Modalidad 100% virtual

Técnico en Ciberseguridad

CERTIPORT
A PEARSON VUE BUSINESS

Microsoft Certified AZURE FUNDAMENTALS

MicrosoftLearn

CISCO

Azure

VITEK ACADEMY

¿Qué aprenderás?

Programa por bloques

Duración 13 meses

Bloque IT Support (2 meses)

CISCO CCST IT Support

Bloque Networking (2 meses)

CISCO CCST Networking

Bloque Cibersecurity (2 meses)

CISCO CCST Cibersecurity

Bloque Fundamentos de Azure (3 meses)

Fundamentos de Azure AZ-900

Bloque Seguridad en Azure (3 meses)

Security Cloud SC-900

Empleabilidad y Marca Profesional en Tecnología

CERTIPORT A PEARSON VUE BUSINESS

MicrosoftLearn

CISCO

Bloque IT Support

CISCO CCST IT Support

Duración 2 meses

Objetivo: Desarrollar competencias esenciales de soporte técnico, atención al usuario y resolución de problemas en entornos de TI.

- **Soporte técnico y help desk**
  - Conceptos clave: SLA, KPIs, gestión de tickets.
  - Documentación de incidentes y buenas prácticas de comunicación.
  - Proceso de resolución de problemas paso a paso.
- **Hardware y componentes**
  - Identificación y reemplazo de partes de PC (RAM, discos, periféricos).
  - Puertos, cables y conectores más comunes.
  - Procedimientos de seguridad y disposición responsable (e-waste).
- **Conectividad y acceso a recursos**
  - Servicios de directorio (Active Directory, Entra ID, AWS IAM).
  - Multifactor Authentication y accesos compartidos.
  - Conexión y solución de problemas con periféricos y redes básicas.
- **Sistemas operativos y aplicaciones**
  - Resolución de problemas en Windows, macOS y móviles.
  - Configuración de virtualización y nube básica (AWS, Azure, GCP).
  - Manejo de aplicaciones de productividad y colaboración.
- **Seguridad básica para usuarios**
  - Amenazas comunes: phishing, malware, ingeniería social.
  - Buenas prácticas de contraseñas y protección de datos.
- **Herramientas de soporte**
  - Uso de acceso remoto (TeamViewer, WebEx, Remote Desktop).
  - Investigación y documentación con foros, KBs y herramientas de IA

Bloque Networking

CISCO CCST Networking

Duración 2 meses

Objetivo: Comprender los fundamentos de redes de datos, protocolos y dispositivos para configurar y mantener infraestructuras seguras y funcionales.

Conceptos de redes
- Modelos OSI y TCP/IP.
- Diferencia entre LAN, WAN, WLAN y topologías de red.
- Protocolos principales: HTTP, HTTPS, DHCP, DNS, ICMP.

Direcciones y subredes
- IPv4 vs IPv6, subredes y NAT.
- Conceptos de CIDR y clases de direcciones.

Medios y dispositivos de red
- Cables (cobre, fibra, coaxial) y conectores (RJ-45, RJ-11).
- Tecnologías Wi-Fi, cableadas y celulares.
- Dispositivos IoT, móviles y servidores.

Infraestructura de red
- Switches, routers y puertos.
- Conceptos básicos de routing y switching.
- VLAN y segmentación de redes.

Diagnóstico y solución de problemas
- Uso de comandos: ping, tracert, nslookup, show commands en Cisco.
- Captura de paquetes con Wireshark.
- Acceso remoto a dispositivos (SSH, VPN, RDP).

Seguridad en redes
- Firewalls y filtrado de tráfico.
- Principios de CIA y AAA (confidencialidad, integridad, autenticación).
- Configuración de redes Wi-Fi seguras (WPA2/WPA3).

Bloque Cibersecurity

CISCO CCST Cibersecurity

Duración 2 meses

Objetivo: Conocer los fundamentos de la seguridad informática, amenazas actuales, gestión de riesgos y respuesta ante incidentes.

Principios de ciberseguridad

- Vulnerabilidades, amenazas, exploits y vectores de ataque.
- Modelo CIA (confidencialidad, integridad, disponibilidad).
- Gestión de accesos (AAA, MFA, políticas de contraseñas).
- Métodos de cifrado y certificados digitales.

Seguridad en redes

- Vulnerabilidades de protocolos TCP/IP.
- Segmentación de redes, NAT y direcciones privadas vs públicas.
- Firewalls, ACLs, VPNs y NAC.
- Configuración de redes inalámbricas seguras.

Seguridad en endpoints

- Seguridad en Windows, Linux y macOS.
- Firewalls locales, permisos y privilegios.
- Herramientas básicas: netstat, nslookup, tcpdump.
- Gestión de actualizaciones y parches.

Gestión de vulnerabilidades y riesgos

- Identificación y análisis de vulnerabilidades.
- Uso de bases de datos de amenazas y CVEs.
- Estrategias de mitigación y planes de continuidad de negocio.

Respuesta a incidentes

- Monitoreo de eventos con SIEM y SOAR.
- Forensia digital y atribución de ataques (Cyber Kill Chain, MITRE ATT&CK).
- Cumplimiento normativo (GDPR, HIPAA, PCI-DSS).
- Ciclo de vida de respuesta a incidentes según NIST.

Bloque Fundamentos de Azure

Microsoft Azure AZ-900

Duración 3 meses

MicrosoftLearn

Objetivo: Validar conocimientos fundamentales de conceptos de la nube y de los servicios de Microsoft Azure.

Conceptos de la nube

- Definición de cloud computing
- Modelos de despliegue (público, privado, híbrido)
- Modelos de servicio (IaaS, PaaS, SaaS)
- Modelo de responsabilidad compartida, consumo, pricing, serverless

Arquitectura y servicios de Azure

- Regiones, zonas de disponibilidad, datacenters, jerarquía de recursos (grupos, suscripciones, management groups)
- Servicios de cómputo: máquinas virtuales, contenedores, funciones, escalamiento, Azure Virtual Desktop
- Networking: VNets, subnets, peering, VPN Gateway, Azure DNS, ExpressRoute, endpoints
- Almacenamiento: tipos de cuentas, capas, redundancia, herramientas de migración como AzCopy y Azure Migrate
- Identidad y seguridad: Entra ID (AD), métodos de autenticación (SSO, MFA, passwordless), RBAC, Zero Trust, acceso condicional

Administración y gobernanza en Azure

- Costos: calculadora de precios, TCO, etiquetas, gestión de costos
- Herramientas de gestión y despliegue: Portal Azure, Azure CLI, PowerShell, Cloud Shell, ARM Templates, IaC, Azure Arc
- Supervisión: Azure Monitor, Log Analytics, Application Insights, Azure Advisor, Service Health

Bloque Seguridad en Azure

Microsoft Azure SC-900

Duración 3 meses

MicrosoftLearn

Objetivo: Acreditar conocimientos fundamentales en seguridad, cumplimiento e identidad basados en servicios de Azure y Microsoft 365

Conceptos de seguridad, cumplimiento e identidad

- Modelos: responsabilidad compartida, defensa en profundidad, Zero Trust
- Conceptos de cifrado, hash, GRC (Gobernanza, Riesgos y Cumplimiento)
- Definición de identidad como perímetro principal, autenticación, autorización, proveedores de identidad, AD, federación

Capacidades de Microsoft Entra

- Funcionamiento de Entra ID
- Tipos de identidades: híbridas, invitados, dispositivos, principios de servicio
- Métodos de autenticación: sincronización de contraseña, passthrough, SSO, MFA
- Accesso condicional, roles Entra, RBAC
- Gobernanza de identidades: PIM, revisiones de acceso, Protección de identidad, Entra ID Governance

Capacidades de soluciones de seguridad de Microsoft

- Servicios: DDoS Protection, Azure Firewall, WAF, NSGs, Azure Bastion, Key Vault, segmentación en red
- Gestión de seguridad: Defender for Cloud, CSPM, políticas de seguridad, protección de workloads
- SIEM y SOAR: Microsoft Sentinel, amenazas, detección, respuesta automatizada
- Defender XDR: Defender for Endpoint, Office 365, Cloud Apps, Identity, Vulnerability Management, Threat Intel

Capacidades de cumplimiento

- Service Trust Portal y principios de privacidad
- Microsoft Purview: Compliance Manager, compliance score
- Protección de información: clasificación, etiquetas de sensibilidad, DLP, políticas de retención y administración de registros
- Riesgos internos, eDiscovery y auditoría en Purview

Modalidad EN VIVO
Plus

1 Clases por semana

2 horas por clase

Clases en vivo + 1 voucher de examen

Acceso al campus virtual

Matrícula gratis

Certificación Vitek Academy

MicrosoftLearn CISCO CERTIPORT A PEARSON VUE BUSINESS

₵26.000

mensualidad

Modalidad EN VIVO

Certified

2 Clases por semana

2 horas por clase

Clases en vivo + Inglés + Voucher de examen

Acceso al campus virtual

Matrícula gratis

Certificación Vitek Academy

MicrosoftLearn

CISCO

CERTIPORT
A PEARSON VUE BUSINESS

₡29.000

mensualidad