POLITICA DE SEGURIDAD DE LA INFORMACION

1. Introducción

NEONLINE SAC, se compromete a desarrollar e implantar las máximas capacidades en materia de seguridad de la información, con el fin de reducir las amenazas para la información, los Sistemas de Redes y de Información utilizados en la organización. Para ello hemos aprobado la presente *Política de Seguridad de la Información,* que constituye la pieza angular del Sistema de Gestión de Seguridad de la Información de NEONLINE.

2. Objeto

El objetivo del presente documento es establecer las políticas de seguridad de la información dentro de los diferentes procesos del NEONLINE para proteger la confidencialidad, disponibilidad e integridad de la información, recursos, servicios e instalaciones.

3. Alcance

Las disposiciones contenidas en el presente documento establecen los lineamientos fundamentales que servirán de base para el desarrollo e implementación del futuro Sistema de Gestión de Seguridad de la Información (SGSI) de NEONLINE. Asimismo, son de cumplimiento obligatorio para los colaboradores, proveedores, terceros y demás partes interesadas.

4. Base Legal

- Ley N° 27933 de Protección de Datos Personales
- Norma ISO 27001
- Política Nacional de Ciberseguridad

5. Definiciones

Activo: Es todo aquello presenta valor para la entidad.

Activos de Información: Cualquier información o recurso relacionado con el tratamiento de la misma que tenga valor para la organización y que se requiera ser protegida adecuadamente, se considera tipos de activos de información a la información generada por la entidad, software, equipos y ambientes físicos, personas y servicios.

Amenazas: Es una causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Gobierno Digital: Es un cambio fundamental en la forma en que los gobiernos del mundo están adoptando su misión, aprovechando el poder de las tecnologías de la información y las comunicaciones en forma realmente transformadoras.

Información: Conjunto organizado de datos, procesados y generados por los sistemas de información de la entidad, se considera un activo principal que, tiene un valor esencial para la institución y requiere en consecuencia una protección

adecuada.

Información generada por la empresa: son de tipo i) electrónica; ii) impresa; iii) electrónica e impresa.

Incidente: Es cualquier evento o situación que representa una amenaza para la confidencialidad, integridad o disponibilidad de los activos de la información.

Oficial de Seguridad y Confianza Digital: Responsable de impulsar la implementación de la presente política.

Propietario de la información: Es cualquier persona, Órgano o Unidad Orgánica que tiene la responsabilidad de custodiar y asegurar un activo de información, así como de preservar la integridad, confidencialidad y disponibilidad de la información de la entidad.

Recurso informático: Son los equipos de cómputo, sistemas de información, licencias de software, aplicativos informáticos, equipos de procesamiento y telecomunicaciones, los mismos que son necesarios para el buen funcionamiento y mantienen la continuidad operativa de la entidad.

Riesgo: Se refiere a la probabilidad de que una amenaza explote una vulnerabilidad específica y cause un impacto negativo en los activos de información de una organización.

Seguridad de la Información: Se puede definir como la protección de la integridad, confidencialidad y disponibilidad de los activos de información, según sean necesarios para alcanzar los objetivos de negocio de la entidad.

Sistema de Gestión de Seguridad de la Información: Basada en un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información en una organización.

Transformación Digital: Es la integración o incorporación de tecnologías digitales en todas las áreas de una empresa o entidad, generando un cambio en el modo de trabajo, que a su vez generan un valor en los productos o servicios que brindan.

Vulnerabilidad: Es una debilidad o fallo de un activo de información que puede ser explotada por una o más amenazas para comprometer la seguridad de la organización.

6. Requisitos básicos de seguridad de la información

Para llevar a cabo la gestión diaria de la seguridad, se procederá siempre conforme a los siguientes requisitos básicos:

- Establecer requerimientos de seguridad desde el diseño y por defecto.
- Prevención, detección, respuesta y conservación.
- Vigilancia continuada y reevaluación periódica.
- Diferenciación de responsabilidades.
- Organización e implantación del proceso de seguridad.
- Análisis y gestión de los Riesgos.
- Gestión del personal.
- Autorización y control de los accesos.
- Protección de las instalaciones.

- Adquisición de productos de seguridad y contratación de servicios de seguridad.
- Mínimo privilegio.
- Integridad y actualización del Sistema de Información.
- Protección de la Información almacenada y en tránsito.
- Prevención ante otros sistemas de Información interconectados.
- Registro de la actividad y detección de código dañino.
- Incidentes de seguridad.
- Continuidad de la actividad.
- Mejora continua del proceso de seguridad.
- Seguridad en la cadena de suministro.
- Confiabilidad, seguridad y resiliencia.

Cada uno de estos requisitos se desarrollará por los correspondientes procedimientos y/o políticas específicas aprobadas internamente.

Toda la documentación de seguridad de la información que se desarrolle en ejecución de los mencionados principios y que integra el SGSI, se gestiona, estructura y conserva conforme a los procedimientos documentados que NEONLINE ha desarrollado teniendo en cuenta la normativa, así como los estándares nacionales e internacionales que apliquen en cada caso.

7. Declaración de la Política de Seguridad de la Información

NEONLINE reconoce que, la información que genera, procesa y distribuye es un activo vital y por ello se compromete a:

• Implantar mecanismos para preservar y asegurar la confidencialidad, disponibilidad e integridad de los activos de información relevantes para la NEONLINE y partes involucrados según corresponda, buscando siempre la eficiencia dentro de un entorno de mejora continua, a fin de garantizar su seguridad permanente.

• Asegurar mediante la adquisición de bienes y/o servicios los activos de información de la NEONLINE según la importancia y valor.

• Establecer controles para garantizar que solo las personas autorizadas tengan acceso a los activos de información y determinar responsabilidad a nivel de los usuarios como propietarios de la información.

• Establecer, implementar, operar, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información – SGSI bajo la NTP-ISO/IEC 27001:2022, garantizando su continuidad y cumplimiento.

• Garantizar el aprovisionamiento de los recursos requeridos para establecer, implementar, operar monitorear, revisar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información de NEONLINE.

• Gestionar de manera oportuna las vulnerabilidades e incidentes de seguridad de la información, y tomar las acciones preventivas y/o correctivas correspondientes para evitar su

recurrencia.

- Evaluar los riesgos asociados con la seguridad de la información, aplicando medidas para reducir el impacto y monitorear continuamente para mantener un nivel aceptable de riesgo.
- Velar por el cumplimiento de la legislación y normatividad vigente relacionadas con la seguridad de la información.
- Realizar la comunicación oportuna de la normativa interna relacionada con la Seguridad de la Información, asegurando que sea comprendida y se encuentre disponible para todos los interesados.
- Concientizar al personal de NEONLINE sobre la importancia de la Seguridad de la Información, estableciendo como meta el fortalecimiento de los valores y compromiso del mismo a fin de velar por el cumplimiento de la presente política.
- Realizar evaluaciones periódicas de los sistemas de información que gestiona o administra NEONLINE para identificar vulnerabilidades y áreas de mejora, y tomar medidas correctivas según sea necesario.

8. Sanciones

El incumplimiento de las disposiciones contenidas en la presente Política, tendrá como resultado la aplicación de medidas correctivas y de mejora necesarias. En caso se encontrará responsabilidad en un personal involucrado en el alcance, se dará inicio a las acciones legales que la ley faculte.

9. Revisiones

Será obligatorio la revisión anual de la presente política, sin embargo será actualizada periódicamente para adaptarse a las necesidades y/o cambios regulatorios, organizativos, técnicos y de procesos de NEONLINE, así como para incorporar las mejores prácticas identificadas en el SGSI.

La modificación y/o actualización de la presente Política será aprobada por el Oficial de Seguridad y Confianza Digital

10. Difusión de la Política

La comunicación de la Política se efectuará empleando disposiciones legales y medios dispuestos por NEONLINE, con la finalidad de garantizar su accesibilidad a todo el personal.

Oficial de Seguridad y Confianza Digital