Básico - Ciberseguridad

PROGRAMA DE ESTUDIOS:

INTRODUCCIÓN A LA CIBERSEGURIDAD

KOICA HANDONG GLOBAL UNIVERSITY CIT UNA

PROGRAMA DE ESTUDIOS

INTRODUCCIÓN A LA CIBERSEGURIDAD

Básico

Para empezar el curso:

1

Orientado a estudiantes que deseen iniciarse en la protección de sistemas. Se requiere un conocimiento básico 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	23de junio del 2026.
Duración	8 semanas (40 horas totales).
Carga Horaria	5 horas semanales: Clases virtuales e interactivas.
Horario	Martes y Jueves de 19:00 a 21:30 h.
Modalidad	100% Online / Sincrónico a través de la plataforma EDUCA.

PROGRAMA DE ESTUDIOS
INTRODUCCIÓN A LA CIBERSEGURIDAD

Básico

Este curso ofrece una introducción fundamental al mundo de la ciberseguridad y la seguridad de redes. A lo largo del programa, se abordarán desde los tipos de amenazas y ataques comunes hasta las estrategias básicas para mitigar riesgos en entornos digitales. Los participantes aprenderán mediante ejercicios aplicados y sesiones de laboratorio con herramientas estándar del sector como Kali Linux. Se explorarán temas de actualidad como la seguridad en la nube, la protección en dispositivos IoT y el uso de inteligencia artificial en la ciberdefensa.
Asimismo, el programa profundiza en la importancia de la gestión de identidades y el control de acceso, dotando a los estudiantes de criterios sólidos para la implementación de políticas de seguridad robustas y protocolos de respuesta.

Objetivos del curso

- Comprender los conceptos fundamentales de amenazas, vulnerabilidades y riesgos.
- Reconocer los principales tipos de ciberataques y sus mecanismos de acción.
- Aplicar protocolos y buenas prácticas de seguridad para proteger datos y redes.
- Utilizar herramientas básicas para la detección y mitigación de riesgos digitales.
- Analizar tendencias emergentes y reflexionar sobre marcos éticos y legales.

Objetivos específicos

COMPRENDER
Conceptos esenciales de amenazas y riesgos.

IDENTIFICAR
Los principales tipos de ciberataques y sus vectores de ejecución.

APLICAR
Protocolos y buenas prácticas para la protección de datos y redes.

UTILIZAR
Herramientas técnicas para la detección y mitigación de riesgos digitales.

Perfil del egresado

El egresado será capaz de identificar y prevenir amenazas cibernéticas, aplicando medidas de protección y valorando los aspectos éticos del entorno digital. Tendrá competencias básicas para manejar herramientas de análisis de vulnerabilidades y estará preparado para continuar su formación en áreas avanzadas de la ciberseguridad.

Básico

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

Cronograma

Semana	Módulo	Enfoque Principal
Semana 1	Fundamentos y Amenazas I	Tríada CIA y conceptos base.
Semana 2	Fundamentos y Amenazas II	Tipos de ataques y escaneo.
Semana 3	Arquitecturas y Criptografía I	Redes seguras y firewalls.
Semana 4	Arquitecturas y Criptografía II	Cifrado y gestión de claves.
Semana 5	Gestión de Incidentes	Planes de respuesta y acción.
Semana 6	Seguridad en Aplicaciones	OWASP y desarrollo seguro.
Semana 7	Tendencias y Ética	Nube, IoT y leyes nacionales.
Semana 8	Examen Final	Proyecto integrador y cierre.

Básico

Contenido del curso

Planificación y Estrategia de Defensa

Se enfoca en el diseño de infraestructuras seguras y la identificación proactiva de activos críticos para anticipar amenazas.

Accesibilidad y Gestión de Identidades

Garantiza que solo los usuarios autorizados accedan a la información, manteniendo la disponibilidad y la integridad de los servicios.

Ejecución y Operaciones de Seguridad

Implementación técnica de herramientas y scripts para la detección y mitigación de ataques en tiempo real.

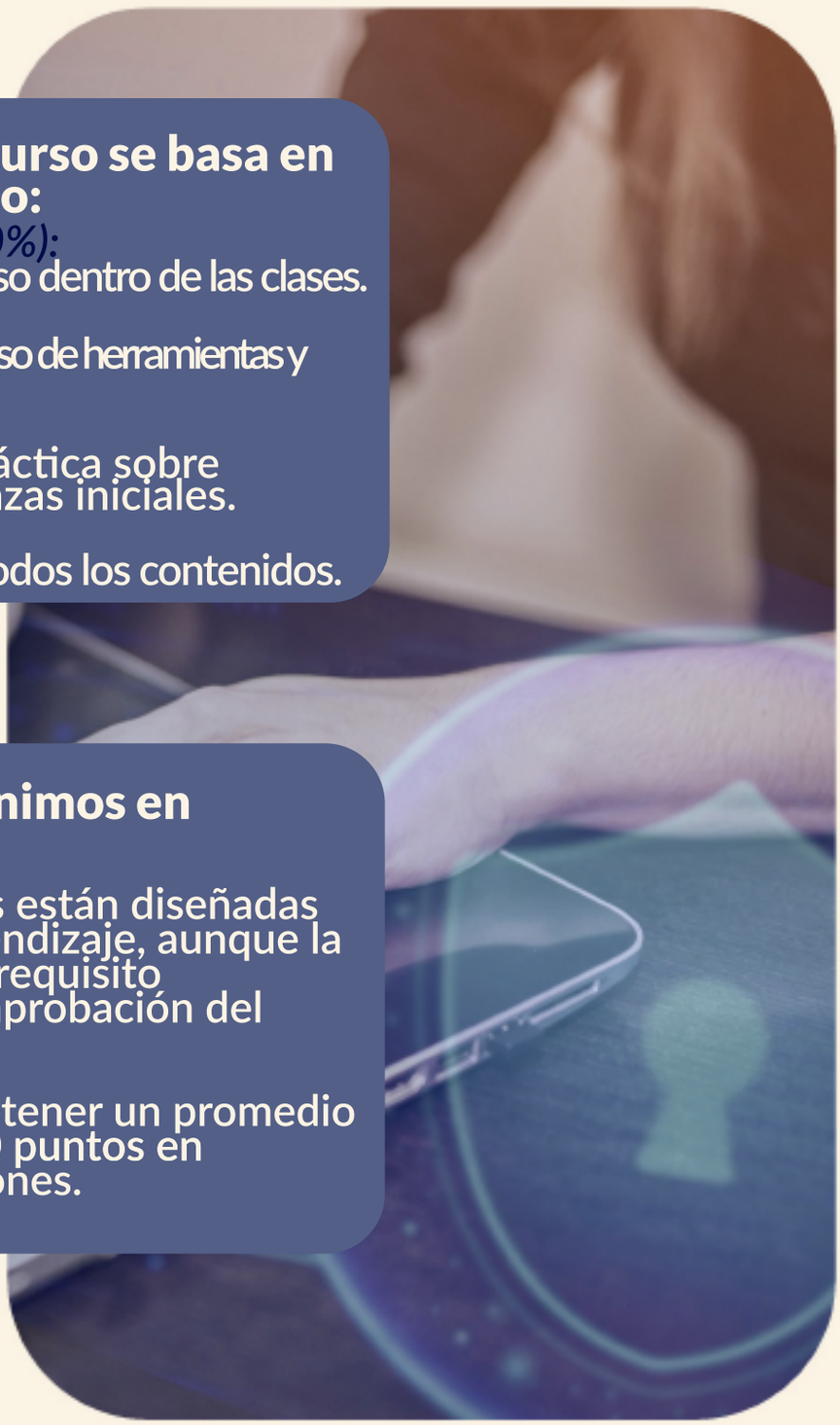
Análisis y Ciberinteligencia

Evaluación profunda de vulnerabilidades y datos de seguridad para fortalecer la postura defensiva de la organización.

Fundamentos: *Introducción a la Tríada CIA (Confidencialidad, Integridad y Disponibilidad) y el modelo de Defensa en Profundidad.*

Colecciones: *Uso y manejo de colecciones de herramientas dentro del entorno de Kali Linux.*

Distribución de la Calificación y Condiciones para Aprobar



La evaluación del curso se basa en un enfoque práctico:

Participación activa (10%):
Intervención y compromiso dentro de las clases.

Tareas prácticas (30%):
Desarrollo de laboratorios, uso de herramientas y ejercicios aplicados.

Examen parcial (30%):
Evaluación teórico-práctica sobre fundamentos y amenazas iniciales.

Examen final (30%):
Evaluación integral de todos los contenidos.

Requerimientos mínimos en cada módulo:

Asistencia: Las sesiones están diseñadas para enriquecer el aprendizaje, aunque la participación no es un requisito condicionante para la aprobación del curso.

Calificación Mínima: Obtener un promedio final superior a 70/100 puntos en el total de las evaluaciones.

cit.pol.una.py