POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

METALPREN S.A como empresa responsable considera que la Información es un activo valioso para el cumplimiento de sus funciones y el alcance de los objetivos estratégicos.

Por tanto, es compromiso fundamental gestionar la seguridad de la información y los activos que la sustentan, estableciendo los mecanismos para proteger su confidencialidad, disponibilidad e integridad ante amenazas internas o externas, deliberadas o accidentales y mejorar continuamente su Sistema de Gestión de Seguridad de la Información.

Nos comprometemos a:

1. Evaluar por anticipado los posibles riesgos en materia de seguridad de información en nuestras actividades y operaciones, adoptando las medidas de gestión que se consideren necesarias en función de su nivel de riesgo.

2. Mantener medidas de seguridad robustas para proteger equipos y dispositivos contra amenazas físicas y tecnológicas, que incluyan firewalls y protección contra malwares.

3. Establecer procedimientos y responsabilidades de respuesta inmediata, eficaz y ordenada ante incidentes de seguridad de información, así como planes de contingencia y continuidad específicos, incluyendo retroalimentación posterior para la mejora continua de los procesos de seguridad.

4. Asegurar la eficacia de las medidas implementadas.

5. Implementar un programa de copias de seguridad de forma regular y garantizar el proceso de restauración de datos.

6. Garantizar que nuestros trabajadores son debidamente informados y capacitados en materia de seguridad de información con el fin de tener presentes las prácticas de trabajo y los procedimientos establecidos para el desempeño de sus funciones. Asimismo, informar sobre la materia a proveedores y contratistas.

7. Mantener los mecanismos para el cumplimiento legal y normativo en políticas en consecuencia.

8. Implementar medidas proactivas para mitigar riesgos de seguridad identificados o en respuesta a cambios en las amenazas y tecnologías emergentes.

9. Establecer protocolos seguros para la transmisión de información crítica, que incluya cifrado robusto para comunicaciones sensibles.

10. Establecer controles estrictos y medidas de monitoreo para supervisar el uso de dispositivos móviles que accedan a la red de la empresa, así como establecer tecnologías seguras para acceder a los sistemas de información de forma remota.

11. Implantar sistemas de monitorización, detección y alerta temprana que permitan una identificación permanente y continuada de las vulnerabilidades, nuevas amenazas e incidentes a nivel global, así como definir los mecanismos oportunos para asegurar que las personas encargadas de la protección de nuestros activos, sus infraestructuras y/o de sus sistemas de información estén informados de dichas incidencias en forma y plazo.

Julio Granda S.
Gerente General

VERSIÓN 01

Aprobación: 15 de Enero 2024