Declaración de Seguridad de la Información / Ciberseguridad

Introducción

En Cencosud promovemos diariamente una cultura basada en la **pasión, el respeto, la transparencia y la confianza**, con el propósito de **servir de forma extraordinaria en cada momento** a nuestros clientes mediante una **propuesta diferenciadora, sostenible y con altos estándares de excelencia** en productos y servicios. Nuestra Estrategia de Sostenibilidad y el Modelo de Negocio, sustentados en los principios de Abastecimiento, Producción y Consumo Responsable, orientan a nuestras Unidades de Negocio hacia la consolidación de una organización sostenible.

En este contexto, se establece la "Declaración de Seguridad de la Información", cuyo propósito es definir los lineamientos generales que permitan gestionar adecuadamente la confidencialidad, integridad y disponibilidad de la información, estableciendo una cultura de seguridad y control acorde a las mejores prácticas internacionales.

Este documento está destinado a terceros (clientes, proveedores, inversionistas, entre otros) vinculados con la compañía y que requieran conocer el enfoque de seguridad adoptado por Cencosud.

La declaración es objeto de revisión y actualización anual.

Compromiso con la Seguridad

Como organización, reafirmamos nuestro compromiso con:

- Preservar la Confidencialidad, Integridad y Disponibilidad de la información.
- Cumplimiento de leyes, normativas y contratos.
- Responsabilidad compartida en todos los niveles de la organización.
- Enfoque basado en riesgos.
- Mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

Este compromiso se extiende de manera explícita a todos los colaboradores, contratistas, proveedores, consultores, inversionistas y demás terceros, quienes deben adoptar activamente estas directrices como parte integral de su relación con Cencosud.

Marco Normativo

La Compañía cuenta con un Marco Normativo basado en estándares internacionales como ISO, NIST, y SANS CIS, además de cumplir con las regulaciones locales aplicables en cada país.

Gobernanza de Seguridad de la información / Ciberseguridad

El CISO del Grupo (Chief Information Security Officer) es responsable de liderar la implementación de esta política, junto con el Comité de Seguridad de la Información y los equipos de Seguridad de la Información de cada país.

Responsabilidades

- Todos los colaboradores deben proteger la información bajo su custodia.
- Líderes de área: deben asegurar el cumplimiento del Marco Normativo en sus equipos.
- Proveedores: deben cumplir con controles definidos contractualmente.

Para garantizar el cumplimiento efectivo de esta declaración, se definen en el Marco Normativo y en los contratos pertinentes responsabilidades claras que deben ser asumidas por todos los actores vinculados a la operación de Cencosud cuya observancia es condición esencial para mantener una relación de confianza y continuidad con la compañía.

Programa de Seguridad de la Información

Incluye:

- Gestión de accesos.
- Seguridad de redes y sistemas.
- Seguridad física y ambiental.
- Gestión de incidentes.
- Continuidad del negocio.
- Gestión de proveedores.
- Monitoreo y auditoría.

Concientización y Capacitación en Seguridad

Cencosud mantiene un programa de concientización permanente para sus colaboradores y terceros, a fin de reforzar las buenas prácticas y mitigar riesgos humanos.

El programa se articula mediante procedimientos definidos y controles específicos, cubriendo desde la revisión de código fuente en aplicaciones críticas hasta el cifrado de datos sensibles, administración de accesos privilegiados, y controles de seguridad física en instalaciones clave.

Evaluación de Riesgos

De manera sistemática, se ejecutan procesos de evaluación para detectar potenciales amenazas y vulnerabilidades, estableciendo acciones correctivas conforme al apetito de riesgo definido por Cencosud.

Gestión de incidentes

Los incidentes deben reportarse de inmediato al equipo de Seguridad Informática. Se aplicará el protocolo de respuesta según criticidad, incluyendo análisis forense, comunicación a stakeholders y medidas de contención. El reporte oportuno y la colaboración activa son esenciales para una gestión eficaz de incidentes, y forman parte de los compromisos asumidos en nuestras relaciones.

Gestión de seguridad de proveedores

Todos los terceros con acceso a sistemas o información deben ser evaluados y cumplir con los controles exigidos por la compañía. Los contratos deben incluir cláusulas de seguridad, derecho a auditoría y recertificaciones periódicas.

El proceso incluye notificación formal, investigación con soporte forense, coordinación regional, registro centralizado de eventos y seguimiento de acciones correctivas hasta su cierre documentado.