



Política general de seguridad de la información



2022



 conTREEbute	 mero Sustainability Information System	Política general de seguridad de la información		Pública
Versión 1.0		Fecha: 18-08-2022	Código: SI-PO-001	Página: 2

Contenido

Control de versiones	3
Objetivo, alcance y usuarios	4
Terminología básica sobre seguridad de la información	4
Gestión de la seguridad de la información	4
Objetivos y medición.....	4
Compromisos	5
Requisitos para la seguridad de la información.....	5
Controles de seguridad de la información.....	5
Continuidad de negocio	5
Responsabilidades	5
Comunicación de la Política	6
Apoyo para la implementación del SGSI.....	6
Validez y gestión de documentos	6

 	Política general de seguridad de la información		Pública
Versión 1.0	Fecha: 18-08-2022	Código: SI-PO-001	Página: 3

Control de versiones

Versión	Fecha	Elaborado por	Revisada por	Aprobado por	Descripción de cambios
1.0	10/08/2022	SGSI	Carlos Velásquez	Carlos Velásquez	Versión inicial

		Política general de seguridad de la información		Pública
Versión 1.0		Fecha: 18-08-2022	Código: SI-PO-001	Página: 4

Objetivo, alcance y usuarios

El propósito de esta Política de alto nivel es definir el objetivo, dirección, principios y reglas básicas para la gestión de la seguridad de la información.

Esta Política se aplica a todo el Sistema de gestión de seguridad de la información (SGSI), según se define en la declaración del Alcance del SGSI.

Los usuarios de este documento son todos los colaboradores y contratistas de conTREEbute, como también terceros externos a la organización.

Terminología básica sobre seguridad de la información

- **Confidencialidad:** característica de la información por la cual solo está disponible para personas o sistemas autorizados.
- **Integridad:** característica de la información por la cual solo puede ser modificada por personas o sistemas autorizados y de una forma permitida.
- **Disponibilidad:** característica de la información por la cual solo pueden acceder las personas autorizadas cuando sea necesario.
- **Seguridad de la información:** es la preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Sistema de gestión de seguridad de la información:** parte de los procesos generales de gestión que se encarga de planificar, implementar, mantener, revisar y mejorar la seguridad de la información.

Gestión de la seguridad de la información

Objetivos y medición

Los objetivos generales para el sistema de gestión de seguridad de la información son los siguientes:

- Asegurar la identificación, evaluación y gestión de los riesgos de seguridad de la información con el fin de garantizar su tratamiento, trazabilidad y no materialización de estos.
- Definir y poner en marcha la gestión de continuidad del negocio y recuperación ante desastres para responder oportunamente ante cualquier incidencia de seguridad y así garantizar los acuerdos de niveles de servicio pactado con los clientes.
- Garantizar la gestión de las Incidencias identificadas como el fin de prevenir eventos o incidentes que puedan afectar la seguridad de los activos de la información y de la plataforma MERO.
- Generar una Cultura y sensibilización asociada a los riesgos y controles de seguridad de la información promoviendo el compromiso de todos los colaboradores que integran el equipo MERO.
- Proteger los activos de información con el fin de mantener la confidencialidad, integridad y disponibilidad de la información relacionada a toda la organización y sus partes interesadas
- Cumplir con los requisitos, controles aplicables al sistema de gestión de la seguridad de la información de acuerdo con el alcance establecido

Los objetivos de seguridad de la información están alineados a los objetivos estratégicos con el fin de fortalecer tanto la visión de la empresa, así como la implementación del sistema de seguridad.

		Política general de seguridad de la información		Pública
Versión 1.0		Fecha: 18-08-2022	Código: SI-PO-001	Página: 5

Esta política, con todos sus objetivos deben ser revisados al menos una vez al año.

ConTREEbute medirá el cumplimiento de todos los objetivos. En el Informe de mediciones El Comité del SGSI es el responsable de definir el método para medir el cumplimiento de los objetivos. La medición se realizará al menos una vez al año, además el Comité analizará y evaluará los resultados y los reportará a la Gerencia General como material para el elaborar el Acta Revisión por la Dirección.

El Comité del SGSI es el responsable de revisar estos objetivos generales del SGSI.

Los objetivos para el sistema de gestión de la información están documentados en el informe de medición.

Compromisos

ConTREEbute, en cumplimiento de sus funciones y entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con el establecimiento, implementación y mejora continua del Sistema de Gestión de Seguridad de la Información, así como de garantizar la confidencialidad, integridad y disponibilidad de nuestra plataforma MERO.

Requisitos para la seguridad de la información

Esta Política, y todo el SGSI, deben cumplir los requisitos legales y normativos importantes para la organización en el ámbito de la seguridad de la información, como lo es la protección de datos personales, además con las obligaciones contractuales.

En la “Lista de Requisitos” se detalla una lista de requisitos contractuales y legales.

Controles de seguridad de la información

El proceso de escoger los controles está definido en la metodología de evaluación y tratamiento de riesgos. Los controles seleccionados y su estado de implementación se detallan en la Declaración de aplicabilidad.



Continuidad de negocio

La Gestión de la continuidad de negocio está reglamentada en la “Política de gestión de la continuidad de negocio”.

Responsabilidades

Las responsabilidades para el SGSI son las siguientes:

- El Comité de SGSI es el responsable de garantizar que el SGSI sea implementado y mantenido de acuerdo con esta Política y de garantizar que todos los recursos necesarios estén disponibles.
- El Comité del SGSI es el responsable de la coordinación operativa del sistema, como también de informar su desempeño.
- El Comité del SGSI es el responsable de revisar el SGSI al menos una vez por año o cada vez que se produzca una modificación significativa; y debe elaborar actas de dichas reuniones. El objetivo de las verificaciones por parte de la dirección es establecer la conveniencia, adecuación y eficacia del SGSI.

 conTREEbute	 mero Sustainability Information System	Política general de seguridad de la información		Pública
Versión 1.0		Fecha: 18-08-2022	Código: SI-PO-001	Página: 6

- La protección de la integridad, disponibilidad y confidencialidad de los activos es responsabilidad del propietario de cada activo.
- Todos los incidentes o debilidades de seguridad deben ser informados siguiendo el “Procedimiento para Gestión de Incidentes”.
- El Comité del SGSI definirá qué información relacionada con la seguridad de la información será comunicada a qué parte interesada (tanto interna como externa), por quién y cuándo, en la “Matriz de Comunicaciones”.
- El Comité del SGSI es el responsable de adoptar e implementar el “Plan de formación MERO”, que corresponde a todas las personas que cumplen una función en la gestión de la seguridad de la información.

Comunicación de la Política

El Comité del SGSI debe asegurarse de que todos los empleados que participan en la gestión y operación del Sistema MERO, como también los participantes externos correspondientes, estén familiarizados con esta Política.

Apoyo para la implementación del SGSI

A través del presente, el sponsor del Sistema MERO declara que en la implementación y mejora continua del SGSI se contará con el apoyo de los recursos adecuados para lograr todos los objetivos establecidos en esta Política, como también para cumplir con todos los requisitos identificados.

Validez y gestión de documentos

El propietario de este documento es el Comité del SGSI, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.