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: Gestão de Riscos e Compliance: Inteligência de Ameaças, Cibersegurança e Inteligência Artificial

CARGA HORÁRIA: 280 horas

PRAZO MÍNIMO PARA CONCLUSÃO: 35 dias.

PRAZO MÁXIMO PARA CONCLUSÃO: 120 dias.

OBJETIVOS GERAIS:

Gestão de Riscos e Compliance para Decisões Estratégicas

O curso **Gestão de Riscos e Compliance: Inteligência de Ameaças, Cibersegurança e Inteligência Artificial** prepara profissionais e servidores públicos para antecipar ameaças, proteger informações e fortalecer controles organizacionais. A formação integra inteligência ativa, análise de riscos e conformidade, oferecendo conhecimentos aplicáveis à tomada de decisões fundamentadas em evidências.

Inteligência de Ameaças e Proteção Organizacional

Aprenda a estruturar o ciclo de inteligência, avaliar a credibilidade das fontes e priorizar riscos conforme probabilidade e impacto. O conteúdo aborda OSINT, pesquisa autorizada em fontes restritas, monitoramento de exposição de dados e proteção de informações sensíveis, com atenção à LGPD e aos limites éticos da coleta.

Cibersegurança Aplicada à Prevenção e à Detecção

Amplie sua compreensão sobre MITRE ATT&CK, Cyber Kill Chain, Diamond Model e ferramentas de detecção como YARA, Snort e Sigma. Estude contrainteligência, OPSEC, threat hunting e compartilhamento de inteligência com OpenCTI e MISP. Esses conhecimentos apoiam a identificação de vulnerabilidades, a avaliação de alertas e a documentação de evidências para auditoria e compliance.

Inteligência Artificial com Supervisão e Responsabilidade

Conheça aplicações da IA generativa na pesquisa, triagem documental e elaboração de relatórios, além do aprendizado de máquina na identificação de anomalias. Desenvolva critérios para validar fontes, controlar vieses e alucinações e preservar dados pessoais. O objetivo é utilizar a tecnologia com supervisão humana e rastreabilidade das análises.

Atualização Profissional para Empresas e Órgãos Públicos

Destinado a profissionais de compliance, auditoria, Direito, tecnologia, segurança da informação e gestão pública, o curso conecta conhecimentos técnicos às responsabilidades institucionais. Exercícios resolvidos e comentados reforçam a aprendizagem e sua aplicação no trabalho. **Matricule-se e desenvolva competências para contribuir com a prevenção de incidentes, a integridade organizacional e a melhoria dos controles.**

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 DA INTELIGÊNCIA ATIVA NA GESTÃO DE RISCOS E NO COMPLIANCE: Conceitos e Elementos da Inteligência Aplicada às Organizações; Modalidades de Inteligência Estratégica, Tática e Operacional; Inteligência Ativa na Antecipação de Ameaças e no Apoio às Decisões; Integração entre Inteligência, Gestão de Riscos e Compliance; Exercícios de Fixação Propostos Resolvidos Comentados;
CICLO DE INTELIGÊNCIA E PRIORIZAÇÃO DE RISCOS ORGANIZACIONAIS: Planejamento e Definição das Necessidades de Inteligência; Coleta, Tratamento e Análise de Dados e Informações; Avaliação de Probabilidade, Impacto e Prioridade dos Riscos; Disseminação dos Resultados, Monitoramento e Aperfeiçoamento dos Controles; Exercícios de Fixação Propostos Resolvidos

Comentados;

FONTES ABERTAS E RESTRITAS NA PRODUÇÃO DE INTELIGÊNCIA: Pesquisa em Fontes Abertas com Open Source Intelligence (OSINT); Exploração Autorizada de Fontes Restritas com Closed Source Intelligence (CSINT); Verificação da Credibilidade, Rastreabilidade e Qualidade das Informações; Proteção de Dados, LGPD e Limites Éticos na Coleta de Informações; Exercícios de Fixação Propostos Resolvidos Comentados;

AMBIENTES DIGITAIS E MONITORAMENTO DE AMEAÇAS EM FONTES NÃO INDEXADAS: Distinções entre Web de Superfície, Deep Web e Dark Web; Funcionamento, Instalação e Uso Seguro da Rede Tor; Identificação de Exposição de Dados, Credenciais e Informações Organizacionais; Procedimentos de Pesquisa Autorizada e Registro de Evidências para Compliance; Exercícios de Fixação Propostos Resolvidos Comentados;

MODELOS DE ANÁLISE DE AMEAÇAS E PRIORIZAÇÃO DE CONTROLES: Pirâmide da Dor na Seleção de Indicadores e Medidas Defensivas; Etapas de Ataque e Pontos de Controle com Cyber Kill Chain; Análise Integrada do Ciclo de Ataque com Unified Kill Chain; Relações entre Adversários, Infraestrutura, Capacidades e Vítimas com Diamond Model; Exercícios de Fixação Propostos Resolvidos Comentados;

MAPEAMENTO DE COMPORTAMENTOS ADVERSÁRIOS E DETECÇÃO DE RISCOS CIBERNÉTICOS: Táticas e Técnicas de Ataque com MITRE ATT&CK; Identificação de Lacunas e Correspondência entre Ameaças e Controles; Criação de Regras de Detecção com YARA, Snort e Sigma; Validação de Alertas, Redução de Falsos Positivos e Documentação de Evidências; Exercícios de Fixação Propostos Resolvidos Comentados;

CONTRAINTELIGÊNCIA E PROTEÇÃO DAS INFORMAÇÕES ORGANIZACIONAIS: Fundamentos da Contrainteligência na Prevenção de Vazamentos e Espionagem; Segurança Operacional e Proteção de Ativos Informacionais com OPSEC; Controle de Acesso, Compartimentação e Tratamento de Informações Sensíveis; Identificação de Desinformação, Fake News e Riscos à Reputação; Exercícios de Fixação Propostos Resolvidos Comentados;

BUSCA PROATIVA DE AMEAÇAS E DEFESA ORIENTADA POR INTELIGÊNCIA: Formulação de Hipóteses e Investigação Proativa com Threat Hunting; Planejamento de Interações Defensivas com MITRE Engage; Uso Controlado de Honeypots na Observação de Atividades Suspeitas; Ameaças Persistentes Avançadas, Ciberguerra e Cenários Emergentes de Risco; Exercícios de Fixação Propostos Resolvidos Comentados;

INTEGRAÇÃO E COMPARTILHAMENTO DE INTELIGÊNCIA PARA COMPLIANCE: Organização e Correlação de Informações sobre Ameaças com OpenCTI; Compartilhamento de Indicadores e Eventos com Malware Information Sharing Platform (MISP); Critérios de Confidencialidade, Autorização e Qualidade no Intercâmbio de Informações; Relatórios de Inteligência, Trilhas de Auditoria e Atualização dos Controles; Exercícios de Fixação Propostos Resolvidos Comentados;

FERRAMENTAS DE INTELIGÊNCIA ARTIFICIAL NA GESTÃO DE RISCOS E NO COMPLIANCE: Ferramentas de IA Generativa na Pesquisa, Triagem Documental e Síntese de Informações; Aprendizado de Máquina na Identificação de Padrões, Anomalias e Sinais de Risco; Automação Assistida do Monitoramento de Ameaças e da Elaboração de Relatórios; Validação de Fontes, Supervisão Humana, Proteção de Dados e Controle de Vieses e Alucinações; Exercícios de Fixação Propostos Resolvidos Comentados.