Código	PL-SI-PU-05
Versión	3.0
Publicación	23/04/2019

INFORMACIÓN PÚBLICA
Páginas: En su totalidad
Fecha: 12/05/2017
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 clasificación y manejo de la información

Contenido

1. Generalidades

1.1 Objetivo

Establecer la clasificación de la información de acuerdo a las disposiciones del INAI (Instituto Nacional de Acceso a la Información y Protección de Datos) para asegurar que la información este clasificada de manera correcta y se le dé el tratamiento de protección de acuerdo a su nivel de clasificación.

1.2 Alcance

La presente política es aplicable para la información que maneja SIFEI y que intervenga en el proceso de CFDI, está dirigida a los empleados que colaboran en SIFEI, auditores internos, proveedores y auditores del Servicio de Administración Tributaria SAT

1.3 Referencias Normativas

Norma	Control
ISO/IEC 17799 Técnicas de Seguridad	7.2 Clasificación de la información
ISO/IEC 27001:2013 Seguridad de la Información	A 8.2 Clasificación de la Información
MATRIZ DE CONTROL	Señalada en la fracción II de la ficha 111/CFF del Anexo 1-A de la RMF
Código Fiscal de la Federación (CFF) 29, 29-A	Resolución Miscelánea Fiscal (RMF) 2018
LFPDPPP	Ley Federal De Protección de Datos Personales en posesión de los particulares
Reglamento de la ley federal de transparencia y acceso a la Información pública gubernamental	
INAI	Instituto Nacional de Acceso a la Información y Protección de Datos
CONAIP/SNT/ACUERDO/EXT18/03/2016-03	Acuerdo del consejo nacional del sistema nacional de transparencia, acceso a la información pública y protección de datos personales, por el que se aprueban los lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

1.4 Términos y Definiciones

Término	Definición
Activo	Cualquier cosa que tenga valor para la empresa
Clasificación	Es la acción de organizar o situar algo según una determinada directiva.
INAI	Organismo Público Autónomo encargado de facilitar y garantizar el acceso de las personas a la información pública y el acceso y protección de los datos personales, promover la cultura de la transparencia en la gestión pública y la rendición de cuentas del gobierno a la sociedad

Término	Definición
Artículo 30 del reglamento de la ley federal de transparencia y acceso a la información pública gubernamental	Los expedientes y documentos clasificados como reservados deberán llevar una leyenda que indique su carácter de reservado, la fecha de la clasificación, su fundamento legal, el periodo de reserva y la rúbrica del titular de la unidad administrativa.
Artículo 37 del reglamento de la ley federal de transparencia y acceso a la información pública gubernamental	La información confidencial no estará sujeta a plazos de vencimiento y tendrá ese carácter de manera indefinida, salvo que medie el consentimiento expreso del titular de la información o mandamiento escrito emitido por autoridad competente.
Artículo 38 del reglamento de la ley federal de transparencia y acceso a la información pública gubernamental	Los particulares que entreguen a las dependencias y entidades información confidencial de conformidad con lo establecido en el artículo 19 de la Ley, deberán señalar los documentos o las secciones de éstos que la contengan, así como el fundamento por el cual consideran que tenga ese carácter.
Datos personales	La información numérica, alfabética, gráfica, acústica o de cualquier otro tipo concerniente a una persona física, identificada o identificable
Aviso de privacidad	Este documento informa a los titulares las características principales o los términos y condiciones a que son sometidos sus datos personales. Puede ser difundido a través de medios electrónicos y físicos. [1]

1.5 Roles y responsabilidades

Actividad	Jefe de Seguridad	Jefe de Infraestructura	Comité de Seguridad	Propietarios de la información
Asignar los niveles adecuados de clasificación de la información	R	C	I	A
Revisar periódicamente la clasificación de la información con el propósito de verificar que se cumplan con los requerimientos de negocio	C	I	R	A
Asegurar que los controles de seguridad aplicados sean consistentes con la clasificación realizada	I	R	I	A
Determinar los niveles de acceso a la información	R	C	I	A

2. Definición de clasificación de la información

Se entenderá por Clasificación de la información al acto por el cual se determina que la información que se posee como entidad es **Reservada** o **Confidencial**, lo anterior en términos del Artículo 2 párrafo I del

Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, tomada como referencia normativa.

Dado lo anterior SIFEI define la clasificación de la información como:

La manera de identificar la información y el impacto que ocasionaría su pérdida, difusión, acceso no autorizado, destrucción o alteración, aplicando para ello criterios de confidencialidad, integridad y disponibilidad. Así sabremos qué información debemos cifrar, quién puede utilizarla y quién es responsable de su seguridad.

3. Requisitos legales establecidos en la Ley Federal de Protección de Datos en Posesión de Particulares LFPDPP

La LFPDPPP tiene por objeto proteger los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado. Esto con el fin de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. Asimismo, este ordenamiento reconoce los principios de interpretación reconocidos como estándar internacional en la materia. Se entiende por datos personales a la información numérica, alfabética, gráfica, acústica o de cualquier otro tipo concerniente a una persona física, identificada o identificable, que da identidad y descripción a la persona, algunos ejemplos de información personal es edad, domicilio, número de teléfono, correo electrónico personal, número de seguridad social, CURP entre otros

En lo que respecta a los sujetos regulados por esta ley, son todas aquellas personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, exceptuando a las sociedades de información crediticia y las personas que traten datos para su uso personal.

Cabe resaltar que, ajustándose a lo que marca la LFPDPPP, los poseedores de los datos deben dar a conocer a los titulares, la información que de ellos se recaba y los fines para los cuales serán utilizados sus datos, a través del aviso de privacidad.

De igual manera, la LFPDPPP estipula obligaciones para los particulares que lleven a cabo el tratamiento de datos personales, respecto a la seguridad administrativa, técnica y física que permita proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. En caso de existir alguna vulneración de seguridad, el responsable deberá informar inmediatamente al titular, a fin de que éste pueda emprender acciones que ayuden a la defensa de sus derechos.

El derecho a la protección de datos personales consiste en un derecho fundamental que busca la protección de la persona en relación con el tratamiento de la información, al poder de decisión y control que faculta a

su titular de decidir cuáles de sus datos proporciona a terceros y al derecho que tiene toda personal a conocer y decidir quién como y de qué manera recaba, utiliza y comparte sus datos personales.

Los organismos que cuenten con datos personales tienen la obligación de:

- Aplicar medidas de seguridad encaminadas a garantizar la confidencialidad, integridad y disponibilidad de la información bajo niveles de protección alto, medio y bajo.
- Obligación del ente público y de quienes intervienen en cualquier fase del tratamiento de datos personales de guardar y respetar la confidencialidad de los mismos mediante un Aviso de privacidad.
- GUARDAR el necesario SECRETO respecto a cualquier tipo de información de carácter personal conocida en función del trabajo desarrollado, incluso una vez concluida la relación laboral con el ente público.

Dado lo anterior, a continuación se enlistas los requisitos legales establecidos en la Ley Federal de Protección de Datos en Posesión de Particulares (LFPDPP):

- Elaboración de avisos de privacidad, cumpliendo con los requisitos de la ley, y redactados con un lenguaje claro y sencillo, que permita entender a los clientes, los alcances del consentimiento que está otorgando, respecto al tratamiento de datos sus personales.
- Una vez que el dato ha sido recabado, garantizar que, durante el ciclo del mismo, se cumplan con los requerimientos señalados en la normativa en la materia y que el tratamiento del dato se haga conforme los principios del derecho a la protección de datos personales.
- Garantizar procedimientos efectivos de ejercicio de derechos de acceso, rectificación, cancelación y oposición (ARCO), así como de portabilidad de los datos.
- Establecer cláusulas de confidencialidad de la información, en los contratos que se celebren para establecer relaciones laborales, para que, de manera expresa, los trabajadores no puedan sustraer, utilizar o transmitir datos personales o información de la empresa.
- Establecer mecanismos técnicos que limiten el acceso a los datos personales, de acuerdo a las funciones de los puestos de trabajo, así como sistemas de autenticación y esquemas de privacidad por diseño.
- Capacitar al personal que lleve a cabo tratamiento de datos personales, a fin de sensibilizarlo en las implicaciones que podría tener hacer un mal uso de la información y de que conozca la regulación jurídica en la materia.
- Verificar las medidas físicas y digitales de seguridad de la información al interior de la empresa, así como las políticas de ciberseguridad instrumentadas a la luz de la normativa en materia de protección de datos personales.
- Revisar que, en la contratación de servicios de almacenamiento de información -como el cómputo en la nube- se garantice, por lo menos: la obligación de dar aviso en caso de cualquier vulneración a las medidas de seguridad de la plataforma electrónica, la portabilidad y destrucción de los datos al término del contrato, mecanismos alternativos de resolución de controversias como la mediación electrónica, la reputación y políticas de transparencia de la empresa a contratar, que se privilegie la

jurisdicción nacional en la prestación del servicio, las medidas compensatorias en caso de vulneraciones y mal uso de la información, así como evitar contratos de adhesión que no atiendan a las características de los datos a almacenar, de acuerdo al tipo de información, servicio y empresa. [2]

4. Descripción de la política

- Los titulares de las áreas en SIFEI llevarán a cabo la clasificación de la información en el momento en que:
    - Se genere, obtenga, adquiera o transforme la información
- Los expedientes y documentos clasificados como **reservados** deberán llevar una leyenda que indique su carácter de reservado, la fecha de la clasificación, su fundamento legal, el periodo de reserva y la rúbrica del titular del área que lo reserva. Lo anterior en concordancia con el Artículo 30 del Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, tomada como referencia normativa.
- La información confidencial no estará sujeta a plazos de vencimiento y tendrá ese carácter de manera indefinida. Lo anterior en concordancia con el Artículo 37 del Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, tomada como referencia normativa.
- Los particulares que entreguen información confidencial, deberán señalar los documentos o las secciones de éstos que la contengan, así como el fundamento por el cual consideran que tenga ese carácter. Lo anterior en concordancia con el artículo 38 del Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, tomada como referencia normativa.
- Todos los activos estarán registrados en un inventario indicando su propietario y el responsable del resguardo.
- Debe existir un procedimiento formal de clasificación, etiquetado y manejo de información.

4.1.1 Niveles de Confidencialidad

De acuerdo a las disposiciones del INAI, toda la información será clasificada en alguno de los siguientes niveles de confidencialidad presentados Tabla 1:

Tabla 1 Niveles de confidecialidad

Nivel de Confidencialidad	Descripción	Criterios de Clasificación	Restricciones de accesos
Pública	Se refiere a la información de uso general que por su contenido o contexto no requiere de protección especial y su distribución pública es a través de canales	Hacer pública la información no representa ningún riesgo para la organización.	La información se encuentra disponible para todo el público.

Nivel de Confidencialidad	Descripción	Criterios de Clasificación	Restricciones de accesos
	autorizados por la empresa. Esta clasificación incluye cualquier otra información que no se encuentre dentro de cualquiera de las otras clasificaciones, que no requiera protección contra accesos no autorizados.		
Reservada	Se refiere a la información cuya divulgación estará restringida únicamente al personal autorizado por el responsable de la misma. Esta clasificación aplica para información únicamente de uso interno de los procesos de negocio de SIFEI y que se requiere tenga esta clasificación por un periodo de tiempo.	El acceso no autorizado a la información podría dañar considerablemente el negocio y/o a la reputación de la organización.	La información se encuentra disponible únicamente para un grupo específico de empleados y de terceros autorizados que laboren en SIFEI y que haya firmado el convenio de confidencialidad correspondiente, así como del responsable y propietario de la información.
Confidencial	Es el más alto nivel de clasificación de la información y será utilizada sobre la premisa de que la divulgación de la misma está estrictamente limitada y predeterminada a un número restringido de personas que asumen la responsabilidad de protegerla. Es la información personal o información sensible de terceros en posesión de SIFEI; se trata además de información clave para SIFEI vinculada con el negocio y la información de aplicación industrial o comercial relacionada con el secreto industrial.	El acceso no autorizado a la información conlleva severos impactos a la operación y reputación de la empresa, sus accionistas, socios de negocio y clientes.	La información está disponible exclusivamente por parte de un reducido grupo de personas dentro de la organización como lo son Directivos y Jefes de Área, así como para el responsable y propietario de la información.

4.1.2 Reclasificación

La clasificación de los activos de la empresa no necesariamente se mantendrá en la misma clasificación a la que fueron asignados. Por esta razón los propietarios de los activos revisarán el nivel de confidencialidad de sus activos de información por lo menos cada dos años y evaluarán si es necesario cambiar el nivel de acuerdo a alguna nueva política establecida por SIFEI.

En caso de el propietario de los activos considere cambiar la clasificación, deberá cambiar la etiquetar y notificar a los usuarios que correspondan.

4.1.3 Etiquetado de la información

Una vez que se han clasificado los activos de la organización, los niveles de confidencialidad son etiquetados de la siguiente forma:

- **Documentos en papel:** la confidencialidad de este tipo de documentos se indica con una etiqueta física en la portada. Adicionalmente, el nivel de confidencialidad se indica también en la parte inferior como pie de página del documento.
- **Documentos electrónicos:** la confidencialidad de los documentos electrónicos se indica con una etiqueta en la portada. Adicionalmente, el nivel de confidencialidad se indica en la parte inferior como pie de página del documento. Finalmente, en la nomenclatura del documento se indica el nivel de confidencialidad de acuerdo a alguna de las siguientes siglas: PU= Pública, RE= Reservada y CO= Confidencial.
- **Sistemas de información:** el nivel de confidencialidad en aplicaciones y bases de datos se indica en la pantalla de acceso al sistema, así como también en la esquina superior derecha de cada pantalla consecutiva que muestra información confidencial.
- **Correo electrónico:** tendrá la siguiente leyenda: La presente información se envía únicamente para el destinatario, y contiene Información de carácter CONFIDENCIAL. La modificación, retransmisión, difusión, copia u otro uso de esta información por cualquier medio, por personas distintas al destinatario está estrictamente prohibido. Si usted no es el destinatario, por favor notifique al remitente respondiendo a este mensaje, y borre el mismo y sus anexos sin retener copia alguna. No garantizamos que este correo electrónico o sus archivos que se encuentren adjuntos están libres de virus u otros defectos, y usted, el receptor, debe confirmar que estén libres de virus u otros defectos. Solución Integral de Facturación Electrónica e Informática SIFEI S. A. de C.V. no se hace responsable por cualquier daño ocasionado por algún virus que pueda ser transmitido por este o cualquier otro correo electrónico.

  The information contained in this message is being sent to the intended recipient, and contains CONFIDENTIAL Information. The modification, retransmission, disclosure, copy or other use of such information by persons other than the intended recipient is strictly prohibited. If you are not the intended recipient, please advise the sender immediately by reply e-mail and delete this message and any attachments without retaining a copy. No warranty is made that this e-mail or its attachments are free from computer viruses or other defects, and you, the recipient, should confirm that it is free of viruses or other defects. Solución Integral de Facturación Electrónica e Informática SIFEI S. A. de C.V. is not liable for any damage caused by viruses that may be transmitted by this or any other e-mail.

  Solución Integral de Facturación Electrónica e Informática SIFEI S. A. de C.V. cumple con lo establecido en la Ley Federal de Protección de Datos Personales en Posesión de Particulares, para más información consulte el Aviso de Privacidad en https://www.sifei.com.mx/privacidad

- **Soporte de almacenamiento electrónico físico (discos, tarjetas de memoria, etc.):** el nivel de confidencialidad se indica sobre la superficie de cada soporte de almacenamiento.
- **Equipos físicos:** el nivel de confidencialidad se indica en la parte de atrás del equipo físico mediante una etiqueta.

4.1.4 Manejo de Información clasificada

- Todo el personal que tiene acceso a información clasificada seguirá las reglas enumeradas en la Tabla 2. El Jefe de Seguridad de la Información aplicará las acciones disciplinarias correspondientes cuando se incumplan las reglas o cuando la información se transmita a personas no autorizadas. Cada incidente relacionado con el manejo de información clasificada debe ser reportado de acuerdo

con lo definido en el documento PR-SI-CO-17 Procedimiento para la Gestión de Incidentes y problemas.

- La salida de los activos de información fuera de las instalaciones será únicamente con la autorización del responsable, de acuerdo a lo establecido en el documento PL-SI-PU-07 Política de generación Reglas para el Uso Aceptable de la Información.

Tabla 2 Reglas de Clasificación de la información

Activo	Reservada	Confidencial
Documentos en papel	Únicamente las personas autorizadas tendrán acceso a la información. El documento que requiera enviarse fuera de la organización, se enviará por correo certificado. Los documentos serán retirados frecuentemente de impresoras y máquinas de fax.	Únicamente las personas autorizadas tendrán acceso a la información. El documento será almacenado en un gabinete con llave. Los documentos serán transferidos dentro y fuera de la organización solamente dentro de un sobre cerrado. Los documentos que se envían fuera de la organización, serán con acuse de recibo. Los documentos serán retirados inmediatamente de impresoras y máquinas de fax. El fotocopiado de documentos será limitado y estará únicamente a cargo del propietario del documento. La documentación que requiera destruirse se convertirá en tiras que se mezclarán antes de enviar a la basura. Únicamente el propietario del documento podrá destruirlo.
Documentos electrónicos	Únicamente las personas autorizadas tendrán acceso a los documentos. Cuando se intercambian archivos a través de servicios como FTP, mensajería instantánea, etc., estarán protegidos con clave.	Únicamente las personas con autorización para este documento podrán acceder. Cuando se intercambian archivos a través de servicios como FTP, mensajería instantánea, etc., estarán protegidos con clave. Únicamente el propietario del documento podrá borrarlo.
Sistemas de Información	Únicamente las personas autorizadas tendrán acceso. El acceso al sistema de información estará protegido por una clave segura. La pantalla se bloqueará automáticamente luego de 10 minutos de inactividad. El sistema de información estará ubicado en habitaciones con acceso físico controlado.	Únicamente las personas autorizadas tendrán acceso. El acceso al sistema de información estará protegido por una clave segura. El acceso al sistema de información estará controlado mediante un proceso de autenticación. El sistema de información estará ubicado en habitaciones con acceso físico y controlado. Los datos serán borrados con un algoritmo que garantice un borrado seguro.
Controles de auditoría	Únicamente las personas autorizadas tendrán acceso.	El acceso al sistema de información estará controlado mediante un proceso de autenticación.

Activo	Reservada	Confidencial
	El acceso al sistema de información estará protegido por una clave segura. La pantalla se bloqueará automáticamente luego de 10 minutos de inactividad. El sistema de información estará ubicado en habitaciones con acceso físico controlado.	El sistema de información estará ubicado en habitaciones con acceso físico controlado Los datos serán borrados con un algoritmo que garantice un borrado seguro.
Correo electrónico	Únicamente las personas autorizadas tendrán acceso. El remitente verificará cuidadosamente el destinatario y la documentación a enviar.	Únicamente las personas autorizadas tendrán acceso. El remitente verificará cuidadosamente el destinatario y la documentación a enviar. Aplican todas las reglas mencionadas en la columna "Sistemas de información".
Equipos Físicos	La información almacenada en los equipos físicos, estará bajo responsabilidad del usuario del equipo. Únicamente las personas autorizadas tendrán acceso.	La información almacenada en los equipos físicos, estará bajo responsabilidad del usuario del equipo. Únicamente las personas autorizadas tendrán acceso.
Soportes de almacenamiento electrónico	Únicamente las personas autorizadas tendrán acceso. Los soportes o archivos estarán protegidos con clave. El documento que requiera enviarse fuera de la organización, se enviará por correo certificado. El soporte estará guardado únicamente en habitaciones con acceso físico controlado.	El soporte se almacenará en un gabinete con llave. El documento que requiera enviarse fuera de la organización, se enviará por correo certificado. Si el soporte requiere enviarse fuera de la organización deberá ser con previa autorización. Sólo el propietario del soporte podrá borrar sus datos o destruirlos. Los datos serán borrados con un algoritmo establecido por el Jefe de Infraestructura que garantice un borrado seguro.

5. Aspectos de clasificación de la información para proveedores

5.1 Directrices de clasificación de información para terceros

Algunos proveedores por sus actividades, manejan información reservada o confidencial, esta información debe ser manejada y clasificada por el proveedor con el mismo nivel de confidencialidad que se declara en el apartado 4.1.1, descrita en la Tabla 1. Del mismo modo, los reportes o cualquier información que el proveedor genere usando documentación o información provista por SIFEI debe ser tratada y clasificada con el mismo nivel de confidencialidad que tiene la información usada para la gestión de dichos reportes.

Todos los proveedores que utilicen o tengan acceso a información de SIFEI y que estén directamente o indirectamente involucrados en el proceso de CFDI deben tener firmado un contrato con cláusulas de confidencialidad que eviten la divulgación y/o mal uso de la información propiedad de SIFEI.

5.2 Cláusulas de clasificación de la información

- SIFEI constituye que toda la información manejada, generada e intercambiada con el proveedor es clasificada como lo indique el INAI y las leyes vigentes.
- Se cumplirán por parte del proveedor, los lineamientos y clasificación de la información establecidas por SIFEI para asegurar su confidencialidad, disponibilidad e integridad de la información.
- El proveedor deberá cumplir las funciones y obligaciones aplicadas a la clasificación de la información según los lineamientos establecidos por SIFEI.
- Se garantizará el manejo de la información de acuerdo a su nivel de clasificación
- Se prohíbe la transmisión de información de SIFEI a otras compañías.

5.3 Manuales de clasificación de información para proveedores

La información acerca de la clasificación para proveedores se establece en el documento "GU-SI-PU-04 Manual de clasificación de información para proveedores".

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

- El presente documento es válido a partir de su fecha de publicación
- La revisión de la presente política se llevará a cabo: cada 12 meses o cuando ocurran cambios significativos.
- El Propietario del presente documento es: el Jefe de Seguridad de la información.

8. Referencias

[1] A. a. l. I. y. P. d. D. P. Instituto Nacional de Transparencia, «Introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados,» Orizaba, 2019.

[2] O. A. M. Enríquez, «Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento,» Revista IUS, 06 2018. [En línea]. Available: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472018000100267. [Último acceso: 23 04 2019].

[3] M. I. R. Rangel, «Instituto Veracruzano de acceso a la información y datos personales IVAI-Protección de datos personales,» Orizaba, 2019.