



Horario y Duración del Postgrado

Horario: Lunes, Miércoles y Viernes de 6:00 pm a 9:00 pm

Inicia el 18 de Agosto y Finaliza 26 de Noviembre 2010

Duración: 120 horas presenciales

Inversión: US\$ 1,800.00

Forma de Pago

Al inscribirse al postgrado se debe pagar el 40% del costo de este y el restante se pagarán en cuatro cuotas mensuales.

El valor del curso incluye la entrega del Diploma, material didáctico y refrigerio.

****Consulte además, los planes de financiamiento***

Matrículas disponibles desde Julio 2010

Cupo Limitado

Mayor información

Lic. Raquel Hurtado

raquel.hurtado@uam.edu.ni

Tel.: 2278-3800 ext.: 5334/5415/5407



UNIVERSIDAD AMERICANA

PROGRAMA DE:

**POSTGRADO DE SEGURIDAD EN
REDES DE COMUNICACIÓN DE DATOS**

I. Introducción

El conocimiento informático y los sistemas digitales han probado sobradamente su utilidad como herramienta de apoyo en numerosas áreas del saber. Un área de conocimiento emergente, como es la seguridad informática de redes no debería ser una excepción.

El desarrollo de las arquitecturas telemáticas que hoy gestionan servicios de vital importancia para el avance de la sociedad y su continuo funcionamiento, se tiene que beneficiar de metodología y conocimiento aplicado para asegurar el correcto y fiable comportamiento de dichos servicios.

El postgrado pretende transmitir el conocimiento y el correcto uso de herramientas que faciliten el análisis de riesgo de la información y protección de la continuidad del negocio que empresas e instituciones pueden demandar con el objeto de mejorar la seguridad de las infraestructuras informáticas que nos rodean.

II. Objetivo General:

Desarrollar un nuevo perfil de profesional que, haciendo uso de las tecnologías digitales y sus aplicaciones concretas, así como de sus conocimientos de seguridad informática, pueda detectar, subsanar y predecir fisuras de seguridad informática.

Elaborar planes de contingencia y dar respuesta a una amplia y creciente necesidad en el mundo empresarial y de las instituciones de proteger y resguardar la información sensible o confidencial que se manejan en las empresas.

III. Objetivos Específicos

- Desarrollar políticas de seguridad confiables contra riesgos en la red
- Configurar Routers de la periferia con las características del software IOS
- Configurar firewalls basados en el IOS para desarrollar operaciones de seguridad en la red
- Configurar VPNs Site-to Site usando las características del IOS
- Configurar IPS en routers
- Configurar dispositivos LAN para controlar accesos, resistir ataques, protección de los dispositivos y tráfico fluyente.
- Administrar de manera eficiente y segura las redes corporativas
- Identificar los diferentes tipos de ataques de la red
- Aplicar técnicas y metodologías de mitigación para la seguridad de la redes

IV. Plan de Estudios

El Plan de estudios del Postgrado está compuesto por 4 módulos:

Módulo I: Seguridad en dispositivos de redes

Módulo II: Métodos de seguridad con AAA y tecnología firewall

Módulo III: Implementación de tecnologías de seguridad

Módulo IV: Implementación de seguridad en redes virtuales

V. Dirigido a:

El posgrado está dirigido a los profesionales egresados de las carreras de Ingeniería en Sistemas, Telecomunicaciones, Licenciatura en Informática, profesionales que se dediquen a la actividad de administración de redes y asesoramiento de servicios de Tecnologías de la Información, Comunicación y profesionales que hayan cruzado el Curso de CCNA.

VI. Metodología Docente

La metodología de trabajo es activa y participativa para conseguir una integración entre a teoría y la práctica y así potenciar las dos vertientes. Se proponen casos reales y ejercicios prácticos para poder resolver en grupos de trabajo y se realizaran aplicaciones y simulaciones de diferentes temas tratados en los distintos módulos.

VII. Facilitadores:

El curso estará impartido por destacados docentes que poseen sólida formación académica, amplia experiencia profesional y con acreditación CISCO.