

Experto Universitario en Hacking Etico (Ethical Hacking)

Información General

Fecha de inicio: 23/06/2026

Frecuencia: Semanal

Carga horaria por clase: 90 min

Presentación

La generalización y expansión del uso de las tecnologías, telecomunicaciones e informática en los diferentes contextos empresariales, académicos, personales y públicos, hacen de las TICs una base común para todas nuestras actividades. Esta plataforma además de ser mantenida en su funcionamiento, debe ser protegida con el fin de controlar que los activos informáticos no sean presa de ataques, fraudes o mal uso por los delincuentes informáticos, empleados desleales o terceros mal intencionados. El entendimiento de la seguridad informática en la práctica comprende entender las plataformas existentes en el mercado, la administración de las mismas, y asegurarlas. Así también es de interés riguroso el monitoreo de vulnerabilidades o debilidades, posibles riesgos, y como mitigarlos. Permitiendo conocer sobre técnicas de intrusión, chequeos de seguridad, modalidad de ataques y defensa. Área, campo o disciplinas de conocimiento del curso: Telecomunicaciones Administración de Servidores Administración de Redes de Datos Seguridad Informática Computación Ethical Hacking

Objetivos Generales

Aprendan a desarrollar el plan estratégico de seguridad requerido por la organización. Adquieran los conocimientos sobre los elementos tecnológicos, redes y servidores de datos que generan un impacto de valor en la organización. Obtengan los conocimientos necesarios para la obtención de la certificación internacional de seguridad CISSP. Obtengan los conocimientos necesarios para rendir satisfactoriamente los exámenes de las siguientes certificaciones oficiales: Instalación y configuración de Windows Server 2019/2022/2025 ISC2 Certified Information Systems Security Professional.

Objetivos Específicos

- Conozcan sobre los sistemas criptográficos y sus aplicaciones prácticas existentes, abordando sus vulnerabilidades más comunes y los potenciales ataques y amenazas.
- Aprendan a planear, diseñar, estructurar e implementar una infraestructura de red informática de manera segura, protegiéndola de potenciales amenazas.
- Conozcan las herramientas esenciales y las buenas prácticas necesarias para obtener el nivel máximo de seguridad en una red de servidores de arquitectura Microsoft Windows Server ó Linux Server, protegiéndola de potenciales amenazas.
- Conozcan los conceptos básicos referentes a la implementación, configuración, mantenimiento y soporte de servidores de infraestructura en tecnologías Windows o Linux.

- Conozcan sobre el mundo de los servidores informáticos, existentes en toda infraestructura informática de mediana y alta gama.
- Aprendan a armar, configurar y administrar una pequeña red fácilmente.
- Conozcan los conceptos generales de las redes de comunicación, los protocolos, los diferentes dispositivos y sus funciones.
- Conozcan las herramientas y metodologías necesarias para realizar tareas de análisis de vulnerabilidades y tests de penetración, con una filosofía enfocada a la ética profesional.
- Aprendan sobre los conceptos del mundo del Hacking

Destinatarios

- Administradores de sistemas, técnicos informáticos, administradores de redes, y analistas, consultores, desarrolladores y auditores de seguridad.

Plan de Estudios

Módulo 1: Diseño de Redes Seguras

- Introducción a las redes informáticas
- Instalación y Configuración de redes
- Redes informáticas potenciales riesgos
- Redes informáticas seguridad aplicada

Módulo 2: Administración de Servidores

- Introducción a los servidores informáticos / Roles y Funciones
- Conociendo Linux (Práctica-Lab)
- Instalando y configurando nuestro servidor (Práctica-Lab).
- Soporte, mantenimiento y solución de problemas (Práctica-Lab).

Módulo 3: Hardening (Windows Servers ó Linux Servers)

- Introducción a implementaciones de seguridad
- Configuraciones y Servicios (Parte 1)
- Configuraciones y Servicios (Parte 2)
- Seguridad Aplicada

Módulo 4: Ethical Hacking

- Introducción sobre el Ethical Hacking
- Metodos de Control de Vulnerabilidades
- Introducción sobre Criptografía
- Introducción sobre un Pentesting
- Reconocimiento Pasivo y Activo
- Vulnerability Scanning (Explicación y Práctica-Lab)
- Ingeniería Social
- Seguridad Wireless / Mobile
- System Hacking (Explicación y Práctica-Lab)/ Denegación de Servicio

- Password Cracking (Explicación y Práctica-Lab) / Phishing / Pharming (Explicación y Práctica-Lab)
- Cross-Site scripting / SQL Injection (Explicación y Práctica-Lab)
- Repaso general cursada Ethical Hacking

Bibliografía

- Hacking: The Art of Exploitation — Jon “Smibbs” Erickson — No Starch Press — 2ª edición (2008) Wikipedia ISBN: 978—1593271442 (común para edición 2ª)
- Hacking ético — José Luis Berenguel Gómez & Pablo Esteban Sánchez — Paraninfo — Edición en español (año según edición local) paraninfo.com.ar ISBN: 978—8428362672
- CEH v12 Certified Ethical Hacker Study Guide — Dale?Meredith — Packt Pub / O'Reilly — Edición correspondiente a CEH v12 (publicado recientemente) O'Reilly Media ISBN: 978—1801813099
- CEH v11 Certified Ethical Hacker Study Guide — Ric?Messier — Sybex Inc — Publicado 2021 book1.es ISBN: 978—1119800286
- Certified Ethical Hacker (CEH) Preparation - Guide Ahmed?Sheikh — Apress - 1ª edición (2021) SpringerLink Softcover ISBN: 978—1—4842—7257—2; eBook ISBN: 978—1—4842—7258—9
- CEH Certified Ethical Hacker Cert Guide Michael?Gregg & Omar?Santos — Pearson IT Certification 5ª edición (2026) pearsonitcertification.com ISBN—13: 978—0—13—548579—8

UTN.BA Campus Online — Universidad Tecnológica Nacional, Facultad Regional Buenos Aires

Mozart 2300, C1407 CABA, Argentina • +54 11 4867-7500 • campus@frba.utn.edu.ar

Documento generado el 23/07/2026 09:38 • UUID: d9287f00-681d-4ed6-97ab-45a8cc465695