Ferreycorp	**POLÍTICA CORPORATIVA DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN**	**CÓDIGO**	**VERSIÓN**
		GEN-GTPI-PC-001	02
		FECHA INICIAL DE VIGENCIA	**FECHA DE PROXIMA REVISION**
		01/03/2023	01/04/2028
GERENCIA ELABORADORA	GERENCIA CORPORATIVA DE TI PROCESOS E INFORMACIÓN		
ELABORADO POR Eduardo Luyo Vicente OFICIAL DE SEGURIDAD DE INFORMACIÓN	**REVISADO POR** Eduardo Tirado Hinojosa GERENTE CORPORATIVO TI PROCESOS E INFORMACIÓN	**APROBADO POR** Mariela García De Fabri GERENTE GENERAL	

1. Objetivo:

Los objetivos de la presente política son proteger los datos, los sistemas y las tecnologías de información de las empresas y entidades de la Corporación Ferreycorp.

2. Alcance:

La presente política es aplicable a todos los colaboradores, así como terceros con acceso a los datos, sistemas y las tecnologías de información de alguna de las empresas de la Corporación.

3. Definiciones:

A continuación, se definen los siguientes términos:

3.1 Ciberataque. - es un tipo de actividad maliciosa realizada por ciberdelincuentes que intenta recopilar, interrumpir, denegar, degradar o destruir los sistemas de información o la información misma.

3.2 Ciberseguridad. - es el proceso para proteger los sistemas de información y la misma información de ciberataques.

4. Contenido

Ciberseguridad:

4.1. En la Corporación Ferreycorp, el uso de nuevas tecnologías y aplicaciones incluyendo movilidad, uso de servicios en nube, uso de aplicaciones como servicio, accesos remotos a nuestra red, integraciones con sistemas de terceros, uso de inteligencia artificial, robots y otros deberán considerar evaluaciones de riesgos, definición e implementación de controles contra ciberataques y pruebas de ciberseguridad.

4.2. Todas las tecnologías en uso, así como las redes y los servicios en nube deberán contar con revisiones periódicas de análisis de vulnerabilidades y hacking ético con el fin de detectar y remediar cualquier brecha de seguridad en las mismas.

4.3. Las tecnologías que no cumplan con los controles de ciberseguridad no deberán ser utilizadas en ninguna operación de negocio debido a que podría exponer la infraestructura tecnología, aplicaciones o datos de la Corporación.

4.4. La Gerencia Corporativa de TPI establecerá los mecanismos de prevención, detección y recuperación.

(i) prevención: desplegar mecanismos de monitoreo temprano y protocolos que aseguren que toda la información y las tecnologías de soporte se encuentren protegidas ante ciberamenazas

(ii) detección: contar con las capacidades de respuesta ante un ciberataque

(iii) recuperación: implementar y planes de recuperación que reduzcan el impacto ante un ciberataque. sistemas de monitoreo y detección de ciberataques, así como los procedimientos de respuesta y/o recuperación de la infraestructura tecnológica, aplicaciones y datos de la Corporación.

4.5. Todas las gerencias y colaboradores que identifiquen algún evento malicioso como spam, phishing, malware en sus equipos de cómputo, redes, correo o aplicaciones; deberán reportarlo inmediatamente al Área de Seguridad de Información para la adopción de las medidas de contención y remediación.

Seguridad de la Información

4.6. Para la Corporación Ferreycorp, los datos provenientes de sus operaciones de negocio, clientes, colaboradores, proveedores y accionistas debe ser considerada un activo intangible.

4.7. Dada la importancia, alto valor y utilidad de los datos, las empresas y entidades de la Corporación Ferreycorp tienen el deber de preservarla y cuidarlos, basándose en los siguientes principios:

- Cumplimiento de la legislación y regulaciones requeridas
- Administración de acceso basado en la “necesidad de conocer” por estricta razón de negocio y de acuerdo al rol que desempeña el colaborador en cada área.
- Compromiso de los colaboradores en el manejo de la información de acuerdo con el rol que desempeñan.
- Los datos deben protegerse de acuerdo con su valor e importancia.

4.8. Las prácticas de seguridad de la información protegerán el valor de los activos de información del negocio y estarán alineadas con las mejores prácticas y estándares internacionales.

4.9. Todos los colaboradores que laboran en las empresas y entidades de la Corporación Ferreycorp son responsables y están comprometidos en

proteger los recursos y la información que manejan, así como cumplir y ejecutar la normativa de seguridad de información.

4.10. La Corporación Ferreycorp está comprometida con el uso legal, el tratamiento de acuerdo con los fines establecidos y la protección de datos personales que recolecta, almacena, usa, circula o suprima de acuerdo con las leyes de protección en cada país en el que operamos.

4.11. Cualquier información y propiedad intelectual (software, marca, base de datos, diseños, manuales, imágenes, entre otros) que pertenezca a alguna de las empresas de la Corporación no debe utilizarse para fines particulares, ni trasladarse a terceros.

4.12. Es responsabilidad de todos los Gerentes y Colaboradores reportar al Oficial de Seguridad de la Información los eventos e incidentes de seguridad de la información ocurridos con el fin de establecer las acciones correctivas.

4.13. Todo incumplimiento de una política, norma, estándar o procedimiento de seguridad de la información por parte de algún empleado será causa para iniciar acciones disciplinarias. Si el incumplimiento se origina por parte de algún contratista, la empresa podrá suspender la prestación del servicio.

-----()-----

EL PRESENTE DOCUMENTO HA SIDO AUTORIZADO EN EL SISTEMA NORMATIVO POR:

ROL	NOMBRE	PUESTO	FECHA
Elaborador	Eduardo Luyo Vicente	OFICIAL DE SEGURIDAD DE INFORMACIÓN Y GESTIÓN TPI	Aprobado - 03/04/2023 14:10
Revisor	Eduardo Tirado Hinojosa	GERENTE CORPORATIVO DE TPI	Aprobado - 10/04/2023 08:36
Aprobador	Mariela Garcia De Fabbri	GERENTE GENERAL	Aprobado - 12/04/2023 15:20