Política de Seguridad de la Información

Autores: Área Estrategia Normativa, Revisores: CSI, Aprobación: Rep. Dir.

Última Revisión **11/08/2025**
Versión: 2.4
Fecha Versión: 11/08/2025
Confidencial: Clientes, Proveedores y Uso Interno

Introducción

La presente Política de Seguridad de la Información se adhiere al plan estratégico de NEURONET S.A. y establece los lineamientos para la implementación, operación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) de la organización, basado en la norma internacional ISO/IEC 27001:2022.

La Política de Seguridad de Información de NEURONET S.A. expresa los lineamientos generales y estratégicos respecto al buen uso de los activos de información, refiriéndose además a la gestión preventiva y reactiva de aquellos riesgos y eventos que puedan comprometer la confidencialidad, integridad y disponibilidad de la información, fijando las directrices en concordancia con los objetivos estratégicos, leyes y regulaciones vigentes.

Objetivo

La política general de la seguridad de la información tiene como objetivo establecer el lineamiento institucional de NEURONET referente a la responsabilidad, resguardo y gestión de riesgos de la información, como también entregar las directrices generales sobre el acceso, manipulación, procesamiento, transmisión, protección, almacenamiento o cualquier otro tratamiento que se realice sobre los activos de información y los centros de tratamiento de estos, garantizando el cumplimiento de requisitos legales, regulatorios y contractuales aplicables.

La organización ha definido así, los siguientes objetivos de seguridad específicos:

- Establecer para todos los colaboradores de la organización las expectativas de la Dirección respecto al correcto uso de los recursos de información, así como las medidas que deben adoptarse para la protección de estos, desalentando conductas riesgosas, ilícitas o que amenacen el sistema de seguridad de la información.
- Capacitar y brindar herramientas a los colaboradores de Neuronet orientadas a promover hábitos o conductas para la correcta protección de los datos y activos de la organización, promoviendo la comprensión de sus responsabilidades individuales.

- Prevenir la materialización de incidentes de Seguridad de la Información a través de la implementación de medidas de protección apropiadas respecto a las amenazas que podrían afectar la confidencialidad, integridad o disponibilidad de la información.
- Velar por la continuidad operativa de los servicios que Neuronet disponibiliza a sus clientes, así como de aquellos que utiliza en sus operaciones internas.
- Promover una cultura de mejora continua, orientada al resguardo de la información y de los activos de Neuronet

Alcance

Esta política de seguridad de la información aplica a todos los activos de información, procesos, personas, tecnologías, infraestructuras y terceros vinculados al funcionamiento y prestación de servicios de NEURONET, independientemente del soporte físico o lógico y del lugar donde estén localizados.

Por tanto, es responsabilidad de todos los colaboradores de NEURONET, además, de los proveedores y clientes, cuando corresponda, conocer, cumplir y hacer cumplir cabalmente las disposiciones de esta Política. El cumplimiento y compromiso con estas regulaciones de seguridad deberán expresarse en los contratos, convenios y/o acuerdos respectivos de servicio.

La gestión de la seguridad de la información se realizará mediante un proceso sistemático, documentado y conocido por toda la organización basándose en metodologías de mejoramiento continuo. Este proceso de gestión deberá ser aplicado a todos los procesos y ámbitos de la organización.

Compromiso de la Dirección

La Dirección de NEURONET, consciente de la importancia del tratamiento adecuado sobre los datos e información de sus clientes, así como la propia, ha implementado como parte de su proceso de maduración, innovación y actualización, la Norma Ch. ISO/IEC 27.001 de Seguridad de la Información, reafirmando el compromiso de la organización con sus clientes.

De esta forma, la dirección asegura su compromiso con el Sistema de Gestión de Seguridad de la Información a través de las siguientes acciones:

- Aprobar la Política y proporcionar los recursos humanos, financieros y tecnológicos necesarios para alcanzar los objetivos de seguridad de la información..
- Designar y apoyar a un Representante de la Dirección del SGSI y/o Responsable de Seguridad de la Información (CISO o función equivalente).
- Evaluar los riesgos en decisiones estratégicas e incluir la seguridad de la información en la gobernanza corporativa.
- Solicitar revisiones periódicas (al menos anualmente) del SGSI y de la Política de Seguridad de la Información.

Responsabilidades y Cumplimiento

Las responsabilidades definidas para la Política son las siguientes:

1. **Gerencia General:** Es el responsable de la promoción y el apoyo para el desarrollo, implementación y seguimiento de la Política de Seguridad.
2. **Representante de la Dirección del SGSI (RD-SGSI):** Punto de contacto entre la Dirección y el SGSI; responsable del mantenimiento del SGSI y de presentar informes a la Dirección.
3. **Área de Estrategia Normativa:** Responsable del desarrollo, adecuación y armonización de la Política de Seguridad de la Información.
4. **Comité Seguridad Información (CSI):** Responsable de validar la presente política, así como de velar por el fiel cumplimiento de esta.
5. **Personal de la organización:** Conocer, entender y dar cumplimiento cabal a esta política de carácter obligatorio. Además, tiene la obligación de alertar de manera oportuna y adecuada, según lo determine la "Política de Gestión de Incidentes", cualquier incidente que atente contra la seguridad de la información

Vigencia y Evaluación de la Política

La presente Política General de Seguridad de la Información entrará en vigencia una vez oficializada por el o la Representante de la Dirección SGSI.

Asimismo, esta será evaluada por el Comité de Seguridad de la Información una vez al año, o bien, cuando se produzca un cambio significativo que la impacte, esto con la finalidad de asegurar la continua idoneidad, eficiencia y efectividad de la política.

Difusión de la Política

La difusión de esta política se realizará mediante publicación en Microsoft Teams o correo electrónico a todo el personal de la organización y proveedores de servicios, además su versión digitalizada quedará publicada y a disposición de sus partes interesadas, a través del Sitio Web público de Neuronet y en su espacio de WIKI interna para facilitar su acceso y conocimiento.

La presente política está alineada con las directrices de las leyes y regulaciones existentes. Cualquier conflicto con estas regulaciones debe ser informado inmediatamente al Comité de Seguridad de la Información.

Política

Cumplimiento Legal y Normativo

La Política de Seguridad de la Información y las subsecuentes políticas de seguridad, deberán mantener un lineamiento acorde a las directrices definidas por la organización, basadas en el estándar de la Nch. ISO/IEC 27.001, siempre considerando el marco constitucional y legislativo vigente, particularmente en lo referido a leyes relacionadas a la propiedad intelectual, el manejo de datos personales, los documentos electrónicos y la firma digital, los delitos penales asociados a la tecnología y los sistemas de información, o sobre las comunicaciones y su privacidad, y, otras leyes aplicables al campo de la información y la tecnología.

Resguardo sobre los activos de Información

Se declara que sobre todos los activos de información que la organización administre, utilice o posea, deberán implementarse los mecanismos y controles de seguridad necesarios para resguardar la confidencialidad, integridad y disponibilidad de la información, permitiendo minimizar los riesgos inherentes a los cuales por su naturaleza puedan verse expuestos.

Organización de la Seguridad

NEURONET mantendrá una adecuada organización relacionada a la seguridad de la información, para lo cual gestionará a través de un Comité de Seguridad de la Información y/o el Representante de la Dirección, normativas, estándares, procedimientos o cualquier otro mecanismo de control que ayuden a mejorar el SGSI de la organización.

Gestión de Activos de Información

Con el objetivo de lograr una gestión de activos de información más eficiente, la organización establece métodos para la identificación, clasificación y valorización de los activos de información, considerando también la asignación de responsabilidades sobre su tratamiento, permitiendo mantener claramente identificación sobre los activos de información relevante para la Institución y mantener mecanismos acordes para el control de los riesgos de información

Gestión de la Seguridad del personal

Considerando la importancia e influencia de los colaboradores de la organización para el SGSI, NEURONET incorpora los conceptos de seguridad de la información dentro de los procesos y etapas de gestión del personal. Incorporando términos legales de confidencialidad y responsabilidades de seguridad en documentos como contratos y descripciones de cargos vigentes.

Adicionalmente, la organización desarrollará planes de sensibilización orientados a generar cultura de seguridad en los colaboradores que se permee en todas las actividades que estos realicen.

Seguridad Física y Ambiental

Para un adecuado resguardo del acceso físico a las dependencias de la organización, sus centros de almacenamiento o procesamiento de datos. NEURONET mantendrá normativas, controles y otros mecanismos que resguarden la seguridad de dichas instalaciones y ambientes de trabajo junto con toda la información que en ellas se contiene, permitiendo garantizar la protección de los activos de información frente a amenazas físicas, ambientales y naturales

Seguridad en las Comunicaciones y Operaciones

Para todo activo de información que se manipule dentro de la organización, se deberán considerar los riesgos inherentes asociados a los medios en que se transporta o comunica, sean estos físicos o digitales, contemplando así los controles pertinentes que deben ser adoptados para entregar un grado razonable de resguardo a los activos de información y lograr un cumplimiento adecuado de esta política de seguridad.

Siempre que las partes internas o externas que deban acceder a datos de la organización, al igual que ésta al acceder a información de clientes, deberá formalizarse el compromiso entre las partes con respecto a la seguridad de la información a través del refrendo de un “Acuerdo de Confidencialidad y Seguridad de la

Información" que aborde los conceptos de disponibilidad, confidencialidad e integridad de la información a la que se accede.

Seguridad en el Acceso a la Información

Neuronet, en aras de garantizar una correcta gestión sobre los accesos a los activos de información, es que ha definido que para todo activo se debe identificar su nivel de acceso, esto es, quienes pueden acceder a él y con qué permisos (lectura o escritura), abordando así los conceptos de confidencialidad e integridad de la información; ejecutando las medidas de control adecuadas para mantener el resguardo de la información y así evitar un acceso o manipulación no autorizada.

Seguridad en la Adquisición, Desarrollo y Mantención de Sistemas de Información

Para todos los sistemas a implementar en la organización, sean estos, ejecutados de manera interna, adquiridos en el mercado o desarrollados por terceros mandatados por Neuronet se deberán considerar los riesgos y/o implicancias de su puesta en marcha dentro de la empresa con respecto al sistema de gestión de seguridad de la información, entendiendo que cualquier proyecto implementado en la organización también incorpora riesgos que son propios de estos, por esto NEURONET ha definido mecanismos y controles que permitan mitigar o reducir estos riesgos utilizando procesos formales para la construcción de sistemas, implementación de controles criptográficos, como también actividades de aseguramiento de software.

Asimismo, los sistemas de información que se encuentran en producción deberán utilizar medidas de seguridad y controles que protejan la información que en ellos se procesa y resguarde del acceso o utilización no autorizada a esta.

Relación con proveedores

En las relaciones de la organización con sus proveedores, se deberán considerar requerimientos que permitan identificar los riesgos derivados de la externalización o adquisición de servicios y/o productos y los controles dispuestos para mitigarlos. Se deberán establecer de este modo, los mecanismos de control para el manejo adecuado de la información con proveedores estratégicos. Lo anterior en concordancia con los procesos de selección, evaluación y reevaluación de proveedores.

Gestión de Incidentes de Seguridad

Con el objetivo de gestionar y prevenir los incidentes de seguridad de la información a los que se vea expuesta la organización, y la posible recurrencia de estos, NEURONET ha conformado un equipo de respuesta a incidentes de seguridad de la información, cuyas principales funciones están orientadas a realizar los mantenimientos adecuados sobre los activos de la organización, apoyando en la sensibilización de los colaboradores y adoptando los controles de seguridad más pertinentes para la organización.

Gestión de la Continuidad de Negocio

NEURONET velará por generar las condiciones necesarias que garanticen la disponibilidad y pronta recuperación de su infraestructura, tecnología, procesos, personas u otros activos de información que soporten la entrega de los servicios a clientes internos y externos, a través de la incorporación de estrategias y planes de recuperación, así como la gestión de copias de seguridad; lo anterior con la finalidad de garantizar en una medida razonable la operación de la organización.

Cumplimiento

NEURONET se compromete con facilitar los recursos necesarios para dar cumplimiento a toda la legislación y regulación aplicable a su actividad en materia de seguridad de la información y establecer la responsabilidad de dicho cumplimiento sobre todos sus miembros. En este sentido, se velará por el cumplimiento de toda legislación, normativa o regulación aplicable.

Gestión de Excepciones

En la necesidad de dar pronta solución a procesos de negocio de la organización de carácter urgente, que conlleven una desviación o incumplimiento a controles de seguridad, procesos, procedimientos, políticas u otros definidos por la organización, se deberá cumplir con el "*Procedimiento de Excepciones*".

Estas excepciones serán analizadas para evaluar los riesgos que podrían introducir a la organización y, en base a la identificación de estos, declarar las medidas que pueden adoptarse para mitigarlos si fuera posible antes (corrección) y después (acción correctiva) de autorizada la excepción, estos riesgos deberán ser aceptados por la gerencia general de la organización.

Auditoría y revisión independiente

Se realizarán auditorías internas periódicas (al menos anuales) del SGSI y revisiones independientes según el plan de auditoría. El CSI y la Dirección revisarán los resultados y los planes de acción derivados.

Documentos relacionados

El presente documento constituye una política de alto nivel, destinada a normar los aspectos más relevantes y generales de la gestión de seguridad de la información; adicionalmente, la Dirección promulgará documentos adicionales que explicitan en mayor detalle las medidas de seguridad de alto nivel dispuestas en esta política.

- Norma Ch. ISO/IEC 27001:2022
- Estamento de Aplicabilidad (SoA)

Control de Versiones

Versión N°	FECHA	DESCRIPCIÓN DEL CAMBIO
1.0	28/08/2020	Creación del Documento
1.1	23/07/2021	Añade aspectos relacionados a la Mejora Continua Añade términos al glosario
1.2	28/07/2021	En responsabilidades y cumplimiento añade referencia a anexo de contrato de seguridad de la información

Versión N°	FECHA	DESCRIPCIÓN DEL CAMBIO
2.0	11/04/2022	Cambio de formato, títulos y contenido
2.1	02/08/2022	Amplia exigibilidad a todos los requisitos aplicables en el apartado 4
2.2	07/06/2024	Ajusta política a versión ISO 27001:2022
2.3	08/08/2024	Actualiza difusión de la política
2.4	11/08/2025	Añade auditoría y realiza cambios de redacción en algunos puntos de política

Anexo I - Definiciones

Definiciones de la Política de Seguridad de la Información

Fundamental es integrar la presente Política en la cultura organizacional, la existencia de un plan de difusión y sensibilización en torno a la seguridad de la información cada vez toma mayor relevancia.

- **Información:** Es un activo que, como otros activos comerciales importantes, es primordial para la actividad de una organización y, en consecuencia, es necesario protegerse la manera adecuada. La información se puede almacenar en muchas formas, incluyendo: en forma digital, en forma material, así como la información no representada en forma de conocimiento de los trabajadores. La información se puede transmitir en diversos medios.
- **Seguridad de Información*:** Preservación de la confidencialidad, integridad y disponibilidad de la información (adicionalmente, puede involucrar otras propiedades como: autenticidad, responsabilidad, no repudio y fiabilidad)
- **Confidencialidad*:** Propiedad de la información que no esté disponible o sea divulgada a individuos, entes o procesos no autorizados.
- **Integridad*:** Propiedad de precisión y completitud.
- **Disponibilidad*:** Propiedad que consiste en ser accesible y usable cuando sea requerido por un ente autorizado.
- **Evento*:** Ocurrencia o cambio de una serie de circunstancias particulares (un evento puede ser una o más ocurrencias y tener varias causas, un evento tambien puede ser algo que no esté ocurriendo y un evento tambien puede ser referido como un "incidente" o "accidente")
- **Incidente de Seguridad*:** Un evento o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información
- **Sistema de información*:** Activos de aplicación, servicio, tecnología de la información, u otros componentes de manipulación de la información.

- **Activo de Información:** Todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la Compañía.
  Se pueden distinguir tres tipos de activos:
  1. La información en sus múltiples formatos.
  2. Los equipos y Sistemas que la soportan.
  3. Los usuarios que la utilizan en sus diferentes funciones.

(*) Definición según ISO/IEC 27000:2018