Curso / Taller Auditor Interno ISO 27001:2013 con Énfasis en Riesgos Bajo la Norma ISO 31000:2009

Código: ISO-27001-ERCA

Propuesta de Valor: ERCA

Duración: 24 Horas

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.

AUDIENCIA

- Gerentes de proyectos o consultores que desean preparar y apoyar a una organización en la implementación de un Sistema de Gestión de Seguridad de la información (SGSI).
- Auditores en seguridad de la información que deseen dominar el proceso de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI).
- Responsables de la seguridad de la información o de la conformidad de una organización con la normatividad vigente. Integrantes de un equipo de seguridad de la información.
- Asesores expertos en tecnología de la información.
- Técnicos expertos que desean prepararse en un rol en la seguridad de la información o en la gestión de un proyecto de implantación de un SGSI.

PRE REQUISITOS

- Se sugiere que el participante tenga un conocimiento previo de la norma ISO 27001:2013 y experiencia en auditoría interna.

OBJETIVOS

Objetivo General:

- Adquirir los conocimientos básicos para realizar de manera efectiva una auditoria 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.
- Fortalecer la Gestión de Riesgo teniendo como marco de referencia el estándar internacional ISO 31000.

CERTIFICACIÓN DISPONIBLE

- Al final del curso se entregará a las personas que aprobaron el examen final, un certificado de finalización exitosa del curso Auditor Interno de la Norma ISO 27001, expedido por ERCA (Registro Europeo de Auditores Certificados).
- En caso que el estudiante no apruebe el examen, le será expedida una constancia de asistencia al curso.

CONTENIDO

1. INTRODUCCIÓN AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN ISO 27001:2013

1.1. CONCEPTOS BÁSICOS DE SEGURIDAD DE LA INFORMACIÓN
1.2. INTRODUCCIÓN A LA NORMA ISO 27001:2013 Y SUS PRINCIPALES DIFERENCIAS CON LA VERSIÓN 2005
1.3. PRINCIPALES ESTÁNDARES DE LA FAMILIA ISO/IEC JTC 1/SC 27 - IT SECURITY TECHNIQUES
1.4. ASPECTOS GENERALES DE LA NORMA ISO 27002:2013
1.5. TALLER: GLOSARIO DE TÉRMINOS ISO 27000:2014

2. REVISIÓN Y ANÁLISIS DE LA NORMA ISO 27001:2013

2.1. TALLER: MODELO PHVA APLICADO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
2.2. ANÁLISIS E INTERPRETACIÓN DE LOS REQUISITOS CONSAGRADOS EN LAS CLÁUSULAS 4 A 10 DE LA ISO 27001:2013
2.3. REVISIÓN Y ANÁLISIS DEL ANEXO A DE LA NORMA ISO 27001:2013
2.4. TALLER: EJEMPLO PRÁCTICO DE UNA IMPLEMENTACIÓN REAL DE UN SGSI

3. FUNDAMENTOS DE LA GESTIÓN DE RIESGOS CONFORME A LA NORMA ISO 31000

3.1. PRESENTACIÓN DE LOS PRINCIPALES COMPONENTES DE LA NORMA ISO 31000

3.2. MARCO DE REFERENCIA DE LA NORMA ISO 31000

3.3. EL PROCESO DE GESTIÓN DE RIESGO DE LA NORMA ISO 31000

3.4. FUNDAMENTOS SOBRE APETITO AL RIESGO

4. AUDITORÍA A UN SISTEMA DE GESTIÓN FUNDAMENTADA EN LA NORMA ISO 19011:2012

4.1. DISEÑO DE UN PROGRAMA DE AUDITORÍA AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

4.2. ASPECTOS FUNDAMENTALES A SER AUDITADOS AL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN

4.3. PRINCIPALES MÉTODOS DE AUDITORÍA Y SU APLICACIÓN DENTRO DE LA AUDITORÍA AL SGSI

4.4. TALLER: DISEÑO DE UN PLAN DE PRUEBAS A UNA SELECCIÓN DE CONTROLES DEL ANEXO A

4.5. ELEMENTOS A CONSIDERAR PARA RECOLECTAR EVIDENCIA PERTINENTE Y SUFICIENTE

4.6. TALLER: FUNDAMENTOS GENERALES SOBRE TÉCNICAS DE MUESTREO

4.7. BREVE RESENA DE HERRAMIENTAS DE AUDITORÍA ASISTIDA POR COMPUTADORA CAAT

4.8. ADMINISTRACIÓN Y MANTENIMIENTO DE LOS PAPELES DE TRABAJO DE AUDITORÍA

5. PREPARACIÓN Y PRESENTACIÓN DEL INFORME DE AUDITORÍA

5.1. VALIDACIÓN DE LAS NO CONFORMIDADES Y OPORTUNIDADES DE MEJORA

5.2. REDACCIÓN DE NO CONFORMIDADES Y DEL INFORME FINAL

5.3. PRESENTACIÓN, SUSTENTACIÓN Y DISTRIBUCIÓN DEL INFORME FINAL

5.4. TALLER: REDACCIÓN Y PRESENTACIÓN DE NO CONFORMIDADES EVIDENCIADAS EN LA AUDITORÍA

6. CIERRE DE LA CAPACITACIÓN

6.1. PRESENTACIÓN DEL EXAMEN COMO AUDITOR INTERNO DE LA NORMA ISO 27001:2013

BENEFICIOS

- Al final del curso se entregará a las personas que aprobaron el examen final, un certificado de finalización exitosa del curso Auditor Interno de la Norma ISO 27001:2013, expedido por ERCA (Registro Europeo de Auditores Certificados.