ISO/IEC 27032 Lead Cybersecurity Manager

Duración: 35 horas

Código: ISO-27032

Descripción:

La capacitación ISO / IEC 27032 Lead Cybersecurity Manager le permite adquirir la experiencia y la competencia necesarias para ayudar a una organización en la implementación y administración de un programa de seguridad cibernética basado en el marco de seguridad cibernética ISO / IEC 27032 y NIST. Durante este curso de capacitación, obtendrá un conocimiento exhaustivo de seguridad cibernética, la relación entre seguridad cibernética y otros tipos de seguridad de TI, y el rol de las partes interesadas en ciberseguridad.

Después de dominar todos los conceptos necesarios de seguridad cibernética, puede presentarse para el examen y solicitar una credencial de "Administrador certificado de ciberseguridad con certificación ISO / IEC 27032 de PECB". Con la celebración de un Certificado de PECB Lead Cybersecurity Manager, podrá demostrar que posee el conocimiento práctico y las capacidades profesionales para apoyar y liderar a un equipo en el manejo de la Ciberseguridad.

Professional Evaluation and Certification Board (PECB) es una certificadora canadiense quién ofrece servicios de certificación para sistemas de gestión, productos y personal.

Objetivos de Aprendizaje:

- Adquirir un conocimiento exhaustivo sobre los elementos y las operaciones de un programa de seguridad cibernética de conformidad con ISO / IEC 27032 y el marco de ciberseguridad del NIST
- Reconozca la correlación entre ISO 27032, el marco de seguridad cibernética del NIST y otras normas y marcos operativos
- Dominar los conceptos, enfoques, estándares, métodos y técnicas utilizados para establecer, implementar y administrar con eficacia un programa de Ciberseguridad dentro de una organización
- Aprenda a interpretar las pautas de ISO / IEC 27032 en el contexto específico de una organización
- Dominar la experiencia necesaria para planificar, implementar, administrar, controlar y mantener un programa de ciberseguridad como se especifica en ISO / IEC 27032 y el marco de seguridad cibernética del NIST
- Adquiera la experiencia necesaria para asesorar a una organización sobre las mejores prácticas para administrar la Ciberseguridad

Audiencia:

Este curso está dirigido a:

- Profesionales de ciberseguridad
- Expertos en seguridad de la información
- Profesionales que buscan administrar un programa de seguridad cibernética
- Personas responsables de desarrollar un programa de seguridad cibernética
- Especialistas en TI
- Asesores expertos en tecnología de la información
- Profesionales de TI que buscan mejorar sus habilidades técnicas y conocimientos

Prerrequisitos:

Una comprensión fundamental de ISO / IEC 27032 y conocimiento integral de Ciberseguridad.

Enfoque Educativo:

- Esta capacitación se basa tanto en la teoría como en las mejores prácticas utilizadas en la implementación y gestión de un programa de ciberseguridad
- Las sesiones de conferencia se ilustran con ejemplos basados en estudios de casos
- Los ejercicios prácticos se basan en un estudio de caso que incluye juegos de roles y discusiones
- Las pruebas prácticas son similares al examen de certificación

Examen y Certificación:

El examen "PECB Certified ISO / IEC 27032 Lead Cybersecurity Manager" cumple completamente los requisitos del Programa de Certificación y Examen PECB (ECP). El examen cubre los siguientes dominios de competencia:

- Dominio 1: Principios fundamentales y conceptos de ciberseguridad
- Dominio 2: Roles y responsabilidades de los interesados
- Dominio 3: Gestión del riesgo de ciberseguridad
- Dominio 4: Mecanismos de ataque y controles de seguridad cibernética
- Dominio 5: intercambio de información y coordinación
- Dominio 6: Programa Integrador de Ciberseguridad en la Gestión de Continuidad del Negocio
- Dominio 7: Gestión de incidentes de ciberseguridad y medición del rendimiento

Contenido:

1. Introducción a la ciberseguridad y conceptos relacionados según lo recomendado por ISO / IEC 27032.
    1. Objetivos y estructura del curso.
    2. Estándares y marcos regulatorios
    3. Conceptos fundamentales en ciberseguridad
    4. Programa de ciberseguridad
    5. Iniciando un programa de Ciberseguridad
    6. Analizando la organización
    7. Liderazgo
2. Políticas de ciberseguridad, gestión de riesgos y mecanismos de ataque.
    1. Políticas de seguridad cibernética
    2. Gestión de riesgos de ciberseguridad
    3. Mecanismos de ataque
3. Controles de seguridad cibernética, intercambio de información y coordinación.
    1. Controles de ciberseguridad
    2. Intercambio de información y coordinación
    3. Programa de formación y sensibilización.
4. Gestión de incidentes, monitoreo y mejora continua.
    1. Continuidad del negocio
    2. Gestión de incidentes de ciberseguridad
    3. Respuesta y recuperación de incidentes de ciberseguridad
    4. Pruebas en ciberseguridad
    5. Medición del desempeño
    6. Mejora continua
    7. Cerrando el ciclo
5. Examen de certificación.

Costos:

Este costo incluye:

- El precio del examen.
- Manual que contiene información y ejemplos prácticos.
- Certificado de participación de 31 CPE (Continuing Professional Education)
- Refrigerios e impuestos de ley.