POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Contenido

1. INTRODUCCIÓN

La Empresa Nacional de Certificación Electrónica S.A., en adelante e-certchile, es una filial de la Cámara de Comercio de Santiago A.G., que se encuentra acreditada ante la Subsecretaría de Economía y Empresas de Menor Tamaño para proveer servicios de certificación de firma electrónica avanzada. Adicionalmente, haciendo sinergia entre sus capacidades tecnológicas y el profundo conocimiento que tiene del mercado se encuentra dedicada a proveer soluciones de valor agregado a través de sus diferentes productos, aplicaciones y servicios, integrando las soluciones de firma electrónica con el ciclo de vida de los documentos electrónicos de forma segura, transparente y eficiente.

A partir de la presente política, la alta dirección de e-certchile reconoce y declara la importancia que tiene para la organización identificar y proteger los activos de información a través de la implementación de un Sistema de Gestión de Seguridad de la Información orientado a definir las directrices que permitan resguardar la confidencialidad, integridad y disponibilidad de la información de la organización y de terceros, asegurando la continuidad del negocio en conjunto con el cumplimiento de las disposiciones legales vigentes.

Esta Política conforma parte del Sistema de Gestión de e-certchile, siendo establecida en base a la Norma Internacional ISO/IEC 27001 y los requerimientos que impone la Subsecretaría de Economía para la acreditación de las certificadoras de firma electrónica avanzada.

Con la finalidad de dar cumplimiento al reglamento interno que se mantiene como prestadora de servicios de certificación, el sistema de gestión de seguridad de la información debe considerar las tecnologías y procedimientos necesarios para el fortalecimiento de los sistemas de protección de las redes internas y externas, claves, respaldo, capacitación del personal u otro elemento que el reglamento requiera, así como también debe evaluar su funcionamiento con las auditorías correspondientes.

2. PROPÓSITO

El propósito de esta política es:

a) Definir lineamientos generales de e-certchile, respecto de la protección de la confidencialidad, integridad y disponibilidad de la información de la organización y de terceros.
b) Establecer directrices, en relación con la gestión de la seguridad de la información tomando como referencia lo establecido en la norma ISO/IEC 27001:2013 “Sistema de Gestión de la Seguridad de la Información - Requisitos”.
c) Minimizar los riesgos que amenazan a los activos de información que gestiona la organización.
d) Implementar y fomentar una cultura de Seguridad de la Información al interior de e-certchile y con terceros con los que se relaciona.

3. ALCANCES

La seguridad de la información es responsabilidad de todos los empleados de e-certchile y también del personal externo que presta servicios a e-certchile, por tal razón, las directivas planteadas en este documento son de conocimiento y cumplimiento obligado para todas las personas a las que la empresa les otorgue acceso a los recursos de información.

La presente Política General de Seguridad de la Información obliga a las Gerencias de e-certchile, quienes son responsables de ponerla en conocimiento de su personal subordinado, así como también de controlar su cumplimiento. El área de Recursos Humanos debe adjuntar una copia del presente documento al contrato de trabajo, de manera que forme parte integral de éste; así como también, facilitar su difusión y entendimiento mediante entrenamiento en seguridad de la información.

4. REFERENCIAS

4.1 Documentos Relacionados

Bajo esta política se sujetan las demás políticas específicas de seguridad de la información de e-certchile, las cuales se encuentran especificadas en la declaración de aplicabilidad del sistema de gestión de seguridad de la información.

- **SGI-PO-01** Política de Gestión Integral de Riesgos.
- **EST-MN-01** Manual de Sistema de Gestión de e-certchile.
- **SGI-FP-07** Ficha de Proceso Gestión de Políticas.
- **RRHH-DG-01** Reglamento Interno de Orden, Higiene y Seguridad.
- **SGI-FP-02** No Conformidades y Acciones Correctivas.

4.2 Definiciones

a) Información

Datos que poseen significado. [ISO 9000:2015, 3.8.2]
Son los datos que individualmente o en su conjunto tienen sentido para quién los accede, los que pueden residir en medios electromagnéticos, físicos o en el conocimiento de las personas como, por ejemplo, puede estar impresa, manuscrita, almacenada electrónicamente, grabada en películas, almacenadas en medios ópticos o electromagnéticos, sistemas de transferencia de archivos y/o transferida en dispositivos de cualquier tipo como pendrives, CD, DVD y similares.

Independiente de la forma en que exista o se transmita la información, siempre debe ser protegida adecuadamente.

b) Seguridad de la Información

Preservación de la confidencialidad (2.12), la integridad (2.40) y la disponibilidad (2.9) de la información. [ISO 27000:2013, 2.33]

Es el conjunto de medidas que protegen el recurso de información de una amplia gama de amenazas con el fin de asegurar la continuidad del negocio, minimizar el daño y maximizar las oportunidades de negocio y el retorno de la inversión.

c) Confidencialidad

Propiedad de la información por la que se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados. [ISO/IEC 27000:2014, 2.12]

Asegurar que la información es accesible sólo por las personas autorizadas a tener acceso.

d) Integridad

Propiedad (de la información) de exactitud y completitud. [ISO/IEC 27000:2014, 2.40].

Salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento.

e) Disponibilidad

Propiedad (de la información) de ser accesible y estar listo para su uso a demanda de una entidad autorizada. [ISO/IEC 27000:2014, 2.9]

Asegurar que los usuarios autorizados tengan acceso a la información y los activos asociados cuando sean requeridos.

f) Usuario

Es toda persona a la cual se le concede autorización para acceder a la información y a los sistemas de e-certchile. Un usuario puede ser interno o externo a la empresa.

g) Buen Uso

Se entiende por "buen uso" de los sistemas e información de e-certchile, el uso acorde a lo estipulado en las políticas, estándares y procedimientos de la empresa. e-certchile se reserva el derecho de tomar medidas administrativas para sancionar al personal en caso de existir evidencias de no-cumplimiento o transgresión de lo establecido.

h) Propiedad de la Información

Es el usuario responsable de la información y de los procesos que la manipulan sean estos mecánicos o electrónicos. Las funciones principales son:

- Definir qué datos son correctos.
- Definir los procedimientos de captura, procesos y salidas de la información.
- Definir los controles que deben existir para asegurar el correcto proceso de la información. Autorizar o revocar el acceso a la información por los usuarios.
- Definir los roles y atributos de acceso de los usuarios.
- Asegurar por el cumplimiento de lo establecido anteriormente.

i) Propietario del Riesgo

Persona o entidad que tiene la responsabilidad y autoridad para gestionar un riesgo. [ISO/IEC 27000:2014, 2.78]

j) Riesgo

Efecto de la incertidumbre sobre la consecución de los objetivos. [ISO/IEC 27000:2014, 2.68]

k) Gestión del Riesgo

Actividades coordinadas para dirigir y controlar la organización con relación al riesgo. [ISO/IEC 27000:2014, 2.76]

l) Parte Interesada

Persona u organización que puede afectar, verse afectada, o percibirse como afectada por una decisión o actividad. [ISO/IEC 27000:2014, 2.82]

m) Control

Medida que modifica un riesgo. [ISO/IEC 27000:2014, 2.16]

n) Alta Dirección

Persona o grupo de personas que dirige y controla una organización al más alto nivel. [ISO/IEC 27000:2014, 2.84]

5. ROLES Y RESPONSABILIDADES

ROL	RESPONSABILDAD
Usuario e-certchile o Usuario externos	Dar cumplimiento a los lineamientos establecidos en esta política, además son responsables de reportar los incidentes de seguridad de la información.
Administradores de Sistema	Cumplir las normas definidas en esta política.
Oficial de Seguridad de la Información	Responsable de la gestión del sistema de seguridad de la información y de la gestión de incidentes de seguridad de la información.
Mesa de Servicios TI	Gestionar los servicios requeridos por los usuarios de la información, mediante la herramienta de gestión de TI.
Responsable de la Información	Verificar la integridad de la información en caso de restauración.
Alta Dirección	Responsable de monitorear y gestionar en forma integral la Gestión de Seguridad.
Propietario del Proceso	Persona o entidad que tiene la responsabilidad y autoridad para gestionar un proceso.
Propietario del Riesgo	Persona o entidad que tiene la responsabilidad y autoridad para gestionar un riesgo.

6. OBJETIVOS DE LA SEGURIDAD

Para la definición de los objetivos del Sistema de Gestión de Seguridad de la Información, se deben realizar las siguientes actividades:

- Identificación de las tareas esenciales que se deben realizar
- Identificación los recursos claves
- Determinación de responsables
- Establecimiento de un período para el cumplimiento de los objetivos
- Establecimiento de un criterio de evaluación de los resultados

Cada uno de estos puntos es evaluado a partir de los resultados del análisis de riesgos que se genera anualmente. En el proceso de determinación de estos objetivos y de los registros respectivos, es necesario tomar en cuenta los requerimientos aplicables de la seguridad de la información, siendo estos consistentes con la presente política de la seguridad de la información. Una vez establecidos los objetivos, estos deben ser gestionados para dar cumplimiento de sus metas. Dicho documento tiene periodicidad anual y es representativo de los objetivos de la seguridad de la información requeridos por el SGSI.

Los objetivos determinados para el período deben ser comunicados a toda la organización. La comunicación se debe realizarse a través de correo electrónico u otro medio que la organización considere apropiado.

7. RIESGOS

Conocer el impacto que los riesgos de la seguridad de la información tienen sobre la organización a raíz de las amenazas y vulnerabilidades en las que operan los distintos sistemas de información, es una herramienta fundamental para identificar los incidentes que pueden ocurrir en la organización y encontrar las maneras más apropiadas para enfrentarlos.

La organización debe implementar una metodología que permita crear un proceso de evaluación de riegos, de acuerdo con lo siguiente:

- Definir cómo identificar los riesgos que podrían causar la pérdida de confidencialidad, integridad o disponibilidad de la información de la organización
- Definir cómo identificar a los dueños del riesgo
- Definir criterios para evaluar las consecuencias del riesgo y su probabilidad de ocurrencia.
- Definir cómo se calcula el riego.
- Definir el criterio de aceptación de riesgos.

La evaluación de riesgos da lugar a la generación de un plan de tratamiento de riesgos.

8. COMITÉ SISTEMA DE GESTIÓN

Con el objetivo de garantizar el cumplimiento de la Política de Seguridad, e-certchile ha establecido una Estructura Organizacional de Seguridad que contempla la definición de funciones específicas en el ámbito de la seguridad.

E-certchile ha conformado el Comité Sistema de Gestión, el cual se debe encargar de implementar desarrollar y realizar seguimiento a todas las iniciativas e incidentes que se relacionen con la Seguridad de la Información, en especial la Política de Seguridad de la Información, sus ajustes y modificaciones, y está formado por personal de la alta administración de la empresa, conforme a su Estatuto.

Las principales funciones del Comité son:

- Aprobar las Políticas de Seguridad.
- Definir el Sistema de Gestión de Seguridad de la Información.
- Solicitar auditorías, diagnóstico y monitoreo de las políticas y del Sistema de Gestión de Seguridad de la Información.
- Solicitar que se regule el tratamiento de la información desde el punto de vista de la seguridad de algún recurso o proceso que no lo tuviese.
- Asegurar el entrenamiento y capacitación en prácticas de seguridad de la información.

9. DOCUMENTOS DE POLÍTICAS

El presente documento constituye una política de alto nivel, destinada a normar los aspectos más relevantes de la gestión de seguridad de la información, con una vigencia de largo plazo.

Adicionalmente, e-certchile debe desarrollar las políticas de seguridad necesarias para regular, con mayor grado de especificación de detalle, los recursos de información de acuerdo con las disposiciones mencionadas en esta Política General.

9.1 Periodicidad, vigencia y revisión de las Políticas de Seguridad de la Información

La alta dirección de e-certchile es responsable por la presente Política General de Seguridad de la Información, quien debe asegurar que sea de conocimiento de todo su personal subordinado.

Para el caso de personal que se contrate con posterioridad a la fecha de publicación, se le debe adjuntar una copia del documento al contrato, de manera que forme parte integral de éste.

Todas las políticas generadas a partir del establecimiento del Sistema de Gestión de Seguridad de la información tendrán un respectivo dueño correspondiente a su área de injerencia, y estos son responsables de revisar, implementar y actualizar cada documento.

Las Políticas de Seguridad de la información deben ser revisadas anualmente por el Comité de Sistema de Gestión y sus cambios validados por el Gerente General.

10. POLÍTICA

10.1 De la Información Interna

La información que se maneja en E-certchile tiene diferentes niveles de importancia en cuanto riesgo que representa su eventual divulgación, adulteración o indisponibilidad. Por lo anterior, se hace necesario "clasificar" la información según el nivel de daño que se genera si se compromete su confidencialidad, integridad o disponibilidad.

El propietario de la información es responsable de su clasificación y definir las personas que tendrán acceso a ella, debiendo periódicamente revisar la clasificación hecha, con el propósito de mantenerla o modificarla según se estime apropiado.

10.2 De la Información de Clientes y Proveedores

E-certchile, tiene información de sus clientes y proveedores, que son considerados información valiosa y confidencial, y se compromete a tratarlos dando pleno cumplimiento a la normativa legal y la política de tratamiento de datos personales.

10.3 Empresas Externas y Consultores

Las empresas y consultores que presten servicios deben cumplir con las políticas, normas y procedimientos de seguridad de los activos de información de e-certchile.

10.4 De las Auditorías

Con el fin de asegurar por el correcto uso de los recursos de su propiedad, e-certchile se reserva el derecho de auditar en todo momento y sin previo aviso, el cumplimiento de las políticas vigentes y que dicen relación con el acceso y uso que los usuarios hacen de los recursos de información, tanto lógicos como físicos.

10.5 Del compromiso de E-certchile

Con el fin de mantener el nivel de seguridad adecuado, la alta dirección se asegura que:

- Establecer, implementar, mantener y continuamente mejorar el Sistema de Gestión de Seguridad de la Información de acuerdo con los requerimientos de la norma internacional ISO/IEC 27001.

- Utilizar los recursos adecuados y que estén a su alcance para proteger sus recursos de información y capacitar a sus empleados en materias de seguridad de la información.
- Cumplir la legislación vigente, respecto de la manipulación y resguardo de la información y materias afines, así como también de los acuerdos alcanzados contractualmente con otras empresas y empleados.
- Adoptar el nivel de seguridad que cumpla estándares internacionales, que garanticen un tratamiento integral en la administración de la seguridad de los recursos de información, tanto al interior de la empresa como en sus comunicaciones con el exterior.
- Definir un estándar mínimo de seguridad a todos los recursos de información.
- Aplicar niveles de seguridad a los recursos de información, proporcionales a su criticidad y riesgo.
- Generar los procedimientos adecuados para que la información se pueda acceder sólo por los usuarios debidamente autorizados, acreditados y autenticados para ello, con los privilegios necesarios para el desempeño de sus funciones.
- Evaluar todos los proyectos relacionados con recursos informáticos de E-certchile, desde la perspectiva de la Seguridad de la Información y a través de las áreas correspondientes.
- Proveer los recursos necesarios para gestionar de forma adecuada los requerimientos de la política de seguridad de la información para el establecimiento, implementación, mantención y mejora del Sistema de Gestión de Seguridad de la Información.
- Garantizar la continuidad de los procesos de negocio, mediante la implementación de planes de contingencia adecuados.
- Realizar y mantener respaldos periódicos de la información y de los sistemas de acuerdo con su criticidad, requerimientos legales y las necesidades de continuidad de negocios.
- Definir responsables de la administración de todo recurso informático, incluyendo los aspectos relacionados con su generación, procesamiento, almacenamiento y transmisión.
- Definir los procedimientos para que cualquier elemento que le sea entregado o retirado a un usuario cumpla con las formalidades definidas, permitiendo además mantener un registro actualizado de los equipos y software de la empresa.
- Aplicar las sanciones correspondientes, sin perjuicio de iniciar las acciones civiles legales que la Ley le confiera, Ante la detección de actividades ilícitas o reñidas con disposiciones internas y/o que caigan dentro de lo penado por la Ley.
- Mantener estricto resguardo de la documentación o evidencia generada a partir de las actividades de monitoreo y revisión y evaluación del sistema de gestión de seguridad de la información.

10.6 De las Responsabilidades y Deberes de los Usuarios

Los Usuarios de los recursos de E-certchile tendrán las siguientes responsabilidades y deberes:

- Mantener debida reserva y bajo resguardo la información a la cual tuviese acceso autorizado.
- Abstenerse de acceder sin autorización escrita o indebidamente a terminales, archivos, documentación o datos de E-certchile, y clientes; así como también de instalar software o conectar equipos personales u otros elementos no autorizados, a la red de datos
- Asegurar por la confidencialidad, integridad y disponibilidad de la información de e-certchile y dar aviso al responsable de la Seguridad de Información de cualquier problema de sistemas u otras circunstancias que podrían indicar riesgos de seguridad.
- Abstenerse de realizar actos contrarios a la propiedad intelectual de e-certchile, particularmente en lo referido a diseños de procesos, modelos de bases de datos y aplicaciones de negocios; así como también de vulnerar contratos de licenciamiento de software y similares, suscritos por E-certchile con sus proveedores de tecnologías de información.
- Utilizar los recursos informáticos para desempeñar las funciones que le fueron asignadas.
- Mantener en adecuadas condiciones los elementos de tecnología de Información entregados para el desempeño de su trabajo. Conocer y cumplir las normas y procedimientos asociadas al uso de los recursos tecnológicos y activos de información a los que se le otorgue acceso, como por ejemplo aquellas asociadas al uso de contraseñas, del correo electrónico y del acceso a redes públicas como Internet.
- Colaborar con los controles y procesos de auditaría orientados a verificar el cumplimiento de las políticas vigentes y que dicen relación con el acceso y uso que los usuarios hacen de los recursos de información, tanto lógicos como físicos.

10.7 De las Sanciones

El cumplimiento de esta Política es obligatorio para los colaboradores de E-certchile y las terceras partes con que se relaciona y las infracciones será sancionadas por el Reglamentos Internos de Orden, Higiene y Seguridad de e-certchile o por el acto jurídico que regule la relación con las terceras partes.

Con relación al personal externo y/o proveedores que no cumplan con lo indicado en esta política, dependiendo del tipo de incumplimiento el Gerente General podrá ordenar que se la amoneste o rescinda el contrato.

11. COMUNICACIÓN

La organización debe determinar las necesidades de comunicaciones internas y externas que son relevantes para el Sistema de Gestión de Seguridad de la Información, para esto debe considerar lo siguiente:

- Qué es lo que se debe comunicar
- En qué momento se debe comunicar
- A quién o quiénes comunicar
- Quién es el responsable de comunicar
- Los medios por los cuales se realiza la comunicación

12. COMPETENCIAS Y CONCIENTIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

- El área de recursos humanos debe determinar las competencias necesarias del personal que pueden afectar el funcionamiento del sistema de gestión de seguridad de la información.
- Se deben establecer los mecanismos adecuados para evaluar y asegurar que el personal posee la educación, entrenamiento o experiencia necesarios y con esto establecer las acciones correspondientes para la capacitación del personal u otra medida que la organización considere apropiada. Para tal efecto, la organización provee un proceso de entrenamiento en seguridad de la información y procura su reedición anual en base a la retroalimentación del propio sistema de gestión de seguridad de la información.
- Asegurar competencias en seguridad de la información a partir de los programas de entrenamiento establecidos.
- El comité de seguridad debe evaluar de forma anual la efectividad del entrenamiento en seguridad de la información, y a partir de esto tomar las acciones pertinentes.
- Toda la información documentada respecto de la efectividad y rendimiento del entrenamiento en seguridad de la información.
- Dentro de los programas de entrenamiento, la organización vela por que todos sus empleados estén conscientes de los siguientes puntos:

    - La presente Política de seguridad de la información.
    - La contribución que los mismos colaboradores realizan para la efectividad del Sistema de Gestión de Seguridad de la Información, incluyendo los beneficios de la mejora continua de la seguridad de la información.
    - Las implicancias no cumplir con los requerimientos del Sistema de Gestión de Seguridad de la Información.

13. EVALUACIÓN DEL DESEMPEÑO DEL SGSI

La organización es responsable de evaluar la implementación del SGSI, a través del establecimiento de diferentes criterios y métodos que incluyan el involucramiento de distintos niveles de la organización.

El monitoreo, medición, revisión y evaluación de la documentación se debe realizar en intervalos establecidos sobre los aspectos relevantes a la seguridad de la información que la organización requiera. Se debe considerar un marco de determinación de los temas a evaluar que incluya el alcance, métodos, responsables, períodos, etc.

Así mismo, se establece que la organización debe ser capaz de realizar auditorías internas para evaluar que el SGSI se encuentra gestionado de acuerdo con lo conformado por E-certchile y los requerimientos de la Norma Internacional ISO/IEC 27001.

E-certchile se compromete a reconocer cuales son las oportunidades de mejora continua y las actualizaciones necesarias para los diferentes aspectos del SGSI. Para tal efecto, la alta gerencia debe dar prioridad al control y revisión de los resultados de la evaluación del desempeño del SGSI.

	ELABORÓ	REVISÓ	APROBÓ
NOMBRE	**Emilio Chaigneau**	**Pamela Masson**	**Rubén Muñoz**
CARGO	**CISO**	**Subgerente de Procesos y Calidad**	**Gerente General**
FECHA	**17-03-2020**	**23-03-2020**	
FIRMA	Emilio Chaigneau Rodriguez Firmado digitalmente por Emilio Chaigneau Rodriguez Fecha: 2020.05.05 11:31:52 -04'00'	Pamela Cristina Masson Manriquez Firmado digitalmente por Pamela Cristina Masson Manriquez Fecha: 2020.05.05 11:24:59 -04'00'	Rubén Fernando Muñoz Silva Firmado digitalmente por Rubén Fernando Muñoz Silva Fecha: 2020.05.06 16:56:38 -04'00'
NOMBRE	**Leovino Fernández**	**Raúl Arrieta**	
CARGO	**Consultor Seguridad de la Información**	**Asesor Legal**	
FECHA	**17-03-2020**	**17-04-2020**	
FIRMA	Leovino Gonzalo Fernández Estefo Digitally signed by Leovino Gonzalo Fernández Estefo Date: 2020.05.05 11:54:11 -04'00'	Raúl Arrieta Cortés Firmado digitalmente por Raúl Arrieta Cortés Fecha: 2020.05.05 12:46:40 -04'00'	
NOMBRE		**Fernando Hurtado**	
CARGO		**Asesor 9000**	
FECHA		**23-03-2020**	
FIRMA		FERNANDO JAVIER HURTADO ARENAS Firmado digitalmente por FERNANDO JAVIER HURTADO ARENAS Fecha: 2020.05.05 12:10:03 -04'00'	

CONTROL DE CAMBIOS

N° DE REVISION	FECHA	DESCRIPCIÓN DE CAMBIOS
0	**Agosto-2018**	Revisión Inicial
1	**Enero-2020**	Actualización Política según norma ISO/IEC 27001:2013 y Compliance IAO 2019
2	**17-04-2020**	Se modifica sección de objetivos, pasándose a llamar Introducción. Se modifica sección de Riesgos Se incorpora sección Objetivos de Seguridad Se incorpora sección Comunicación Se incorpora sección Competencias y Concientización en Seguridad de la Información Se incorpora sección Evaluación del Desempeño del SGSI