**POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN**

**I.- DEFINICIONES ESTRATÉGICAS**

La empresa, a través de su [Comité de Riesgos y Seguridad de la Información] presentan en este documento, las características, responsabilidades y consideraciones operacionales mínimas obligatorias para la administración de los activos de información de interés a fin de garantizar la continuidad operacional y la seguridad de la información en lo que se refiere a su confidencialidad, integridad y disponibilidad.

Un activo de información en el contexto de la norma ISO/IEC 27001 es: “algo que una empresa valora y por lo tanto debe proteger”.

La gestión de activos de información es una tarea de gestión de la información que involucra el diseño, establecimiento e implementación de un proceso que permita la identificación, valoración, clasificación y tratamiento de los activos de información más importantes del negocio.

**a.- Declaración**

La empresa se compromete a todo nivel, a instaurar el Sistema de Gestión de Seguridad de la Información (SGSI) para proteger los activos de información de los procesos que hacen posible existencia de la empresa, estableciendo una adecuada gestión del riesgo, aplicando y monitoreando controles para la mitigación del riesgo detectado para llevarlo a niveles compatibles con el riesgo residual tolerable o definido por el [Directorio o la Gerencia General]. Los resultados de la aplicación del SGSI serán evaluados bajo la perspectiva de la mejora continua, asegurando el cumplimiento de los requisitos legales y aplicando una estrategia de seguridad basada en las mejores prácticas y controles sobre los activos de información.

La empresa se compromete a disponer y utilizar adecuadamente plataformas electrónicas cumpliendo con estándares de seguridad, interoperabilidad, interconexión y ciberseguridad, así como las condiciones de accesibilidad, seguridad, funcionamiento, calidad, protección y conservación de los documentos, establecidas en los estándares técnicos establecido por los reguladores, la ley vigente y las propias definiciones estratégicas.

La empresa se compromete a colaborar con el ecosistema digital en materia de ciberseguridad, tanto es sus aspectos técnicos como jurídicos.

La empresa se compromete a establecer e incorporar en su diario quehacer los requisitos para la seguridad de la información, la continuidad operacional del servicio y la continuidad de la administración de la seguridad de la información ante situaciones adversas, es decir, durante una crisis, desastre o Estado de Excepción Constitucional.

Ante la eventual ausencia de estándares o normas fijadas por los órganos llamados a esta función, atingentes a seguridad de la información o ciberseguridad, la empresa considerará como estándar referencial válido a utilizar e implementar, los estándares vigentes ISO 27.001, ISO 27.002, ISO 27.032, ISO 22.301 y en general, los que sean técnicamente validados por la [Unidad TIC] mediante informe técnico fundado.

**b.- Objetivo general**

Establecer los principios y marco general de trabajo de la empresa para administrar, mantener, sensibilizar, monitorear y revisar el Sistema de Gestión de Seguridad de la Información (SGSI) acorde a las Definiciones Estratégicas, la misión/visión y objetivos estratégicos del negocio, asegurando la confidencialidad, integridad y disponibilidad de los activos de la información a través de su adecuada implementación, asignación de roles, funciones y responsabilidades.

**c.- Objetivo específicos**

* Asegurar el cumplimiento de los requisitos normativos, estatutarios, reglamentarios y contractuales, que estén orientados hacia la seguridad de la información.
* Establecer los niveles de acceso apropiados a la información, brindando y asegurando la confidencialidad, integridad y disponibilidad que requiera cada sistema, proceso, actividad crítica y usuario.
* Implementar una metodología enfocada en la gestión del riesgo institucional.
* Apoyar al modelo de gestión de continuidad de negocio.
* Establecer un marco de Gestión de Riesgo Cibernético para cada sistema, proceso, actividad crítica, que permita alcanzar los objetivos estratégicos.
* Definición del ámbito de trabajo y responsabilidades corporativas e individuales respecto al uso de los recursos tecnológicos que provee la empresa y al manejo de la información.

**d.- Alcance**

Esta política se aplica a todos los trabajadores y terceras partes que tengan o no una relación directa o indirecta de acceso a la información que pueda afectar los activos de información de la [Empresa XXX]. También se aplica a cualesquiera de sus relaciones con terceros que impliquen el acceso a sus datos, utilización de sus recursos o a la administración y control de sus sistemas de información.

Esta política rige independientemente del lugar en el trabajador presta sus servicios a la empresa, total o parcialmente, e indistintamente de la modalidad de trabajo ya sea “presencial”, “a distancia”, “teletrabajo” u otra, en las condiciones que establezca la legislación vigente, los planteamientos de la Dirección del Trabajo o los Estados de Excepción Constitucional decretados por el Presidente de la República.

Esta política gobierna la seguridad de la información de todos los procesos de la [Empresa XXX], establecidos por el [Directorio o Gerencia General], cubriendo a toda la organización independiente de su ubicación geográfica en el país (Chile Continental, Chile Insular o la Antártica Chilena).

**e.- Revisión Independiente de la Seguridad de la Información**

El [Comité de Riesgos y Seguridad de la Información] podrá solicitar a una Unidad interna u organismo auditor externo, la realización de auditorías o revisiones independientes sobre el cumplimiento de la Política de Seguridad de la Información, las Políticas específicas, los Procedimientos establecidos para operativizar las políticas, el proceso de Gestión del Riesgo, y en general el funcionamiento y operación del Sistema de Gestión de Seguridad de la Información.

**f.- Marco referencial**

Los contenidos y controles esenciales de carácter legal que se consideraran en las políticas de la Subsecretaría y del Servicio de Gobierno Interior son:

* NCh-ISO 27001/27002 - Tecnología de la Información – Código de prácticas para la gestión de seguridad de la información - INN Chile.
* Ley N° 19.799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.
* Ley N°19.628: sobre Protección de la vida privada.
* Ley N° 19.223: sobre Delitos informáticos.
* Ley N° 17.336: de Propiedad Intelectual.
* [Agregar otros marcos legales pertinentes a la empresa o sector económico].

**g.- Vigencia y actualización**

La Política se considera vigente desde la fecha de su aprobación por parte de la autoridad, documento que será revisado y actualizado cada dos años o cuando el Comité de Riesgos y Seguridad de la Información lo determine, o toda vez que se produzca un cambio significativo que modifique el nivel de riesgo presente de la [Empresa XXX].

La Política deberá ser revisada por el Comité de Seguridad de la Información. No obstante, aquello, la [Unidad responsable de Ciberseguridad] promoverá la revisión permanente de esta Política y generará las propuestas de actualización que sean necesarias, con el objetivo de apoyar el ciclo de mejora continua del SGSI.

Entre los cambios que hacen necesaria la revisión de las políticas, se debe destacar:

* Cambios en las leyes o reglamentos que afecten a la [Empresa XXX].
* Incorporación o modificaciones relevantes de procesos o actividades críticas de la [Empresa XXX].
* Cambios significativos al soporte tecnológico.
* Modificaciones en la estructura de la organización.
* Cambios significativos en los niveles de riesgo a que se expone la información.
* Cambios relevantes en las Definiciones Estratégicas.
* Ajustes necesarios producto de Estados de Excepción Constitucional.
* Ajustes necesarios para proteger las infraestructuras críticas.

Las revisiones que se efectúen a la Política de General de Seguridad de la Información deben considerar tanto la actualidad de ella, como su eficacia, eficiencia y cumplimiento.

**h.- Revisión del cumplimiento**

El Comité de Riesgos y Seguridad de la Información, anualmente, asignará la responsabilidad de ejecutar un proceso formal de revisión del cumplimiento a cargo de una o varias unidades organizacionales, pudiendo optar también por una revisión independiente interna o una externa ejecutada por una tercera parte.

Además, este Comité determinará la metodología y los alcances que estime necesarios para cumplir los objetivos estratégicos de revisión y cumplimiento de las políticas y su mejora continua.

**i.- Control de documentos**

Los documentos requeridos por el Sistema de Gestión de la Seguridad de la Información (SGSI) deben protegerse y controlarse. Con este objetivo, las acciones necesarias a implementar son:

* Revisar y actualizar los documentos cuando sea necesario y aprobarlos nuevamente.
* Registrar los cambios o actualizaciones de los documentos una vez que son aprobados por el Comité de Riesgos y Seguridad, incorporando Tabla en Capitulo final en cada documento.
* Se deberá controlar el uso no intencionado de documentos obsoletos.
* En caso de mantenerse los documentos por cualquier propósito, éstos deberán tener una adecuada identificación a efecto de diferenciarse de los vigentes.

Las versiones pertinentes de los documentos aplicables se encontrarán disponibles para quienes lo necesiten y serán almacenados y transferidos de acuerdo con los procedimientos aplicables a su clasificación.

**j.- Roles y responsabilidades**

La formalización de las tareas, funciones y responsabilidades sobre los procesos de tratamiento y gestión de la información, por su amplitud, son establecidos en la primera Política Específica, denominada:

PE-SGSI-001: POLÍTICA DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

**k.- Difusión**

El mecanismo de difusión de la Política será a través de la Intranet, circulares informativas, correos electrónicos masivos o cualquier otro medio que el [Comité de Riesgos y Seguridad de la Información] estime pertinente, procurando apoyar la sensibilización con infografías que faciliten la comprensión de esta por todos los usuarios en general.

**II.- PRINCIPIOS Y RESPONSABILIDADES TRANSVERSALES**

**a.- Principios generales**

La política general de seguridad busca armonizar los controles necesarios con la debida funcionalidad de los procesos tanto de cara a los usuarios internos como a los clientes que utilizan los servicios y productos, alineados con las diferentes normativas, en función de la evaluación de riesgo y costo de los procesos.

Esta política estará basada en un modelo de gestión del riesgo que permita al [Directorio o Gerencia General] enfrentar el riesgo sujeto a los recursos económicos, tecnológicos y humanos disponibles.

Se han de considerar los diferentes desafíos que afecten la ciberseguridad con criterios de priorización, privilegiando los procesos que permitan el cumplimiento de los objetivos estratégicos del negocio y las regulaciones vigentes.

**b.- Principios específicos**

* Principio de constitucionalidad y legalidad: La presente política, se deberá interpretar de manera tal que su aplicación se concilie con las normas constitucionales y legales vigentes, referidas a los derechos y libertades de las personas.
* Principio de responsabilidad transversal: El incumplimiento de las obligaciones establecidas en la Política General Seguridad de la Información podrá constituir una transgresión que puede ser motivo de acciones administrativas internas. Lo anterior sin perjuicio de la responsabilidad civil o penal que corresponda.
* Principio del buen uso de los recursos institucionales: El uso de los sistemas de comunicaciones electrónicas debe enmarcarse en el ámbito de competencia de la empresa, teniendo como finalidad el ejercicio de las funciones propias e inherentes para las cuales el usuario ha sido contratado o se ha convenido su prestación de servicios. Se promueve el buen uso de los sistemas de comunicaciones electrónicas, especialmente para aquellas prácticas que protejan a los sistemas de eventuales daños ocasionados por amenazas cibernéticas, entre las que se pueden mencionar: físicas, desastres naturales, por pérdida de servicios esenciales, por perturbación debido a radiación, por compromiso de información sensible, por fallas técnicas, por acciones no autorizadas, por compromiso de funciones, por acción de hacker, por acción de ciberdelincuentes, por acción terrorista, por espionaje industrial, por acción interna y otros.
* Principio para obtención de prueba en investigación interna: Con motivo de una investigación interna, el [Directorio o Gerencia] podrá autorizar que la [Unidad TIC] ejecute, en determinado sistema informático o en los servidores de la Unidad a cargo de la administración, procesos definidos tendientes a obtener la información necesaria, de tal forma que se garantice la menor afectación a la privacidad del trabajador.
* Principio de responsabilidad por uso malicioso: La apertura de archivos adjuntos o la ejecución de programas que se reciban por medios electrónicos, constituyen acciones que pueden vulnerar la estabilidad, calidad o seguridad de las redes o del sistema informático. El personal no debe guardar, abrir o ejecutar en el equipo informático, programas o documentos electrónicos; si la fuente de éstos no es conocida; si no está autorizado por el propietario intelectual o industrial; como tampoco, si no se ha adquirido la licencia respectiva.
* Principio de Acciones especiales de seguridad: El personal autorizado de la [Unidad TIC] podrá restringir, bloquear o cancelar el acceso de un usuario a los servicios tecnológicos o a otro servicio o sistema informático, siempre que dicha acción de seguridad sea indispensable en los siguientes casos:
* Cuando existan requerimientos legales o judiciales, ante la presunta perpetración de algún ilícito.
* Cuando existan antecedentes fundados, previa calificación del [Directorio o Gerencia General], que den cuenta de la violación grave de la normativa interna, o de la comisión de un ilícito.
* Cuando por motivo del acceso, se cause o pueda causar un daño grave e inminente a la calidad o estabilidad del servicio informático o de las redes. Esta circunstancia deberá ser informada por el jefe de la [Unidad TIC] al [Directorio o Gerencia General], a más tardar dentro del día hábil siguiente desde que se inició la acción de seguridad.
* La [Unidad TIC] deberá informar al usuario afectado por la acción de seguridad, dentro del día hábil siguiente, salvo que el [Directorio o Gerencia General] disponga lo contrario.
* Principio de confidencialidad e integridad de la información: Se deberá garantizar y mantener la confidencialidad e integridad de toda la información y datos de los usuarios, que tenga acceso con ocasión de la administración del sistema informático y los servicios de redes.
* Principio de Seguridad ante la navegación en la Internet: El personal autorizado de la [Unidad TIC] podrá ejecutar sistemas de filtro, monitoreo y registro del tráfico de la navegación en la Internet, que se realice a través de las redes de la empresa, incluyendo las extranet (VPN), sólo para efectos de mantener protegida la seguridad y estabilidad del sistema informático, así como para procurar que su uso común y regular esté abocado a los fines establecidos.

**III.- DIFUSIÓN**

**a.- Obligación de conocimiento y cumplimiento**

El personal o terceras partes que usen los recursos informáticos de la red de la empresa, deberán conocer y dar cumplimiento a esta Política General de Seguridad de la Información.

**b.- Incorporación de la norma a los actos administrativos y contratos**

Las normas y política expresadas en este documento, se considerarán parte integrante de los contratos de trabajo, y de cualquier otro contrato de servicio que signifique el uso de los medios informáticos proporcionados por la empresa.

**c.- Publicidad y fomento de su cumplimiento**

Se deberá mantener publicada en la intranet institucional, las normas de uso y políticas de seguridad de la información establecidas en el presente reglamento. A la vez se difundirá con la frecuencia que el [Comité de Riesgos y Seguridad de la Información] determine o que los actores internos relacionados impulsen, a través de correo masivo invitando a conocerlas, cada vez que sean modificadas tanto la Política General como las Específicas y las respectivas guías, procedimientos y protocolos atingentes, que hayan sido aprobadas, incorporando en lo posible estrategias comunicacionales que simplifiquen educativamente los contenidos para hacerlos fácilmente comprensibles, interpretables, asimilables y adoptables por todo el personal.

Asimismo, la [Unidad TIC] en coordinación con el [Departamento de Desarrollo y Gestión de Personas] favorecerán acciones destinadas a sensibilizar, entrenar, capacitar y educar a los usuarios para operar los servicios y sistemas informáticos en conformidad a dichas normas y políticas.

El [Departamento Desarrollo y Gestión de Personas] será la unidad encargada de gestionar la capacitación del personal y deberá incorporar las materias de seguridad de la información como elemento informativo relevante dentro de sus planes anuales. En este sentido deberá velar por la asignación de recursos para estos entrenamientos y sensibilización. Se considera un aspecto clave para el éxito de esta política hacer llegar el conocimiento a los diferentes niveles jerárquicos, razón por la que el plan de capacitación y de difusión de estas materias debe contemplar las diferentes necesidades del público objetivo, adecuando los niveles de profundidad del material a entregar y seleccionando las tecnologías óptimas que permitan una entrega eficiente y eficaz de los conocimientos.

**IV.- POLÍTICAS ESPECÍFICAS**

Se deberán aprobar, validar y mantener, según corresponda, de acuerdo con los compromisos de revisión establecidos, al menos las siguientes políticas específicas para cubrir en detalle los dominios de la normativa vigente sobre Seguridad de la Información Institucional, junto a los procedimientos, normas e instructivos que sean necesarios para la implementación y operación de éstas.

* PE-SGSI-001: De organización de la seguridad de información.
* PE-SGSI-002: De gestión de Administración de activos de información, Equipamiento y Plataforma de Servicios Informáticos para usuarios.
* PE-SGSI-003: De seguridad ligada a los recursos humanos.
* PE-SGSI-004: De seguridad física y del ambiente.
* PE-SGSI-005: De gestión de comunicaciones y operaciones.
* PE-SGSI-006: De control de acceso.
* PE-SGSI-007: De proceso de desarrollo de software.
* PE-SGSI-008: De gestión de incidentes de seguridad de la información.
* PE-SGSI-009: Del uso correo electrónico institucional.
* PE-SGSI-010: De planificación de la continuidad de la seguridad de la información.
* PE-SGSI-011: De trabajo a distancia y teletrabajo

**V.- SANCIONES**

El no cumplimiento de la Política de Seguridad y Específicas, será sancionado en conformidad a las disposiciones administrativas internas. Lo anterior, sin perjuicio de la responsabilidad civil o penal que corresponda.

**VI.- GLOSARIO DE TÉRMINOS**

Definiciones. Para los propósitos de esta Política, se entenderá por:

Activos de la información: Todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la Institución, cualquiera sea el formato que la contenga y los equipos y sistemas que la soporten. Por ejemplo: dispositivos móviles, tarjetas de accesos, software, equipamiento computacional, personal, edificios, infraestructura tecnológica y física.

Amenaza: Causa potencial de un incidente no-deseado por el cual puede resultar dañado o afectado un sistema u organización. Ejemplos: terremotos, inundaciones, sabotajes, amenazas de bombas, negligencias humanas, cortes eléctricos, fallas en sala de servidores, entre otras.

Confidencialidad: La información debe estar protegida de accesos no autorizados. Por lo tanto, se debe asegurar que la información es accedida únicamente por las personas autorizadas.

Disponibilidad: Certeza del acceso a la información cuando es requerida por los usuarios autorizados.

Documento electrónico: Toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior.

Dueños de los datos : Se refiere a la Unidad de negocios que maneja datos institucionales, contenidos tanto en medios tradicionales como en sistemas informáticos a que pertenecen los usuarios que son funcionarios del Ministerio, en la calidad contractual que sea.

Estación de Trabajo: Equipo computacional conectado a una red de computadores que facilita a los usuarios el acceso a los servidores y periféricos de la red.

Evaluación del riesgo: Proceso consistente en la comparación de los niveles de riesgo encontrados contra los criterios de riesgo prestablecidos (si es que han sido establecidos por la dirección) considerando el balance entre los beneficios potenciales y resultados adversos, para posteriormente ordenar y priorizar mediante un ranking los riesgos analizados.

Gestión del riesgo: Proceso definido para identificar, evaluar, manejar y controlar acontecimientos o situaciones potenciales, con el fin de proporcionar un aseguramiento razonable respecto al alcance de los objetivos de la organización. Es un proceso iterativo que debe contribuir a la mejora organizacional a través del perfeccionamiento de los procesos.

Incidente de Seguridad: Cualquier evento o situación que comprometa la disponibilidad, integridad y confidencialidad de la información, o bien afecte a la plataforma tecnológica, proceso y aplicativos que la contienen, impidiendo acceder a ésta en forma oportuna. En general, es una transgresión de una política, estándar o procedimiento de seguridad, que no permite prestar los servicios institucionales por medios informáticos o tradicionales. Ejemplos de incidentes: Acceso no autorizado, robo de contraseñas, robo de información, denegación de servicio en internet, un malware actuando en los equipos institucionales o un phishing que ataca a los usuarios institucionales.

Integridad: La información debe estar completa, actualizada y ser veraz, sin modificaciones o alteraciones no autorizadas o corruptas.

Política de Seguridad: Conjunto de normas o buenas prácticas, declaradas y aplicadas por una organización, cuyo objetivo es disminuir el nivel de riesgo en la realización de un conjunto de actividades de interés, o bien garantizar la realización periódica y sistemática de este conjunto.

Proceso: Conjunto de actividades o eventos que se realizan o suceden (alternativa o simultáneamente) con un fin determinado.

Programa malicioso (malware): Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora. También se denominan malware.

Restricción del acceso: Acción consistente en la delimitación de acceso de los funcionarios, servidores públicos a honorarios y terceras partes a determinados recursos físicos o lógicos.

Riesgo : Es la contingencia de un daño a un activo de información. A su vez, contingencia significa que el daño puede materializarse en cualquier momento o no suceder nunca.

Sanción: Consecuencia jurídica de naturaleza administrativa, civil o penal derivada del incumplimiento de un deber.

Seguridad de la Información: Proceso encargado de asegurar y proteger los recursos de un sistema de información para que sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización, preservando la Integridad, Confidencialidad y Disponibilidad.

Sistema informático: Software asociado, periféricos, terminales, procesos físicos, medios de transferencia de información y otros, que forman un todo autónomo capaz de realizar procesamiento de información o transferencia de información.

Sistema de comunicaciones electrónicas: Se refiere a todo medio o dispositivos que permite comunicarse. Entiéndase: correo electrónico, mensajería instantánea (WhatsApp, Instagram, Discord, WeChat, Facebook Messenger, Line, Viber, Snapchat, Skype u otros), Teleconferencia (Skype, Zoom, Microsoft Team, Webex, Jitsi u otros), Telefonía fija y móvil, u otros.

Teletrabajo: si los servicios son prestados mediante la utilización de medios tecnológicos, informáticos o de telecomunicaciones o si tales servicios deben reportarse mediante estos medios. Válida mientras no exista una disposición legal que la sustituya o modifique en el contexto gubernamental.

Terceras partes: Persona u organismo ajeno a la relación directa establecida entre dos partes principales. Para estos efectos, se entenderá como terceras partes, entre otros a los proveedores de servicios y de red, los proveedores de productos de software y servicios de información, outsourcing de instalaciones y operaciones, servicios de asesoría de seguridad y auditores externos.

Trabajo a distancia: aquel en el que el trabajador o funcionario presta sus servicios, total o parcialmente, desde su domicilio u otro lugar o lugares distintos de los establecimientos, instalaciones o faenas de la empresa. Válida mientras no exista una disposición legal que la sustituya o modifique en el contexto gubernamental.

Usuario: Persona que utiliza el sistema informático o los medios de la empresa con independencia de su calidad contractual y la modalidad de trabajo (presencial, teletrabajo o trabajo a distancia).