**PROJETO PEDAGÓGICO – PROGRAMA DE QUALIFICAÇÃO PROFISSIONAL**

| INSTITUIÇÃO DE ENSINO | |
|---|---|
| **INTITUIÇÃO DE ENSINO** | Unieducar |
| **CREDENCIAMENTO** | Parecer 0305/2021 - Câmara de Educação Superior e Profissional |
| **MANTENEDORA** | Unieducar Inteligência Educacional – CNPJ 05.569.970/0001-26 |
| **REGISTRO MEC SISTEC** | 43970 – SISTEC - Parecer CEE-CE No. 305/2021 |
| **REGISTRO SICAF – PJ** | 170038 |
| **REGISTRO ABED** | 5.139 – Categoria Institucional |
| **REGISTRO CFA/CRA** | PJ – 3457 – CE |

Declaramos, a pedido do(a) interessado(a), e para fins de prova junto ao respectivo órgão empregador, que o curso abaixo citado encontra-se disponível para matrícula, como programa de **Extensão / Capacitação**, junto à **Unieducar**, com data para início e término a definir, conforme carga horária assinalada.

**METODOLOGIA**: O conteúdo dos cursos de Extensão pode ser disponibilizado conforme a evolução do programa, e em função de sua correspondente carga horária. Os objetos instrucionais são apresentados em uma interface diagramada de fácil navegação no Ambiente Virtual de Aprendizagem – AVA. O acesso às videoaulas e demais objetos instrucionais, além de materiais extras disponíveis na biblioteca (e-books), exercícios, audioaulas e videoteca é bastante intuitivo e proporciona uma experiência de interatividade no processo de aprendizagem a distância. Os programas preveem a participação do aluno em atividades de interação no AVA. Tais atividades - passíveis de serem comprovadas, podem ocorrer por meio de conversação em tempo real, fóruns, videoconferências, jogos, aulas participativas, trabalhos em equipe, discussões, dinâmicas de grupo, estudos de caso ou simulações.

**CRONOGRAMA DE ATIVIDADES DA AÇÃO DE DESENVOLVIMENTO**: O programa de Extensão / Capacitação prevê a participação ativa do inscrito nas diversas atividades propostas. O aluno matriculado em um programa de capacitação deve cumprir rigorosamente com o cronograma de atividades a seguir detalhado, aplicando 8 (oito) horas diárias no desenvolvimento das seguintes ações durante todo o período de acesso ao conteúdo:

| ATIVIDADES/HORÁRIOS | 08h-09h | 09h-10h | 10h-11h | 11h-12h | 12h-14h | 14h-15h | 15h-16h | 16h-17h | 17h-18h |
|---|---|---|---|---|---|---|---|---|---|
| Videoaulas Audioaulas | ■ | ■ | | | INTERVALO | ■ | ■ | | |
| E-books Audiobooks | | ■ | ■ | | INTERVALO | | ■ | ■ | |
| Atividades/Interação | | | | ■ | INTERVALO | | | | ■ |
| Suporte c/Tutoria | | | ■ | ■ | INTERVALO | | | ■ | |
| TOTAL DE HORAS DIÁRIAS APLICADAS NO DESENVOLVIMENTO DE ATIVIDADES | | | | | | | | | 8 (OITO) |

**SINCRONICIDADE**: Os programas de Extensão / Capacitação são caracterizados como síncronos, a partir do momento da inscrição, com a indicação por parte do aluno, da data que iniciará, tendo em vista que passa a ter as datas de início e término definidas.

**TUTORIA E FORMAS DE INTERAÇÃO**: Os programas de Extensão / Capacitação recebem suporte de uma tutoria especificamente designada para acompanhamento do rendimento dos alunos. A interação é realizada online por meio da plataforma AVA. A tutoria é desenvolvida de modo proativo e consiste na assistência didática, compartilhamento de informações, troca de experiências, estímulo ao cumprimento dos exercícios propostos e cooperação visando o melhor aproveitamento dos conteúdos estudados. A tutoria é desempenhada pelo corpo de tutores da Unieducar e a interação entre tutores, estudantes e a coordenação do curso é exclusivamente online, onde são agendadas ações síncronas em outras modalidades (fóruns, videoconferências, chats etc.). A tutoria efetiva encaminhará módulos de conteúdos com atividades avaliativas semanalmente, para que o estudante possa complementar os estudos quanto ao tema desenvolvido no curso.

**AVALIAÇÃO/CERTIFICAÇÃO**: Nos programas de Extensão / Capacitação a avaliação é qualitativa e múltipla. A nota da avaliação final pode contemplar fatores e formas de avaliação diversas, tais como a elaboração de redações durante e ao término do programa, bem como a frequência e participação em eventos de conversação em tempo real, nas quais são observadas as contribuições de ordem teórica e prática, além de outras modalidades de avaliação individual, bem, como: a realização de atividade avaliativa ao término de cada aula ou módulo de conteúdo e a realização de atividade avaliativa final, com pontuação, ao término da capacitação. A geração do certificado eletrônico é condicionada à verificação de aproveitamento mínimo de 70% nas atividades de

avaliação. Todos os cursos contam com ferramenta de avaliação de conteúdo (aprendizagem) e institucional, que somente é disponibilizada após transcorrido o prazo mínimo correspondente à carga horária certificada.

**ORGANIZAÇÃO CURRICULAR**: Os programas de Extensão / Capacitação apresentam organização curricular elaborada a partir de projetos pedagógicos específicos, elaborados por uma equipe pedagógica multidisciplinar, que acompanha o projeto, desenvolvimento e atualização de conteúdo. TECNOLOGIA DE EAD/E-LEARNING: Após a elaboração dos conteúdos é realizada a migração para o Ambiente Virtual de Aprendizagem - AVA, o que demanda a aplicação de tecnologias de Design Instrucional adequadas aos assuntos abordados. MATERIAIS DIDÁTICOS: Os conteúdos programáticos dos cursos de Extensão / Capacitação são lastreados em materiais didáticos constantemente atualizados. Dentre os objetos de aprendizagem podem ser disponibilizados videoaulas; livros eletrônicos (e-books); audioaulas; desafios; exercícios e testes; além de conteúdos de fontes externas, a partir de material relacionado. INTERAÇÃO E SUPORTE ADMINISTRATIVO: Os programas de Extensão / Capacitação contam – além do suporte de tutoria especializada - com uma infraestrutura de apoio que prevê a interação entre alunos e alunos; alunos e professores/tutores; e alunos e pessoal de apoio Administrativo. Essa interação é garantida por meios eletrônicos com registros de chamados e/ou por meio telefônico, conforme o caso. O AVA utilizado pela Unieducar é uma plataforma proprietária, desenvolvida e atualizada permanentemente, e permite, dentre outras facilidades, o acompanhamento das horas de estudo a distância e presencial, conforme o caso. SOBRE A

**INSTITUIÇÃO DE ENSINO**: A Unieducar é uma Instituição de Ensino Superior mantida pela Unieducar Inteligência Educacional, que atua – desde 2003 - com a idoneidade e credibilidade atestada por diversos órgãos públicos, e empresas privadas, além de milhares de profissionais, servidores públicos, estudantes e professores universitários de todo o Brasil. Instituição de Ensino Credenciada pelo MEC; cadastrada junto ao SICAF - Sistema de Cadastramento Unificado de Fornecedores do Governo Federal - como fornecedores de cursos e treinamentos junto à Administração Federal. A Unieducar é associada à ABED – Associação Brasileira de Educação a Distância e à IELA - International E-Learning Association. Atende mediante Nota de Empenho todos os órgãos públicos Federais, Estaduais, Distritais e Municipais, emitindo a respectiva documentação fiscal (Nota Fiscal de Prestação de Serviços Eletrônica) vinculada às matrículas.

**ESTRUTURA DO CURSO - COMPONENTES CURRICULARES**

**TÍTULO DO PROGRAMA:** Hacking Ético e Contrainteligência Digital com Inteligência Artificial

**CARGA HORÁRIA:** 400 horas

**PRAZO MÍNIMO PARA CONCLUSÃO:** 50 dias.

**PRAZO MÁXIMO PARA CONCLUSÃO:** 150 dias.

**OBJETIVOS GERAIS:**

O curso **Hacking Ético e Contrainteligência Digital com Inteligência Artificial**, desenvolvido pela Unieducar, capacita profissionais a atuar estrategicamente na proteção de sistemas, redes e dados frente ao crescente número de ataques cibernéticos. O programa aborda desde os **fundamentos do hacking ético**, com uso de **OSINT**, **CSINT**, **Deep Web** e **Tor**, até o domínio de frameworks de segurança como **MITRE ATT&CK**, **Cyber Kill Chain** e **Diamond Model**, além da criação de regras de detecção automatizadas com **Yara**, **Snort** e **Sigma**. Também explora práticas de contrainteligência digital, incluindo **OPSEC**, t**hreat hunting com IA**, **honeypots** e **combate a fake news**, além do uso de plataformas colaborativas como MISP. Trata-se de uma formação completa para quem busca se destacar em cibersegurança, auditoria de sistemas, defesa digital e proteção contra ameaças avançadas, unindo **inteligência artificial** e técnicas modernas de segurança da informação.

**OBJETIVOS ESPECÍFICOS:** Proporcionar ao estudioso na área uma visão abrangente sobre os temas elencados no Conteúdo Programático.

**DESENVOLVIMENTO DO CONTEÚDO:** O desenvolvimento do conteúdo programático requer a realização das seguintes atividades/dinâmicas, com vistas ao cumprimento da correspondente carga horária deste programa de capacitação:

- O aluno deverá assistir e eventualmente voltar a assistir às videoaulas, com o objetivo de fixar o conteúdo trabalhado pelo professor;
- Para cada aula ministrada, o Ambiente Virtual de Aprendizagem – AVA disponibiliza um ou mais e-books, a fim de que o

aluno possa ler e reler os textos de apoio, aprofundando o estudo sobre cada um dos tópicos ministrados, objeto de seu desenvolvimento neste programa;

- O programa disponibiliza ainda uma lista de exercícios propostos, visando a fixação do conteúdo trabalhado, especialmente com questões/problemas que exigem a aplicação dos conceitos desenvolvidos nas aulas e nos livros-texto às situações concretas apresentadas;
- O aluno é também acompanhado por um ou mais tutores designados pela Instituição de Ensino. No AVA, o aluno dispõe ainda de um canal de interação com esses professores especialistas nas matérias objeto das aulas.

Cumprindo então todas essas atividades, agrupadas nos quatro itens acima, o aluno poderá usufruir de uma experiência de aprendizado enriquecedora, aproveitando todas as ferramentas que a Instituição coloca à sua disposição e, consequentemente, aprimorando sua qualificação profissional. Resta evidenciado que a carga horária total não está atrelada ao tempo de duração das videoaulas, mas à diligente observância do que é proposto neste projeto pedagógico.

**CONTEÚDO PROGRAMÁTICO:**

**INTRODUÇÃO AO HACKING ÉTICO**
Conceitos fundamentais de hacking ético e segurança ofensiva; O papel do hacker ético na proteção corporativa; Ciclo de vida de um teste de intrusão; Ética e limites legais do hacking;
**FONTES DE INFORMAÇÃO PARA OPERAÇÕES DE HACKING ÉTICO**
Exploração de **Open Source Intelligence (OSINT)** em auditorias de segurança; Aplicação de **Closed Source Intelligence (CSINT)** em ambientes restritos; Investigação em **Deep Web e Tor** para análise de riscos e ameaças emergentes;
**FRAMEWORKS E FERRAMENTAS APLICADAS AO HACKING E DEFESA DIGITAL**
Uso da **Pirâmide da Dor** na identificação de padrões de ataque; Aplicação da **Cyber Kill Chain** para mapeamento de ataques cibernéticos; Utilização do **MITRE ATT&CK** como referência prática para testes de penetração; Integração de modelos como **Unified Kill Chain** e **Diamond Model** na análise de ameaças; Criação e automação de regras de detecção com **Yara, Snort e Sigma**; Implementação prática com plataformas como **OpenCTI**;
**CONTRAINTELIGÊNCIA DIGITAL COM SUPORTE DE IA**
Definição e importância da contrainteligência no ambiente digital; O papel da **OPSEC (Operational Security)** na proteção de dados e operações; Estratégias avançadas de **Threat Hunting** com auxílio de Inteligência Artificial; Aplicação de **MITRE Engage** em operações de defesa ativa; Utilização de **honeypots** e táticas de engano digital; Identificação e combate a campanhas de **fake news** e manipulação da informação;
**COMPARTILHAMENTO DE INTELIGÊNCIA DIGITAL**
Importância da colaboração no ecossistema de segurança cibernética; Uso da **Malware Information Sharing Platform (MISP)** para integração e resposta a incidentes em rede;
**PANORAMA ATUAL E TENDÊNCIAS EM HACKING E CONTRAINTELIGÊNCIA**
O cenário global da **ciberguerra** e o papel da Inteligência Artificial em operações de ataque e defesa; Estudo das **APT (Ameaças Persistentes Avançadas)** e seus impactos no mundo corporativo; Tendências emergentes no uso da IA em **hacking ético e contrainteligência**; O futuro da cibersegurança baseada em automação e análise inteligente de dados;
**ATIVIDADES PRÁTICAS E SIMULAÇÕES**
Execução de testes práticos de intrusão em ambientes simulados; Exercícios de coleta e análise de dados em cenários reais de ameaças; Elaboração de um **plano de contrainteligência digital com suporte de IA.**