Política de Seguridad de la Información

PROYECTO: Seguridad de la organización

FECHA: 12/06/2025

☒ Interno ☐ Confidencial ☐ Borrador

ÍNDICE

1. Entrada en vigor 6
2. Introducción 7
3. Principios y directrices 8
3.1 Prevención 10
3.2 Detección 11
3.3 Respuesta 12
3.4 Recuperación 12
4. Misión 13
5. Alcance 14
6. Marco normativo 15
7.1 Acrónimos y siglas 18
7.2 Roles, funciones y responsabilidad 18
7.2.1 Tareas 18
7.2.2 Respuesta a incidentes de seguridad de la información 20
7.3 Responsabilidad 22
7.4 Roles definidos conforme al ENS 22
7.5 Incompatibilidades designadas 23
7.6 Procedimiento de designación 25
7.7 Comité de Seguridad de la Información 25
7.8 Responsable de los servicios de información 28
7.9 Responsable del servicio 29
7.10 Responsable de la seguridad de la información 29
7.11 Responsable del Sistema 30

7.13 Responsable de la Seguridad del Sistema 32
7. Tratamiento de datos personales 34
8. Gestión de riesgos 34
9. Desarrollo de normativa de seguridad 35
10.1 Política de seguridad de la información 35
10.2 Procedimientos y procesos de seguridad 35
10.3 Instrucciones técnicas de seguridad 35
10. Obligaciones de empleados y asociados 36
11. Terceras partes 37
13. Acuerdos de confidencialidad 38

Historial de revisiones

Fecha	Editor	Cambios realizados
30/10/2023	S. Izquierdo	Redacción inicial
07/11/2023	S. Izquierdo	Modificación cumplimiento.
01/04/2025	M.Corbella	Actualización TISAX
09/06/2025	M.Corbella	Modificación cumplimiento.
12/06/2025	Gerencia	Aprobación del documento

1. Entrada en vigor

Este documento contiene la Política de Seguridad de la Información (PSI) que entrará en vigor al día siguiente de su aprobación por la Gerencia de Neo Digital Solutions S.L. con fecha 1 de abril de 2025.

La entrada en vigor supone la derogación de cualquier otra política previa existente y estará vigente hasta que sea reemplazada por una nueva política aprobada.

Está política ha sido aprobada por la dirección de NEO DIGITAL y se revisará anualmente o ante cualquier cambio significativo en el entorno de la NEO DIGITAL o en los requisitos legales o reglamentarios.

Director de NEO DIGITAL

Jesús Moya

2. Introducción

La presente política de seguridad de la información establece los lineamientos y principios generales para garantizar la protección y el manejo seguro de la información en Neo Digital Solutions S.L.

El propósito de esta política de seguridad de la información es proteger los activos de información de NEO DIGITAL, en particular, los sistemas de información que dan soporte a la prestación de servicios de digitalización en los servicios de asistencia técnica, programación y mantenimiento asociados a esta tecnología para el sector de la automoción. Esta política está alineada con la dirección estratégica de NEO DIGITAL y busca apoyar los objetivos de negocio de la NEO DIGITAL a través de la gestión adecuada de la seguridad de la información.

Nuestro compromiso con la confidencialidad, integridad y disponibilidad de los datos es fundamental para garantizar la confianza de nuestros clientes, socios y empleados.

Reconocemos la importancia de los sistemas de información y comunicaciones para la consecución de nuestros objetivos. Siendo de vital importancia administrar los sistemas con diligencia para protegerlos frente a datos accidentales o deliberados que puedan afectar a la seguridad (confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad) de la información tratada o los servicios prestados.

Con el objeto de estar a la vanguardia en la digitalización y poder prestar un servicio eficaz a nuestros clientes requerimos de una estrategia que sea

adaptable a los numerosos cambios tecnológicos para poder seguir garantizando una prestación continúa de nuestros servicios con calidad.

Los objetivos del sistema de gestión de seguridad de la información son:

- Proteger la información contra pérdidas de disponibilidad, confidencialidad e integridad.
- Evaluar y gestionar los riesgos de seguridad de la información de forma sistemática y periódica, implementando controles adecuados para mitigar los riesgos identificados.
- Cumplir los requisitos legales aplicables, los requisitos aplicables a la seguridad de la información y los sistemas de información, las expectativas de los clientes y los compromisos contractuales, en cuanto a seguridad de la información y la protección de datos.
- Mejorar continuamente el sistema de gestión de seguridad de la información.
- Cumplir con los objetivos de evaluación específicos
    - *Confidential:* Manejo de información con necesidad de protección alta en el contexto de la confidencialidad.
    - *High availability*: Manejo de información con necesidad de protección alta en el contexto de la disponibilidad.
- Alinearse con TISAX VDA ISA AL2

3. Principios y directrices

Esta política es de aplicación obligatoria para todos los miembros de la organización y será revisada y actualizada periódicamente para adaptarse a los cambios tecnológicos y normativos.

Se aplicarán las medidas exigidas por el Esquema Nacional de Seguridad (ENS) como referente normativo de ciberseguridad:

- Seguimiento continuo de niveles de prestación de servicios.
- Análisis, corrección y/o mitigación de vulnerabilidades.
- Preparación de una respuesta efectiva a las incidencias.
- Tomar la seguridad de la información como una parte integral de cada etapa del ciclo de vida de cada sistema, desde su análisis, desarrollo o adquisición y las actividades de explotación.
- Nuestros empleados estarán preparados para prevenir, detectar, reaccionar y recuperarse de forma efectiva de las incidencias.
- En la elaboración de nuestros productos y trabajos a nuestros clientes velaremos por una implementación segura conforme a todas las directrices necesarias, realizando un proceso continuo de mejora.

En el marco del Esquema Nacional de Seguridad, serán de aplicación los siguientes preceptos:

- Análisis y gestión de los riesgos.
- Gestión de personal.
- Profesionalidad.
- Autorización y control de los accesos.
- Protección de las instalaciones.
- Adquisición de productos.
- Seguridad por defecto.
- Integridad y actualización del sistema.
- Protección de la información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados.
- Registro de actividad.
- Incidentes de seguridad.

- Continuidad de la actividad.
- Mejora continua del proceso de seguridad.

3.1 Prevención

Los empleados de Neo Digital Solutions serán formados en materia de seguridad informática aplicable tanto a su actividad diaria en la empresa conforme a sus funciones y responsabilidades. Adicionalmente recibirán formación específica sobre prácticas seguras y metodología apropiada en cada caso.

El objetivo de la organización es evitar, en la medida que sea posible, que la información, servicios o información se vean afectados por incidentes de seguridad.

Todos los departamentos funcionales implementarán, de forma obligatoria, las medidas mínimas de seguridad que se detallan en este documento. Estas medidas y procedimientos se verán complementados por controles adicionales identificados a través de una evaluación de amenazas y riesgos y un proceso de identificación y seguimiento de cambios.

Para una correcta gestión de su aplicación y conocimiento, serán documentados todos los roles, funciones, controles y responsabilidades derivadas.

Se velará por una supervisión continua del cumplimiento para observar los posibles cambios o desviaciones en su aplicación.

Antes de que un sistema o proceso informático inicie su operación deberá ser validado y aprobado.

Se solicitará una revisión periódica por parte de terceras personas para poder obtener evaluación independiente.

Se mantendrá el software actualizado de manera sistemática, instalando las últimas versiones y parches de seguridad disponibles, para proteger los sistemas contra vulnerabilidades conocidas y reducir el riesgo de incidentes de seguridad.

3.2 Detección

La organización determina que los servicios y sistemas deberán ser monitorizados para observar cambios no deseados, posibles degradaciones de servicio y detectar otras anomalías en los niveles de prestación de servicios.

El objetivo tanto de las pruebas periódicas como de la monitorización continua es la detección, corrección y estudio.

Si se determina que la eficacia de las medidas de seguridad, en materia de seguridad de informática, no es suficiente en un ámbito particular, las medidas deberán replantearse teniendo en cuenta el origen, necesidades, riesgos y sistema de protección involucrados.

Del mismo modo, los parámetros que determinan un funcionamiento correcto deberán ser reevaluados periódicamente.

Los mecanismos de detección, análisis y reporte llegarán a los responsables de forma regular y cuando se produzca una desviación significativa de los parámetros establecidos.

3.3 Respuesta

Neo Digital Solutions establecerá mecanismos para poder responder de forma eficaz a las incidencias de seguridad.

La organización designará un punto de contacto para las comunicaciones con respecto a las incidencias detectadas en departamentos, entidades o relaciones externas.

Se establecerán protocolos de intercambio de información relacionada con la incidencia.

Todo proceso iniciado deberá llevar un seguimiento hasta su cierre para asegurar que se cumple el ciclo de vida establecido.

3.4 Recuperación

Para garantizar la disponibilidad de los servicios críticos, Neo Digital Solutions desarrollará planes de continuidad de los sistemas de información como una parte integral de su plan general de continuidad de negocio y actividades de recuperación.

4. Misión

Neo Digital Solutions es una empresa tecnológica experta en Digitalización.

La misión fundamental de la organización es desarrollar y ofrecer tanto productos como soluciones tecnológicas a clientes industriales de diferentes sectores de actividad para la gestión de la producción, orientadas a conseguir una digitalización estructurada potente, escalable y sostenible. Todo ello sin dejar de lado la seguridad informática y la prevención de riesgos.

Los valores con los que se compromete la organización son:

- Personas.
- Profesionalidad.
- Sostenibilidad.
- Calidad.
- Cliente.
- Integridad.
- Confiabilidad.

es una empresa centrada en la gestión de filiales tecnológicas con la misión de gestionar y dinamizar empresas tecnológicas para dotarlas de los métodos y sistemas corporativos idóneos, generar sinergias, y desarrollar y ofrecer soluciones tecnológicas integrales a clientes industriales de diferentes sectores de actividad para una producción inteligente y optimizada.

La visión de Neo Digital Solutions es ser una empresa líder en el mercado por:

- Proporcionar un espacio de desarrollo y trabajo excelente.
- Elevado nivel de know-how: dominar la tecnología más actual en cada momento.
- Implantar productos y soluciones que provechen las posibilidades tecnológicas al máximo.

- Implantar productos y soluciones adaptadas a las necesidades reales del cliente.
- Ser un referente en productos de gestión para empresas, por producto, amplitud, servicio e integración.

En el desarrollo e integración de *Industrias Inteligentes* o *Smart Factories* se apuesta por una correcta y potenciada estrategia de digitalización en todas sus capas. Neo Digital Solutions ofrece servicios y soluciones para los diferentes niveles, siguiendo los estándares de la industria y normativas de seguridad como UNE-EN IEC 62264 para ofrecer un alto valor tecnológico.

5. Alcance

La política de seguridad de la información descrita se aplicará a todos los sistemas de tecnología de la información de Neo Digital Solutions, a toda su información y a todos sus miembros, sin ninguna excepción.

En esta consideración de miembro se considerará tanto a los empleados internos, externos vinculados por contratos o acuerdos con terceros.

Todo miembro afectado por el alcance del Esquema Nacional de Seguridad tiene la obligación de conocer y cumplir la política de seguridad de información y las normativas de seguridad que correspondan.

El Comité de Seguridad de la Información deberá disponer de los medios para que la información llegue a toda persona afectada.

6. Marco normativo

El marco normativo de las actividades de la organización en el ámbito de la Política de Seguridad de la Información está integrado por las siguientes normas, recomendaciones y directrices:

- 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.
- Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.
- 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.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Nacional de Seguridad en el ámbito de la Administración Electrónica.
-

- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el Ámbito de la Administración Electrónica.
- Ley 37/2007, de 16 de noviembre.
- Reglamento evaluación y certificación de seguridad de TIC.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Guía Nacional de Notificación y Gestión de Ciberincidentes, INCIBE.
- EU Digital Strategy.
- EU Strategy for Data.
- EU on AI White Paper and EU Cybersecurity Package.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- NTI SICRES 4, según la Resolución de 22 de julio de 2021, de la Secretaría de Estado de Digitalización e Inteligencia Artificial, por la que se aprueba la Norma Técnica de Interoperabilidad de Modelo de Datos.
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, reglamento de leyes 39 y 40.
- Centro Criptológico Nacional, Guía de Seguridad. CCN-STIC 805, 801, 803, 804, 806, 811, 812, 813, 802, 808, 809, 815 y 885X, 884X.
- Reglamento (UE) 2021/887 del Parlamento Europeo y del Consejo, de 20 de mayo de 2021, por el que se establecen el Centro Europeo de

- Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación.

- Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación.
- Carta de derechos digitales.
- Plan de Recuperación, Transformación y Resiliencia, Componente 15. Conectividad Digital, impulso de la ciberseguridad y despliegue del 5G.
- Centro Criptológico Nacional, Mayo 2020, Obligaciones de los prestadores de servicios a las AAPP.
- Ley 11/2022, de 8 de junio, General de Telecomunicaciones.
- Plan Nacional de Ciberseguridad - Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley 11/2023, de 8 de mayo, de trasposición de Directivas de la Unión Europea en materia de accesibilidad de determinados productos y servicios, migración de personas altamente cualificadas, tributaria y digitalización de actuaciones notariales y registrales.
- Centro Criptológico Nacional, Guia de Seguridad de seguridad de las TIC. CCN-STIC 808/Octubre 2023.
- TISAX VDA ISA en su edición en vigor.

También se consideran parte del marco normativo las normas aplicables a las actividades propias de Neo Digital Solutions.

La organización dispone de instrumentos organizativos para gestionar la normativa aplicable y la supervisión de todo lo relativo a las actualizaciones periódicas (anuales o cuando aparezcan cambios significativos) por parte del Comité de Seguridad de la Información.

Organización de la seguridad

La organización de la seguridad se establece mediante la identificación y definición de diferentes tareas, funciones, responsabilidades e implementaciones en materia de gestión y seguridad en los sistemas.

7.1 Acrónimos y siglas

Se definen los siguientes acrónimos para la definición de roles funcionales:

Identificador	Rol asociado
GER/Gerencia	Persona con la máxima responsabilidad en la organización.
CSI	Comité de Seguridad de la Información.
RINFO	Responsable de la Información.
RSERV	Responsable del Servicio.
RSEG-CISO	Responsable de la Seguridad.
RSIS	Responsable del Sistema.
ASS-CISM	Administrador de la Seguridad del Sistema.

7.2 Roles, funciones y responsabilidad

7.2.1 Tareas

		Responsable							
ID	Tarea	Principal	Elabora	Aprueba	Aplica	Monitoriza	Informa a	Coordina	Ejercicios
PSITR-001	Determinación de los niveles de seguridad requeridos en cada dimensión.	CSI	RINFO + RSERV o CSI						
PSITR-002	Determinación de la categoría del sistema.	RSEG	RSEG	RSEG	RSEG		CSI	CSI	CSI
PSITR-003	Análisis de riesgos.	RSEG	RSEG	RSEG	RSEG		CSI	CSI	CSI
PSITR-004	Declaración de aplicabilidad.	RSEG	RSEG	RSEG	RSEG		CSI	CSI	CSI
PSITR-005	Medidas de seguridad adicionales.	RSEG	RSEG	RSEG	RSEG		CSI	CSI	CSI
PSITR-006	Configuración de seguridad	RSEG	RSEG	RSEG	ASS	RSEG	CSI	CSI	CSI
PSITR-007	Implantación de las medidas de seguridad.	ASS			ASS	ASS	ASS	RSEG	
PSITR-008	Aceptación del riesgo residual.	RINFO+RSERV	RINFO+RSERV	CSI o GER	RINFO+RSERV	RINFO+RSERV	RINFO+RSERV	RSEG	
PSITR-009	Documentación de seguridad del sistema.	RSEG	RSEG						
PSITR-010	Política de seguridad.	CSI	CSI	GER	RSEG	CSI	CSI	CSI	
PSITR-011	Normativa de seguridad.	RSEG	RSEG	GER	RSEG	CSI	CSI	CSI	
PSITR-012	Procedimientos operativos de seguridad.	RSEG	RSEG	CSI	ASS	CSI	CSI	CSI	
PSITR-013	Estado de la seguridad del sistema.	ASS				ASS	RSEG	RSEG	
PSITR-014	Planes de mejora de la seguridad.	RSIS + RSEG	RSIS + RSEG	CSI + GER			CSI	RSEG	
PSITR-015	Planes de concienciación y formación.	RSEG	RSEG	CSI			CSI	RSEG	
PSITR-016	Planes de continuidad.	RSIS	RSIS	RSEG + GER	CSI	RSEG	CSI	CSI	RSIS
PSITR-017	Suspensión temporal del servicio	RSIS	RSIS						
PSITR-018	Ciclo de vida: especificación, arquitectura, desarrollo, operación y cambios.	RSIS + RSEG	RSIS	RSEG	RSIS		CSI	CSI	

7.2.2 Respuesta a incidentes de seguridad de la información

ID	Tarea	Principal
PSITI-001	Llevar a cabo el registro, contabilidad y gestión de los incidentes de seguridad en los Sistemas bajo su responsabilidad.	ASS
PSITI-002	Aislar el incidente para evitar la propagación a elementos ajenos a la situación de riesgo.	ASS
PSITI-003	Tomar decisiones a corto plazo si la información se ha visto comprometida de tal forma que pudiera tener consecuencias graves (estas actuaciones deberían estar procedimentadas para reducir el margen de discrecionalidad del ASS al mínimo número de casos).	ASS
PSITI-004	Asegurar la integridad de los elementos críticos del Sistema si se ha visto afectada la disponibilidad de estos (estas actuaciones deberían estar procedimentadas para reducir el margen de discrecionalidad del ASS al mínimo número de casos).	ASS
PSITI-005	Mantener y recuperar la información almacenada por el Sistema y sus servicios asociados.	ASS
PSITI-006	Investigar el incidente: Determinar el modo, los medios, los motivos y el origen del incidente.	ASS + RSEG
PSITI-007	Analizar y proponer salvaguardas que prevengan incidentes similares en el futuro.	RSEG
PSITI-008	Planificar la implantación de las salvaguardas en el sistema.	RSIS
PSITI-009	Aprobar el plan de mejora de la seguridad, con su dotación presupuestaria correspondiente.	CSI
PSITI-010	Coordinar y ejecutar el plan de seguridad aprobado.	RSIS

COMPROMISO DE LA DIRECCIÓN

NEO DIGITAL se compromete a:

- Establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información.
- Asegurar que esta política sea comunicada a todo el personal de NEO DIGITAL y a otras partes interesadas.
- Revisar periódicamente esta política para asegurar su adecuación y eficacia continua.
- Implementar un proceso de mejora continua para evaluar y ajustar la política y los controles de seguridad en respuesta a cambios en el entorno de la NEO DIGITAL, avances tecnológicos y lecciones aprendidas de incidentes de seguridad.
- Fomentar una cultura de seguridad de la información en toda la organización.
- Proporcionar formación y concienciación continua a todos los empleados sobre las mejoras prácticas en seguridad de la información y sus responsabilidades individuales en la protección de los activos de información de la NEO DIGITAL.
- Establecer procedimientos para la identificación, reporte, respuesta y recuperación ante incidentes de seguridad.
- Implementar y mantener un plan de continuidad del negocio y recuperación ante desastres que garantice la capacidad de la organización para continuar operando y recuperarse de interrupciones que puedan afectar la disponibilidad de los servicios y la información.

7.3 Responsabilidad

Todos los empleados y miembros de la organización serán responsables de las acciones que puedan realizar y de dar un uso correcto de los activos conforme a sus atribuciones profesionales, académicas y funciones dentro de la organización.

Independiente del concepto de uso responsable, se estima que la gestión de la seguridad de la información es responsabilidad específica de un conjunto de personas y comités con las funciones concretas, definidas y documentadas.

La organización se mantendrá con relaciones de cooperación en materia de seguridad informática con las autoridades competentes, proveedores de servicios de seguridad certificados y otras entidades comprometidas en promover la seguridad de sistemas de información.

Cada empleado es responsable de cumplir esta política y sus procedimientos según aplique a su puesto de trabajo. El no hacerlo puede resultar en una acción disciplinaria.

7.4 Roles definidos conforme al ENS

En base al Esquema Nacional de Seguridad (ENS) se definirán los siguientes roles fundamentales de seguridad de la información:

- **Responsable de Seguridad de la Información del ENS** (conocido también como Responsable de la Información) determinará los requisitos de seguridad de la información según lo establecido en el Esquema Nacional de Seguridad con el asesoramiento del Responsable de Seguridad. Tiene la responsabilidad última del uso que sea haga de la información y, por lo tanto, de su protección.

- **Responsable del Servicio del ENS** determinará los requisitos de seguridad de los servicios prestados según lo establecido en el Esquema Nacional de Seguridad, con el asesoramiento del Responsable de Seguridad y la opinión del Responsable del Sistema.
- **Responsable de Seguridad del ENS** coordinará las actuaciones globales, elaborará la planificación en materia de seguridad y supervisará que se han cumplido los objetivos fijados.
- **Responsable del Sistema de Información del ENS**, será quién esté encargado de las operaciones del sistema.

7.5 Incompatibilidades designadas

El Responsable de Seguridad (RSEG) es compatible con cualquier rol de responsable de la información, del servicio o responsable de sistema de información.

No podrá ser designada una persona para un rol cuando no tenga la experiencia demostrable y capacitación académica que le sea exigible para ese rol y funciones a desempeñar.

Según el informe 2018-0170 elaborado por la Agencia Española de Protección de datos: El DPD asesorará al responsable, tanto en las evaluaciones de impacto como en cualquier aspecto de las actividades de tratamiento que lleve a cabo. Pero en última instancia, será el RSEG quién tome las decisiones atendiendo, o no, al asesoramiento del DPD, pues es el responsable quien determina los fines y los medios, decidiendo el modo en el que van a ser tratados los datos.

Atendiendo a este informe y a las recomendaciones ISO/IEC 29151:2017, el rol de Delegado de Protección de Datos (DPD) definido en la organización no será compatible con el de Responsable de Seguridad, salvo la ausencia del rol y no pudiendo observar dicha separación por la dimensión de la organización. Por lo que esta decisión final, a pesar de la recomendación, recaerá en la Gerencia de la organización pero siempre documentando dicha

designación, haciendo constar los motivos por los que no se separan las funciones y las medidas que garantizan la independencia del delegado de protección de datos.

7.6 Procedimiento de designación

El Comité de Seguridad de la Información y los responsables serán designados por Gerencia siempre que no entren en conflicto con las incompatibilidades descritas en la política de seguridad.

Estos nombramientos serán revisados por Gerencia, siempre que lo considere oportuno, cuando un puesto quede vacante, un rol quede sin asignación (sin necesidad de baja en la empresa) o cada tres años de forma periódica.

7.7 Comité de Seguridad de la Información

Según se estipula el Comité de Seguridad de la Información (CSI) coordinará la seguridad de la información a nivel de la organización atendiendo a:

- La coordinación es necesaria para racionalizar el gasto.
- Evitar disfunciones que puedan ocasionar fallos de seguridad, accidentes o ataques.
- Cumplir con las normativas establecidas.
- Asesorar y atender inquietudes en materia de Seguridad de la Información, a todos los miembros de la organización, siempre y cuando le sea requerido.
- Resolver los conflictos de responsabilidad que puedan aparecer, de forma puntual, entre diferentes responsables y/o diferentes áreas o departamentos de la organización, elevando a Gerencia aquellos casos en los que no tenga suficiente autoridad para decidir.
- Recoger las funciones y obligaciones de los Responsables de la Información y los Servicios ENS, en aquellas acciones transversales, en las que le sea solicitado y/o se considere necesario.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información.

Al CSI se le reconocen las siguientes funciones:

- Atender las inquietudes de la Gerencia y de los diferentes departamentos o áreas.
- Informar regularmente del estado de la seguridad de la información a la Gerencia.
- Velar por que la Seguridad de la Información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación atendiendo a "Privacidad por Diseño".
- Velar por la creación y utilización de servicios que reduzcan duplicidades y unifiquen un funcionamiento homogenéo en todos los sistemas TIC.
- Promover la mejora continua del sistema de gestión de la seguridad de la información
- Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por la Gerencia.
- Aprobar la normativa de seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
-

- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de la organización. En particular velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Divulgación de la normativa y política de seguridad de la Empresa.
- Desarrollo del procedimiento de designación de roles y responsabilidades.
- Supervisión y aprobación de las tareas de seguimiento de:
    - Tareas de adecuación
    - Análisis de Riesgos.
    - Auditoría bienal.
- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas TI en su ámbito de responsabilidad.
- Realizar o promover las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Promover la formación y concienciación del Servicio de Informática dentro de su ámbito de responsabilidad.

- Coordinar con los distintos responsables que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y los servicios prestados.

- Analizar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
- Aprobación de los procedimientos de seguridad elaborados por el Responsable del sistema.

7.8 Responsable de los servicios de información

La organización designa las siguientes funciones para el Responsable de los servicios de información:

- Tiene la potestad de establecer los requisitos de una información en materia de seguridad.
- Establecimiento y aprobación de los requisitos de los servicios e información TI en materia de seguridad.
- Aceptación del riesgo residual.
- Determinación de los niveles de seguridad requeridos en cada dimensión.

- Trabajo en colaboración con el Comité de Seguridad de la Información.

7.9 Responsable del servicio

El Responsable de los servicios de información tendrá las siguientes funciones reconocidas:

- Tiene la potestad de establecer los requisitos de una información en materia de seguridad.
- Establecimiento y aprobación de los requisitos de los servicios.
- Aceptación del riesgo residual.
- Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, se puede recabar una propuesta al Responsable de la Seguridad y conviene que se escuche la opinión del Responsable del Sistema.
- Trabajo en colaboración con el Comité de Seguridad de la Información.

7.10 Responsable de la seguridad de la información

La organización designa las siguientes funciones para el Responsable de la Seguridad de la Información:

- Determinación de la categoría del sistema.
- Declaración de aplicabilidad.
- Medidas de seguridad adicionales.
- Elaborar Configuración de seguridad.
- Documentación de seguridad del sistema.
- Elaboración Normativa de seguridad.
- Aprobar los Procedimientos operativos de seguridad.
- Reportar el Estado de la seguridad del sistema.

- Elaborar Planes de mejora de la seguridad.

- Elaborar Planes de concienciación y formación.

- Elaborar Planes de continuidad.
- Aprobar Ciclo de vida: especificación, arquitectura, desarrollo, operación y cambios.

7.11 Responsable del Sistema

El Responsable del Sistema tendrá las siguientes funciones:

- Desarrollar, operar y mantener el sistema durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y política de gestión del sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Definir la política de conexión o desconexión de equipos y nuevas personas usuarias en el sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del sistema.
- Decidir las medidas de seguridad que aplicarán los suministradores de componentes del sistema durante las etapas de desarrollo, instalación y prueba del mismo.
- Implantar y controlar las medidas específicas de seguridad del sistema y cerciorarse de que estas se integren adecuadamente dentro del marco general de seguridad.
- Determinar la configuración autorizada de hardware y software a utilizar en el sistema.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.

- Llevar a cabo el preceptivo proceso de análisis y gestión de riesgos en el sistema.
- Determinar la categoría del sistema realizando la evaluación de riesgos, evaluando las amenazas y los riesgos a los que puede estar expuesto y determinar las medidas de seguridad que deben aplicarse para eliminación, mitigación y/o asumir estos riesgos.

- Elaborar y aprobar la documentación de seguridad del sistema.
- Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del sistema.
- Investigar los incidentes de seguridad que afecten al sistema, y en su caso, comunicación a la persona responsable de seguridad o a quien está determine.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Además, la persona responsable del sistema puede acordar la suspensión del manejo de una cierta 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 debe ser acordada con las personas responsables de la información afectada, el servicio afectado y la persona responsable de seguridad, antes de ser ejecutada.
- Elaboración Planes de mejora de la seguridad y Planes de Continuidad.
- Suspensión temporal del Servicio.
- Elaborar el Ciclo de vida: especificación, arquitectura, desarrollo, operación y cambios.
- Planificar la implantación de las salvaguardas en el sistema.
- Ejecutar el plan de seguridad aprobado.
- Elaboración de los procedimientos de seguridad necesarios para la operativa en el sistema.

7.13 Responsable de la Seguridad del Sistema

El rol de Responsable de la Seguridad del Sistema contemplará las siguientes funciones:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.
- Ejecutar el plan de seguridad aprobado.

- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- La aplicación de los Procedimientos Operativos de Seguridad.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Monitorizar que los procedimientos aprobados son aplicados para gestionar el sistema de información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- Informar a los Responsables de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.

- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.
- Llevar a cabo el registro, contabilidad y gestión de los incidentes de seguridad en los Sistemas bajo su responsabilidad
- Tomar decisiones a corto plazo si la información se ha visto comprometida de tal forma que pudiera tener consecuencias graves (estas actuaciones deberían estar procedimentadas para reducir el margen de discrecionalidad del ASS al mínimo número de casos).
- Aislar el incidente para evitar la propagación a elementos ajenos a la situación de riesgo.
- Asegurar la integridad de los elementos críticos del Sistema si se ha visto afectada la disponibilidad de estos (estas actuaciones deberían estar procedimentadas para reducir el margen de discrecionalidad del ASS al mínimo número de casos).
- Investigar el incidente: Determinar el modo, los medios, los motivos y el origen del incidente.
- Mantener y recuperar la información almacenada por el Sistema y sus servicios asociados.

7. Tratamiento de datos personales

Neo Digital Solutions gestiona datos de carácter personal. El Registro de Actividades de Tratamiento está únicamente a disposición de las personas autorizadas y recogerá los ficheros afectados y los responsables designados correspondientes.
Todos los sistemas de información de la organización se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos para su tratamiento. Estas disposiciones están documentadas en el documento de uso interno NDS_GES_D031.

8. Gestión de riesgos

Todos los sistemas de información en los que esta política sea aplicable dispondrán de su correspondiente análisis de riesgos, evaluación de amenazas y riegos a los que están expuestos.

Se volverá analizar cuando se produzcan estas circunstancias:

- Cuando cambie la información tratada o gestionada.
- Cuando cambien los servicios prestados.
- Cuando ocurra una incidencia grave de seguridad.
- Cuando se informe de vulnerabilidades graves.
- Periódicamente cada año.

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

9. Desarrollo de normativa de seguridad

Se definirán directrices para la estructuración de la documentación de seguridad del sistema, su gestión y su acceso.

Neo Digital Solutions ha determinado que realizará una política de directrices por niveles.

El primer nivel estará constituido por la Política de Seguridad, seguido por las normas internas y un tercer nivel de procedimientos internos.

Las normas indicarán que debe o no debe hacerse, mientras que los procedimientos indicarán cómo debe hacerse.

Para cada nivel de indicará quién debe elaborarlos, aprobarlos, modificarlos y acceder a ellos.

10.1 Política de seguridad de la información

Responsable SI

10.2 Procedimientos y procesos de seguridad

Responsable SI

10.3 Instrucciones técnicas de seguridad

Responsable SI

10. Obligaciones de empleados y asociados

Todos los miembros de Neo Digital Solutions, con independencia de su afiliación, contrato o empresa de pertenencia, tienen la obligación de conocer y cumplir esta política de seguridad de la información.

Esta obligación se extiende a toda la documentación que se desarrolla en la medida que les afecte.

Será responsabilidad del Comité de Seguridad de la Información disponer de los medios necesarios para que la información les llegue.

Todos los miembros de la organización deberán atender a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Las personas con responsabilidad en el uso, operación o administración de sistemas de información recibirán formación complementaria para el uso seguro de los sistemas en medida en que la necesiten para realizar su trabajo.

La organización se reserva el derecho de forzar sesiones de formación generales o específicas, de carácter obligatorio, en base a vulneraciones de políticas por parte de uno o más miembros, con independencia de la asistencia o no de las sesiones anteriormente descritas.

Neo Digital Solutions sancionará disciplinariamente a aquellos miembros que incumplan la normativa de seguridad de la información, la normativa protección de datos, las normativas internas específicas y protocolos establecidos.

11. Terceras partes

Cuando Neo Digital Solutions preste servicios a otras entidades o maneje información de otros organismos, se les hará partícipe de esta política de seguridad de información junto con las normativas asociadas. Se establecerán canales para el reporte y la coordinación de los respectivos Comités de Seguridad de Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando Neo Digital Solutions reciba servicios prestados por proveedores, les hará participe de esta política y normativas de seguridad asociadas que ataña a esos servicios o información.

Los proveedores estarán sujetos a las mismas obligaciones establecidas en esta política, pudiendo desarrollar sus propios procedimientos operativos siempre que la satisfagan.

En el caso de que no se pueda conciliar o satisfacer algún aspecto de esta política de seguridad, se requerirá un informe del Responsable de Seguridad (ENS) que precise los riegos en los que incurre y la forma de tratarlos. No se admitirán excepciones sin la aprobación del informe por parte de los Responsables de Información y Servicios afectados antes de continuar. Cualquier medida aplicada se considerará de carácter temporal hasta que la política pueda satisfacerse al completo.

13. Acuerdos de confidencialidad