SEGURIDAD DE LA INFORMACIÓN

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Dueño de la Información	Dueño del Proceso	Dueño del Sistema	Dueño del Riesgo	Clasificación de Información
Jefe de Seguridad	Chief Technology Officer	Gerente General	Gerente de Cumplimiento y Consultoría	Uso Interno

CONTENIDO

1 PROPÓSITO

Establecer las directrices para asegurar la integridad, confidencialidad y disponibilidad para toda la información relevante, con el objeto de asegurar la continuidad operacional del negocio, a través de un Sistema de Gestión de Seguridad de la Información en ECERT.

2 ALCANCE

Esta política del Modelo de Seguridad de la Información establece de manera clara los lineamientos generales para el uso adecuado de los activos de información de las partes interesadas, tanto internas como externas.

Proporciona directrices y soporte para la gestión de la seguridad de la información, asegurando su alineación con los requerimientos estratégicos de la organización y con los aspectos legales, regulatorios, contractuales y operacionales aplicables.

La responsabilidad de proteger la información recae tanto en los colaboradores internos como en las personas o entidades externas que, debido a sus funciones, acceden a los activos de información de la empresa. Esto incluye proveedores de servicios, asesores y cualquier otro usuario que tenga acceso a las instalaciones o sistemas de la organización.

El conocimiento y cumplimiento de esta política es obligatorio para todas las partes involucradas, y su cumplimiento debe quedar explícito en los contratos, acuerdos o compromisos respectivos

3 REFERENCIAS

3.1 Referencias Normativas

- ISO/IEC 27001:2022 – Sistema de Gestión de Seguridad de la Información:
  - Control A. 5.1.
- Ley N° 21.663 - Ley Marco de Ciberseguridad.
- Ley N° 19.628 - Sobre la Protección de la Vida Privada.

- Ley N° 21.719 - Regula la Protección y el Tratamiento de los Datos Personales y Crea la Agencia de Protección de Datos.

ECERT declara y garantiza que dará estricto cumplimiento a todas las obligaciones establecidas en la Ley N° 21.663, que crea la Agencia Nacional de Ciberseguridad (ANCI), así como a las instrucciones generales, reglamentos, normas técnicas y demás disposiciones que de ella emanen y le sean aplicables.

Asimismo, ECERT declara y garantiza que dará estricto cumplimiento a la Ley N° 19.628 y a la Ley N° 21.719 sobre Protección de Datos Personales, una vez que esta última entre en vigencia, junto con sus normas complementarias. En este marco, ECERT adoptará las medidas técnicas, organizativas y contractuales necesarias para asegurar la licitud, lealtad, finalidad, proporcionalidad, calidad, responsabilidad, seguridad, transparencia y confidencialidad en el tratamiento de datos personales y datos sensibles.

ECERT tendrá a disposición del público su Política de Protección de Datos Personales y contará con los canales de comunicación que permitan a los titulares ejercer sus derechos ARCO.

3.2 Referencias Documentales Internas

- Política del Sistema de Gestión Integrado (SGI-PE-101-0003).
- Política de Propiedad intelectual (SGI-PL-104-0012).
- Política de Cumplimiento Legal (SGI-PL-104-0011).
- Política de Sanciones (SGI-PL-104-0031).
- Reglamento Interno de Orden, Higiene y Seguridad (SGI-F-301-0019).

4 DEFINICIONES

- **Activo:** Cualquier elemento que tenga valor para la organización. Para el ámbito de seguridad de la información, se puede clasificar en:
    - **Activos de Información:** se entenderá por Activo de Información todo elemento en que se registre, se almacene y/o procese datos e información,

sea a través de medios tecnológicos o no, tales como: personas, bases de datos y archivos, contratos y acuerdos, documentación del sistema, manuales de usuario, material de entrenamiento, procedimientos operacionales o de soporte, plan de continuidad de negocio, información de auditorías, información archivada, activos de software, activos físicos y servicios.

  - **Activos de Software:** Constituidos por las aplicaciones de software, Software de sistemas y Herramientas de desarrollo y utilidades.
  - **Activos Físicos:** Constituidos por el equipamiento computacional, Equipamiento de comunicaciones, Medios móviles y otros equipamientos.

- **Servicios:** Servicios de computación y comunicaciones. Utilidades generales (ej. electricidad, luz, aire acondicionado, entre otros).
- **Personas:** Constituidos por los usuarios, que utilizan la estructura tecnológica, el área de comunicaciones y que gestionan la información.
- **Intangibles:** Constituidos por los activos referidos a la reputación e imagen de la empresa.
- **Amenaza:** Una causa potencial de un incidente no deseado, el cual puede derivar en daño a un sistema u organización.
- **Análisis de Riesgos:** Uso sistemático de la información para identificar las fuentes y calcular el riesgo.
- **Confidencialidad:** Garantía de que accedan a la información sólo aquellas personas autorizadas a hacerlo.
- **Integridad:** Mantenimiento de la exactitud y totalidad de la información y los métodos de procesamiento.
- **Disponibilidad:** Garantía de que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.
- **Política:** Intención y dirección general expresada formalmente por la autoridad máxima en la institución.

- **Riesgo:** Es la probabilidad de que ocurra un evento o posible incidente que pudiera ocasionar pérdida o daño al patrimonio.
- **Seguridad de la Información:** Preservación de confidencialidad, integridad y disponibilidad de la información; además, también puede involucrar otras propiedades como autenticidad, responsabilidad, no-repudio y confiabilidad.
- **Sistema Informático:** Constituido por el conjunto de computadores, software asociado, periféricos, terminales, procesos físicos, medios de transferencia de información y otros, que forman un todo autónomo capaz de realizar procesamiento de información y/o transferencia de información.
- **Software malicioso:** También conocido como Malware (del inglés "malicious software") entendiéndose por tal todo software que tiene como objetivo infiltrarse en un sistema informático y dañar la (o las) computadora(s) que lo sustenta(n) sin el conocimiento de su dueño, con finalidades muy diversas. En esta categoría, encontramos desde Virus informáticos hasta Troyanos y Spyware. El Malware hace referencia a una variedad de software o programas de códigos hostiles e intrusivos. Se debe considerar que el ataque a la vulnerabilidad por malware puede ser a una aplicación, una computadora, un sistema operativo o una red completa.
- **Tecnología de la Información y de las Comunicaciones (TIC):** Constituida por la agrupación de los elementos y las técnicas utilizadas en el tratamiento y la transmisión de la información, principalmente de informática, internet y telecomunicaciones.

5 RESPONSABILIDADES

5.1.1 Gerente General

- Asegura el establecimiento de esta Política, así como de su adecuación a los procesos y al negocio.
- Revisa al menos una vez al año esta Política.

- Informa al Directorio y junto a la plana ejecutiva sobre los riesgos asociados y lo que está por resolver respecto de las medidas de tratamiento a implementar.

5.1.2 Comité de Sistema de Gestión

- Asume la responsabilidad de asegurar la aplicación y seguimiento de la presente Política y documentación relacionada.
- Conoce los riesgos y oportunidades asociados para aportar en el análisis del cambio propuesto en el Comité Sistema de Gestión.

5.1.3 Propietario del Proceso, del Riesgo o del Activo de Información

- Asume la responsabilidad de asegurar la aplicación y seguimiento de la presente Política y documentación relacionada.
- Conoce los riesgos y oportunidades asociados, define planes de mitigación y procura la implementación de estos.

6 CONTENIDO DE POLÍTICA DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN

6.1 De Carácter General

El modelo de Seguridad de la Información en ECERT se fundamenta en la implementación de prácticas que abarcan todas las fases del ciclo de vida de los procesos y sistemas, garantizando que la seguridad esté integrada desde la planificación hasta el retiro o disposición final. Para cumplir con los objetivos de protección y asegurar un entorno seguro, ECERT aplica los siguientes principios generales:

6.1.1 Política

- La alta dirección y el Comité de Seguridad de la Información deben procurar una correcta administración de la información de la empresa y velar por su adecuado

uso, conservación y mantenimiento, conforme a leyes, normas y acuerdos contractuales.

- Definen, elaboran, aprueban, implementa, publican, comunican, revisan, monitorean y actualizan cuando sea requerido la Política de Seguridad de la Información, para prevenir, detectar y corregir para mitigar cualquier amenaza y/o vulnerabilidad asociada a la información de la organización.
- La empresa reconoce que la seguridad de la información tiene alta prioridad para cumplir con el cumplimiento de los aspectos legales, normativos y contractuales, lo que constituye un compromiso de la Alta Dirección y de sus colaboradores, estableciendo criterios y lineamientos relacionados con la Seguridad de la Información para lo cual se establece el marco normativo, políticas y procedimientos que faciliten disponer de controles para gestionar, generar, procesar, intercambiar y almacenar los activos de información, para el aseguramiento de los niveles de Confidencialidad, Integridad y Disponibilidad que favorezca la continuidad de las operaciones.
- La alta dirección y el Comité de Seguridad de la Información deben procurar una correcta administración de la información de la empresa y velar por su adecuado uso, conservación y mantenimiento, conforme a leyes, normas y acuerdos contractuales.
- Definen, elaboran, aprueban, implementa, publican, comunican, revisan, monitorean y actualizan cuando sea requerido la Política de Seguridad de la Información, para prevenir, detectar y corregir para mitigar cualquier amenaza y/o vulnerabilidad asociada a la información de la organización.
- La empresa reconoce que la seguridad de la información tiene alta prioridad para cumplir con el cumplimiento de los aspectos legales, normativos y contractuales, lo que constituye un compromiso de la Alta Dirección y de sus colaboradores, estableciendo criterios y lineamientos relacionados con la Seguridad de la Información para lo cual se establece el marco normativo, políticas y procedimientos que faciliten disponer de controles para gestionar, generar, procesar, intercambiar y

almacenar los activos de información, para el aseguramiento de los niveles de Confidencialidad, Integridad y Disponibilidad que favorezca la continuidad de las operaciones.

- En función de lo antes expuesto la alta dirección ha establecido su compromiso: La Alta Dirección establece su compromiso con el desarrollo y la implementación del Sistema de Gestión de Seguridad de la Información –SGSI conforme a ISO/IEC 27001:2022, así como la mejora continua de su efectividad mediante las siguientes acciones:
  - Autorizando la implementación y aprobación del SGSI.
  - Estableciendo la política y objetivos del SGSI.
  - Asignando roles y responsabilidades en seguridad de la información.
  - Asegurando que la Política de Seguridad de la Información es comunicada, conocida y entendida por todos y cada uno de los colaboradores que pertenecen a la organización, así como también por sus proveedores, clientes y terceras partes.
  - Proporcionando los recursos necesarios para la correcta implementación del SGSI.
  - Asegurando que todo el personal a quien se asignó las responsabilidades definidas en el SGSI sea competente para realizar las tareas requeridas.
  - Mejorando continuamente los procesos, mediante el Sistema de Gestión de la Seguridad de la Información, conforme a las directrices establecidas en la Norma Internacional ISO 27001:2022.
  - Satisfaciendo los requerimientos de sus clientes en temas de seguridad de la información, asignando los recursos necesarios para lograr un óptimo desempeño.
  - Promoviendo la seguridad de la información, comprometiendo para ello la participación de todo su personal, valorando su participación y aportes.
  - Promoviendo la mejora continua del Sistema de Gestión de Seguridad de la Información, para aumentar la competitividad en el mercado, utilizando

herramientas de control de procesos, auditorías, análisis de riesgos, capacitaciones y la toma de conciencia de las partes involucradas para comprometer su participación.

- Asegurando la actividad constante de la organización, en función de los requerimientos legales, reglamentarios y contractuales de seguridad de la información.
- Manteniendo el impulso y apoyo para asegurar la información: Confidencialidad, Integridad y Disponibilidad.
- Revisando y actualizando la Política de Seguridad de la Información cuando sea requerido, coincidiendo y realizando la revisión del SGSI por la Dirección y/o cuando se produzcan cambios significativos, con el fin que se mantenga idoneidad y adecuación, asegurando así su conveniencia, suficiencia y eficacia continua, dejando registro de estas revisiones.
- Apoyando la definición y establecimiento de políticas, procedimientos, instructivos y planes asociados a seguridad de la información que sean necesarios en la organización.

6.1.2 Tópicos de la Política

6.1.2.1 Organización de la Seguridad de la Información

El objetivo es establecer un marco de trabajo de la dirección para comenzar y controlar la implementación y funcionamiento de la Seguridad de la Información dentro de la organización. A continuación, algunos aspectos que se han establecido como parte de la gestión:

- Implementación del sistema y la definición clara de funciones y responsabilidades.
- Elaboración de políticas asociadas a la Norma ISO/IEC 27001:2022, Anexo “A” adecuadas a los requerimientos de Seguridad de la Información aplicable al alcance del SGSI.

- Definición y establecimiento de mecanismos de actualización periódica de la información documentada relacionada con el sistema de gestión de la seguridad de la información.
- Mejora continua de la seguridad de la información, en función de los procesos establecidos en el alcance del SGSI.
- Establecimiento de medidas de seguridad relacionados con los accesos de partes interesadas externas que requieran acceso a la información.

La creación del Comité de Seguridad de la Información es fundamental para el apoyo a la alta dirección para velen por el cumplimiento de las políticas, procedimientos, gestión de los incidentes de seguridad de la información, cuyos roles y responsabilidades se han establecido en el reglamento del Comité de la Seguridad de la Información, en el documento de roles y responsabilidades y en el descriptor de cargos relacionados con dicho comité.

El comité tiene como finalidad asegurar la confidencialidad, integridad y disponibilidad de los activos de información establecidos en el alcance del SGSI, así como los medios que soporten la información, sean estos tecnológicos o de otro tipo. Se debe tener en cuenta que determinadas actividades pueden requerir el acceso de terceros a la información interna, así mismo, externalizar hacia terceros algunas funciones relacionadas con la información que se maneja dentro del alcance del SGSI. Cuando el servicio es tercerizado, se debe evaluar el nivel de exposición de la información sensible que puede estar expuesta a riesgos si las terceras partes.

Este aspecto de la Política se aplica a todos los recursos del área establecida en el alcance y a todas sus relaciones con terceras partes que requieran tener acceso a los activos de información establecidos dentro del alcance del SGSI. Adicionalmente se han establecido las buenas prácticas de la norma ISO/IEC 27002:2022, señaladas a continuación:

6.1.2.2 Contacto con las autoridades

Se mantienen los contactos apropiados con las autoridades pertinentes al cumplimiento de la ley, entidades regulatorias, autoridades de supervisión, proveedores de servicios básicos y telecomunicaciones, servicios de emergencia, electricidad, agua, salud, seguridad,

bomberos, entre otras, cuando corresponda, en caso de existir un evento o incidente de seguridad, informando los incidentes de seguridad de la información identificados de manera oportuna, conforme a los lineamientos establecidos en el procedimiento Gestión de Incidentes de Seguridad. Se utiliza para ello un documento interno (Identificar el documento) con la lista de contactos y un breve instructivo de cómo proceder.

6.1.2.3 Contacto con grupos de interés

Se mantienen los contactos con grupos de interés especiales y/o foros especializados en seguridad, así como asociaciones de profesionales, para apoyar el mejoramiento del conocimiento sobre las buenas prácticas y permanecer al tanto de la información de seguridad actualizada del contexto y oportuna para la toma de decisiones, o ejecución de acciones, alertas, relacionados con ataques y vulnerabilidades; obtener acceso a información de especialistas sobre consejos de seguridad; compartir e intercambiar información sobre nuevas tecnologías, productos, amenazas y vulnerabilidades; proporcionar puntos de enlace adecuados al tratar con incidentes de seguridad de la información. Los contactos que conforman los grupos de interés especial, foros de seguridad de especialistas y asociaciones profesionales se enumeran en un documento interno con las instrucciones pertinentes (identificar el documento).

6.1.2.4 Seguridad de la información relacionada con la gestión de proyectos

Dentro del alcance del SGSI, sin importar el tipo de proyecto, se integra la Seguridad de la Información en los métodos de administración de proyectos, para asegurarse de que se identifican y abordan los riesgos de seguridad de la información como parte de un proyecto, sin importar su carácter. Para ello, los métodos de administración de proyectos deben incluir los objetivos de seguridad de la información en los objetivos del proyecto; realizar una evaluación de riesgos de seguridad de la información antes de iniciar el proyecto de manera de definir y establecer los controles que sean necesarios, estableciendo que la seguridad de la información sea parte de todas las fases de la metodología aplicada al proyecto.

6.1.2.5 Seguridad de Recursos Humanos

Se han establecido los siguientes lineamientos asociados a la gestión de personas:

- Asegurar que los colaboradores y contratistas conocen, entienden y cumplan sus responsabilidades, y que sean aptos para los roles para los cuales están siendo considerados.
- Proteger los intereses de la organización como parte del proceso de cambio o desvinculación del empleo.
- Reducir los riesgos en el manejo de información y establecer compromisos y mecanismos necesarios para fortalecer las debilidades en materia de seguridad a este respecto.
- Considerar en los procesos de selección, incorporación, capacitación y desvinculación de Gestión de Personas, aquellos roles necesarios que permitan mantener el debido resguardo de los activos de información.
- Para resguardar los activos de información en relación con Gestión de Personas, se realizarán las siguientes acciones, no siendo la siguiente lista taxativa:
    - Definición de roles, cargos y accesos del personal perteneciente a la empresa a los activos de información definidos y establecidos dentro del alcance del SGSI.
    - Inclusión en el proceso de reclutamiento de personal, las políticas, procedimientos e instructivos establecidos por la empresa.
    - Establecimiento de los procesos de capacitación, inducción, talleres y formación en general, los deberes y responsabilidades, correspondientes al personal y a la empresa en general, en materia de Seguridad de la Información.
    - Toma de conciencia al personal en aquellas materias relacionadas a Seguridad de la Información.
    - Definición, establecimiento, implementación, mantenimiento y actualización de políticas, acuerdos y/o procedimientos de resguardo de activos de información en los procesos de desvinculación del personal.

6.1.2.6 Gestión de activos

Se han establecido políticas y procedimientos para mantener la debida protección de los activos de la información, considerando las siguientes actividades:

- Clasificación y elaboración de un inventario de los activos de información de la empresa, así como de su actualización, conforme al tipo, formato, ubicación física y/o virtual según corresponda, importancia, responsable y procedimiento de manipulación, proveyendo adicional protección a aquellos activos de información que lo requieran dentro del marco legal.
- Realización, identificación, análisis, evaluación y tratamiento de riesgos potenciales que puedan impactar en los activos de la información.
- Identificación y clasificación de los activos de la información asociados a los procesos de la empresa, para el aseguramiento de la continuidad de las operaciones y del negocio.
- Realización de un análisis de los riesgos asociados a los activos de información, de acuerdo con su importancia y ubicación, de manera de determinar, en forma permanente, las posibles brechas de seguridad existentes para determinar las mejores medidas de mitigación de las amenazas y vulnerabilidades que pudieran explotar la materialización de los riesgos y que sus consecuencias atenten contra la continuidad de las operaciones y del negocio.
- Toma de conciencia a las partes interesadas internas y externas sobre la divulgación no autorizada, la modificación, eliminación o destrucción de la información almacenada en los medios.

6.1.2.7 Control de acceso

Se han establecido las medidas de control de acceso para:

- Restringir el acceso a la información y a las instalaciones de procesamiento de la información.
- Asegurar el acceso de usuarios autorizados y evitar el acceso sin autorización a los sistemas y servicios. Responsabilizar a los usuarios del cuidado de su información de autenticación.
- Evitar el acceso sin autorización a los sistemas y aplicaciones.

- Validar, verificar y proveer el acceso lógico a la información (aplicaciones, bases de datos y servicios en general) de forma adecuada.

Cada usuario de los activos de información tendrá acceso a los datos de las aplicaciones informáticas definidas en el alcance del SGSI, de acuerdo con el rol que tenga definido su cargo y al nivel de acceso que le haya asignado la Jefatura Directa. Estos privilegios de acceso entregados a usuarios internos y externos estarán basados en la necesidad de uso, con el mínimo de información de acuerdo con su rol y funciones definidos dentro del alcance del SGSI.

La información a la que tengan acceso el personal es de exclusivo uso para desarrollar sus tareas conforme al alcance definido para el SGSI, de acuerdo con su rol y tareas asignadas, no pudiendo ser entregada ni divulgada de ninguna forma, ni integral ni parcial a terceras partes que no sean sus superiores inmediatos y dentro del contexto del trabajo encomendado. Se podrá acceder a la información de acuerdo con un plan de cuentas de acceso usuario, diseñado y controlado por el contenido en el alcance del SGSI y debidamente aprobado por el Comité de Seguridad de la Información de la empresa.

6.1.2.8 Criptografía

Este control tiene como finalidad asegurar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad o integridad de la información. Para ello será desarrollada una política sobre el Uso de Controles Criptográficos.

6.1.2.9 Seguridad física y ambiental

Este control tiene como finalidad:

- Evitar accesos físicos no autorizados, interferencias contra las instalaciones de procesamiento de la información y la información de la organización contenida en el alcance del SGSI.
- Prevenir pérdidas, daños, hurtos o el compromiso de los activos, así como la interrupción de las actividades de la empresa contenidas en el alcance del SGSI.

Serán consideradas áreas de acceso restringido, las instalaciones en las que se encuentren equipos de procesamiento o comunicaciones de datos, conforme al alcance del SGSI, como son sala de servidores, dependencias donde se encuentran equipos de comunicaciones pertenecientes al cableado estructurado de la red, oficina de administradores y monitoreo, soporte, estaciones de trabajo y las instalaciones que el Comité de Seguridad de la Información determine deban ser de acceso restringido.

6.1.2.10 Seguridad de las operaciones

Este control tiene como finalidad:

- Asegurar la operación correcta y segura de las instalaciones de procesamiento de la información.
- Asegurar que la información y las instalaciones de procesamiento de información están protegidas contra el código malicioso. Proteger en contra de la pérdida de datos.
- Registrar eventos y generar evidencia.
- Asegurar la integridad de los sistemas operacionales.
- Evitar la explotación de las vulnerabilidades técnicas.
- Minimizar el impacto de las actividades de auditoría en los sistemas operacionales.

6.1.2.11 Seguridad de las comunicaciones

Este control tiene como finalidad:

- Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información de apoyo, dirigido a mantener disponible y en correcto funcionamiento las instalaciones definidas en el alcance del SGSI.
- Mantener la Seguridad de la Información transferida dentro del alcance del SGSI y con cualquier entidad externa.

El Gerente de Operaciones gestiona el apoyo, servicios informáticos y de Seguridad de la Información, a las áreas definidas en el alcance SGSI, de acuerdo con lo establecido por el Comité de Seguridad de la Información de la empresa.

A su vez, el Comité de Seguridad de la Información definirá los procedimientos a seguir en la Gestión de Incidentes de Seguridad, que serán implementados por las áreas contenidas en el alcance del SGSI, con la coordinación del Jefe de Seguridad.

Se realizan auditorías internas, conforme a un cronograma establecido por la empresa en función de las necesidades.

Se deben implementar mecanismos de protección preventiva y activa contra software maliciosos, que pudiesen penetrar en forma física y/o lógica a la red o estaciones de trabajo.

La información de los sistemas y configuraciones de los servidores de servicios importantes para las funciones del área contenida en el alcance del SGSI, se realizan respaldos periódicos, conforme a lo definido por el Comité de Seguridad de la Información.

Para asegurar un adecuado uso de los servicios informáticos por parte de los usuarios internos o externos del área definida en el alcance del SGSI, ésta propone normas de uso de los servicios que estén a disposición del personal o de otras instituciones que hacen uso de los activos de la información contenidos en el alcance del SGSI, las que deberán ser aprobadas por el Comité de Seguridad de la Información.

6.1.2.12 Adquisición, desarrollo y mantenimiento de los sistemas de información

Este control tiene como finalidad:

- Asegurar que la Seguridad de la Información es parte integral de los sistemas de información en todo el ciclo.
- Asegurar que la Seguridad de la Información está diseñada e implementada dentro del ciclo de desarrollo de los sistemas de información.
- Asegurar la protección de los datos usados para prueba.

Todo Activo de Información con alcance al SGSI será evaluado por el Comité de Seguridad conforme a un análisis de riesgos, de manera de considerar antes de la compra, los requerimientos de seguridad que correspondan a tales activos de información.

Todo software operacional debe ser controlado, administrado y mantenido en una biblioteca técnica, junto a todas sus actualizaciones. Software computacional,

compilaciones de datos, adaptaciones y cualquier documento relacionado con ello, son propiedad de la empresa, en caso de aquellos realizados por personal de la empresa, en el desempeño de sus funciones, ya sea porque éstos se construyesen en forma individual o colectiva.

Los activos de la información identificados como importantes para la continuidad de las operaciones y del negocio en el alcance del SGSI, deben contar con contrato de mantenimiento y/o soporte con los proveedores que correspondan, de manera de asegurar su funcionamiento o reemplazo de acuerdo con niveles de servicio requeridos y su actualización.

6.1.2.13 Relación con los proveedores

Este control tiene como finalidad:

- Asegurar la protección de los activos de la organización a los que tienen acceso los proveedores.
- Mantener un nivel acordado de Seguridad de la Información y entrega del servicio, en línea con los acuerdos del proveedor.
- Gestión de seguridad de proveedores de servicio en la nube.

6.1.2.14 Gestión de los incidentes de seguridad de la información

Este control tiene como finalidad asegurar un enfoque consistente y eficaz sobre la gestión de los incidentes de la seguridad de la información, incluida la comunicación sobre eventos de seguridad y vulnerabilidades.

6.1.2.15 Aspectos relacionados con la seguridad de la información en la gestión de la continuidad del negocio

Este control tiene como finalidad:

- Incorporar la Continuidad de la Seguridad de la Información en los Sistemas de Gestión de Continuidad de Negocio de la organización.
- Asegurar la disponibilidad de las instalaciones de procesamiento de la información.

- Minimizar el impacto causado por interrupciones en las actividades ejecutadas dentro del alcance del SGSI, protegiendo los procesos críticos de eventos significativos funestos que pudieran presentarse.

Se establece una estrategia, aprobada por el Comité de Seguridad de la Información, que asegure continuidad de las operaciones y del negocio contenidos en el alcance del SGSI, considerados como procesos críticos. Así mismo, deberá gestionar los planes de contingencia, conforme a la estrategia definida.

El Jefe de Seguridad asumirá la responsabilidad de ejecución de la planificación de contingencia que permita asegurar la continuidad de los procesos críticos.

6.1.2.16 Cumplimiento

Este control tiene como finalidad:

- Evitar incumplimientos de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas con la Seguridad de la Información y todos los requisitos de seguridad.
- Asegurar que la Seguridad de la Información se implemente y funcione de acuerdo a las políticas y procedimientos de la organización.
- Impedir posibles infracciones o violaciones a las normas, reglamentos, contratos y requisitos de Seguridad de la Información que se establezcan como parte de la implementación definida para el alcance del SGSI.

Cualquier transgresión de cualquiera de los puntos establecidos en la presente Política de Seguridad de la Información de la empresa, dará lugar a la aplicación de sanciones disciplinarias.

6.1.2.17 Seguridad en pantalla clara y escritorio despejado

Este control tiene como finalidad del establecimiento de controles para el manejo de información clasificada como confidencial o secreta, plantea la necesidad de mantener los escritorios y pantallas limpias y despejadas a fin de evitar el daño o acceso no autorizado, así como facilitar a los usuarios de la información la transmisión y la promoción de toma de

conciencia sobre las buenas prácticas para mantener los escritorios y pantallas limpias, como gestionar los equipos compartidos, el manejo seguro de salas y pizarras, así como la ubicación de los equipos en forma segura.

6.1.2.18 Política de propiedad intelectual

Este control tiene como finalidad garantizar el cumplimiento de los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos patentados.

6.1.2.19 Dispositivos móviles y trabajo remoto

Este control tiene como finalidad implementar medidas de seguridad cuando el personal trabaja de forma remota para proteger la información a la que se accede, procesa o almacena fuera de las instalaciones de la organización y gestiona la seguridad de la información cuando el personal está trabajando de forma remota.

6.1.2.20 Gestión de medios de almacenamiento extraíbles

Este control tiene como finalidad de gestionar los medios de almacenamiento a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización.

6.1.2.21 Copias de seguridad

Este control tiene como finalidad de mantener copias de respaldo de la información a fin de permitir la recuperación en caso de pérdidas, así como abordar los requisitos de seguridad de la información y retención de datos de la organización.

6.2 Contexto Normativo

- La presente Política de ECERT debe cumplir los requerimientos de la norma internacional ISO 9001 vigente, ISO/IEC 27001 vigente y con las regulaciones que el Ministerio de Economía, Fomento y Turismo, en adelante MINECON, dicte para el desarrollo de la actividad de certificación de firma electrónica en forma acreditada.

- Esta Política, las normas, procedimientos y demás documentos complementarios, deben mantener coherencia con los procesos, los objetivos, indicadores y los requerimientos del negocio.
- Esta Política debe ser complementada con las demás políticas de ECERT, en especial con las relativas a la Gestión de la Calidad y de la Seguridad de la Información.

6.3 Publicación

- El Gerente General de ECERT debe asegurar los mecanismos para que todas las políticas, en especial la presente y sus futuras modificaciones sean conocidas y estén a disposición permanentemente por todos los directores, ejecutivos y colaboradores y sean dadas a conocer a las partes interesadas pertinentes, inclusive los proveedores, en el contexto de los servicios que le sean prestados a ECERT.

6.4 Sensibilización y Capacitación

- El Gerente General de ECERT reconoce como tareas prioritarias la sensibilización, capacitación y entrenamiento del personal, en materias de las indicadas en la presente Política.
- Los ejecutivos de ECERT deben crear mecanismos para que esta política, las normas y sus procedimientos, sean conocidos y considerados permanentemente por todos los integrantes de la organización, asegurándose que los colaboradores asumen y comprenden sus responsabilidades. Estas acciones estarán contenidas en las actividades de capacitación anual al personal de ECERT.
- Los ejecutivos de ECERT deben asegurar que todos los colaboradores cuenten con una inducción y sean capacitados en materias de esta política, manteniendo un canal de comunicación formal para informar a toda la organización respecto a los avances, logros y novedades en la materia, con el objetivo de crear una cultura de calidad dentro de la Organización.

6.5 Incumplimiento

- Ante la ocurrencia de algún incumplimiento a las medidas orientadas a resguardar la presente política, el usuario que lo detecte debe informar a la brevedad a su jefatura directa y al Comité Sistema de Gestión, quienes analizarán el incumplimiento y deben gestionar las medidas necesarias para minimizar los potenciales daños a la empresa y lograr el cumplimiento integral de esta política, evitando que se reiteren situaciones similares.
- Todo colaborador tiene la obligación de notificar cualquier actividad o situación que afecte o pueda afectar lo dispuesto en la presente Política. Dicha notificación se debe registrar conforme al procedimiento de y Acciones Correctivas y de Mejora.
- Los incumplimientos graves, es decir, aquellos que afecten a los clientes, y/o a los clientes de los clientes y/o que manifiesten como quejas del cliente o del MINECON, deben ser informados al Gerente General.

6.6 Sanciones

- Al colaborador que contravenga lo indicado en esta Política y/o los documentos relacionados a la misma, se le debe aplicar lo establecido en el SGI-F-301-0019 - Reglamento Interno de Orden, Higiene y Seguridad, en cuanto a sanciones y multas.
- Con relación al personal externo y/o proveedores que no cumplan con lo indicado en esta Política, dependiendo del tipo de incumplimiento se debe amonestar o rescindir el contrato.

7 CONTROL DE VERSIONES

Control de versiones		
Versión	**Fecha**	**Descripción**
0	17-04-2025	• Se crea documento en nuevo gestor documental IS Contacto.

1	30-04-2025	• Se reemplaza la palabra "Modelo" por "General" y la palabra "requerimientos" por "Requisitos".
2	27-05-2026	• Debido a Auditoría Interna de ISO 9001:2015, se estandariza el formato de la información documentada. • Se reemplaza “e-certchile” y “E-Cert” por “ECERT”. • Se incorporan cláusulas de cumplimiento normativo en ciberseguridad (Ley N° 21.663 – Agencia Nacional de Ciberseguridad) y protección de datos personales (Leyes N° 19.628 y 21.719), incluyendo obligaciones legales y derechos ARCO. • Se actualiza el documento en el marco de la revisión anual programada.

Fin del documento