UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN

SECRETARÍA GENERAL
EXÁMENES PROFESIONALES

TELECOMUNICACIONES

OBJETIVO

Proporcionar al participante un alto nivel de conocimientos, en el diseño, instalación y operación de un sistema de Telecomunicaciones para redes LAN, WAN e INTERNET.

DIRIGIDO A

Alumnos que quieran fortalecer su competencia profesional profundizando en un área específica y prefieran una opción de cursos escolarizados con fecha certera de terminación.

MÓDULO I

REDES DE DATOS

Objetivo: Establecer las bases generales para el óptimo entendimiento de las redes de cómputo y de las telecomunicaciones, así como la operación de los principales estándares y los equipos que intervienen.

1. Origen y evolución de las redes de telecomunicaciones.
   - 1.1. Conceptos básicos
2. Redes de computadoras
3. Componentes de una red de datos
   - 3.1.Conceptos básicos de una red de datos
   - 3.2.Clasificación
   - 3.3. Redes de Área Local (LAN´s)
     - 3.3.1. Definición de Redes LAN
     - 3.3.2. Tipos de redes LAN
     - 3.3.3. Estándares LAN
   - 3.4.Redes de Área Amplia (WAN´s)
     - 3.4.1. Definición de una red WAN
     - 3.4.2. Tipos de redes WAN
     - 3.4.3. Estándares WAN
4. Características generales del Modelo OSI
5. Transmisión de datos
   - 5.1. Clasificación de medios de transmisión
   - 5.2.Cable coaxial, par de cobre y sus aplicaciones
   - 5.3.Tecnologías DSL
   - 5.4.Fibra óptica y sus aplicaciones
   - 5.5.Sistemas satelitales y sus aplicaciones
6. Protocolos
   - 6.1. Definición de protocolos
   - 6.2.Clasificación de protocolos
7. Switcheo
8. Ruteo
9. Administración de redes
10. Historia reciente de las Telecomunicaciones en México
    - 10.1. La privatización de TELMEX
    - 10.2. La evolución de los servicios 1990-96
11. Marco Jurídico de las telecomunicaciones en México
    - 11.1. Marco legal básico de las telecomunicaciones
    - 11.2. Ley de las Vías Generales de Comunicación
    - 11.3. Elementos de la Ley Federal de Telecomunicaciones
    - 11.4. Reglamento de telecomunicaciones
    - 11.5. Ley Federal de Competencia y mercado de Telecomunicaciones

Duración: 40 horas.

MÓDULO II

TCP/IP

Objetivo: Proveer al participante de los conocimientos y herramientas necesarias para diseñar, integrar y configurar Internetworks en ambientes heterogéneos basadas en el protocolo de internet TCP/IP.

1. Arquitectura de TCP/IPv4
   - 1.1. Definición y conceptos básicos
   - 1.2. Antecedentes históricos
   - 1.3. Arquitectura de TCP/ IP
   - 1.4. Modelo DoD
   - 1.5. Protocolos capa 2: IP, ARP,ICMP,Bootp, otros.
   - 1.6. Protocolos capa 3: TCP,UDP
   - 1.7. Protocolos capa aplicaciones
   - 1.8. Estructura y monitoreo de paquetes
   - 1.9. Utilerías y herramientas de mantenimiento
2. Classfull IP Addressing
   - 2.1.Direcciones IP y máscara de redes
   - 2.2.Subnetting y Supernetting
3. Classless Inter- Domain Rounting
   - 3.1.VLM´s
   - 3.2.Resolución de problemas de direccionamiento
4. Introducción al IP Rounting
   - 4.1. Ruteo estático y elaboración de tablas de ruteo
   - 4.2. Ruteo dinámico
   - 4.3. Implementación de protocolos de ruteo
   - 4.4.Configuración de ruteadores Linux/ Microsoft
   - 4.5.Troubleshooting
5. Introducción a IPv6
   - 5.1. Historia de Ipv6 y los antecedentes e Ipv5
   - 5.2. Network ardes translation

5.3. Características de Ipv6
5.4. Seguridad

Duración: 40 horas.

MÓDULO III

TECNOLOGÍAS DE CONECTIVIDAD EN REDES

Objetivo: Adquirir los conocimientos necesarios para el diseño e implantación de Redes informáticas.

1. Dispositivos de Interconexión
2. Revisión de modelo OSI
3. Infraestructura para redes de datos
   - 3.1 Cobre
   - 3.2 Fibra óptica
   - 3.3 Inalámbricos
4. Integración de estándares LAN/WAN
   - 4.1 Medios de transmisión
   - 4.2 Estándares
5. Equipos activos de redes
   - 5.1 Switches
   - 5.2 Routers
   - 5.3 Otros
6. Diseño de redes
   - 6.1 Medios de transmisión
   - 6.2 Tecnologías
7. Caso práctico

Duración: 40 horas.

MÓDULO IV

SEGURIDAD EN REDES

Objetivo: Proporcionar al asistente los conocimientos para la impresión, implementación y administración de la seguridad en redes de datos.

1. Fundamentos de seguridad en redes
   - 1.1 Introducción a la seguridad en cómputo
   - 1.2 Tipos de seguridad
2. Seguridad en red
   - 2.1 Direcciones IP y direcciones de Internet
     - 2.1.1 Direcciones de Internet clásicas
     - 2.1.2 Enrutamiento (routing)
     - 2.1.3 Nombres de host
     - 2.1.4 Clientes y servidores
   - 2.2 Servicios
     - 2.2.1 FTP
     - 2.2.2 TFTP
     - 2.2.3 Correo electrónico
     - 2.2.4 WEB
     - 2.2.5 Conexión segura (secure shell)
   - 2.3 Implicaciones de seguridad de los servicios de red
   - 2.4 Medidas de seguridad de los servicios de red
     - 2.4.1 Mantener el sistema operativo y las aplicaciones actualizadas
     - 2.4.2 Proporcionar solo los servicios indispensables
     - 2.4.3 Mecanismos de autentificación de usuarios
     - 2.4.4 Definición de permisos de objetos
     - 2.4.5 Identificar y habilitar mecanismos de registro del sistema
     - 2.4.6 Respaldos
     - 2.4.7 Restringir el acceso físico
3. Seguridad física
   - 3.1 El plan de seguridad
     - 3.1.1. Protegiendo el hardware
     - 3.1.2. El ambiente
     - 3.1.3. Previniendo accidentes
     - 3.1.4. Acceso físico
4. Mecanismos de seguridad
   - 4.1 Políticas, estándares y procedimientos
     - 4.1.1. Políticas
     - 4.1.2. Estándares
     - 4.1.3. Procedimientos
     - 4.1.4. Diferencias entre políticas y procedimientos
   - 4.2 Firewall
     - 4.2.1. Introducción a los firewalls
     - 4.2.2. Firewalls internos
     - 4.2.3. Componentes de un firewall
     - 4.2.4. Planeación de la configuración
     - 4.2.5. ¿Qué puede hacer un firewall?
     - 4.2.6. ¿Qué no puede hacer un firewall?
     - 4.2.7. Tipos de firewalls
     - 4.2.8. Configuración de firewalls
   - 4.3 Cifrado
     - 4.3.1. Sistema de cifrado simétrico
     - 4.3.2. Sistema de cifrado asimétrico
     - 4.3.3. Ventajas del cifrado
     - 4.3.4. Aplicaciones
   - 4.4 Monitoreo
     - 4.4.1. Servicios
     - 4.4.2. Usuarios
     - 4.4.3. Procesos
     - 4.4.4. Sistemas de archivos
     - 4.4.5. Memoria
   - 4.5 Respaldos
     - 4.5.1. Introducción a los respaldos
     - 4.5.2. ¿Por qué son importantes los respaldos?
     - 4.5.3. ¿Qué se debe respaldar?
     - 4.5.4. ¿Con que periodicidad debemos respaldar?
     - 4.5.5. Precauciones
     - 4.5.6. Simulacros y planes de contingencia
5. Herramientas de seguridad
   - 5.1 Tcp-wrappers
   - 5.2 Tripwire
   - 5.3 Nmap
   - 5.4 Nessus
   - 5.5 Md5
   - 5.6 GNU privacy Guard
6. Manejo de violaciones de seguridad
   - 6.1.Manejo de incidentes
   - 6.2.Detección
   - 6.3.Revisión de archivos de bitácora
   - 6.4.Reparación de daños
   - 6.5.Reportes

Duración: 40 horas.

Duración Total: 160 horas.

DIRECTORIO

Mtro. Tomás Humberto Rubio Pérez
Director FCA

Dr. Armando Tomé González
Secretario General

Mtra. Norma Angélica González Buendía
Jefa de Exámenes Profesionales

Admisión e informes

Departamento de Exámenes Profesionales
http://titulacion.fca.unam.mx

Correo electrónico
seminarios@fca.unam.mx

Lunes a viernes de 9:00-14:00 y 16:00-19:00
Teléfono: 56228398 ext. 108,109 y 111