Elaboración de Documentación de SGSI

DESCRIPCION DEL CURSO:

La implantación de un **SGSI** (Sistema de Gestión de Seguridad de la Información) basado e**n ISO 2700**1 implica la correcta elaboración y recopilación de la Documentación, para garantizar la confidencialidad, integridad y disponibilidad de la información asociada a dicho SGSI.

En la nueva **ISO 27001:2013** se habla de información documentada para hacer referencia a los denominados documentos y registros diferenciados en la anterior versión.

CONTENIDO:

- Documentación requerida por el estándar ISO 27001:2013.
- Principios para elaborar procedimientos.
- Metodología para el manejo de la información documentada.
- Documentación de políticas e instrucciones de trabajo.
- Gestión de la información documentada controlada.
- Manejo de un proyecto de documentación.

Documentos obligatorios y registros requeridos por ISO 27001:2013

Aquí están los documentos que necesita elaborar si quiere cumplir con la norma ISO 27001

- Análisis de Contexto (cláusula 4.1)
- Requerimientos de Seguridad de las Partes Interesadas (cláusula 4.2)
- Alcance del sistema de gestión de seguridad de la información (cláusula 4.3)
- Interferencias y dependencias entre las actividades realizadas por la organización y aquellas realizadas (cláusula 4.3.c)
- Política de seguridad de la información (cláusulas 5.2)
- Gestión de Riesgos y Oportunidades del SGSI (cláusula 6.1.1)
- Metodología de identificación, análisis, evaluación y tratamiento de riesgos de seguridad de la información(cláusula 6.1.2)
- Declaración de aplicabilidad (cláusula 6.1.3 d)
- Objetivos de Seguridad de la Información (cláusula 6.2)
- Informe sobre evaluación de riesgos (cláusula 8.2)

- Definición de roles y responsabilidades de seguridad (cláusula 5.3)
- Evidencia de la competencia (cláusula 7.2)
- Plan de Comunicaciones del SGSI (cláusula 7.4)
- Control de Documentos internos y externos del SGSI (cláusula 7.5)
- Evaluación del desempeño del SGSI (cláusula 9.1)
- Auditoría Interna del SGSI (cláusula 9.2)
- Revisión por la Dirección del SGSI (cláusula 9.3)
- Mejora continua del SGSI (cláusula 10)

Registros obligatorios:

- Registros de formación, habilidades, experiencia y calificaciones (cláusula 7.2)
- Registros de gestión de riesgos y oportunidades del SGSI (cláusula 6.1.1)
- Registros de gestión de riesgos de seguridad de la información (cláusula 6.1.2)
- Seguimiento y resultados de medición (cláusula 9.1)
- Programa de auditoria interna (cláusula 9.2)
- Resultados de auditorías internas (cláusula 9.2)
- Resultados de la Revisión por Dirección (cláusula 9.3)
- Resultados de acciones correctivas (cláusula 10.1)
- Registros de las actividades de usuario, excepciones y eventos de seguridad (cláusulas A.12.4.1 y A.12.4.3)

Documentos no obligatorios

Hay numerosos documentos no obligatorio que pueden ser utilizados para la implementación de la ISO 27001, especialmente para los controles de seguridad del anexo A. Sin embargo, estos documentos no son obligatorios pero comúnmente son los más usados:

- Política BYOD (Bring Your Own Device = Trae tu propio dispositivo) (cláusula A.6.2.1)
- Política de dispositivo sobre dispositivos móviles y tele-trabajo (cláusula A.6.2.1)
- Política de clasificación de la información (cláusulas A.8.2.1, A.8.2.2 y A.8.2.3)
- Política de claves (cláusulas A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1 y A.9.4.3)
- Política de eliminación y destrucción (cláusulas A.8.3.2 y A.11.2.7)
- Procedimientos para trabajo en áreas seguras (cláusula A.11.1.5)
- Política de pantalla y escritorio limpios (cláusula A.11.2.9)
- Política de gestión de cambios (cláusulas A.12.1.2 y A.14.2.4)
- Política de Copias de seguridad (cláusula A.12.3.1)

- Política de transferencia de información (cláusulas A.13.2.1, A.13.2.2, y A.13.2.3)
- Análisis de impacto en el negocio (BIA) (cláusula A.17.1.1)
- Plan de pruebas y verificación (cláusula A.17.1.3)
- Plan de mantenimiento y revisión (cláusula 17.1.3)
- Estrategia de continuidad de negocio (cláusula A.17.2.1)