



# ISO 27001 LEAD IMPLEMENTER CERTIFIED



I27001CLI Versión 052022

**CertiProf®**

## ISO 27001 Certified Lead Implementer I27001CLI

### Syllabus V052022

Introducción	3
Objetivos de Aprendizaje	3
Formato y Duración del Examen	3
Público Objetivo	3
Contenido	4



## Introducción

Esta certificación ayuda a comprender e implementar un sistema de gestión global, basado en un enfoque hacia los riesgos de un negocio, para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

Incluye estructura organizacional, políticas, planes, responsabilidades, procedimientos, procesos y recursos.

## Objetivos de Aprendizaje

- Proporcionar explicación y orientación sobre la ISO/IEC 27001 con base en la ISO/IEC 27003:2017 para el diseño e implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI)
- Interpretar los requisitos de ISO/IEC 27001 para un SGSI desde la perspectiva de un implementador
- Entender los componentes necesarios para determinar el estado actual de un sistema de gestión de seguridad de la información que sirva como punto de partida
- Determinar la implementación de los requisitos necesarios para lograr implementar un sistema que cumpla con los requisitos y logre pasar una auditoría de tercera parte

## Formato y Duración del Examen

- Formato: Opción múltiple
- Libro Abierto: No
- Preguntas: 40
- Puntuación de aprobación: 32/40 o 80 %
- Idioma: Español
- Duración: 60 minutos
- Libro abierto: No
- Entrega: Este examen está disponible en línea
- Supervisado: Si. En vivo

## Público Objetivo

- Gerentes de proyecto y consultores involucrados y preocupados por la implementación de un SGSI
- Asesores expertos que buscan dominar la implementación de un SGSI
- Individuos responsables de garantizar la conformidad con los requisitos de seguridad de la información dentro de una organización
- Miembros de un equipo de implementación de SGSI

## Contenido

### 1. Introducción a los Sistemas de Gestión

- Información y Principios Generales
- La Seguridad de la Información
- El Sistema de Gestión
- Factores Críticos de Éxito de una SGSI
- Beneficios de la Familia de Normas SGSI
- ISO/IEC 27003:2017 Tecnología de la Información. Técnicas de Seguridad
- ISO 27001: Administrativo
- ISO 27001: Controles Técnicos
- ISO 27002
- Ruta de Navegación

### 2. Planificación de la Implementación de un SGSI

- Visión de Proyecto
- Documento: Plan del Proyecto
- Caso de Negocio
- Partes de un Caso de Negocio

### 3. Pasos Generales en la Implementación

- Objetivo del Módulo
- Referencia :Etapas de Implementación de un SGSI
- Pasos Generales en la Implementación
- PHVA Aplicado a la Implementación del SGSI
- PHVA – Planeación
- Análisis de Brechas - Análisis GAP
- Objetivos Análisis GAP
- Cómo Realizar un Análisis de Brechas GAP
- Modelos de Madurez
- Modelo de Madurez COBIT
- Cómo Realizar un Análisis de Brechas GAP

### 4. Contexto de la Organización: Interpretar los Requisitos de ISO/IEC 27001

- Estructura de ISO/IEC 27001
- Objetivo del Módulo
- Recomendación
- Comprensión de la Organización y su Contexto
- Cuestiones Externas
- Cuestiones Internas
- Cuestiones Internas y Externas
- Comprensión de las Necesidades y Expectativas de las Partes Interesadas

Partes Interesadas Internas  
Partes Interesadas Externas  
Alcance del SGSI

#### **5. Liderazgo: Interpretar los Requisitos ISO/IEC 27001**

Estructura de ISO/IEC 27001  
Objetivo del Módulo  
Recomendación  
Liderazgo y Compromiso  
Políticas  
Contenido de una Política  
Política de Seguridad de la Información  
Roles, Responsabilidades y Autoridades de S.I

#### **6. Planificación: Interpretar los Requisitos de ISO/IEC 27001**

Estructura de ISO/IEC 27001  
Objetivo del Módulo  
Recomendación  
¿Por qué realizar una gestión al riesgo?  
Proceso de Gestión del Riesgo Basado en ISO-IEC 27005  
Establecimiento del Contexto  
Identificación de los Activos  
Clasificación de los Activos  
Amenaza  
Perfil de una Amenaza  
Amenazas a la Información  
Vulnerabilidad  
¿Riesgo = Incertidumbre?  
Ciclo de la Gestión de Riesgos  
Gestión De Riesgos SGSI  
Identificación del Riesgo  
Declaración de Aplicabilidad  
Acciones para Tratar los Riesgos y Oportunidades  
Objetivos de Seguridad de la Información  
Expresión de los Objetivos de Seguridad

#### **7. Soporte: Interpretar los Requisitos de ISO/IEC 27001**

Estructura de ISO/IEC 27001  
Objetivo del Módulo  
Recomendación  
Recursos  
Competencia

Toma de Conciencia  
Comunicación  
Información Documentada

#### **8. Operación: Interpretar los Requisitos de ISO/IEC 27001**

Estructura de ISO/IEC 27001  
Recomendación  
Planificación y Control Operacional  
Evaluación de Riesgos de Seguridad de la Información  
Tratamiento de Riesgos de Seguridad de la Información

#### **9. Evaluación del Desempeño: Interpretar los Requisitos de ISO/IEC 27001**

Estructura de ISO/IEC 27001  
Objetivo del Módulo  
Recomendación  
Seguimiento, Medición, Análisis y Evaluación  
Auditoría Interna  
Revisión por la Dirección

#### **10. Mejora: Interpretar los Requisitos de ISO/IEC 27001**

Estructura de ISO/IEC 27001  
Recomendación  
No Conformidad y Acción Correctiva  
Mejora Continua

#### **Estructura: Caso de Negocio**

Creación Caso de Negocio

#### **Metodología: Alcance y Límite del SGSI**

Definir  
Pasos para la Definición del Alcance SGSI  
Método de las Elipses  
Diagrama Estructura Funcional  
Diagrama Planta Física  
Diagrama Planta Lógica

#### **Metodología: Gestión de Activos**

Identificación  
Clasificación y Valoración  
Analizar Activos de Información

#### **Metodología: Gestión de Riesgos**

#### **Metodología: Política SGSI**

Pasos Creación Política SGSI  
Necesidades Internas  
Necesidades Externas

Relación Necesidades  
Revisión Entrega  
Redacción Política  
Entradas para la Política  
Vista General Final  
Talleres Pareo

## Preparación para la Auditoría de Certificación

Auditoría Interna  
Auditorías Internas con Énfasis en Competencias de Auditor Líder  
Estructura de la ISO 19011:2018  
Alcance ISO 19011:2018  
Auditoría  
Tipos de Auditoría  
Criterios de Auditoría  
Evidencia de la Auditoría  
Resultados de la Auditoría  
Conclusiones de la Auditoría

## Anexo A: Normativo

Anexo A: Normativo  
Anexo A: Cláusulas, Objetivos y Controles  
A.5 Políticas de Seguridad de la Información  
A.6 Organización de la Seguridad de la Información  
A.7 Seguridad de los Recursos Humanos  
A.8 Gestión de Activos  
A.9 Control de Acceso  
A.10 Criptografía  
A.11 Seguridad Física y del Entorno  
A.12 Seguridad de las Operaciones  
A.13 Seguridad de las Comunicaciones  
A.14 Adquisición, Desarrollo y Mantenimiento de Sistemas  
A.15 Relaciones Con Los Proveedores  
A.16 Gestión de Incidentes de Seguridad de la Información  
A.17 Seguridad de la Información de la Gestión de Continuidad de Negocio  
A.18 Cumplimiento  
Bibliografía  
Acerca del Examen