Técnico en **Ciberseguridad** METODOLOGÍA ONLINE

Adquirí conocimientos y herramientas prácticas de las principales técnicas de seguridad en la información, actuando proactivamente antes las necesidades de esta área.

Te ofrecemos 5 módulos bimestrales + Certificación CompTIA Security+ (SYO-701)

- **MÓDULO 1 -** Implementación de Seguridad de red.
- **MÓDULO 2 -** Amenazas y ataques informáticos.
- **MÓDULO 3 -** Seguridad del Host y servicios de red.
- **MÓDULO 4 -** Administración y manejo del riesgo.
- **MÓDULO 5 -** Criptografía – Preparación examen de certificación

800-ULATINA | ulatina.ac.cr

CompTIA.

UNIVERSIDAD LATINA DE COSTA RICA
POWERED BY Arizona State University

Técnico en
Ciberseguridad

Este programa de especialización, bajo la Certificación CompTIA Security+ (SYO-701), le permitirá al estudiante obtener los conocimientos acerca de las principales tecnologías relacionadas con la seguridad de la información, capacitándole para actuar proactivamente antes los problemas emergentes en esta área, planteando distintas respuestas alternativas y anticipando posibles resultados que permitan seleccionar la respuesta más efectiva ante las amenazas de seguridad más actuales.

MÓDULO 1: **IMPLEMENTACIÓN DE SEGURIDAD DE RED.**
- Fundamentos de CiberSeguridad.
- Introducción a la Seguridad de red, protocolos y estándares.
- Seguridad de la infraestructura de red, dispositivos de seguridad en redes como: IDS / HIDS / NIDS, Honeypots y Honeynets, web application FW y network Firewalls.
- Seguridad de Red Avanzada: Conceptos acerca de protección

avanzada de malware (AMP), sistema de prevención de intrusiones de próxima generación (NGIPS)y firewalls de próxima generación (NGN,UMTS).
- Encripción a nivel de capa de transporte (SSL, TLS).
- Redes Inalámbricas: amenazas y aplicación de seguridad.

MÓDULO 2: **AMENAZAS Y ATAQUES INFORMÁTICOS**
- Definición de un ataque y tipos de atacantes.
- Identificar amenazas a la seguridad:
- Amenazas basadas en la red
- Amenazas basadas en aplicaciones y servicios
- Seguridad redes inalámbricas
- Pruebas de Penetración
- Identificar vulnerabilidades, evaluar e implementar pruebas de penetración.
- Principios acerca de Ethical Hacking

MÓDULO 3: **SEGURIDAD DEL HOST Y SERVICIOS DE RED.**
- Manejo de Seguridad de los Datos, Asegurando los datos.
- Seguridad del host (End Point), Seguridad en sistemas operativos servidores.
- Seguridad a nivel de las aplicaciones (Desarrollo Software)
- Seguridad en bases de Datos.
- Gestión de Identidad, control de acceso y autenticación.

MÓDULO 4: **ADMINISTRACIÓN Y MANEJO DEL RIESGO**
- Concepto del Riesgo
- Análisis de Riesgos y verificación de vulnerabilidades
- Analizar el impacto del riesgo en el negocio-Cálculo matemático del riesgo.
- Políticas de Seguridad.
- Seguridad Física.
- Planeamiento de desastres y recuperación: Continuidad del negocio, tolerancia a fallas, recuperación y respuesta a incidentes.

MÓDULO 5: **CRIPTOGRAFÍA – PREPARACIÓN DE EXAMEN DE CERTIFICACIÓN**
- Principios de criptografía.
- Public Key Infrastructure (PKI), estándares y protocolos.
- Algoritmos de encriptación.
- Encriptación simétrica y asimétrica.
- Aplicaciones de la Criptografía: firmas digitales, autentificación e integridad, criptografía en aplicaciones y certificados digitales.
- Seguridad aplicada en Cloud y virtualización
- Preparación examen de certificación CompTIA Security + (SYO-701)

Requisito de ingreso: Noveno año.

CompTIA®

FACULTAD DE INGENIERÍAS Y TICs
UNIVERSIDAD LATINA DE COSTA RICA

UNIVERSIDAD LATINA DE COSTA RICA
POWERED BY Arizona State University