POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Código – Versión	DE-POL-001 Versión 1
Vigencia	Noviembre 2023
Próxima Revisión	Anualmente
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
DE-POL-001	
Cotrisa	

Aprobación del Directorio/Comité

Aprobación	No. Sesión y Fecha
	Directorio No. 767 de 24/11/2023

Control de Cambios

No. Versión	Modificación	Fecha	Aprobó	Descripción del cambio
1	CAR	Noviembre 2023	Directorio	Cambio formato

Cotrisa

I. ANTECEDENTES

La Empresa Comercializadora de Trigo S.A., COTRISA corresponde a una sociedad anónima cerrada constituida en escritura pública de 16 de noviembre de 1986. Su funcionamiento se rige conforme a las disposiciones contenidas tanto en la Ley N°18.046, como en su escritura de constitución.

Entre sus objetivos estratégicos se cuentan:

- Ejecutar iniciativas de inversión que permitan disponer de instalaciones de acopios de granos donde puedan ser brindados servicios de acondicionamiento, almacenaje y gestión de compra acordes a los requerimientos de los clientes de la empresa.
- Apoyar la implementación de políticas públicas sectoriales que promuevan el funcionamiento competitivo del mercado interno de granos y el mejoramiento de las condiciones de comercialización de los pequeños productores.
- Propiciar la creación de valor económico, social y ambiental en la empresa.

Conforme a lo señalado, la información que genera y gestiona la Empresa se constituye un activo imprescindible para realizar sus actividades en forma eficiente. Es así como posee un valor fundamental para la organización y debe ser protegida de un modo adecuado.

En este contexto, se establece la PSI que regula el manejo de la información en COTRISA orientada a definir las medidas que resguarden la confidencialidad, integridad y disponibilidad de la información de la empresa, el acceso a la información en conformidad con las disposiciones legales vigentes y el aseguramiento de la continuidad de sus actividades.

Un aspecto relevante considerado en la formulación de esta política es el tamaño de la empresa y el tipo de información que se maneja en la empresa por lo cual los principios de la PSI deberán adaptarse a esta condición con la finalidad que sean útiles y funcionales a la realidad organizacional. Sin perjuicio de lo anterior, en el diseño de esta política han sido considerados referencias específicas, procedimientos de seguridad y algunas prácticas definidas en normas ISO 27.000 asociadas a estas materias.

II. OBJETIVOS DE LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN

- Establecer políticas, normativas y procedimientos que permitan resguardar y proteger los activos de información de la empresa.
- Identificar, controlar y prevenir y/o mitigar los riesgos de seguridad de la información.
- Determinar medidas esenciales de seguridad de la información que la empresa debe adoptar para protegerse apropiadamente contra amenazas que pudieren afectar la confidencialidad, integridad y disponibilidad de la información, utilizando criterios y recomendaciones referenciales indicadas en Normas ISO 27.000 relacionadas con la seguridad de la información.
- Promover el correcto uso de la información por parte del personal de la empresa.

III. ALCANCE

Esta política se aplica a todo el personal que trabaja en la empresa, indistintamente del régimen laboral, y al personal externo que otorgue servicios.

También es aplicable a todo activo de información que la organización posea en la actualidad o en el futuro, de manera que la no inclusión explícita en el presente documento no constituye argumento para no proteger estos activos de información.

La política cubre indistintamente toda la información de la empresa, ya sea impresa o electrónica.

De la política general de SI se derivarán políticas específicas complementarias, las cuales contarán con procedimientos asociados, mecanismos de control y sanciones asociadas al no cumplimiento.

IV. RESPONSABILIDADES

Se define como responsable de liderar la PSI de la empresa al Gerente de Desarrollo, quien será apoyado en esta tarea por el Encargado de Informática.

En este contexto, le corresponderá el desarrollo de la PSI al interior de la empresa, el control de su implementación y velar por su correcta aplicación.

En particular deberá:

- Realizar un levantamiento de los riesgos que pueden afectar la SI de la empresa, así como identificar brechas, evaluar riesgos de SI e instaurar controles y/o medidas de mitigación a los riesgos identificados.
- Proponer anualmente al Comité de Directorio un plan de trabajo para implementar adecuadamente la PSI en la empresa.
- Coordinar la formulación de un plan de contingencia para asegurar la continuidad de las actividades de la empresa.
- Mantenerse informado respecto a nuevos lineamientos y directrices que pudieren surgir desde los entes rectores en materia de SI.
- Difundir e informar la PSI.

A nivel directivo, le corresponderá al Comité de Directorio supervisar el cumplimiento de la Política de Seguridad de la Información, y en particular, establecer normas, políticas y procedimientos que permitan resguardar y proteger los activos de información y velar por la implementación de técnicas para la gestión de la seguridad de la información

V. PRINCIPIOS GENERALES DE LA PSI

a. Usuarios internos

La información deberá ser accesible sólo para aquellos usuarios autorizados, considerando que es bien que tiene valor para la organización y consecuentemente requiere ser protegida en forma adecuada.

En este contexto, los usuarios internos deberán proteger la información siguiendo reglas y procedimientos definidos en las sub políticas que emanen de la Política General de SI. En este contexto, la Administración deberá proveer los recursos necesarios para implementar los controles requeridos.

La empresa proveerá los mecanismos para que la información sea accedida y utilizada por el personal que de acuerdo con sus funciones así lo requiera. Sin embargo, se reserva el derecho de

revocar al personal, el privilegio de acceso a la información y tecnologías que la soportan, si la situación y las condiciones lo ameritan.

b. Usuarios externos

La información de usuarios externos que pueda ser manejada por la empresa, ya sean datos personales o sensibles de acuerdo con la normativa vigente, no deberá ser divulgada sin previa autorización y estará protegida de igual manera que la información interna.

c. Acceso a la información

La empresa implementará los controles necesarios para garantizar que tanto la información física como lógica sea accesible sólo por usuarios autorizados. Para resguardar lo anterior, se formularán políticas específicas y se definirán perfiles de acceso para el personal de acuerdo con sus funciones y responsabilidades en cada sistema de información.

- **Acceso físico a las instalaciones**

Se definirá una política de acceso físico a las instalaciones con la finalidad de minimizar los riesgos de daños e interferencias a la información y a las operaciones de la organización. Para ello, se establecerán perímetros de seguridad y áreas protegidas con lo cual se facilita la implementación de controles de protección de las instalaciones de procesamiento de información crítica o sensible de la organización, contra accesos físicos no autorizados.

d. Retención de información

Se cumplirá con las normativas vigentes sobre retención de información legal relacionada con archivos públicos, que buscan regular la conservación, el almacenamiento clasificación y eliminación de documentos que contienen información pública.

e. Arquitectura tecnológica

La empresa definirá la tecnología que debe soportar las distintas soluciones del negocio, así como los mecanismos de almacenamiento de datos e información, las redes de datos, los centros de procesamiento de datos y los servicios integrados de tecnología.

f. Políticas de seguridad específicas

Se emitirán políticas de seguridad especificas con la finalidad de dar lineamientos y definir estándares de cumplimiento con el propósito de regular aspectos específicos relacionados con la SI.

El desarrollo de nuevas políticas estará enfocado a cubrir brechas detectadas y dar cumplimiento a controles específicos contemplados en nuevas normativas asociadas a la SI (Normas ISO u otras).

g. Revisiones

La PSI será revisada periódicamente o en caso de que existan cambios en el ambiente de la empresa. Las modificaciones al presente documento estarán a cargo del Responsable de implementar la PSI en la empresa y deberán ser aprobadas por el Comité de Directorio. Asimismo, para la implementación operativa de las políticas vigentes, se definirán documentos complementarios tales como instructivos, procedimientos, guías de implementación entre otros.

h. Difusión

La difusión de la PSI será abordada por el responsable de la implementación de la PSI en la empresa. En este contexto, la PSI, políticas específicas, normas, procedimientos serán comunicados y difundidos a todo el personal de la empresa, a terceros que otorguen servicios a la empresa (si ello procede) y a los entes controladores relevantes (SEP).

Para la difusión de los contenidos de la política de seguridad de la información al interior de la institución, se utilizarán los medios de difusión que COTRISA disponga (internet, boletines), así como también instancias de capacitación. Para lo anterior se deberá definir, implementar y evaluar las acciones e iniciativas contenidas en el plan de difusión de la PSI.

i. Evaluación del cumplimiento de la política de seguridad de la información

Todos los Gerentes de Área, serán responsables del respecto a la implementación de esta política de seguridad de la información, dentro de sus áreas de responsabilidad, así como el cumplimiento de las políticas, normativas y procedimientos por parte de su equipo de trabajo.

La Empresa podrá realizar auditorías internas al sistema de seguridad de la información para verificar el cumplimiento de las políticas, normas y procedimientos de seguridad de la información.

El incumplimiento de las disposiciones contenidas en la Política de Seguridad de la Información tendrá como resultado la aplicación de sanciones, conforme a la magnitud y características del aspecto no cumplido.

VI. Definiciones relevantes

- Activos de Información: Son todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución, en la que se distinguen tres niveles:
    - La Información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.)
    - Los Equipos/Sistemas/infraestructura que soportan esta información
    - Las Personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales.
- Seguridad de la Información: La preservación de la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio (ISO 17799).
- Disponibilidad: Vinculado con la seguridad de la información se refiere a la propiedad de ser accesible y utilizable por una entidad autorizada (ISO 13335-1).
- Confidencialidad: La propiedad vinculada con la seguridad de la información por la que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados (ISO 13335-1).
- Integridad: La propiedad de salvaguardar la exactitud y completitud de los activos (ISO/IEC 13335-1).
- Evaluación de riesgos de SI: El proceso general de análisis y estimación de los riesgos en la seguridad de la información (ISO Guide 73).

- Gestión de riesgos de SI: Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos de la seguridad de la información (ISO/IEC Guide 73).
- Tratamiento de riesgos de SI: El proceso de selección e implementación de las medidas encaminadas a modificar los riesgos de la seguridad de la información (ISO/IEC Guide 73).