Introducción:

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.

Objetivos de Aprendizaje:

- Comprender los principios, conceptos y requisitos de ISO/IEC 27001:2013.
- Identificar cómo desarrollar un SGSI.
- Desarrollar habilidades para realizar auditorías.
- Entender ISO 27001:2013 Anexo A.

Público objetivo:

Aquellas personas que necesitan conocer de qué se trata la norma ISO 27001, así como ejecuta e informar sobre una auditoría conforme con la ISO/IEC 27001:2013.

Requisitos previos:

No hay ningún requisito formal para esta certificación.

Formación:

- Código de certificación: I27001A.
- Tipo de curso: Lead Auditor.

El trabajo del curso incluye conferencias, debates, juegos de roles, ejercicios individuales y grupales para que comiences a comprender la norma ISO 27001. Después de pasar el examen de auditor ISO 27001, tendrá los conocimientos necesarios para realizar auditorías eficaces de SGSI.

Examen de certificación:

Se debe realizar un examen complementario con preguntas abiertas de forma presencial con el partner, con libro abierto, para permitir a los estudiantes demostrar su comprensión del proceso de auditoría y las responsabilidades de ser un auditor líder.

- Idiomas: Español.

Temario:

1.Introducción y Antecedentes

Introducción

Historia de la Norma

ISO/IEC 27001:2013 – Estructura

ISO 27000 Familia de Normas

2. 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

3.Términos y Definiciones (Ver Anexo)

Estructura de ISO/IEC 27001

Ciclo Deming PHVA Y SGSI

4. Contexto de la Organización

4.1 Comprensión de la Organización y de su Contexto

Taller: Determinar el Contexto de la Organización Haciendo Uso de una Matriz de Análisis FODA

4.2 Comprensión de las Necesidades y Expectativas de las Partes Interesadas

4.3 Determinación del Alcance del Sistema de Gestión de la Seguridad de la Información

4.4 Sistema de Gestión de la Seguridad de la Información

Taller: Definir el Alcance del SGSI

5. Liderazgo

5.1 Liderazgo y Compromiso

5.2 Política

5.3 Roles, Responsabilidades y Autoridades en la Organización

6. Planificación

6.1 Acciones para Tratar los Riesgos y Oportunidades

Plan de Tratamiento de Riesgos

6.1 Acciones para Tratar los Riesgos y Oportunidades

Estructura de la Norma ISO 31000 Gestión de Riesgos – Directrices

Taller: Definir Declaración de Aplicabilidad para 5 Controles del Anexo A

6.2 Objetivos de Seguridad de la Información y Planificación para su Consecución

Taller: Definir los Objetivos de Seguridad de la Información

7. Soporte

7.1 Recursos

7.2 Competencia

7.3 Concienciación

7.4 Comunicación

7.5 Información Documentada

8. Operación

8.1 Planificación y Control Operacional

8.2 Apreciación de los Riesgos de Seguridad de la Información

8.3 Tratamiento de los Riesgos de Seguridad de la Información

Evaluación y Tratamiento de Riesgos

9. Evaluación del Desempeño

9.1 Seguimiento, Medición, Análisis y Evaluación

9.2 Auditoría Interna

Auditoría

9.3 Revisión por la Dirección

10. Mejora 57

10.1 No Conformidad y Acciones Correctivas

10.2 Mejora Continua

Anexo 1: Términos y Definiciones

Taller: Revisar los Términos y Definiciones de Seguridad de la Información

3.1 Control de Acceso

3.2 Modelo Analítico

3.3 Ataque

3.4 Atributo

3.5 Auditoría

3.6 Alcance de la Auditoría

3.7 Autenticación

3.8 Autenticidad

3.9 Disponibilidad

3.10 Medida Básica

3.11 Competencia

3.12 Confidencialidad

3.13 Conformidad

3.14 Consecuencia

3.15 Mejora Continua

3.16 Control

3.17 Objetivo de Control

3.18 Corrección

3.19 Acción Correctiva

3.20 Datos

3.21 Criterios de Decisión

3.22 Medida Derivada

3.23 Información Documentada

3.24 Eficacia

3.25 Evento

3.26 Dirección Ejecutiva

3.27 Contexto Externo

3.28 Gobernanza de la Seguridad de la Información

3.29 Órgano de Gobierno

3.30 Indicador

3.31 Necesidades de Información

3.32 Recursos (instalaciones) de Tratamiento de Información

3.33 Seguridad de la Información

3.34 Continuidad de la Seguridad de la Información

3.35 Evento o Suceso de Seguridad de la Información

3.36 Incidente de Seguridad de la Información

3.37 Gestión de Incidentes de Seguridad de la Información

3.38 Colectivo que Comparte Información

3.39 Sistema de Información

3.40 Integridad

3.41 Parte Interesada

3.42 Contexto Interno

3.43 Proyecto del SGSI

3.44 Nivel de Riesgo

3.45 Probabilidad (likehood)

3.46 Sistema de Gestión

3.47 Medida

3.48 Medición

3.49 Función de Medición

3.50 Método de Medición

3.51 Resultados de las Mediciones

3.52 Supervisión, Seguimiento o Monitorización (monitoring)

3.53 No Conformidad

3.54 No Repudio

3.55 Objeto

3.56 Objetivo

3.57 Organización

3.58 Contratar Externamente (verbo)

3.59 Desempeño

3.60 Política

3.61 Proceso

3.62 Fiabilidad

3.63 Requisito

3.64 Riesgo Residual

3.65 Revisión

3.66 Objeto en Revisión

3.67 Objetivo de la Revisión

3.68 Riesgo

3.69 Aceptación del Riesgo

3.70 Análisis del Riesgo

3.71 Apreciación del Riesgo

3.72 Comunicación y Consulta del Riesgo

3.73 Criterios de Riesgo

3.74 Evaluación del Riesgo

3.75 Identificación del Riesgo

3.76 Gestión del Riesgo

3.77 Proceso de Gestión del Riesgo

3.78 Dueño del Riesgo

3.79 Tratamiento del Riesgo

3.80 Escala

3.81 Norma de Implementación de la Seguridad

3.82 Parte Interesada

3.83 Amenaza

3.84 Alta Dirección

3.85 Entidad de Confianza para la Comunicación de la Información

3.86 Unidad de Medida

3.87 Validación

3.88 Verificación

3.89 Vulnerabilidad

3.90 Información

3.91 Activo

Modulo de Auditoría ISO 19011

ISO 19011:2018

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

Cliente de la Auditoría

Auditado

Auditor

Equipo Auditor

Experto Técnico

Observador

Guía

Programa de Auditoría

Alcance de la Auditoría

Plan de Auditoría

Conformidad

No Conformidad

Pruebas de Auditoria

Métodos de Auditoría

Cláusula 4: Principios de Auditoría

Cláusula 7: Competencia y Evaluación de los Auditores

Métodos para Evaluar a los Auditores

Cláusula 7: Atributos Personales

Cláusula 7: Conocimientos Genéricos y Habilidades

Cláusula 5: Programa de Auditoría

Establecimiento de Objetivos del Programa de Auditoría

Determinación y Evaluación de Riesgos y Oportunidades del Programa de Auditoría

Establecimiento del Programa de Auditoría

Competencia de (los) Individuo(s) que Gestiona(n) el Programa de Auditoría

Establecer el Alcance del Programa de Auditoría

Determinar los Recursos del Programa de Auditoría

Implementación del Programa de Auditoría

Definición de Objetivos, Alcance y Criterios para una Auditoría Individual

Selección y Determinación de Métodos de Auditoría

Selección de los Miembros del Equipo de Auditoría

Asignación de Responsabilidades al Líder del Equipo Auditor para una Auditoría Individual

Gestión de los Resultados del Programa de Auditoría

Administrar y Mantener los Registros del Programa de Auditoría

Revisión y Mejora del Programa de Auditoría

Cláusula 6: Actividades de la Auditoría

Establecer Contacto con el Auditado

Determinación de la Viabilidad de la Auditoría

Realizar Revisión de Información Documentada

Planificación de Auditoría

Taller 1

Taller 2

Cláusula 6: Actividades de la Auditoría

Asignación de Tareas al Equipo Auditor

Funciones y Responsabilidades de Guías y Observadores

Preparación de los Documentos de Trabajos

Posibles Ventajas de las Listas de Verificación

Uso de las Listas de Verificación

Taller 3

Reunión de Apertura 110 Revisión de la Documentación en la Auditoría

Comunicación Durante la Auditoría

Métodos para Recopilar Información

La Entrevista

Preguntas Claves del Auditor

Tipo de Preguntas

Ejecutando la Auditoría

Realización de Entrevistas

¿Cómo entorpecer la Auditoría (Auditado)?

Administración del Tiempo

Manejo de Situaciones Difíciles 115 Resultados de la Auditoría

Tipos de Hallazgo

Incumplimientos Más Comunes

Redacción de las No Conformidades

Fórmula de Redacción de No Conformidades

Conclusiones de Auditoría

Informe de Auditoría

Reunión de Cierre

Preparación y Distribución del Informe de Auditoría

Realización de Seguimiento de Auditoría

Las Auditorías de Seguimiento

Taller 4

Conclusiones

Conclusiones