Política de seguridad de la información

Uso Público

Responsabilidad y control de cambios

Propietario	Área de riesgo
Revisor	Subgerente de riesgo operacional, continuidad de negocio y seguridad de la información.
Aprobador	Comité de riesgo

Versión	Fecha	Descripción del cambio	Realizado por
0.1	11-11-2013	Creación del documento	Comité de riesgo
0.1	24-04-2014	Aprobación del documento	Comité de riesgo
0.2	05-08-2015	Revisión del documento	Comité de riesgo
0.2	15-09-2015	Revisión del documento	Comité de riesgo
0.3	07-01-2016	Aprobación del documento	Comité de riesgo
0.4	05-01-2017	Revisión del documento	Comité de riesgo
0.5	18-01-2018	Aprobación del documento	Comité de riesgo
0.6	19-04-2018	Aprobación del documento	Comité de riesgo
0.7	15-06-2021	Revisión del documento	Comité de riesgo
0.7	25-06-2021	Aprobación del documento	Comité de riesgo
0.8	03-09-2021	Se ajusta la política a los principios del marco de referencia NCh-ISO 27.001:2020	Cristian Vargas Z.
0.8	21-09-2021	Revisión del documento	César Miranda
0.8	21-09-2021	Aprobación del documento	Comité de riesgo
0.9	08-03-2022	Se añade principio de mejora continua	César Miranda
0.9	27-04-2022	Aprobación del documento	Comité de riesgo
1.0	21-03-2023	Revisión del documento	César Miranda
1.0	17-05-2023	Aprobación del documento	Comité de riesgo
1.1	20-12-2023	Se modifican los documentos relacionados, se reestructuran los principios de la política, se realizan ajustes de formato.	Pallavicini Consultores – Pablo Meneses – Ma. Fernanda Z.
1.1	26-12-2023	Revisión del documento	Ma. Fernanda Z.
1.1	20-03-2024	Aprobación del documento	Comité de riesgo

Índice de contenidos

1. Objetivo del Documento 4
2. Alcance 4
3. Documentos Relacionados 4
4. Política 5
5. Roles y Responsabilidades 6
6. Aprobación, Publicación y Actualización 6

1. Objetivo del documento

Entregar disposiciones, basadas en buenas prácticas, consideradas como lineamientos estratégicos necesarios, para el establecimiento del Sistema de Gestión de Seguridad de la Información (SGSI) de Cibergestión.

2. Alcance

Esta política es aplicable a Cibergestión, y considera en su alcance todos los procesos y recursos clave, el contexto en el que opera, incluyendo a todos los colaboradores internos, externos, y terceras partes, que participen en las actividades de establecer, implementar, operar, monitorear, mantener y mejorar el SGSI.

3. Documentos relacionados

Esta política está relacionada a las políticas específicas de seguridad de la información vigentes.

Adicionalmente, se relaciona a:

- Roles y Responsabilidades del SGSI.
- Alcance del SGSI
- Contexto de la Organización
- Objetivos del SGSI
- Partes Interesadas del SGSI - Requisitos y expectativas

4. Política

- Cibergestión debe resguardar la confidencialidad, integridad y disponibilidad de la información y sus activos de información mediante la implementación de controles. Para ello la Organización debe:
    - Mantener inventarios de todos sus activos de información.
    - Establecer, implementar y mantener un proceso formal de evaluación de riesgos que sistemáticamente identifique, analice y evalúe las amenazas y vulnerabilidades a las que se encuentran expuestos los activos.
    - Evaluar las medidas de mitigación adecuadas para cada riesgo, de acuerdo con la Metodología de riesgo de seguridad de la información vigente, e implementar el plan de tratamiento que se defina.

- La Alta Administración debe determinar y proporcionar el apoyo y los recursos necesarios que permitan establecer, implementar y mantener un SGSI, alineado con los objetivos estratégicos de la organización.

- La Alta Administración debe designar uno o más responsables, con atribuciones y competencias necesarias para gestionar la seguridad de la información, con roles y responsabilidades claramente establecidos.

- Se debe disponer de un protocolo de respuesta ante incidentes, con una estructura de roles y responsabilidades definidas.

- Cibergestión debe fomentar una cultura de gestión de riesgos en materia de seguridad de la información, mediante planes formales de concientización/difusión y capacitación, de forma apropiada, entendible y accesible hacia los colaboradores de la organización.

- La gestión de seguridad de la información se debe alinear a las directrices y exigencias propias del cumplimiento de las normativas vigentes, y del marco de referencia ISO 27.001, en su versión vigente.

- Cibergestión debe llevar a cabo auditorías internas a intervalos planificados, para verificar la conformidad del SGSI con los requerimientos internos, normativos y las buenas prácticas adoptadas.

- Los documentos del SGSI de Cibergestión deben estar disponibles para los todos los colaboradores que se defina, y deben ser actualizados anualmente y/o cuando existan cambios significativos.

- Cibergestión debe identificar las oportunidades de mejora, así como los incumplimientos y no conformidades relativas al SGSI, y determinar las causas para poner en práctica las acciones correctivas apropiadas, que permitan alcanzar los resultados esperados.

- Cibergestión debe realizar mejoras continuas al SGSI para asegurar su actualización, idoneidad, adecuación y eficacia.

5. Roles y responsabilidades

Las funciones de los participantes en la gestión de la seguridad de la información de Cibergestión se encuentran registrados en el documento de Roles y responsabilidades del SGSI.

6. Aprobación, publicación y actualización

El área de Riesgo es responsable de revisar y/o actualizar la Política de seguridad de la información, anualmente y/o cuando existan cambios significativos.

Los cambios deberán ser expuestos al Comité de riesgos, para su revisión y aprobación. De igual forma, de no existir modificaciones, se deberá ratificar su vigencia en el mismo.

La Alta Administración de Cibergestión debe asegurar los mecanismos para que esta Política y sus modificaciones sean conocidas y estén disponibles permanentemente para todos los integrantes de la organización y de terceros.

La versión vigente de este documento está a disposición de todo el personal en la aplicación corporativa (Talana), y también para todas las partes interesadas, en el portal web de Cibergestión.