

Ciberseguridad en la protección de infraestructuras de red

Modalidad:	Semipresencial	Tipo:	Programa Integral
Duración:	200.0 (horas académicas de 50 minutos)		

Acerca de este Programa

En la actualidad, cualquier negocio o empresa sin importar su tamaño, popularidad o recursos económicos, puede verse afectada por un ciberataque en cualquier momento. Nuestra falta de conocimiento para responder a estos ataques nos vuelven vulnerables. Necesitamos en lo posible eliminar todo tipo de riesgo de ataques maliciosos con los dispositivos informáticos que usamos. En este programa integral la prioridad es ofrecer la seguridad de un bien valioso: la información.

Módulos y Temario

Módulo 1: Infraestructura de redes (36 h.)

Nro.	Tema
1	Introducción a las redes y diseño de topologías de red con packet tracer
2	Seguridad en Windows 10. Políticas de seguridad con usuarios. Compartir recursos y asignar permisos. Crear políticas GPO. Auditorías.
3	Introducción al GNU/Linux. Instalación y comandos básicos parte I.
4	GNU/Linux: Comandos básicos II y Servicios básicos.
5	Herramientas de monitoreo: Herramientas internas y externas
6	Implementar herramientas y escaneo de vulnerabilidades en clientes de Windows 10.

Módulo 2: Diseño de la seguridad informática (28 h.)

Nro.	Tema
1	Fundamentos de Seguridad Informática
2	Seguridad y la Gestión de Riesgos
3	Revisión de la Metodología Magerit para el Análisis y Gestión de riesgos de los Sistemas de Información
4	Revisión de la Metodología Magerit para el Análisis y Gestión de Riesgos de los Sistemas de Información
5	Evaluación, tratamiento y Estudio
6	Revisión del estándar ISO/IEC 27001
7	Casos prácticos

Módulo 3: Ethical Hacking (36 h.)

Nro.	Tema
1	Introducción al Ethical Hacking y pruebas de penetración
2	Planificación y determinación del alcance de una evaluación de pruebas de penetración
3	Metodologías de pruebas de penetración
4	Pruebas de reconocimiento con Kali Linux e identificación de vulnerabilidades
5	Herramientas de escaneo de redes
6	Explotación de vulnerabilidades de Windows con Metasploit
7	Escalando privilegios en Windows y manteniendo el acceso
8	Sniffing and Spoofing
9	Desarrollo de reportes de test de penetración

Módulo 4: Implementación de la Seguridad con Mikrotik (36 h.)

Nro.	Tema
------	------

1	Introduccion a equipos MikroTik
2	RouterOS y RouterBoard
3	Administracion de usuarios e identidad del router
4	Habilitacion y desactivacion de servicios
5	Introduccion al Firewall de Router OS
6	Habilitación y bloqueo de puertos físicos y lógicos
7	DHCP, servidores rogue, ataques starvation y prevencion
8	Port Knoking
9	Detección de escaneo de puertos y prevención

Módulo 5: Implementacion de la Seguridad con Fortigate (36 h.)

Nro.	Tema
1	Introducción a equipos FortiGate
2	Firewall Policies
3	Firewall Autenticacion
4	Web Filter
5	Control de Aplicaciones
6	Antivirus
7	VPN IPSec y SSL
8	Prevención de Pérdida de Datos (DLP)
9	Sistema de Prevención de Intrusos

Módulo 6: Análisis Forense en Seguridad Empresarial (28 h.)

Nro.	Tema
1	El procedimiento forense
2	Recolección de Data
3	Desarrollo de la Línea de Tiempo
4	Filesystem Análisis y recuperación de datos
5	Análisis de Registry
6	Análisis de Archivos
7	El reporte forense