Gestión y Operaciones de Ciberseguridad

Modalidad:	Presencial	**Tipo:**	Programa de Especialización
Duración:	140.0 (horas académicas de 50 minutos)		

Acerca de este Programa

Este programa de especialización en Gestión y Operaciones de Ciberseguridad ofrece una inmersión completa en los aspectos fundamentales y avanzados de la protección digital. Desde el dominio de herramientas esenciales hasta la implementación de operaciones tácticas y estratégicas, pasando por el fortalecimiento de la seguridad en redes y la gestión eficaz de la ciberseguridad, este programa aborda de manera integral los desafíos contemporáneos en materia de seguridad informática. Con un enfoque en la auditoría como medida preventiva y correctiva, los participantes adquirirán habilidades cruciales para evaluar, diseñar y ejecutar estrategias robustas de protección cibernética, garantizando la resiliencia y confiabilidad de las infraestructuras digitales en un entorno cada vez más amenazante.

Módulos y Temario

Módulo 1: Herramientas de Ciberseguridad (30 h.)

Nro.	Tema
1	Introducción al Ethical Hacking y Test de Penetración
2	Planificación y alcance de una evaluación de pruebas de penetración
3	Recopilación de información y escaneo de vulnerabilidades
4	Ataques de ingeniería social
5	Explotación de redes cableadas
6	Explotación de vulnerabilidades basadas en aplicaciones
7	Seguridad en la nube, móvil e IoT
8	Realización de técnicas de postexplotación
9	Informes y comunicación
10	Herramientas y análisis de código

Módulo 2: Operaciones de Seguridad Cibernética (40 h.)

Nro.	Tema
1	Características de seguridad del sistema operativo Windows Implemente la seguridad básica de Linux.
2	Principios de la seguridad de red
3	Analisis de las PDU del protocolo de resolución de direcciones en la red.
4	Infraestructura de seguridad de la red Amenazas y ataques comunes
5	Monitoreo del tráfico de red.
6	Vulnerabilidad en TCP/IP, aplicaciones y servicios de red comunes
7	Enfoques para la defensa de la seguridad de la red.
8	Control de acceso como método de protección de la red.
9	Inteligencia de amenazas
10	Evaluación de vulnerabilidades en terminales
11	Datos de seguridad de la red y evaluación de alertas
12	Trabajo con datos de seguridad de la red
13	Análisis y respuesta de incidentes e informática forense digital

Módulo 3: Seguridad en Redes (40 h.)

Nro.	Tema
1	Seguridad en Redes
2	Amenazas de Red Mitigación de Amenazas
3	Acceso Seguro a Dispositivos
4	Listas de Control de Acceso
5	Tecnologías de Firewall
6	Firewalls Basados en Zonas
7	Operación e Implementación de IPS
8	Seguridad de Punto Final
9	Consideraciones de Seguridad de Capa 2
10	Integridad y Autenticidad Básicas
11	Implementar VPN IPsec de Sitio a Sitio con CLI
12	Configuración de NGFW
13	Pruebas de Seguridad de Red

Módulo 4: Gestion de Riegos de la Ciberseguridad (0 h.)

Nro.	Tema
1	Definición de Política de Seguridad
2	Identificación de Activos y Evaluación de Riesgos
3	Gestión de Riesgos
4	Selección de Controles
5	Implementación de Controles
6	Formación y Concienciación
7	Monitoreo y Revisión de Controles

Módulo 5: Auditoria de la Ciberseguridad (30 h.)

Nro.	Tema
1	Fundamentos de la Auditoría de Ciberseguridad
2	Estandarización de la Auditoría
3	Auditoría de la Continuidad del Negocio
4	Gestión de Cumplimiento y Auditoría
5	Control y Auditoría de Ciberseguridad
6	Modelos de Riesgo de Ciberseguridad
7	Auditoría de Arquitecturas Cloud en AWS
8	Obtención y Análisis de Evidencia Electrónica
9	Automatización de Auditorías de Ciberseguridad
10	Casos Prácticos y Simulaciones de Auditoría de Ciberseguridad