



CURSO /TALLER AUDITOR INTERNO ISO 27001:2013



ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en cualquier tipo de empresa. La revisión más reciente de esta norma fue publicada en 2013.

Esta norma internacional se ha convertido en el principal referente a nivel mundial para la seguridad de la información. Está elaborada por reconocidos especialistas del mundo en el tema y proporciona una metodología para implementar, operar, revisar, monitorear y mejorar continuamente la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; lo cual significa que una entidad de certificación independiente, confirma que la seguridad de la información ha sido implementada con base en las mejores prácticas como lo es la norma ISO 27001.

Este curso ha sido diseñado para preparar a los participantes con los conocimientos y habilidades necesarias para evaluar e informar sobre la correcta implantación de un sistema de gestión de la seguridad de la información (SGSI) bajo la norma ISO 27001 en su última revisión correspondiente al año 2013; dando así cumplimiento al requisito 9.2 exigido por la norma para conservar la certificación.

COMPETENCIAS

Al concluir la formación usted fortalecerá sus habilidades para:

- Identificar y comprender los nuevos requisitos de la norma ISO 27001:2013 respecto a la anterior norma ISO 27001 del año 2005.
- Conocer y entender las responsabilidades del auditor interno y la función de la auditoría interna en el mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información, conforme a las normas ISO 27001 e ISO 19011.
- Planificar y preparar una auditoría interna, así como reunir pruebas válidas de auditoría mediante la observación, la entrevista y la toma de muestras de documentos y registros.
- Redactar informes de auditoría detallados que ayuden a mejorar la efectividad del sistema de Gestión de Seguridad de la Información SGSI.
- Proponer modos de verificar la eficacia de las acciones correctivas.

La formación incluye presentaciones magistrales, ejercicios prácticos y transferencia de lecciones aprendidas por el instructor en sus años de experiencia.

OBJETIVO GENERAL

Adquirir los conocimientos básicos para realizar de manera efectiva una auditoría al sistema de gestión de seguridad de la información bajo la última versión de la norma **ISO 27001:2013**.

OBJETIVOS ESPECÍFICOS

- Promover programas de capacitación al interior de la empresa con el fin de lograr mayor grado de conciencia entre los principales involucrados en la gestión de seguridad de la información. SGSI.
- Actualizar los conocimientos sobre la última revisión de la norma ISO 27001:2013, apoyado en el conocimiento del instructor quien hace parte del comité 181 de Icontec; empresa colombiana encargada de normalizar ISO 27001:2013 para Colombia.
- Dar conformidad a los requisitos de la norma, contando con personal capacitado como auditor interno en la versión actualizada ISO 27001:2013.
- Conocer lecciones aprendidas por el instructor en sus años de experiencia diseñando, implementando, liderando y auditando sistemas de gestión de seguridad de la información en reconocidas empresas internacionales.

MÓDULO 1

Introducción al Sistema de Gestión de Seguridad de la Información ISO 27001:2013

- Conceptos básicos de Seguridad de la Información.
- Introducción a la norma ISO 27001:2013 y sus principales diferencias con la versión 2005.
- Principales estándares de la familia ISO/IEC JTC 1/SC 27 - IT Security techniques
- Aspectos generales de la norma ISO 27002:2013.
- Taller: Glosario de términos ISO 27000:2014.

MÓDULO 2

Revisión y análisis de la norma ISO 27001:2013

- ✓ Taller: Modelo PHVA aplicado al Sistema de Gestión de Seguridad de la Información.
- ✓ Análisis e interpretación de los requisitos consagrados en las cláusulas 4 a 10 de la ISO 27001:2013.
- ✓ Revisión y análisis del anexo A de la norma ISO 27001:2013.
- ✓ Taller: Ejemplo práctico de una implementación real de un SGSI

MÓDULO 3

Auditoria a un Sistema de Gestión fundamentada en la norma ISO 19011:2012

- Diseño de un programa de auditoria al Sistema de Gestión de Seguridad de la Información.
- Aspectos fundamentales a ser auditados al Sistema de Gestión de Seguridad de Información.
- Principales métodos de auditoria y su aplicación dentro de la auditoria al SGSI.
- Taller: Diseño de un plan de pruebas a una selección de controles del anexo A.
- Elementos a considerar para recolectar evidencia pertinente y suficiente.
- Taller: Fundamentos generales sobre técnicas de muestreo.
- Breve reseña de herramientas de auditoria asistida por computadora CAAT
- Administración y mantenimiento de los papeles de trabajo de auditoria.

MÓDULO 4

Preparación y presentación del informe de auditoría

- Validación de las No Conformidades y oportunidades de mejora.
- Redacción de No conformidades y del informe final.
- Presentación, sustentación y distribución del informe final.
- Taller: Redacción y presentación de No conformidades evidenciadas en la auditoria

MÓDULO 5

Cierre de la capacitación

- Presentación del examen como Auditor Interno de la norma ISO 27001:2013



DURACIÓN

- 19 horas de clase.
- 1 hora de presentación de examen final

CERTIFICACIÓN

Al final del curso se entregará a las personas que aprobaron el examen final, una certificación como Auditor Interno de la Norma **ISO 27001:2013**.

En caso que el estudiante no apruebe el examen, le será expedida una constancia de asistencia al curso.

CARLOS ALFONSO RESTREPO ORAMAS

(CISA, CISM, CGEIT, CRISC, CBCP, Lead Implementer ISO 22301, ISO 27001, ISO 20000 Lead Auditor ISO 22301, ISO 27001, ISO 20000, Risk Manager ISO 31000, ITIL V3, Cobit 5).

Formador certificado por el Instituto Tecnológico de Monterrey México, con 20 años de experiencia profesional en el sector financiero colombiano; capacitando, diseñando, auditando, implementando, operando y liderando sistemas de gestión integral de riesgo y continuidad del negocio para empresas de reconocido prestigio internacional.

Carlos A. Restrepo se ha desempeñado en los últimos 17 años como: Gerente General en Restrepo&Oramas SAS, Gerente de Procesos y Riesgo en Visa_Colombia, Experto de Seguridad TI y Continuidad del Negocio en Synapsis Colombia, Consultor E.R.S en Deloitte&Touche, Jefe (e) de la Oficina de Control Interno de la hoy Superintendencia Financiera de Colombia y Director de Riesgo Operativo en IQ Outsourcing S.A".

Su capacidad de combinar conocimiento y experiencia como catedrático, consultor, auditor, implementador de Sistemas de Gestión Integral de Riesgo y Continuidad; así como ejercer su rol de Gerente de Procesos y Riesgos en VISA, le han permitido obtener las máximas calificaciones en calidad y satisfacción para la totalidad de los seminarios impartidos en México, Costa Rica, Honduras, Nicaragua, Guatemala, Panamá, República Dominicana, Colombia, Venezuela, Perú, Bolivia, Chile, Ecuador, Paraguay y Argentina.

