Política de Seguridad de la Información en la Gestión de la Continuidad del Negocio

Fecha: 10/11/2022
Versión: 1.0

Control de versiones

Fecha	Versión	Descripción	Autor
10/11/2022	1.0	Creación del Documento	Comité de Seguridad de la Información

Contenido

1 Revisiones

Fecha	Versión	Descripción	Autor
10/11/2022	1.0	Creación del Documento	Comité de Seguridad de la Información

2 Objetivo

Establecer los lineamientos generales para el mantenimiento de la seguridad de la información en el contexto del proceso de continuidad del negocio de ISA.

3 Alcance

Todos los activos de información involucrados en la continuidad del negocio de ISA.

4 Vigencia

La presente norma entra en vigor a partir de su aprobación y publicación por parte del Directorio de la empresa.

Esta política será revisada en un período no mayor a tres años, o ante cambios que así lo ameriten.

5 Responsabilidades

- Directorio
- Comité de Seguridad de la Información
- Propietarios de los activos de información

6 Desarrollo

- **Directorio** - es responsable de generar las condiciones adecuadas para la ejecución y comunicación de la presente política, así como de establecer el alcance para su aplicación.
- **Comité de Seguridad de la información** - es responsable de:

- Velar por el cumplimiento de la presente política y brindar asesoramiento en la identificación de las amenazas que pueden afectar a los activos de información y las vulnerabilidades que propician las mismas.
- Definir los aspectos de seguridad de la información en el plan de continuidad y recuperación ante desastres y gestionarlos en forma conjunta con los propietarios de los activos de información, los referentes de seguridad y el Área de Infraestructura /Operaciones.
- Brindar lineamientos, estándares, procedimientos funcionales y herramientas que faciliten la implementación de la gestión integral de riesgo a la Jefatura de Seguridad de la información.
- Cumplir con los lineamientos de la "Política de Gestión de la Seguridad de la Información en la Continuidad del Negocio" al momento de definir Planes de Continuidad del Negocio

- **Propietarios de los activos de información** son responsables de:
  - Identificar los procesos críticos, los activos y sistemas que lo soportan, así como de participar en la creación y las pruebas del plan de continuidad.
  - Realizar el análisis de impacto en el negocio si se vieran afectados los procesos críticos de sus áreas.

Continuidad de la seguridad de la información

Se debe:

- Monitorear los procedimientos y controles, así como el alcance de la presente política para mejorarlos ante cambios que así lo ameriten.
- Considerar, en el contexto del proceso de gestión de la continuidad del negocio todos los requisitos de seguridad de la información necesarios.
- Desarrollar un plan para restaurar las operaciones y asegurar la disponibilidad de la información al nivel requerido por la Administración.
- Documentar, implantar y mantener los procesos, procedimientos y controles para garantizar el nivel requerido de continuidad para la seguridad de la información durante una situación adversa.
- Realizar pruebas periódicas de los planes establecidos e implementados de la continuidad de la seguridad de la información, para verificar su validez y efectividad en situaciones adversas.

Redundancia

- Las instalaciones de procesamiento de información críticas para el negocio deben implantarse con la redundancia suficiente para cumplir con los requisitos de disponibilidad de la información requeridos por el negocio