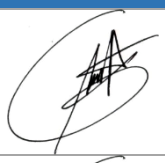
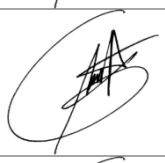
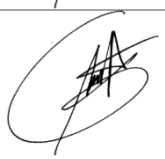
Código	PL-SI-PU-02
Versión	2.0
Publicación	24/05//2018

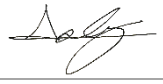
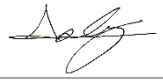
INFORMACIÓN PÚBLICA
Páginas: En su totalidad
Fundamento Legal: Arts. 3, 110 Y 113 de la LFTAIPG, y 37 del RLFTAIPG
Responsable que la clasifica
Gloria Minerva González Hernández
Jefe de Seguridad de la Información

Política de seguridad de la información

Control de versiones

Nombre	Puesto	No. Versión	Modificaciones	Fecha	Firma
Gloria Minerva González Hernández	Jefatura de seguridad de la información	1.0	Cambio de plantilla del documento, actualización de clasificación y reestructuración del documento	03/05/2017	
Gloria Minerva González Hernández	Jefatura de seguridad de la información	2.0	Se revisa el documento sin cambios	31/01/2018	
Gloria Minerva González Hernández	Jefatura de seguridad de la información	3.0	Cambio de plantilla, se agregan los siguientes puntos: Definición de Seguridad de la información, Medidas disciplinarias en caso de incumplimiento. De acuerdo a nueva matriz de controles	24/05/2018	

Control de revisiones

Nombre	Puesto	No. Versión	Modificaciones	Fecha	Firma
Asley Alberto Cristales Pavón	Dirección de Operaciones	1.0	Sin observaciones	04/05/2017	
Asley Alberto Cristales Pavón	Dirección de Operaciones	2.0	Sin observaciones	31/01/2018	
Raquel Vásquez Ramírez	Consultor Externo	3.0	Redacción, ortografía y estilo	24/05/2018	

Control de autorizaciones

Nombre	Puesto	No. Versión	Modificaciones	Fecha	Firma
Juan Carlos González Hernández	Director general	1.0	Sin observaciones	04/05/2017	

Nombre	Puesto	No. Versión	Modificaciones	Fecha	Firma
Juan Carlos González Hernández	Director general	2.0	Sin observaciones	31/01/2018	
Juan Carlos González Hernández	Director General	3.0	Sin observaciones	25/05/2018	

Contenido

1. Generalidades

1.1 Objetivo

Definir las políticas y lineamientos específicos de seguridad de la información establecidas por SIFEI, los cuales son de manera obligatoria para todos sus colaboradores, cualquiera sea su calidad contractual, con el fin de preservar la confidencialidad, disponibilidad e integridad de la información que manejen.

1.2 Alcance

La presente política es aplicable para todo el personal de la compañía, interno o externo que interactúe con el proceso crítico de CFDI, entendiéndose como proceso crítico lo relacionado a la emisión y generación de CFDI de acuerdo a lo establecido en el anexo 20.

1.3 Referencias normativas y legislación vigente

Tabla 1. Referencias normativas y legislación vigente

Norma	Control
ISO 27001:2013	A.5 Política de Seguridad de la Información A.5.1 Dirección de Gestión de Seguridad de la Información A.5.1.1 Políticas de seguridad de la información
ISO 17799:2005	5 Política de Seguridad 5.1 Política de Seguridad de la Información
MATRIZ DE CONTROL	Señalada en la fracción II de la ficha 111/Código Fiscal de la Federación (CFF) del Anexo 1-A de la Resolución Miscelánea Fiscal (RMF)

1.4 Términos y Definiciones

Tabla 2. Términos y definiciones del documento

Término	Definición
SGSI	El Sistema de Gestión de Seguridad de la Información, por sus siglas SGSI es una herramienta de gestión que permite conocer, gestionar y minimizar los posibles riesgos que atenten contra la seguridad de la información en nuestra empresa.

Término	Definición
Activo	Cualquier cosa que tenga valor para la organización
Amenaza	Son las causas potenciales de eventos o incidentes que producen daño en los activos, son el factor subyacente en el entorno y en el contexto de explotación del activo capaz de aprovechar la vulnerabilidad y causar daño.
Vulnerabilidad	Es la capacidad, las condiciones y características que hacen susceptible a los activos de información a amenazas, con el resultado de sufrir algún daño.
Continuidad del Negocio	Es un plan logístico para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcialmente o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada.
Riesgo	Combinación de la probabilidad de un evento de seguridad y su ocurrencia.
Evento de Seguridad	Cualquier evento de seguridad de la información es una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible falla en la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.
Confidencialidad	Es la propiedad de la información por la que se tiene la certeza de que esta solo puede ser accedida (vista y entendida), por quienes tienen la necesidad de ello y han sido autorizados por el propietario de la misma.
CFF	Código Fiscal de la Federación
RMF	Resolución Miscelánea Fiscal

1.5 Roles y responsabilidades

Las responsabilidades para el SGSI se describen en la matriz RACI de la Tabla 3:

Tabla 3. Roles y responsabilidades de seguridad de la información

Actividad	Jefe de Seguridad de la Información	Coordinador de Seguridad	Comité de Seguridad de la Información	Propietario del activo	Director General
Responsable de la asignación de recursos financieros y legales para el cumplimiento de los objetivos de la Política de Seguridad de la información					RA
Garantizar que el SGSI sea implementado y mantenido de acuerdo con esta Política	RA		C		I
Garantizar que todos los recursos necesarios estén disponibles.	RA				I
Coordinación operativa del SGSI, como también de informar su desempeño.		RA			I
Revisar el SGSI al menos una vez por año o cada vez que			RA		

Actividad	Jefe de Seguridad de la Información	Coordinador de Seguridad	Comité de Seguridad de la Información	Propietario del activo	Director General
se produzca una modificación significativa.					
Elaborar minutas de dichas reuniones. El objetivo de las verificaciones por parte de la dirección es establecer la conveniencia, adecuación y eficacia del SGSI.			RAC		
Protección de la integridad, disponibilidad y confidencialidad de sus activos.	C	A		R	I
Informar al jefe de seguridad de la Información sobre los incidentes o debilidades de seguridad.	C			R	
Definir qué información relacionada con la seguridad de la información será comunicada a qué parte interesada (tanto interna como externa), por quién y cuándo.	RA		C		
Adoptar e implementar el Plan de capacitación y concienciación, que corresponde a todas las personas que cumplen una función en la gestión de la seguridad de la información.	RA				
R – Responsable, A – Autoriza, C – Consultado, I – Informado					

Nota: Consultar el documento *IF-SI-PU-09 Organización de seguridad de la información* donde se detallan los roles y responsabilidades en cuestión de Seguridad de la Información.

2. Definición de Seguridad de la Información

La información es un activo que como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia necesita ser protegido adecuadamente. Esto es especialmente importante en el ambiente comercial cada vez más interconectado. Como resultado de esta creciente interconectividad, la información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades.

La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales.

Una definición de seguridad de la información es la siguiente:

Preservación de confidencialidad, integración y disponibilidad de la información; además, también puede involucrar otras propiedades como autenticidad, responsabilidad, no repudio y confiabilidad

3. Gestión de la seguridad de la información

Es política de Seguridad de la Información de SIFEI:

> ***"Asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información de nuestros clientes procesada al proporcionar el servicio de certificación de CFDIS aplicando estándares internacionales y cumplimiento con la matriz de controles establecida por el SAT para operar como PCCFDI"***

Dicha política es conocida por todo el personal interno, externo y temporal. Se encuentra a la vista en puntos estratégicos de la empresa; que comprueba la presentación y conocimiento de la misma por parte del personal involucrado.

3.1 Objetivos y medición

Los objetivos generales para el SGSI son los siguientes:

- Proteger los recursos de información, los recursos humanos y la tecnología utilizada por SIFEI frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información.
- Establecer los lineamientos necesarios para asegurar la protección y la integridad de los activos de información de SIFEI mediante el ciclo de mejora continua.
- Asegurar que el acceso a la información está adecuadamente autorizado.
- Salvaguardar la precisión y completitud de la información y sus métodos de procesamiento.
- Asegurar que los usuarios autorizados tengan disponible la información cuando la necesitan.

Las metas están en línea con los objetivos comerciales, con la estrategia y los planes de negocio de SIFEI.

3.2 Lineamientos de la política de seguridad de la información

SIFEI cuenta con una política de seguridad de información documentada que establece la dirección a seguir en materia de seguridad de la información.

SIFEI implementa una serie de políticas y procedimientos de seguridad de la información para identificar y minimizar las amenazas a las cuales se expone la información, reducir los costos operativos y financieros,

establecer una cultura de seguridad y garantizar el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigente.

En este sentido se expresan los siguientes lineamientos específicos para dar cumplimiento a la política de seguridad de la información y así poder asegurar la confidencialidad, integridad y disponibilidad de la información:

- Las políticas de seguridad de la información se revisarán al menos dos veces al año, para asegurar que se cumplan los propósitos de la compañía.
- Las políticas de seguridad de la información permanecerán disponibles para consulta de todos los colaboradores que requieran acceso a información de la compañía, en el tablero informativo y canales internos de SIFEI.
- Todos los colaboradores de la compañía están obligados a conocer, observar, cumplir y mantenerse actualizados sobre estas políticas de seguridad de la información.
- Se realizarán talleres de concientización con el todo el personal por lo menos cada 12 meses, con el fin de mantener una cultura de seguridad bien definida y actualizada.
- Implementar los mecanismos necesarios para evitar el robo de información o intrusión a personas no autorizadas.
- Implementar los mecanismos necesarios para prevenir la divulgación de la información a personas o sistemas que no se encuentran autorizados.
- Implementar los mecanismos necesarios para prevenir modificaciones no autorizadas de la información

3.3 Requisitos para la seguridad de la información

Esta Política, y todo el SGSI, deben cumplir los requisitos legales y normativos importantes para la organización en el ámbito de la seguridad de la información, como también con las obligaciones contractuales.

En el documento IF-SI-PU-08 Lista de obligaciones legales, normativas y contractuales se detalla una lista de requisitos contractuales y legales.

3.4 Acciones para hacer frente a los riesgos y oportunidades

El proceso de escoger los controles (protección) está definido en el documento ***GU-SI-PU-01 Metodología para el Análisis y Tratamiento de Riesgos***.

Los controles seleccionados y su estado de implementación se detallan en la ***IF-SI-PU-10 Declaración de Aplicabilidad***

3.5 Controles de seguridad de la información

- **Organización de la seguridad de la información**: Este control permite establecer un marco de gestión para iniciar y controlar el funcionamiento de seguridad de la información dentro de la organización, donde se refinan claramente los roles y responsabilidades de control de la seguridad de la información.
- **Seguridad ligada a los recursos humanos.** Este control permite asegurar que los empleados, contratistas y terceros entiendan sus derechos, obligaciones y responsabilidades, de los roles para los cuales se les considera; y reducir el riesgo de robo, fraude o mal uso de los recursos asignados por parte de la organización. También contempla la planificación de la capacitación y concientización en temas de seguridad de la información.
- **Gestión de Activos**. Este control permite lograr y mantener una protección apropiada de los activos organizacionales del proceso de negocio crítico para SIFEI.
- **Seguridad Física y del Entorno**. Este control permite prevenir el acceso físico no autorizado, daño e interferencia a la información y a las instalaciones de procesamiento de información de la organización.
- **Gestión de Comunicaciones.** Este control permite garantizar la protección de la información en las redes y sus instalaciones de apoyo de procesamiento de información
- **Control de accesos físicos**. Este control está orientado a limitar y controlar el acceso a las instalaciones de procesamiento de la información de la organización.
- **Adquisición, mantenimiento y desarrollo de sistemas**. Este control permite garantizar que la seguridad informática es una parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan servicios públicos.
- **Control de accesos**: Este control permite limitar los accesos a los sistemas, bases de datos, sistemas operativos para evitar el uso no autorizado.
- **Criptografía**: Este control permite garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y / o integridad de la información.
- **Seguridad física y ambiental**: Este control permite prevenir el acceso no autorizado física, daño e interferencia a la información y a las instalaciones de procesamiento de información de la organización.
- **Seguridad en las operaciones**: Este control permite asegurar la operación correcta y segura de los medios de procesamiento de la información.
- **Seguridad en las comunicaciones**: Este control permite garantizar la protección de la información en las redes y sus instalaciones de apoyo de procesamiento de información.

- **Control de accesos**: Este control permite asegurar que los empleados, contratistas y terceros entiendan sus derechos, obligaciones y responsabilidades, de los roles para los cuales se les considera; y reducir el riesgo de robo, fraude o mal uso de los recursos asignados por parte de la organización. También contempla la planificación de la capacitación y concientización en temas de seguridad de la información.
- **Cifrado**: Garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y / o integridad de la información.
- **Adquisición, desarrollo y mantenimiento de los sistemas de información.** Garantizar que la seguridad informática es una parte integral de los sistemas de información a través de todo el ciclo de vida de desarrollo de software.
- **Relaciones con los proveedores**. Para garantizar la protección de los activos de la organización que sea accesible por los proveedores.
- **Gestión Incidentes de Seguridad**: Este control permite garantizar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.
- **Los aspectos de seguridad de la información con respecto a la gestión de la continuidad del negocio**: Este control permite garantizar la continuidad del negocio ante una situación adversa.

3.6 Comunicación de la Política

El Jefe de Seguridad debe asegurar que todos los empleados de SIFEI, como también los participantes externos correspondientes, estén familiarizados con esta Política.

4. Apoyo para la implementación del SGSI

A través del presente, el Director General declara que en la implementación y mejora continua del SGSI se contará con el apoyo de los recursos adecuados para lograr todos los objetivos establecidos en esta política, como también para cumplir con todos los requisitos identificados. Se ratifica el compromiso mediante el documento: AC-2A.6.1.1-CS-04 ACTA DE COMPROMISO DE DIRECCION GENERAL CON EL SGSI FEBRERO 2018 [1]

5. Medidas disciplinarias en caso de incumplimientos a la política

En el caso de que un colaborador de SIFEI incumpla con alguna de las políticas establecidas en el presente documento, se hará merecedor de las siguientes sanciones:

- Amonestación verbal y registro de una falta de disciplina asentándose en Acta Administrativa.

Lo anterior conforme lo señalado en el Artículo 41 del Reglamento Interior de Trabajo, tomándose este acto como equivalente al señalado en el numeral e) "Incumplimiento de las actividades que deban desarrollar".

En caso de que la conducta sea reiterada, se aplica lo señalado en el Artículo 25 del mismo Reglamento en lo referente a:

- Es causal de rescisión la acumulación de Actas Administrativas por falta de disciplina en el plazo allí señalado.

6. Validez y Gestión de la presente Política

- Este documento es válido: a partir del día de su publicación.
- Esta política se debe revisar con periodicidad: cada 6 meses o cuando haya cambios significativos que pudieran afectar los objetivos de seguridad de la información.
- El Propietario del presente documento es: el Titular del Área de Seguridad de la Información quien es responsable de mantener actualizado y vigente este documento, así como asegurarse de que se esté correctamente clasificado, resguardado y reservado/publicado.

7. Referencias

[1] A. C. Cabrera, «ACTA DE COMPROMISO DE DIRECCION GENERAL CON EL SGSI FEBRERO 2018,» Orizaba, 2018.

[2] R. V. Ramírez, «Guía general para elaboración de documentos,» Orizaba, 2018.