Programa

Redes de comunicación

¡Aprendizaje ***real*** que potencia tu ***conocimiento!***

Axon Group | Axon Empowering

Programa
Redes de comunicación

Al finalizar este programa tendrás los **conocimientos y habilidades prácticas** necesarias para diseñar, configurar y diagnosticar exitosamente la infraestructura de las redes de comunicación

Accede a la plataforma de contenido donde encontrarás:
- **+ 24 de lecciones por desarrollar.**
- **40 horas lectivas por cumplir.**

Cada semana podrás ingresar a **sesiones en vivo con expertos**, un espacio donde se resolverán dudas e inquietudes.

Prácticas en laboratorio

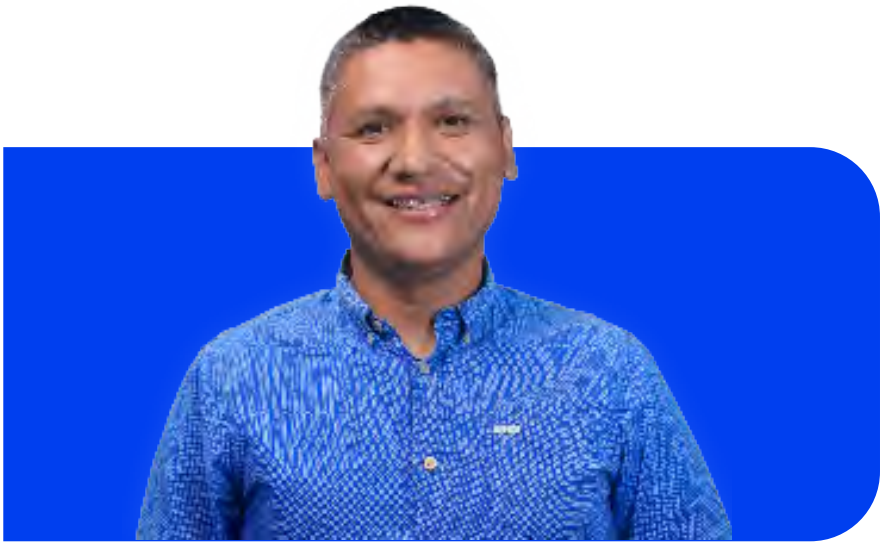
Azure

Desarrollo de **7 sesiones prácticas** con el objetivo de potenciar habilidades en el configuración, **diagnóstico y resolución de problemas** a nivel de configuración de canales de comunicación y condiciones de red.

Podrás resolver tus dudas e inquietudes a través de **asesorías personalizadas** con el fin de lograr una correcta ejecución en los proyectos a elaborar durante la formación.

Al superar los contenidos teóricos y prácticos realizarás una evaluación donde evidenciarás lo aprendido y de esta forma se te otorgará un certificado del **programa en redes**.

Nuestroo experto
A cargo del programa



Alonso Rojas

¡Hola a todos! Me llamo Alonso Rojas y soy tecnólogo en electrónica, ingeniero en telecomunicaciones y activista de la programación.

Con 12 años de experiencia en el sector eléctrico he desarrollado diferentes softwares de simulación, monitoreo y control como IHMS, Gateways de comunicaciones, entre otros, también en puesta en marcha y servicios en el campo del sector eléctrico.

El **programa de redes de comunicación** de está diseñado para proporcionarte los conocimientos teóricos y prácticos que necesitas para sobresalir en el sector eléctrico.

¡No pierdas la oportunidad de destacar en tu trabajo!

Tendremos sesiones en vivo en donde nos podremos conocer y practicar en los laboratorios de Azure in Cloud para afianzar los temas vistos; allí dispones de todas las herramientas necesarias y una cantidad de horas que las puedes usar cuando desees.

¡Esperamos verte pronto en Axon Empowering!

Temario **del programa**

MÓDULO	CONTENIDOS
 **Módulo 1:** **Introducción a las Telecomunicaciones en el Sector Eléctrico y Fundamentos de Redes y Direccionamiento IP**	**Introducción a las Telecomunicaciones en el Sector Eléctrico:** • Importancia de las telecomunicaciones en la infraestructura eléctrica moderna (subestaciones, redes inteligentes, control remoto, SCADA, etc.). • Tipos de redes de telecomunicaciones utilizadas en el sector eléctrico (fibra óptica, radioenlaces, redes celulares, etc.). • Estándares relevantes para telecomunicaciones en el sector eléctrico. **Introducción a las Redes de Datos:** • Componentes de una red (dispositivos finales, medios de transmisión, dispositivos de red). • Modelos de referencia OSI y TCP/IP (capas, funciones principales). • Tipos de topologías de red (estrella, bus, anillo, malla). **Direccionamiento MAC:** **Direcciones MAC:** Estructura, función, unicast, multicast, broadcast. **Protocolo ARP (Address Resolution Protocol):** resolución de direcciones IP a MAC. • Tabla ARP y su gestión.

Temario **del programa**

MÓDULO	CONTENIDOS
	Direccionamiento IP (IPv4 e IPv6): • **Direcciones IPv4:** estructura, clases de direcciones, direcciones públicas y privadas. • **Subredes y máscaras de subred:** cálculo de subredes, segmentación de redes. • **Direcciones IPv6:** estructura, ventajas sobre IPv4, tipos de direcciones IPv6. • Configuración de direcciones IP (estática y DHCP). • **Protocolo ICMP (Internet Control Message Protocol):** Ping, traceroute y su utilidad para diagnóstico de redes. • **Práctica:** • **Cálculo de Subredes IPv4 Virtualizado:** Ejercicios en hojas de cálculo o herramientas online virtualizadas para practicar el cálculo de subredes. • **Configuración de Direcciones IP Estáticas en VMs:** Configuración manual de IP, máscara, gateway en sistemas operativos (packet tracer). • **Uso de Comandos para MAC e IP:** Uso de ipconfig/ifconfig, arp -a, ping, traceroute dentro de las VMs o en simuladores de red. • **Servidor DHCP:** Implementación de un servidor DHCP en una VM (ej: Windows Server DHCP o ISC DHCP y switches 'packet tracer') y configuración de clientes virtuales para obtener IP automáticamente. • **Análisis de Tráfico con Wireshark:** Captura y análisis de tráfico de red utilizando Wireshark instalado en una Máquina conectada a la red.

Temario **del programa**

MÓDULO	CONTENIDOS
 **Módulo 2:** **VLANs y Redes de Capa 2**	• **Temario Teórico:** • **Redes de Capa 2 y Conmutación (Switching):** · Dispositivos de capa 2: switches. · Direccionamiento MAC y tablas de direcciones MAC en switches. · Dominios de broadcast y dominios de colisión. • **Spanning Tree Protocol (STP-Rstp):** prevención de bucles en redes conmutadas. · Prp y Hsr · Protocolo ICMP (Internet Control Message **Protocol):** ping, traceroute y su utilidad para diagnóstico de redes. • **VLANs (Virtual LANs):** • **Concepto de VLAN:** segmentación lógica de redes físicas. • **Beneficios de las VLANs:** seguridad, rendimiento, gestión. · Tipos de VLANs (VLAN de datos, VLAN de voz, VLAN nativa, etc.). • **VLAN tagging (IEEE 802.1Q):** Encapsulamiento de tramas Ethernet para VLANs. · Puertos de acceso y puertos troncales (trunk) en switches. • **Protocolo VTP (VLAN Trunking Protocol):** propagación de información de VLANs (consideraciones de seguridad y alternativas más modernas).

Temario **del programa**

MÓDULO	CONTENIDOS
	Práctica: **Configuración de VLANs en switches:** Creación de VLANs, asignación de nombres, asignación de puertos a VLANs. **Configuración de puertos de acceso y puertos troncales:** Implementación de enlaces troncales entre switches para permitir el tráfico de múltiples VLANs. **Verificación de la segmentación de VLANs:** Pruebas de conectividad entre dispositivos dentro de la misma VLAN y entre diferentes VLANs (con y sin enrutamiento entre VLANs). **Análisis del tráfico de VLANs con analizador de protocolos:** Visualización de etiquetas VLAN en tramas Ethernet. Configuración básica de Spanning Tree Protocol (STP) para prevenir bucles en una topología redundante y en equipos de telecontrol como Siemens u otros. Simuladores como AT5 para contextualizar enrutamientos reales .
Módulo 3: **Seguridad Física**	• **Temario Teórico:** • **Seguridad de Puertos Físicos en Equipos de Telecomunicaciones:** · Tipos de puertos en equipos de telecomunicaciones (Ethernet, fibra óptica, puertos de consola, USB, etc.). · Vulnerabilidades asociadas a puertos no seguros (accesos no autorizados, conexión de dispositivos maliciosos).

Temario **del programa**

MÓDULO	CONTENIDOS
	• Deshabilitación de puertos no utilizados. • Implementación de seguridad de puertos (Port Security) a nivel de switch para controlar el acceso por MAC address. • Sellado físico de puertos para prevenir conexiones no autorizadas. • **Protocolos de Autenticación Centralizada:** • **RADIUS (Remote Authentication Dial-In User Service):** Arquitectura, funcionamiento, casos de uso en acceso a red y dispositivos de telecomunicaciones. • **TACACS+ (Terminal Access Controller Access-Control System Plus):** Arquitectura, ventajas sobre RADIUS (separación de funciones, cifrado), casos de uso en administración de dispositivos de red. • **LDAP (Lightweight Directory Access Protocol):** Introducción a LDAP como servicio de directorio y su uso para autenticación y autorización. • **Componentes de un Sistema de Autenticación Centralizada:** Servidores de autenticación, bases de datos de usuarios, clientes RADIUS/TACACS+ en dispositivos de red. • **Flujo de Autenticación en RADIUS y TACACS+:** Intercambio de mensajes, proceso de validación de credenciales. • **Integración con Control de Acceso Basado en Roles (RBAC):** Cómo los sistemas de autenticación centralizada permiten implementar RBAC para una gestión de permisos granular.

Temario **del programa**

MÓDULO	CONTENIDOS
	• **Consideraciones de Seguridad en Sistemas de Autenticación Centralizada:** Protección de servidores de autenticación, cifrado de comunicaciones, gestión de credenciales de administrador. • Práctica: • **Configuración de Port Security en switches:** Implementación de restricciones de acceso basadas en MAC address en puertos de switches. **Implementación de un Servidor RADIUS en un entorno virtualizado:** • Instalación y configuración de un servidor RADIUS (ej: FreeRADIUS en una máquina virtual Linux). • Creación de usuarios y definición de atributos en el servidor RADIUS. **Configuración de un Switch Virtual como Cliente RADIUS:** • Configuración de un switch virtual (ej: en Packet Tracer o GNS3) para utilizar RADIUS como método de autenticación para acceso a la línea de comandos (consola/SSH) o acceso a la red (802.1X). • Verificación del proceso de autenticación RADIUS al intentar acceder al switch virtual. **Escenarios de Autenticación con RADIUS:** • Simulación de diferentes escenarios de autenticación exitosa y fallida utilizando diferentes credenciales y atributos configurados en el servidor RADIUS.

Temario **del programa**

MÓDULO	CONTENIDOS
	• Análisis de logs del servidor RADIUS para rastrear intentos de autenticación. • **Exploración de TACACS+ (Opcional):** • Instalación y configuración básica de un servidor TACACS+ (ej: TACACS+ server en una máquina virtual Linux). • Configuración de un router virtual como cliente TACACS+ para autenticación de administración. • Comparación de la configuración y funcionamiento básico con RADIUS.
Módulo 4: **TLS (Transport layer security)Seguridad confidencialidad, integridad y autenticación de los datos**	• Conceptos básicos de criptografía • Introducción a la norma IEC62351 • Seguridad en enlaces por medio de TLS (IEC60870-5-104, DNP3, ICCP, IEC61850) • Certificados X.509 • Práctica: • Autenticación y encriptación generando llaves públicas, privadas y certificados. • Configuración en Cliente y servidor (DNP3 o ICCP) AB3

Temario **del programa**

MÓDULO	CONTENIDOS
 **Módulo 5:** **Túneles VPN y Gestión de Equipos de Telecomunicaciones**	• **Temario Teórico:** • **Túneles VPN (Virtual Private Networks):** • **Concepto de VPN:** creación de conexiones seguras y encriptadas a través de redes públicas. • **Tipos de VPNs:** • VPN site-to-site: interconexión segura de redes LAN a través de internet. • VPN de acceso remoto (client-to-site): acceso seguro de usuarios remotos a la red corporativa. • **Protocolos VPN:** • IPsec (Internet Protocol Security): seguridad a nivel de capa de red, modos de transporte y túnel, protocolos AH y ESP. • SSL/TLS VPN (OpenVPN, etc.): seguridad a nivel de capa de transporte, uso de certificados. • GRE tunnels (Generic Routing Encapsulation): túneles para encapsular tráfico de red, no ofrece encriptación por defecto (generalmente combinado con IPsec). • Criptografía básica aplicada a VPNs: cifrado simétrico y asimétrico, hashes, certificados digitales.

Temario **del programa**

MÓDULO	CONTENIDOS
	• **Gestión de Equipos de Telecomunicaciones:** • **Protocolos de gestión:** • **SNMP (Simple Network Management Protocol):** Monitorización y gestión de dispositivos de red, versiones de SNMP (v1, v2c, v3 - seguridad). • **SSH (Secure Shell):** acceso remoto seguro a la línea de comandos de dispositivos. • Telnet: acceso remoto no seguro (desaconsejado por seguridad, solo para equipos legacy o entornos controlados). • Interfaces web de gestión (HTTPS). • **Herramientas de gestión de red:** Software de monitorización, sistemas de gestión centralizada (ejemplos de herramientas open source y comerciales). • Configuración de copias de seguridad y restauración de configuraciones de equipos. • Gestión de contraseñas y políticas de acceso a equipos de gestión. • Práctica: • Configuración de un túnel VPN site-to-site básico utilizando IPsec en routers. • Configuración de acceso remoto seguro a dispositivos utilizando SSH. • Configuración básica de SNMP en dispositivos de red y uso de una herramienta de monitorización SNMP para obtener información de los dispositivos.

Temario **del programa**

MÓDULO	CONTENIDOS
	Implementación de políticas de contraseñas seguras en dispositivos de telecomunicaciones. · Ejercicio de copia de seguridad y restauración de la configuración de un router o switch. · Análisis de tráfico VPN con analizador de protocolos para verificar el cifrado.
Módulo 6: **Seguridad de Redes y Firewalls**	**Seguridad de Redes y Firewalls** • **Temario Teórico:** • **Conceptos de Seguridad en Redes:** · Amenazas y vulnerabilidades comunes en redes de telecomunicaciones del sector eléctrico (ataques DDoS, malware, intrusiones, etc.). · Principios de seguridad: confidencialidad, integridad, disponibilidad (CIA Triad). · Políticas de seguridad y mejores prácticas. • **Firewalls:** • **Función de un firewall:** Control de acceso, inspección de tráfico. • **Tipos de firewalls:** Firewalls de software, firewalls de hardware, firewalls de nueva generación (NGFW). • **Tipos de filtrado de firewalls:** Filtrado de paquetes, inspección de estado, inspección profunda de paquetes (DPI). • **Reglas de firewall (ACLs - Access Control Lists):** Permitir, denegar, acciones de registro. • **Zonas de seguridad en firewalls (DMZ - Demilitarized Zone):** Separación de servicios públicos y redes internas. · NAT (Network Address Translation) y su relación con la seguridad.

Temario del programa

MÓDULO	CONTENIDOS
	• **Práctica:** • **Configuración de reglas de firewall básicas:** Permitir/denegar tráfico basado en direcciones IP, puertos y protocolos. · Implementación de una DMZ en un firewall: Configuración de reglas para proteger servidores expuestos a internet. • **Pruebas de funcionamiento del firewall:** Verificación de que el firewall bloquea el tráfico no autorizado y permite el tráfico autorizado. · Uso de herramientas de escaneo de puertos (Nmap u otra) para identificar puertos abiertos en un sistema antes y después de aplicar reglas de firewall. · Análisis de logs de firewall para identificar eventos de seguridad.
Módulo 7: **Enrutamiento y Redes de Capa 3**	• **Temario Teórico:** • **Redes de Capa 3 y Enrutamiento (Routing):** · Dispositivos de capa 3: routers. · Direccionamiento IP y tablas de enrutamiento en routers. · Funciones de enrutamiento: determinación de la mejor ruta, reenvío de paquetes. • **Protocolos de enrutamiento:** · Protocolos de enrutamiento estático: configuración manual de rutas.

Temario **del programa**

MÓDULO	CONTENIDOS
	• **Protocolos de enrutamiento dinámico:** · RIP (Routing Information Protocol): protocolo de vector distancia (breve introducción). · OSPF (Open Shortest Path First): protocolo de estado de enlace (introducción más detallada). · BGP (Border Gateway Protocol): protocolo de enrutamiento entre sistemas autónomos (mención breve y su relevancia en interconexión de redes). • **Enrutamiento Estático:** · Configuración de rutas estáticas: destino, siguiente salto, interfaz de salida. · Casos de uso del enrutamiento estático. • **NAT (Network Address Translation) en detalle:** · Tipos de NAT: NAT estático, NAT dinámico, PAT (Port Address Translation). · Beneficios y desventajas de NAT: ahorro de direcciones IP públicas, seguridad (ocultamiento de red interna), complejidad. · Configuración de NAT en routers. • **Práctica:** • **Configuración de enrutamiento estático en routers:** Implementación de rutas estáticas para conectar diferentes redes. • **Verificación de tablas de enrutamiento en routers:** Análisis de las rutas configuradas y aprendidas. · Pruebas de conectividad a través de rutas estáticas. · Configuración de NAT dinámico y PAT en un router para permitir el acceso a internet desde una red privada. · Uso de comandos para visualizar información de enrutamiento: show ip route, traceroute, pathping.

Temario

Bootcamp redes de comunicación

PROGRAMA REDES DE COMUNICACIÓN		
	Duración	Inversión de tiempo
Videos	7	13
Lecturas	4	6
Laboratorios	4	8
Sesiones en vivo	7	10
Evaluación	1	2
Asesoría	1	1
Total	**24**	**40**

Inversión
Programa

Programa redes de comunicación

Fecha de inicio:
17 de septiembre de 2025

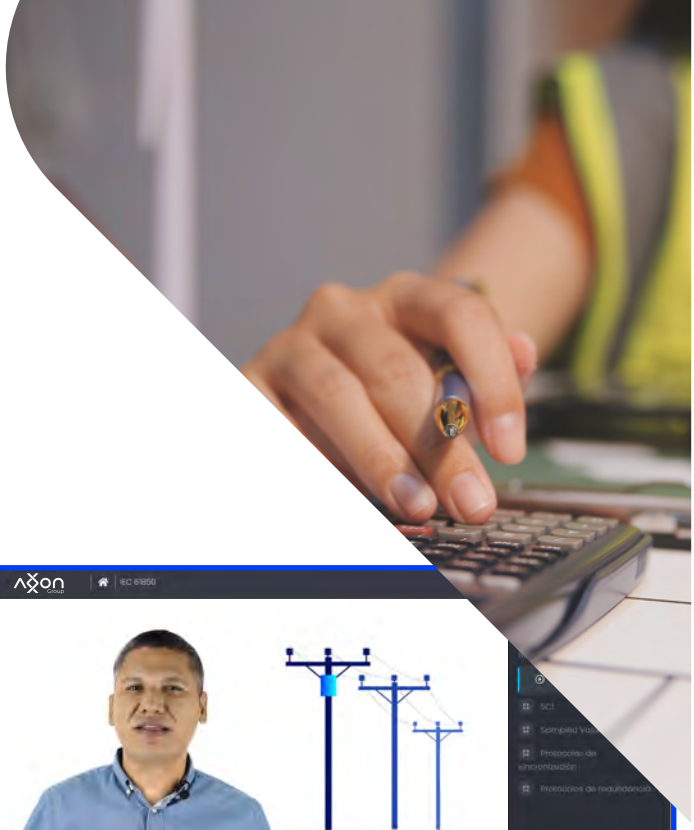
Duración de 6 semanas

Obtén descuento por lanzamiento del 20%

~~$USD 1100~~

$USD 800

Entorno **Virtual**



Plataforma en línea

Tienes a tu disposición la plataforma E-learning de Axon Empowering que te permite acceder a múltiples contenidos multimedia desde cualquier lugar y a tu propio ritmo.

Prácticas Azure

Un laboratorio con escenarios reales para afianzar los conocimientos.

- Software de configuración de equipos
- Simuladores
- SCADAs
- Software concentrador de señales

Asesorías personalizadas y grupales

Acompañamiento continuo con canales directos de comunicación para resolver preguntas, tener sesiones agendadas para resolver dudas y estudiar escenarios reales de trabajo.

¿Qué lograrás **con esta formación?**

Beneficios del programa Redes de comunicación

- Tendrás el conocimiento suficiente para diagnosticar los problemas comunes en los sistemas eléctricos.
- Obtendrás los conceptos necesarios para diseñar y asegurar redes de comunicación industriales en entornos OT.

¡Si superas todas las pruebas y aplicas lo aprendido, recibirás el diploma que certifica tu experiencia en redes de comunicación!

Programa

Redes de comunicación

¿Qué esperas para ser un experto?

¡Contáctanos!

+57 301 233 08 82

comercial@axongroup.com.co

axongroup.com.co/formacion/formacion-configuracion-de-redes-de-comunicacion/

https://empowering.axongroup.com.co/

¡Síguenos!

Axon Group | Axon Empowering