Clasificación de la Información	PÚBLICA	PL-PT-01-01

Documentación de Política Interna

Política de Seguridad de la Información

Historial de Versiones

Fecha	Versión	Creado por	Descripción	Aprobó
12/05/2024	1.0	Mariano Casero	Documentación Inicial	Dirección

Índice

1. Objeto

Establecer las pautas a seguir y las obligaciones a cumplir en materia de Seguridad de la Información, tendiente a proteger los activos de la compañía.

2. Alcance

Los empleados, personal externo, proveedores, contratistas, socios de negocio y terceras partes que accedan, procesen y/o manejen Información de FINNEGANS.

2.1. Consideraciones generales

Una buena estrategia de Seguridad de la Información es contar con una Política implementada y documentada, donde se establezcan las pautas a seguir y las obligaciones a cumplir en materia de Seguridad de la Información y que además sirva como punto de partida para elaborar normas y procedimientos tendientes a proteger los activos de la compañía y la mejora continua del sistema de gestión de Seguridad de la Información.

3. Definiciones

Características:
La seguridad de la información se entiende como la preservación de las siguientes características:

- **Confidencialidad**

La información debe ser accedida solamente por personas, entidades o procesos autorizados y los derechos de propiedad sobre la información deben estar adecuadamente establecidos.

- **Integridad**
  La información debe mantenerse precisa y completa, sin modificaciones no autorizadas.

- **Disponibilidad**
  La información debe mantenerse accesible y utilizable por las personas, entidades o procesos debidamente autorizados, en el momento en que sea requerido.

- **Gestión del Riesgo**
  Los activos de información de importancia deben identificarse y clasificarse; las vulnerabilidades y las amenazas sobre los activos deben identificarse y analizarse; los riesgos deben evaluarse y tratarse con controles de Seguridad de la Información.

- **Información**
  Se refiere a un conjunto organizado de datos procesados, que se presentan de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisuales u otros.

- **Sistema de Información**
  Es un conjunto de elementos orientados al tratamiento y administración de datos e información que ayudan a administrar, recolectar, recuperar, procesar, almacenar y distribuir información relevante para los procesos fundamentales y las particularidades de la organización.

- **Tecnología de la Información**
  Hardware y software operados en el ámbito de la empresa o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Negocio.

- **Participación del Personal**
  El personal es la esencia de la empresa, y su total implicación mediante las actividades de concientización, educación y entrenamiento posibilita que sus capacidades sean utilizadas para beneficio de los objetivos de seguridad.

4. Política

La información es un recurso que, como el resto de los activos, tiene valor para la Compañía y por consiguiente debe ser debidamente protegida. Es importante que los principios de la Política de Seguridad de la Información sean parte de la cultura de la compañía. Para esto, se debe asegurar un compromiso manifiesto de la Dirección, de los Gerentes y Coordinadores para la difusión, consolidación y cumplimiento de la presente Política. Esta Política se conforma de una serie de pautas sobre aspectos específicos de la Seguridad de la Información, que incluyen los siguientes tópicos:

Concientización y capacitación

Todos los empleados deberán conocer la importancia de la seguridad de información para el éxito comercial de FINNEGANS y su rol individual en el aseguramiento de la protección de los recursos informáticos que tiene bajo su responsabilidad. Se deberán comunicar los lineamientos de seguridad que aplica a los empleados de FINNEGANS, contratados y personal externo.

Apoyo de niveles jerárquicos

Debe existir compromiso visible de los gerentes y los niveles directivos, en el cumplimiento de políticas y prácticas de Seguridad de la información.

Entrenamiento del personal de seguridad

Se debe proporcionar capacitación técnica continua a todo el personal que va a desarrollar tareas relacionadas a la administración de seguridad.

Capacitación del personal

Toda modificación a esta política deberá incluir una capacitación al personal, asegurándose de que hayan comprendido los conceptos definidos en esta. Las mismas deben ser registradas y guardadas como evidencia del entendimiento.

Tecnología avanzada

Se debe implementar tecnología que soporte los procesos del negocio de manera eficiente y proporcione niveles apropiados de protección de información.

Evaluaciones y gestión del riesgo

Se debe analizar los riesgos comerciales a los que se expone el negocio con cada nuevo proyecto de desarrollo, lanzamiento de un nuevo producto, diseño de una nueva arquitectura tecnológica, o todo proyecto que involucre información de FINNEGANS, desarrollando un análisis de costo–beneficio.
Complementario a este documento, se cuenta con la política PL-PT-02-01 “Gestión del Riesgo de SI”, que indica los métodos utilizados para identificar los riesgos y evaluar la efectividad de sus mitigantes, minimizando el impacto en los procesos de la empresa.

Uso apropiado de los recursos

El equipamiento informático, software e infraestructura que Finnegans pone a disposición de sus empleados, debe utilizarse para los propósitos de negocio para los que ha sido concebido. Además, la información que procesan estos recursos es propiedad de Finnegans y debe ser tratada de manera confidencial.
El uso apropiado de los recursos se encuentra detallado en el documento PL-PT-03-01 “Política de uso de los recursos”, complementario a esta política.

Métricas e indicadores

Se debe definir un sistema de indicadores que permita verificar el funcionamiento del esquema de administración de seguridad de

información y optimizarlo a través de la retroalimentación con los resultados obtenidos.

Monitoreo

Se deben establecer revisiones continuas de las actividades de manipulación de la información, para asegurar que existan mecanismos apropiados de seguridad y que los procedimientos implementados sean efectivos.
Controlar el acceso a la información y a los sistemas que la procesan en base a los requisitos del negocio y de la seguridad; los mismos solo deben ser concedidos de acuerdo con la necesidad de conocimiento. Se debe prevenir a través de controles técnicos apropiados los accesos no autorizados a los sistemas de información.

Gestión de la continuidad del negocio

Desarrollar controles sobre los planes de recuperación ante desastres y de continuidad del negocio para garantizar el normal funcionamiento de las unidades de negocio y ambientes de tecnología ante una contingencia.

Propiedad de la Información

Todos los datos, programas, sistemas y procedimientos (en adelante denominados “información”) recolectados, almacenados, procesados y/o mantenidos por la Compañía, para propósitos del negocio, son de propiedad de FINNEGANS a menos que se haya establecido explícitamente de otra manera en un acuerdo contractual.

Criticidad de la información

La información es un activo clave para FINNEGANS, por esto la Compañía debe contar con un ambiente de administración, procesamiento, transporte y distribución de esta adecuadamente seguro. La “confidencialidad, integridad y disponibilidad” de información son esenciales para preservar la competitividad, facturación, rentabilidad y el cumplimiento de los requisitos legales, además de la imagen de la Compañía en el mercado.

FINNEGANS debe asegurar la protección de información y recursos estratégicos propios y de sus clientes, siempre que se encuentren bajo el control de FINNEGANS.

Confidencialidad de la Información

La información en concordancia con lo definido por la Política de Tratamiento de Datos Personales debe protegerse en forma efectiva. El carácter de confidencialidad de la información propiedad de los clientes y aquella que se encuentre alcanzada por la ley 25.536 de Protección de Datos Personales (Argentina) podrá ser intervenido y revocado única y exclusivamente por una orden judicial competente.

Seguridad física y ambiental

Realizar controles sobre la eficacia de las medidas de protección físicas implementadas para proteger instalaciones y equipos de procesamiento de información contra amenazas físicas, lógicas y/o ambientales que podrían afectar la seguridad de la información.

Gestión de incidentes de Seguridad de la Información

Una apropiada gestión de los incidentes de seguridad reduce al mínimo el daño causado por los mismos, permite el monitoreo y desarrollo de una base de conocimiento.

4.1. Responsabilidades

El área de Seguridad de la Información debe coordinar la implementación y el mantenimiento de un conjunto de acciones y medidas adecuadas para garantizar que la información y la estructura que la soporta se encuentre protegida de destrucción, corrupción, accesos no autorizados y violación de la confidencialidad, tanto sea en forma accidental como deliberada.

Una seguridad de información efectiva sólo puede obtenerse a través de medidas y acciones consistentes, vigilancia confiable, monitoreo continuo, una estrecha cooperación y concientización de

todos los niveles corporativos. A tal efecto, se detallan las siguientes medidas y acciones:

- Definir la estructura funcional necesaria para administrar y controlar la seguridad de la información dentro de FINNEGANS y mantener los niveles de seguridad de la información apropiados cuando la responsabilidad por el procesamiento de la información es delegada a otra organización.
- Asegurar que el personal de FINNEGANS esté capacitado para respaldar las políticas de seguridad de la organización, en el desarrollo de sus tareas habituales.
- Establecer controles físicos para proteger los sitios que contienen los bienes de información de la empresa, los soportes físicos de la información y el equipamiento e instalaciones utilizadas en el procesamiento de la información.
- Asegurar la protección de la infraestructura de apoyo y de los procesos operativos asociados.
- Mantener la seguridad del software y los sistemas de información desarrollados en FINNEGANS, y garantizar que se encuentran documentados los procesos de desarrollo para asegurar que, proyectos y actividades de soporte y pruebas de sistemas, se lleven a cabo de manera segura.
- Controlar el acceso a la información y a los sistemas que soportan el manejo de esta, impedir accesos no autorizados y establecer mecanismos de control que permitan detectar actividades no autorizadas.
- Asegurar el cumplimiento de leyes, estatutos, normas, reglamentos o contratos en lo referente a Seguridad de la información y garantizar la compatibilidad de los sistemas con las políticas, estándares y normas de seguridad de la organización.

4.2. Validez y gestión del documento

El propietario de este documento es el responsable de Seguridad de la información, quién debe utilizarlo como guía de control para

generar un plan de concientización apropiado para la organización.

El propietario de este documento debe realizar una revisión anual de este y en caso de que lo considere, realizar las actualizaciones correspondientes.

5. Excepciones

Toda excepción a este documento deberá contar con la aprobación formal de la Dirección y quedar documentada de forma adecuada.

6. Consecuencias del Incumplimiento

En caso de incurrir en el incumplimiento de esta política, o de las normas, procedimientos y estándares relacionados con la seguridad de la información; podrá ser pasible de sanciones disciplinarias. El área de Recursos Humanos analizará las medidas a implementar en caso de incumplimiento de la presente política.

7. Referencias y Anexos (opcional)

- PL-PT-02 Política de Gestión del Riesgo de SI
- PL-PT-03 Política de uso de los recursos