Objetivo

Definir el compromiso y proporcionar el marco de la organización para la implementación y operación del Sistema de Gestión de Seguridad de la Información.

Alcance del documento

El alcance de esta política abarca todos los procesos y áreas operativas de la organización.

Política del Sistema de Gestión de la Seguridad de la información

Nuestro principal enfoque está en desarrollar soluciones tecnológicas a la medida para satisfacer las necesidades de nuestros clientes. Optando por construir aplicaciones y sistemas que se ajusten a los requisitos particulares de cada proyecto.

En la Asociación de ingenieros de sistemas 3D Grupo Empresarial, desarrollamos software a la medida, reconociendo la importancia de la gestión de la información en la consecución de nuestros objetivos.
Asumimos la responsabilidad de garantizar la confidencialidad, integridad y disponibilidad de datos, información y recursos a través de la implementación y mejora del Sistema de Gestión de la Seguridad de la Información basado en la norma ISO 27001:2022.

Esta elección refleja nuestra firme determinación de establecer y mantener estándares sólidos de seguridad de la información, por ello, a través de este sistema, nos comprometemos a:

1. Identificar y mitigar proactivamente los riesgos de seguridad de la información. Reconocemos que, al anticipar y abordar eficazmente los riesgos, podemos asegurar la integridad y la confidencialidad de nuestros activos de información, así como garantizar la continuidad operativa en un entorno seguro.

2. Promover una cultura de seguridad que involucre a todos los miembros de la organización, asegurando su continua capacitación y concientización por la seguridad de la información.

3. Proporcionar los recursos necesarios para el mantenimiento y la operación efectiva del sistema de gestión de la seguridad de la información.

4. Establecer controles de acceso adecuados para garantizar la confidencialidad, la integridad y disponibilidad de la información.

5. Establecer los canales de comunicación necesarios para notificar incidentes, eventos, vulnerabilidades, riesgos que puedan afectar los activos de información de la organización.

6. Actuar con agilidad y destreza en la respuesta a incidentes de seguridad, reduciendo al mínimo los efectos adversos.

7. Cumplir con los requisitos legales y regulaciones relacionadas con la seguridad de la información.

La dirección promueve esta política para asegurar que sea entendida, implementada, difundida y mantenida en todos los niveles de la organización.