TEMARIO DEL CURSO

ISO/IEC 27001:2022 Lead Auditor Professional (I27001LA™)

20 horas

Aprende a planificar, ejecutar, informar y realizar seguimiento de auditorías internas y externas de un Sistema de Gestión de la Seguridad de la Información (SGSI) conforme a ISO/IEC 27001:2022, aplicando las directrices de auditoría establecidas en ISO 19011:2018.

OBJETIVOS DEL CURSO

- Entender e interpretar los requisitos de ISO/IEC 27001:2022.
- Analizar la estructura y alcance del SGSI.
- Desarrollar la capacidad de auditar los procesos conforme a la norma.
- Identificar oportunidades de mejora en el SGSI.
- Aplicar ISO 19011:2018 para auditorías internas y de certificación.
- Gestionar programas de auditoría.
- Redactar no conformidades correctamente.
- Liderar equipos auditores.

A QUIÉN VA DIRIGIDO

- Auditores internos.
- Auditores líderes.
- CISO y responsables de seguridad.
- Consultores ISO 27001.
- Gerentes de TI.
- Profesionales de cumplimiento.
- Equipos de implantación SGSI.

EL CURSO INCLUYE

- Manuales digitales
- Diploma de asistencia
- Tramitación de FUNDAE incluida

TEMARIO

MÓDULO 01.
Introducción y SGSI

- Introducción.
- Historia de la norma.
- ISO/IEC 27001:2022 estructura.
- Familia ISO 27000.
- Sistema de Gestión de la Seguridad de la Información.

MÓDULO 02.
Conceptos Claves

- ¿Qué es un SGSI?
- Información y principios generales.
- Seguridad de la información.
- Factores críticos de éxito.
- Beneficios de la familia SGSI.

MÓDULO 03.
Diseño e Implementación del SGSI

- Fases de diseño.
- Etapas de implementación.
- Ciclo PHVA aplicado al SGSI.
- Estructura ISO/IEC 27001.

MÓDULO 04.
Contexto de la Organización (Cláusula 4)

- Comprensión del contexto.
- Partes interesadas.
- Determinación del alcance.
- Sistema de gestión.

MÓDULO 05.
Liderazgo (Cláusula 5)

- Liderazgo y compromiso.
- Política.
- Roles y responsabilidades.

MÓDULO 06.
Planificación (Cláusula 6)

- Acciones para tratar riesgos y oportunidades.
- Plan de tratamiento de riesgos.
- ISO 31000 – gestión del riesgo.
- Objetivos de seguridad.

MÓDULO 07.
Soporte (Cláusula 7)

- Recursos.
- Competencia.
- Concienciación.
- Comunicación.
- Información documentada.

MÓDULO 08.
Operación (Cláusula 8)

- Planificación y control operacional.
- Apreciación del riesgo.
- Tratamiento del riesgo.
- Evaluación y tratamiento.

MÓDULO 09.
Evaluación del Desempeño (Cláusula 9)

- Seguimiento y medición.
- Auditoría interna.
- Revisión por la dirección.

MÓDULO 10.
Mejora (Cláusula 10)

- No conformidades.
- Acciones correctivas.
- Mejora continua.

MÓDULO 11.
Anexo A – Controles ISO/IEC 27001:2022

- Controles organizacionales.
- Controles de personas.
- Controles físicos.
- Controles tecnológicos.

MÓDULO 12.
Gestión de Riesgos (ISO/IEC 27005)

- Proceso de gestión del riesgo.
- Establecimiento del contexto.
- Identificación y clasificación de activos.
- Amenazas y vulnerabilidades.
- Perfil de amenaza.
- Ciclo de gestión del riesgo.

MÓDULO 13.
Auditoría según ISO 19011:2018

- Principios de auditoría.
- Programa de auditoría.
- Plan de auditoría.
- Tipos de auditoría.
- Criterios y evidencias.
- Equipo auditor.
- Competencia del auditor.
- Métodos de auditoría.
- Evaluación de auditores.
- Gestión del programa de auditoría.
- Determinación de objetivos y alcance.

MÓDULO 14.
Ejecución de la Auditoría

- Reunión de apertura.
- Revisión documental.
- Comunicación durante la auditoría.
- Técnicas de entrevista.
- Recopilación de evidencias.
- Manejo de situaciones difíciles.
- Redacción de no conformidades.
- Informe de auditoría.
- Reunión de cierre.
- Auditorías de seguimiento.