Paseo del País Valenciano, 6, entresuelo 1
46760 Tavernes de la Valldigna
Teléfono: +34 963 604 540
tesi@tesigandia.com
www.tesigandia.com

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Fecha: 2/5 /2024
Versión: 1

Introducción

TÉCNICAS EQUIPOS Y SERVICIOS INFORMÁTICOS SL depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.
Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que la organización debe aplicar las medidas mínimas de seguridad exigidas por la norma UNE ISO/IEC 27001, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Objetivos del SGSI

Los siguientes objetivos del SGSI implementados por la organización, se basan en la implementación de medidas de seguridad proporcionales a la naturaleza de la información y servicios prestados, de acuerdo con las políticas y normativas de gestión y protección de la información, teniendo en cuenta un adecuado análisis de riesgo. Así siendo, asumimos:

- Seguridad como un proceso integrado por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema.
- Garantizar que los sistemas cumplen los requisitos básicos de seguridad, eliminando las funcionalidades innecesarias y inadecuadas.
- Acciones de concienciación de las personas que intervienen en el/los procesos.
- Proporcionar a todos los miembros de la organización el continuado conocimiento sobre las políticas y normativas de seguridad de información por medio de acciones de formación y difusión para la protección y correcta utilización de los sistemas de información.
- Gestión de personal y profesionalidad.
- Gestión de la seguridad basada en los riesgos y análisis y gestión de riesgos.
- Prevención, reacción y recuperación, para protección de activos de información en caso de eventuales incidentes de seguridad.
- Gestión de riesgos por medio de análisis periódicos, adecuando el SGSI a nuevas realidades anteriormente no previstas.
- Protección de la información almacenada y en tránsito y continuidad de la actividad.
- Protección de las instalaciones.
- Registros de actividad documentados
- Mejora continua con revisión periódica de la política de seguridad de información adecuándola a las normativas y reglas legales.