POLÍTICA

General de Seguridad de la Información

Norma(s) que Aplican	Referencia Normativa	Área Proceso	Código
ISO 9001:2015	5.2 Política	GER: Gerencia General	PO-GER-0003
ISO/IEC 27001:2022	Control A.5.1 Políticas de seguridad	GPQ27: Gestión seguridad de la información ISO 27001	
G.A.M. FEA	4.9 Requisito PS02 - Política de seguridad		
G.A.M. BIO	4.6 Requisito PS02 - Política de seguridad		
G.A.M. TSA	4.6 Requisito PS02 - Política de seguridad		

Nombre Aprobador	Fecha Creación	Fecha Aprobación	Fecha Vigencia	Revisión	Primera Revisión
Alfredo Guardiola	31-07-2025	31-07-2025	14-08-2025	6	11-01-2021

Propietario de la Información	Propietario del Proceso	Propietario de Sistema	Propietario del Riesgo	Clasificación de la Información
Jefe de Seguridad	Jefe de Seguridad	Gerente General	Chief Technology Officer	Público

CONTENIDO

1. INTRODUCCIÓN

La seguridad de la información es un pilar fundamental en la gestión operativa y estratégica de ECERT. En un entorno global en constante cambio y donde las amenazas cibernéticas evolucionan rápidamente, proteger la integridad, confidencialidad y disponibilidad de la información se convierte en un compromiso esencial. La Política General de Seguridad de la Información establece los lineamientos y directrices que guían la implementación, mantenimiento y mejora continua del Sistema de Gestión Integrado (SGI) de ECERT, alineado con los estándares de la ISO/IEC 27001:2022.

Esta política refleja el compromiso de la alta dirección y de todos los colaboradores de ECERT para garantizar la seguridad de los activos de información y cumplir con los requisitos legales, normativos y contractuales aplicables. Asimismo, proporciona un marco para el establecimiento de objetivos de seguridad que aseguren la protección de la información y la continuidad de los procesos críticos, fortaleciendo la confianza de nuestros clientes, socios y partes interesadas.

ECERT se compromete a implementar controles adecuados y promover una cultura de seguridad proactiva, asegurando que todos los niveles de la organización comprendan y participen en la protección de la información. La mejora continua y la adaptación a las mejores prácticas internacionales son parte integral de nuestra política, reforzando la capacidad de la organización para enfrentar nuevos desafíos en materia de ciberseguridad.

2. OBJETO

El propósito de esta Política es:

- Establecer los lineamientos generales de ECERT para la protección integral de la confidencialidad, integridad y disponibilidad de la información, tanto de la organización como de terceros con los que se interactúa.

- Definir directrices claras para la gestión de la seguridad de la información, alineadas con los principios y requisitos de la norma ISO/IEC 27001:2022, asegurando un enfoque actualizado y eficaz en la protección de los datos y activos informáticos.
- Reducir y gestionar los riesgos asociados a los activos de información bajo la gestión de ECERT, a través de controles y medidas preventivas y reactivas.
- Promover e instaurar una cultura sólida de Seguridad de la Información dentro de ECERT y entre los terceros con los que la organización colabora, fortaleciendo el compromiso de todos los actores involucrados en el mantenimiento de un entorno seguro y confiable.

3. ALCANCE

El alcance de esta Política abarca a toda la organización de ECERT, conforme a lo definido en el Campo de Aplicación del Manual del Sistema de Gestión Integrado. Esta política se extiende a todos los procesos, productos y servicios que la empresa desarrolla, así como a los directores, ejecutivos y colaboradores en todos los niveles. Además, incluye a todas las partes interesadas pertinentes con las que ECERT interactúa, garantizando que la seguridad de la información sea un compromiso compartido y mantenido en todas las áreas y actividades de la organización.

La política se aplica a toda la infraestructura tecnológica, física y lógica, así como a cualquier medio o entorno donde se almacene, procese o transmita información. Esto incluye los activos digitales y físicos, tanto internos como aquellos compartidos o gestionados por terceros, asegurando una cobertura integral de la gestión de la seguridad de la información y la protección de los datos en toda la cadena de valor de la organización.

4. DEFINICIONES

- **Activo de Información**: Aquello que tenga valor y es importante para el ECERT, sean documentos, sistemas o personas y todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la organización. Se distinguen tres niveles:
    - La Información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.)
    - Los equipos, sistemas e infraestructura que soportan o contienen esta información.
    - Las personas que utilizan la información, y que tienen el conocimiento de los procesos de la organización.
- **Colaborador:** Toda persona que tenga un vínculo contractual de trabajo con ECERT, sea éste indefinido, a plazo fijo o a honorarios.
- **Política:** Directriz u orientación general expresada formalmente por la administración de ECERT.
- **Procedimiento:** Sucesión cronológica de acciones concatenadas entre sí, para la realización de una actividad o tarea específica dentro del ámbito de los controles, en este caso, de Seguridad de la Información.
- **Riesgo:** Es la posibilidad que ocurra un evento que afecte adversamente el logro de los objetivos de ECERT. Se mide combinando las consecuencias del evento (impacto) y su probabilidad de ocurrencia.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede dar lugar a daños a un sistema o proceso.
- **Vulnerabilidad:** Debilidad de un activo o grupo de activos que puede ser materializada por una o más amenazas.
- **Evento de Seguridad de la Información:** Actividad o serie de actividades sospechosas que amerita ser analizada desde la perspectiva de la Seguridad de la Información.

- **Incidente de Seguridad de la Información:** Evento o serie de eventos de Seguridad de la Información, no deseados o inesperados, que compromete la Seguridad de la Información y amenaza la operación del negocio.
- **Confidencialidad:** Propiedad de la información que determina que sólo podrá ser accedida por personas, entidades o procesos debidamente autorizados.
- **Integridad:** Propiedad de la información según la cual sólo puede ser modificada, agregada o eliminada por las personas o sistemas autorizados para cada proceso, de tal forma de salvaguardar la exactitud y completitud de los activos de información.
- **Disponibilidad:** Propiedad de la información según la cual es accesible y utilizable oportunamente por las personas o sistemas o procesos autorizados, en el formato requerido para su procesamiento.

5. PRINCIPIOS GENERALES

5.1. Deber del Colaborador

Todos los colaboradores de ECERT tienen la responsabilidad de proteger la información y cumplir con las políticas de seguridad establecidas. La rendición de cuentas se refuerza a través de formaciones periódicas, evaluaciones de desempeño y revisiones de cumplimiento.

5.2. Aplicación a Terceros

ECERT garantiza que las relaciones con terceros, incluidos proveedores y socios, cumplan con las normas de seguridad internas. Los acuerdos de confidencialidad y las evaluaciones de riesgo se aplican a todas las colaboraciones para proteger la información compartida y evitar brechas de seguridad.

5.3. Cumplimiento Normativo

Se establecen y se consideran como parte de este marco normativo de Seguridad de la Información, Políticas Específicas de Seguridad de la Información de ECERT, de acuerdo a los dominios definidos en la norma ISO 27002, a saber:

- Controles de Organización.
- Controles de Personas
- Controles Físicos
- Controles Tecnológicos

5.4. Confidencialidad

En ECERT, la confidencialidad de la información es una prioridad. Se implementan controles de acceso estrictos para asegurar que solo el personal autorizado tenga acceso a la información sensible, protegiendo los datos de los clientes y de la propia organización. Esto se logra mediante políticas de acceso y el uso de tecnologías de cifrado para proteger la información en tránsito y en reposo.

5.5. Integridad

ECERT garantiza la precisión y la consistencia de la información a lo largo de su ciclo de vida. Para ello, se implementan auditorías regulares y medidas de control de versiones en los documentos críticos, así como validaciones y pruebas periódicas para confirmar la integridad de los sistemas y datos.

5.6. Disponibilidad

Asegurar la disponibilidad de la información es esencial para los servicios de ECERT. Por ello, se implementan estrategias de respaldo, planes de continuidad del negocio y pruebas de recuperación ante desastres para minimizar los tiempos de inactividad y garantizar la prestación continua de servicios a los clientes.

5.7. Autenticidad

ECERT adopta mecanismos sólidos de autenticación multifactor (MFA) y el uso de certificados digitales para validar la identidad de los usuarios y garantizar que las transacciones electrónicas y accesos sean legítimos. Esto protege la autenticidad de las operaciones y asegura que solo personal verificado acceda a los sistemas.

5.8. No Repudio

En ECERT, el principio de no repudio se gestiona a través del registro detallado de todas las acciones en sistemas críticos. Esto garantiza que las acciones realizadas puedan ser atribuidas de forma confiable a los individuos responsables, evitando posibles disputas o negaciones de participación.

5.9. Cultura de Seguridad

ECERT promueve activamente una cultura de seguridad en la que los colaboradores son conscientes de los riesgos de la información y participan activamente en la protección de los datos. Programas de sensibilización y capacitaciones continuas refuerzan este compromiso.

5.10. Adaptabilidad

La política de seguridad de ECERT es revisada regularmente para adaptarse a nuevos riesgos, cambios regulatorios y avances tecnológicos. La capacidad de la organización para evolucionar y responder a amenazas emergentes es clave para mantener un entorno seguro.

6. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

Los objetivos de seguridad de la información en ECERT son un componente fundamental de su Sistema de Gestión Integrado (SGI). Estos objetivos están alineados con los requisitos de la ISO 27001:2022 y tienen como propósito garantizar la protección de la información y la

continuidad de los servicios. Los objetivos se miden y revisan periódicamente para asegurar su cumplimiento y efectividad.

6.1. Objetivo general Sistema de gestión Integrado

Proteger y asegurar los activos de información de ECERT mediante la implementación de controles adecuados, gestionando eficazmente los riesgos de seguridad de la información, asegurando el cumplimiento normativo, y promoviendo la mejora continua del Sistema de Gestión de Seguridad de la Información, con el fin de asegurar la confidencialidad, integridad y disponibilidad de los servicios de firma electrónica avanzada.

6.2. Objetivos específicos del sistema de gestión Integrado

- **Asegurar la protección de los activos de información:** Proteger los activos de información asegurando su confidencialidad, integridad y disponibilidad mediante la implementación y actualización continua de controles de seguridad, gestión de riesgos y monitoreo de incidencias.
- **Gestionar los riesgos de seguridad de la información:** Gestionar eficazmente los riesgos de seguridad de la información, garantizando que al menos el 75% de los riesgos identificados se mantengan en niveles aceptables, mediante análisis, seguimiento y verificación de controles.
- **Cumplir con los requisitos legales y regulatorios:** Cumplir con los requisitos legales y regulatorios aplicables a la organización, actualizando y revisando la matriz de requisitos legales de forma periódica para evitar sanciones y garantizar el cumplimiento normativo.
- **Promover la mejora continua del SGSI:** Fomentar la mejora continua del SGSI, implementando acciones correctivas y preventivas que aseguren la eficacia del sistema, con un 80% de acciones cerradas y evaluaciones periódicas a través de auditorías internas.

- **Fortalecer la cultura de seguridad de la información a través de la capacitación y sensibilización:** Fortalecer la cultura de seguridad de la información, asegurando que al menos el 85% del personal reciba capacitación adecuada y comprenda sus responsabilidades para salvaguardar los activos de información.

6.3. Indicadores de objetivos específicos del sistema de gestión integrado

En ECERT, los indicadores para medir los objetivos específicos de seguridad de la información son esenciales para evaluar el cumplimiento y la efectividad de las estrategias establecidas. Estos indicadores permiten un monitoreo constante y proporcionan datos que respaldan la mejora continua del Sistema de Gestión Integrado (SGI).

Cada objetivo específico de seguridad de la información en ECERT está asociado a indicadores clave que permiten evaluar su desempeño y cumplimiento. Los detalles completos de estos indicadores, incluyendo su definición, método de cálculo, frecuencia de monitoreo y responsables, se encuentran documentados en el Manual del Sistema de Gestión Integrado.

7. COMPROMISOS DE LA ALTA DIRECCIÓN

La Alta Dirección se compromete a liderar y promover un entorno de trabajo seguro, enfocado en la protección de los activos de información de la organización. Este compromiso se refleja en los siguientes principios y acciones clave:

- **Liderazgo Activo y Ejemplar:** La Alta Dirección asume un papel de liderazgo activo, fomentando una cultura organizacional que priorice la seguridad de la información y sirviendo como modelo a seguir en la implementación de prácticas seguras en todos los procesos y operaciones.
- **Cumplimiento Normativo y de Buenas Prácticas:** ECERT asegura el cumplimiento de los requisitos legales y reglamentarios aplicables, así como de los estándares

internacionales de seguridad de la información, incluidos los principios de la ISO/IEC 27001:2022 y otras normativas relevantes.

- **Compromiso con la Mejora Continua:** La Alta Dirección promueve la mejora continua del Sistema de Gestión Integrado (SGI) mediante revisiones periódicas, análisis de resultados, auditorías internas y la implementación de medidas correctivas y preventivas que optimicen los procesos de seguridad.
- **Integración de la Seguridad en Todos los Procesos:** Se garantiza que la seguridad de la información esté presente de manera integral en los procesos de negocio, manteniendo la confidencialidad, integridad y disponibilidad de la información como principios rectores.
- **Capacitación y Concienciación:** La Alta Dirección se asegura de que todos los colaboradores estén informados, capacitados y comprometidos con las políticas y procedimientos de seguridad de la información, fomentando un entendimiento sólido y una cultura de responsabilidad compartida.
- **Gestión Proactiva de Riesgos:** La identificación, evaluación y gestión de riesgos relacionados con la seguridad de la información son prioridades para la Alta Dirección, que supervisa la implementación de controles adecuados para mitigar las amenazas potenciales y proteger los activos críticos.
- **Compromiso con las Partes Interesadas:** La Alta Dirección reconoce la importancia de mantener la confianza de los clientes, socios, reguladores y otras partes interesadas, asegurando la protección de la información y promoviendo la transparencia en la gestión de la seguridad.
- **Revisión y Actualización Constante:** La política será revisada y actualizada periódicamente para adaptarse a los cambios normativos, tecnológicos y del entorno, garantizando así su relevancia y efectividad.

Estos compromisos de la Alta Dirección refuerzan la intención de ECERT de establecer un entorno seguro y confiable que respalde los objetivos estratégicos de la organización,

protegiendo la información y los activos críticos mientras se mantiene la confianza de todas las partes interesadas.

8. ROLES Y RESPONSABILIDADES

Para el cumplimiento y sostenibilidad de la Política General de Seguridad de la Información de ECERT, se definen las siguientes responsabilidades asignadas a los principales roles de la organización:

- Gerente General:
    - Asegurar el establecimiento, implementación y mantenimiento de esta Política, así como los objetivos y medidas que de ella se deriven.
    - Garantizar que la gestión de riesgos y oportunidades esté alineada con el propósito y el contexto estratégico de ECERT, apoyando la dirección y objetivos generales de la organización.
    - Proporcionar un marco de referencia claro para establecer objetivos de seguridad de la información e indicadores de desempeño.
    - Asignar los recursos necesarios y promover las competencias adecuadas en el equipo para la gestión efectiva de la seguridad de la información y la mitigación de riesgos.
    - Revisar y aprobar el alcance y contexto del SGSI y los criterios de gestión de riesgos, así como la lista de riesgos inherentes y los planes de tratamiento de riesgos.
    - Promover y fomentar una cultura de seguridad de la información y una actitud preventiva en todos los niveles de la organización.
    - Revisar y aprobar la política al menos una vez al año, actualizándola según los cambios normativos o de contexto.
    - Informar de manera periódica al Directorio y a los altos ejecutivos sobre los riesgos relacionados con la seguridad de la información y las medidas de mitigación adoptadas.

- Comité de Sistema de Gestión Integrado:
    - Implementar y supervisar el cumplimiento de esta política, realizando un seguimiento constante de la gestión de riesgos y oportunidades en cada sesión del comité.
    - Proponer y validar la metodología de gestión de riesgos y oportunidades y asegurar su implementación efectiva, incluyendo la definición del marco de referencia, la identificación, análisis, valoración y tratamiento de riesgos.
    - Coordinar la actualización y valoración de los riesgos de ECERT, apoyando a los responsables en sus procesos de gestión.
    - Dar visibilidad y reportar a las partes interesadas internas sobre los avances y resultados de la gestión de riesgos y oportunidades.
    - Asegurar la existencia y asignación de Propietarios de Procesos, Riesgos y Activos de Información.
- Propietario del Proceso, Riesgo o Activo de Información:
    - Implementar, supervisar y asegurar el cumplimiento de políticas, normas y procedimientos en sus áreas de responsabilidad.
    - Identificar riesgos y oportunidades relacionados con sus procesos y definir e implementar los planes de mitigación o potenciación adecuados.
    - Monitorear los indicadores de desempeño asociados a sus procesos y realizar las acciones necesarias para la mejora continua.
    - Aprobar la identificación, valoración y tratamiento de los riesgos en coordinación con el Comité de Seguridad de la Información.
- Auditores Internos:
    - Realizar auditorías independientes anuales o según lo requieran las circunstancias, evaluando la efectividad del SGSI y el cumplimiento de esta Política y los procedimientos relacionados.
    - Reportar hallazgos y sugerir mejoras para el fortalecimiento del SGSI.
- Usuarios Internos y Externos de ECERT:

- Cumplir con los lineamientos establecidos en esta Política y en otros documentos relacionados con la seguridad de la información.
- Informar de manera inmediata cualquier incidente o situación sospechosa que pueda comprometer la seguridad de la información.
- Participar activamente en programas de capacitación y sensibilización promovidos por la organización.

9. CUMPLIMIENTO DE REQUISITOS APLICABLES

- La presente Política de ECERT debe cumplir con los requerimientos establecidos por la norma internacional **ISO/IEC 27001:2022** y las normas complementarias de la familia **ISO 27000**, así como con las regulaciones emitidas por el **Ministerio de Economía, Fomento y Turismo (MINECON)** de Chile, aplicables a las actividades de certificación de **"Firma Electrónica Avanzada"**, **"Sellado de Tiempo"** y **"Biometría"**, y las disposiciones emitidas por el **Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI)** en Perú, correspondientes a las actividades de **"Entidad de Registro"** y **"Sistema de Intermediación Digital"**, áreas en las que la empresa se encuentra acreditada.
- Esta Política, junto con las normas, procedimientos y demás documentos de apoyo, debe estar en plena coherencia con los procesos de negocio, objetivos estratégicos, indicadores de desempeño y otros requisitos aplicables a la operación de ECERT, asegurando que se integren y alineen con la visión y misión de la organización.
- Esta Política debe complementarse y aplicarse de manera conjunta con las demás políticas internas de ECERT, especialmente aquellas relacionadas con la Gestión de la Calidad, la Gestión de Riesgos y la Seguridad de la Información, garantizando una estructura de cumplimiento integral y coordinada en todas las áreas de la empresa.

10.MEJORA CONTINUA

El compromiso de ECERT con la mejora continua del Sistema de Gestión de Integrado (SGI) es fundamental para mantener la eficacia y relevancia del sistema. Para ello, se adoptan las siguientes estrategias y enfoques:

- Monitoreo constante de los procesos de seguridad de la información para identificar áreas de mejora.
- Realización de auditorías internas periódicas y análisis de resultados para detectar oportunidades de optimización.
- Implementación de planes de acción basados en los hallazgos de auditorías y revisiones de desempeño.
- Fomento de la participación activa de los colaboradores en la identificación y propuesta de mejoras a los procesos de seguridad de la información.
- Evaluación de nuevas tecnologías y prácticas del sector para garantizar que el SGI evolucione en línea con los cambios del entorno.

11.COMUNICACIÓN Y DIVULGACIÓN

La política de seguridad de la información debe ser comunicada eficazmente dentro y fuera de la organización. Los mecanismos de comunicación y divulgación incluyen:

- Publicación de la política en un repositorio accesible a todos los colaboradores y directivos.
- Reuniones informativas y boletines internos para divulgar las actualizaciones y novedades de la política.
- Aseguramiento de que las partes interesadas externas, como socios y proveedores, tengan acceso a la política cuando sea relevante para sus interacciones con ECERT.

12.DOCUMENTACIÓN Y DISPONIBILIDAD

La política de seguridad de la información debe estar documentada y disponible de manera que todos los miembros de la organización puedan consultarla fácilmente. Los requisitos sobre la documentación incluyen:

- La política debe estar almacenada en el Sistema de Gestión Documental de ECERT y actualizada con cada revisión.
- Se debe garantizar la disponibilidad de la política a todos los colaboradores y directivos.
- Las versiones más recientes de la política deben ser accesibles a las partes interesadas externas, si es pertinente, a través de un portal de proveedores o mediante solicitud.

13.SENSIBILIZACIÓN Y CAPACITACIÓN

El éxito de la política depende de que todos los colaboradores estén plenamente informados y capacitados. Las iniciativas de sensibilización y capacitación incluyen:

- Programas de inducción para nuevos colaboradores que aborden los principios y directrices de la política.
- Capacitaciones anuales obligatorias para actualizar a los colaboradores sobre sus responsabilidades y sobre las mejores prácticas de seguridad de la información.
- Simulacros y ejercicios prácticos para evaluar la comprensión de la política y preparar al personal para responder a incidentes de seguridad.
- Creación de campañas de sensibilización que refuercen la importancia de la seguridad de la información en las actividades cotidianas.

14.SANCIONES

El incumplimiento de la política de seguridad de la información puede poner en riesgo a la organización y a sus partes interesadas. Por ello:

- Las infracciones menores se abordarán con medidas correctivas que promuevan la mejora, mientras que los incumplimientos graves podrán resultar en sanciones disciplinarias que van desde advertencias hasta la rescisión del contrato, según lo estipulado en el Reglamento Interno de Orden, Higiene y Seguridad.
- Las infracciones cometidas por proveedores y personal externo se gestionarán mediante amonestaciones o la terminación del contrato, dependiendo de la gravedad del incumplimiento.

15.REVISIÓN Y ACTUALIZACIÓN

Para garantizar la vigencia y adecuación de la política:

- La política debe revisarse al menos una vez al año o cuando haya cambios significativos en la legislación, la estructura organizacional o el entorno de amenazas.
- Las revisiones estarán a cargo del Comité Sistema de Gestión Integrado con aprobación final del Gerente General.
- Cualquier cambio en la política será comunicado de manera oportuna a todos los colaboradores y partes interesadas pertinentes.

16.REFERENCIAS NORMATIVAS

Esta política se sustenta en las siguientes normativas y estándares:

- ISO/IEC 27001:2022 – Sistemas de Gestión de Seguridad de la Información – Requisitos.
- ISO/IEC 27002:2022 – Controles de seguridad de la información.
- Otras políticas internas de ECERT que complementan y refuerzan los lineamientos establecidos en esta política.

17.CONTROL DE VERSIONES

Control de versiones		
Versión	**Fecha**	**Descripción**
1	14-02-2021	Migración ISO Easy
2	08-07-2022	Revisión Anual IAO 2022
3	30-01-2023	Se reemplaza e-certchile por ECERT
4	24-07-2024	Revisión Anual IAO 2024 Se ajustan objetivos de seguridad Se incluyen referencias de la política
5	11-11-2024	Se migra documento desde la versión ISO 27001:2013 a ISO 27001:2022
6	24-06-2025	Revisión y actualización IAO 2025

Fin del documento