

# CERTIFICACIÓN

**CertiProf**<sup>®</sup>  
Professional Knowledge

**I27001IA ISO 27001  
INTERNAL AUDITOR**

## **I27001IA ISO 27001 INTERNAL AUDITOR**

Esta certificación abarca la norma internacional publicada por la **Organización Internacional de Normalización (ISO)**, que describe cómo administrar la seguridad de la información en una empresa. La **ISO 27001** se puede implementar en cualquier tipo de organización, con o sin ánimo de lucro, privada, pequeña o grande de propiedad gubernamental. Fue escrita por los mejores expertos del mundo en el campo de la seguridad de la información y proporciona metodologías para la implementación de la gestión de seguridad de la información en una organización. También permite a las empresas obtener la certificación, lo que significa que la organización ha implementado la seguridad de la información de acuerdo a la **norma ISO 27001**.

### **Al finalizar este curso usted conocerá:**

- Como realizar una auditoría interna con base en la norma **ISO 27001**
- Aprender a gestionar un equipo implementador del **SGSI**
- Comprender la aplicación del sistema de gestión de seguridad en el contexto de la norma **ISO 27001**
- Comprender el cumplimiento de los requisitos de los diferentes participantes de la organización

# CERTIFICACIÓN

**CertiProf**<sup>®</sup>  
Professional Knowledge

**I27001IA ISO 27001  
INTERNAL AUDITOR**

## Dirigido a:

- Personas que deseen aprender a realizar auditorías de certificación de Sistema de Gestión de Seguridad de la información (**SGSI**) conforme con la **ISO/IEC 27001:2013**.
- Gerentes de proyecto que deseen dominar los procesos de auditoría de Sistemas de Gestión de Seguridad de la Información (**SGSI**).
- Personas responsables de la seguridad de la información. Miembros de un equipo de seguridad de la información.
- Consultores de Seguridad Informática

## Requisitos:

- Una comprensión fundamental de la norma **ISO/IEC 27001**

## Beneficios:

- Prevenir o minimizar el riesgo de que produzca la pérdida o sustracción de información
- Prevenir a la organización ante posibles sanciones legales derivadas de pérdida o mala gestión de la información

# CERTIFICACIÓN

**CertiProf**<sup>®</sup>  
Professional Knowledge

**I27001IA ISO 27001  
INTERNAL AUDITOR**

## Incluye:

- Manual de Participante
- Manual de Ejercicios
- Instructores Certificados
- Presencial y/o en Línea
- Exámenes muestra
- Diploma de participación
- Examen de Certificación

**Duración:** 24 hrs.

## Formato y duración del examen

**Tipo:** Opción múltiple

**Preguntas:** 40

**Puntaje de aprobación:** 24/40 o 60 %

**Duración:** 60 minutos

**Libro abierto:** No

**Entrega:** Este examen está disponible en línea

# CERTIFICACIÓN

**CertiProf**<sup>®</sup>  
Professional Knowledge

**I27001IA ISO 27001  
INTERNAL AUDITOR**

## Temario:

### Introducción y Antecedentes

- Historia de la Norma
- **ISO/IEC 27001:2013** – Estructura
- **ISO 27000** Familia de Normas

### Conceptos Claves

- 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**

### Términos y Definiciones

- Control de Acceso
- Modelo Analítico
- Ataque
- Atributo
- Auditoría
- Alcance de la Auditoría
- Autenticación
- Autenticidad

# CERTIFICACIÓN

**CertiProf**<sup>®</sup>  
Professional Knowledge

**I27001IA ISO 27001  
INTERNAL AUDITOR**

- Disponibilidad
- Medida Básica
- Competencia
- Confidencialidad
- Conformidad
- Consecuencia
- Mejora Continua
- Control
- Objetivo de Control
- Corrección
- Acción Correctiva
- Datos
- Criterios de Decisión
- Medida Derivada
- Información Documentada
- Eficacia
- Evento
- Dirección Ejecutiva
- Contexto Externo
- Gobernanza de la Seguridad de la Información
- Órgano de Gobierno

# CERTIFICACIÓN

**CertiProf**<sup>®</sup>  
Professional Knowledge

**I27001IA ISO 27001  
INTERNAL AUDITOR**

- Indicador
- Necesidades de Información
- Recursos (instalaciones) de Tratamiento de Información
- Seguridad de la Información
- Continuidad de la Seguridad de la Información
- Evento o Suceso de Seguridad de la Información
- Incidente de Seguridad de la Información
- Gestión de Incidentes de Seguridad de la Información
- Colectivo que Comparte Información
- Sistema de Información
- Integridad
- Parte Interesada
- Contexto Interno
- Proyecto del SGSI
- Nivel de Riesgo
- Probabilidad (likelihood)
- Sistema de Gestión
- Medida
- Medición
- Función de Medición

# CERTIFICACIÓN

**CertiProf®**  
Professional Knowledge

**I27001IA ISO 27001  
INTERNAL AUDITOR**

- Método de Medición
- Resultados de las Mediciones
- Supervisión, Seguimiento o Monitorización (monitoring)
- No Conformidad
- No Repudio
- Objeto
- Objetivo
- Organización
- Contratar Externamente (verbo)
- Desempeño
- Política
- Proceso
- Fiabilidad
- Requisito
- Riesgo Residual
- Revisión
- Objeto en Revisión
- Objetivo de la Revisión
- Riesgo

# CERTIFICACIÓN

**CertiProf**<sup>®</sup>  
Professional Knowledge

**I27001IA ISO 27001  
INTERNAL AUDITOR**

- Aceptación del Riesgo
- Análisis del Riesgo
- Apreciación del Riesgo
- Comunicación y Consulta del Riesgo
- Criterios de Riesgo
- Evaluación del Riesgo
- Identificación del Riesgo
- Gestión del Riesgo
- Proceso de Gestión del riesgo
- Dueño del Riesgo
- Tratamiento del Riesgo
- Escala
- Norma de Implementación de la Seguridad
- Parte Interesada
- Amenaza
- Alta Dirección
- Entidad de Confianza para la Comunicación de la Información
- Unidad de Medida
- Validación
- Verificación
- Vulnerabilidad



# CERTIFICACIÓN

**CertiProf**<sup>®</sup>  
Professional Knowledge

**I27001IA ISO 27001  
INTERNAL AUDITOR**

## Contexto de la Organización

- Comprensión de la Organización y de su Contexto
- 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

## Liderazgo

- Liderazgo y Compromiso
- Política
- Roles, Responsabilidades y Autoridades en la Organización

## Planificación

- Acciones para Tratar los Riesgos y Oportunidades
- Objetivos de Seguridad de la Información y Planificación para su Consecución

## Soporte

- Recursos
- Competencia
- Concienciación
- Comunicación
- Información Documentada

# CERTIFICACIÓN

**CertiProf**<sup>®</sup>  
Professional Knowledge

**I27001IA ISO 27001  
INTERNAL AUDITOR**

## Operación

- Planificación y Control Operacional
- Apreciación de los Riesgos de Seguridad de la Información
- Tratamiento de los Riesgos de Seguridad de la Información

## Evaluación del Desempeño

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

## Mejora

- No Conformidad y Acciones Correctivas
- Mejora Continua

## Auditoría

- Auditor
- Términos y Definiciones **ISO 19011:2011**
- Tipos
- Criterios de Auditoría
- Evidencia de la Auditoría
- Hallazgos de la Auditoría

# CERTIFICACIÓN

**CertiProf**<sup>®</sup>  
Professional Knowledge

**I27001IA ISO 27001  
INTERNAL AUDITOR**

- Conclusiones de la Auditoría
- Cliente de la Auditoría
- Auditado
- Auditor
- Equipo Auditor
- Experto Técnico
- Observador
- Guía
- Programa de Auditoría
- Alcance de la Auditoría
- Plan de Auditoría
- Riesgo
- Competencia
- Conformidad
- No Conformidad
- Sistema de Gestión

## Taller

- Programa de Auditoría
- Principios de Auditoría
- Atributos de los Auditores
- Auditoría y Evidencia

# CERTIFICACIÓN

**CertiProf**<sup>®</sup>  
Professional Knowledge

**I27001IA ISO 27001  
INTERNAL AUDITOR**

- Reunión de Apertura

## Taller

- Establecer un Programa de Auditoría
- Competencias de los Auditores
- Métodos de Auditoría Aplicables
- Objetivos de la Auditoría Interna
- Auditoría Interna Evidencia Objetiva
- Actividades de Auditoría
- Preparación de las Actividades Auditoría en Sitio
- Responsabilidades del Auditor Líder
- Responsabilidades del Co-Auditor

## Taller

- Preparación Individual del Auditor
- Plan de Auditoría
- Listas de Chequeo o Verificación
- Preguntas Claves del Auditor
- Tipo de Preguntas
- Recolección de Evidencia Objetiva

# CERTIFICACIÓN

**CertiProf**<sup>®</sup>  
Professional Knowledge

**I27001IA ISO 27001  
INTERNAL AUDITOR**

- Ejecutando la Auditoría
- Fuentes de Información
- Realización de Entrevistas
- Técnicas de Entrevista del Auditor
- Actitudes a Tomar para Controlar la Auditoría
- ¿Cómo entorpecer la Auditoría (Auditado)?
- Administración del Tiempo
- Manejo de Situaciones Difíciles
- Resultados de la Auditoría
- Tipos de Hallazgos
- Incumplimientos más Comunes

## Taller

- La Reunión de Cierre
- Dirigida por el Auditor Líder
- Informe de Auditoría
- ¿Qué no incluir en el informe de auditoría?
- Plantilla de Informe
- Acciones Correctivas
- Las Auditorías de Seguimiento

# CERTIFICACIÓN

**CertiProf**<sup>®</sup>  
Professional Knowledge

**I27001IA** ISO 27001  
INTERNAL AUDITOR

- Redacción de las No Conformidades
- Fórmula de Redacción de No Conformidades
- Fases de la Auditoría

## Conclusiones