Evaluación, Auditoría y Certificación

Las certificaciones tienen los siguientes beneficios:

- Mejor seguridad a menor coste
- Credibilidad y confianza: Muestra que se han tomado las precauciones requeridas para minimizar los riesgos del negocio
- Cumplimiento: Demuestra cumplimiento con regulaciones
- Cumplir responsabilidades de confianza como organización en la protección de los activos de la compañía.

Cumplimiento, Certificación y Acreditación

- Cumplimiento: Cualquier organización puede implementar un estandar y decir que cumple, pero no hay ninguna evidencia
- Certificación: Es una forma de probar que la organización cumple con los estándares.
- Acreditación: Se le entrega a la organización que realiza la certificación. Los cuerpos de certificación tiene que demostrar que sus métodos de certificación son justos, creibles y confiables, para ello suelen haber autoridades de acreditación nacionales.

Certificación y Acreditación en España

En españa está la Entidad Nacional de Acreditación (ENAC). Tiene los siguietes servicios de acreditación:

- Certificación de los Sistemas de Gestión de la seguridad (ISO27001): Asegura la confidencialidad, integridad y disponibilidad de la información..
- Certificación dentro del Esquema Nacional de Seguridad (ENS): Fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la adminsitración pública.

ISO 27001

ISO 27001: La Certificación

Se suelen seguir los siguientes pasos:

- Pre-auditoría: Existencia y alcance apropiado del SGSI
- Auditoría de certificación
    - Fase 1: Revisión de la documentación
    - Fase 2: Procesos y control
- Certificación: Emisión del certificado
- Seguimiento anual: Mejora continua.

ISO 27001: El ciclo de certificación

1. Revisión de preparación
2. Certificación
3. Auditoría de supervisión: Comienza el cliclo, estas auditorías revisan las auditorías internas, gestión de las revisiones, acciones correctivas y preventivas, mejoras...
4. Auditoría de recertificación: Revisa el sistema completo de forma menos profunda que la primera audotoría, centrándose en las capacidades de mejora.

Documentos y registros necesarios

1. Alcance del sistema de gestión de seguridad de la información
2. Política de seguridad de la información
3. Proceso de evaluación de riesgos
4. Proceso de tratamiento de riesgos
5. Objetivos de seguridad de la información
6. Evidencia de la competencia de las personas que trabajan en SI
7. Otros documentos relacionados con el SGSI considerados necesarios en la organización
8. Documentos de planificación y control operacional
9. Resultados de las evaluaciones de riesgo
10. Decisiones con respecto al tratamiento del riesgo
11. Evidencia del seguimiento y medición de seguridad de la información
12. Porgrama de auditoría interna sobre SGSI y sus resultados
13. Evidencia de las principales revisiones de la gestión del SGSI
14. Evidencia de las no conformidades identificadas y acciones correctivas que surjan

Problemas comunes

- Registro de activos incompleto
- Riesgo del personal no incluido
- Métodos demasiado complicados
- No aprobado por gerencia
- Ubicación de la sala de servidores
- Sala de servidores no segura
- Incidentes no reportados por el personal
- Pruebas insuficientes para demostra mejora

Esquema Nacional de Seguridad (ENS)

RD 3/2010 Artículo 34: Auditoría de seguridad

- Los sistemas de información serán objeto de una auditoría regular ordinaria al menos cada 2 años para verificar el cumplimiento de los requerimientos del ENS
- Se debe realizar una auditoría siempre que se produzcan modificaciones sustanciales en los sistemas de la información.