



ExecuTrain

Impulsamos tu talento tecnológico



MICROSOFT

RED HAT

VIRTUALIZACIÓN

CIBERSEGURIDAD

DESARROLLO

OFFICE

BIG DATA

BLOCK CHAIN

BASES DE DATOS

GESTIÓN DE
SERVICIOS IT

CLOUD
COMPUTING

METODOLOGÍAS
EN PROYECTOS

SISTEMAS
OPERATIVOS

Y MÁS...



www.executrain.com.mx



¿Por qué ExecuTrain?

ExecuTrain es un proveedor de entrenamiento corporativo a nivel internacional y líder mundial en la capacitación empresarial. Contamos con más de 30 años de Experiencia y con más de 75 mil personas capacitadas a nivel Nacional.

Te guiamos en la definición de tus requerimientos de capacitación, en las diferentes etapas:

- ✓ Detección de necesidades, evaluación de conocimientos, plan de capacitación y seguimiento posterior para elegir el plan de capacitación como tú lo necesitas.
- ✓ El **más amplio catálogo de cursos**, desde un nivel básico hasta los niveles de conocimientos más especializados.
- ✓ En ExecuTrain el material y la **metodología están diseñados por expertos en aprendizaje humano**. Lo que te garantiza un mejor conocimiento en menor tiempo.
- ✓ Tú puedes confiar y estar seguro del aprendizaje porque nuestro **staff de instructores es de primer nivel**, algunos de los cuales son consultores en reconocidas empresas.
- ✓ No pierdas tu tiempo, los cursos están diseñados para un aprendizaje práctico.

Nuestro compromiso es que tú aprendas, si no quedas satisfecho con los resultados del programa, podrás volver a tomar los cursos hasta tu entera satisfacción o la devolución de tu dinero.

Modalidad de Servicio



Cursos en Fecha Calendario

Súmate a nuestros grupos en fechas públicas.



Cursos Privados

On site, en nuestras instalaciones o en línea con instructor en vivo.



Autoestudio con soporte de instructor

Cursos en modalidad autoestudio, con acceso 24/7 a la plataforma de estudio, con soporte de instructor y foros de ayuda

ISO/IEC 27001:2022 Auditor Líder

Este curso intensivo permite a los participantes desarrollar las habilidades necesarias para auditar Sistemas de Gestión de Seguridad de la Información (SGSI) y para dirigir equipos de auditores, mediante la aplicación de principios, procedimientos y técnicas de auditoría, ampliamente reconocidos.

Durante este curso, los participantes adquirirán los conocimientos y las herramientas necesarias para planificar y realizar auditorías internas y externas de acuerdo con el proceso de certificación de la norma ISO/IEC 27001:2022. Sobre la base de ejercicios prácticos, los participantes desarrollarán las habilidades (dominio de técnicas de auditoría) y competencias (gestión de equipos de auditoría y programa de auditoría, comunicación con los clientes, resolución de conflictos, etc.) necesarias para llevar a cabo una auditoría de manera eficiente.

Esta formación se complementa también con la norma ISO 19011:2018 para auditar sistemas de gestión elaborada para la auditar cualquier sistema ISO.

Perfil del Público

- Auditores Internos o que quieran liderar auditorías de certificación de Sistemas de Gestión de Seguridad de la Información (SGSI).
- Los gerentes de proyecto o consultores que quieren dominar los procesos de auditoría de Sistemas de Gestión de Seguridad de la Información (SGSI).
- Las personas responsables de la Seguridad de la Información o de la conformidad de una organización.
- Los miembros de un equipo de seguridad de la información, ciberseguridad, privacidad y protección de datos, la continuidad del negocio.
- Asesores expertos en Tecnología de la Información.
- Los técnicos expertos que desean prepararse para asumir cargos de auditores de la seguridad de la información.
- Interesados en cumplir con requerimientos regulatorios (nacionales/internacionales) basados en la seguridad de la información.

Objetivos

Los principales objetivos de este curso son los siguientes:

- Adquirir los conocimientos necesarios para realizar una auditoría interna de la norma ISO 27001 como se especifica en la norma ISO 19011.
- Adquirir los conocimientos necesarios para realizar una auditoría de certificación ISO 27001 como se especifica en las normas ISO 19011, ISO 17021 e ISO 27006.
- Adquirir los conocimientos necesarios para gestionar un equipo de auditoría SGSI.
- Comprender la aplicación del sistema de gestión de seguridad en el contexto de la norma ISO 27001.
- Comprender la relación entre un Sistema de Gestión de Seguridad, incluida la Gestión de Riesgos, controles y el cumplimiento de los requisitos de los diferentes participantes de la organización.
- Mejorar la capacidad de analizar el entorno interno y externo de una organización, la evaluación de riesgos y auditoría de la toma de decisiones en el contexto de un SGSI.
- Preparar al participante para el examen de certificación ISO 27001 Auditor Líder.



Prerrequisitos

Se recomienda tener conocimientos básicos de ISO 27001, ISO 27002, conceptos de seguridad de la información, ciberseguridad. Es recomendable tener conocimientos de riesgos tecnológicos, amenazas y controles de seguridad. Aunque no es requisito, es deseable conocer la norma ISO 19011 o estar familiarizado con conceptos de auditoría de sistemas.



Temario

El curso cubre los temas para el examen de certificación de la norma internacional ISO/IEC 27001 como Auditor Líder, el cual abarca lo siguiente:

Día 1: Introducción a la gestión de un Sistema de Gestión de Seguridad (SGSI) basado en ISO 27001

- Marco normativo y jurídico sobre seguridad de la información.
- Principios fundamentales de la seguridad de la información.
- El proceso de certificación ISO 27001.
- El Sistema de Gestión de Seguridad de la Información (SGSI).
- La presentación detallada de los capítulos 4 a 10 de la norma ISO27001.

Día 2: Planificación y lanzamiento de una auditoría de ISO 27001

- Los conceptos y principios fundamentales de auditoría.
- Enfoque de la auditoría basada en la evidencia y en riesgo.
- Elaboración de una auditoría de certificación ISO 27001.
- La documentación de una auditoría SGSI.

- Llevar a cabo una sesión de apertura.

Día 3: La realización de una auditoría de ISO 27001

- La comunicación durante la auditoría.
- Auditoría de los procedimientos: observación, revisión de documentos, entrevistas, técnicas de muestreo, la verificación técnica, la corroboración y evaluación.
- Elaboración de planes de prueba.
- Formulación de los resultados de auditoría.
- Elaboración de informes de no conformidad.

Día 4: Conclusiones y asegurar el seguimiento de una auditoría de ISO27001

- Auditoría de la documentación.
- Estudio de calidad.
- Llevar a cabo una reunión de cierre y conclusión de una auditoría de ISO 27001.
- Evaluación de los planes de acción correctiva
- Auditoría de vigilancia según ISO 27001.
- Programa de gestión de auditorías.
- La auditoría interna y auditoría de segunda parte.

Día 5: Examen de Certificación



Materiales y Recursos Adicionales

- Materiales del curso
- Caso de Estudio de Seguridad de la Información
- Cuaderno de ejercicios
- Certificado de asistencia al curso
- Examen de certificación ISO 27001 Auditor Líder



Nuevos Conocimientos

Los nuevos conocimientos adquiridos en el curso serán:

- Nuevas normas y marcos de auditoría de seguridad de la información.

- Conocimiento de la norma ISO 19011.
- Metodología para la auditoría de la norma ISO 27001.
- Conceptos clave de un Sistema de Gestión de Seguridad de la Información (SGSI).
- Profundizar conceptos de Auditoría de la Seguridad de la Información



Nuevas Capacidades

Al finalizar el curso el participante:

- Comprenderá la importancia de la seguridad de la información y las amenazas tecnológicas en su organización.
- Incrementará sus habilidades como Auditor de la norma ISO 27001.
- Llevará a cabo una Auditoría para un sistema de Gestión de Seguridad de la Información.
- Entenderá los procedimientos y acciones a llevar a cabo durante una auditoría.
- Realizará entrevistas y comunicar resultados de Auditoría según principios aceptados.
- Desarrollará técnicas de observación, levantamiento de información, hallazgos entrevistas y validaciones necesarias en una auditoría.
- Desarrollará acciones posteriores de seguimiento y corrección de no conformidades después de una auditoría.
- Entenderá cómo mitigar riesgos y aplicar controles correctivos asociados a la seguridad de la información, la ciberseguridad y la protección y privacidad de datos.