POLÍTICA DE CIBERSEGURIDAD

Código – Versión	DE-POL-002 Versión 1
Vigencia	Noviembre 2023
Próxima Revisión	Anualmente
POLÍTICA DE CIBERSEGURIDAD	
DE-POL-002	
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	LSR	Noviembre 2023	Directorio	Se cambian algunos párrafos a la realidad de la empresa.

Cotrisa

I. Introducción

Nuestra Política de Ciberseguridad describe las directrices y disposiciones para preservar la seguridad de la infraestructura de datos y tecnología de COTRISA.

La Política de Ciberseguridad está dirigida a gestionar eficazmente la seguridad de la información que se manejan en los sistemas informáticos de la empresa, así como los activos que participan en sus procesos.

II. Objetivo

Esta Política tiene como objetivo garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información, y cumplir con las Leyes y Reglamentaciones vigentes y en especial medida cumplir con Instructivo Presidencial N°8 del 23 de octubre de 2018, manteniendo un equilibrio entre los niveles de riesgo y un uso eficiente de los recursos.

III. Alcance

Esta política de ciberseguridad se aplica a todos los empleados, jefes de planta, gerentes, directores y cualquier persona que tenga acceso permanente o temporal a los sistemas y hardware de COTRISA.

IV. Definiciones

a. Tecnología de la Información de la Empresa (TIE)

Envuelve todo el espectro de tecnologías de procesamiento de información, incluyendo software, hardware, tecnologías de comunicación y servicios relacionados.

b. Tecnología de Operación de la Empresa (TOE)

Abarca hardware, software y sistemas de comunicación que forman parte de los productos y soluciones desarrollados por COTRISA.

c. Ciberseguridad

Engloba la seguridad del ámbito digital a través de TIE y TOE. La Ciberseguridad es complementaria al ámbito de la seguridad física, pero está estrechamente relacionada y en interdependencia con la misma.

V. Principios básicos

- Garantizar que los sistemas de información (TIE) y sistemas de operación (TOE) de la empresa tengan un grado de seguridad y resiliencia adecuado y apliquen los modelos más avanzados en los activos tecnológicos que respaldan la operación de infraestructuras críticas.
- Ejecutar las medidas de seguridad necesarias para proteger la integridad, la confidencialidad y la disponibilidad de la información y los sistemas de operación en función de su criticidad y los riesgos existentes, siguiendo un enfoque basado en el riesgo.
- Sensibilizar a todos los empleados, jefes de planta, gerentes, directores y cualquier persona que tenga acceso permanente o temporal a los sistemas y hardware sobre los riesgos de Ciberseguridad y velar que tengan la preparación, destrezas, experiencia y capacidades tecnológicas necesarios para respaldar los objetivos de la empresa.

- Incentivar las habilidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación contra incidentes y actividades del cibercrimen.
- Promover la implementación de mecanismos de seguridad y resiliencia adecuados para los sistemas y operaciones gestionados por terceros que prestan servicios a la empresa.
- Garantizar el cumplimiento normativo asociado a las áreas de ciberseguridad en toda la empresa.
- Colaborar con otras empresas estatales, organizaciones y stakeholders para contribuir a la mejora nacional de la ciberseguridad.

VI. Modelo de Gestión de Ciberseguridad

Con el fin de sostener los objetivos y principios de esta política, COTRISA implementará un Modelo de Gestión de Ciberseguridad basado en una apropiada definición y asignación de funciones y responsabilidades de gestión y operación, así como procedimientos, reglas, metodologías, herramientas e información o sistemas de operación apropiados para diferentes ámbitos considerados como parte del sistema.

a. Funciones y responsabilidades

Asignación de un conjunto de funciones y responsabilidades en materia de ciberseguridad claramente definidas y asignadas en el organigrama de la empresa.

b. Gestión e identificación de los riesgos

Implementar estructuras y procesos para mantener y desarrollar capacidades de seguridad y que incluye los siguientes objetivos:

- Promover la organización de Ciberseguridad con una visión integral y global en la empresa, fundada en la identificación continua de riesgos y la minimización del nivel de exposición, asegurando el cumplimiento de las obligaciones con los stakeholders.
- Estandarizar y mantener un Modelo de Gestión de Ciberseguridad basado en el riesgo, estándares claros y controles supervisados que optimicen la inversión de recursos.

c. Protección de las amenazas

Mejorar las medidas de protección de los activos digitales antes de materializarse el riesgo y que contempla como objetivo el desarrollo de las tecnologías de seguridad aplicables a la protección integral de los activos a lo largo de su ciclo de vida, su criticidad y el desarrollo de las amenazas.

d. Detección de amenazas

Detectar las amenazas mediante el uso de diversas fuentes de inteligencia para poder gestionarlas de manera proactiva y que considera como objetivo aumentar las capacidades de detección de amenazas internas o externas.

e. Respuesta a incidentes de Ciberseguridad

La respuesta debe minimizar el impacto en la empresa y debe contemplar como objetivo asegurar la continuidad de los servicios soportados por los activos que conforman la infraestructura tecnológica y digital de la compañía y reducir el impacto de los incidentes a través de protocolos de la empresa.

f. Revisión y actualización continua del modelo

Un proceso de revisión y actualización continua del modelo de gestión de ciberseguridad para adecuarlo en todo momento a las ciber amenazas que van surgiendo y puedan afectar.