

Intermedio - Ciberseguridad

PROGRAMA DE ESTUDIOS: SEGURIDAD DE REDES Y EN LA NUBE



KOICA

IFU HANDONG GLOBAL
UNIVERSITY



UNA

Para empezar el curso:

1

Conocimientos previos en lenguajes de Programación.

2

Disponer de PC/servidor con conexión a internet

3

Capacidad para configurar entornos virtuales de prueba y simuladores.

Información Esencial:

Inversión Pago único de 450.000 Gs.

Inicio 29 de septiembre del 2026

Duración 8 semanas (40 horas totales).

Carga Horaria 5 horas semanales: Clases virtuales e interactivas.

Horario Martes - 18:00 a 21:00 h (Clases sincrónicas)
Jueves - 18:00 a 20:00 h (Clases asincrónicas)

Modalidad 100% Online / Sincrónico a través de la plataforma EDUCA.

El curso está diseñado para explorar las teorías fundamentales y las estrategias prácticas necesarias para proteger los sistemas en red modernos y los servicios basados en la nube. A partir de una combinación de conocimientos teóricos y habilidades prácticas, el programa enfatiza el uso de herramientas de ciberseguridad, evaluaciones de vulnerabilidad y la implementación de controles en entornos simulador e infraestructuras corporativas. El curso abarca desde la seguridad en infraestructura de redes y sistemas Linux hasta la gestión de seguridad en la nube (IAM, cifrado, cumplimiento normativo) y tecnologías emergentes, preparando a los estudiantes para diseñar, implementar y evaluar marcos de seguridad integrales.



Objetivos del curso

- Comprender los conceptos fundamentales de la arquitectura de red y la computación en la nube (IaaS, PaaS, SaaS).
- Identificar y evaluar riesgos de seguridad y vulnerabilidades en infraestructuras tradicionales y entornos cloud.
- Aplicar tecnologías de cifrado, protocolos de comunicación seguros y mecanismos de control de acceso (RBAC).
- Implementar medidas de seguridad perimetral, firewalls, proxies y detección/prevencción de intrusiones.
- CDiseñar políticas de seguridad y evaluar el cumplimiento normativo e implicaciones éticas/legales.

Objetivos específicos



REDES

Configurar y asegurar infraestructuras de red y sistemas operativos Linux.



ESCANEEO

Identificar amenazas y vulnerabilidades mediante herramientas especializadas.



SEGURIDAD

Implementar controles de seguridad, IAM y cifrado en entornos Cloud y contenedores.



CUMPLIMIENTO

Diseñar políticas de seguridad y configurar firewalls, proxies, NAT y VPNs.



Perfil del egresado

El egresado del curso de Seguridad de Redes y en la Nube será capaz de diseñar, evaluar e implementar soluciones de seguridad en arquitecturas de red y servicios cloud. Podrá identificar y mitigar vulnerabilidades utilizando herramientas estándar de la industria, configurar seguridad perimetral (firewalls, proxies, VPNs) y administrar accesos e identidades en entornos de red y la nube. Además, estará capacitado para elaborar políticas de seguridad y auditar el cumplimiento normativo respetando los marcos legales y éticos de la ciberseguridad.

Plantel Docente

Docente e investigador del Centro de Innovación TIC de la Facultad Politécnica de la Universidad Nacional de Asunción (FPUNA), en el marco de la cooperación internacional con KOICA ISU y Handong Global University.

Profesional especializado en ciberseguridad, seguridad en redes, infraestructuras en la nube y administración de sistemas Linux, con amplia trayectoria en la implementación de controles de seguridad, gestión de vulnerabilidades y políticas de seguridad informática.

Además, se enfoca en la formación académica y técnica orientada a la resolución de problemas reales, promoviendo el uso de herramientas especializadas.



Prof. Ing. Alberto Capli

Cronograma

Semana	Módulo	Enfoque Principal
Semana 1	Fundamentos de la Nube	Modelos de servicio e introducción a Docker y contenedores.
Semana 2	Seguridad en Redes y Linux	VLANs, ACLs en Packet Tracer y hardening básico en Linux .
Semana 3	Amenazas y Vulnerabilidades	Escaneo e identificación con Nmap, Dirb, OWASP ZAP, iptables y SELinux.
Semana 4	Monitoreo y Examen Parcial	Prácticas con SIEM y Examen Parcial Teórico/Práctico.
Semana 5	Seguridad Cloud	Controles de acceso, SSH seguro, cifrado SSL/TLS, copias de seguridad y pruebas de estrés.
Semana 6	Políticas y Cumplimiento	Análisis y redacción de políticas de seguridad, CIS Controls y políticas de acceso.
Semana 7	Seguridad Perimetral	Configuración de firewalls, Proxies, NAT y conexiones VPN.
Semana 8	Evaluación Final	Examen Final teórico integrador y presentación del Proyecto Final.

Contenido del curso

Seguridad en Infraestructura y Linux

Segmentación de red (VLANs, ACLs), aseguramiento de sistemas Linux, permisos, SSH seguro y firewalls básicos.

Gestión de Vulnerabilidades

Análisis de amenazas con Nmap, Dirb, OWASP ZAP, escaneo con OpenVAS y monitoreo de eventos de seguridad con SIEM Wazuh.

Seguridad en la Nube y Cifrado

Implementación de SSL/TLS, gestión de claves, copias de seguridad automatizadas y políticas de seguridad en la nube.

Automatización y Hardening de Sistemas

Desarrollo de scripts para la automatización de auditorías, análisis de registros (logs), verificación de integridad y bastionamiento (hardening) de servidores y servicios.

Fundamentos: Modelos de servicio (IaaS, PaaS, SaaS), arquitectura cloud y despliegue básico con Docker y Kubernetes.

Colecciones: Manejo y procesamiento de datos con colecciones, tuplas y manipulación de archivos y estructuras de registros para la gestión y análisis de información de seguridad.

Distribución de la Calificación y Condiciones para Aprobar

La evaluación del curso se basa en un enfoque práctico:

Actividades y Tareas (Plataforma): Resolución de problemas propuestos y participación en foros de debate dentro de la plataforma EDUCA para reforzar los conceptos teóricos.

Evaluación Final: Examen integral estructurado para evaluar la comprensión de conceptos, teorías y la capacidad práctica.

Requerimientos mínimos en cada módulo:

Asistencia: Participación activa en las sesiones síncronas de Google Meet y seguimiento de las actividades asíncronas en la plataforma.

Calificación Mínima: Obtener un rendimiento superior al 70% en la evaluación final del curso.

Certificación: El cumplimiento del porcentaje mínimo de calificación es requisito indispensable para la expedición del certificado de finalización.



cit.pol.una.py

