

Xestión da seguridade da información nun sistema baseado en ISO/IEC 27001



Laboratorio
de Seguridade
da Información

ISO/IEC 27001 é unha norma internacional certificable que define os requisitos para crear, xestionar, implementar e documentar un SGSI (Sistema de xestión da seguridade da información). A norma é adoptada a calquera tipo de organización, é independente de calquera plataforma IT e está estruturada para que sexa compatible con outros estándares de sistemas de xestión, tales como ISO 9001.

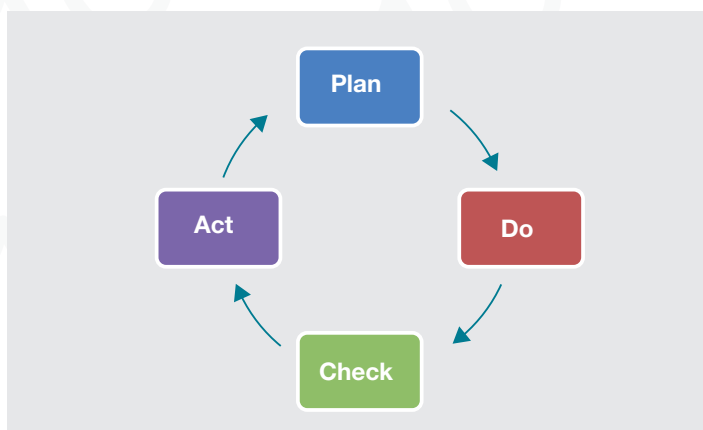
Un SGSI é unha ferramenta que permite coñecer, xestionar e minimizar os riscos de seguridade da información ós que se enfronta a organización, e débese adaptar ós cambios internos e externos da mesma.

¿Que vantaxes ten un SGSI?:

- Reduce os riscos de seguridade da información e a probabilidade e o impacto dos incidentes.
- A organización asegúrase do cumprimento da lexislación vixente.
- A seguridade considérase un sistema e convértese nunha actividade de xestión.
- Proporciona vantaxes de marketing/marca.
- Permite aforro de custos.

¿Que desvantaxes ten un SGSI?:

- Débese certificar e manter.
- Require deseño, desenvolvemento, realizar probas e implementalo.
- Necesita recursos da organización.



Un SGSI baseado en ISO/IEC 27001 emprega o Ciclo de Deming ou ciclo PDCA (Plan, Do, Check, Act), método de xestión iterativo composto polas seguintes fases:

SGSI: Creación e Xestión (Plan):

- Nesta fase débese realizar un estudo da situación da organización con respecto á seguridade da información, e estimar as medidas a implantar en función das súas necesidades.

SGSI: Implementación e operación (Do):

- Aquí implantaranse os controis de seguridade que se escolleron na fase anterior. Os controis seleccionados recolléranse na Declaración de Aplicabilidade (SOA).

SGSI: Supervisión e revisión (Check):

- Esta fase avalía a eficacia e o éxito dos controis implantados. Débense establecer un conxunto de indicadores que permitan determinar o estado do sistema.

SGSI: Mantemento e mellora (Act):

- Finalmente, hai que realizar as tarefas de mantemento do SGSI, e axustaranse ou controlaranse as desviacións atopadas aplicando medidas correctivas e de mellora.

**“É NECESARIO PROTEXERSE
FRONTE ÁS AMEAZAS DE
SEGURIDADE DA INFORMACIÓN”**