Avanzado - Ciberseguridad

PROGRAMA DE ESTUDIOS:
CIBERSEGURIDAD AVANZADA

KOICA

HANDONG GLOBAL UNIVERSITY

CIT

UNA

PROGRAMA DE ESTUDIO
CIBERSEGURIDAD AVANZADA

Avanzado - Ciberseguridad

Para empezar el curso:

1

Es necesario que el estudiante tenga conocimientos avanzados de programación.

2

El estudiante debe contar con una computadora y conexión a internet.

3

Manejo básico de PC para configurar herramientas necesarias para el curso.

Información Esencial:

Inversión	Pago único de 450.000 Gs.
Inicio	7 de abril del 2026.
Duración	8 semanas (40 horas totales).
Carga Horaria	5 horas semanales: Clases virtuales e interactivas.
Horario	Martes, 19:00 a 21:30 (Síncrona) Jueves, (Asíncrona)
Modalidad	100% Online / Sincrónico a través de la plataforma EDUCA.

PROGRAMA DE ESTUDIO
CIBERSEGURIDAD AVANZADA

Avanzado - Ciberseguridad

Este curso de Ciberseguridad Avanzada está orientado a profesionales que desean profundizar en tácticas, técnicas y procedimientos utilizados tanto por equipos ofensivos (Red Team) como defensivos (Blue Team).
La metodología se basa en el enfoque “Learning by Doing”, utilizando laboratorios especializados, simulaciones de ataques reales y desafíos tipo Capture The Flag (CTF).
Los estudiantes trabajarán con herramientas de análisis forense, hacking ético, explotación de vulnerabilidades web, seguridad en la nube, protección de infraestructuras críticas (IoT/SCADA) y seguridad en Inteligencia Artificial.
Además, se abordarán aspectos legales y éticos, preparando al estudiante para la gestión integral de incidentes y la defensa proactiva ante amenazas avanzadas (APT).

Objetivos del curso

- Ejecutar simulaciones de ataques avanzados y diseñar estrategias de defensa resilientes.
- Analizar amenazas persistentes avanzadas (APT) utilizando marcos como MITRE ATT&CK.
- Implementar arquitecturas Zero Trust y técnicas de defensa en profundidad.
- Aplicar metodologías de respuesta a incidentes y forense digital.
- Fortalecer la capacidad de detección y monitoreo, mediante el uso de herramientas de análisis de tráfico.
- Evaluar vulnerabilidades en tecnologías emergentes, incluyendo entornos cloud, IoT e Inteligencia Artificial.

Objetivos específicos

ANÁLISIS
Identificar tácticas y vectores de ataque mediante inteligencia de amenazas.

DEFENSA
Diseñar arquitecturas seguras basadas en Zero Trust y monitoreo avanzado.

EXPLOTACIÓN
Ejecutar pruebas de penetración en aplicaciones web, bases de datos y entornos cloud.

RESPUESTA
Aplicar procesos de gestión de incidentes y análisis forense digital.

Perfil del egresado

El egresado será capaz de analizar amenazas complejas, ejecutar pruebas de penetración avanzadas y diseñar estrategias de defensa resilientes en infraestructuras híbridas. Tendrá competencias para desempeñarse en equipos Red Team, Blue Team o SOC, aplicando marcos internacionales y principios éticos en la gestión de incidentes de seguridad.

Plantel Docente

El Prof. MSc. Chrystian Ruiz Diaz es Magíster en Tecnologías de la Información y la Comunicación, con una sólida formación tanto técnica como pedagógica.
Desde el año 2021 se desempeña como docente universitario en asignaturas vinculadas a la Seguridad TICs y la ciberseguridad, habiendo formado parte de instituciones como la UCSA, la FPUNA y UPA.
Cuenta con más de 19 años de experiencia en la ANDE, donde se ha especializado en automatización, sistemas SCADA y ciberseguridad industrial

Prof. MSc. Chrystian Ruiz Diaz

PROGRAMA DE ESTUDIO
CIBERSEGURIDAD AVANZADA

Avanzado - Ciberseguridad

Cronograma

Semana	Módulo	Enfoque Principal
Semana 1	Ciberguerra y APTs	Inteligencia de amenazas + CTF
Semana 2	Defensa de Red y Zero Trust	Análisis de tráfico y DPI
Semana 3	Compromiso de Identidad	Active Directory y Kerberos
Semana 4	Seguridad Cloud y Contenedores	Auditoría e IAM
Semana 5	Inyección SQL y Exfiltración	Laboratorio sqli-labs
Semana 6	Infraestructuras Críticas	Seguridad OT
Semana 7	Transfer Learning	Uso de modelos preentrenados (VGG, ResNet) y fine-tuning.
Semana 8	Examen Final	Evaluación integral teóric práctica del curso.

PROGRAMA DE ESTUDIO
CIBERSEGURIDAD AVANZADA

Avanzado - Ciberseguridad

Contenido del curso

Ciberguerra y Amenazas Avanzadas

APTs, MITRE ATT&CK, inteligencia de amenazas y técnicas de evasión.

Seguridad de Redes e Identidad

DPI, Zero Trust, Active Directory, Kerberos y ataques de identidad.

Explotación Web y Cloud

Inyección SQL, análisis de contenedores, auditoría cloud e IAM.

Tecnologías Emergentes y Forense

Seguridad en IoT, SCADA, IA adversarial y análisis forense avanzado.

Fundamentos: *Principios de defensa en profundidad, criptografía aplicada, análisis de vulnerabilidades, gestión de incidentes, marcos internacionales de ciberseguridad y ética profesional.*

Colecciones: *Uso de plataformas CTFd, servidores sqli-labs, máquinas virtuales con Kali Linux, análisis de tráfico con Wireshark, herramientas de pentesting y forense como Volatility.*

Distribución de la Calificación y Condiciones para Aprobar

La evaluación del curso se basa en un enfoque práctico:

Participación en foros (10%): Aportes técnicos en debates y análisis.
Trabajos prácticos y laboratorios (40%): Resolución de retos CTF y ejercicios técnicos.
Proyecto final (50%): Desarrollo y defensa de un proyecto integrador.

Requerimientos mínimos en cada módulo:

Asistencia: Participación en clases síncronas y cumplimiento de actividades en plataforma.
Calificación Mínima: Alcanzar el porcentaje mínimo establecido en las evaluaciones.
Certificación: Cumplir con los requisitos académicos para la emisión del certificado.

cit.pol.una.py