TÍTULO DE LA POLÍTICA:	RESPUESTA A INCIDENTES Y ATAQUES DE CIBERSEGURIDAD
CÓDIGO DE LA POLÍTICA:	PTI-06
FECHA ÚLTIMA REVISIÓN:	10/05/24
N° DE REVISIÓN:	1
ELABORÓ:	Tecnologías de Información
ALCANCE:	Todos los colaboradores de la Organización, contratistas, proveedores y terceros.
OBJETIVO:	La presente política tiene como objetivo establecer procedimientos claros y efectivos para identificar, responder y mitigar incidentes de seguridad cibernética, minimizando así los impactos negativos en la organización. También busca garantizar la continuidad del negocio y proteger la confidencialidad, integridad y disponibilidad de los datos.

POR L.F.T:

Sin fragmento o disposición jurídica.

POLÍTICAS Y LINEAMIENTOS GENERALES

a) Establecer un lineamiento general para respuesta en situación de ciberataques potenciales.

b) Asegurar que todo el personal de la empresa entienda sus deberes y responsabilidades al momento de ser blancos de posibles ciberataques.

c) Prevenir el mal uso, accidental o intencional de la información y mitigar el impacto de las amenazas de ciberseguridad.

ALCANCE Y DISPOSICIÓN GENERAL

En disposición de la autorización que se otorga a los colaboradores de Fibra Inn que interactúen con los sistemas, datos y recursos de la organización se determina que tiene un impacto directo en Tecnologías de la Información, procesos y en personas. A continuación, se enlista el alcance que esta política pretende:

Alcance de política seguridad de la información	
Tecnologías de Información	El equipo de tecnologías de Información es el responsable de gestionar la continuidad operativa de las herramientas y/o plataformas seleccionadas para mantener la operación tecnológica de la organización, esto incluye las herramientas de uso diario que albergan la información de cualquier nivel de la organización. Así como también, de proveer capacitación constante para garantizar la actualización de conocimientos de factores de riesgo que puedan afectar la organización.
Procesos	Son procesos aquellos que se implementan para garantizar la respuesta oportuna en un posible evento de ataque tecnológico.
Personas	Esta política aplica a todos los usuarios activos en la organización y que cuenten con la identificación de número de empleado vigente, así como aquellos proveedores y terceros que tengan un contrato que los vincule con el rendimiento de los objetivos de la empresa.

DISPOSICIÓN GENERAL

Esta política de ciberseguridad proporciona un marco sólido para abordar incidentes y ataques cibernéticos de manera efectiva y proteger los activos de la organización. Es esencial adaptarla a las necesidades específicas de tu organización, involucrando a expertos en ciberseguridad para garantizar su efectividad y relevancia.

RESPONSABILIDADES

Equipo de Respuesta a Incidentes (Soporte TI)

- Designar un líder del equipo de respuesta a incidentes. Véase Anexo A "**Matriz de escalabilidad de ciberataques"**
- Identificar, analizar, contener, mitigar y recuperarse de los incidentes de seguridad cibernética. Véase Anexo B "**Matriz de responsabilidad tecnológica según escala del incidente"**
- Coordinar y colaborar con los equipos relevantes para garantizar una respuesta eficiente y efectiva.
- Mantener la documentación actualizada de los incidentes, acciones tomadas y lecciones aprendidas.
- Realizar simulacros y pruebas de respuesta a incidentes regularmente.

Equipo de TI y Seguridad

- Brindar apoyo técnico para investigar incidentes de seguridad y ejecutar acciones de respuesta.
- Colaborar en la implementación de medidas preventivas y correctivas basadas en las lecciones aprendidas.
- Mantener actualizado el inventario de activos y su estado de seguridad.

Personal de la Organización

- Reportar inmediatamente cualquier sospecha o incidente de seguridad a los canales designados.
- Colaborar con el equipo de soporte TI en la investigación y respuesta a incidentes.
- Participar en programas de capacitación y concienciación sobre seguridad cibernética.

PROCEDIMIENTOS DE RESPUESTA A INCIDENTES

Detección e Identificación de Incidentes

- Establecer alertas y sistemas de monitoreo para detectar posibles incidentes de seguridad.
- Fomentar la cultura de reporte de incidentes para detectarlos de manera temprana.
- Investigar y evaluar la naturaleza y el alcance del incidente para determinar su gravedad y el tipo de incidente.

Clasificación y Priorización de Incidentes

- Clasificar los incidentes según su gravedad, impacto y nivel de riesgo para el negocio. Véase Anexo C **"Matriz de Riesgos Cibernéticos"**
- Utilizar un sistema de puntuación o matriz de riesgo para priorizar las acciones de respuesta.
- Establecer un grupo de revisión para validar la clasificación y priorización.

Contención y Mitigación

- Tomar medidas inmediatas para contener y mitigar el incidente y evitar su propagación.
- Implementar soluciones temporales y parches de seguridad, si es necesario, siguiendo un proceso de cambio controlado.
- Establecer líneas de comunicación claras y canales de autorización para las acciones de contención.

Investigación y Análisis Forense

- Realizar un análisis forense para determinar la causa raíz del incidente y las vulnerabilidades explotadas.
- Documentar todas las evidencias de forma segura y confidencial para futuras acciones legales o investigativas.

Notificación y Comunicación

- Notificar a las partes interesadas internas y externas sobre el incidente y las acciones tomadas.
    - Notificar periódicamente en plazos mensuales a la Dirección de Administración y Finanzas y/o Dirección General todos los eventos reportados como posibles amenazas y riesgos de ciberseguridad que puedan afectar a Fibra inn.
- Coordinar la comunicación con las autoridades regulatorias y legales según las leyes y regulaciones aplicables.

- Preparar plantillas de comunicación para responder de manera rápida y precisa.

Recuperación y Mejora Continua

- Restaurar los sistemas y datos afectados a un estado seguro y funcional.
- Analizar el incidente para identificar lecciones aprendidas y recomendaciones de mejora.
- Actualizar las políticas, procedimientos y medidas de seguridad en consecuencia.
- Realizar reuniones post incidencias para discutir mejoras y ajustes necesarios.

CAPACITACIÓN Y CONCIENTIZACIÓN

Realizar capacitaciones periódicas sobre ciberseguridad, incluyendo simulacros de incidentes, para todos los empleados. También se deben llevar a cabo programas de concienciación regulares para fomentar la cultura de seguridad.

REVISIÓN Y ACTUALIZACIÓN

Revisar y actualizar esta política y sus procedimientos regularmente para asegurar que estén alineados con las mejores prácticas de ciberseguridad y los cambios en la tecnología y el entorno operativo de la organización. Realizar auditorías internas y externas para evaluar el cumplimiento de la política.

CONSECUENCIAS DE MAL USO

La omisión de las prácticas o por el incumplimiento a lo descrito en esta política, da lugar a la aplicación de medidas administrativas, disciplinarias o legales que establece la organización.

ANEXO A. MATRIZ DE ESCALABILIDAD DE CIBERATAQUES

Esta matriz describe la escala de ataques cibernéticos en función del alcance, la complejidad y el área de la empresa a quien debe reportarse.

Escala de Ataque	Descripción	Ejemplos	Notificación inmediata
Baja Escala	Ataques aislados o de bajo alcance que afectan a individuos o sistemas específicos.	Ataque de phishing a un empleado individual.	1.- Soporte Técnico 2.- Dirección de Tecnología
Mediana Escala	Ataques dirigidos a un grupo más amplio de usuarios o sistemas, pero aún controlables con medidas de seguridad adecuadas.	Ataque de ransomware que afecta a un departamento o sucursal.	1.- Dirección de Tecnología 2.- Soporte Técnico 3.- Dirección de Administración y Finanzas 4.- Dirección General
Alta Escala	Ataques masivos que pueden comprometer múltiples sistemas y redes a gran escala, afectando a una organización en su conjunto.	Ataque de DDoS a la infraestructura de la empresa.	1.- Dirección de Tecnología 2.- Soporte Técnico 3.- Dirección General 4.- Dirección de Administración y Finanzas comités??, IR (BMV)?, Legal?
Muy Alta Escala	Ataques altamente coordinados y sofisticados que se dirigen a múltiples organizaciones o incluso a nivel nacional o global.	Ataque de un grupo de hackers respaldados por un Estado-nación que afecta a múltiples organizaciones en varios países.	1.- Dirección de Tecnología 2.- Soporte Técnico 3.- Dirección General 4.- Dirección de Administración y Finanzas comités ??,

ANEXO B. MATRIZ DE RESPONSABILIDAD TECNOLÓGICA SEGÚN ESCALA DEL INCIDENTE

Esta matriz proporciona una estructura para entender cómo varía la respuesta del equipo de Soporte TI según la gravedad y el alcance del incidente. Cada nivel de escalabilidad implica un aumento en la complejidad de las acciones y la necesidad de coordinación con varios equipos y partes interesadas, tanto internas como externas.

Escala de Incidente	Descripción	Acciones del equipo de Soporte TI
Baja Escala	Incidentes aislados o de baja gravedad que pueden ser manejados internamente con procedimientos establecidos.	- Investigación y análisis del incidente. - Contención y mitigación inmediata. - Documentación y lecciones aprendidas para mejora continua.
Mediana Escala	Incidentes que requieren una coordinación y respuesta más elaborada que involucra a varios departamentos o sistemas.	- Coordinación con otros departamentos relevantes. - Análisis forense detallado. - Acciones de contención y mitigación ampliadas. - Notificación y comunicación interna.
Alta Escala	Incidentes graves que impactan en una amplia parte de la organización y requieren una respuesta urgente y coordinada a nivel organizativo.	- Actuación inmediata según un plan de respuesta a incidentes detallado. - Coordinación interdepartamental y con expertos externos. - Comunicación ampliada y coordinada con las autoridades competentes.
Muy Alta Escala	Incidentes masivos que afectan a toda la organización o incluso a nivel nacional o global, requiriendo coordinación a gran escala y posiblemente la ayuda de organizaciones externas o gobiernos.	- Coordinación integral y ágil con todos los departamentos y equipos relevantes. - Colaboración activa con agencias gubernamentales, expertos de la industria y organismos de ciberseguridad. - Movilización de recursos adicionales según sea necesario para la respuesta.

ANEXO C. MATRIZ DE RIESGOS CIBERNÉTICOS

En esta matriz de riesgos, la **probabilidad** indica cuán probable es que ocurra un tipo específico de ataque, mientras que el **impacto** refleja la gravedad de las consecuencias si el ataque se materializa. **El nivel de riesgo** se determina combinando la probabilidad y el impacto, lo que proporciona una visión general de la severidad del riesgo.

Tipo de Ataque	Probabilidad (Alta, Media, Baja)	Impacto (Alto, Medio, Bajo)	Nivel de Riesgo (Alto, Medio, Bajo)
Phishing	Alta	Alto	Alto
Malware	Media	Alto	Alto
Ataque de DDoS	Media	Alto	Alto
Inyección de SQL	Media	Alto	Alto
Ataque de Fuerza Bruta	Media	Medio	Medio
Ataque de Ingeniería Social	Alta	Medio	Alto
Ataque a la Web	Media	Medio	Medio
Ataque a la Red	Media	Medio	Medio
Ataque Zero-day	Baja	Alto	Medio
Ransomware	Media	Alto	Alto

SECCIÓN DE FIRMAS

Autoriza/Revisado por	Puesto	Firma
MIGUEL ALIAGA GARGOLLO	Dirección General	
JUAN A. RIVAS CARRIÓN	Dirección de Tecnologías de la Información	