Política de seguridad de la información y ciberseguridad

Uso público

Responsabilidad y control de cambios

Propietario	Jefe de seguridad de la información y ciberseguridad
Revisor	Gerente de riesgo operacional 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

Índice de Contenidos

1. Objetivo del Documento 4
2. Alcance 4
3. Documentos Relacionados 4
4. Declaración de la Política 4
5. Principios de la Política 5
6. Roles y Responsabilidades 6
7. 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 y Ciberseguridad (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 terceros, queparticipen en las actividades de establecer, implementar, operar, monitorear, mantener y mejorar elsistema de gestión de la seguridad de la información y ciberseguridad.

3. Documentos Relacionados

- Política del Sistema de Gestión de Continuidad de Negocio.
- Política de Riesgo Operacional.
- Política Protección de Datos Personales
- Roles y Responsabilidades del sistema de gestión de seguridad de la información yciberseguridad.

4. Declaración de la Política

Cibergestión acuerda que el desarrollo de las actividades de la Organización y la consecución de los objetivos de la misma, requieren garantizar, en todo momento, el cumplimiento de los niveles establecidos de confidencialidad, disponibilidad e integridad para sus activos de información y cumplircon las Leyes y Reglamentaciones vigentes, manteniendo un equilibrio entre los niveles de riesgo y eluso eficiente de los recursos.

Con esta finalidad, se ha desarrollado e implantado el Sistema de Gestión de la Seguridad de la Información (SGSI), basado en la norma internacional ISO 27001:2020, que establece el marco de referencia para tratar de forma segura los activos de la Organización, y es aplicable a toda la organización.

Esta declaración se simplifica y se transmite a todos nuestros colaboradores y demás partes interesadas bajo el siguiente slogan:

No lo dejemos al azar, preparémoslo.

Para la aplicación del Sistema de Gestión se establecen como elementos primordiales los siguientes principios.

5. Principios de la Política

- La Alta administración debe determinar y proporcionar los recursos necesarios que permitan establecer un sistema de gestión de seguridad de la información y ciberseguridad, alineado con los objetivos estratégicos de la organización y que permita un modelo basado en mejora continua.
- Se debe fomentar las actividades y controles necesarios que permita preservar la confidencialidad, integridad y disponibilidad de la información, para el inventario actualizado de los activos de valor, así como aquellos críticos de la organización.
- Se debe realizar una efectiva evaluación y gestión del riesgo de seguridad de la información y ciberseguridad, mediante controles aplicables con el objeto de mitigar los efectos adversos, la gestión de alertas y amenazas y vulnerabilidades inherentes, que puedan afectar la seguridad de la información y la continuidad del negocio de la organización.
- La Alta Administración designará uno o más responsables, con atribuciones y competencias necesarias para gestionar la seguridad de la información y ciberseguridad, con roles y responsabilidades claramente establecidos.
- Se debe disponer de una estructura de alto nivel para la administrar y gestionar los incidentes de seguridad y ciberseguridad de alto impacto, como también los de menor impacto, pero mayor frecuencia, que afecten o pudieran afectar los activos de información, propios o los de sus clientes.
- La Alta Administración debe fomentar una cultura de riesgos en materia de seguridad de la información y ciberseguridad, mediante planes formales de difusión, capacitación y concientización, de forma apropiada, entendible y accesible hacia los colaboradores de la organización.
- La organización debe alinear el cumplimiento de las leyes y normativas vigentes para proceso de gestión de la seguridad de la información y ciberseguridad, así como la adhesión a los requisitos de las normativas Nch-ISO 27.001:2020 y el Capítulo 20-10 de la recopilación actualizada de normas (RAN) de la Comisión para el Mercado Financiero (CMF), así como también el tratamiento de desviaciones y excepciones.
- La organización debe garantizar que los sistemas de información y telecomunicaciones que dispone Cibergestión posean adecuado nivel de ciberseguridad y resiliencia. Se debe abordar temas específicos de seguridad de la información y ciberseguridad, a un nivel operacional, apoyado en políticas que profundicen la implantación de controles que indica el Anexo A de la normativa Nch-ISO 27.001:2020, así como el uso de buenas prácticas que indiquen otros estándares internacionales de ciberseguridad, y la mitigación de los riesgos asociados.
- La organización debe programar y realizar procesos de auditoría al proceso de gestión de seguridad de la información y ciberseguridad, considerando aspectos normativos de las políticas, y la eficacia de los procedimiento y controles definidos en estas materias.
- Cibergestión debe realizar mejoras continuas al SGSI para asegurar su idoneidad, adecuación y eficacia.

6. Roles y Responsabilidades

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

7. Aprobación, Publicación y Actualización

La Gerencia de riesgo operacional y seguridad de la información es responsable de revisar y/o actualizar la Política de Seguridad de la Información y Ciberseguridad, 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 terceros.