Política del Sistema de Gestión de Seguridad de la Información (SGSI)

CONTROL DE CAMBIOS DEL DOCUMENTO
Ver. 01: Versión inicial - 18/02/2022 **Ver. 02:** Se incluyó el control de cambios y directrices generales respecto al cumplimento de la seguridad de la información para la organización y sus colaboradores – 16/06/2023 **Ver. 03:** Se incluyó objetivos, alcance , terminología, roles y responsabilidades, para robustecer el documento de la política del SGSI - 05/06/2024

Versión:	Fecha de aprobación	Elaborado por:	Revisado por:	Aprobado por:
03	05/06/2023	Oficial de seguridad de la información	Gerente General	Gerente general

Política del Sistema de Gestión de Seguridad de la Información (SGSI)

1. **Introducción**

   PECANO SOFTWARE S.A.C. es una empresa de desarrollo de software que brinda soluciones tecnológicas al mercado B2B con dos productos de desarrollo propio:

   - El ERP PECANO especializado en la vertical de estaciones de servicios – grifos.
   - El software como servicio de "Facturación Electrónica" como PSE y OSE, que atiende a todo tipo de sectores empresariales.

2. **Objetivo**

   Establecer los lineamientos generales, principios y reglas para la protección de los activos de información de la organización y la información de sus partes interesadas ante cualquier amenaza que pudiera causar algún evento o incidente de seguridad, a través de una adecuada gestión de la seguridad de la información en la entrega de los servicios de Facturación Electrónica como PSE y OSE.

3. **Alcance:**

   Esta política aplica al Sistema de Gestión de Seguridad de la Información, según lo definido en el documento de alcance del SGSI (M-01-F-03), y su cumplimiento aplica a todos los colaboradores de la organización, así como a sus partes interesadas.

4. **Terminología en seguridad de la información**

   A continuación, se definen los diferentes términos que se utilizan en el SGSI de la empresa. Para ello se ha tomado como referencia la norma ISO/IEC 27000:

   - **Alcance del SGSI:** Ámbito de la organización que queda sometido al SGSI.
   - **Activo de la información:** Cualquier elemento, componente o funcionalidad de un sistema de información que tenga valor para la empresa.
   - **Amenaza:** Causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización.
   - **Confidencialidad:** Propiedad de la información para que no esté disponible, ni sea revelada a personas, procesos o empresas no autorizadas.
   - **Disponibilidad:** Propiedad de la información de ser accesible y utilizable a petición de una empresa o persona autorizada.
   - **Gestión de riesgos**: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo de seguridad de los activos de información.
   - **Incidente de seguridad de información:** Única o una serie de eventos de seguridad de la información no deseados o inesperados que tiene una probabilidad

significativa de comprometer operaciones del negocio y amenazar la seguridad de los activos de información.

- **Integridad:** Propiedad de la información de exactitud e integridad.
- **Mejora continua:** Actividad recurrente para mejorar el rendimiento.
- **Parte interesada:** Persona u organización (interna o externa) que puede afectar, ser afectados por, o percibirse a sí mismos de ser afectados por una decisión o actividad.
- **Política:** Intenciones y dirección de una organización formalmente expresadas por la alta dirección.
- **Requisito:** Necesidad o expectativa establecida, generalmente implícita u obligatoria.
- **Revisión:** Actividad que se realiza para determinar la idoneidad, la adecuación y la eficacia del tema estudiado para conseguir los objetivos establecidos.
- **Riesgo:** Efecto de la incertidumbre sobre la consecución de los objetivos.
- **Seguridad de la información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información.
- **Tratamiento del riesgo:** Proceso para reducir el riesgo.

5. Roles y responsabilidades

En Pecano Software, se han definido los roles y responsabilidades de seguridad de la información según manual del SGSI M-01-F-21.

- **Alta Dirección:** Responsable de la definición y aprobación de la política, alcance y objetivos del Sistema de Gestión de Seguridad de la Información (SGSI).
- **El Oficial de seguridad de la información:** Responsable de velar por el cumplimiento y la mejora continua del SGSI por parte de los colaboradores y de sus partes interesadas.
- **Tecnología:** Responsable de asegurarse del mantenimiento de los sistemas desarrollados en entornos On-premises y cloud para que funcionen adecuadamente manteniendo la seguridad de la información.
- **Soporte TI**: Responsable de asegurarse que el despliegue de los sistemas On - premises en los equipos informáticos se realice adecuadamente garantizando su funcionamiento y manteniendo la seguridad de la información.
- **Comité de crisis:** Responsable de diseñar estrategias de comunicación para las áreas internas afectadas y/o partes interesadas, así como supervisar el cumplimiento de las estrategias de recuperación definidas por el responsable o área pertinente ante un evento disruptivo que compromete la continuidad de las operaciones de la empresa.

- **Jefes de área:** Responsables de asegurarse del cumplimiento de las políticas de seguridad y procedimientos en sus equipos de trabajo que han siso establecidas en la organización.
- **Los trabajadores de la empresa:** Responsables de cumplir con las políticas de seguridad y procedimientos establecidos en la organización, así como reportar cualquier vulnerabilidad de seguridad de la información en los sistemas utilizados por la empresa.

6. Principios y directrices de la política de seguridad de nuestro SGSI

La alta dirección, en el marco del Sistema de Gestión de Seguridad de la Información (SGSI), dispone de los siguientes compromisos para la empresa:

- Establecer, implementar, operar, monitorear, mantener y mejorar un Sistema de Gestión de Seguridad de la Información bajo la norma ISO/IEC 27001.
- Asegurar la confidencialidad, disponibilidad e integridad de la información relevante de la organización y partes interesadas pertinentes, según corresponda.
- Cumplir con los requisitos legales, regulatorios, contractuales y otros suscritos aplicables; referentes a la seguridad de la información.
- Gestionar los riesgos de seguridad de la información de los activos de la organización, aplicando el tratamiento adecuado, mediante la implementación de controles, políticas de seguridad y procedimientos para evitar se materialicen y minimizar su impacto.
- Crear y fomentar una cultura de seguridad de la información en la organización y sus colaboradores, mediante charlas y capacitaciones de concientización.
- Facilitar y proporcionar los recursos necesarios para el logro de los objetivos de la seguridad de la información.
- Mantener actualizada y resguardar adecuadamente la documentación e información de los procesos de la organización según clasificación establecida.
- Gestionar los eventos e incidentes de seguridad de la información respondiendo y recuperándonos de manera oportuna para mantener la continuidad de las operaciones de la organización.
- Garantizar que nuestros procesos y el Sistema de Gestión de Seguridad de la información (SGSI) se mejoren continuamente.
- Programar auditorías internas para medir la eficacia del SGSI y la mejora continua.
- Comunicar la importancia del sistema de Gestión de Seguridad de la Información a las partes interesadas como clientes y proveedores.

- El compromiso por parte de los colaboradores de la organización con el cumplimiento de la política del SGSI establecida en la organización.

7. Revisión de la política del SGSI

Esta política proporciona un marco de referencia para el establecimiento de objetivos del SGSI, y debe ser revisada periódicamente , al menos una vez al año, para garantizar su continua adecuación por cambios internos o externos que puedan afectar a la organización.

Lima, 05 de junio de 2024.