TÍTULO DE LA POLITICA:	SEGURIDAD DE LA INFORMACIÓN
CÓDIGO DE LA POLÍTICA:	PTI-04
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 las reglas y lineamientos necesarios para garantizar la seguridad de la información de la empresa, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información en todos sus formatos

POR L.F.T:

Sin fragmento o disposición jurídica.

POLÍTICAS Y LINEAMIENTOS GENERALES

a) Identificar los requisitos necesarios y mejores prácticas recomendadas para resguardar la seguridad e integridad de la información de Fibra Inn.

b) Asegurar que todo el personal de la empresa entienda sus deberes y responsabilidades al tener acceso a información de la empresa, independientemente del formato en el que se encuentre.

c) Prevenir el mal uso, accidental o intencional de la información y mitigar el impacto de las amenazas de ciberseguridad, el acceso no autorizado, daño causado por negligencia o desconocimiento, actividades ilegales, acoso o fraude.

ALCANCE Y DISPOSICIÓN GENERAL

En disposición de la autorización que se otorga a los colaboradores de Fibra Inn para acceder y conocer la información que se genera en 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.
Procesos	Son procesos aquellos que se implementen para garantizar y resguardar la calidad e integridad de la información.
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

- La presente política establece los lineamientos para:
  - Acceso a información
  - Protección de la información
  - Uso de dispositivos personales
  - Protección según su nivel de confidencialidad y tipo de información
  - Incidentes de seguridad
  - Formación y concientización

- La creación y manipulación de información debe tratarse según los niveles de confidencialidad descritos en esta política.

- La disponibilidad de información tanto en dispositivos electrónicos como en material físico debe tratarse con la misma rigurosidad aplicando las mejores prácticas para salvaguardar la integridad y confidencialidad de la información.

- Toda decisión de divulgación de información es responsabilidad de cada usuario y deberá apegarse a los lineamientos permitidos por la organización.

- Si, en el ejercicio de sus funciones, el personal de tecnologías de información detecta cualquier situación que muestre indicios de riego informático que pueda poner en riesgo la integridad y confidencialidad de la información como lo establece esta política, lo pondrá en conocimiento del líder del área de tecnología y de la Dirección de Administración y Finanzas o la Dirección General.

- Es obligación de la empresa concientizar y capacitar al personal para entender y ejecutar adecuadamente la responsabilidad de uso descrita en esta política en materia de protección de información, así como también es responsabilidad de cada empleado, contratista o tercero, hacer valer el reglamento descrito.

- El área de Tecnologías de Información es responsable de establecer los lineamientos y reglamentos de usos de dispositivos que salvaguarden la calidad y confidencialidad de la información.

ACCESO A LA INFORMACIÓN EN MEDIO DIGITALES

- Se deben establecer permisos de acceso a la información de acuerdo con el perfil y función del empleado.
- Los usuarios deben autenticarse antes de acceder a la información.
- El acceso a la información debe ser restringido a los empleados que lo necesiten para realizar sus funciones.
- Se deben establecer políticas de separación de funciones para reducir el riesgo de fraude y error.

PROTECCIÓN DE LA INFORMACIÓN

- Todos los dispositivos móviles que contengan información de la empresa deben contar con contraseñas de acceso seguras (**POLÍTICA DE CONTRASEÑAS GENERALES**) y cifrado de datos.
- Los documentos físicos que contengan información confidencial deben estar resguardados en lugares seguros y bajo llave.
- Los documentos electrónicos deben ser almacenados en servidores seguros y con copias de seguridad periódicas.
- La información crítica debe ser respaldada de forma regular en dispositivos de almacenamiento externos y en la nube.
- Se deben establecer políticas de retención y disposición de información para garantizar que la información se conserve el tiempo necesario y se destruya de manera segura cuando ya no sea necesaria.
- Se deben implementar controles de acceso y vigilancia en los centros de datos y en las instalaciones de la empresa

USO DE DISPOSITIVOS PERSONALES

- Los dispositivos personales no deben ser utilizados para el acceso a información crítica de la empresa, a menos que se haya establecido previamente un acuerdo formal entre la empresa y el empleado.
- Se deben establecer políticas claras para el uso de dispositivos personales en el trabajo.

- Los dispositivos personales que se utilicen para acceder a información de la empresa deben contar con las medidas de seguridad adecuadas.
- Se deben establecer políticas claras de borrado remoto de datos en caso de pérdida o robo de dispositivos personales.
- Los empleados deben informar inmediatamente cualquier pérdida o robo de un dispositivo personal que haya sido utilizado para acceder a información de la empresa.

PROTECCIÓN SEGÚN SU NIVEL DE CONFIDENCIALIDAD Y TIPO DE INFORMACIÓN

Se deberá definir un modelo de clasificación de la información que permita conocer e implantar las medidas técnicas y organizativas necesarias para mantener su disponibilidad, confidencialidad e integridad. El modelo de clasificación deberá integrar los requisitos y condiciones establecidos en la presente política.

1. **Tipos de información**
   a. **Soportes lógicos:** información que esté siendo utilizada mediante medios ofimáticos, correo electrónico o sistemas de información desarrollados a medida o adquiridos a un tercero.
   b. **Soportes físicos:** información que esté en papel, soportes magnéticos como USBs, CD, DVDs, etcétera.

2. **Niveles de clasificación**
   En función de la sensibilidad de la información, Fibra Inn catalogará la información en cinco niveles, véase la definición precisa en el Anexo A **"Niveles de clasificación de información"**:
   a. Uso público
   b. Difusión limitada
   c. Información confidencial
   d. Información reservada
   e. Información secreta

3. **Gestión de información privilegiada**
   La información que se considere reservada, confidencial o secreta se deberá tratar con especial cuidado. Se deberán definir medidas de seguridad extraordinarias o adicionales para el adecuado tratado de la información privilegiada. Este tipo de información se deberá enviar cifrada y mediante protocolos seguros. Véase Anexo B **"Herramientas para la gestión de información privilegiada"**:

4. **Privacidad de la información**
    - La organización y sus colaboradores deberán garantizar la privacidad de los datos de carácter personal con el objetivo de proteger los derechos fundamentales de las personas físicas, especialmente su derecho al honor, intimidad personal y familiar y a la propia imagen, mediante el establecimiento de medidas para regular el tratamiento de los datos.
    - La organización y sus colaboradores deberán cumplir con la legislación vigente en materia de protección de datos personales en función de la jurisdicción en la que esté establecida y opere en las Leyes Mexicanas de Protección de Datos y deberá incluir las medidas necesarias para cumplir con la normativa.

INCIDENTES DE SEGURIDAD

- Los empleados deben informar inmediatamente cualquier incidente de seguridad que hayan identificado o que les hayan notificado.
- La empresa debe contar con un plan de respuesta a incidentes que incluya procedimientos de notificación, evaluación, contención, recuperación y mejora.
- Se debe establecer un equipo responsable de la gestión de incidentes de seguridad.
- Los incidentes de seguridad deben ser registrados y analizados para determinar las causas raíz y establecer medidas preventivas.

FORMACIÓN Y CONCIENTIZACIÓN

- La organización deberá asegurar que todo el personal reciba un nivel de formación y concienciación adecuado en materia de Seguridad de la Información en los plazos que exija la normativa vigente, especialmente en materia de confidencialidad y prevención de fugas de información.
- Asimismo, los empleados deberán ser informados de las actualizaciones de las políticas y procedimientos de seguridad en los que se vean afectados y de las amenazas existentes, de manera que pueda garantizarse el cumplimiento de esta Política.
- Por otro lado, los empleados tienen la obligación de obrar con diligencia con respecto a la información, debiéndose asegurar que dicha información no caiga en poder de empleados o terceros no autorizados.

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. NIVELES DE CLASIFICACIÓN DE INFORMACIÓN

NIVELES DE CLASIFICACIÓN:

Nivel	Detalle Nivel	Ejemplos
Uso público	Los datos pueden ser adquiridos por cualquier individuo, y el empleo malicioso de dicha información no representa una amenaza para los intereses de FINN	Cualquier información está disponible en la página Web oficial de Fibra Inn.
Difusión limitada	Es la información que son empleados por los distintos departamentos de FINN, y si se utilizan de forma fraudulenta, podrían representar un riesgo leve para los intereses de la empresa	Cualquier información como los correos electrónicos y los documentos de trabajo.
Información Confidencial	Son aquellos datos confidenciales que solo un grupo selecto de personas tiene acceso, y el uso fraudulento de los mismos podría tener un impacto considerable en los intereses de FINN.	Cualquier informe de auditoría o planes estratégicos de dirección organizacional.
Información Reservada	Es la información que debe ser exclusivamente conocida por su propietario y cuya revelación podría causar daños significativos a los intereses de FINN	Comunicación o estrategia de negocio entre altos directivos y accionistas que representen decisiones de continuidad operativa.
Información Secreta	Es información que, si se divulga sin autorización, puede generar un daño sumamente grave a los intereses de FINN	Información de adquisiciones, desincorporaciones o cualquier situación que pueda afectar el precio de la acción en el mercado de valores.

ANEXO B. HERRAMIENTAS PARA LA GESTIÓN DE INFORMACIÓN PRIVILEGIADA

NIVELES DE CLASIFICACIÓN Y HERRAMIENTAS AUTORIZADAS:

Nivel	Herramientas Autorizadas
Uso público	Página WEB oficial de Fibra inn, correo electrónico corporativo, unidades de almacenamiento internas o externas, Redes Sociales corporativas, Whatsapp, Google Drive, ShareFile, DropBox, Diligent
Difusión limitada	Correo electrónico corporativo, unidades de almacenamiento internas o externas cifradas y con autenticación, Redes Sociales corporativas, Whatsapp con doble autenticación, Google Drive, ShareFile, DropBox, Diligent.
Información Confidencial	Correo electrónico corporativo, unidades de almacenamiento internas o externas cifradas y con autenticación, Whatsapp con doble autenticación, Google Drive, ShareFile, DropBox, Diligent.
Información Reservada	Correo electrónico corporativo, Google Drive, ShareFile, DropBox, Diligent.
Información Secreta	Correo electrónico corporativo, Diligent.

SECCIÓN DE FIRMAS

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