

 Seguridad energética	PE-05-18-015	Vigencia a partir 2023	
		Versión 3	Página 1 de 4

Política de Seguridad de la Información

1. Propósito

Proteger la disponibilidad e integridad y confidencialidad de la información, cuando así se requiera, contra el uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales en cumplimiento a la adopción de la Norma INTE//ISO/IEC 27001:2013 Sistema de Gestión de Seguridad de la Información.

2. Alcance

Aplica a todas las áreas de la empresa, así como a terceros a través de contratos o acuerdos de prestación de servicios y a todo el personal de la empresa.

3. Definiciones

Activos de información: Los datos creados o utilizados por un proceso de la organización en medio digital, en papel o en otros medios y que, por tanto, debe protegerse.

Responsables de activos de información: titular subordinado o encargado de un área responsable de datos o informaciones que responden a la ejecución de sus funciones o los procesos de negocio que tiene bajo su cargo.

Terceros: personal contratista o externo a la empresa.

4. Fundamento Normativo

- Norma INTE//ISO/IEC 27001:2013 – Sistema de Gestión de Seguridad de la Información
- Marco de Gobierno y Gestión de Tecnologías de Información – MICIIT
- Instrumento de medición de la Contraloría General de la República para la “Aplicación de prácticas de seguridad de la información en las instituciones públicas”
- Ley de Información no Divulgada, Ley N°7975 del 2 de enero de 2000
- Ley General de Control Interno, artículo 6, Ley N°8292 del 31 de julio de 2002
- Ley de Protección de la persona frente al tratamiento de sus datos personales, N° 8968 del 5 de setiembre de 2011. (del 7 de julio del 2011).
- Decreto Ejecutivo Transparencia y Acceso a la Información Pública, N° 40200-MP-MEIC-MC.
- Decreto Apertura de Datos Públicos, N° 40199-MP-MEIC-MC
- Código de Gobierno Corporativo de RECOPE.

5. Contenido (Declaración de la política)

RECOPE se compromete con la seguridad de la información reconociendo su valor estratégico en la gestión del negocio, implementando un sistema de gestión de seguridad de la información que considere la ciberseguridad para

asegurar el cumplimiento de los principios de confidencialidad, integridad y disponibilidad de la información.

La información estará disponible, sin alteración alguna, para las personas autorizadas a accederla, en el momento en que se necesite, asegurando su resguardo independientemente de si es almacenada, procesada o transferida dentro de la empresa. Adicionalmente, RECOPE asegurará que la información cuente con las medidas de seguridad apropiadas cuando salga de la empresa.

6. Responsabilidades

Gerencia General:

- a) Aprobar las propuestas de integración de los procesos institucionales y asegurar el cumplimiento de la política de seguridad de la información y la implementación del Sistema de Gestión de Seguridad de la Información.
- b) Destinar los recursos necesarios para lograr el cumplimiento de los requerimientos del Sistema de Gestión de Seguridad de la Información.

Gerencia de Innovación:

- a) Promover el cumplimiento de las acciones para la implementación del sistema de seguridad de la información por parte de todos los actores internos y externos de conformidad con su responsabilidad en la gestión de los activos de información.
- b) Promover la ejecución y evaluación del cumplimiento de los objetivos estratégicos que la empresa debe alcanzar para el alineamiento de la seguridad de la información.

Dirección de Tecnología

- a) Ejecutar las acciones para la implementación del sistema de seguridad de la información.
- b) Aprobar los controles del Sistema de Gestión de seguridad de la información en los entornos tecnológicos de los sistemas administrativos e industriales de la empresa.

Oficial de Seguridad de la Información:

- a) Proponer la adecuada implementación de un Sistema de Gestión de Seguridad de la Información, mediante el desarrollo de directrices, procedimientos y lineamientos.

- b) Supervisar el cumplimiento de los controles implementados para proteger la integridad, confidencialidad y disponibilidad de la Seguridad de la Información.
- c) Implementar programas de capacitación y concienciación a los empleados sobre seguridad de la información, en conjunto con el Departamento de Desarrollo de Capital Humano.

Oficial de Seguridad Informática:

- a) Proponer y supervisar el cumplimiento de los controles de ciberseguridad en los entornos administrativos e industriales de la empresa.
- b) Analizar y validar herramientas tecnológicas en conjunto con los arquitectos de diseño para lograr el cumplimiento de los controles de seguridad de la información y de la ciberseguridad.

Responsables de activos de información:

Aplicar las medidas de seguridad de la información que se definan.

Funcionarios y terceros:

Cumplir con esta política, las directrices relacionadas a ella y los controles del sistema de gestión de seguridad de la información.

7. Vigencia de la política

La vigencia de la presente política será a partir de la aprobación por parte de la Junta Directiva.