



# **CURSO /TALLER ACTUALIZACIÓN NORMA ISO 27001:2013 CON ÉNFASIS EN GESTIÓN DEL RIESGO ISO 31000:2009**



**ISO 27001:2013** 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 a finales de 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 internacionales como lo es, la norma ISO 27001.

Este curso ha sido diseñado para identificar y analizar los cambios producidos en la versión 2005 de la norma que originaron la nueva versión 2013, con sus controles relacionados en el anexo A; promoviendo al interior del equipo discusiones enfocadas en la interpretación de los nuevos requisitos y el posible impacto sobre el Sistema de Gestión de Seguridad de la Información SGSI implementado en la organización.

Tendremos como referencia para el desarrollo del curso, los objetivos de control y descripción detallada de su guía de implementación conforme a la norma ISO 27002:2013; sobre la cual identificaremos de manera general los principales cambios ocurridos en su versión anterior respecto a su última versión y el posible impacto sobre el Sistema de Gestión de Seguridad de la Información SGSI implementado y certificado en Nuevatel PCS de Bolivia S.A, contemplando los aspectos principales a tener en cuenta para el proceso de transición dentro del proceso de mantenimiento de la certificación ISO 27001.

Como parte integral del sistema, incluiremos un análisis y entendimiento conceptual de las diferentes fases contempladas en ISO 31000 para la gestión del riesgo, aplicado a la Tecnología de Información.

## COMPETENCIAS

Al concluir la formación usted fortalecerá sus habilidades para:

- Identificar y comprender los nuevos requisitos de la norma ISO 27001:2013 respecto al diseño, implementación, operación, mantenimiento, revisión y mejora de un Sistema de Gestión de Seguridad de la Información SGSI.
- Dimensionar el impacto de la modificación de la norma frente al Sistema de Seguridad de la Información implementado en la organización.
- Facilitar la integración de los diferentes sistemas de gestión ISO implementados en la organización.
- Fortalecer la Gestión de Riesgo teniendo como marco de referencia el estándar internacional ISO 31000.
- Evaluar el plan de trabajo que soporta la transición entre las versiones de la norma ISO 27001, contra los nuevos conceptos aprendidos.

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

## OBJETIVO GENERAL

Adquirir o fortalecer los conocimientos y habilidades necesarias para mantener y mejorar el Sistema de Gestión de Seguridad de la Información SGSI implementado en la organización de conformidad a los nuevos requisitos obligatorios de la **norma ISO 27001** en su última versión 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 e ISO 27002:2013 para Colombia.
- Dar conformidad a los requisitos de la norma, contando con personal capacitado en la versión actualizada ISO 27001:2013.
- Incrementar la competencia del equipo de trabajo de seguridad de la información, mediante la participación en este tipo de capacitaciones adquiriendo nuevos conocimientos y enterándose de experiencias reales que permitan impulsar la mejora continua en la práctica profesional.
- 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.
- Respalda el conocimiento y habilidad mediante una capacitación de actualización de la norma ISO 27001:2013, expedida por una empresa de reconocimiento internacional.
- Ajustar el Sistema de Gestión de Seguridad de la Información a los nuevos requisitos de la norma ISO 27001:2013.
- Prepararse para recibir una auditoria externa de seguridad de la información.

## 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
- ✓ Taller: Glosario de términos ISO 27000:2014
- ✓ Integración de la norma ISO 27001:2013 con otros sistemas de gestión ISO.

## 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; identificando principales diferencias respecto al anexo A de la versión 2005.
- ✓ Taller: Aspectos a tener en cuenta para la etapa de transición ISO 27001:2013

## MÓDULO 3

### Aspectos generales de la norma ISO 27002:2013

- Análisis e implementación de los principales componentes de la norma ISO 27002:2013.
- Identificación y análisis de los cambios presentados frente a la versión 2005.
- Taller: Selección de controles y su guía de implementación según ISO 27002:2013.

## MÓDULO 4

### Fundamentos de la Gestión de Riesgos conforme a la norma ISO 31000

- Presentación de los principales componentes de la norma ISO 31000
- Marco de referencia de la Norma ISO 31000
- El proceso de gestión de riesgo de la norma ISO 31000
- Fundamentos sobre apetito al riesgo.
- Taller gestión de riesgos ISO 31000 aplicado a la seguridad de la información

## MÓDULO 5

### Conclusiones y comentarios

- Resumen de las principales conclusiones logradas por el equipo de asistentes



## DURACIÓN

- 24 horas de clase/Taller.

## CERTIFICACIÓN

Al final del curso se entregará un certificado de actualización en la norma **ISO 27001:2013** con énfasis en **ISO 31000**.

 **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.



**Para mayor información por favor contáctenos  
al correo: [info@ro-sas.com](mailto:info@ro-sas.com)**