Diplomado

Tecnologías de Ciberseguridad - Live

Duración 115 horas

Objetivo general:

Integra servicios, mecanismos y controles para contribuir a las mejores prácticas de la arquitectura, operación y gobierno de ciberseguridad alineados con los objetivos de la organización.

Beneficio:

Conocer y aplicar conceptos relacionados con la ciberseguridad, dando una perspectiva de amenazas y soluciones al participante para cubrir la demanda actual de profesionales en el área.

Que la organización cuente con profesionales en el área de ciberseguridad capaces de responder a las amenazas actuales.

Dirigido a:

Analistas y Gerencia que cuenta con 1 a 15 años de experiencia

Formación de Tecnologías de la Información (técnica o profesional) con interés y/o necesidad de conocer o actualizarse sobre el área de ciberseguridad.

Requisito:

Se recomienda contar con una licenciatura terminada (solo experiencia equivalente en el área de Tecnologías de la Información) con aproximadamente 3 años de experiencias en tecnologías de información y contar con conocimientos básicos en administración y uso de sistemas operativos, fundamentos de redes, fundamentos de computación, lógica de programación y conceptos básicos de seguridad.

Contenido:

Módulo 1 Introducción y Tendencias de Ciberseguridad

Identifica en un contexto general de la ciberseguridad, a través de un recorrido de la evolución de ataques, tecnologías de seguridad y sus implicaciones y retos en el ámbito corporativo actual.

Temario

1. Antecedentes y conceptos de seguridad informática.
2. Estadísticas relacionadas a la seguridad informática.
3. Certificaciones y estándares en seguridad informática.
4. Tecnologías de Ciberseguridad.
5. Estado actual de la ciberseguridad.
6. Evolución de los ataques.

Duración del módulo: 10 horas

Módulo 2 Gestión de Riesgos y Comunicación con el Negocio

Evalúa la mejor manera para gestionar un programa de seguridad de la información y así poder minimizar riesgos, desde la definición de la estrategia hasta cómo conectar cada actividad del día a día.

Temario

1. Contexto del área de ciberseguridad en la organización.
2. Análisis de costos.
3. Riesgos de negocio.
4. Presentaciones ejecutivas.
5. Gobierno de seguridad.
6. Evaluación y análisis de riesgos (Ejercicio costo-beneficio)
7. KPIs & Key Risk Indicators.
8. Estructuras de análisis de riesgo (OCTAVE, FAIR, NIST[1] [2] [3]).

Duración del módulo: 10 horas

Módulo 3 Marcos de referencias de Ciberseguridad

Identifica el marco de ciberseguridad adecuado de acuerdo a los objetivos de la organización.

Temario

1. Uso de regulaciones y frameworks de seguridad
2. ISO 27000
3. NIST
4. CIS
5. Implementación de Marcos de Ciberseguridad.

Duración del módulo: 10 horas

Módulo 4 Seguridad en Sistema Operativos y Herramientas de Seguridad

Valora las características principales de los sistemas Windows/Unix/Linux, así como herramientas, mejores prácticas para asegurar los sistemas y herramientas de seguridad.

Temario

1. Orígenes e Historia.
2. Criptografía
3. Arquitectura de Seguridad de Windows y UNIX
4. Elementos principales los Sistemas Operativos.
5. Los sistemas de archivos.
6. Los archivos de inicialización.
7. Monitoreo del sistema.
8. Bitácoras.
9. Los servicios del sistema.
10. Calendarización tareas.
11. Sistemas de archivos de red.
12. Introducción a herramientas de seguridad
13. Firewalls de Host
14. Detectores de intrusos
15. Malware

Duración del módulo: 15 horas

Módulo 5 Seguridad en Redes

Evalúa el funcionamiento y características de los dispositivos que conforman una red física e inalámbrica, al igual que definir arquitecturas de seguridad dentro de una organización.

Temario

1. Introducción a la seguridad de la red
2. Definición y componentes del perímetro de seguridad.
3. Seguridad en Capa 1, Capa 2 y Capa 3
4. Soluciones generales a ataques
5. Introducción a tecnologías inalámbricas.
6. El protocolo IEEE 802.11.
7. Protocolos (WEP/WPA/WPA2)
8. Ataques a redes inalámbricas
9. Esquemas de defensa para redes inalámbricas.

Duración del módulo: 15 horas

Módulo 6 Seguridad en IoT y Nube

Evalúa los componentes de la ciberseguridad aplicado en elementos de nube y dispositivos móviles.

Temario

1. Introducción a la nube (OnPremise vs Cloud) y IoT
2. Modelo de Servicios: SaaS, PaaS and IaaS
3. Responsabilidades del cliente de los servicios en la nube
4. Arquitectura Cloud y IoT
5. Retos Operativos
6. Amenazas
7. Elementos de seguridad
8. Modelo Pardue

Duración del módulo: 10 horas

Módulo 7 Pruebas de Penetración

Identifica técnicas y tácticas de ataque utilizadas dentro de las metodologías de pruebas de penetración.

Temario

1. Introducción a Ethical Hacking
2. Sniffers
3. Software para inyección de paquetes
4. Crackeo de contraseñas en línea y fuera de línea
5. Escaneo de puertos y vulnerabilidades

Duración del módulo: 10 horas

Módulo 8 Gestión de Vulnerabilidades, Monitoreo de Seguridad y Ciberinteligencia

Define los procesos para ejecutar un programa de gestión de vulnerabilidades dentro de una organización.

Sintetiza la información de elementos internos y externos a la organización para la identificación de amenazas.

Temario

1. Gestión de activos
2. Herramientas para la gestión de vulnerabilidades
3. Priorización y remediación de vulnerabilidades
4. Sistemas de parcheo
5. Definición de la tecnología de IDS/IPS
6. Herramientas para colección y correlación de eventos.
7. El problema de la definición de las intrusiones.
8. Marco de referencia ATT&CK MITRE
9. Threat Hunting
10. Análisis y detección de evento malicioso
11. Indicadores de compromiso (IOC)

Duración del módulo: 15 horas

Módulo 9 Respuesta a Incidentes

Define los principales procesos de respuesta a incidentes para lograr una recuperación eficaz y eficiente de un ciberataque.

Temario

1. Definición y principios.
2. Preparándose para el incidente
3. La respuesta al incidente.
4. Errores técnicos.
5. Respuesta en vivo.
6. Búsqueda de evidencia en diversas plataformas y sistemas operativos (Windows, Android y IOS)

Duración del módulo: 10 horas

Módulo 10 Forense Digital

Identifica procesos y metodologías de cómputo forense

Temario

1. Necesidad de investigación.
2. Tipos de análisis forense.
3. Metodologías del cómputo forense.
4. Importancia de la evidencia.
5. Cadena de custodia.
6. Manejo de evidencia.
7. Ejecución de análisis forense.
8. Presentación de hallazgos

Duración del módulo: 10 horas