POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN

ÁREA	FIRMA	DEPARTAMENTO	FECHA
Elaboró Luis Alejandro Blanco Sepúlveda		Procesos	11/04/2018
Revisó Alberto Salas Acosta		Dirección de Operaciones Comerciales	11/04/2018
Aprobó José Cruz Aarón Hernández		Dirección de Operaciones	11/04/2018

TABLA DE CONTROL DE CAMBIOS

FECHA	NIVEL DE REVISIÓN	CAMBIOS
01/09/2017	7	Se agrega el apartado de Clasificación de información SAT y la Política de Autorización de documentos.
11/04/2018	8	De acuerdo con los nuevos lineamientos del SAT se realizan cambios en los siguientes puntos: • Roles y Responsabilidades • Lineamientos • Clasificación de la Información • Autorización de Políticas y Procedimientos Internos • Aspectos de Clasificación de la Información para Proveedores • Sanciones

Nivel de clasificación: Reservada.
"Información cuya divulgación debe ser restringida únicamente al personal de la compañía que la requiere".

ÍNDICE

1. INTRODUCCIÓN

Con el desarrollo de la tecnología, la información es en uno de los activos más importantes para las organizaciones, convirtiéndose en el recurso vital para la gestión y la toma de decisiones. Teniendo en cuenta esta importancia, es necesario que la compañía identifique y organice la información, acorde con las políticas establecidas.

A. DEFINICIÓN

La empresa define Clasificación de información como: La actividad de organizar elementos de información para la preservación, aseguramiento y cumplimiento de las siguientes características:

- **Confidencialidad**: Los activos de información sólo pueden ser accedidos y custodiados por usuarios que tengan permisos para ello.
- **Integridad:** El contenido de los activos de información debe permanecer inalterado y completo. Las modificaciones realizadas deben ser registradas asegurando su confiabilidad.
- **Disponibilidad:** Acceso y utilización de los servicios sólo en el momento de ser solicitado por una persona autorizada.

B. OBJETIVOS

- Establecer los lineamientos y disposiciones para una adecuada identificación y clasificación de la información según su criticidad en términos de confidencialidad, integridad y disponibilidad.
- Establecer las normas para mantener y alcanzar una apropiada protección de la información de la empresa donde los colaboradores asignados deben cumplir con las políticas señaladas de clasificación.
- Garantizar la adecuada identificación y clasificación de la información.

C. ALCANCE

El presente documento es de carácter obligatorio y aplicable a la información obtenida, proporcionada y/o generada independientemente del formato en que se encuentre física o electrónica, por aquellas personas vinculadas a la Compañía, o que trabajan o prestan un servicio bajo cualquier modalidad en la Compañía, y que en el desarrollo de sus actividades puedan acceder a Información tales como:

Director de operaciones: Alta dirección designada por el Representante Legal como responsable del cumplimiento de los objetivos de la empresa.

Colaborador interno: Es aquel contratado directamente por la compañía y labora dentro de las instalaciones de la compañía.

Colaborador externo: Es aquel que presta sus servicios y labora dentro de las instalaciones de la compañía, sin embargo este no pertenece directamente a la misma, no obstante tiene las mismas responsabilidades y obligaciones en materia de seguridad de la información, debido a que cuenta con acuerdos de confidencialidad con la empresa.

Proveedor de centro de datos. Aquel que proporciona el servicio de centro de datos donde se encuentran los activos físicos que soportan el proceso critico de CFDI.

Terceros: Cualquier persona ajena a la compañía, que por alguna razón tiene un interés común en la información de la compañía.

D. MARCO DE REFERENCIA, NORMATIVA Y LEGISLACIÓN VIGENTE

- ISO/IEC 27001:2013 “Sistema de Gestión de Seguridad de la Información”.
- **MATRIZ DE CONTROL** señalada en la fracción II de la ficha 111/CFF del Anexo 1-A de la RMF.
- CFF **29**, 29-A, RMF 2018
- Ley Federal De Protección de Datos Personales en posesión de los particulares.

2. ROLES Y RESPONSABILIDADES

ROL	RESPONSABILIDAD	ACTIVIDADES
Director de Operaciones	Alta dirección designada por el Representante Legal como responsable del cumplimiento de los objetivos de la empresa.	-Autorizar la Política que dan soporte a la debida clasificación de la información.
Gerente De Procesos	Responsable de la implementación y aseguramiento de seguridad de la información en la empresa.	-Diseñar e implementar las políticas y procedimientos necesarios para la **clasificación** de la información. -Verificar el cumplimiento de la política. -Identificar canales de información. -Concientizar a los colaboradores sobre la importancia de la clasificación de la información para la adecuada operación. -Asegurar que se cumplan los controles para preservar la confidencialidad, la integridad y la disponibilidad de la información.
Cliente	Persona o entidad titular responsable de leer y aceptar los términos y condiciones de haber proporcionado información sensible a la empresa.	-Proporcionar información para ejecutar los servicios requeridos.
Responsable de la Información	Responsable de decidir sobre la clasificación de la información a la que tenga acceso y/o genere.	-Clasificar la información que genera -Conocer los tipos de clasificación de la información y las normas concernientes a estos. -Identificar todas las fuentes de información, estar consiente sobre la importancia de la clasificación de la información para su adecuado manejo.

Tercero	La persona física o moral, distinta del propietario o del responsable de la información.	-Recibir información clasificada como publica.
Proveedor de centro de datos	Responsable de recibir y dar un correcto uso al activo de información y garantizar la confidencialidad de la información que conoce, de acuerdo a sus responsabilidades y funciones.	-Conocer los tipos de clasificación de la información y las normas concernientes a él. -Responsable de proteger la información, manteniendo los controles definidos por la compañía.

3. LINEAMIENTOS

- El departamento de Procesos es el encargado de establecer los lineamientos que permitan la clasificación de la información utilizada en los procesos de la compañía.
- El departamento de Procesos deberá dar a conocer a los colaboradores de la compañía acerca de cómo se clasifica la información y la importancia que esta tiene.
- Los colaboradores deberán conocer los tipos de clasificación de la información y los lineamientos concernientes a estos.
- Los colaboradores deberán tener acceso a la información que les permita realizar su trabajo, estando comprometidos con el uso responsable de la información, siendo cada uno responsable de la clasificación de la información generada u obtenida.

4. CLASIFICACIÓN DE LA INFORMACIÓN

La presente clasificación de información es la establecida por la compañía, con el fin de preservar, asegurar y cumplir la:

- **Confidencialidad**: Los activos de información sólo pueden ser accedidos y custodiados por usuarios que tengan permisos para ello.
- **Integridad:** El contenido de los activos de información debe permanecer inalterado y completo. Las modificaciones realizadas deben ser registradas asegurando su confiabilidad.
- **Disponibilidad:** Acceso y utilización de los servicios sólo en el momento de ser solicitado por una persona autorizada.

Esta clasificación comprende:

- **Información confidencial**
- **Información reservada**
- **Información publica**

A. INFORMACIÓN CONFIDENCIAL

Es toda aquella información que de ser revelada sin autorización puede causar perjuicios importantes a la compañía o impactar negativamente a la reputación de la misma, debe ser 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.

B. INFORMACIÓN RESERVADA

Información cuya divulgación debe ser restringida únicamente al personal de la compañía que la requiera. Esta información incluye toda aquella información que requiere de cierto nivel de protección pero que no cumple con los criterios necesarios para ser clasificada como Confidencial.

C. INFORMACIÓN PÚBLICA

Información de uso general que por su contenido o contexto no requiere de protección especial, puede ser compartida sin ninguna restricción y su distribución pública ha sido permitida a través de canales autorizados por la empresa. Para esta información sólo se deben de implementar los controles adecuados para asegurar la integridad y disponibilidad de la misma.

5. AUTORIZACIÓN DE POLÍTICAS Y PROCEDIMIENTOS INTERNOS.

Con el fin de reducir el uso de papel que implica la impresión de los documentos que soportan la implementación de la matriz de controles, la compañía establece los siguientes lineamientos de autorización:

Lineamientos

- Los documentos digitalizados serán generados en formato .pdf y estos serán resguardados por el área de procesos de la compañía.
- Los documentos se autorizarán y validaran a través de **FIRMAS DIGITALES** las cuales serán asignadas por las áreas correspondientes (Área que Elabora, Revisa y Aprueba).
- Las políticas, procedimientos y calendarios que sean autorizadas a través firmas digitalizadas en formato PDF solo serán impresos para su consulta.
- La firma digital deberá ser agregada desde el formato .pdf, siendo equivalente a una firma autógrafa, esta debe contar con una contraseña la cual es de uso exclusivo del personal que genera, revisa y/o aprueba el documento.Con esto se garantiza la autoría e integridad de los mismos ya que su función homologa a la firma manuscrita en los documentos impresos.

Exclusiones

Las políticas, procedimientos, documentos, etc. que deban ser autorizados por la alta dirección deberán mantener un formato impreso y firmados autógrafamente para su autorización, el único formato digital valido de estos documentos será el scanner de los mismos.

Dicha política aporta beneficios tales como:

- La reducción de consumo de papel.
- Ahorro de espacio, materiales y recursos.
- Ahorro de tiempo, incremento de eficiencia.
- Reducción de costos.
- Mejorar la sustentabilidad ambiental.

- Los documentos digitalizados para ser autorizados requieren una contraseña que solo el encargado posee.

- Los documentos no están expuestos a manchas, agua, deterioro, cortes, rayones… u otras eventualidades que pongan en riesgo a los mismos.

Es por eso que los documentos, procedimientos, políticas, etc. relacionado a la Matriz de controles SAT se manejarán en formato digital.

6. ASPECTOS DE CLASIFICACIÓN DE LA INFORMACIÓN PARA PROVEEDORES

A. DIRECTRICES DE CLASIFICACIÓN DE INFORMACIÓN PARA TERCEROS

La compañía determina que la información para terceros es considerada como publica:

Información Pública:
Información de uso general que por su contenido o contexto no requiere de protección especial, puede ser compartida sin ninguna restricción y su distribución pública ha sido permitida a través de canales autorizados por la empresa. Para esta información sólo se deben de implementar los controles adecuados para asegurar la integridad y disponibilidad de la misma.

CRITERIOS DE CLASIFICACIÓN
Este nivel de clasificación está asignada a los activos que contengan lo siguiente:

- Manuales de usuarios
- Comunicados al público
- Publicidad
- Promociones

Puede ser divulgada a cualquier persona que la requiera.

El criterio de clasificación es único y aplica a cualquier tipo de información generada en la Compañía, adquirida o administrada en medios electrónicos, escritos, entre otros. Esta clasificación de información debe ser empleada por los colaboradores de la compañía.

Los colaboradores de la compañía tienen la responsabilidad de no revelar o comunicar información confidencial o privilegiada a terceros.

B. CLAUSULAS DE CLASIFICACIÓN DE INFORMACIÓN

- La compañía establece que toda la información manejada, generada e intercambiada con el proveedor (Centro de datos) es clasificada como confidencial, teniendo el proveedor la responsabilidad de aplicar este carácter sobre la misma.

- Se cumplirán, por parte del proveedor, los lineamientos y clasificación de la información establecidas por la compañía para su gestión de la seguridad de la información.

- Toda la información relacionada con las actividades de la compañía y el proveedor se considera confidencial. El proveedor deberán cumplir las funciones y obligaciones aplicadas a la clasificación de la información según los lineamientos establecidos por la compañía.

- La información de la compañía así como la información propietaria de los clientes de la misma es confidencial, y no debe ser accedida, usada, transferida, modificada, revelada, destruida, o desechada a menos que la compañía así lo disponga.

- Se garantizará el manejo de la información de acuerdo al criterio de clasificación establecido.

- Se prohíbe la transmisión de información de la compañía a otras organizaciones.

C. MANUAL DE CLASIFICACIÓN DE INFORMACIÓN PARA PROVEEDORES

La información acerca de la clasificación para proveedores se establece en el documento “MP-08 Manual de clasificación de información para proveedores”.

7. SANCIONES

A. MEDIDAS DISCIPLINARIAS

Se entiende por medidas disciplinarias a las medidas implementadas por la compañía para evitar la reincidencia del incumplimiento de las políticas.
El incumplimiento se documentará en el formato Registro De Incumplimiento De Políticas, donde se registrará la descripción del incumplimiento, la causa, las acciones correctivas en caso de ser necesarias y por último la penalización a la que se es acreedor el colaborador que incumplió.
Esto con el fin de tener un registro del incumplimiento a las políticas y poder mitigar las áreas de oportunidad que estas presenten.

B. SANCIONES DE ACTIVIDAD MALICIOSA NO AUTORIZADA Y/O ILEGAL.

Se entenderá por actividad maliciosa a cualquier actividad que se realice con el fin de perjudicar o causar alguna vulnerabilidad a la compañía, las cuales incluyen, mas no limitan las siguientes:

- Tomar fotografías, videos o audios con cualquier medio electrónico dentro de las instalaciones sin autorización previa.

- Compartir información sensible (número telefónico, nombre, RFC etc.) de algún cliente interno o externo, así como la información de su actividad o relación con la compañía.

Se sancionará (penal o administrativa) dependiendo el impacto hacia la compañía a aquel colaborador que realice actividades sospechosas, maliciosas, que ingrese o penetre a una red en forma ilegal o no autorizada, evadiendo los mecanismos de seguridad lo cual provoque alguna clase de impacto a la compañía o bien a terceros. Será inmediatamente dado de baja y se dará por concluida su relación laboral con la compañía.

La Dirección de la compañía colaborará de manera completa con investigaciones hacia sospechosos de actividades criminales o de violaciones a sistemas de seguridad de cómputo y redes, bajo la coordinación y dirección de las fuerzas de seguridad, de la ley o autoridades correspondientes.

C. SANCIONES DE INCUMPLIMIENTO DE LAS POLÍTICAS DE LA COMPAÑÍA.

Quién no de cumplimiento y/o viole las políticas establecidas, recibirá el siguiente tratamiento:

a) En primera Instancia se sancionará con una amonestación verbal

b) En segunda instancia se sancionará con una amonestación escrita, notificando de que su posición en la compañía está en riesgo.

c) En tercera instancia, se dará por concluido su contrato laboral. Situación que le fue notificada y aceptó al iniciar la relación laboral.

Dependiendo del incumplimiento a las políticas de seguridad de la información el colaborador podrá ser dado de baja, dando por concluida su relación con la compañía y aplicadas las sanciones administrativas o penales derivadas de dicha falta.

8. REVISIÓN DE POLÍTICA

Se revisará la política de Clasificación de la Información al menos una vez por año con la finalidad de verificar que lo establecido es aplicable y vigente, en caso de presentarse una actualización en dicha política antes del periodo señalado se realizara una nueva revisión.