POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

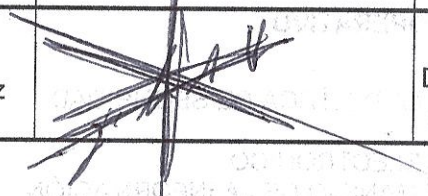
ÁREA	FIRMA	DEPARTAMENTO	FECHA
Elaboró Luis Alejandro Blanco Sepúlveda		Procesos	25/01/2022
Revisó Alberto Salas Acosta		Dirección de Operaciones Comerciales	25/01/2022
Aprobó José Cruz Aarón Hernández		Dirección de Operaciones	25/01/2022

TABLA DE CONTROL DE CAMBIOS

FECHA	NIVEL DE REVISIÓN	CAMBIOS
11/03/2021	18	Revisión programada, no se efectúan cambios ya que su contenido es aplicable y vigente.
08/09/2021	19	Actualización del punto 5.I Equipo desatendido, escritorio limpio y pantalla despejada.
25/01/2022	20	Revisión programada, no se efectúan cambios ya que su contenido es aplicable y vigente.

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

ÍNDICE

1. INTRODUCCIÓN

Servicios Tecnológicos Avanzados en Facturación 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.

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.

B. ALCANCE

La presente política será conocida y cumplida por el personal de la compañía, interno o externo que interactúe con el proceso critico de CFDI, entendiéndose como proceso critico lo relacionado a la emisión y generación de CFDI de acuerdo a lo establecido en el anexo 20.

C. 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 2019
- Ley Federal De Protección de Datos Personales en posesión de los particulares.

D. ROLES Y RESPONSABILIDADES

FIGURA	RESPONSABILIDAD	ACTIVIDADES
Representante Legal	Responsable de la asignación de recursos financieros y legales para el cumplimiento de los objetivos de la Política de Seguridad de la información	Asignar los recursos necesarios para el cumplimiento de los objetivos establecidos en temas de seguridad de la información.
Director de Operaciones	Responsable del cumplimiento de los objetivos operativos y de seguridad de la información de la empresa.	Asegurar el funcionamiento de los sistemas que dan soporte al proceso de CFDI, así como asegurarse que las tareas que soportan la seguridad de la información se lleven a cabo.
Director de Operaciones Comerciales	Responsable del cumplimiento de los objetivos operativos que soportan el proceso interno, así como los procesos de seguridad relacionados a la oficina comercial.	Asegurar el funcionamiento de los sistemas que soportan el proceso comercial y los procesos internos relacionados a la seguridad de la información.
Encargado de Procesos	Responsable de la implementación y aseguramiento de seguridad de la información de la empresa.	Elaboración de políticas y procedimientos que dan cumplimiento a la Matriz SAT. Implementar los controles de la Matriz del SAT.
Encargado de Recursos Humanos	Responsable de la ejecución de los procesos de contratación y baja de acuerdo a lo establecido por la matriz de controles	Asegurar el cumplimiento de los procedimientos relacionados a la selección y baja del personal.
Supervisor de infraestructura y redes	Responsable de monitorear los activos del proceso de CFDI. Responsable de estado de los activos físicos dentro de la compañía.	Monitorear los sistemas que dan soporte al proceso de CFDI. Garantizar la seguridad de los equipos de cómputo, así como el manejo e inventariado de los activos de la compañía.
Encargado del Departamento Jurídico	Responsable de aspectos jurídicos de la empresa.	Elaboración de contratos de confidencialidad y la revisión de documentos fiscales.

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 Servicios Tecnológicos Avanzados en Facturación 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 Servicios Tecnológicos Avanzados en Facturación S.A. de C.V. 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 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 crítico 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.

i) La compañía diseña, prueba e implementa los procesos y procedimientos necesarios para dar cumplimiento cabalmente a cada uno de los 86 controles tecnológicos establecidos en la matriz de controles tecnológicos para PCCFDI.

5. POLÍTICAS DE SEGURIDAD A NIVEL OPERATIVO

Se cuenta con una matriz de controles tecnológicos que da cumplimento a los requerimientos por La Secretaría De Administración Tributaria (SAT) la cual otorga la certificación como PCCFDI Proveedor Certificado De Comprobantes Digitales Por Internet, dicha matriz da soporte a la presente política ya que dentro de los 86 controles implementados se pueden mencionar algunos de los descritos a continuación.

A. POLÍTICA DE SEGURIDAD

Se cuenta con una política de seguridad de información documentada que establece la dirección a seguir en materia de seguridad de la información.

La compañía 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 vigentes.

Lineamientos:

- Las políticas de seguridad de la información se revisarán al menos dos veces al año, para asegurar que se cumplan los propósitos de la compañía.
- Las políticas de seguridad de la información permanecerán disponibles para consulta de todos los colaboradores que requieran acceso a información de la compañía. De acuerdo con las restricciones de seguridad del puesto de cada colaborador, la información de la compañía puede ser utilizada para consulta, procesamiento, almacenamiento y/o transmisión.
- Todos los colaboradores de la compañía están obligados a conocer, observar, cumplir y mantenerse actualizado sobre estas políticas de seguridad de la información.
- Se realizarán talleres de concientización con el todo el personal, con el fin de mantener una cultura de seguridad bien definida y actualizada.

Control aplicado: 01 Política de seguridad de la información.

B. POLÍTICA DE CUMPLIMENTO DE LA POLÍTICA DE SEGURIDAD

Se verificará cada seis meses que todos los involucrados conocen sus responsabilidades de seguridad de información y cumplen todas y cada una de ellas, garantizando la satisfacción de los requisitos de seguridad establecidos, para esto se realizará una plática donde se darán a conocer los cambios o actualizaciones a la presente política.

Lineamientos:

- La compañía conoce y acepta sus responsabilidades de seguridad de la información y cumplirá con las metas de seguridad. Se generarán, revisarán, aprobarán, e implementarán las políticas de seguridad de la información. La compañía proporcionará los recursos necesarios, e iniciará planes y programas para mantener los conocimientos de seguridad de la información actualizados.
- Todos los colaboradores deberán conocer sus responsabilidades con respecto al uso que le den a los sistemas de información, a los equipos de cómputo y la información que manejan.

- 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.

- Cláusula de Auditoria, esta especifica que se podrán hacer auditorías al centro de datos para verificar el cumplimiento de los controles físicos y administrativos implementados en materia de seguridad de la información.

Cabe mencionar que se cuentan con más responsabilidades las cuales pueden ser identificadas dentro de los contratos antes mencionados.

Control aplicado: 04 Acuerdos de Confidencialidad y/o no divulgación
Adicional a eso se tienen implementados diferentes lineamientos los cuales incluyen mas no limitan los siguientes:

- El centro de datos cuenta con controles físicos y ambientales que permiten asegurar la disponibilidad, integridad y confidencialidad de los activos que soportan el proceso de CFDI como son:
    - Control de accesos
    - Medidas contra incendios
    - Aire acondicionado
    - Medidas contra inundaciones
    - Redundancia en la alimentación eléctrica, Etc.

Control aplicado: Del control 50 al 57

- Solo el personal autorizado tiene acceso a los activos ubicados en el centro de datos y estos permisos son revisados periódicamente.

Control aplicado: 44 Política de Control de Accesos, 48 Revisión de Permisos

- Se cuentan con protocolos de comunicación en caso de incidentes establecidos a nivel contractual con el cual se define de manera formal el cómo actúa el centro de datos en caso de un incidente de seguridad.

Control aplicado: 29 Protocolos de comunicación en caso de incidentes

H. USO DE CONTRASEÑAS

Los usuarios de sistemas, aplicaciones y equipos de cómputo estarán conscientes de la importancia de mantener la seguridad de información y de la responsabilidad que tienen con respecto a mantener controles de acceso efectivos, en particular el buen manejo y uso que le deben dar a sus contraseñas.

Control aplicado: 15 Uso de contraseñas

I. EQUIPO DESATENDIDO, ESCRITORIO LIMPIO Y PANTALLA DESPEJADA

Los colaboradores que dejen su lugar de trabajo deberán bloquear su equipo, adicionalmente todos los equipos de cómputo de la compañía están configurados por el directorio activo para que se bloqueen en 3 min por inactividad.

El lugar de trabajo debe mantenerse ordenado y limpio en todo momento, así mismo debe mantenerse ordenada la pantalla de cada equipo de cómputo, es decir sin documento de cualquier tipo en el escritorio de la pantalla, para asegurar este principio se realizarán inspecciones aleatorias a los colaboradores d ela compañía.

Debido a que las **condiciones sanitarias de salud no permiten la asistencia presencial en las instalaciones, no se podrá llevar a cabo dicha inspección por el área de procesos,** por la cual la evidencia del escritorio limpio y pantalla despejada **serán tomas por los mismos usuarios**

Control aplicado: 16 Equipo desatendido y 17 Escritorio limpio y pantalla despejada

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.

B. ADMINISTRACIÓN DE INCIDENTES Y PROBLEMAS DE SEGURIDAD DE LA INFORMACIÓN

Los empleados, contratistas y terceros que laboren o presten servicio para la compañía reportarán cualquier evento, debilidad o incidente de seguridad de información que detecten a la brevedad posible por medio de los canales establecidos para tal efecto.

Control aplicado: 28 Incidentes y Problemas

C. ADMINISTRACIÓN Y MONITOREO DE EVENTOS DE SEGURIDAD

La administración de la bitácora de eventos de seguridad permitirá reaccionar ante un incidente de seguridad, el objetivo de este procedimiento es describir el proceso para tener disponibles las bitácoras de eventos de seguridad requeridas para el monitoreo de eventos de seguridad. Además de la definición de pasos para respaldar dichos archivos.

Control aplicado: 31 Definición y registro de Eventos de Seguridad y 33 Monitoreo activo de Seguridad.

D. PLAN Y PRUEBAS DE CONTINUIDAD DE NEGOCIO

La compañía contará con un proceso de continuidad de negocio el cual será puesto en marcha en caso de desastres naturales, accidentes, fallas de equipos o acciones deliberadas, minimizando el impacto en la compañía y acelerando la recuperación de una pérdida de activos e información a un nivel aceptable.

A través de una serie de controles preventivos, de recuperación y pruebas previas de los procesos críticos de la compañía, se garantizará la preservación de la compañía aún en un caso de desastre.

Control aplicado: 38 Plan de Continuidad del Negocio y 39 Pruebas de BCP.

E. GESTIÓN DE CAPACIDAD TECNOLÓGICA Y OPERATIVA

La Gestión de la Capacidad Tecnológica es la encargada de que todos los servicios TI se vean respaldados por una capacidad de proceso, almacenamiento y comunicación debidamente dimensionada.

Se Identificará la capacidad tecnológica y operativa actual, así como la infraestructura utilizada en los procesos críticos de generación del CFDI garantiza su óptima funcionalidad mediante el proceso de análisis y monitoreo.

Control aplicado: 40 Capacidad Tecnológica y 41 Capacidad Operativa

F. PLAN DE RECUPERACIÓN DE DESASTRES

Un Plan de recuperación de desastres (Disaster Recovery Plan) por sus siglas DRP es la estrategia que se seguirá para restablecer el proceso de CFDI (Hardware y Software) después de haber sufrido una afectación por una catástrofe natural, epidemiológica, falla masiva, daño premeditado, ataque de cualquier tipo el cual atente contra la continuidad del negocio.

La intención es la de restaurar operaciones tan rápidamente como sea posible con los datos últimos y más actualizados disponibles.

Control implementado: 42 Plan de Recuperación de Desastres DRP

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

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 acepto 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.