TEMARIO DEL CURSO

Cybersecurity Foundation Professional (CSFPC™)

15 horas

La ciberseguridad es un componente crítico en cualquier organización moderna. Este curso proporciona una visión estructurada de los fundamentos técnicos, organizativos y normativos de la seguridad digital.

EL CURSO INCLUYE

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

TEMARIO

MÓDULO 01.

NIST – Ciberseguridad para Negocios Pequeños

- Objetivos de ciberseguridad: Confidencialidad, Integridad, Disponibilidad.
- Amenazas comunes: Phishing, Ransomware, Hacking.
- Identificación y valoración de activos.
- Marco de trabajo NIST:
- Identificar
- Proteger
- Detectar
- Responder
- Recuperar

MÓDULO 02.

CyBOK – Fundamentos de Ciberseguridad

- Definición de ciberseguridad.
- Áreas de conocimiento CyBOK.
- Principios y temas interdisciplinarios.
- Ciberespacio y sistemas de gestión de protección.

MÓDULO 03.
Gestión de Riesgos

- Concepto de riesgo.
- Evaluación y gestión del riesgo cibernético.
- Gobernanza del riesgo.
- Cultura y comunicación de seguridad.
- Métodos de evaluación.
- Métricas de seguridad.
- Continuidad del negocio.
- ISO/IEC 27035.
- Sistemas ciberfísicos y tecnología operativa.

MÓDULO 04.
Ley y Regulación

- Fundamentos legales.
- Jurisdicción y soberanía de datos.
- Protección de datos y privacidad.
- Delitos informáticos.
- Responsabilidad civil y penal.
- Propiedad intelectual.
- Ética y códigos de conducta.
- Gestión del riesgo legal.

MÓDULO 05.
Factores Humanos

- Capacidades y limitaciones humanas.
- Seguridad utilizable.
- Error humano.
- Conciencia y educación.
- APIs y bibliotecas criptográficas utilizables.

MÓDULO 06.
Privacidad y Derechos en Línea

- Definiciones de privacidad.
- Privacidad como confidencialidad, control y transparencia.
- Tecnologías de privacidad.
- Ingeniería y evaluación de privacidad.

MÓDULO 07.
Malware y Tecnologías de Ataque

- Taxonomía del malware.
- Cyber Kill Chain.
- Análisis estático y dinámico.
- Técnicas de evasión.
- Detección basada en ML.
- Respuesta y atribución.

MÓDULO 08.
Comportamiento Adverso

- Tipos de adversarios.
- Modelos de operación maliciosa.
- Árboles de ataque.
- Criminología ambiental.
- Atribución.

MÓDULO 09.

Operaciones de Seguridad y Gestión de Incidentes

- Modelo MAPE-K.
- Arquitectura SOC.
- SIEM.
- Detección de intrusiones.
- Correlación de eventos.
- Ciclo de vida de gestión de incidentes.