INTRODUCCIÓN

La dirección de Adrián Mercado Subastas entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en concordancia con la misión y visión de nuestra empresa.

Para nuestra empresa, la protección de la información gestionada busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con el propósito de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de dicha información, acorde con las necesidades de los diferentes grupos de interés identificados.

La protección de la información es fundamental para salvaguardar los intereses de la compañía y de sus clientes en el ámbito físico como en el digital, en pro de prevenir impactos que afecten o generen pérdidas a la organización y partes interesadas.

PRINCIPIOS

Los objetivos de la presente política están orientados a salvaguardar los activos de información en el entorno físico, de red local y los que se encuentran interconectados a través de internet.

Siendo los mismos:

- Asegurar la Confidencialidad, Integridad y Disponibilidad de los activos de información a través de la ejecución de políticas, gestión de riesgo y aseguramiento informático de plataformas IT.
- Fortalecer la cultura de seguridad de la información.
- Garantizar la continuidad del negocio frente a incidentes.
- Definir e implementar controles informáticos para mitigar ataques cibernéticos conocidos, a los que se encuentran expuestas las aplicaciones y plataformas IT de la organización.
- Gestionar las vulnerabilidades técnicas y tratar el riesgo asociado a través de los análisis de vulnerabilidades sobre las plataformas IT.
- Protección de la información creada, procesada, transmitida o resguardada para nuestros procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta,

aplicando controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

RESPONSABILIDADES

Las responsabilidades en la organización, frente a la seguridad de la información y la ciberseguridad se encuentra jerárquicamente establecidas así:

1. Alta dirección: (Sr. Mauro Sosa)
   - Revisa y aprueba de forma periódica la eficacia y aplicabilidad de la/s política/s de acuerdo con la dinámica del negocio.
2. RSI: (Coordinación en Soporte IT y Programación) (Sr. Ricardo Chantada)
   - Diseña y gestiona la/s política/s de Seguridad y las políticas relacionadas
   - Revisa y evalúa la aplicación de procedimientos de seguridad de la información y controles de ciberseguridad para asegurar la adecuada ejecución de las políticas relacionadas.
3. Soporte IT y Programación Jr. (Sr. Diego Ranieri).
   - Verifica el cumplimiento de las políticas de seguridad relacionadas con la infraestructura de Redes.
4. Programador Semi Sr. (Sr. Luciano Giménez Ausfet)
   - Verifica el cumplimiento de las políticas de Desarrollo Seguro.

POLÍTICAS RELACIONADAS

Esta política se encuentra soportada sobre diferentes políticas, las cuales se encuentran relacionadas y tienen como propósito reglamentar el cumplimiento de los lineamientos de la política integral de Seguridad de la Información.
Las mismas guían el adecuado tratamiento de la información a los fines de garantizar los principios de confidencialidad, integridad, disponibilidad y seguridad de datos.

La revisión de este compendio de políticas y procedimientos se realiza de forma anual o si ocurre algún cambio que lo amerite, para asegurar su conveniencia, adecuación y eficacia continua. La Dirección y el Equipo de IT (Seguridad), son los responsables de esta revisión.
Son ejemplos de estas:

1. Política de Transferencia de la información (Resp. Ricardo Chantada)
2. Política de Requerimiento e Instalación de Software. (Resp. Diego Ranieri)
3. Política de Gestión de Vulnerabilidades. (Resp. Ricardo Chantada)
4. Política de Desarrollo seguro. (Resp. Luciano Giménez Ausfet)
5. Política Backup y plan de contingencia (Resp. Luciano Giménez Ausfet)
6. Política de Antivirus. (Resp. Diego Ranieri)
7. Política Seguridad Física y Ambiental (Resp. Diego Ranieri)
8. Política de Pantalla y Escritorio Limpios (Resp. Diego Ranieri)
9. Política de Trabajo Remoto (Resp. Diego Ranieri)

10. Política de Control de Accesos (Resp. Luciano Giménez Ausfet)
11. Política Uso Controles Criptográficos (Resp. Ricardo Chantada)
12. Registro y Monitoreo (Resp. Ricardo Chantada)
13. Plan de Continuidad (Resp. Diego Ranieri)
14. Gestión de Redes y Comunicaciones (Resp. Diego Ranieri)
15. Gestión de Cambios de Seguridad de la Información (Resp. Diego Ranieri)
16. Gestión de la Capacidad (Resp. Ricardo Chantada)
17. Gestión de Activos (Resp. Diego Ranieri)

Todo lo definido en esta Política se concretará y desarrollará, mediante las buenas prácticas y procedimientos incluidos en el Sistema de Gestión de Seguridad de la información, las cuales se integrarán con nuestras herramientas de gestión, en pro de la optimización y buscando la mejora continua en la gestión.

Esta política aquí fijada entra en vigor a partir del 31/07/2023.
Esta política es comunicada a todos los colaboradores y se halla disponible para nuestros clientes y otras partes interesadas.