Implementación del Sistema de Gestión de Seguridad de la Información (SGSI) - ISO 27001

Objetivo:

Este documento detalla los pasos necesarios para implementar un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO 27001, garantizando la protección de la información crítica de la empresa a través de un enfoque estructurado de gestión de riesgos y seguridad.

1. Análisis de Riesgos

- Identificación de activos de información críticos y evaluación de posibles amenazas y vulnerabilidades.
- Evaluación del impacto de cada riesgo en los procesos de negocio y la infraestructura.
- Priorización de riesgos según su probabilidad e impacto, utilizando una matriz de riesgos.
- Desarrollo de un plan de mitigación para reducir los riesgos a un nivel aceptable.

2. Definición de Políticas de Seguridad

- Establecer políticas claras sobre el uso de recursos tecnológicos, acceso a la información y protección de datos.
- Desarrollar procedimientos para la gestión de incidentes de seguridad, control de accesos y auditorías periódicas.
- Incluir en las políticas la regulación de la seguridad física y lógica de los activos.

3. Implementación de Controles de Seguridad

- Aplicar controles técnicos (firewalls, cifrado de datos, sistemas de detección de intrusiones).

- Implementar controles físicos (acceso restringido a las instalaciones, controles de seguridad en el entorno físico).
- Desarrollar controles administrativos (gestión de accesos, capacitación continua y sensibilización del personal).

4. Planes de Acción para Proteger la Información Crítica

- Desarrollar y mantener planes de contingencia ante incidentes que puedan comprometer la información crítica.
- Establecer planes de recuperación ante desastres (DRP) para restaurar la operatividad tras incidentes.
- Garantizar la correcta gestión de respaldos y la implementación de procedimientos de restauración en tiempo y forma.

Conclusión

La implementación de un SGSI conforme a la norma ISO 27001 permite gestionar de manera proactiva los riesgos de seguridad, asegurando la protección de la información crítica de la empresa. El seguimiento de las políticas de seguridad y la mejora continua son fundamentales para mantener un entorno seguro y confiable.