WebPOS
Facturación Electrónica

Soluciones de Punto de Venta S.A.

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Código:	Versión:	Fecha de la versión:	Creado por:	Aprobado por:	Nivel de confidencialidad:
WP-DCSI- 04	04	27-NOV-24	AUDITOR INTERNO DE SEGURIDAD	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	RESTRINGIDO

Tabla de contenido

1. RESUMEN POLÍTICA GENERAL **3**

2. OBJETIVO **3**

3. ALCANCE **3**

4. USUARIOS **3**

5. PUNTOS CLAVE **4**

6. DESARROLLO DE LA POLÍTICA **5**

6.1. GENERALIDADES 5

7. DOCUMENTOS DE REFERENCIA **7**

8. CUMPLIMIENTO DE NORMATIVA **8**

9. CONTROL ALCANZADO **8**

1. Resumen Política General

En **Soluciones Punto de Venta S.A**. se presta el servicio de APROBACION DE DOCUMENTOS PARA LA FACTURA ELECTRÓNICA como PAC autorizado por la DGI de Panamá, por lo cual la alta dirección demuestra su compromiso con la seguridad de la información asegurando que esta se integre en todas las actividades fundamentales de la organización. Como parte de este compromiso, se establecen estrategias y controles alineados con los objetivos del negocio, garantizando la protección de los activos de información, la continuidad operativa y el cumplimiento normativo. Todos los niveles de la organización deben asumir la responsabilidad de aplicar y mejorar continuamente las medidas de seguridad, promoviendo una cultura de conciencia, prevención y resiliencia ante riesgos de seguridad.

2. Objetivo

Establecer los lineamientos estratégicos para la planeación, implementación, seguimiento y mejora continua de un sistema de gestión de seguridad de la información, manteniendo la confidencialidad, disponibilidad e integridad de la información, así mismo como la ciberseguridad y privacidad. Además, para la asignación de responsabilidades, divulgación, educación y retroalimentación del SGSI a todo el personal de la compañía.

3. Alcance

Esta política aplica a todas las áreas y procesos que interfieren con la información confiada por los clientes, inclusive con la información que la compañía genere por sí misma dentro del alcance del SGSI de **Soluciones Punto de Venta S.A**.

4. Usuarios

Los usuarios de esta política son responsabilidad de todo el personal de la compañía, mantener la información en condiciones de seguridad con un mínimo o con riesgo residual, cumpliendo con las políticas y controles implementados, detectando

oportunamente incidentes de seguridad, implementando acciones correctivas y preventivas, además de proporcionar oportunidades de mejora.

5. Puntos clave

- Las responsabilidades frente a la seguridad de la información se establecerán y ser aceptadas por todos los miembros de la compañía, ya sea empleados, contratistas o personal externo.
- Mantener una motivación en la organización para el cumplimiento de las políticas de seguridad de la información.
- Mantener una capacitación regular a todo el personal en cuanto a temas de seguridad de la información y cuidado de activos de información.
- La información siempre debe estar protegida, sin importar que sea generada, procesada o almacenada producto de los activos de información propios o de propiedad de terceros confiados a la compañía. Además, la infraestructura tecnológica que soporta los procesos más críticos también será protegida.
- Controlar las operaciones de los procesos de la compañía dentro del alcance del SGSI, para garantizar la seguridad de los recursos tecnológicos y redes de datos.
- Mantener un control de acceso a la información, sistemas, redes y accesos físicos.
- Mantener una mejora continua con el adecuado uso de la gestión de los eventos de seguridad y debilidades asociadas a la infraestructura tecnológica.
- Mantener la disponibilidad y continuidad del negocio basado en el análisis del impacto que puedan generar las vulnerabilidades más críticas.
- Por la naturaleza de la prestación del servicio de aprobación de documentos de factura electrónica, no se contempla la transferencia de medios físicos que contengan información.

- Especificar los requerimientos de seguridad en la gestión de nuevos proyectos. Estos cambios deben estar controlados especialmente si afectan la seguridad de la información.
- La legislación aplicable y los requisitos contractuales sobre la seguridad de la información se identificarán y quedarán registrados y controlado su cumplimiento a través de auditorías internas en los contratos con clientes, proveedores o de seguros. Esto con el fin de garantizar la privacidad y protección de la información que contenga datos personales. Lo anterior con el apoyo de la matriz de identificación de requisitos legales.
- Difusión a todo el personal de la presente y de todas las políticas de seguridad de la información.
- Las excepciones a los lineamientos de la presente política general de seguridad de la información o a las políticas específicas, serán analizadas entre la Gerencia y el comité de seguridad de la información para su aprobación.

6. Desarrollo de la política

6.1. Generalidades

En la presente política se establecen los lineamientos para planear, implementar, seguir y mejorar un sistema de gestión de seguridad de la información (SGSI) en la compañía, manteniendo la confidencialidad, integridad y disponibilidad de la información con sus complementos de ciberseguridad y privacidad, además establece las responsabilidades para el cumplimiento de los controles implementados, las revisiones del sistema y el funcionamiento en el tiempo.

La base para que la compañía, pueda operar de una forma confiable en materia de Seguridad de la información comienza con la definición de las políticas generales y específicas. Estas a su vez son la base para evaluar y administrar los riesgos para cubrir en materia de seguridad la totalidad de la organización con el fin de mantener la DISPONIBILIDAD, INTEGRIDAD Y CONFIDENCIALIDAD de la información.

Así que, un sistema de seguridad de la información es aquel que me permite reducir los riesgos ocasionados por el aprovechamiento de las vulnerabilidades de los activos de información por parte de un conjunto de amenazas mediante la implementación de controles, políticas y controles específicos. Además, permite reducir el impacto de los incidentes de seguridad manteniendo la mejora continua, lo que ayuda a mantener la confianza puesta en la compañía. por los clientes, empleados, y demás partes interesadas.

Para lo anterior se establecen procedimientos que determinen los riesgos, identifiquen, clasifiquen y definan los propietarios de los activos de acuerdo con su sensibilidad y criticidad. Procedimientos que identifiquen, analicen amenazas y vulnerabilidades de activos para evitar la posibilidad de ocurrencia e impacto al negocio; establecer los niveles de riesgo darle su tratamiento y llevarlo a un nivel aceptable e implementar actividades de monitoreo para establecer la eficacia de los controles establecidos y continuar con la mejora continua.

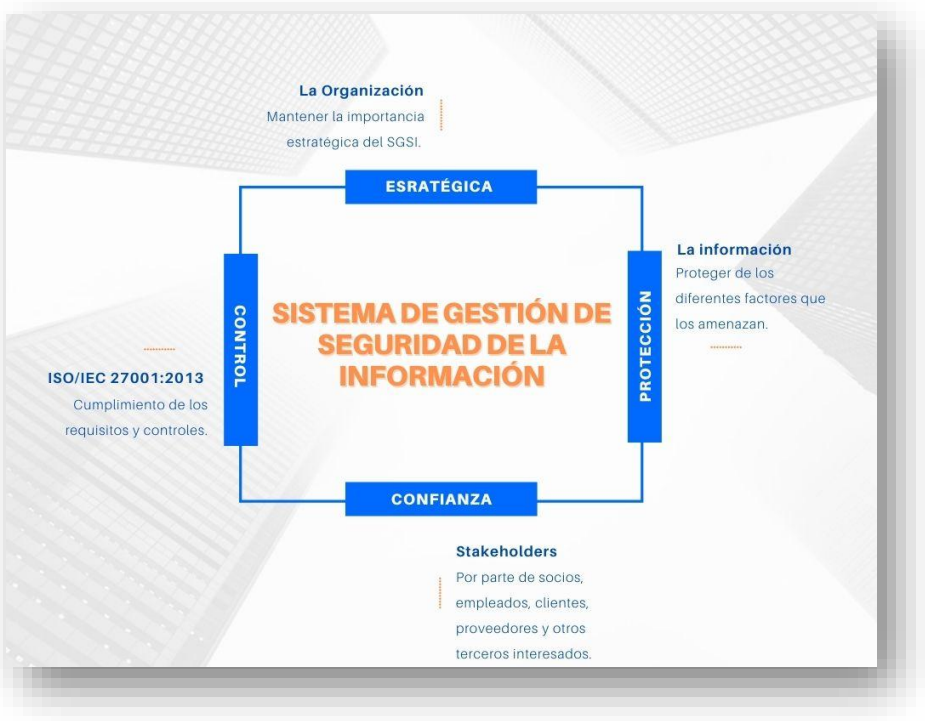
Soluciones Punto de venta S.A, establece su compromiso con la organización para proporcionar todos los recursos necesarios para implementar un sistema de seguridad de la información de forma eficiente y eficaz, además el compromiso para su divulgación y concientización.

Se conformará un comité de seguridad de la información, el cual estará integrado por personal idóneo de la organización y que hagan parte de la alta dirección, los cuales aprobarán esta política y políticas específicas requeridas como evidencia del compromiso, el apoyo a la implementación y en el mantenimiento de políticas eficaces que garanticen la seguridad de la información. Así mismo, verificarán las actividades de planeación, implementación, seguimiento y mejora del SGSI. De otra forma como mínimo de forma anual o cuando sea requerido, se realizará una revisión a esta política a las otras implementadas, para verificar su efectividad y aplicabilidad,

incluyendo todos los controles implementados es decir se debe realizar una revisión general al SGSI.

Es responsabilidad del Auditor de seguridad y del Oficial de cumplimiento o quien haga sus funciones, velar por el cumplimiento de esta política, la documentación de procedimientos, instructivos y formatos con los lineamientos estandarizados, haciendo cumplir los controles implementados en este sistema.

Además, todo el personal que labora en la compañía será responsable de cumplir con todos los lineamientos establecidos en esta política y las demás que se establezcan con el fin de mantener la información en estado óptimo de seguridad y sus características de CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD



7. Documentos de referencia

- Norma ISO/IEC 27001:2022

- Norma ISO/IEC 27002:2022
- Declaración de aplicabilidad para el SGSI
- Políticas específicas de seguridad de la información.

8. Cumplimiento de Normativa

Norma o ley	Capitulo	Numeral / Requisito / Control
ISO/IEC 27001:2022	Anexo A – Controles Organizacionales	A.5.1

9. Control alcanzado

- Política de seguridad de la información y las políticas específicas asociadas definidas, aprobadas por la dirección, publicadas, comunicadas y reconocidas por el personal pertinente y partes interesadas pertinentes.

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
25/OCT/2021	01	Auditor interno Seguridad de la información	Creación y aprobación inicial de la Política.
02/NOV/2022	02	Auditor interno Seguridad de la información	Revisión anual de la política.
22/NOV/2023	03	Auditor interno Seguridad de la información	Revisión anual de la política – Infografía resultados clave.
27/NOV/2024	04	Auditor interno Seguridad de la información	Revisión anual de la política – Uso de la palabra política específicas – refuerzo para excepciones a los controles – Orientación a la revisión de los requisitos.

Ramón Cabezas - Gerente General