PSI01 - POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1.0 OBJETIVO

Establecer la postura en seguridad de la información de la compañía, lineamientos para su debida gestión y los roles y responsabilidades pertinentes.

2.0 ALCANCE

Esta política deberá ser informada y estar disponible a todo el personal interno o externo (Proveedores o Clientes) de Feeling Company

3.0 RESPONSABLES

3.1 RESPONSABLE DE DEFINIRLA

El Encargado de Seguridad de la Información deberá revisar la presente política y relacionadas por lo menos una vez al año o toda vez que haya un cambio significativo, con el fin de garantizar que es adecuada a las necesidades de la organización.

3.2 RESPONSABLE DE CUMPLIRLA

Esta política es de carácter obligatorio para todo el personal interno o externo que acceda a los recursos o activos de información de Feeling Company.

3.3 RESPONSABLE DE HACERLA CUMPLIR

El Gerente de Estrategia y Comercial deberá velar por el cumplimiento de la presente política y escalar las excepciones al Comité de Gerencia o máxima instancia en seguridad de la información, para su respectiva aprobación.

3.4 RESPONSABLE DE MONITOREARLA

El Coordinador de Calidad será el encargado de definir e implementar la estrategia de monitoreo de cumplimiento de la presente política.

3.5 RESPONSABLE DE VALIDAR SU CUMPLIMIENTO

El Controller será responsable de validar el cumplimiento de esta política.

4.0 POLÍTICAS

4.1 POLÍTICA/DECLARACIÓN GENERAL

Proteger la información que nuestros clientes nos han confiado, hace parte fundamental de nuestro compromiso y propósito. En Feeling Company, la seguridad de la información es un atributo de nuestro servicio, y por ello, trabajamos día a día para que la información generada, procesada o resguardada en nuestros procesos e infraestructura tecnológica, esté protegida.

Feeling Company, coherente con su propósito, se compromete en la aplicación y la mejora continua de la seguridad de la información orientada a la protección de los activos de información, con el fin de asegurar su confidencialidad, integridad y disponibilidad, favoreciendo el eficiente cumplimiento de los objetivos estratégicos de la organización.

Para ello, Feeling Company dispone de un Programa para la Gestión del Ciber Riesgo y Ciber Seguridad impulsado por la Junta de Socios que aporta un enfoque sistemático para la gestión oportuna de riesgos y su respectivo tratamiento. La referencia para establecer, implantar, mantener y mejorar dicho programa es la serie de estándares ISO/IEC 27000 y NIST Cyber Security Framework.

Objetivos y principios

Feeling Company velará por:

1. Que todo proyecto o contrato especifique los requisitos o expectativas de seguridad de la información entre las partes.
2. Proteger la información de las amenazas originadas por parte del personal.
3. Mantener una protección adecuada de los activos de información, según su sensibilidad o criticidad.
4. Implementar control de acceso a la información, sistemas y recursos de red.
5. Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.
6. Proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
7. Controlar la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos
8. Asegurar la protección de la información en las redes y mantener la seguridad de la información transferida interna o externamente.
9. Garantizar que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
10. Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.
11. Implementar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.
12. Garantizar la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
13. Garantizar el cumplimiento de las obligaciones legales, regulatorias y/o contractuales establecidas.

Roles y Responsabilidades en Seguridad de la Información

- La Junta de Socios es responsable de velar por que la seguridad de la información se gestiona adecuadamente en toda la organización.
- El Encargado de Seguridad de la Información asesora al equipo directivo, proporcionando apoyo especializado en el establecimiento y mantenimiento del programa de ciberseguridad de la compañía.
- El Encargado de Seguridad de la Información mantiene contactos apropiados con las autoridades pertinentes.
- El Encargado de Seguridad de la Información también mantiene contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
- Cada líder de área es responsable de garantizar que las personas que trabajan bajo su control protegen la información de acuerdo con las normas establecidas por la organización.
- Cada líder de área y en general el personal, es responsable de identificar y separar responsabilidades en conflicto, para reducir las posibilidades de modificación no autorizada.
- Cada miembro del personal interno o externo tiene la responsabilidad de mantener la seguridad de información dentro de las actividades relacionadas con su trabajo.

Indicadores

- (Número de vulnerabilidades críticas identificadas y mitigadas dentro de un tiempo predefinido/Número de vulnerabilidades críticas identificadas durante un determinado tiempo) * 100
- (Número de personas que ha completado o presenciado jornadas de entrenamiento o sensibilización en seguridad de la información/Total de personas) * 100
- (Número de productos nuevos que han sido sometidos a pruebas de seguridad antes de ser entregados/Total de productos nuevos) * 100
- (Número de sistemas de información cuyos planes de contingencia han sido probados/ Total número de sistemas en el inventario) * 100
- (Número de sistemas o servicios adquiridos que incluyen especificaciones o requisitos de seguridad/Total números de sistemas o servicios adquiridos) * 100

Incumplimiento

El incumplimiento de la presente política por parte de un funcionario, contratista o tercero, será sancionada de acuerdo con el Reglamento Interno Vigente.

4.2 POLÍTICAS RELACIONADAS

- Política de Seguridad de la Información
- Política de la Organización de Seguridad de Información
- Política de Seguridad para Dispositivos Móviles
- Política de Seguridad para el Trabajo Remoto
- Política de Seguridad en el Proceso de Gestión del Recurso Humano
- Política de Gestión de Activos de Información
- Política de Clasificación de Activos de Información
- Política para el Uso Aceptable de los Activos de Información
- Política de Dispositivos Removibles
- Política de Control de Acceso
- Política de Control de Acceso a Sistemas y Aplicaciones
- Política de Gestión de Contraseñas
- Política de Uso de Redes y Servicios de Red
- Política de Controles Criptográficos
- Política de Gestión de Llaves Criptográficas
- Política de Seguridad Física en las instalaciones
- Política de Seguridad Física en Equipos
- Política de Seguridad en las Operaciones
- Política de Copias de Respaldo
- Política de Registro y Protección de Logs
- Política de Gestión de Vulnerabilidades
- Política de Seguridad de las Comunicaciones
- Política de Transferencia de Información segura
- Política de Desarrollo Seguro
- Política de Relación con Proveedores
- Política para el Alojamiento de Sitios Web con Terceros
- Política de Gestión de incidentes de Seguridad
- Política de Continuidad
- Política de Cumplimiento

5.0 GLOSARIO

- **Seguridad de la información:** Implementación de un conjunto de medidas destinadas a preservar la confidencialidad, integridad y disponibilidad de la información.

- **Confidencialidad:** La información debe ser accedida sólo por las personas autorizadas. Es necesario acceder a la información mediante autorización y control. La confidencialidad hace referencia a la necesidad de ocultar o mantener secreto determinada información. Su objetivo es prevenir la divulgación no autorizada de la información.

- **Integridad :** La integridad supone que la información se mantenga inalterada ante accidentes o intentos maliciosos. Sólo se podrá modificar la información mediante autorización. El objetivo de la integridad es prevenir modificaciones no autorizadas de la información.

- **Disponibilidad :** La información deberá permanecer accesible a elementos autorizados. El objetivo es prevenir interrupciones no autorizadas.