CMCS – Certificado MILE-SEC CiberSeguridad

Temario

- Arquitectura de Red
- Ataques contra Dispositivos de Red
- Topologías y Diseño de Red
- Capa3 IP, ICMP
- Capa 4 TCP, UDP
- Dispositivos de Red
- Encaminamiento
- Seguridad de Dispositivos
- Seguridad en Virtualización y la Nube
- Asegurar Redes Inalámbricas
- Defensa en Profundidad
- Riesgo, Amenazas, Vulnerabilidades
- Triada CIA
- Estrategias para Defensa en Profundidad
- Control de Acceso
- Gestión de Contraseñas
- Políticas en Seguridad
- Controles CIS
- Brechas en Seguridad
- Ransomware
- Estrategias para Defensa
- Tipos Comunes de Ataque
- Funcionamiento de las Aplicaciones Web
- Mejores Prácticas para Crear Aplicaciones Web Seguras
- Identificar y Arreglar Vulnerabilidades en Aplicaciones Web
- Gestión de Amenazas y Vulnerabilidades
- Escaneo de Redes
- Pruebas de Penetración
- Dispositivos para Seguridad de Redes
- Firewalls, NIDS, NIPS
- Seguridad de Endpoints
- HIDS y HIPS
- Gestión de Logs / SIEM
- Técnicas y Herramientas para Defensa Activa
- Criptografía
- Tipos de Criptosistemas
- Conceptos Criptográficos
- Criptosistemas Simétricos y Asimétricos
- Encriptación de Datos en Tránsito y Reposo
- Gestión de Llaves
- Fundamentos de Manejo de Incidentes
- Etapas del Proceso para Manejo de Incidentes
- Planes de Contingencia
- Gestión de Riesgos
- Mejores Prácticas para Gestión de Riesgos
- Evaluación de Amenazas, Análisis, y Reporte para Gestión

Presentación

Las organizaciones son el principal objetivo de los ciberatacantes, por lo cual deben estar preparadas para un eventual e inminente compromiso. En la actualidad la detección y respuesta oportunas son fundamentales. Cuanto más tiempo esté presente un ciberatacante en la infraestructura o entorno de la organización, más devastador y dañino será el impacto. La ciberseguridad implica asegurarse de centrarse en las áreas de defensa correctas, especialmente en las referentes a la peculiaridades de la organización. Por lo cual es importante conocer el lenguaje y funcionamiento subyacente de la seguridad informática y seguridad de la información, además de entender la mejor manera de aplicarlos hacia necesidades específicas. Obteniendo los conocimientos en ciberseguridad esenciales y eficaces para la responsabilidad de proteger sistemas y organizaciones.

CMCS
CERTIFICADO MILE-SEC
CIBERSEGURIDAD

Objetivos

Este curso enseña las etapas más efectivas para prevenir ataques, además de detectar ciberatacantes con técnicas prácticas, las cuales pueden ser utilizadas inmediatamente. Se exponen consejos y sugerencias diseñados para ganar la batalla contra una amplia diversidad de cibercriminales, quienes pueden dañar la infraestructura. Ya sea requiera iniciarse en ciberseguridad, o sea un profesional experimentado con un enfoque especializado, este curso le proporciona las habilidades y técnicas en ciberseguridad esenciales necesarias, para proteger y asegurar información crítica, además de activos tecnológicos. También expone cómo aplicar directamente los conceptos aprendidos en una estrategia defensiva en base a los realizado por los ciberatacantes.