Procedimiento a seguir ante la ausencia de un sistema de seguridad en una organización

En calidad de expertos en seguridad, ante una organización que nunca ha implantado un sistema de seguridad, el procedimiento a seguir debe ser metódico, estructurado y adaptado a las características específicas de dicha organización. A continuación se detallan los pasos clave que deberían seguirse:

1. Diagnóstico inicial

El primer paso consiste en realizar un diagnóstico de la situación actual. Esto implica reunirse con la dirección para comprender los objetivos del negocio, el entorno operativo y los activos críticos. Es fundamental definir el alcance del sistema de seguridad, así como identificar posibles carencias actuales en cuanto a políticas, procedimientos o medidas técnicas.

2. Identificación de activos y análisis de riesgos

Se debe elaborar un inventario de activos que incluye hardware, software, datos, procesos y personas. A partir de este inventario, se realiza un análisis de riesgos, identificando las amenazas y vulnerabilidades asociadas, y evaluando el impacto y la probabilidad de ocurrencia. Este paso permite priorizar los riesgos y decidir qué medidas deben aplicarse.

3. Definición de la política de seguridad

Una vez identificado el contexto y los riesgos, es esencial establecer una Política de Seguridad de la Información. Esta política debe estar alineada con los objetivos de la organización y definir los principios básicos de seguridad, el compromiso de la alta dirección y las responsabilidades generales en materia de seguridad.

4. Diseño e implementación del SGSI

Se procede al diseño e implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), preferiblemente basado en estándares reconocidos como ISO/IEC 27001. En esta fase se definen:

- Los objetivos de seguridad.
- Los controles a implantar (tanto técnicos como organizativos).
- Los procedimientos necesarios para operar y mantener dichos controles.
- Los roles y responsabilidades de las personas involucradas.

5. Formación y concienciación

Es imprescindible desarrollar programas de formación y concienciación en seguridad dirigidos a todo el personal. La seguridad no solo depende de la tecnología, sino también del comportamiento humano. Fomentar una cultura de seguridad es esencial para garantizar la efectividad del SGSI.

6. Monitorización y auditoría

Una vez implementado el SGSI, se deben establecer mecanismos de monitorización y evaluación continua. Esto incluye auditorías internas, revisiones periódicas y seguimiento de incidentes de seguridad. El objetivo es garantizar que los controles implantados sean eficaces y estén alineados con los riesgos identificados.

7. Revisión por la dirección y mejora continua

Finalmente, se realiza una revisión por la dirección para evaluar el desempeño del SGSI y tomar decisiones estratégicas de mejora. Este proceso debe repetirse periódicamente, fomentando un ciclo de mejora continua (PDCA: Plan – Do – Check – Act) que mantenga el sistema actualizado frente a nuevas amenazas y necesidades organizativas.

Referencias

INCIBE | INCIBE. (s. f.). https://www.incibe.es/

ISO/IEC 27001:2022. (s. f.). ISO. https://www.iso.org/standard/27001

ISO/IEC 27005:2018. (s. f.). ISO. https://www.iso.org/standard/75281.html