

TITULO DEL CURSO

CURSO DE PERITO/A JUDICIAL EXPERTO/A EN OSINT AVANZADO Y
CIBERINTELIGENCIA FORENSE

PROGRAMA ACADÉMICO

MÓDULO 1: RECORDATORIO OPERATIVO DE OSINT Y CICLO DE INTELIGENCIA

TEMA 1. REPASO DE OSINT

- Metodología de obtención OSINT y fuentes abiertas.
- Entorno seguro de investigación (VM, VPN, identidades, perfiles).
- Técnicas de búsqueda, pivoteo y filtrado.
- Herramientas OSINT clave y su finalidad.
- Síntesis del proceso de documentación e informe OSINT.

TEMA 2. INTRODUCCIÓN AL CICLO DE INTELIGENCIA Y SU INTEGRACIÓN CON OSINT

- Conceptos de inteligencia (estratégica / operativa / táctica).
- Etapas del ciclo (planificación, obtención, análisis, difusión).
- Requerimientos de información y matrices PIR (Private Information Retrieval).
- Inteligencia accionable vs. conocimiento descriptivo.
- Papel del OSINT dentro de la multi-inteligencia (SIGINT, HUMINT, TECHINT, GEOINT).

TEMA 3. REQUERIMIENTOS DE INFORMACIÓN, TASKING Y TRADECRAFT CON OSINT

- Definición y refinado de requerimientos (RFI).
- Modelo de hipótesis y enfoque por necesidades.
- Tradecraft y estándares profesionales (NATO, IC, LEA, SOC/CTI).
- Trazabilidad y rigor analítico.
- Evaluación de fuentes (Fiabilidad, veracidad, oportunidades y riesgos).

Sistema de evaluación: 1 examen tipo test y un caso práctico relacionado con los temas del módulo

MÓDULO 2: CIBERINTELIGENCIA CON OSINTPLICADA A AMENAZAS Y ACTIVOS

TEMA 4. OSINT EN LA INTELIGENCIA DE AMENAZAS (CTI) Y ACTORES HOSTILES

- Frameworks de amenaza (MITRE ATT&CK, D3FEND, Diamond Model).
- Tipologías de actores (APT, criminal, hacktivismo, insider, competidor).
- TTPs observables y artefactos rastreables OSINT.
- Correlación OSINT con CTI técnico (IOCs, TTPs y campañas).
- Casos reales y simulaciones de actores.

TEMA 5. OSINT EN LA INTELIGENCIA DE SUPERFICIE, DEEP Y DARK WEB

- Modelización del espacio digital (surface / deep / dark).
- Fuentes y mercados ilícitos OSINT-accessibles.
- Productos de inteligencia útiles (credenciales, leaks, vendor rating).

- Metodologías de análisis de leaks y data-breaches.
- Riesgos legales, técnicos y operativos.

TEMA 6. DETECCIÓN, ATRIBUCIÓN Y CORRELACIÓN CON OSINT

- Técnicas de atribución (infraestructura, tiempo, idioma, cadena comercial).
- Pivoting y fingerprinting de actores / dominios / perfiles.
- Resolución de identidades digitales y alias.
- Contraste multi-fuente y exclusión de falsos positivos.
- Limitaciones, incertidumbre y estándares de atribución.

Sistema de evaluación: 1 examen tipo test y un caso práctico relacionado con los temas del módulo

MÓDULO 3: ANALÍTICA E INTELIGENCIA DECISIONAL CON OSINT

TEMA 7. ANALÍTICA ESTRUCTURADA Y REDUCCIÓN DE SESGOS CON OSINT

- Sesgos cognitivos frecuentes en inteligencia.
- Técnicas ACH (Analysis of Competing Hypotheses).
- Red-teaming y challenge analysis.
- Técnicas de visualización y clustering/relaciones.
- Evaluación de escenarios y conclusiones narrativas.

TEMA 8. OSINT EN LA CIBERINTELIGENCIA EMPRESARIAL / GUBERNAMENTAL

- Inteligencia competitiva y corporativa.
- Inteligencia para ciberdefensa institucional.

- Inteligencia para cumplimiento normativo y due diligence.
- Inteligencia en crisis, reputación y gestión de incidentes.
- Modelos de madurez de inteligencia (SOC/CTI/Threat Intelligence Units).

Sistema de evaluación: 1 examen tipo test y un caso práctico relacionado con los temas del módulo

MÓDULO 4: PRODUCCIÓN, INFORMES Y OPERACIONES

TEMA 9. OPERACIONES DE CIBERINTELIGENCIA Y EJERCICIOS PRÁCTICOS

- Operaciones continuas vs. puntuales (tasking, watch y tracking).
- Integración de feeds, monitoreo y alertas.
- Simulación de incidentes y campañas hostiles.
- Trabajo multidisciplinar (LEA, SOC, CERT, Legal, Dirección).

TEMA 10. PRODUCCIÓN DE INTELIGENCIA ORIENTADA A LA LABOR PERICIAL

- Estándares y formatos del dictamen pericial basado en inteligencia digital.
- Requisitos legales, probatorios y procesales del informe pericial.
- Trazabilidad de fuentes OSINT y documentación de evidencias digitales.
- Metodologías analíticas y niveles de confianza aplicados al dictamen.
- Presentación del informe con anexos técnicos y limitaciones formales.

Sistema de evaluación: 1 examen tipo test y realización de un informe pericial (1)

MÓDULO 5:

Realización de un informe pericial (2)

Bibliografía

Anexos

CURSO DE 300 H LECTIVAS
12 CRÉDITOS