POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Clasificación: Uso Interno

Autor		Revisión		Aprobación	
Nombre	**Nassim Hamer**	**Nombres**	**Comité de Seguridad de la información y Riesgos**	**Nombre**	**Hernan Moller**
Cargo	CISO	**Área**	N/A	**Cargo**	Alta Direccion
Fecha	05-05-2020	**Fecha**	07-05-2020	**Fecha**	07-05-2020

CONTROL DE CAMBIOS				
VERSIÓN	**FECHA**	**RESUMEN DE MODIFICACIONES**	**ELABOORADO POR:**	**APROBADO POR:**
1.0	07-05-2020	Entrega primera versión del documento.	Hernán M.	Fernando L.
1.1	05-07-2021	Segunda versión con modificaciones por auditoría.	Hernán M.	Fernando L.
2.0	09-01-2023	Revisión anual	Hernán M.	Fernando L.
3.0	22-04-2024	Revisión anual: Inclusión de cláusulas	CISO	Alta Dirección
3.0	25-10-2024	Revisión anual - revisión por la Dirección	CISO	Alta Dirección

NOTA: La presente versión sustituye completamente a todas las precedentes, de manera que este sea el único documento válido entre todos los de la serie.

Tabla de Contenido

1. Introducción

NIVEL4 en su misión de velar por la protección de la información de sus clientes y activos corporativos, define la información cómo un activo estratégico clave, la cual debe ser correctamente gestionada y protegida, por este motivo, se establece la siguiente política que busca regular el manejo de la información y las medidas que resguarden la confidencialidad, integridad y disponibilidad de la información.

Además de controlar el acceso a la información en conformidad con la constitución, las leyes, y demás normas jurídicas, asegurando la continuidad operacional de los servicios estratégicos.

2. Marco de Referencia

- Norma ISO 27001:2022
- Norma ISO 27002:2022
- Políticas y Procedimientos del SGSI

3. Definiciones

La presente Política de Seguridad entrega las directrices respecto de la forma en que se debe implementar la seguridad de la Información conforme a las normativas vigentes.

- ***Seguridad de la información***: Conjunto de prácticas y medidas destinadas a proteger la confidencialidad, integridad y disponibilidad de la información. Esto implica proteger los datos contra accesos no autorizados, alteraciones, pérdidas o daños, tanto en formato digital como físico. Incluye controles técnicos, como el cifrado y las contraseñas;

procedimientos organizativos, como políticas y auditorías; y la concienciación del personal para garantizar que la información se maneje de manera segura.

- ***Información*:** Conjunto de datos organizados en poder de una entidad que poseen valor para la misma.

- **Activo de información**: todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para NIVEL4. En este sentido, podemos distinguir 3 tipos de activos:

    - La Información propiamente tal, en sus múltiples formatos (papel o digital, texto, imagen, audio, video, otros.)

    - Los equipos, sistemas u otros medios que se consideren.

    - Las personas que la utilizan.

- ***NDA (Non Disclosure Agreement):*** Acuerdo de Confidencialidad, es un contrato legal de al menos 2 partes, el cual describe material, conocimiento o información confidencial que las partes desean compartir entre sí para ciertos fines, pero requieren restringir el acceso a terceros.

- **Protección de Datos Personales:** Conjunto de principios que los responsables y encargados del tratamiento deben considerar al tratar datos personales. Se trata del control de la propia información frente a su tratamiento automatizado o no, es decir, no solo a aquella información albergada en sistemas computacionales, sino en cualquier soporte que permita su utilización: almacenamiento, organización y acceso.

4. Principios de Seguridad de la información

El Sistema de Gestión de Seguridad de la Información – SGSI establecerá distintos controles a nivel de gestión, con el objeto de garantizar que los activos de información cumplan con los siguientes principios:

- **Confidencialidad**: Los activos de información se encuentran protegidos de personas/usuarios no autorizados.
- **Integridad**: Los activos de información se encuentran completos, actualizados y son veraces, sin modificaciones inapropiadas o corruptas.
- **Disponibilidad**: Los usuarios autorizados pueden acceder a los activos de información cuando requieran utilizarlos para desempeñar sus funciones.
- **Licitud, transparencia y lealtad:** Garantizar que los datos son tratados de manera lícita, leal y transparente para el interesado.
- **Limitación de la finalidad:** Garantizar, por una parte, la obligación de que los datos sean tratados con una o varias finalidades determinadas, explícitas y legítimas y, por otra, que se prohíbe que los datos recogidos con unos fines determinados, explícitos y legítimos sean tratados posteriormente de una manera incompatible con esos fines.

5. Objetivos del SGSI

- Asegurar que todos los colaboradores y clientes comprendan las expectativas y el compromiso de NIVEL 4 con respecto al uso responsable y seguro de los recursos de información
- Participación de los colaboradores al menos en una actividad de concientización sobre seguridad de la información durante el año.
- Divulgación efectiva de principios de seguridad de la información en proyectos o contratos.
- Colaboradores de la organización demuestran un conocimiento adecuado de las amenazas a la seguridad de la información y las buenas prácticas para protegerla.

6. Objetivos Estratégicos del SGSI

- Cumplimiento de los servicios ejecutados bajo las metodologías ocupadas por NIVEL4.
- Reducción del número de incidentes relacionados con la ejecución de servicios en un 20%.
- Cumplimiento del 80% de los informes entregables incluyen evidencias que respaldan las conclusiones.
- Mantener la base de conocimientos actualizada al 90% con respecto a nuevas estrategias de amenazas en un plazo de 72 horas
- Cumplimiento del 80% de capacitaciones por procesos
- Cumplimiento del 90 de capacitaciones de Skill SGSI

7. Alcance

La presente política será de aplicación obligatoria para todos los colaboradores de NIVEL4, cualquiera sea el tipo de contratación (indefinida, plazo fijo u honorarios), el área a la cual dependa y el nivel de sus labores. Se aplicará también a todo el personal externo que preste o prestare servicios, remunerados o no, y cuenten con acceso privilegiado a la información.

El alcance del Sistema de Gestión de Seguridad de la Información comprende la totalidad de áreas de la organización en un nivel de cumplimiento interno.

8. Clasificación de la Información

- **Información de uso confidencial**: La información de uso confidencial abarca datos especialmente sensibles para NIVEL4, ya sea que estén almacenados en sistemas computacionales o en cualquier otro medio que permita su utilización, como soportes físicos. Esto incluye su almacenamiento, organización y acceso, ya sea de forma automatizada o no. Su acceso está estrictamente restringido únicamente a la alta Dirección y a aquellos empleados que cuenten con los privilegios necesarios para conocerla y desempeñar sus funciones de manera adecuada. Además de los datos corporativos, también abarca información de carácter personal, especialmente aquellos considerados como categorías especiales de datos.
- **Información de uso Interno:** Información a la cual tienen acceso los colaboradores de NIVEL4 en todas sus áreas y no es de conocimiento de clientes ni de individuos

particulares a excepción de entes regulatorios o auditores externos los cuales requieran bajo supervisión o autorización la revisión de dicha información.

- **Información de uso Público**: Toda información a la cual cualquier organismo o persona puede tener acceso y contiene datos no sensibles de la empresa. Va mayormente relacionada a la parte comercial e información de contactos de la Organización.

9. Roles y Responsabilidades

Todo el personal de NIVEL 4 en todas sus áreas debe conocer y entender la presente política y dar fiel cumplimiento de las directrices descritas en esta y otras directrices relacionadas a la seguridad de la información.

Las políticas, estrategias y procesos de Seguridad de la Información son supervisados por el responsable de seguridad de la información y son discutidos en el Comité de Seguridad de la información y Riesgos.

Las responsabilidades de administración se distribuyen de la siguiente manera:

Alta Dirección

- Ejecutar de forma efectiva y eficiente todo lo relacionado a las políticas, normativas y los procedimientos previamente establecidos.
- Asegurar y proporcionar los recursos necesarios para el desempeño del SGSI
- Evaluar y aprobar todo tipo de solicitudes (de accesos, actualizaciones, modificaciones, nuevas directrices, entre otros).
- Formar parte del Comité de Seguridad de la información y Riesgos.

CISO

- Desarrollar, actualizar y asegurar la implementación de las políticas, procedimientos e iniciativas.
- Conocer y transmitir a la Organización, el estado de Seguridad de la información a nivel corporativo.
- Implantar un programa de concientización en los distintos niveles de la Organización.
- Velar por la existencia, actualización y pruebas de los Planes y Procedimientos de Contingencia y Continuidad para los diferentes servicios prestados por NIVEL4.
- Monitorear, mitigar y gestionar las vulnerabilidades que afecten la seguridad de la información y la continuidad del negocio.
- Desarrollar y gestionar la implementación de controles y medidas de protección para los activos de información de acuerdo con su clasificación.
- Mantener y gestionar el SGSI.

10. Disponibilidad.

La política y normativas de seguridad de la información necesitan estar disponibles para el acceso de los colaboradores y protegidas frente a cambios.

La política se encontrará disponible para las partes interesadas según corresponda cada caso. Para el personal interno de NIVEL4 se encuentra comunicada y compartida mediante el GoogleDrive de la organización.

La política representa la seguridad y el tratamiento de la información de carácter organizacional y de carácter personal, englobando todo tipo de información sensible y crítica de NIVEL4 y de sus partes interesadas.

11. Directrices de Seguridad de la Información

La Organización considera que la información, los sistemas asociados e infraestructura crítica son activos que deben ser protegidos para asegurar el correcto funcionamiento de NIVEL 4.

La Seguridad de la Información en la Organización establece los principales controles, denominados directrices:

- La información de la Organización y de sus clientes se debe tratar de forma ética y sigilosa, de acuerdo con las leyes vigentes y normas internas, evitándose el mal uso y la exposición indebida.
- La información se debe utilizar de forma transparente y solamente para la finalidad para la cual se obtuvo.
- Todo el proceso, durante su ciclo de vida, debe garantizar la segregación de funciones, por medio de la participación de más de un colaborador o equipo de colaboradores.
- El acceso a la información y recursos sólo aplica en usuarios que se encuentren debidamente autorizados.
- La identificación de cualquier colaborador debe ser única, personal e intransferible, calificándolo como responsable por las acciones realizadas.
- La concesión de accesos debe obedecer el criterio de menor privilegio, en el cual los usuarios tienen acceso solamente a los recursos de información imprescindibles para el pleno desempeño de sus actividades a no ser que la Gerencia General autorice el otorgamiento de privilegios de administrador al usuario por alguna gestión específica.
- Los riesgos asociados a la información de la Organización se deben informar al encargado de seguridad de la información, quien lo canalizará al Comité o a la Gerencia General para su evaluación y tratamiento.

- Las responsabilidades en lo que se refiere a la Seguridad de la Información se deben divulgar ampliamente a los colaboradores, que deben entender y asegurar estas directrices.
- Se debe tener un correcto tratamiento de los riesgos asociados a vulnerabilidades técnicas y actualizaciones de los sistemas.
- Se debe tener el compromiso de satisfacer los requisitos aplicables concernientes a la seguridad de la información.
- Se debe gestionar periódicamente el mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información.

12. Tratamiento de la Información

La información debe recibir una protección adecuada en concordancia a los principios y directrices de Seguridad de la Información de la Organización en todo su ciclo de vida, que abarca: Generación, Manejo, Almacenamiento y Desecho.

También, los contratos que se constituyan con terceros, proveedores y/o aliados, acuerdos de confidencialidad o acuerdos de transferencia de información, dejando explícitas las responsabilidades y obligaciones legales asignadas a estos por el uso y/o divulgación no autorizada de información suministrada por la entidad que les ha sido entregada.

Con relación a los datos personales se debe garantizar los derechos y libertades de las personas desde la misma definición del tratamiento de sus datos personales. El interesado puede en cualquier momento solicitar acceder, rectificar y/o borrar los datos sobre su persona que existan en poder de la organización. La información de datos personales será tratada conforme a los principios definidos en la presente política.

13. Gestión de la Seguridad de la Información

Para asegurar que la Información tratada esté adecuadamente protegida, la Organización adopta los siguientes procesos:

- **Control de Accesos:** Las asignaciones, revisiones y exclusiones de acceso deben alinearse a los procesos y protocolos de la Organización. Los accesos deben ser rastreables, a fin de garantizar que todas las acciones posibles de auditoría puedan identificar individualmente al Colaborador, lo que le hace responsable absoluto de sus acciones
- **Clasificación y manejo de la Información:** La información se debe clasificar de acuerdo con la confidencialidad y las protecciones necesarias, en los siguientes niveles: Confidencial, Interna y Pública. Para ello, se deben considerar las necesidades relacionadas al negocio, el debido acceso y los impactos en el caso de utilización indebida de la Información.
- **Seguridad física y ambiental:** Las medidas y controles diseñados para proteger tanto los activos físicos como el entorno en el que se encuentran, asegurando así la protección de la información y la infraestructura de una organización contra una variedad de amenazas y riesgos. Esta categoría de seguridad es crucial para mantener la integridad, confidencialidad y disponibilidad de la información.
- **Administración de usuarios:** Es un aspecto crucial de la seguridad de la información que se centra en la gestión de los accesos y permisos de los usuarios a los sistemas y datos de una organización. Este proceso asegura que solo las personas autorizadas tengan acceso a la información adecuada y que dicho acceso sea gestionado de manera segura y controlada.
- **Copias de respaldo:** Son una parte esencial del sistema de gestión de la seguridad de la información. Su objetivo principal es garantizar la protección y disponibilidad de la información al proporcionar una forma de recuperar datos en caso de pérdida, daño, corrupción o cualquier otra contingencia que afecte la integridad de la información original.

- **Transferencia de información:** Es el proceso de intercambiar datos y documentos entre diferentes partes, ya sea dentro de una organización o entre organizaciones externas. Establece requisitos y controles para asegurar que la transferencia de información se realice de manera segura, protegiendo la confidencialidad, integridad y disponibilidad de los datos durante el tránsito.
- **Protección ante el software malicioso:** Son las medidas y controles implementados para prevenir, detectar, y responder a amenazas causadas por software malicioso que puede comprometer la seguridad de la información y los sistemas de una organización. El malware puede incluir virus, gusanos, troyanos, ransomware, spyware, y otros tipos de software malicioso que pueden dañar o acceder a los datos de manera no autorizada.
- **Gestión de vulnerabilidades:** Consiste en identificar, evaluar, y mitigar vulnerabilidades en los sistemas y procesos de una organización para proteger la información y los activos de seguridad. Las vulnerabilidades son debilidades en los sistemas de TI, aplicaciones, o procesos que pueden ser explotadas por amenazas para comprometer la confidencialidad, integridad, o disponibilidad de la información.
- **Controles criptográficos:** Se debe considerar la aplicación de técnicas de cifrado para proteger la información y asegurar la integridad y confidencialidad de los datos dentro de una organización. La criptografía es fundamental para asegurar que la información sensible esté protegida contra el acceso no autorizado y otros riesgos de seguridad.
- **Seguridad en las comunicaciones:** En Nivel 4 se maneja de manera prioritaria la protección de la información durante su transmisión a través de redes y sistemas de comunicación. El objetivo es garantizar que la información intercambiada entre diferentes partes, ya sean sistemas internos o externos, se mantenga confidencial, íntegra y disponible, protegiendo así los datos contra accesos no autorizados, modificaciones y pérdidas.
- **Privacidad y protección de la información identificativa de personas:** Los controles destinados a asegurar que los datos personales de individuos, tales como nombres, direcciones, números de identificación y otros datos identificativos, sean manejados de manera segura y respetuosa con la privacidad.

- **Relación con proveedores:** Nivel 4 se maneja con fundamentos la gestión de las interacciones y acuerdos con terceros que proporcionan productos o servicios que pueden afectar la seguridad de la información de una organización. Los proveedores pueden incluir desde servicios de TI y soporte técnico hasta proveedores de servicios en la nube y consultores. Es esencial asegurar que estos proveedores no introduzcan riesgos indebidos a la seguridad de la información y que cumplan con los requisitos de seguridad establecidos por la organización.
- **Gestión de Activos de la Información:** Los activos de la información se deben identificar de forma individual, inventariar, proteger de accesos indebidos y contar con documentación actualizada y supervisión.
- **Gestión de Riesgos**: Los riesgos se deben identificar a través del Procedimiento de Gestión de Riesgos el cual se basa en la Política de Gestión de Riesgos de NIVEL4. Toda evaluación de riesgos y el tratamiento de estos debe ser ejecutada en función de la información definida por NIVEL4 como crítica.
- **Tratamiento de Incidentes de Seguridad de la Información:** Los incidentes internos de Seguridad de la Información de la Organización se deben informar al encargado de seguridad de la información o ante el Comité de Seguridad de la información y Riesgos; y deben ser gestionados y documentados conforme lo dispongan las autoridades de NIVEL4.
- **Concientización en Seguridad de la Información**: La Organización promueve y comunica los principios y directrices de Seguridad de la Información por medio de programas de concientización y capacitación, con el objetivo de fortalecer la cultura de Seguridad de la Información.
- **Comunicación entre Partes Interesadas y la Organización**: La Organización dispone de herramientas seguras administradas bajo protocolos apropiados de seguridad con lo cual las partes interesadas se comunican confidencialmente con la organización. La comunicación con las partes interesadas es transparente, segura y constante.
- **Evaluación Independiente de Auditoría**: La efectividad de las políticas de Seguridad de la Información y procedimientos relacionados, así como el cumplimiento del SGSI se verifica

por medio de evaluaciones periódicas de auditoría interna, promoviendo la mejora continua mediante planes de acción definidos.

14. Propiedad Intelectual

La propiedad intelectual se compone de bienes materiales, tales como: marca, señales distintivas, eslogan publicitarios, nombres de dominio, nombres empresariales, indicaciones geográficas, diseños industriales, patentes de invención y de modelo de utilidad, obras intelectuales (tales como base de datos, fotografías, dibujos, ilustraciones, proyectos, obras audiovisuales, textos, etc.), programas de informática y secretos empresariales (incluidos secretos de industria y comercio), tecnologías, marcas, metodologías y cualquiera de estas informaciones que pertenezcan a la Organización no se deben utilizar para fines particulares, ni transferir a otro, aunque hayan sido obtenidas o desarrolladas por el propio colaborador en su ambiente de trabajo.

15. Declaración de Responsabilidad

Los Colaboradores de NIVEL4 y Prestadores de Servicios directamente contratados por la Organización deben adherirse y comprometerse a actuar de acuerdo con la presente política de Seguridad de la Información y directrices asociadas establecidas por NIVEL4.

Los contratos de la Organización con terceros deben tener una cláusula que asegure la confidencialidad de la información y los acuerdos en los niveles de servicios.

16. Sanciones disciplinarias

Cualquier violación de la presente Política de Seguridad de la Información puede resultar en la toma de las acciones disciplinarias correspondientes de acuerdo con el proceso interno del NIVEL4. Es responsabilidad de todos los colaboradores del NIVEL4 notificar al responsable de Seguridad de la Información cualquier evento o situación que pudiera suponer el incumplimiento de alguna de las directrices definidas por la presente Política.

17. Excepciones a la Política

El Gerente de un área responsable de la Organización, que solicite algún tipo de excepción a la política, deberá someterla a análisis por parte del encargado de seguridad de la información, quien definirá los pasos a seguir.

18. Normas de Difusión y Control de Versiones

La presente política, al igual que las versiones posteriores que puedan existir de la misma, deben ser comunicadas a todas las áreas y personal de NIVEL4, utilizando para ello un medio accesible y confiable, y asegurándose de la correcta recepción y entendimiento de ella. Será responsabilidad del personal de NIVEL4, conocer y dar cumplimiento cabal a la Política de Seguridad de la Información.

Esta política debe contar con una revisión anual o cada vez que se presenten modificaciones significativas, las que se pudiesen producir debido a cambios en el entorno de negocios, estructura organizacional o por cualquier otro motivo, dicha revisión debe ser

realizada por el Comité de Seguridad de la información y Riesgos con su respectiva aprobación por la Alta Dirección.