
	Servicio y Soporte en Tecnología Informática S.A. de C.V. (Pegaso Tecnología) Proceso de Operaciones de Tecnología de Información		
	Políticas de OperIT para CFDI - Seguridad de la Información		
Fecha: 10/05/2023	Área de Proceso: CPI	Clave del documento: PEGTEC_OPERIT_CPI_Po_Seguridad	Versión: 4.0

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN



1. INTRODUCCIÓN

En "Servicio y Soporte en Tecnología Informática S.A. de C.V." (en adelante "SSTI"), consciente de la importancia que tiene la información y sobre todo lo que representa la protección de los datos personales, la regulación de su tratamiento legítimo, controlado e informado tiene establecido como objetivo primario el de garantizar la CONFIDENCIALIDAD e INTEGRIDAD de la información, no dejando de lado la disponibilidad de la misma. Bajo este contexto, SSTI entiende por **SEGURIDAD DE LA INFORMACIÓN** como el conjunto de medidas preventivas y reactivas de las empresas para sus sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.

SSTI con la Gestión de la Seguridad de la Información se busca establecer, implementar, operar, monitorear y mejorar los procesos y sistemas relativos a la confidencialidad, integridad y disponibilidad de la información, alineado a nuestra misión, visión y valores.

Bajo este contexto SSTI, consciente de la importancia que tiene la información ha establecido una serie de Medidas de Seguridad administrativa, física y técnica. Así mismo, pretende estar alineada a una gestión de seguridad de la información bajo el estándar internacional del ISO27001-2013.

2. MARCO DE REFERENCIA

	Servicio y Soporte en Tecnología Informática S.A. de C.V. (Pegaso Tecnología) Proceso de Operaciones de Tecnología de Información		
	Políticas de OperIT para CFDI - Seguridad de la Información		
Fecha: 10/05/2023	Área de Proceso: CPI	Clave del documento: PEGTEC_OPERIT_CPI_Po_Seguridad	Versión: 4.0

Se da cumplimiento a los controles de seguridad de la información descritos en la matriz de control, señalada en la fracción II de la ficha 111/CFF, del Anexo 1-A de la RMF, vigente a partir del 1 de mayo de 2018, en la que se indican los 86 controles de seguridad de la información y 12 de validación tecnológica a implementar.



Se da cumplimiento a los requisitos de la norma nacional NMX-I-NYCE-27001-2015 y la norma internacional ISO/IEC 27001:2013 con base a los requisitos del Sistema de Gestión de Seguridad de la Información que permite mantener la confidencialidad, integridad y disponibilidad de la información contenida en los sistemas de emisión de CFDI.

Se da cumplimiento a lo dispuesto por diversas entidades y organizaciones como el INAI atendiendo sus principios de **licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad** previstos en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (en adelante "LFPDPPP"), su reglamento.

3. ALCANCE



En SSTI, en su carácter de responsable conforme al **SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN** y la "LFPDPPP", respecto al tratamiento de los Datos Personales y la Seguridad de la Información se busca establecer, implementar, operar, monitorear y mejorar los procesos y sistemas relativos a la protección de la Información y los Datos Personales con los que cuenta, por lo que el ámbito y alcance de aplicación será toda la organización, clientes y proveedores que de forma general realizan el manejo de Seguridad de la Información incluyendo el tratamiento de Datos Personales.

4. OBJETIVOS GENERALES

	Servicio y Soporte en Tecnología Informática S.A. de C.V. (Pegaso Tecnología) Proceso de Operaciones de Tecnología de Información		
	Políticas de OperIT para CFDI - Seguridad de la Información		
Fecha: 10/05/2023	Área de Proceso: CPI	Clave del documento: PEGTEC_OPERIT_CPI_Po_Seguridad	Versión: 4.0

Proteger la Información con la que cuenta SSTI a través de acciones de aseguramiento de la Información teniendo en cuenta los requisitos legales, operativos, tecnológicos, de seguridad y aquellas que la organización determine.

- Dar cumplimiento a la normatividad existente en materia de seguridad de la información, incluyendo la protección de Datos Personales y demás documentos aplicables.
- Proteger la información incluyendo los Datos Personales con los que cuenta la Organización incluyendo sus activos en donde se disponen.
- Dar a conocer la Política de Seguridad de la Información y concientizar sobre la importancia de su cumplimiento.
- Implementación de tecnologías adecuadas para la seguridad de la información.
- Identificar y clasificar la información que es tratada por la Organización.
- Conocer el flujo de la información en la Organización.
- Conocer qué personas son las que tienen privilegios y/o acceso a las fuentes de información en la Organización.
- Identificar en dónde se almacena la información, así como los mecanismos o tecnología utilizada para tal efecto.
- Aplicar las políticas específicas para el manejo de información.
- Verificar la eficacia de la implementación de las políticas específicas para el manejo de información.
- Identificar y realizar mejoras y/o actualizaciones a las políticas específicas para el manejo de información.

	Servicio y Soporte en Tecnología Informática S.A. de C.V. (Pegaso Tecnología) Proceso de Operaciones de Tecnología de Información		
	Políticas de OperIT para CFDI - Seguridad de la Información		
Fecha: 10/05/2023	Área de Proceso: CPI	Clave del documento: PEGTEC_OPERIT_CPI_Po_Seguridad	Versión: 4.0

5. POLÍTICA DE ALTO NIVEL DE SEGURIDAD DE LA INFORMACIÓN



Pegaso Tecnología proporciona, establece y opera los servicios con base al Sistema de Gestión de Seguridad de la Información que permite mantener la confidencialidad, integridad y disponibilidad de la información contenida en los sistemas de emisión de CFDI el cual considera las necesidades de las partes interesadas; alineados con la estrategia de negocio y en cumplimiento con los requisitos de nuestros clientes, los requisitos de la norma nacional NMX-I-NYCE-27001-2015, la norma internacional ISO/IEC 27001:2013, la LFPDPPP y con los requisitos de leyes y regulaciones aplicables.

El propósito del Sistema de Gestión de Seguridad de la Información es cumplir con los objetivos establecidos, enfocados a proteger la información por medio de la implementación de planes de tratamiento, los cuales consideran la implementación, operación y mantenimiento de controles físicos, administrativos y técnicos de seguridad relacionados con las instalaciones, recursos humanos, sistemas o aplicaciones, equipo y medios móviles e infraestructura tecnológica.



Para el logro de estos objetivos la Dirección se compromete a revisar y mejorar los controles y procesos del Sistema de Gestión Seguridad de la Información mediante la actualización de la valoración de riesgos y de los planes de tratamiento de riesgos, el establecimiento de políticas para la mejora continua, la realización de auditorías internas, revisiones por la dirección y la implementación de acciones de mejora.

6. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN



- La capacitación a todo el personal de la Organización respecto a la seguridad de la información, garantizando la concientización de que las medidas de seguridad son necesarias con el propósito de proteger la información y datos, así como para lograr que se contribuya para generar la efectividad de las medidas de seguridad.

	Servicio y Soporte en Tecnología Informática S.A. de C.V. (Pegaso Tecnología) Proceso de Operaciones de Tecnología de Información		
	Políticas de OperIT para CFDI - Seguridad de la Información		
Fecha: 10/05/2023	Área de Proceso: CPI	Clave del documento: PEGTEC_OPERIT_CPI_Po_Seguridad	Versión: 4.0



- SSTI realizará de forma anual y/o cada vez que ocurra alguna modificación significativa en los procesos de la organización que afecten los objetivos de la presente política, con el objeto de garantizar que su contenido se encuentre acorde con la legislación y normatividad aplicable.
- SSTI realizará de forma anual la revisión de los objetivos de la presente política, con el objeto de mantener los controles de seguridad implementados para la protección de la información y datos personales tratados por la Organización.
- SSTI realizará el análisis de los riesgos en los activos de la información, con el objetivo de poder elaborar un proceso que contemple las acciones de respuesta y tratamiento los riesgos y áreas de oportunidad detectadas.
- Se elaborarán controles para la vigilancia, revisión y modificación de los alcances en el tratamiento y cumplimiento de la presente política de seguridad de la información, y en su caso, se determinarán sanciones para el personal que realice actos en contravención, así como la documentación y registro de las violaciones y/o eventos a la seguridad confirmadas en la Organización.
- SSTI a través del área encargada de la difusión, aplicación y adecuación de la presente política será responsable de brindar asesoría y orientación sobre la misma, así como la solución de los conflictos que puedan surgir derivados de su aplicación.
- SSTI protegerá las instalaciones de procesamiento (Centro de Datos y sitio alternativo), y en general su infraestructura tecnológica.
- SSTI establecerá un control en sus procesos de operación, para garantizar la seguridad de sus activos tecnológicos, redes y BD.
- SSTI implementará de forma general controles de acceso limitado a la información, recursos, aplicativos, portales, ambientes QA y Productivo, incluyendo accesos remotos.

	Servicio y Soporte en Tecnología Informática S.A. de C.V. (Pegaso Tecnología) Proceso de Operaciones de Tecnología de Información		
	Políticas de OperIT para CFDI - Seguridad de la Información		
Fecha: 10/05/2023	Área de Proceso: CPI	Clave del documento: PEGTEC_OPERIT_CPI_Po_Seguridad	Versión: 4.0

- SSTI vigilará que los recursos humanos no revelen sus claves de identificación a ninguna otra persona para asegurar su uso legítimo en los sistemas, aplicaciones y bases de datos que contienen información.
- SSTI generará claves de acceso personalizadas, robustas y estandarizadas para el manejo de aplicaciones, sistemas, herramientas, etc. de la organización.
- SSTI establecerá que los criterios para la creación de contraseñas seguras estén constituidas de al menos 8 (ocho) caracteres, contener caracteres tanto en mayúsculas como en minúsculas, puedan tener dígitos y caracteres especiales como , / , \$, ¿ , & , *; no pueden ser basadas en información personal ni contener patrones como 1234, aabbcc, etc. Se observará que ninguna de las claves contenga palabras o nombres relacionados con la vida personal de los empleados.
- SSTI ordenará que el personal se asegure que NO se tenga acceso al (los), equipo (s), de cómputo que están a su cargo en su ausencia, bloqueándolo, utilizando un protector de pantalla automático con clave personal o bien apagándolo para evita el acceso no autorizado.
- SSTI prohibirá la instalación de software en el (los), equipo (s), de cómputo que tengan asignado el personal sin la previa autorización de las personas designadas para tal efecto.
- SSTI ordenará que no se active ningún archivo ejecutable desconocido como aquellos descargados de Internet, recibidos vía correo electrónico o de cualquier otra fuente.
- SSTI determinará que únicamente el equipo de cómputo sea exclusivamente utilizado para cuestiones laborales y no personales.
- SSTI determinará la prohibición de modificar los sistemas y parámetros de la seguridad de los sistemas de la red y Centro de Datos.

	Servicio y Soporte en Tecnología Informática S.A. de C.V. (Pegaso Tecnología) Proceso de Operaciones de Tecnología de Información		
	Políticas de OperIT para CFDI - Seguridad de la Información		
Fecha: 10/05/2023	Área de Proceso: CPI	Clave del documento: PEGTEC_OPERIT_CPI_Po_Seguridad	Versión: 4.0

- SSTI adoptará una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.
- En materia de Datos Personales, SSTI velará porque su tratamiento sea en atención con las finalidades que se encuentran descritas en el Aviso de Privacidad de Datos Personales, limitando su tratamiento a las finalidades enunciadas.
- En materia de Datos Personales, SSTI administrar los privilegios, atributos y permisos para el acceso al BD que contienen Datos Personales de clientes, proveedores, empleados y candidatos.
- SSTI almacenará toda aquella información que contenga Datos Personales en su Data Center. Por lo que NO se utilizará, reproducirá, transformará ni almacenará información en ninguna computadora portátil, ni en ningún sistema de recuperación de información electrónica a que se pueda tener acceso externamente.
- SSTI prohibirá la utilización del correo electrónico institucional para fines diversos a los relacionados con la misma, así como la difusión de "cadenas" o propagandas (correos SPAM), incluida la revelación de información que concierne de Datos Personales.
- No se divulgará por cualquier medio escrito, verbal, visual, electrónico, magnético, planos, dibujos, diagramas o de cualquier otra forma o medio, conocido o por conocerse; el contenido total o parcial de cualquier información y/o documento que contenga Datos Personales.
- SSTI en aquellos casos en que tenga que realizar transferencia de Datos Personales lo hará únicamente a través de canales seguros y en su caso cifrado.

	Servicio y Soporte en Tecnología Informática S.A. de C.V. (Pegaso Tecnología) Proceso de Operaciones de Tecnología de Información		
	Políticas de OperIT para CFDI - Seguridad de la Información		
Fecha: 10/05/2023	Área de Proceso: CPI	Clave del documento: PEGTEC_OPERIT_CPI_Po_Seguridad	Versión: 4.0

- SSTI establecerá restricciones de acceso a sitios de Internet con contenido malicioso, de violencia, terrorismo, juegos, videos, espectáculos y de música ya que por su uso son sitios propicios para la distribución de virus y código malicioso, que pudiera provocar una vulneración en el resguardo de información y Datos Personales.
- SSTI restringirá el acceso a sitios web concernientes a redes sociales.
- SSTI establecerá que todo el personal celebre un convenio de confidencialidad o Non Disclosure Agreement (NDA), en donde se reconozca la obligación de no revelar información con carácter de confidencial y datos personales a personas ajenas a la Organización.
- SSTI establecerá la seguridad para proveedores y partes interesadas con los cuales establezca relaciones de negocio y comerciales celebrando la documentación legal requerida, acuerdos de confidencialidad y cualquier otro documento necesario para proteger la información de la organización, los servicios que proporciona, los accesos físicos a la organización y a todos aquellos accesos a sus activos de información, los derechos de propiedad intelectual y de uso de marca, así como las sanciones a violaciones y actos mal intencionados. Lo anterior está contenido en la política de seguridad de relación con proveedores "PEGTEC_OPERIT_CPI_Po_Seguridad Relación con Proveedores".



Patricia Santoni
 Directora General
 Mayo, 2023.