monitorizar el estado de la seguridad técnica mediante herramientas de gestión de eventos (SIEM) y mecanismos de auditoría técnica o registro de logs.

7.3 Procedimiento de Designación y Renovación

NEMERGENT SOLUTIONS, a través de su Dirección General, formalizará la designación y renovación de los distintos roles de seguridad, así como la constitución del Comité de Seguridad de la Información. Con el fin de garantizar la vigencia y adecuación de dichos cargos, todos los nombramientos serán objeto de revisión cada cuatro años o de forma inmediata en caso de que el puesto quede vacante.

8 DATOS DE CARÁCTER PERSONAL

En cumplimiento de la normativa vigente en materia de privacidad (RGPD y LOPDGDD) y en consonancia con el Real Decreto 311/2022 (ENS), NEMERGENT SOLUTIONS

garantiza la protección de los datos de carácter personal integrando controles específicos en el ciclo de vida de sus sistemas. Las medidas de seguridad implantadas corresponden a la naturaleza de los datos tratados y a las conclusiones de sus análisis de riesgos periódicos, asegurando la confidencialidad, integridad y disponibilidad de la información personal gestionada en el ámbito de sus competencias.

9 OBLIGACIONES DEL PERSONAL

Todo el personal de NEMERGENT SOLUTIONS tiene el deber de conocer y dar estricto cumplimiento a la presente Política de Seguridad de la Información y a su normativa de desarrollo. Corresponde al Comité de Seguridad de la Información habilitar los canales y medios necesarios para garantizar la correcta difusión y accesibilidad de estos documentos a todos los usuarios afectados.

El incumplimiento de las directrices establecidas en esta Política o en la regulación interna sobre el uso seguro de los activos de información y recursos tecnológicos podrá dar lugar a la aplicación de las medidas disciplinarias y sancionadoras oportunas. Dichas medidas se ejecutarán de conformidad con la legislación laboral aplicable, ponderando la gravedad, el impacto y las circunstancias específicas de la infracción.

10 VIGENCIA Y REVISIÓN DE LA POLÍTICA

Esta Política de Seguridad de la Información entrará en vigor de manera inmediata a partir de la fecha de su publicación oficial. El Comité de Seguridad auditará y revisará este documento con una periodicidad mínima anual, o de forma extraordinaria cuando acontezcan cambios significativos, con el fin de asegurar su idoneidad, adecuación y eficacia continuas.

Este proceso de revisión se orientará tanto a la identificación de oportunidades de mejora en la gobernanza de la seguridad como a la alineación del marco normativo con las transformaciones organizativas, legales o de la infraestructura tecnológica de la compañía. La presente Política será ratificada por el Comité de Dirección y difundida a todas las partes interesadas.

11 DESARROLLO DE LA POLÍTICA DE SEGURIDAD

El Comité de Seguridad de la Información lidera el despliegue del Sistema de Gestión de la Seguridad de la Información (SGSI), el cual será establecido, implementado,

mantenido y optimizado de acuerdo con las mejores prácticas y estándares internacionales. Este SGSI actuará como el marco operativo para la gestión y cumplimiento de los controles del Esquema Nacional de Seguridad (ENS).

El sistema estará plenamente documentado y diseñado para generar las evidencias necesarias que demuestren la eficacia de los controles y el grado de consecución de los objetivos fijados. A tal efecto, se dispondrá de un procedimiento de gestión documental que regulará la estructura, el ciclo de vida y los permisos de acceso a la documentación de seguridad.

Toda la información y normativa del SGSI estará disponible para el personal propio y externo de la organización, restringiendo el acceso exclusivamente bajo el principio de «necesidad de conocer» para el correcto desempeño de sus funciones. Asimismo, el SGSI se someterá de forma periódica a auditorías internas y externas, de carácter total o parcial, con el objetivo de evaluar su rendimiento, certificar su cumplimiento legal y promover acciones correctoras enfocadas en la mejora continua.

12 RELACIÓN CON TERCERAS PARTES

Cuando NEMERGENT SOLUTIONS actúe como proveedor de servicios o custodie información de organismos externos, compartirá formalmente los principios de esta Política de Seguridad, habilitando canales de coordinación directa entre los respectivos Comités de Seguridad y unificando los protocolos de respuesta ante incidentes.

Por otro lado, cuando la organización subcontrate servicios de terceros o realice cesiones de datos, exigirá contractualmente la adhesión de los proveedores a esta Política y a la normativa técnica aplicable a su ámbito. Las terceras partes quedarán sujetas a las obligaciones de seguridad de la empresa, estando facultadas para desarrollar sus propios procedimientos operativos siempre que cumplan o superen los niveles de protección requeridos. Adicionalmente, se establecerán flujos específicos para el reporte y resolución de incidencias, garantizando que el personal externo cuente con una capacitación y concienciación en ciberseguridad equivalente a la del personal propio.