CONSERFLOW S.A. DE C.V.
Calle Mezquite N° 5.
Col. Santa Clara C.P. 75820
Santiago Miahuatlán, Puebla.
RFC: **CON1912026U2**

POLITICA DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de la Información de CONSERFLOW tiene la finalidad de garantizar la confidencialidad, integridad y disponibilidad de nuestros activos de información. Esta política establece las directrices y responsabilidad para proteger la información, los equipos y los servicios tecnológicos que respaldan nuestros procesos.

En la actualidad, las tecnologías de la información se enfrentan a un creciente número de amenazas, lo cual requiere de un esfuerzo constante por adaptarse y gestionar los riesgos introducidos por estas.

OBJETIVO

Preservar la confidencialidad, integridad y disponibilidad de la información y los recursos tecnológicos de CONSERFLOW

ALCANCE

Esta política es aplicable a todos los empleados, contratistas, proveedores y clientes que interactúan con los recursos de información de CONSERFLOW. El alcance de la presente política abarca toda la información de CONSERFLOW con independencia de la forma en la que se procese, quien acceda a ella, el medio que la contenga o el lugar en el que se encuentre, ya se trate de información impresa o almacenada electrónicamente.

a) Ley Federal de Protección de Datos Personales de los Particulares.

La Política de Seguridad de la Información deberá estar disponible en nuestro sistema ERP y será entregada en la plática de inducción a todo el personal, de forma que sea accesible para todas las personas de CONSERFLOW.

INTRODUCCIÓN

La presente Política de Seguridad de la Información responde a las recomendaciones del Estándar Internacional ISO/IEC 27001, así como el cumplimiento de la legislación vigente en materia de protección de datos personales y de las normativas que, en el ámbito de la Seguridad de la Información, puedan afectar a CONSERFLOW. Se establecen los siguientes principios como directrices que han de tenerse presentes en cualquier actividad relacionada con el tratamiento de la información:

- **Alcance estratégico:** La política debe contar con el compromiso y apoyo de todos los niveles directivos de CONSERFLOW. Debe coordinarse e integrarse con otras iniciativas para formar un marco de trabajo coherente y eficaz.
- **Seguridad Integral:** La seguridad debe considerarse parte de las operaciones habituales en todo el ciclo de vida, desde el diseño hasta el mantenimiento de los sistemas de información. Debe estar presente en todas las etapas, incluyendo diseño, desarrollo, fabricación y comercialización.
- **Gestión de Riesgos:** El análisis y gestión de riesgos son esenciales. Controlar y minimizar los riesgos hasta niveles aceptables garantizara un entorno seguro.
- **Proporcionalidad:** Las medidas de protección, detección y recuperación deben ser proporcionales a los riesgos potenciales y al valor crítico de la información.
- **Mejora Continua:** Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adaptarse a la evolución constante de los riesgos y sistemas de protección.
- **Auditoria y Revisión:** La seguridad de la información será atendida, revisada y auditada por personal cualificado.
- **Integración en todos los niveles:** Las funciones de seguridad de la información deben estar integradas en todos los niveles jerárquicos del personal de CONSERFLOW. Todos los empleados deben conocer, comprender y asumir su responsabilidad en la seguridad.

1. COMPROMISO DE LA DIRECCIÓN

La dirección estratégica de CONSERFLOW, consciente de la importancia de la seguridad de la información para llevar a cabo el cumplimiento del objetivo, se compromete a:

a) Promover en la organización las funciones y responsabilidades en el ámbito de seguridad de la información.
b) Facilitar los recursos adecuados para alcanzar los objetivos de seguridad de la información.
c) Impulsar la divulgación y la concientización de la Política de Seguridad de la Información entre los empleados de Conserflow.
d) Exigir el cumplimiento de la Política y de los requisitos de los reguladores en el ámbito de la seguridad de la información.
e) Considerar los riesgos de seguridad de la información en la toma de decisiones.

2. FORMACIÓN Y CONCIENTIZACIÓN

CONSERFLOW deberá asegurar que todo el personal recibe un nivel de formación y concientización adecuado en materia de Seguridad de la Información en los plazos que exija la normativa, especialmente en materia de confidencialidad y prevención de fugas de información.
Así mismo los colaboradores deberán ser informados de las actualizaciones de las políticas y procedimientos de seguridad en los que se vean afectados y de las amenazas existentes, de manera que se garantice el cumplimiento de la política.

Por otro lado, todos tienen la obligación de trabajar con diligencia con respecto a la información, debiéndose asegurar que dicha información no caiga en poder de empleados o terceros no autorizados.

3. ORDEN Y LIMPIEZA EN EL TRABAJO

Se establece los siguientes requisitos con el objetivo de mantener la seguridad en los lugares de trabajo:

- Se deberá bloquear la sesión de los equipos cuando el empleado deje el puesto, tanto por medios manuales (bloqueo por parte del usuario) como de forma automatizada mediante la configuración del bloqueo de pantalla.
- Se deberá dejar recogido el entorno de trabajo al finalizar la jornada. Incluye la necesidad de que todo documento o soporte de información quede fuera de la vista, los que por su clasificación sean confidenciales o privados.
- Se deberá mantener ordenados el lugar de trabajo y despejados de documentos o soportes de información que puedan ser vistos o accesibles por otras personas.

4. GESTIÓN DE EQUIPOS INFORMATIVOS

Se deberá tener identificados e inventariados los equipos informáticos necesarios para la prestación de los procesos de CONSERFLOW. Adicionalmente, se deberá mantener actualizado el inventario de los mismos.
Se deberá realizar la clasificación de los equipos en función del tipo de información que se vaya a tratar, de acuerdo con lo dispuesto en el apartado.
Se asignará a un responsable de Tecnologías de la Información para realizar la gestión propia de los equipos informáticos durante todo el ciclo de vida. El Responsable de T.I. deberá mantener un registro formal de los usuarios con acceso autorizado a dicho equipo informático mediante el formato *PTI-01/F-01 Matriz de requisitos de equipos de tecnologías de la información por puesto.*

5. GESTIÓN DE DISPOSITIVOS PERSONALES

En CONSERFLOW se permite a los empleados utilizar sus recursos o dispositivos móviles personales para acceder a recursos o información de la propia empresa.

Adicionalmente, los usuarios deberán tener en cuenta los siguientes requisitos establecidos:

- Se aplicarán las mismas medidas y configuraciones de seguridad a los dispositivos personales que traten información igual que al resto de dispositivos de CONSERFLOW.
- Los usuarios deberán mantener actualizado su dispositivo personal donde traten información de cualquier tipo de CONSERFLOW.
- Los empleados deberán recibir autorización de su responsable de área para utilizar su dispositivo personal.
- Cualquier incidencia que pueda afectar la confidencialidad, integridad o disponibilidad de estos dispositivos deberá ser reportada al Responsable de TI. y Recursos Humanos
- Para asegurar una gestión eficiente y segura de la información a través de aplicaciones de mensajería como WhatsApp y Telegram, se deberá adicionar como administradores de estos grupos a personal que cuente con una línea corporativa de CONSERFLOW

6. GESTIÓN DE RESPALDOS DE INFORMACIÓN

Se deberán realizar respaldos de información, del sistema, para ello se deberán realizar copias de seguridad de aplicaciones, bases de datos, correos, drive de acuerdo a como el área de Tecnologías de la Información lo determine, salvo que el responsable de un área lo solicite. En su caso, se podrá establecer una frecuencia alta de respaldos de información a los equipos correspondientes a su área, si es de impacto alto para CONSERFLOW o de elevado nivel de transaccionalidad.

Como de manera general, la frecuencia con la que se realizan los respaldos de información se determina en función de la sensibilidad de las aplicaciones o datos de acuerdo con los criterios de clasificación de información. Esta quedará plasmada en el formato *PT-01/F-01 Matriz de requisitos de equipos de tecnologías de la información por puesto.*

CLASIFICACIÓN DE LA INFORMACIÓN

A) TIPOS DE INFORMACIÓN:

CONSERFLOW clasifica la información en función del soporte en el que está siendo utilizado:

- **Soporte Digital:** Información que esté siendo utilizada mediante correo electrónico, drive o sistemas de información desarrollados a medida o adquiridos a un tercero, así como la información contenida en USB, Discos duros o dispositivos externos.
- **Soporte Físico:** Información que esté en papel.

B) NIVEL DE CLASIFICACIÓN:

En función de la sensibilidad de la información, en CONSERFLOW se cataloga la información en cinco niveles

- **Uso público:** Se trata de información que puede ser conocida por cualquier tipo de persona y su utilización no supone un riesgo para los intereses de CONSERFLOW
- **Difusión limitada:** Es la información utilizada por las áreas de CONSERFLOW y cuya utilización fraudulenta supone un riesgo para los intereses, poco significativo.

- **Información confidencial:** Es aquella información que solo puede ser conocida por un número reducido de personas y para la que un uso fraudulento puede suponer un impacto para los intereses de CONSERFLOW, significativo.
- **Información reservada:** Es la información que únicamente debe conocer el propietario de la misma y cuya divulgación puede suponer graves perjuicios para los intereses de CONSERFLOW
- **Información privada:** Es aquella cuya revelación no autorizada puede causar un perjuicio excepcionalmente grave a los intereses esenciales de CONSERFLOW.

7. PREVENCIÓN DE FUGAS DE INFORMACIÓN:

La fuga de información es una salida no controlada de información (intencionada o no intencionada) que provoca que la misma llegue a personas no autorizadas o que su propietario pierda el control sobre el acceso a la misma por parte de terceros.
Se deberán analizar los posibles procesos donde exista fuga de información, en función de las condiciones y operaciones de trabajo de CONSERFLOW. Para ello, se deberán identificar las áreas cuya fuga supone mayor riesgo para cada proceso, basándose en la criticidad y el nivel de clasificación de la información que contenga. Además, se deberán identificar las posibles vías de robo, perdida o fuga en sus diferentes estados del ciclo de vida.

Se deberá asegurar la formación y capacitación de todos los empleados en torno a buenas prácticas para la prevención de fugas de información. Especialmente se deberán tener en cuenta, al menos los siguientes aspectos:

- Proceso para el manejo de dispositivos de alta criticidad.
- Uso de dispositivos extraíbles como USB´s, CD/DVD´s, discos duros o similares.
- Uso del correo electrónico.
- Comunicación efectiva en el trabajo.
- Impresión de Documentación.
- Salida de Documentación.
- Uso de Dispositivos Móviles.
- Uso de Internet
- Orden y Limpieza en el Trabajo.
- Manejo Adecuado de las Herramientas de Respaldo y Protección de Datos.

8. AUDITORIAS DE GESTIÓN DE INFORMACIÓN

La identificación, gestión y corrección de las vulnerabilidades se llevará a cabo siguiendo un enfoque basado en riesgos, considerando la criticidad y exposición de la información. En Conserflow, esto se determinará de acuerdo con el formato PTI-01/F-01 Matriz de requisitos de equipos de tecnologías de la información por puesto, el cual será de apoyo para determinar la periodicidad de cuando realizar una revisión de los sistemas de información y aplicaciones utilizadas en la organización

9. SANCIONES DISCIPLINARIAS

Cualquier violación de la presente Política de Seguridad de la Información puede resultar en la toma de acciones disciplinarias, conforme al proceso interno de CONSERFLOW. Es responsabilidad de todos los empleados de CONSERFLOW notificar al área de Tecnologías de la Información de cualquier evento o situación que pudiera suponer el incumplimiento del alguna de las directrices definidas por la presente Política.

10. REVISIÓN Y SEGUIMIENTO

La aprobación implica que su implementación contará con el apoyo de la Alta Dirección para lograr el objetivo establecido, como también cumplir con los requisitos necesarios.

La presente información, será revisada y aprobada anualmente por toda la Dirección Estratégica. No obstante, si tuviera lugar cambios relevantes o se identificarán cambios significativos en el entorno de amenazas y riesgos, ya sean estos de tipo operativo, legal, regulatorio o contractual se procederá a su revisión siempre que se considere necesario, asegurando que la política permanezca adoptada en todo momento a la realidad de CONSERFLOW

Una vez recibida y comprendida la presente política, es responsabilidad del personal el cumplimiento de la misma.

Laura D. Flores Lozano
Director Administrativo
CONSERFLOW