POLÍTICA

Seguridad de la Información

Proceso	Cargo	Firma
Elaborado por:	Jefe de Informática	Powered by ecert Firma electrónica avanzada LILIANNE DEL RAMOS SALGADO 2025.03.06 09:29:43 -0300
Aprobado y revisado por:	Gerente General	FRANCO RAFAEL ACEITUNO GANDOLFO Firmado digitalmente por FRANCO RAFAEL ACEITUNO GANDOLFO Fecha: 2025.03.06 09:55:28 -03'00'

1. Objetivo

Garantizar la seguridad, confidencialidad, integridad y disponibilidad de la información, mediante la administración de sus riesgos y la incorporación de controles debidamente implementados.

2. Alcance

El objetivo del Sistema de Gestión de Seguridad de la Información consiste en proteger la confidencialidad, integridad y disponibilidad de la información dentro de la Cooperativa Regional Eléctrica Llanquihue Ltda. (CRELL) y sus sucursales, asegurando así la continuidad del negocio y minimizando los riesgos asociados.

2.1. Aplicación

El SGSI cubre todas las operaciones, procesos y servicios de la Cooperativa Eléctrica Llanquihue Ltda., (CRELL) relacionados con la gestión de la información para su servicio de distribución de energía eléctrica. Esto incluye, pero no se limita a, la gestión de datos de clientes, colaboradores y socios cooperados, así como la protección de sistemas y tecnologías de la información utilizadas para el almacenamiento, procesamiento y transmisión de datos.

2.2. Áreas y Ubicaciones Incluidas

El alcance incluye:

- Casa Matriz ubicada en Puerto Varas
- Sucursales de centro de pago y atención al cliente de Puerto Varas y Puerto Montt.
- Sala de servidores ubicadas en casa Matriz Edificio Principal
- Equipamiento de respaldo
- Operaciones en línea y servicios web proporcionados a través de plataformas digitales.
- Sistema de Medición Monitoreo y Control de la red de distribución
- Proceso de facturación, proyectos y planificación

2.3. Información Cubierta

El SGSI abarca toda la información sensible y crítica alojada en los sistemas de información de la cooperativa.

3. Referencia Normativa

La presente política se define considerando las recomendaciones de las siguientes normativas:

Seguridad de la Información, ciberseguridad y protección de la privacidad - sistemas de gestión de la seguridad de la información- Requisitos., Control A.5.1.

4. Definiciones

Confidencialidad: La información debe ser conocida únicamente por aquellas personas que estén autorizadas para acceder información específica del negocio. Esto es necesario para proteger los asuntos reservados como planes estratégicos, información legal, de recursos humanos, información de los colaboradores y cualquier dato sensitivo.

Integridad: La información de CRELL solamente puede ser agregada, modificada o eliminada por personas y/o procesos debidamente autorizados. Esto es necesario para garantizar que la información que soporta el negocio sea precisa y completa para que las decisiones que se tomen utilizándola produzcan los resultados que se esperan.

Disponibilidad: La información debe estar cuando se necesita en el formato requerido para su procesamiento, para asegurar que los procesos de negocio y las decisiones sean oportunas.

Propietarios de la Información y otros activos asociados: Es el dueño del proceso que utiliza o genera dicha información y tiene propiedad sobre otros activos.

Usuarios de la Información y otros activos asociados: Es aquella persona, colaborador interno o externo, que con la debida autorización introduce, borra, cambia o lee información de la compañía o utilizar el activo asociado.

Los usuarios sólo deben tener acceso a la información y a los activos a la que cuales autorizados para ver o procesar y las autorizaciones que se otorguen deben limitar su capacidad, de forma que no puedan realizar actividades distintas de aquellas para las que se otorgó permiso.

Activos de información: Es cualquier componente que contenga información (sea humano, tecnológico, software, hardware, etc.) que sustenta uno o más procesos de negocios de una unidad o área de negocio.

5. Roles y Responsabilidades

Gerente General / Representante Alta Dirección / Comité de Seguridad de la Información: Asegurar que las materias abordadas en esta política se ejecutan y se cumplan, identificar cómo se manejan

los no cumplimientos, promover la difusión y sensibilización de las materias abordadas en este documento, revisar periódicamente la presente política detectando y proponiendo mejoras.

Encargada de SGSI / Departamento TI: Apoyar al Comité de Seguridad de la Información en la supervisión de la implementación de la presente política. Recibir y dar respuesta a los incidentes de seguridad de la información asociados a actividades descritas en la presente política.

Colaboradores: Dar cumplimiento a la presente política de seguridad de la información y a todas las responsabilidades en materia de seguridad de la información que hayan sido definidas y asignadas.

6. Descripción de la Política

Cooperativa Regional Eléctrica Llanquihue Ltda. (CRELL) empresa de la décima región emplazada en la comuna de Puerto Varas, cuyo giro principal es la distribución de Energía Eléctrica abasteciendo de suministro de energía clientes de 8 comunas de la Región de Los Lagos, que ha decidido implementar un Sistema de Gestión de la Seguridad de la Información (SGSI), por lo cual se compromete a cumplir con los requisitos legales y los aplicables a la norma ISO 27001:2022, con el fin de conseguir la mejora continua del sistema de gestión de seguridad de la información.

Lo anterior se sustenta en el cumplimiento de los siguientes compromisos del Sistema de Gestión de Seguridad de la Información y sus respectivos objetivos, por parte de CRELL:

Mejorar continuamente la efectividad del Sistema de Gestión de Seguridad de la Información (SGSI).

Implementar anualmente mejoras del sistema de gestión de seguridad de la información.

Implementar planes de acción para incidentes de seguridad de la información y no conformidades que resuelvan de raíz los problemas identificados.

Cumplir con los requisitos legales y los aplicables a la seguridad de la información, según lo establecido en la norma ISO 27001:2022

Mantener en cero las multas o sanciones por incumplimiento legal y contractual relativo a la Seguridad de la Información.

Mantener vigente el Sistema de Gestión de la Seguridad de la Información implementado por la norma ISO 27001:2022.

Proteger la confidencialidad de la información sensible relacionada con la empresa y sus clientes.

Implementar planes de acción para tratamiento de incidentes de seguridad de la información y no conformidades relacionadas con afectación de la confidencialidad

Garantizar la integridad de la información de la empresa, que la misma sea precisa y completa.

Implementar planes de acción para tratamiento de incidentes de seguridad de la información y no conformidades relacionadas con afectación de la integridad

Asegurar la disponibilidad de la información cuando se necesite, para asegurar la continuidad de los procesos.

Implementar planes de acción para tratamiento de incidentes de seguridad de la información y no conformidades relacionadas con afectación de la disponibilidad.

Promover en sus colaboradores el conocimiento de dicha Política de Seguridad de la Información, así como la importancia de su contribución a la eficacia del SGSI.

Difundir el Sistema de Seguridad de la Información por medio de la ejecución de un Plan de difusión anual.

Capacitar en Seguridad de la Información por medio de la ejecución de un Plan de capacitación anual.

6.1 Relación con proveedores (A.5.19, A.5.20, A.5.21)

Todo proveedor crítico externo de la compañía debe contar con un documento formal que respalde la relación con la Compañía, además de firmar documento Declaración Ética Modelo de Prevención de Delito, de acuerdo con la Ley 20.393 Prevención del Delito, ya sea un acuerdo de servicios o un Contrato. En dicho documento se deben abordar todos los requisitos de seguridad de información pertinente, para mitigar riesgos asociados al acceso del proveedor a los activos de la cooperativa.

Al momento de definir cada acuerdo de servicio o contrato de servicio se deben tener en cuenta los siguientes ámbitos de acción a controlar según sean los servicios por contratar:

- Control de accesos físicos.
- Control de accesos a información.
- Control de activos.
- Confidencialidad de información

Seguridad en las operaciones y todos aquellos ámbitos regulados por la presente política de seguridad de la información.

En caso de ausencia de un documento formal, el proveedor crítico debe aceptar explícitamente la presente cláusula 7 de la POL-01 Política de Seguridad de la Información de la compañía, y comprometerse a su cumplimiento.

Dicho proveedor debe comprometerse a administrar y tratar la información y otros activos de Crell con la debida confidencialidad y uso de información únicamente con fin de cumplir con las obligaciones contractuales.

Queda formalmente prohibido que los proveedores hagan uso de la información de la compañía o de sus clientes para fines personales o fuera del alcance del contrato de servicio.

En caso de tener proveedores que generen una cadena de suministro de tecnologías de información y comunicación, dichos proveedores deben velar por el cumplimiento de la presente política según la aplicabilidad.

Es decir, para los servicios de tecnologías de información y comunicación, se requiere que se propaguen los requisitos de seguridad de la información en toda la cadena de suministro, si los proveedores realizan subcontrataciones para partes del servicio de tecnología de información y comunicación proporcionados a Crell.

Igualmente, para los productos de tecnologías de información y comunicación, se requiere que se propaguen las prácticas de seguridad correspondientes a través de toda la cadena de suministro, si estos productos incluyen componentes comprados a otros proveedores.

También se debe obtener una garantía de que los productos de tecnología de información y comunicación entregadas funcionan según lo esperado y que la garantía de los componentes críticos y su origen, se puede rastrear a través de toda la cadena de suministro.

6.2 Políticas Complementarias Relacionadas

Crell, adicionalmente a lo mencionado en el punto anterior, donde se detalla la política de seguridad de la información, considera la definición de las siguientes políticas que son parte integral del conjunto de políticas de seguridad de la información:

- POL- SGSI-AG-002 Respaldo de datos
- POL- SGSI-AG-003 Teletrabajo
- POL- SGSI-AG-004 Control de Acceso
- POL- SGSI-AG-005 Dispositivos de Punto Final de Usuario
- POL- SGSI-AG-006 Desarrollo Seguro
- POL- SGSI-AG-007 Control Criptográfico
- POL- SGSI-AG-008 Transferencia de Información
- POL- SGSI-AG-009 Puesto de Trabajo Despejado y Pantalla Limpia
- POL- SGSI-AG-010 Seguridad para los Servicios en la Nube
- POL- SGSI-AG-011 Gestión de Activos

7. Actualización de la Política

Dentro de la mejora continua de las políticas de seguridad de la información, esta política debe ser revisada al menos una vez al año, a partir de la fecha de entrada en vigor. El proceso se debe realizar según las definiciones del procedimiento **PRO-AG-001 Control y Confección de Documentos**

8. Difusión de la Política

Todas las políticas son revisadas en el comité de sistema de gestión que se reúne los segundos miércoles de cada mes, en donde cada uno de sus integrantes es el encargado de comunicar estas a sus colaboradores directos. Además de la publicación en el portal interno (intranet) de la cooperativa.

9. Documentos Relacionados

PRO-AG-001 Control y Confección de Documentos
POL- SGSI-AG-002 Respaldo de datos
POL- SGSI-AG-003 Teletrabajo
POL- SGSI-AG-004 Control de Acceso
POL- SGSI-AG-005 Dispositivos de Punto Final de Usuario
POL- SGSI-AG-006 Desarrollo Seguro
POL- SGSI-AG-007 Control Criptográfico
POL- SGSI-AG-008 Transferencia de Información
POL- SGSI-AG-009 Puesto de Trabajo Despejado y Pantalla Limpia
POL- SGSI-AG-010 Seguridad para los Servicios en la Nube
POL- SGSI-AG-011 Gestión de Activos

10. Control de Revisiones

N°	Actividad	Fecha
001	Versión inicial	19/11/2024