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: Inteligência Artificial Aplicada à Segurança Cibernética e Cyber Threat Intelligence

CARGA HORÁRIA: 200 horas

PRAZO MÍNIMO PARA CONCLUSÃO: 25 dias.

PRAZO MÁXIMO PARA CONCLUSÃO: 90 dias.

OBJETIVOS GERAIS:

Domine a Defesa Digital com I.A. Aplicada à Segurança Cibernética

O Curso online Inteligência Artificial Aplicada à Segurança Cibernética e Cyber Threat Intelligence é a formação definitiva para quem busca antecipar ataques e proteger infraestruturas críticas. O programa mergulha no ciclo de vida da inteligência, ensinando a coleta estratégica de dados em fontes de OSINT e ambientes de Deep Web. Através do uso de IA, o aluno aprende a transformar dados brutos em inteligência acionável, mapeando o comportamento de adversários com precisão cirúrgica.

Frameworks Avançados, MITRE ATT&CK e Modelagem de Ameaças

O conteúdo prioriza a aplicação prática dos principais modelos de defesa do mercado. Você dominará a Cyber Kill Chain e a matriz MITRE ATT&CK, além de utilizar a Pirâmide da Dor para elevar o custo dos ataques para o invasor. A formação ensina a criar regras de detecção automatizada com Yara, Snort e Sigma, integrando-as à plataforma OpenCTI. Com o suporte da Inteligência Artificial, a modelagem de ameaças torna-se um processo dinâmico e preditivo.

Threat Hunting, Contrainteligência e Resposta com IA

Prepare-se para atuar no Threat Hunting proativo, utilizando IA para identificar Ameaças Persistentes Avançadas (APTs). O curso aborda estratégias de contrainteligência, uso de honeypots e o framework MITRE Engage. Além disso, você aprenderá a gerenciar o compartilhamento de informações via MISP, essencial para a cooperação em ecossistemas de ciberguerra. O treinamento encerra com projetos práticos, simulando cenários reais de ataque e defesa sob a ótica da governança de dados inteligente.

Diferencial para o Mercado Global

Este curso une a robustez da segurança cibernética à agilidade da Inteligência Artificial, preparando o profissional para os desafios de um futuro movido a dados.

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:

FUNDAMENTOS DE INTELIGÊNCIA CIBERNÉTICA
Conceitos essenciais de Inteligência em Segurança Digital; O ciclo de vida da Inteligência Cibernética; Principais tipos de inteligência utilizados em ambientes corporativos e governamentais;
FONTES DE DADOS E INFORMAÇÕES PARA ANÁLISE DE AMEAÇAS
Coleta e análise de dados em **Open Source Intelligence (OSINT)**; Fontes restritas e proprietárias: **Closed Source Intelligence (CSINT)**; Monitoramento de ambientes como **Deep Web e Tor**, com técnicas de acesso e segurança;
FRAMEWORKS E MODELOS DE ANÁLISE EM CYBER THREAT INTELLIGENCE
Estruturas de apoio à detecção de ataques: **Pirâmide da Dor**; Ciclo de ataque cibernético: **Cyber Kill Chain**; Matriz de ataque e defesa: **MITRE ATT&CK**; Modelagem avançada com **Unified Kill Chain** e **Diamond Model**; Criação de regras de detecção automatizada: **Yara, Snort e Sigma**; Integração de processos com ferramentas de inteligência: **OpenCTI**;
CONTRAINTELIGÊNCIA DIGITAL E MITIGAÇÃO DE AMEAÇAS
Conceitos de **contrainteligência** e papel da **OPSEC (Operational Security)**; Estratégias de **Threat Hunting** baseadas em IA; Aplicação do **MITRE Engage** em operações de defesa; Uso de honeypots e técnicas de desinformação como barreiras contra ataques; Identificação e combate a **fake news** e campanhas de manipulação digital;
COMPARTILHAMENTO E GESTÃO DE INFORMAÇÕES DE AMEAÇAS
Conceitos de **Intelligence Sharing** no ecossistema digital; Utilização da **Malware Information Sharing Platform (MISP)** para cooperação entre equipes e organizações;
PANORAMA ATUAL E FUTURO DA CYBER THREAT INTELLIGENCE
Cenários de **ciberguerra** e o papel da Inteligência Artificial; Análise de **APT (Ameaças Persistentes Avançadas)** e seu impacto global; Tendências emergentes em **Cyber Threat Intelligence** com suporte de IA; Perspectivas sobre o futuro da segurança

cibernética baseada em dados inteligentes;

ATIVIDADES PRÁTICAS E PROJETOS

Simulações de ataques e defesa com base em frameworks apresentados; Exercícios de coleta, análise e correlação de dados de ameaças reais; Desenvolvimento de um mini projeto de **plano de inteligência cibernética com IA.**