Gestión de la seguridad de la información en un sistema basado en ISO/IEC 27001

Laboratorio de Seguridad de la Información

ISO/IEC 27001 es una norma internacional certificable que define los requisitos para crear, gestionar, implementar y documentar un SGSI (Sistema de gestión de la seguridad de la información). La norma es adecuada a cualquier tipo de organización, es independiente de cualquier plataforma IT y está estructurada para que sea compatible con otros estándares de sistemas de gestión, tales como ISO 9001.

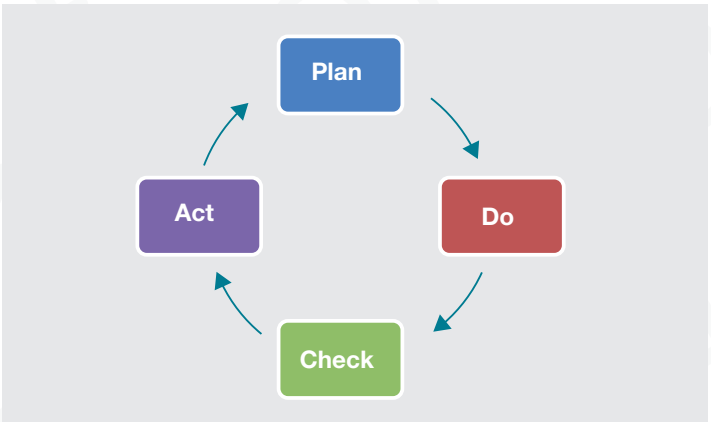
Un SGSI es una herramienta que permite conocer, gestionar y minimizar los riesgos de seguridad de la información a los que se enfrenta la organización, y se debe adaptar a los cambios internos y externos de la misma.

¿Qué ventajas tiene un SGSI?:

- Reduce los riesgos de seguridad de la información y la probabilidad y el impacto de los incidentes.
- La organización se asegura del cumplimiento de la legislación vigente.
- La seguridad se considera un sistema y se convierte en una actividad de gestión.
- Proporciona ventajas de marketing/marca.
- Permite ahorro de costes.

¿Qué desventajas tiene un SGSI?:

- Se debe certificar y mantener.
- Requiere diseñarlo, desarrollarlo, realizar pruebas e implementarlo.
- Necesita recursos de la organización.



Un SGSI basado en ISO/IEC 27001 utiliza el Ciclo de Deming o ciclo PDCA (Plan, Do, Check, Act), método de gestión iterativo compuesto por las siguientes fases:

SGSI: Creación y Gestión (Plan):

- En esta fase se debe realizar un estudio de la situación de la organización con respecto a la seguridad de la información, y estimar las medidas a implantar en función de sus necesidades.

SGSI: Implementación y operación (Do):

- Aquí se implantarán los controles de seguridad que se han escogido en la fase anterior. Los controles seleccionados se recogerán en la Declaración de Aplicabilidad (SOA).

SGSI: Supervisión y revisión (Check):

- Esta fase evalúa la eficacia y el éxito de los controles implantados. Se deben establecer un conjunto de indicadores que permitan determinar el estado del sistema.

SGSI: Mantenimiento y mejora (Act):

- Finalmente, hay que realizar las tareas de mantenimiento del SGSI, y se ajustarán o se controlarán las desviaciones encontradas aplicando medidas correctivas y de mejora.

"ES NECESARIO PROTEGERSE FRENTE A LAS AMENAZAS DE SEGURIDAD DE LA INFORMACIÓN"

XUNTA DE GALICIA
CONSELLERÍA DE SANIDADE

SERVIZO GALEGO de SAÚDE

MINISTERIO DE ECONOMÍA Y COMPETITIVIDAD

UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa