**Plan Curricular**

**MÓDULO 1 – EVALUACIONES DE CIBERSEGURIDAD.**

**Duración:** 36 (TREINTA Y SEIS) horas

**Contenidos:** Tipos de evaluaciones. Revisiones de seguridad física y ambiental. Cyber Kill Chain. Ingeniería social. OSINT. Reconocimiento, acceso inicial, escalada de privilegios y movimiento lateral para explotar vulnerabilidades y debilidades de sistemas. Pruebas de intrusión. Hacking ético. Método de Red Team. Herramientas de evaluación. Tácticas, técnicas y procedimientos de ciberataques. Simulación y emulación de ciberataques. Elaboración de informes y acciones de mejoras.

**MÓDULO 2 – ANÁLISIS DE MALWARE.**

**Duración:** 36 (TREINTA Y SEIS) horas

**Contenidos:** Tipos de malware. Enumeración y caracterización de atributos (MAEC). Fundamentos de ingeniería inversa. Métodos de análisis de malware. Métodos de obtención de malware. Laboratorio análisis de malware. Técnicas de Ofuscación. Restricción de los entornos de ejecución. Amenazas Avanzadas Persistentes (APT). Fases de un ataque de un APT. Estrategias de defensa antimalware.

**MÓDULO 3 – ANÁLISIS DE CIBERATAQUES.**

**Duración:** 36 (TREINTA Y SEIS) horas

**Contenidos:** Tácticas, técnicas y procedimientos en las diferentes fases de un ciberataque. Reconocimiento. Desarrollo de recursos. Acceso inicial. Ejecución. Persistencia. Escalamiento de privilegios. Evasión de defensa. Acceso a credenciales. Descubrimiento. Movimiento lateral. Colección. Comando y control. Exfiltración. Impacto. Mapa de APT. Análisis de tendencias de ciberataques.

**MÓDULO 4 – ANÁLISIS FORENSE Y RESPUESTA A INCIDENTES.**

**Duración:** 36 (TREINTA Y SEIS) horas

**Contenidos:** Particularidades del Análisis Forense en otras plataformas (Linux, Cloud, Android). Respuesta inmediata a incidentes, búsqueda de amenazas y análisis forense digital. Análisis forense en memoria. Análisis forense de redes. Análisis forense en TO. Análisis forense en criptosistemas. Técnicas antiforenses. Descubrimiento proactivo de amenazas en desarrollo.

**MÓDULO 5 – INFRAESTRUCTURA DE CIBERDEFENSA.**

**Duración:** 36 (TREINTA Y SEIS) horas

**Contenidos:** Seguridad (security) e inmunidad (safety). Amenazas a las Tecnologías de Operación (TO). Amenazas a SCADA/ICS. Tecnologías de sistemas embebidos, IoT, sistemas de control, SCADA y sistemas de control industrial. Estándares para seguridad (security) e inmunidad (safety) de infraestructuras críticas. Ciberseguridad en sistemas militares: Sistemas de Comando y Control, Sistemas de Armas, Sistemas de Comunicaciones, Sistemas de Control y Sistemas de Cómputo de las Infraestructuras Críticas del Instrumento Militar. Ciberdefensa de sistemas y componentes de Objetos de Valor Estratégicos.

**MÓDULO 6 – EJERCICIO FINAL INDIVIDUAL**.

**Duración: 20 (VEINTE) horas.**

**Desarrollo:** Se planteará una situación o problema a solucionar representado por casos hipotéticos en base a hechos reales. El/la estudiante deberá resolverlo aplicando técnicas y procedimientos de operaciones de ciberdefensa.

**Contenidos:** Ejercicios de nivel táctico sobre escenarios hipotéticos de operaciones cibernéticas, basados en casos de estudio conocidos:

Ciberdefensa frente de herramientas ofensivas desarrolladas por un Estado.

Revisión técnica de ciberarmas. Herramientas de vigilancia y control del ciberespacio soberano. Operaciones cibernéticas contra datos informáticos. Campaña de ransomware. Ciberengaño durante un conflicto armado. Métodos cibernéticos de guerra. Ciberoperaciones como detonante del derecho internacional de los conflictos armados.