ISO 27001 FOUNDATION

(I27001F)

CERTIFIED

CertiProf

Professional Knowledge

ISO 27001 FOUNDATION

Introducción

La certificación ISO 27001:2022 Foundation - I27001F tiene como objetivo describir los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de seguridad de la información, ciberseguridad y protección de la privacidad en el contexto de la organización. La ISO 27001 es una norma internacional publicada por la Organización Internacional de Normalización (ISO).

La seguridad de la información y la protección de la privacidad son hoy en día activos de incalculable valor, ya que la pérdida de los mismos por diferentes motivos puede tener un gran impacto en las organizaciones y afectar negativamente su reputación. La norma ISO 27001:2022 puede implantarse en cualquier tipo de organización, con o sin ánimo de lucro, privada o estatal, pequeña o grande.

La formación consistirá en presentaciones de temas con el uso del material y ejemplos. Se espera que durante la formación los alumnos aprendan las prácticas fundamentales para la implantación y gestión de un SGSI. Es muy recomendable trabajar con la traducción oficial de la norma de cada país.

Objetivos

- Comprender y analizar los fundamentos de la norma ISO 27001:2022.
- Familiarizarse con los principios, conceptos y requisitos de la norma ISO/IEC 27001:2022.
- Entender cómo desarrollar un SGSI.
- Revisar y comprender el Anexo A de la norma ISO 27001.

Agenda

1. Introducción y antecedentes

Introducción
Historia de la Norma
ISO/IEC 27001:2022 - Estructura
ISO 27000 - Familia de Normas

2. Conceptos Clave

Información y Principios Generales
Seguridad de la Información
El Sistema de Gestión
Factores Críticos del Éxito de un SGSI
Beneficios de la Familia de Normas SGSI

3. Terminos y Definiciones (Ver suplemento N°1 Glosario 27001)

Estructura de la ISO/IEC 27001
Ciclo Deming PHVA y SGSI

4. Contexto Organizacional

Comprensión de la Organización y su Contexto
Taller: Determinar el contexto de la organización haciendo uso de una matriz de análisis FODA
Comprensión de las Necesidades y Expectativas de las Partes Interesadas
Determinación del Alcance del Sistema de Gestión de la Seguridad de la Información
Sistema de Gestión de la Seguridad de la Información
Taller: Definir el alcance del SGSI
Taller: Definir el alcance del SGSI

5. Liderazgo

Liderazgo y compromiso
Política
Roles, Responsabilidades y Autoridades en la Organización

6. Planificación

Acciones para tratar los Riesgos y las Oportunidades
Estructura de la Norma ISO 31000 de Gestión de Riesgos - Directrices
Taller: Definir la Declaración de Aplicabilidad para 5 Controles del Anexo A
Objetivos de Seguridad de la Información y Planificación para su consecución
Taller: Definir los Objetivos de Seguridad de la Información

7. Soporte

Recursos
Competencia
Concienciación
Comunicación
Información Documentada

8. Operación

Planificación y Control Operacional
Evaluación de los Riesgos para la Seguridad de la Información
Tratamiento de los Riesgos para la Seguridad de Información
Evaluación y Tratamiento de los Riesgos

9. Evaluación del Desempeño

Seguimiento, Medición, Análisis y Evaluación
Auditoría Interna
Auditoría
Revisión por la Dirección

10. Mejora

No conformidad y acciones correctivas
Mejora continua

Anexo 1: Términos y Definiciones

Taller: Revisión de los Términos y Definiciones de la Seguridad de la Información

Análisis y estudio de una lista de 90 términos clave relacionados con la serie ISO 27000 y la seguridad de la información, definidos en el contexto de los sistemas de gestión de la seguridad de la información.

Conclusiones