TEMARIO DEL CURSO

Lead Cybersecurity Professional (LCSPC™)

15 horas

OBJETIVOS DEL CURSO

- Comprender los conceptos fundamentales de la ciberseguridad y el ecosistema del ciberespacio.
- Aplicar el Marco de Ciberseguridad del NIST (versión 1.1) para proteger sistemas, redes y programas.
- Identificar amenazas, vectores de ataque y vulnerabilidades en entornos digitales.
- Establecer y mejorar programas de ciberseguridad dentro de la organización.
- Comunicar los requisitos de ciberseguridad a las partes interesadas y tomar decisiones de compra informadas.
- Preparar al alumno para superar el examen oficial Lead Cybersecurity Professional Certificate (LCSPC™) de CertiProf.

A QUIÉN VA DIRIGIDO

- Profesionales de TI; responsables de seguridad; directivos; perfiles de gestión que deban comunicar riesgos y tomar decisiones sobre ciberseguridad.

EL CURSO INCLUYE

- Manuales digitales
- Diploma de asistencia
- Tramitación de FUNDAE incluida

TEMARIO

MÓDULO 01.

— Conceptos fundamentales de ciberseguridad

- Explicación básica del ciberespacio: definición, actores y principios fundamentales.
- Los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad (triada CIA).
- Diferencias entre seguridad de la información, seguridad informática y ciberseguridad.
- Dominio de la seguridad: seguridad en Internet, seguridad web y seguridad de red.

MÓDULO 02.

— Descripción general de la ciberseguridad

- El panorama actual de las amenazas cibernéticas: tendencias y evolución.
- Tipos de ciberataques: virus, gusanos, troyanos, ransomware, phishing, ingeniería social.
- Vectores de ataque y superficie de ataque.
- Vulnerabilidades comunes en sistemas y aplicaciones.
- Gestión de riesgos en Internet: identificación, evaluación y mitigación.

MÓDULO 03.

— ISO/IEC 27032 — Ciberseguridad

- Introducción al estándar ISO/IEC 27032 y su aplicación en ciberseguridad.
- Roles y responsabilidades de las partes interesadas en el ciberespacio.
- Importancia de la colaboración internacional y multisectorial en la gestión de incidentes.

MÓDULO 04.

— Introducción al Marco de Ciberseguridad del NIST (CSF 1.1)

- Estructura y componentes del Framework: Funciones, Categorías y Subcategorías.
- Las cinco funciones principales del NIST CSF: Identificar, Proteger, Detectar, Responder y Recuperar.
- Niveles de implementación del Framework (Tiers): parcial, riesgo informado, repetible y adaptativo.
- Perfiles del Framework: perfil actual vs. perfil objetivo.

MÓDULO 05.

— Revisión básica de prácticas de ciberseguridad

- Prácticas esenciales de ciberseguridad para individuos y organizaciones.
- Higiene cibernética: gestión de contraseñas, actualizaciones, autenticación multifactor.
- Seguridad en el puesto de trabajo y en entornos remotos.
- Protección de datos personales y corporativos.

MÓDULO 06.

— Establecimiento o mejora de un programa de ciberseguridad

- Pasos para crear o mejorar un programa de ciberseguridad usando el NIST CSF.
- Priorización de actividades de ciberseguridad según el riesgo organizacional.
- Fomento de una cultura de ciberseguridad dentro de la organización.
- Integración de la ciberseguridad en los procesos de negocio.