Designação do Curso	Ciber Inteligência e Operações Baseadas em Inteligência de Fontes Abertas (OSINT)
Àrea de Formação:	481 - Informática
Modalidade de formação:	B-learning
Forma de organização:	
Nº Mínimo de Formandos	8
Nº Máximo de Formandos	16
Carga horária total:	44
Horas de formação teórica:	20
Horas de formação prática:	24
Equipa Pedagógica:	
Coordenador Pedagógico:	
Formadores	
Data de início	
Data de Fim	
Horário de funcionamento	
Local de realização	

OBJETIVOS DO PROGRAMA

Objetivos Gerais:	No Final do Curso os formandos devem estar aptos a: • Desenvolver uma compreensão abrangente das operações de inteligência e seu papel nos desafios contemporâneos de segurança. • Adquirir conhecimentos e capacidades na utilização de ferramentas, técnicas e metodologias de OSINT para recolha de inteligência. • Compreender as considerações éticas e legais associadas ao OSINT e às operações de inteligência. • Analisar e avaliar fatores geopolíticos e estratégias de dissuasão (deterrence) relevantes para operações de inteligência. •
Objetivos especificos:	No final da formação espera-se que os formandos estejam aptos a: • Obter insights sobre o cenário de ciber-ameaças e a integração do OSINT na ciber-guerra. • Aplicar técnicas avançadas de OSINT para inteligência em *media* social, recolha de dados na web, investigações na darkweb e métodos analíticos dos mesmos. • Aprender abordagens de fusão de inteligência, colaboração e elaboração efetiva de relatórios de descobertas de inteligência.

PRÉ-REQUISITOS E FORMA DE SELEÇÃO

Condições de Acesso:	Conhecimentos de Informática, Cibersegurança, Segurança de redes
Forma de seleção	Entrevista Individual

AVALIAÇÃO

A avaliação dos formandos será feita, de forma contínua, através de parâmetros **quantitativos**:

- Ficha de avaliação no Final de cada Unidade (Formativa)
- Ficha de Avaliação Final (Sumativa)
- Assiduidade (frequência mínima de 90% da carga total do curso, não podendo faltar a uma unidade por completo)

E com base em parâmetros **qualitativos**, por observação:

- Pontualidade, Participação, Motivação, Interesse, Maturidade, Relacionamento com os colegas e Relacionamento com os formadores

A Classificação Final = **Classificação da Ficha de avaliação final** (ponderada em relação aos parâmetros qualitativos)

Serão aprovados todos os formandos com uma **Classificação Final igual ou superior a 50%**, de acordo com a seguinte escala avaliativa:

0% - 49%	Insuficiente	Não Apto
50% - 69%	Suficiente	Apto
70% a 89%	Bom	
90% a 100%	Muito Bom	

A todos os formandos que obtiverem aproveitamento será entregue um Certificado de Formação Profissional emitido pela entidade formadora.

O não cumprimento das regras de assiduidade, a falta de aproveitamento, ou o não pagamento das prestações previstas determinam a não emissão do Certificado de Formação Profissional.

Conteúdos e Estratégia pedagógica

Unidades Temática/ Módulo 1	Objectivos No final da unidade os formandos deverão estar aptos a:	Temas/Conteúdos Programáticos	Metodologia Pedagógica	Recursos e atividades Didáticas
Introdução às Operações de Inteligência e OSINT	• Compreender os fundamentos das operações de inteligência e OSINT. • Entender a importância do OSINT na recolha de inteligência na atualidade. • Desenvolver consciência das considerações legais e éticas associadas ao OSINT. • Adquirir conhecimentos básicos sobre ferramentas, técnicas e metodologias de OSINT.	• Introdução às Operações de Inteligência: Conceitos, princípios e objetivos • Compreensão do Papel do OSINT na recolha de Inteligência • Visão Geral do Panorama de Ameaças Modernas e a Importância do OSINT • Considerações Éticas e enquadramentos Legais no OSINT • Introdução às Ferramentas, Técnicas e Metodologias de OSINT	Sessões Teóricas expositivas e práticas em laboratóro	Laboratório de redes informáticas, computadores, servidores e software de sistemas operativos

Conteúdos e Estratégia pedagógica

Unidades Temática/ Módulo 2	Objectivos No final da unidade os formandos deverão estar aptos a:	Temas/Conteúdos Programáticos	Metodologia Pedagógica	Recursos e atividades Didáticas
Operações Encobertas (Covert) e Inteligência	• Compreender o conceito e objetivo das operações encobertas. • Obter insights sobre o planeamento e execução de operações clandestinas. • Reconhecer o papel da recolha de inteligência em operações encobertas. • Analisar a relação entre operações encobertas e OSINT. • Avaliar estudos de caso para compreender a aplicação prática de operações encobertas e recolha de inteligência.	• Operações Clandestinas: Definição, objetivos e contexto histórico • Planeamento e Execução de Operações Encobertas • Recolha de Inteligência em Operações Encobertas • Operações Encobertas e OSINT: Sinergias e Desafios • Estudos de Caso: Exemplos reais de operações encobertas bem-sucedidas e seus aspectos de inteligência.	Sessões Teóricas expositivas e práticas em laboratório	Laboratório de redes informáticas, computadores, servidores e software de sistemas operativos

Conteúdos e Estratégia pedagógica

Unidades Temática/ Módulo 3	Objectivos No final da unidade os formandos deverão estar aptos a:	Temas/Conteúdos Programáticos	Metodologia Pedagógica	Recursos e atividades Didáticas
Geopolítica, Dissuasão e Cibersegurança	• Avaliar os fatores geopolíticos com impacte nas operações de inteligência. • Compreender a teoria e aplicação de estratégias de dissuasão. • Identificar principais ciber-ameaças, atores e motivações. • Analisar o papel do OSINT na avaliação de riscos geopolíticos e estratégias de dissuasão. • Utilizar técnicas de OSINT para recolher e analisar inteligência sobre ciber-ameaças.	• Considerações Geopolíticas em Operações de Inteligência • Compreendendo a Dissuasão: Teoria e Aplicação • Cenário de Cibersegurança: Ameaças, Atores e Motivações • O Papel do OSINT na Avaliação de Riscos Geopolíticos e Estratégias de Dissuasão • Análise de Inteligência sobre Ciber-ameaças por meio de OSINT	Sessões Teóricas expositivas e práticas em laboratóro	Laboratório de redes informáticas, computadores, servidores e software de sistemas operativos

Conteúdos e Estratégia pedagógica

Unidades Temática/ Módulo 4	Objectivos No final da unidade os formandos deverão estar aptos a:	Temas/Conteúdos Programáticos	Metodologia Pedagógica	Recursos e atividades Didáticas
Doutrina Militar e Ciber Guerra	• Compreender a doutrina militar no domínio cibernético. • Explorar estratégias e táticas de Ciber Operações ofensivas e defensivas. • Identificar o papel do OSINT em Ciber Operações militares. • Analisar estudos de caso que integrem OSINT em Ciber Operações militares.	• Doutrina Militar no Domínio Cibernético: Princípios e Componentes • Ciber Operações Ofensivas: Estratégias e Táticas • Ciber Operações Defensivas: Técnicas e Melhores Práticas • Integrando o OSINT em Ciber Operações Militares • Estudos de Caso: Ciber Operações Militares e Integração de OSINT	Sessões Teóricas expositivas e práticas em laboratóro	Laboratório de redes informáticas, computadores, servidores e software de sistemas operativos

Conteúdos e Estratégia pedagógica

Unidades Temática/ Módulo 5	Objectivos No final da unidade os formandos deverão estar aptos a:	Temas/Conteúdos Programáticos	Metodologia Pedagógica	Recursos e atividades Didáticas
Técnicas Avançadas de OSINT	• Explorar técnicas avançadas para inteligência em social media (SOCMINT) • Compreender a data scrapping na web e mineração de dados para fins de OSINT. • Familiarizar-se com técnicas e considerações para investigações na dark web. • Aprender métodos analíticos avançados para análise de OSINT.	• Inteligência em Social Media (SOCMINT): Estratégias e Ferramentas • Web Data Scrapping e Mining de Dados para OSINT • Investigação na Dark Web: Técnicas e Considerações • Métodos Analíticos Avançados em OSINT	Sessões Teóricas expositivas e práticas em laboratório	Laboratório de redes informáticas, computadores, servidores e software de sistemas operativos

Conteúdos e Estratégia pedagógica

Unidades Temática/ Módulo 6	Objectivos No final da unidade os formandos deverão estar aptos a:	Temas/Conteúdos Programáticos	Metodologia Pedagógica	Recursos e atividades Didáticas
Fusão de Inteligência e Relatórios	• Compreender o conceito e a importância da fusão de inteligência. • Explorar centros de fusão e colaboração em operações de inteligência. • Aprender técnicas eficazes de relatórios e disseminação de descobertas de inteligência. • Descobrir como aproveitar o OSINT para fins de fusão de inteligência e relatórios.	• Fusão de Inteligência: Conceitos e Abordagens • Centros de Fusão e Colaboração em Operações de Inteligência • Relatórios e Disseminação de Descobertas de Inteligência • Aproveitando o OSINT para Fusão de Inteligência e Relatórios	Sessões Teóricas expositivas e práticas em laboratório	Laboratório de redes informáticas, computadores, servidores e software de sistemas operativos

Conteúdos e Estratégia pedagógica

Unidades Temática/ Módulo 7	Objectivos No final da unidade os formandos deverão estar aptos a:	Temas/Conteúdos Programáticos	Metodologia Pedagógica	Recursos e atividades Didáticas
Recolha de Inteligência na Darknet	• Compreender o conceito e a importância da Darknet no cenário de cibersegurança. • Obter insights sobre os conceitos-chave, tecnologias e ferramentas associadas à recolha de inteligência na Darknet. • Identificar e analisar diferentes tipos de atividades e atores de ameaças na Darknet. • Adquirir conhecimento sobre considerações legais e éticas ao conduzir investigações na Darknet. • Aplicar habilidades práticas por meio de estudos de caso e exercícios práticos para recolher inteligência na Darknet de forma eficaz.	• Introdução à Darknet e Cibersegurança • Conceitos-chave de Recolha de Inteligência na Darknet • Ferramentas e Técnicas para Coleta de Inteligência na Darknet • Atores e Atividades de Ameaças na Darknet • Estudos de Caso e Exercícios Práticos	Sessões Teóricas expositivas e práticas em laboratório	Laboratório de redes informáticas, computadores, servidores e software de sistemas operativos

Conteúdos e Estratégia pedagógica

Unidades Temática/ Módulo 8	Objectivos No final da unidade os formandos deverão estar aptos a:	Temas/Conteúdos Programáticos	Metodologia Pedagógica	Recursos e atividades Didáticas
Exercício Real baseado em Gamificação	• Aplicar o ciclo de inteligência e metodologias para operações eficazes de inteligência cibernética. • Adquirir experiência prática em resposta a incidentes, busca de ameaças e análise de APTs com base em cenários da vida real. • Desenvolver habilidades na condução de investigações de OSINT e coleta de inteligência de fontes abertas. • Aprimorar habilidades de tomada de decisão e formulação de contramedidas contra ciber-ameaças. • Aplicar ferramentas e técnicas de OSINT para coletar informações em cenários do mundo real. • Desenvolver habilidades em resposta a incidentes, perfil de atores de ameaças e investigações de engenharia social.	• Cenário Realista 1: Resposta a Incidentes e Buca de Ciber Ameaças • Cenário Realista 2: Análise de Ameaças Persistentes Avançadas (APT) • Cenário Realista 3: Engenharia Social e Ameaças Internas • Atribuição e Relatórios para Mitigação • Condução de Coleta Cibernética e OSINT para Identificar Atores de Ameaças e Malware • Revisão dos Resultados e Insights dos Exercícios	Sessões Teóricas expositivas e práticas em laboratório	Laboratório de redes informáticas, computadores, servidores e software de sistemas operativos

Carga horária Total	**60 h**