Diploma en CIBERSEGURIDAD

Comienzo 3 de Junio

CURSO ONLINE

CEI
CARRERAS CORTAS Y
CURSOS DE ESPECIALIZACIÓN

Objetivos Generales

Brindar formación sobre técnicas, habilidades y metodologías aplicadas para la identificación,evaluación y mitigación de riesgos, así como para garantizar la confidencialidad, integridad y disponibilidad de la información.
Capacitando para:

- ✓ Formar parte activa en equipos multidisciplinarios participando en proyectos de ciberseguridad.
- ✓ Desarrollar habilidades analíticas y críticas que permitan la adaptación de los profesionalesen ciberseguridad al permanente cambio tecnológico.
- ✓ Desarrollar proyectos de investigación en ciberseguridad que respondan a las necesidadesdel contexto.
- ✓ Operar y administrar sistemas informáticos siguiendo las buenas prácticas de ciberseguridad.
- ✓ Diseñar y operar arquitecturas de sistemas seguros.
- ✓ Incluir la ciberseguridad en el ciclo de desarrollo

Metodología:

Dictado totalmente en línea. Clases teórico-prácticas para aplicar los temas abordados. Se realizarán ejercicios que requiere de los estudiantes trabajen en equipo.

Tel: 42232209 Whatsapp 099100234
Info@cei.edu.uy www.cei.edu.uy

CEI
CARRERAS CORTAS Y
CURSOS DE ESPECIALIZACIÓN

Dirigido a:

Universitarios, técnicos y estudiantes avanzados de carreras de Informática o afines, quedeseen implementar la ciberseguridad en diversas disciplinas.
Profesionales interesados en fortalecer sus conocimientos de ciberseguridad y ser capacesde proteger sus instalaciones de amenazas de ciberataques.
Personal de TI y áreas afines del sector público o privado que buscan comprender los riesgosde la seguridad de la información en el entorno digital.
Desarrolladores que deseen incluir ciberseguridad en el ciclo de desarrollo.

Requisitos:

Cada estudiante deberá concurrir con su propia notebook con los siguientes requisitos mínimos paraque puedan correr las herramientas a utilizar en los prácticos:

Procesador i3 o similar
8GB de memoria
Al menos 20GB de espacio en disco.
Virtualización habilitada en la BIOS.

Contenido curricular y resumen temático

La propuesta educativa brinda formación en técnicas, herramientas y metodologías para implementar, gestionar y operar la ciberseguridad de manera transversal en la organización.

Módulo 1.- Seguridad de Sistemas Informáticos (24hs)

Objetivos específicos: Brindar un marco teórico sobre los conceptos de confidencialidad,integridad y disponibilidad. Comprender de forma integral la gestión de ciberseguridad brindando una base teórica sobre los aspectos técnicos que engloban los sistemas informáticos.

Programa:

- Principios generales de ciberseguridad
- Normativa local e internacional
- Controles de seguridad
- Programas de concienciación
- Gestión de Riesgos
- Criptografía
- Modelo OSI – TCP/IP
- Introducción a Redes de datos

Módulo 2.- Respuesta de Incidentes e Introducción al Hacking Ético (32hs)

Objetivos específicos: Conocer las diversas tácticas, técnicas y procedimientos (TTPs) utilizadas por los atacantes para poder brindar servicios profesionales de hacking ético o pentesting.Además, brindar las herramientas y un marco teórico-práctico para la respuesta a incidentes e investigación forense.

Programa:

- Introducción al hacking y ética hacker
- Respuesta ante incidentes
- Investigación de fuentes abiertas (OSINT)
- Ingeniería social
- Metodologías
- Fases y tipos de ataque
- Framework MITRE
- Hacking de aplicaciones web
- Hacking Windows
- Hacking Linux/Unix
- Hacking WiFi
- Reporte de descubrimientos y planes de remediación

Módulo 3.- Desarrollo Seguro de Software (24hs)

Objetivos específicos: Brindar conocimientos sobre técnicas y buenas prácticas de desarrollo seguro de software y arquitectura en diversos ambientes (web, cloud, móvil) mediante eluso de metodologías y frameworks para la prevención de fallos de seguridad.

Programa:

- Conceptos de seguridad en el software
- Ciclo de vida del software y SDLC
- Taxonomía de vulnerabilidades
- Modelado de amenazas
- Seguridad en requerimientos
- Seguridad en diseño
- Seguridad en codificación
- Prácticas criptográficas
- Desarrollo y herramientas de software seguro

Módulo 4.- Arquitectura de Seguridad (24hs)

Objetivos específicos: Conocer las diversas soluciones de seguridad para defensa, reacción y recuperación. Brindar la perspectiva de un administrador / operador de SOC en la gestiónde herramientas de seguridad tanto cloud como on-premise. Consolidar las bases para

una arquitectura segura.

Programa:

- Arquitectura y diseño de seguridad
- Continuidad del negocio y recuperación
- Dispositivos IoT
- Seguridad perimetral
- Arquitectura de seguridad de red (Firewalls, VPN, WAF, etc.)
- Virtualización y contenedores
- Antimalware
- SIEM

Evaluación
Asistencia mínima del 70%.
El curso se evalúa con un EXAMEN FINAL.

Certificado
Diploma en Ciberseguridad
UNIVERSIDAD CLAEH

Duración
104 horas.

Horario:
Jueves de 18:30 a 22:30.

Comienzo:
Jueves 3 de Junio de 2021.

Descuentos:
25% de Descuento Egresados, Alumnos y Ex Alumnos.

POR CONSULTAS E INCRIPCIONES

Tel: 42232209
Whatsapp 099100234
Info@cei.edu.uy
www.cei.edu.uy