

Código	PL-SI-RE-02
Versión	7.0
Publicación	21/08/2019



INFORMACIÓN RESERVADA

Páginas: En su totalidad

Fecha de clasificación: 21/08/2019

Plazo de clasificación: 5 años

Fundamento Legal: Arts. 3, 110 Y 113 de la LFTAIPG, y 37 del RLFTAIPG

Responsable que clasifica

Gloria Minerva González Hernández

Jefe de Seguridad de la Información

Política de seguridad de la información

Código	PL-SI-RE-02
Versión	7.0
Publicación	21/08/2019

Contenido

- 1. Generalidades..... 1
 - 1.1 Objetivo..... 1
 - 1.2 Alcance 1
 - 1.3 Referencias normativas y legislación vigente..... 1
 - 1.4 Marco de referencia 1
 - 1.5 Términos y Definiciones 2
 - 1.6 Roles y responsabilidades 3
- 2. Definición de Seguridad de la Información 5
- 3. Gestión de la seguridad de la información..... 5
 - 3.1 Objetivos y medición..... 6
 - 3.2 Lineamientos de la política de seguridad de la información..... 6
 - 3.2.1 Lineamientos para asegurar la confidencialidad de la información..... 7
 - 3.2.2 Lineamientos para asegurar la disponibilidad de la información 8
 - 3.2.3 Lineamientos para asegurar la integridad de la información 8
 - 3.3 Requisitos para la seguridad de la información..... 8
 - 3.4 Acciones para hacer frente a los riesgos y oportunidades..... 9
 - 3.5 Controles de seguridad de la información..... 9
 - 3.6 Comunicación y publicación de la Política 10
- 4. Aspectos contractuales de seguridad de la información para proveedores 11
- 5. Apoyo para la implementación del SGSI 13
- 6. Medidas disciplinarias en caso de incumplimientos a la política 13
- 7. Validez y Gestión de la presente Política 13
- 8. Referencias..... 13



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/IEC 27001:2013 "Sistema de Gestión de Seguridad de la Información"	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/IEC 17799:2005 "Código de buenas prácticas para el Sistema de Gestión de Seguridad de la Información"	5 Política de Seguridad 5.1 Política de Seguridad de la Información
Matriz de controles de Seguridad emitida por el SAT	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 Marco de referencia

El presente documento de PL-SI-PU-02 Política de seguridad de la información está alineado al estándar para la seguridad de la información ISO/IEC 27001 en su versión más reciente 2013, el cual especifica los requerimientos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) de acuerdo al "Ciclo de Deming", mejor conocido como el ciclo PDCA – por su acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Este estándar es consistente con el código de buenas prácticas para implementar el SGSI el cual es el estándar ISO/IEC 17799:2005.

Por otro lado y de acuerdo a los requerimientos que se tienen que cumplir para que SIFEI opere como PCCFDI, el SAT establece un documento denominado Matriz de controles el cual contiene los lineamientos que se deben cumplir. Por lo cual el presente documento también está alineado a la Matriz de controles establecida por el SAT.

En la Figura 1 se muestra la relación que tiene la política de seguridad de la información de SIFEI con respecto a la referencia normativa vigente.



Figura 1. Relación de estándares con política de seguridad de la información de SIFEI

1.5 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.
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.

Término	Definición
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

1.6 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

Descripción de actividades	Director General	Dirección operativa	Dirección administrativa	Jefe de seguridad de la información	Proveedores	Usuarios de la información	Jefe de Infraestructura
El director General, o en su ausencia el director de operaciones deberá asignar y autorizar los recursos humanos y materiales necesarios para la implementación de esta política.	R	A	C	I			
Elaborar, promover y mantener la política de seguridad de la información		CI		RA			

Descripción de actividades	Director General	Dirección operativa	Dirección administrativa	Jefe de seguridad de la información	Proveedores	Usuarios de la información	Jefe de Infraestructura
Establecer y documentar las responsabilidades de la organización en cuanto a seguridad de la información		CI		RA			
Conocer, observar, cumplir y mantenerse actualizados sobre estas políticas de seguridad de la información				CI	R	RA	
Monitorear el cumplimiento de los estándares, guías, políticas, procedimientos y registros establecidos por SIFEI		CI		RA			
Informar, en particular, a la alta dirección sobre el desempeño del Sistema de Gestión de Seguridad de la Información y sobre las oportunidades de mejora	I	CI		RA			
Reportar supuestas violaciones, eventos e incidentes que afecten la seguridad de la información de SIFEI		I		I		RA	C



Descripción de actividades	Director General	Dirección operativa	Dirección administrativa	Jefe de seguridad de la información	Proveedores	Usuarios de la información	Jefe de Infraestructura
Establecer un plan de capacitación y concientización al personal en materia de seguridad de la información de manera anual		CI		RA		I	

Nota: Consultar el documento IF-SI-RE-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, integridad 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. De tal manera que se mitiguen en un 30% los riesgos presentados durante el proceso de emisión y certificación de comprobantes fiscales digitales por internet.
- Establecer los lineamientos necesarios para asegurar la protección y la integridad de los activos de información de SIFEI mediante el ciclo de mejora continua para asegurar un nivel de protección del 99% en los activos de información que participan en el proceso de CFDI
- Asegurar que el acceso a la información está adecuadamente autorizado para disminuir en un 50% los accesos no autorizados a la información clasificada con el más alto nivel de confidencialidad.
- Salvaguardar la precisión y completitud de la información y sus métodos de procesamiento para aumentar en un 90% la integridad de la información que interviene en el proceso de CFDI.
- Concientizar al personal interno y externo en temas de seguridad de la información para disminuir en un 40% los errores humanos cometidos.

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 la información documentada que establece la dirección a seguir en materia de seguridad de la información. De igual forma, 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 SIFEI.

Código	PL-SI-RE-02
Versión	7.0
Publicación	21/08/2019

- Las políticas de seguridad de la información permanecerán disponibles en el tablero informativo y canales internos de SIFEI para consulta de todos los colaboradores que requieran acceso a información de la compañía.
- 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.
- Informar a la Dirección sobre el desempeño de la implementación del SGSI y las oportunidades de mejora
- Reportar supuestas violaciones, eventos e incidentes que afecten la seguridad de la información de SIFEI.

3.2.1 Lineamientos para asegurar la confidencialidad de la información

La confidencialidad es la garantía de que la información personal será protegida para que no sea divulgada a personas no autorizadas. Dicha garantía se lleva a cabo por medio de un grupo de lineamientos que limitan el acceso a ésta información tales como los que se describen a continuación:

- Toda la información confidencial debe ser protegida con cifrados y contraseñas.
- Los empleados deben limpiar siempre el escritorio de su computadora y eliminar o guardar bajo "llave" cualquier información confidencial.
- Los empleados deben abstenerse de dejar información confidencial visible en los monitores de su computadora cuando salen de sus puestos de trabajo.
- Toda la información confidencial, ya sea contenida en documentos escritos o electrónicos, debe ser marcada como tal.
- Proporcionar acceso a la información clasificada como confidencial solo a personas autorizadas. Así como velar siempre que las credenciales usadas sean válidas.
- Antes de deshacerse o cambiar de equipo de cómputo, utilizar programas de software para borrar los datos contenidos o destruir el disco duro.



3.2.2 Lineamientos para asegurar la disponibilidad de la información

La disponibilidad hace referencia a que la información del sistema debe permanecer accesible a elementos autorizados. El objetivo de la disponibilidad es, entonces, prevenir interrupciones no autorizadas/controladas de los recursos informáticos. Para lograr que nuestros sistemas, infraestructura y redes internas y externas estén disponibles se establecen los siguientes lineamientos:

- Realizar copias de seguridad e imágenes de respaldo, para que en caso de fallos nos permita la recuperación de la información perdida o dañada.
- Desarrollar procedimientos y planes de continuidad de negocio con el fin de garantizar la disponibilidad de los procesos de negocio de SIFEI.
- Desarrollar planes de recuperación ante desastres con el fin de recuperarse en el menor tiempo posible y con la menor pérdida de datos ante algún evento, o incidente de seguridad.
- Monitorear los sistemas, infraestructura y redes con el fin de detectar con antelación cualquier problema de seguridad de la información y estar preparados para cuando se requiera.

3.2.3 Lineamientos para asegurar la integridad de la información

La integridad hace referencia a la cualidad de la información para ser correcta y no haber sido modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros. Para poder lograr lo mencionado anteriormente SIFEI establece los siguientes lineamientos:

- Monitorear los eventos de seguridad que puedan desencadenar algún riesgo o una brecha de seguridad de la información.
- Monitorear la red y su tráfico con el fin de detectar comportamientos anormales.
- Contar con alertas de seguridad que permitan avisar oportunamente algún comportamiento anormal.
- Implementar la cualidad de autenticación a los sistemas de información, infraestructura, bases de datos y bitácoras de acceso que permitan identificar las acciones realizadas por los usuarios de la empresa.
- Implementar características de privilegios de usuario con el fin de limitar lo que puede o no hacer el usuario.

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.

Código	PL-SI-RE-02
Versión	7.0
Publicación	21/08/2019

En el documento IF-SI-RE-08 Lista de obligaciones legales, normativas y contractuales [1] 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-RE-01 Metodología para el Análisis y Tratamiento de Riesgos. [2].

Los controles seleccionados y su estado de implementación se detallan en la IF-SI-RE-10 Declaración de Aplicabilidad [3].

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 [4].
- **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 [5].
- **Gestión de Activos.** Este control permite lograr y mantener una protección apropiada de los activos organizacionales del proceso de negocio crítico para SIFEI [6].
- **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 [7].
- **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.



Código	PL-SI-RE-02
Versión	7.0
Publicación	21/08/2019

- **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 físico no autorizado, 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.
- **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.
- **Revisiones de seguridad de información.** Este control permite revisar que la seguridad de la información es implementado y operado de acuerdo con las políticas y procedimientos establecidos por SIFEI

3.6 Comunicación y publicación de la Política

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

La política de seguridad de la información se publica en los siguientes puntos estratégicos:

- a) Página principal de SIFEI
- b) Tablero informativo de comunicación interna



- c) Sala de juntas
- d) Área de desarrollo
- e) Área de soporte técnico
- f) Gafete del empleado
- g) Gafete de visitante

Las imágenes se muestran en el documento Publicación de la política de seguridad de la información [8].

4. Aspectos contractuales de seguridad de la información para proveedores

Respecto a los aspectos contractuales que se deben observar de los proveedores en relación con la seguridad de la información, ya sea que el contrato sea elaborado por SIFEI o sea un contrato elaborado por un proveedor, se deberán incluir las cláusulas (no limitativas) siguientes:

1. Auditoría de servicios. El proveedor debe permitir a SIFEI la realización de auditorías en materia de seguridad de la información periódicamente.
2. Confidencialidad. El proveedor reconoce que el uso de la información Confidencial es única y exclusivamente para los propósitos de las negociaciones de las que derive el objeto del contrato.
3. Propiedad de la información. El proveedor y la empresa reconoce que la "Información Confidencial" que manejen entre ellas es propiedad exclusiva de la parte que entregue dicha información.
4. Notificaciones sobre infracciones en la seguridad. El proveedor debe de informar a SIFEI sobre cualquier violación a la seguridad de la información que afecte sus operaciones o sus negocios.
5. Aceptación de las prácticas de seguridad. El proveedor declara que conoce y acepta sin restricciones las prácticas de seguridad de la información propuestas por SIFEI, y que comunicará en forma oportuna su imposibilidad de adherirse a alguna, algunas o todas ellas en un momento determinado.
6. Tiempo de respuesta ante una violación. El proveedor debe comunicar a SIFEI los planes de tratamiento que contempla ante posibles violaciones de la seguridad, y los tiempos en que tendrán efecto esas acciones.
7. Demostración de cumplimiento. El proveedor debe demostrar con evidencia irrefutable, que los controles que ha implementado y las acciones correctivas que ha diseñado cumplen con los requisitos contractuales.
8. Comunicación sobre cambios. el proveedor debe informar a la organización contratante, todos los cambios en su entorno que afecten el negocio o la operación de su cliente, en forma oportuna.
9. El Proveedor debe acreditar que su personal tiene conocimientos en materia de seguridad de la información.
10. Patente. Si el PROVEEDOR o su personal crean algún invento basado en información que el PROVEEDOR debe mantener confidencial en virtud del objeto del contrato, inmediatamente lo informará a SIFEI.

11. Marcas. Las partes se obligan a no hacer mal uso de la imagen, logotipos, tipografía, marcas, diseños o imágenes en la publicidad, obligándose a retirarlo inmediatamente y a corregir dicho material publicitario en un plazo no mayor a tres días posteriores al momento en que se solicite la corrección por escrito de dicho material publicitario.
12. Derechos de patente. El término "Derechos de Patente" significa patentes y solicitudes de patente motivadas por inventos creados por el PROVEEDOR o su personal, que están basados en información que el PROVEEDOR debe mantener confidencial en virtud del mismo y que fueron concebidos durante su vigencia. El proveedor renuncia expresamente a cualquier derecho de patente sobre las innovaciones técnicas que desarrolle en la ejecución del contrato, aceptando la cesión incondicional a SIFEI de los derechos de patente y derechos de explotación que se puedan deducir de los mismos.
13. Propiedad Intelectual. Las partes convienen que el presente instrumento no otorga a las mismas, licencia alguna, o algún tipo de derecho respecto de la "Propiedad Intelectual" de la parte contraria. Para efectos de este contrato, "Propiedad Intelectual" incluye todas las marcas registradas y/o usadas en México o en el extranjero por cualquiera de las partes, así como todo derecho sobre invenciones (patentadas o no), diseños industriales, modelos de utilidad, información confidencial, nombres comerciales, avisos comerciales, reservas de derechos, nombres de dominio, así como todo tipo de derechos patrimoniales sobre obras y creaciones protegidas por derechos de autor y demás formas de propiedad industrial o intelectual reconocida o que lleguen a reconocer las leyes correspondientes.

Cada una de las partes se obliga a no usar, comercializar, revelar a terceros, distribuir, regalar, o de cualquier otro modo disponer de cualquier desarrollo realizado por la otra parte, ni de cualquier material o material excedente que sea resultado de la Propiedad Intelectual, sin tener permiso previo y por escrito de la parte titular; mismos, que una vez concluida la vigencia del contrato, deberán ser devueltos a su propietario.
14. Transferencia de derechos. No podrá ceder en forma parcial ni total a favor de cualquier otra persona, los derechos y obligaciones que se deriven del presente contrato, con excepción de los derechos de cobro, en cuyo caso, deberá contar con el consentimiento previo y por escrito del representante legal de SIFEI.
15. Obligaciones. Cumplir en todo momento con el objeto del contrato así como con toda diligencia y empeño, respetando en todo momento todas y cada una de las políticas y demás lineamientos administrativos que SIFEI establece sobre seguridad de la información, no podrá alegar desconocimiento de cualquier política, procedimiento, lineamiento administrativo o modificación de los mismos cuando hayan sido actualizados por SIFEI independientemente de que estén publicados en la página de internet.

Adicionalmente, el proveedor deberá suscribir el "Convenio de Confidencialidad" proporcionado por SIFEI para los propósitos de cobertura de los numerales 2 y 3 arriba señalados; lo anterior con independencia de que el propio proveedor ofrezca un documento de similar propósito.

5. 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: AT-SI-RE-01 Acta compromiso 22082019 [9]

6. 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.

7. 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.

8. Referencias

- [1] G. M. G. Hernández, «IF-SI-RE-08 Lista de obligaciones legales, normativas y contractuales,» Orizaba, 2018.
- [2] G. M. G. Hernández, «GU-SI-RE-01 Metodología de Análisis de Riesgos,» Orizaba, 2018.
- [3] G. M. G. Hernández, «IF-SI-RE-10 Declaración de Aplicabilidad,» Orizaba, 2018.
- [4] G. M. G. Hernández, «IF-SI-RE-09 Organización de Seguridad de la Información,» Orizaba, 2018.



Código	PL-SI-RE-02
Versión	7.0
Publicación	21/08/2019

- [5] A. A. C. Pavón, «IF-RH-RE-07 Roles y Responsabilidades del Personal,» Orizaba, 2018.
- [6] G. M. G. Hernández, «IF-SI-CO-16 Inventario de activos,» Orizaba, 2019.
- [7] G. M. G. Hernández, «IF-SI-RE-12 Informe de Seguridad Física y Ambiental,» Orizaba, 2019.
- [8] G. M. G. Hernández, «Publicación de la política de seguridad de la información,» Orizaba, 2018.
- [9] J. C. G. Hernández, «AT-SI-RE-01 Acta compromiso 22082019,» Orizaba, 2019.
- [10] R. V. Ramírez, «Guía general para elaboración de documentos,» Orizaba, 2018.
- [11] A. C. Cabrera, «ACTA DE COMPROMISO DE DIRECCION GENERAL CON EL SGSI FEBRERO 2018,» Orizaba, 2018.

