SCD-PPCI-01

Política y Procedimiento de Clasificación de la Información.

Sistemas de Comercio Digital

Versión 1.7

ÍNDICE

1. Introducción

Sistemas de Comercio Digital, S. de R.L. de C.V., en adelante Sistemas de Comercio Digital o SCD, ha decidido cumplir con la matriz de controles de seguridad emitida por el SAT. Uno de los requisitos es contar con una política y procedimientos formales para la clasificación de la información de acuerdo a su relevancia o sensibilidad y en cumplimiento a las disposiciones del INAI.

2. Objetivos del Documento

Los principales objetivos de este documento son:

1. Documentar las políticas y procedimientos para la clasificación de la información que SCD recibe en cumplimiento de sus operaciones, estableciendo los lineamientos que regulan dicha clasificación.

3. Alcance

El alcance del documento "SCD-PPCI-Política y Procedimiento de Clasificación de la Información" y las actividades que se presentan son para uso del personal

El alcance comprende:

I. Hacer del conocimiento de todo el personal de SCD los criterios relacionados con la clasificación de la información relacionada con el proceso de operación de SCD

4. Audiencia

Este documento está dirigido a:

I. Las autoridades revisoras del cumplimiento de los requerimientos de seguridad por parte del SAT.
II. La Presidencia y Dirección de Sistemas de Comercio Digital.
III. El personal de Sistemas de Comercio Digital.

Referencias Utilizadas

Las fuentes que directamente o indirectamente fueron usadas para la elaboración de este documento, son las siguientes:

1. LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL *(última reforma publicada en el DOF)*
2. Requerimientos de control y seguridad emitidos por el SAT (Matriz de Controles de Seguridad de Información Emitidos por el SAT en el Sito Web Oficial del SAT: http://www.sat.gob.mx).
3. Marco de mejores prácticas de ITIL v3 de OGC del Reino Unido.
4. Estándar Internacional de Seguridad de Información - ISO/IEC 27001:2005.
5. Estándar Internacional de Gestión de Servicios de TI – ISO/IEC 20000:2005
6. Marco de Trabajo de Controles de Seguridad de Información - Cobit 4.1.

5. Marco Legal

Las políticas de seguridad presentadas en este manual se encuentran definidas dentro de un marco legal que contempla los principales ordenamientos vigentes Constitucionales y aquellos relacionados con el Sistema de Administración

Tributaria "SAT" en los Estados Unidos Mexicanos, así como los relacionados con el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

I. Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.
II. Ley Federal de Protección de Datos Personales en Posesión de los Particulares
III. Ley Federal de Derechos.
IV. Ley del Servicio de Administración Tributaria.
V. Ley Federal de los Derechos del Contribuyente.
VI. Ley Orgánica del Tribunal Federal de Justicia Fiscal y Administrativa.
VII. ANEXO 20 de la Resolución Miscelánea Fiscal para 2017
VIII. Reglamento del Código Fiscal de la Federación.
IX. Reglamento Interior del Servicio de Administración Tributaria.
X. Reglamento de la Ley Orgánica del Tribunal Federal de Justicia Fiscal y Administrativa.
XI. Reglamento Interior de la Secretaría de Hacienda y Crédito Público.
XII. Especificaciones técnicas conforme a las cuales las instituciones del sistema financiero, deben verificar la clave del RFC y los datos de identidad de sus clientes.
XIII. Procedimiento que deberán seguir los Proveedores de Certificación de CFDI autorizados para recibir el Certificado de Sello Digital.

6. Consideraciones Generales

Durante del presente documento se tomaron en cuenta las siguientes consideraciones generales:

I. La política y procedimiento de clasificación de la información ha sido desarrollado desde la perspectiva de los controles de seguridad emitidos por el SAT.
II. El presente documento:
   - ❖ Ha sido desarrollado desde la perspectiva de los responsables de la seguridad de información en "Sistemas de Comercio Digital" y se enfoca a los controles del etiquetado y manejo de la información.
   - ❖ Es un documento que debe ser publicado en un servidor con acceso para todo el personal de SISTEMAS DE COMERCIO DIGITAL por parte de la Dirección de la empresa. Adicionalmente este documento se hace del conocimiento del personal.

II. El incumplimiento accidental o deliberado de las políticas, normas y procedimientos, será considerado una falta administrativa y tendrá consecuencias laborales y/o legales a consideración de "Sistemas de Comercio Digital", dependiendo de la gravedad de la falta.

7. Política y Procedimiento de Clasificación de la Información

Sistemas de Comercio Digital, S. de R.L. de C.V. provee servicios electrónicos de PAC, efectivos y rápidos a Contribuyentes Mexicanos. Como líder de la industria, es crítico para Sistemas de Comercio Digital implementar esta política de Clasificación de Información para ayudar a manejar y proteger sus activos informáticos en cumplimiento a las disposiciones del INAI.

Antes de proceder con la clasificación de la información, los documentos Políticas y Procedimientos, pueden ser identificados con una nomenclatura específica para facilitar su localización y administración. En SCD, se ha optado por dar la nomenclatura a los documentos de la siguiente forma:

Anteponer las siglas SCD, seguidas de un guion, y la primara letra de cada palabra del nombre del documento, seguido de un guion y la versión superior del documento a dos dígitos. Como ejemplo se tiene al documento "Procedimiento de Contacto con las Autoridades" en una versión **1**.13, su nomenclatura quedaría como "SCD-PCA-01".

La cantidad de letras (solo la primera letra de cada palabra o poder incluir una segunda letra) de cada palabra, así como la inclusión o exclusión de la primera letra de palabras como "de", "la", etc., son opcionales en casos donde se pretenda dar mejor sentido a la abreviatura, diferenciar entre nomenclaturas similares de documentos diferentes o determinar una nomenclatura más fácil de recordar. Por otro lado, documentos que su nombre contengan solo una palabra, como el caso de "Comunicaciones", no requerirán de este tipo de nomenclatura y solo se antepondrá las siglas SCD y el guion.

7.1. Lineamientos Legales de Clasificación de la Información.

Sistemas de Comercio Digital, define la clasificación de la información como el acto de colocar los datos en categorías para determinar el nivel de seguridad y tratamiento que se le debe dar a la misma de acuerdo al valor que tiene para el negocio. De esta forma, se pueden estandarizar los controles de seguridad para proteger adecuadamente la información

El INAI establece una clasificación de la información de la siguiente manera: Pública, Reservada y Confidencial. La descripción de cada tipo de información y sus lineamientos legales se describen a continuación:

INFORMACION PUBLICA: Información de uso general que por su contenido o contexto no requiere de protección especial y su distribución pública ha sido permitida a través de canales autorizados por la empresa. Es la información que no es considerada como protegida, cuyo acceso al público es permanente, libre, fácil, gratuito y expedito. También se considera información pública, la información de libre acceso que debe publicarse y difundirse de manera universal, permanente, actualizada y, en el caso de la información electrónica, a través de formatos amigables para el ciudadano, sin que se requiera solicitud de parte interesada.

INFORMACION RESERVADA. Se considera información cuya divulgación debe ser restringida únicamente al personal que la requiere conocer, previa autorización del responsable de la misma.
La Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, en su Artículo 3, sección VI, define a la Información Reservada como: "Aquella información que se encuentra temporalmente sujeta a alguna de las excepciones previstas en los Artículos 13 y 14 de esta Ley"

Especificando los Artículos 13 y 14 de la mencionada Ley, lo siguiente:

"Artículo 13. *Como información reservada podrá clasificarse aquélla cuya difusión pueda:*

I. *Comprometer la seguridad nacional, la seguridad pública o la defensa nacional;*

II. *Menoscabar la conducción de las negociaciones o bien, de las relaciones internacionales, incluida aquella información que otros estados u organismos internacionales entreguen con carácter de confidencial al Estado Mexicano;*

III. *Dañar la estabilidad financiera, económica o monetaria del país;*

IV. *Poner en riesgo la vida, la seguridad o la salud de cualquier persona, o*

V. *Causar un serio perjuicio a las actividades de verificación del cumplimiento de las leyes, prevención o persecución de los delitos, la impartición de la justicia, la recaudación de las contribuciones, las operaciones de control migratorio, las estrategias procesales en procesos judiciales o administrativos mientras las resoluciones no causen estado.*

Artículo 14. *También se considerará como información reservada:*

I. *La que por disposición expresa de una Ley sea considerada confidencial, reservada, comercial reservada o gubernamental confidencial;*

II. *Los secretos comercial, industrial, fiscal, bancario, fiduciario u otro considerado como tal por una disposición legal;*

III. *Las averiguaciones previas;*

IV. *Los expedientes judiciales o de los procedimientos administrativos seguidos en forma de juicio en tanto no hayan causado estado;*

V. *Los procedimientos de responsabilidad de los servidores públicos, en tanto no se haya dictado la resolución administrativa o la jurisdiccional definitiva, o*

VI. *La que contenga las opiniones, recomendaciones o puntos de vista que formen parte del proceso deliberativo de los servidores públicos, hasta en tanto no sea adoptada la decisión definitiva, la cual deberá estar documentada.*

Cuando concluya el periodo de reserva o las causas que hayan dado origen a la reserva de la información a que se refieren las fracciones III y IV de este Artículo, dicha información podrá ser pública, protegiendo la información confidencial que en ella se contenga.

No podrá invocarse el carácter de reservado cuando se trate de la investigación de violaciones graves de derechos fundamentales o delitos de lesa humanidad."

La vigencia de la clasificación de la información reservada, se delimita en el Articulo 15 de dicha ley, de la siguiente manera:

"Artículo 15. *La información clasificada como reservada según los artículos 13 y 14, podrá permanecer con tal carácter hasta por un periodo de doce años. Esta información podrá ser desclasificada cuando se extingan las causas que dieron origen a su clasificación o cuando haya transcurrido el periodo de reserva. La disponibilidad de esa información será sin perjuicio de lo que, al respecto, establezcan otras leyes."*

El Instituto, de conformidad con el Reglamento, o la instancia equivalente a que se refiere el Artículo 61, establecerán los criterios para la clasificación y desclasificación de la información reservada.

INFORMACION CONFIDENCIAL. Este tipo de información es protegida, intransferible e indelegable, queda prohibido su acceso, distribución, comercialización, publicación y difusión generales de forma permanente, con excepción de las autoridades competentes que, conforme a la ley, tengan acceso a ella, y de los particulares titulares de dicha información. Es el más alto nivel de clasificación de la información y debe ser utilizado 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.

La **Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental,** en su **Artículo 18**, define a la **Información Confidencial** como:

"I. *La entregada con tal carácter por los particulares a los sujetos obligados, de conformidad con lo establecido en el Artículo 19, y*

II. *Los datos personales que requieran el consentimiento de los individuos para su difusión, distribución o comercialización en los términos de esta Ley.*

No se considerará confidencial la información que se halle en los registros públicos o en fuentes de acceso público."

Para el proceso de destrucción de la información contenida en papel o en medios de almacenamiento referirse al documento "SCD-SAME-01 - Procedimiento de Sanitización de medios v.0.1"

7.2. Lineamientos Generales del Manejo y Clasificación de la Información

- Basándose en las definiciones del punto 7.2, la información debe ser clasificada por el dueño de la información y este a su vez debe informar SCD sobre su clasificación de manera que se tomen las medidas requeridas para preservar la confidencialidad e integridad de la misma.
- El dueño de la información es responsable por la actualización de la clasificación de la información.
- El dueño de la información es autónomo de reclasificarla cuando lo considere necesario y debe notificar cualquier cambio del rotulo al Director de Operaciones y/o al Gestor de Servicios de Comercio Digital, así como notificar a los usuarios y custodios de la información.
- Los funcionarios de la Dirección de Informática son claramente custodios, así como los administradores de sistemas locales. Siempre que la información sea almacenada en un computador personal, el usuario inmediatamente será su custodio.

- Los usuarios son responsables de familiarizarse y atender todos los aspectos de la política de seguridad. En caso de existir dudas por parte de los usuarios con respecto a la manipulación apropiada de la información estas deben ser consultadas con el custodio o dueño.
- Se debe firmar un acuerdo de confidencialidad con terceras partes, en caso de requerir entregar información electrónica o escrita confidencial o interna, con las restricciones de su uso.
- Se deben utilizar los mecanismos apropiados de control de acceso a la información dependiendo de su nivel de clasificación.
- Los empleados, contratistas o terceros no pueden tomar información secreta, confidencial o interna cuando dejan de trabajar para SCD.
- Destrucción de Información secreta, confidencial o interna: Cuando ya no se requiera una información clasificada como confidencial/reserva o interna, debe ser destruida mediante un método aprobado. Si la información se encuentra contenida en papel, la destrucción debe ser mediante trituración, para los casos en que al información se encuentre contenida en un dispositivo de almacenamiento electrónico (memoria usb, equipo de cómputo, etc.) deberá solicitarse el borrado seguro o en su caso, la destrucción del dispositivo de almacenamiento.
- La información que sea catalogada como secreta o confidencial que requiera ser transmitida por medios de comunicación públicos debe utilizar un esquema de cifrado con el fin de proteger su confidencialidad e integridad.
- Los empleados de los terceros con los cuales SCD tiene acuerdos comerciales, no deben revelar información confidencial a terceras partes a menos que el originador de la información haya aprobado su revelación y la parte que la reciba haya firmado un acuerdo de confidencialidad.

7.3. Clasificación de la información por terceros.

Existen proveedores que por sus actividades, manejan información reservada o confidencial de “Sistemas de Comercio Digital” para sus actividades. Esta información debe ser manejada y clasificada por el proveedor con el mismo nivel de confidencialidad durante su uso. Del mismo modo, los reportes o cualesquier información que el proveedor genere usando documentación o información provista por “Sistemas de Comercio Digital” debe ser tratada y con el mismo nivel de confidencialidad que tiene la información usada para la gestión de dichos reportes.
Todos los proveedores de que usen o tengan acceso a información de “Sistemas de Comercio Digital” deben tener firmado un contrato con cláusulas de confidencialidad que eviten la divulgación y/o mal uso de la información propiedad de la empresa.