POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

ÁREA	FIRMA	DEPARTAMENTO	FECHA
Elaboró Luis Alejandro Blanco Sepúlveda		Procesos	10/09/2020
Revisó Alberto Salas Acosta		Dirección de Operaciones Comerciales	10/09/2020
Aprobó José Cruz Aarón Hernández		Dirección de Operaciones	10/09/2020

TABLA DE CONTROL DE CAMBIOS

FECHA	NIVEL DE REVISIÓN	CAMBIOS
04/09/2019	15	Se actualiza el apartado 4. Compromiso de la dirección en el inciso e. Se agrega información a los puntos 5.A, 5.B y 5.K.
09/03/2020	16	Se revisa la política, se determina que no es necesario cambiar o modificar algún apartado, se mantiene aplicable y vigente.
10/09/2020	17	Revisión programada, se verifica que los controles contenidos sigan aplicables y vigentes, se actualiza el punto 3.D Roles y responsabilidades.

FEL Facturar en Línea ©CFDI
Facturar en Linea, S. de R.L. de C.V.
Privada Topacio 3506 501 Residencial Esmeralda
PROVEEDOR AUTORIZADO SAT No. 55029

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

1. INTRODUCCIÓN

Facturar en línea como Proveedor Autorizado de Comprobantes Fiscales Digitales por Internet tiene la responsabilidad de aplicar la siguiente Política de Seguridad de la Información siguiendo los objetivos que a continuación se establecen.

A. DEFINICIÓN DE SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información se entiende como 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.

2. AUTORIZACIÓN DE POLÍTICAS

Las políticas y procedimientos implementados por la compañía para dar cumplimiento a la matriz de controles del SAT serán revisados por la **Dirección de Operaciones Comerciales** y autorizados por la **Dirección de Operaciones** ya que es la Dirección de Operaciones la **responsable del cumplimiento de los objetivos de la empresa**.

3. OBJETIVO

Este documento define las políticas y lineamientos específicos de seguridad de la información de la empresa, los cuales son de observancia general y obligatoria para todos sus colaboradores, cualquiera sea su calidad contractual, con el fin de preservar:

- Su confidencialidad, asegurando que sólo personal autorizado puede acceder a la información.
- Su integridad, asegurando que la información y sus métodos de proceso son exactos y completos.
- Su disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando sea requerido.

A. OBJETIVOS ESPECÍFICOS

- Establecer lineamientos de comportamiento en los colaboradores.
- Generar un cambio en la cultura de trabajo del personal.
- Generar conciencia en los colaboradores hacia sus procedimientos de trabajo.
- Crear una base que deberá ser detallada y evaluada continuamente por la Dirección de la compañía.
- Mantener la integridad y confidencialidad de la información.

E. ACTUALIZACIONES Y/O REVISIONES

La presente política cambiará en respuesta a las necesidades de la compañía, del negocio y a las nuevas tecnologías. Por lo tanto, debe revisarse al menos 2 veces al año para verificar que lo establecido es aplicable y vigente.

4. COMPROMISO DE LA DIRECCIÓN

La Alta Dirección de Facturar en línea S.A. de C.V. expresa su compromiso activo con la Seguridad de la Información dentro de la compañía, con la finalidad de afianzar los objetivos establecidos en este tema y asegurar que las políticas y procedimientos son compatibles con la dirección estratégica.

La Política de Seguridad de la Información no solo es comunicada y entendida también aplicada, promoviendo el conocimiento del enfoque de los procesos y la mejora continua, cumpliendo así con los lineamientos establecidos para los Proveedores Certificados de Comprobantes Fiscales Digitales por Internet (PCCFDI) título emitido por el Servicio de Administración Tributaria (SAT).

La Alta Dirección establece, revisa y mejora la Política de la Seguridad de la información, en la cual se fundamenta el cumplimiento de los lineamientos establecidos por la autoridad.

Da cumplimiento a todas las regulaciones, leyes y normativas vigentes relacionadas con Seguridad de la Información

Asigna razonablemente los recursos requeridos para la concepción, implementación, mantenimiento y mejora de la Matriz de Controles SAT.

Para ello, la dirección de Facturar en línea lleva a cabo las siguientes acciones concretas:

a) La empresa cuenta con una Política de Seguridad de la Información actualizada la cual es comunicada, entendida y aplicada, se encuentra disponible para personal interno y terceros que colaboren en la misma.

b) Cuenta con dos departamentos (Proceso, Infraestructura) los cuales están especializados en el cumplimiento de los lineamientos en materia de seguridad de la información.

c) Dentro de la empresa se imparten talleres de concientización de la Política de Seguridad de la Información a todos sus colaboradores como lo muestra el calendario de talleres 2019 impartido por el área de capacitación y servicio al cliente de la empresa.

d) La compañía cuenta con contratos de confidencialidad firmados por el personal interno, los cuales se revisan al menos dos veces al año.

e) La compañía lleva a cabo un riguroso proceso de reclutamiento y selección del personal, en el cual se incluyen la carta de antecedentes no penales, estudio socio económico y convenio de confidencialidad considerando la información sensible que se maneja.

f) La empresa cuenta con políticas y procedimientos formales para la clasificación de la información de acuerdo a su relevancia y sensibilidad, en cumplimiento a las disposiciones del INAI (antes IFAI).

g) La compañía cuenta con la Matriz de análisis de riesgos la cual identifica y evalúa las amenazas y vulnerabilidades que afectan al proceso critico de CFDI, la aplicación representa un valioso resultado que permitirá a los niveles superiores lograr una toma de decisiones para mitigar o reducir los riesgos existentes.

h) Se cuenta con el Plan de Continuidad de Negocios, este es la política que la compañía implementa, para responder organizadamente a eventos que interrumpen la operación normal de sus procesos y que pueden generar impactos sensibles en el logro de los objetivos.

- Los colaboradores deberán estar plenamente conscientes de sus obligaciones laborales y legales, las cuales se especifican en el **Contrato de Trabajo y El Contrato de Confidencialidad**. Éstos se deberán dar a conocer a todos los colaboradores al inicio de la relación laboral.

Control aplicado: 02 revisión de política de seguridad de la información.

C. POLÍTICA DE USO DE INTERNET

Se clasificará la información como reservada o confidencial aquella que pase sobre redes públicas como Internet, se controlará el uso de Internet tomando en cuenta el flujo de datos, el monitoreo de la información transmitida por este medio y las implicaciones legales aplicables. Todos los equipos de cómputo se encontrarán registrados en un directorio activo que permite al área de Redes y Comunicaciones realizar el monitoreo de todos los equipos.

D. POLÍTICA DE USO DEL CORREO ELECTRÓNICO

El uso del correo electrónico proporcionado por la compañía estará permitido estrictamente para fines laborales, toda la información transmitida por este medio será controlada, evitando exposición no autorizada de información reservada y/o confidencial.

E. CLASIFICACIÓN, ETIQUETADO Y MANEJO DE LA INFORMACIÓN

La información se clasificará con un nivel de protección apropiado, definido y se encontrará identificada de acuerdo con sus necesidades, prioridades y grado esperado de protección.

Toda información proporcionada por el Servicio de Administración Tributaria (SAT) se clasificará con el más alto nivel de confidencialidad.
Los activos de información estarán identificados y tienen un propietario designado, responsable de proteger la seguridad de información del mismo, a su vez se encontrarán etiquetados, generando el inventario de los activos.

Control aplicado: 08 Clasificación de la Información y 09 Etiquetado y Manejo de la Información.

F. SELECCIÓN Y CAPACITACIÓN DEL PERSONAL

El personal que labora en la compañía pasará por un proceso de selección y capacitación en materia de seguridad de la información en el área de Recursos Humanos, previo a su contratación, durante el tiempo de la relación laboral, y hasta que deje de laborar en la compañía o cambie de puesto dentro de la misma.

Control aplicado: 10 Selección del Personal y 12 Capacitación del personal en materia de Seguridad de la Información.

G. RESPONSABILIDADES DEL PROVEEDOR DE CENTRO DE DATOS

Las responsabilidades del centro de datos para asegurar la Confidencialidad, Integridad y Disponibilidad de la información ubicada en centro de datos se encuentran descritos en los contratos suscritos con el mismo centro de datos (KIO Networks) así como en sus anexos. Entre los aspectos contractuales de seguridad de la información más relevantes podemos encontrar:

- Cláusula de confidencialidad la cual especifica las responsabilidades del centro de datos para con la información de la compañía, dicha cláusula especifica que la información generada, almacenada, transmitida y procesada en dicha infraestructura es propiedad de la empresa en todo momento y que el proveedor no tiene acceso a dicha información.

J. DEVOLUCIÓN DE ACTIVOS

Cuando la relación laboral con el colaborador se da por terminada o se cambie el activo que tiene asignado, se resguardarán y revisarán los activos tangibles e intangibles con los que desempeñaba sus funciones.

Control aplicado: 19 Devolución de activos

K. USO ACEPTABLE DE LOS ACTIVOS

El uso de equipos de cómputo y la asignación de privilegios o derechos de acceso a los mismos estará controlado con base en los requerimientos de seguridad establecidos, manteniendo la confidencialidad, integridad y disponibilidad- de la información procesada, transmitida y/o almacenada en dichos equipos. Para la asignación de cuentas y claves de acceso se analizará el perfil del colaborador para determinar el alcance de las mismas.

PROTECCIÓN DE REDES
Se controlará el acceso de los usuarios a los servicios de red interna y externa para garantizar la seguridad de los servicios.

PROTECCIÓN DE EQUIPOS DE CÓMPUTO
Los mecanismos de procesamiento de información, aplicaciones y sistemas de información restringirán el acceso a los sistemas operativos únicamente para usuarios autorizados.

Control aplicado: 23 Uso aceptable de los activos.

L. CONTROL DE ACCESO A LAS INSTALACIONES Y SEGURIDAD FÍSICA

Cualquier acceso a las instalaciones, mecanismos de procesamiento de información, comunicaciones y/o información de la compañía realizado por terceros, está debidamente controlado.

De acuerdo con los riesgos identificados, se proporcionará la protección física pertinente para evitar accesos no autorizados, daño, destrucción o interferencia a información de seguridad.

El área legal de la compañía verificará la implementación, y monitorea el cumplimiento, de los contratos de prestación de servicios de tecnología de información y comunicaciones celebrados con terceros, administrará cambios a dichos contratos a fin de garantizar que los servicios entregados reúnan y cumplan todos los requerimientos acordados en el mismo.

Control aplicado: 24 Perímetro de seguridad física y 25 Controles de entrada.

6. POLÍTICAS DE SEGURIDAD A NIVEL TECNOLÓGICO

A. ANÁLISIS DE RIESGOS

Para la ejecución del análisis de riesgos el departamento de Operaciones participará activamente, y contará con el apoyo de la Dirección General a fin de prevenir las debilidades de los controles, minimizar el riesgo y reducir el impacto de los riesgos y amenazas.

Control aplicado: 26 Análisis de Riesgos.

G. CONTROL DE ACCESOS

El área de operaciones permitirá controlar el ingreso a la Información, al centro de datos, así como a los ambientes de desarrollo y pruebas, así como administrar el ciclo de vida de los usuarios, desde la creación de las cuentas, roles y permisos necesarios hasta su eliminación.

Control implementado: 44 Política de Control de Accesos.

H. GESTIÓN DE CUENTAS Y PRIVILEGIOS

GESTIÓN DE CUENTAS

Se garantizará la disponibilidad de información a los usuarios que realmente la necesitan, se llevará un control de las actividades que debe realizar cada persona y actualizar la lista de permisos de cada usuario. Este procedimiento permitirá conocer los accesos activos que posee un usuario y si corresponde al rol otorgado.

GESTIÓN DE PRIVILEGIOS

Se gestionará de forma correcta los privilegios en las cuentas, para asegurar el acceso y control a los activos del proceso de CFDI. Ya que cada usuario hace diferentes funciones solo necesitará los privilegios para realizar dichas actividades. En este documento se definirá la forma en que se asignan los privilegios usando el rol de una cuenta de usuario en un activo específico.

Control implementado: 45 Altas, Bajas y Cambios de accesos de usuarios y 46 Gestión de Privilegios.

I. ACTUALIZACIONES EN EQUIPOS

La compañía contará con las últimas actualizaciones de componentes de software ya que se solucionan posibles brechas de seguridad, se incrementa el rendimiento, se solucionan errores y demás mejoras. Sin embargo, la compañía controlará la instalación de actualizaciones ya que también pueden tener un impacto significativo en el rendimiento o en el mismo funcionamiento de los equipos.

Control implementado: 62 Actualizaciones.

J. RESPALDO Y ELIMINACIÓN DE INFORMACIÓN

La información clasificada como confidencial y/o de uso interno, se respaldará en medios magnéticos.
Se contarán con procedimientos para proteger los documentos, medios de cómputo (cintas, discos, etc.), datos de entrada/salida y documentación de sistemas para evitar exposiciones no autorizadas, modificación, eliminación y/o destrucción de información.

Control implementado: 63 Respaldos y 67 Destrucción y Borrado.

K. USO DE BITÁCORAS DE LOS SISTEMAS/APLICACIONES

Los sistemas/aplicaciones de la compañía serán monitoreados y los eventos de seguridad de información registrados en bitácoras para detectar actividades no autorizadas y garantizar que los problemas de los sistemas/aplicaciones sean identificados.
El proveedor de centro de datos almacenará el respaldo completo de las bitácoras. En caso de que la compañía requiera las bitácoras, se solicitarán directamente al Centro de Datos.

Control implementado: 80 Bitácoras.