TITULO DEL CURSO

PERITO JUDICIAL EXPERTO/A EN CIBERTERRORISMO Y DELITOS INFORMÁTICOS

PROGRAMA ACADÉMICO

MÓDULO 1. ORIGEN Y FUNDAMENTOS TÉCNICOS DEL CIBERTERRORISMO

TEMA 1: INTRODUCCIÓN AL CIBERTERRORISMO Y CIBERESPACIO

- Origen y primeros pasos del ciberterrorismo
- Definición y tipologías de ciberterrorismo
- Diferencias entre ciberterrorismo, cibercrimen y hacktivismo
- Principales actores y motivaciones
- Evolución tecnológica y adaptación de los grupos terroristas
- El ciberespacio como nuevo ámbito de conflicto
- Breve síntesis del Marco jurídico nacional e internacional

TEMA 2. CARACTERÍSTICAS DEL CIBERTERRORISMO: HERRAMIENTAS Y TÉCNICAS DE ATAQUE

- Métodos de intrusión y explotación de vulnerabilidades
- Malware, ransomware y ataques DDoS
- Ingeniería social y phishing dirigido
- Técnicas de anonimización y ocultamiento de la identidad
- Uso de la inteligencia artificial: deepfakes, fakes new y el juego de la desinformación

TEMA 3: INFRAESTRUCTURAS CRÍTICAS Y CIBERSEGURIDAD

- Concepto y clasificación de infraestructuras críticas
- Vulnerabilidades de sistemas SCADA e industriales
- Medidas de protección y reacción ante ataques
- Ejemplos recientes de ataques a infraestructuras críticas

MÓDULO 2: **INVESTIGACIÓN Y CIBERINTELIGENCIAA**

TEMA 4: OBTENCIÓN Y ANÁLISIS DE INFORMACIÓN EN EL CIBERESPACIO

- Concepto y clasificación de infraestructuras críticas
- Vulnerabilidades de sistemas SCADA e industriales
- Medidas de protección y reacción ante ataques
- Ejemplos recientes de ataques a infraestructuras críticas

TEMA 5: CIBERINTELIGENCIA POLICIAL Y OPERATIVA

- Ciclo de inteligencia aplicado a ciberterrorismo
- Producción y análisis de CYBINT (Cyber Intelligence)
- Herramientas de cibervigilancia y monitorización
- Caso práctico: identificación y seguimiento de amenazas

MÓDULO 3: RESPUESTA LEGAL NACIONAL E INTERNACIONALA AL CIBERTERRORISMO

TEMA 7: NORMATIVA INTERNACIONAL Y COMUNITARIA SOBRE CIBERTERRORISMO

- Metodología de análisis forense en incidentes de ciberterrorismo
- Extracción y preservación de evidencias digitales
- Recuperación de datos y elaboración de informes
- Colaboración con fuerzas y cuerpos de seguridad

TEMA 8: NORMATIVA ESPAÑOLA EN MATERIA DE CIBERTERRORISMO

- Delitos informáticos y tipificación penal en España
- Competencias y actuación de las Fuerzas y Cuerpos de seguridad del Estado
- Procedimientos de investigación y obtención de pruebas
- Protección de infraestructuras críticas en la legislación nacional

TEMA 9: RESPONSABILIDAD Y LÍMITES DE LA CIBERVIGILANCIA.

- Garantías constitucionales y derechos fundamentales
- Límites legales en la obtención de información digital
- Figura del agente encubierto y registro remoto de equipos
- Control judicial y protección de datos personales

MODULO 4: EL CIBERTERRORISMO EN EL ÁMBITO DEL DERECHO PENAL Y DERECHO PROCESAL PENAL

TEMA 10: LA OBTENCIÓN DE PRUEBA EN MATERIA DE CIBERDELINCUENCIA

- La obtención de prueba de cargo para poder condenar por estos delitos
- La intervención de Europol y Eurojust en la obtención de las fuentes de prueba
- Retos probatorios en delitos de ciberterrorismo
- Admisibilidad y la importancia de la cadena de custodia de la evidencia digital
- Prueba pericial informática en procesos de ciberterrorismo

TEMA 11: POLÍTICAS PÚBLICAS Y PLANES DE PREVENCIÓN

- Estrategias nacionales de ciberseguridad y lucha antiterrorista
- Planes de prevención y respuesta ante incidentes
- Colaboración público-privada en la protección de infraestructuras
- Evaluación de riesgos y análisis DAFO aplicado a ciberterrorismo

TEMA 12: PROPUESTAS Y ESTRATEGIAS DE RESPUESTA. DEBATE ÉTICO-JURÍDICO.

- Estudio de casos reales de ciberterrorismo
- Simulación de respuesta legal ante un ataque
- Debate jurídico sobre nuevas amenazas y lagunas legales
- El dilema entre el control y la libertad
- Propuestas de mejora en la política criminal diseñada para combatir el ciberterrorismo

MODULO 5: REDACCIÓN DE UN INFORME PERICIAL SEGÚN NORMA UNE 197001:2011

REALIZACIÓN DE UN INFORME PERICIAL (2)

Bibliografía

Anexos

IMPARTIDO POR LA UNED MÁLAGA

300 H LECTIVAS (12 CRÉDITOS)