

DIPLOMADO DE ESPECIALIZACIÓN PROFESIONAL EN
REDES, TELECOMUNICACIONES Y SEGURIDAD
EN CISCO, MIKROTIK Y UBIQUITI



De 6 pm a 9 pm



224 HORAS



Lunes, Miércoles
y Viernes

CODIT



- *Instructores Certificados*
- *Clases Online en Vivo*
- *Preparación para Certificación*
- *Material Didáctico*
- *Evaluaciones y Certificado*



Dirigido a Certificación



MikroTik



RESUMEN DEL DIPLOMADO

Tecnología

Cisco, MikroTik y Ubiquiti

A quien va dirigido

- ✓ Administradores de Red
- ✓ Ingenieros de Soporte de Red
- ✓ Ingenieros de Redes Asociadas.
- ✓ Especialistas en Redes
- ✓ Analistas de Redes

Exámenes de Certificación

Dirigido a la certificación:



Módulos

- ✓ **Módulo 1:** Introducción a Redes
Duración 8 Horas
- ✓ **Módulo 2:** Cableado Estructurado
Duración 24 Horas
- ✓ **Módulo 3:** Telefonía IP
Duración 16 Horas
- ✓ **Modulo 4:** Cisco Certified Network Associate (CCNA)
Routing and Switching
Duración 40 Horas
- ✓ **Modulo 5:** Cisco Certified Network Associate (CCNA)
Security
Duración 40 Horas
- ✓ **Modulo 6:** MikroTik Certified Network Associate (MTCNA)
Duración 24 Horas
- ✓ **Modulo 7:** MikroTik Certified Routing Engineer (MTCRE)
Duración 16 Horas
- ✓ **Modulo 8:** Ubiquiti Enterprise Wireless Admin (UEWA)
Duración 16 Horas
- ✓ **Modulo 9:** Ubiquiti Broadband Wireless Admin (UBWA)
Duración 16 Horas
- ✓ **Modulo 10:** Ubiquiti Broadband Routing & Switching Specialist (UBRSS)
Duración 24 Horas

Pre-requisitos

- ✓ Conocimientos básicos de computación
- ✓ Navegación básica del sistema operativo de la PC
- ✓ Uso básico de internet
- ✓ Direccionamiento IP básico
- ✓ Buena comprensión de los fundamentos de la red.

Objetivos

- ✓ Describir los fundamentos de la red y construir redes LAN simples.
- ✓ Establecer conectividad a internet.
- ✓ Administrar y proteger dispositivos de red.
- ✓ Opere una LAN de tamaño mediano con varios conmutadores, que admitan VLAN, trunking y spanning tree
- ✓ Solucionar problemas de conectividad IP
- ✓ Describir cómo configurar y solucionar problemas de EIGRP en un entorno IPv4, y configurar EIGRP para IPv6
- ✓ Configurar y solucionar los problemas de OSPF en un entorno IPv4
- ✓ Definir características, funciones y componentes de una WAN
- ✓ Describir cómo implementar la administración de dispositivos.
- ✓ Comprender la QoS, los servicios de virtualización y en la nube, y la capacidad de programación de la red relacionada con los segmentos de WAN, acceso y núcleo.
- ✓ Describir conceptos comunes de seguridad de red.
- ✓ Infraestructura segura de enrutamiento y conmutación
- ✓ Desplegar servicios básicos de autenticación, autorización y contabilidad.
- ✓ Implementar servicios básicos de cortafuegos.
- ✓ Describir el uso de servicios de seguridad más avanzados, como la protección contra intrusos, la seguridad del contenido y la administración de identidades.

Introducción a Redes

(8 Horas)

Módulo 1: Construyendo una red simple

1. Como las redes nos rodean en el día a día
2. Tipos de redes
3. Tipos de topologías
4. Elementos que componen una red.

Módulo 2: Ancho de banda y medios de acceso

1. Formas de medir el ancho de banda.
2. Diferencia entre ancho de banda analógico y ancho de banda digital.
3. Forma de acceso al medio.
4. Especificaciones Ethernet
5. Estándar de cableado UTP.
6. Medio de fibra óptica
7. Medio inalámbrico.

Módulo 3: Protocolos de redes

1. Protocolo de aplicaciones.
2. Protocolo de red.
3. Protocolo de transporte.
4. Protocolo de internetworking
5. Estándar OSI
6. Diferencias y similitudes entre el modelo OSI y el modelo Internet.
7. Servicios de DNS, DHCP, WWW y FTP.

Módulo 4: Ethernet y Protocolo de Internet

1. Estándar Ethernet
2. Estructura de una trama Ethernet
3. Uso y función de Gateway
4. Estructura de una red IPv4.
5. Estructura de una red IPv6.
6. Mascara de subred y su influencia en TCP/IP
7. Distintos entes reguladores y sus funciones.
8. ¿Cómo calcular Subredes?



Módulo 5: Capa de transporte, VPN y acceso inalámbrico

1. Protocolo de datagramas de usuario (UDP).
2. Protocolo de control de transmisión (TCP).
3. Direccionamiento de puertos.
4. Tecnología VPN
5. Distintos accesos de VPN.
6. Acceso inalámbrico a banda ancha

Cableado Estructurado

(24 Horas)

Módulo 1: Historia y desarrollo del cableado de redes. Topologías existentes

Módulo 2: Estándares y normas

Módulo 3: Cableado estructurado. Definición

Módulo 4: Normas TIA-568A; TIA569A

Módulo 5: Tierra de telecomunicaciones

Módulo 6: Futuro de normas: categorías 5e, nivel 6

Módulo 7: Diseño de cableado horizontal

Módulo 8: Diseño de closet de telecomunicaciones

Módulo 9: Diseño de Back-Bone

Módulo 10: Diseño de closet de telecomunicaciones principal

Módulo 11: Sistema de identificación

Módulo 12: Certificación, Memoria Descriptiva, Cálculo de impuestos

Módulo 13: Seguridad: Descargas eléctricas e incendios

Módulo 14: Planteamiento de la necesidad y proyecciones

Módulo 15: Norma EIA-TIA-570AA

Módulo 16: Tomas, cables y centros de distribución

Módulo 17: Diseño de cableado en unidad habitacional

Módulo 18: Diseño de Backbone de edificio

Módulo 19: Tips de instalación

Módulo 20: Redes inalámbricas

Módulo 21: Simbología



Telefonía IP

(16 Horas)

Módulo 1: Fundamentos de VoIP

Módulo 2: Fundamentos de QoS.

Módulo 3: Fundamentos de Diseño de Centrales IP Asterisk.

Módulo 4: Fundamentos de Diseño de Centrales IP Cisco Systems.

Módulo 5: Implementando una Central de Telefonía IP con Asterisk.

Módulo 6: Fundamentos de la Señalización Análoga.

Módulo 7: Fundamentos de la Señalización Digital.

Módulo 8: Troncales IAX y Troncales SIP.

Módulo 9: Técnicas de Diseño de Redes LAN para la correcta implementación de Telefonía IP.

Cisco Certified Network Associate (CCNA) Routing and Switching

(40Horas)

Módulo 1: Construyendo una red simple

1. Explorando las funciones de la red
2. Entender el modelo de comunicaciones de host a host
3. Introduciendo LANs
4. Operar el software Cisco IOS®
5. Comenzando un interruptor
6. Entendiendo el funcionamiento de Ethernet y Switch
7. Solución de problemas comunes de los medios de conmutación

Módulo 2: Estableciendo conectividad a internet

1. Entendiendo la capa de Internet TCP / IP
2. Entender el direccionamiento IP y las subredes
3. Entendiendo la capa de transporte TCP / IP
4. Explorando las funciones de enrutamiento
5. Configurando un Cisco Router
6. Explorando el proceso de entrega de paquetes
7. Habilitación de enrutamiento estático
8. Conceptos básicos de aprendizaje de listas de control de acceso (ACL)
9. Habilitando la conectividad a internet

Lab: Establecer conectividad a internet

Lab: Solucionar problemas de conectividad a Internet

Módulo 3: Implementando redes escalables de tamaño mediano

1. Implementación y solución de problemas de VLAN y troncales
2. Construcción de topologías redundantes conmutadas
3. Mejora de topologías redundantes conmutadas con EtherChannel
4. Enrutamiento entre VLANs
5. Uso de un dispositivo de red Cisco IOS como servidor de protocolo de configuración dinámica de host (DHCP)
6. Entendiendo la Redundancia de Capa 3
7. Implementación del protocolo de información de enrutamiento (RIP) v2

Módulo 4: Introduciendo IPv6

1. Introduciendo Basic IPv6
2. Entendiendo el funcionamiento de IPv6
3. Configuración de rutas estáticas de IPv6

Módulo 5: Solución de problemas de conectividad básica

1. Solución de problemas de conectividad de red IPv4
2. Solución de problemas de conectividad de red IPv6

Módulo 6: Implementación de seguridad de dispositivos de red

1. Asegurar el acceso administrativo
2. Implementando el endurecimiento del dispositivo
3. Implementando Seguridad Avanzada

Módulo 7: Implementando una solución basada en EIGRP

1. Implementando EIGRP
2. Implementando EIGRP para IPv6
3. Solución de problemas de EIGRP

Módulo 8: Implementar una solución basada en OSPF escalable

1. Entendiendo OSPF
2. Implementando Multiarea OSPF IPv4
3. Implementando OSPFv3 para IPv6
4. Solución de problemas de Multiarea OSPF

Lab: Solución de problemas de una red de tamaño mediano

Lab: Solución de problemas de una red escalable de tamaño mediano

Módulo 9: Implementando redes de área amplia

1. Entendiendo las Tecnologías WAN
2. Entendiendo los Protocolos Punto a Punto
3. Configuración de túneles de encapsulación de enrutamiento genérico (GRE)
4. Configuración del protocolo de puerta de enlace de frontera externa (EBGP)

Módulo 10: Gestión de dispositivos de red

1. Implementación de la gestión básica de dispositivos de red
2. Aprendiendo sobre la evolución de las redes inteligentes
3. Introduciendo QoS
4. Gestión de dispositivos Cisco

Módulo 11: Laboratorios

1. Comenzar con la interfaz de línea de comandos de Cisco (CLI)
2. Realizar la configuración básica del switch
3. Observar cómo funciona un interruptor
4. Solucionar problemas de conmutación de medios y puertos
5. Inspeccionar aplicaciones TCP / IP
6. Comenzar con la configuración del router Cisco

7. Configurar el protocolo de descubrimiento de Cisco
8. Configurar la puerta de enlace predeterminada
9. Explorar el reenvío de paquetes
10. Configurar y verificar rutas estáticas
11. Configurar y verificar las ACLs
12. Configurar una dirección IP asignada por el proveedor
13. Configurar la traducción de direcciones de red estática (NAT)
14. Configurar NAT dinámica y traducción de dirección de puerto (PAT)
15. Solucionar problemas de NAT
16. Configurar VLAN y Troncal
17. Solucionar problemas de VLAN y troncales
18. Configure el puente de raíz y analice la topología del protocolo de árbol de expansión (STP)
19. Solucionar problemas de STP
20. Configurar y verificar EtherChannel
21. Configurar un enrutador en un stick
22. Configurar un router Cisco como un servidor DHCP
23. Solucionar problemas de DHCP
24. Configurar y verificar el protocolo de enrutador Hot Standby (HSRP)
25. Solucionar problemas de HSRP
26. Configurar y verificar RIPv2
27. Solucionar problemas de RIPv2
 - a. Implementando RIPv2
28. Configurar la conectividad básica de IPv6
29. Configurar rutas estáticas IPv6
 - a. Implementar enrutamiento estático IPv6
30. Utilizar herramientas de solución de problemas
31. Configurar SPAN
32. Configure y verifique las listas de acceso extendido de IPv4
33. Solucionar problemas de conectividad de red IPv4
 - a. Solucionar problemas de conectividad IPv4
34. Configurar y verificar las listas de acceso extendido de IPv6
35. Solucionar problemas de conectividad de red IPv6
 - a. Solucionar problemas de conectividad IPv6
36. Mejorar la seguridad de la configuración inicial
37. Limitar la conectividad de acceso remoto
 - a. Asegurar el acceso administrativo del dispositivo
38. Configurar y verificar la seguridad del puerto
39. Configurar y verificar el protocolo de tiempo de red (NTP)
 - a. Implementando el endurecimiento del dispositivo

41. Configurar la autenticación externa mediante el servicio de acceso telefónico de usuario de acceso remoto (RADIUS) y el control de acceso de terminal Access Control Service Plus (TACACS +)
42. Configurar y verificar EIGRP
43. Configure y verifique EIGRP para IPv6
 - a. Solucionar problemas de EIGRP
44. Configurar y verificar OSPF de área única
45. Configure y verifique Multiarea OSPF
46. Configurar y verificar OSPFv3
47. Solucionar problemas de Multiarea OSPF
 - a. Solucionar problemas de OSPF
48. Configurar la interfaz en serie y el protocolo punto a punto (PPP)
49. Configurar y verificar MLP
50. Configure y verifique un cliente de protocolo punto a punto a través de Ethernet (PPPoE)
51. Configurar y verificar un túnel GRE
52. Configurar y verificar EBGp de un solo hogar
 - a. Implementar EBGp de un solo hogar
53. Configurar Syslog

Cisco Certified Network Associate (CCNA) Security

(40 Horas)

Módulo 1: Desarrollar una política de seguridad de red integral para contrarrestar las amenazas contra seguridad de información.

Módulo 2: Redes sin fronteras seguras

Módulo 3: Aprender a usar Cisco IOS Network Foundation Protection (NFP) y Cisco Configuración Profesional (CCP)

Módulo 4: Implementar de forma segura las funciones de administración y generación de informes de dispositivos Cisco IOS

Módulo 5: Implementar las características de seguridad de Cisco Catalyst Switch

Módulo 6: Comprender las características de seguridad de IPv6.

Módulo 7: Planificar estrategias de control de amenazas.

Módulo 8: Filtrar tráfico con listas de control de acceso.

Módulo 9: Configure los cortafuegos basados en zonas ASA y Cisco IOS

Módulo 10: Implementar sistemas de prevención de intrusiones (IPS) y traducción de direcciones de red (NAT)

Módulo 11: Conectividad segura con VPN IPsec de sitio a sitio y VPN de acceso remoto

MikroTik Certified Network Associate (MTCNA)

(24 Horas)

Módulo 1: Introducción

1. Sobre MikroTik
 - a. ¿Qué es RouterOS?
 - b. ¿Qué es RouterBOARD?
2. Primera vez accediendo al router
 - a. WinBox y MAC-WinBox
 - b. WebFig y Quick Set
 - c. Configuración por defecto
3. Interfaz de línea de comandos de RouterOS (CLI)
 - a. Cable de módem nulo
 - b. SSH y Telnet
 - c. Nueva terminal en WinBox / WebFig
4. Principios de RouterOS CLI
 - a. <tab>, doble <tab>, “?”, navegación
 - b. La historia del comando y sus beneficios.
5. Configuración inicial (acceso a internet)
 - a. Cliente DHCP WAN
 - b. Dirección IP de LAN y puerta de enlace predeterminada
 - c. Cortafuegos básico - mascarada NAT
6. Actualizando RouterOS
 - a. Tipos de paquetes
 - b. Maneras de mejorar
 - c. Actualización del firmware de RouterBOOT
7. Identidad del router
8. Administrar los inicios de sesión de RouterOS
9. Administrar los servicios de RouterOS
10. Gestión de copias de seguridad de configuración
 - a. Guardando y restaurando la copia de seguridad
 - b. Diferencia entre una copia de seguridad y un archivo de exportación (.rsc)
 - c. Edición de un archivo de exportación
11. Restablecer un dispositivo RouterOS
12. Reinstalar un dispositivo RouterOS (Netinstall)
13. Niveles de licencia de RouterOS
14. Laboratorio

Módulo 2: DHCP

1. Servidor DHCP y cliente
 - a. Cliente DHCP
 - b. Configuración del servidor DHCP
 - c. Gestión de arrendamientos
 - d. Configuración de red del servidor DHCP
2. Protocolo de resolución de direcciones (ARP)
 - a. Modos ARP
 - b. Tabla RouterOS ARP
3. Laboratorio

Módulo 3: Punteo

1. Visión general de puente
 - a. Conceptos y ajustes del puente.
 - b. Creando puentes
 - c. Añadiendo puertos a puentes.
2. Redes inalámbricas puente
 - a. Puente de la estación
3. Laboratorio

Módulo 4: Enrutamiento

1. Visión general de enrutamiento
 - a. Conceptos de enrutamiento
 - b. Banderas de ruta
2. Enrutamiento estático
 - a. Creando rutas
 - b. Configuración de la ruta por defecto
 - c. Gestionando rutas dinámicas.
 - d. Implementando enrutamiento estático en una red simple.
3. Laboratorio

Módulo 5: Inalámbrico

1. Conceptos 802.11a / b / g / n / ac
 - a. Frecuencias (bandas, canales) velocidades de datos / cadenas (potencia tx, sensibilidad de rx, regulaciones de país)
2. Configurar un enlace inalámbrico simple
 - a. Configuración del punto de acceso
 - b. Configuración de la estación
3. Seguridad inalámbrica y cifrado
 - a. Lista de acceso
 - b. Conectar lista
 - c. Autenticación predeterminada
 - d. Predeterminado Adelante

- e. WPA-PSK, WPA2-PSK
 - f. WPS accept, WPS client
4. Herramientas de monitoreo
 - a. Snooper
 - b. Mesa de registro
 5. Laboratorio

Módulo 6: Firewall

1. Principios de cortafuegos
 - a. Seguimiento de conexiones y estados.
 - b. Estructura, cadenas y acciones.
2. Filtro de firewall en acción
 - a. Acciones de filtro
 - b. Protegiendo su enrutador (entrada)
 - c. Protección de sus clientes (adelante)
3. Lista de direcciones básica
4. Fuente NAT
 - a. Mascarada y acción src-nat.
5. Destino NAT
 - a. Acciones dst-nat y redirect.
6. Vía rápida
7. Laboratorio

Módulo 7: QoS

1. Cola simple
 - a. Objetivo
 - b. Destinos
 - c. Límite máximo y límite de
 - d. Muy lleno
2. Una cola simple para toda la red (PCQ)
 - a. Configuración pcq-rate
 - b. Configuración de pcq-limit
3. Laboratorio

Módulo 8: Túneles

1. Configuración de PPP
 - a. Perfil de PPP
 - b. PPP secreto
 - c. Estado de PPP
2. Conjunto de IP
 - a. Creando pool
 - b. Rangos de gestión
 - c. Asignar a un servicio

3. Red local segura
 - a. Nombre de servicio PPPoE
 - b. Cliente PPPoE
 - c. Servidor PPPoE
4. Direcciones punto a punto
5. Comunicación segura de redes remotas
 - a. Cliente PPTP y servidor PPTP (conjunto rápido)
 - b. Cliente SSTP
6. Laboratorio

Módulo 9: Misc

1. Herramientas de RouterOS
 - a. Email
 - b. Netwatch
 - c. Silbido
 - d. Traceroute
 - e. Perfilador (carga de CPU)
2. Vigilancia
 - a. Monitor de tráfico de interfaz
 - b. Antorcha
 - c. Graficas
 - d. SNMP
 - e. El tipo
3. Contactando a support@mikrotik.com
 - a. supout.rif, autosupout.rif y visor
 - b. Registros del sistema, habilitando registros de depuración.
 - c. Configuración legible (comentarios y nombres del artículo)
 - d. Diagramas de red
4. Laboratorio

MikroTik Certified Routing Engineer (MTCRE)

(16 Horas)

Módulo 1: Enrutamiento estático

1. Rutas más específicas
2. ECMP
3. Cómo forzar el gateway sobre una interfaz específica
4. Verificación de accesibilidad y distancia de la ruta
5. Marca de ruta y política de ruta.
6. Uso recursivo de próximo salto y alcance / alcance de destino
7. Laboratorio

Módulo 2: Direccionamiento punto a punto

1. Configuración de dirección punto a punto
2. Laboratorio

Módulo 3: VPN

1. ¿Qué es VPN?
2. Diferentes tipos de VPN
3. Conectividad sitio a sitio con túneles.
4. IPsec, EoIP, PPTP, SSTP, L2TP, PPPoE
5. VLAN y su uso
6. Implementación QinQ VLAN y switch gestionado
7. Configuración de VLAN y chip de conmutador en RouterBOARDS
8. Laboratorio

Módulo 4: OSPF

1. ¿Qué es OSPF?
2. Cómo funciona el protocolo OSPF
3. Hola protocolo
4. Distribución de bases de datos y tipos de LSA explicados
5. Estructura de la red OSPF
6. Áreas
7. Tipos de enrutador
8. Vecinos de OSPF y estados vecinos (elección de DR y BDR)
9. Métodos de distribución de rutas externas (tipo 1, tipo 2)
10. Costos y tipos de interfaz (broadcast, NBMA, etc.)
11. Algoritmo de cálculo SPT
12. OSPF y multicast (problemas con NBMA)
13. Stub, NSSA y rangos de área (agregación de rutas)
14. Enlaces virtuales, usos y limitaciones.
15. Filtros y limitaciones de enrutamiento OSPF

Ubiquiti Enterprise Wireless Admin (UEWA)

(16 Horas)

Módulo 1: Fundamentos de WLAN

1. Espectro de radio sin licencia
2. Operación del canal
3. Dominios regulatorios
4. Estándares WLAN
5. Métodos de acceso inalámbrico
6. Equipo de red

Módulo 2: Planificación WLAN

1. Tecnología inalámbrica
2. Cobertura y Canales
3. Poder TX
4. Ganancia de la antena
5. Disponibilidad de canal
6. Señales contra ruido
7. Tiempo de aire, capacidad y densidad
8. Redes mixtas

Módulo 3: Despliegue

1. Encuestas de sitio
2. Superposición
3. Cableado y PoE
4. Benchmarking

Módulo 4: Adopción y configuración básica

1. Multi-sitio
2. Adopción Layer-2
3. Grupos WLAN
4. SSID, seguridad y VLAN
5. Analítica

Módulo 5: Adopción avanzada e invitados

1. Alojamiento en la nube
2. Adopción Layer-3
3. Descubrimiento, SSH, DNS y DHCP
4. RSSI mínimo
5. Roaming sin transferencia
6. Portal de invitados
7. Controles de acceso

Ubiquiti Broadband Wireless Admin (UBWA)

(16 Horas)

Módulo 1: Teoría de RF

1. Frecuencia vs. propagación
2. Bandas sin licencia
3. Máscaras espectrales OFDM
4. Frecuencias con licencia
5. Decibelios en sistemas RF
6. Pérdida del camino del espacio libre
7. Pire
8. Línea de vista y zonas de Fresnel
9. Presupuestos de energía de enlace
10. Fade Margin

Módulo 2: Operación de Radio

1. Circuito de RF estándar
2. Señales portadoras
3. Sensibilidad de radio
4. Selectividad de radio
5. Señal, ruido e interferencia
6. Cadenas, tasas de datos y MIMO
7. Ruido térmico
8. Flexión de canales
9. tecnología de airprism
10. Modulación, EVM y tasas de datos

Módulo 3: Teoría de la antena

1. ¿Qué es la ganancia?
2. Radiadores isotrópicos
3. Función de la antena
4. Ganancia, eficiencia y VSWR
5. Ganancia, Superficie y Directividad
6. Parcelas polares
7. MIMO, polarización y XPD
8. Tipos de Antenas
9. Alineación de la antena
10. Downtilt, Lobes & Nulls

Módulo 4: Proveedores de servicios de Ubiquiti

1. Protocolo TDMA y airMAX
2. 802.11, CSMA / CA y interior
3. Problema de Nodo Oculto
4. airMAX-AC, airOS-6 y -8
5. Trazado y explosión de tráfico
6. Escalabilidad vs. Rendimiento
7. Seguridad y VLAN
8. Tecnología y Protocolos de AirFiber
9. AirOS Tools & Redudancy
10. ISP puenteado vs. enrutado

Ubiquiti Broadband Routing & Switching Specialist (UBRSS)

(24 Horas)

Módulo 1: Gestión de dispositivos

1. Configurar equipo de laboratorio
2. Familia de productos EdgeMAX

Módulo 2: IPv4 y Subnetting

1. Fundamentos de direccionamiento
2. Subnetting
3. VLSM para proveedores
4. Resumen

Módulo 3: Diseño de red

1. Modelo OSI y Encapsulación
2. Fundamentos de topología de red
3. Interfaces de red
4. La red local
5. Red de comunicación
6. La red de área amplia

Módulo 4: Enrutamiento

1. Tablas de enrutamiento
2. Protocolos de enrutamiento estático
3. Protocolos de enrutamiento dinámico

Módulo 5: Servicios y Seguridad

1. DHCP
2. DNS
3. NAT
4. Cortafuegos
5. Túneles y VPN

Módulo 6: Apéndices

1. Introducción a IPv6
2. Comandos de EdgeOS
3. Tablas de direccionamiento y enrutamiento

RESUMEN DEL DIPLOMADO

Información de Contacto

María Isabel Salas

CCO

E-mail: maria.salas@codit.us

Teléfonos:

+58-212-750-7190

+58-212-750-7191

+57-320-901-0878

Tipos de Pago

Financiado:

- ✓ **Inscripción:** 30%
- ✓ **Mensualmente:** 70% (7 meses)

De contado:

- ✓ **10% de descuento**

Formas de Pago: Transferencias

Pagos en DÓLARES

Banco Intermediario: CITIBANK de Nueva York

Código ABA: 021000089

SWIFT: CITIUS33

Cuenta: N° 36006658 (BANCOLOMBIA)

Pagos en PESOS COLOMBIANOS (COP)

Banco BANCOLOMBIA

Cuenta de Ahorro: N° 54080298971

A nombre de: Soluciones CODIT SAS

NIT 901100997

OBSERVACIONES

1. Capacitación orientada a mayores de 18 años de edad.
2. Para la inscripción se requiere:
 - a. Documento de Identidad
 - b. Planilla de Datos
 - c. Soporte de Pago (Particulares) O Carta de Compromiso de Pago (Empresas)
3. Al inscribirse, lo participantes recibirán el siguiente material:
 - a. Cuaderno
 - b. Bolígrafo
 - c. Material de estudio digital
4. Una vez completados todos los módulos del diplomado y de haber aprobado satisfactoriamente todas las evaluaciones, los participantes recibirán:
 - a. Certificado de participación
5. Las clases serán impartidas en la modalidad on line.
6. En el caso de los pagos a crédito: todos los participantes (empresas o particulares) deberán cancelar puntualmente los primeros cinco (5) días del mes a cursar, de lo contrario no podrán acceder a las aulas virtuales.
7. Son cien (100) cupos disponibles a nivel internacional.
8. No se hacen reembolsos de ningún tipo.

