Curso de Especialização

Análise e Deteção de Ameaças de Cibersegurança com Inteligência Artificial

TECH é membro da:

tech global university

tech global university

Curso de Especialização

Análise e Deteção de Ameaças de Cibersegurança com Inteligência Artificial

- Modalidade: **online**
- Duração: **6 meses**
- Certificação: **TECH Global University**
- Acreditação: **18 ECTS**
- Horário: **ao seu próprio ritmo**
- Exames: **online**

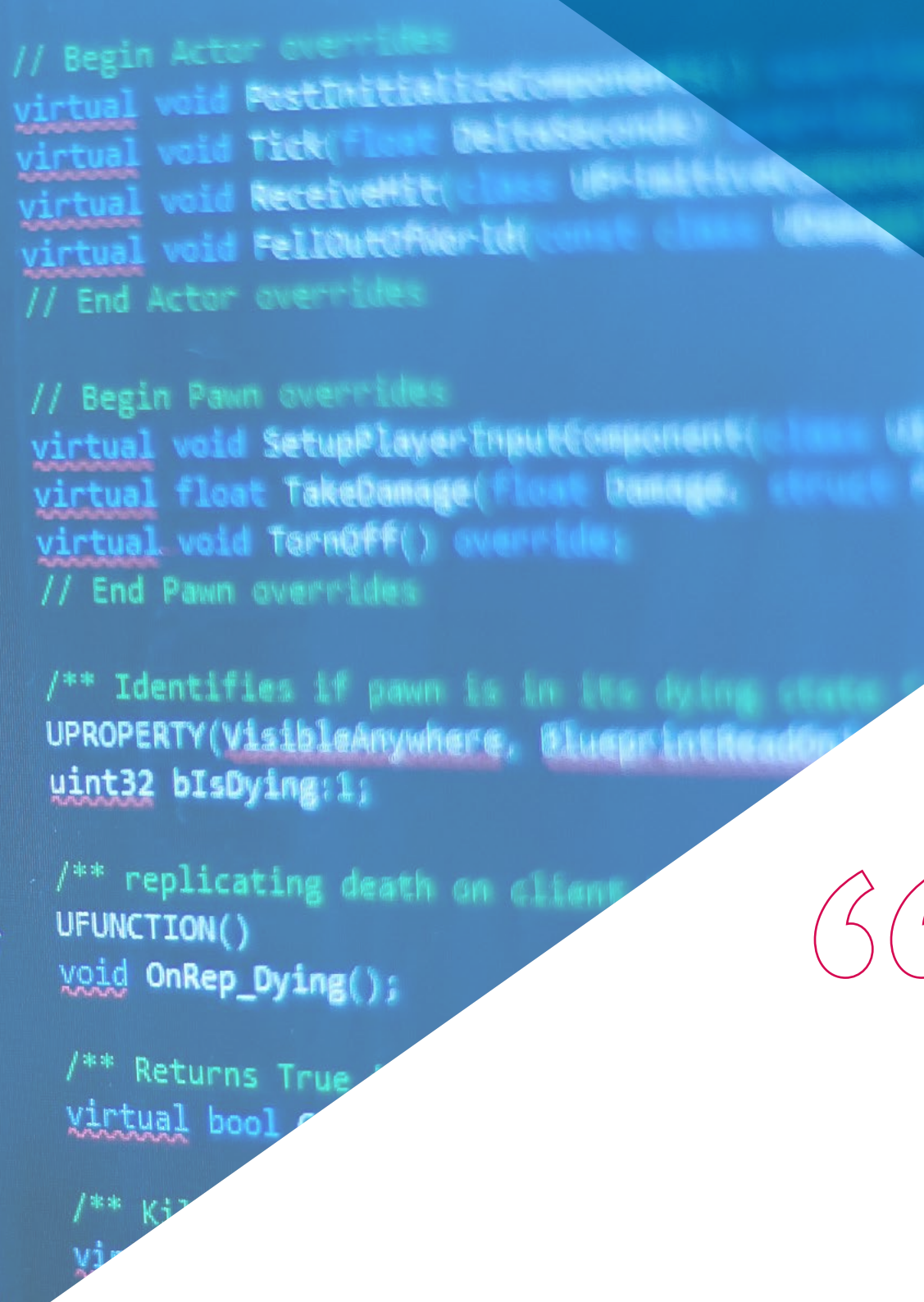
Acesso ao site: **www.techtitute.com/pt/informatica/curso-especializacao/curso-especializacao-analise-detecao-ameacas-ciberseguranca-inteligencia-artificial**

Índice

01

Apresentação do programa

A transformação digital, associada ao aumento exponencial de dispositivos conectados e ao volume de dados gerados, impulsionou a evolução das ciberameaças, levando à necessidade de abordagens mais sofisticadas para a deteção, prevenção e mitigação de ataques. Neste contexto, a Inteligência Artificial posicionou-se como uma ferramenta fundamental para reforçar as capacidades de ciberdefesa. Por este motivo, a TECH concebeu um programa universitário 100% online que prepara os profissionais para integrar ferramentas de Inteligência Artificial nas estratégias de Cibersegurança, dotando-os de competências práticas e conhecimentos avançados para liderar a ciberdefesa em qualquer contexto. Tudo isto, ministrado por especialistas reconhecidos, utilizando a metodologia de ensino mais inovadora: o *Relearning*.



Com este Curso de Especialização 100% online, adquirirá competências avançadas para identificar, prevenir e atenuar ciberataques utilizando ferramentas inovadoras como o ChatGPT"

A cibersegurança surgiu como uma das principais prioridades globais da atualidade. Desde a proteção dos dados pessoais até à segurança de infra-estruturas críticas, como os sistemas financeiros e as redes de energia, este domínio tornou-se um pilar essencial para garantir a estabilidade e a confiança no mundo digital. Além disso, o advento da Inteligência Artificial transformou as estratégias de defesa tradicionais, permitindo uma evolução para sistemas de proteção mais preditivos e automatizados. Neste sentido, os sistemas inteligentes não só reforçam as capacidades de deteção de ameaças, como também permitem respostas proativas e adaptativas que minimizam os riscos.

Com esta ideia em mente, a TECH apresenta um Curso de Especialização exaustiva em Análise e Deteção de Ameaças de Cibersegurança com Inteligência Artificial, através da qual os profissionais de TI irão aprofundar os aspetos mais relevantes para identificar, prevenir e mitigar os ciberataques modernos utilizando ferramentas avançadas como o Gemini. Este programa universitário permitir-lhes-á dominar técnicas de análise preditiva, simulação de ataques e deteção de intrusões, bem como implementar sistemas de defesa proactivos optimizados com Inteligência Artificial. Além disso, adquirirão as competências necessárias para proteger as infra-estruturas da Internet das Coisas e gerir incidentes cibernéticos em tempo real, consolidando-os como especialistas em segurança informática num mercado altamente procurado.

Ao mesmo tempo, esta titulação universitária é 100% online, permitindo aos profissionais conciliar a sua aprendizagem com as suas responsabilidades profissionais e pessoais. Os recursos académicos deste programa universitário, tais como vídeos explicativos, resumos interactivos e infografias, estão disponíveis 24 horas por dia, 7 dias por semana, a partir de qualquer dispositivo com ligação à Internet. Além disso, este percurso académico baseia-se no inovador método *Relearning*, que otimiza a assimilação de conceitos-chave através da repetição estratégica, garantindo uma aprendizagem dinâmica e eficaz.

Este **Curso de Especialização em Análise e Deteção de Ameaças de Cibersegurança com Inteligência Artificial** conta com o conteúdo educacional mais completo e atualizado do mercado. As suas principais características são:

- O desenvolvimento de estudos de caso apresentados por especialistas com um profundo conhecimento em Cibersegurança e Inteligência Artificial, que aplicam estas ferramentas para a deteção, prevenção e mitigação de ciberameaças em ambientes tecnológicos avançados
- Os conteúdos gráficos, esquemáticos e eminentemente práticos com que foi concebido, recolhem informação científica e prática sobre as disciplinas essenciais para a prática profissional
- Exercícios práticos onde o processo de autoavaliação pode ser levado a cabo a fim de melhorar a aprendizagem
- O seu foco especial em metodologias inovadoras
- As aulas teóricas, perguntas ao especialista, fóruns de discussão sobre questões controversas e atividades de reflexão individual
- A disponibilidade de acesso aos conteúdos a partir de qualquer dispositivo fixo ou portátil com conexão à Internet

> *Implementará sistemas de deteção de intrusão baseados em Inteligência Artificial, otimizando a proteção de infra-estruturas críticas"*

Terá a sua disposição vídeos explicativos, resumos interactivos e infografias 24 horas por dia, a partir de qualquer dispositivo e sem interferir com as suas responsabilidades pessoais”

Domina os algoritmos de aprendizagem automática para antecipar e neutralizar os crimes informáticos.

Otimizará os processos de deteção e análise de riscos em ambientes digitais, posicionando-se como um especialista estratégico em ciberdefesa.

O curso inclui no seu corpo docente, profissionais do setor que trazem a experiência do seu trabalho para esta formação, bem como especialistas reconhecidos das principais sociedades e universidades de prestígio.

O seu conteúdo multimédia, desenvolvido com a mais recente tecnologia educativa, permitirá ao profissional uma aprendizagem situada e contextual, ou seja, um ambiente simulado que proporcionará uma formação imersiva programada para treinar-se em situações reais.

O design deste curso foca-se na Aprendizagem Baseada em Problemas, através da qual o profissional deverá tentar resolver as diferentes situações da atividade profissional que surgem ao longo do curso. Para tal, contará com a ajuda de um sistema inovador de vídeo interativo desenvolvido por especialistas reconhecidos.

02

Porquê estudar na TECH?

A TECH é a maior universidade digital do mundo. Com um impressionante catálogo de mais de 14.000 programas universitários, disponíveis em 11 línguas, posiciona-se como líder em empregabilidade, com uma taxa de colocação profissional de 99%. Além disso, possui um enorme corpo docente de mais de 6.000 professores de renome internacional.

Estuda na maior universidade digital do mundo e garante o teu sucesso profissional. O futuro começa na TECH”

A melhor universidade online do mundo segundo a FORBES

A prestigiada revista Forbes, especializada em negócios e finanças, destacou a TECH como «a melhor universidade online do mundo». Foi o que afirmaram recentemente num artigo da sua edição digital, no qual fazem eco da história de sucesso desta instituição, «graças à oferta académica que proporciona, à seleção do seu corpo docente e a um método de aprendizagem inovador destinado a formar os profissionais do futuro».

O melhor corpo docente top internacional

O corpo docente da TECH é composto por mais de 6.000 professores de renome internacional. Professores, investigadores e quadros superiores de multinacionais, incluindo Isaiah Covington, treinador de desempenho dos Boston Celtics; Magda Romanska, investigadora principal do Harvard MetaLAB; Ignacio Wistumba, presidente do departamento de patologia molecular translacional do MD Anderson Cancer Center; e D.W. Pine, diretor criativo da revista TIME, entre outros.

A maior universidade digital do mundo

A TECH é a maior universidade digital do mundo. Somos a maior instituição educativa, com o melhor e mais extenso catálogo educativo digital, cem por cento online e abrangendo a grande maioria das áreas do conhecimento. Oferecemos o maior número de títulos próprios, pós-graduações e licenciaturas oficiais do mundo. No total, são mais de 14.000 títulos universitários, em onze línguas diferentes, o que nos torna a maior instituição de ensino do mundo.

Os planos de estudos mais completos do panorama universitário

A TECH oferece os planos de estudos mais completos do panorama universitário, com programas que abrangem os conceitos fundamentais e, ao mesmo tempo, os principais avanços científicos nas suas áreas científicas específicas. Além disso, estes programas são continuamente atualizados para garantir aos estudantes a vanguarda académica e as competências profissionais mais procuradas. Desta forma, os cursos da universidade proporcionam aos seus alunos uma vantagem significativa para impulsionar as suas carreiras com sucesso.

Um método de aprendizagem único

A TECH é a primeira universidade a utilizar o *Relearning* em todos os seus cursos. É a melhor metodologia de aprendizagem online, acreditada com certificações internacionais de qualidade de ensino, fornecidas por agências educacionais de prestígio. Além disso, este modelo académico disruptivo é complementado pelo "Método do Caso", configurando assim uma estratégia única de ensino online. São também implementados recursos didáticos inovadores, incluindo vídeos detalhados, infografias e resumos interativos.

A universidade online oficial da NBA

A TECH é a Universidade Online Oficial da NBA. Através de um acordo com a maior liga de basquetebol, oferece aos seus estudantes programas universitários exclusivos, bem como uma grande variedade de recursos educativos centrados no negócio da liga e noutras áreas da indústria desportiva. Cada programa tem um plano de estudos único e conta com oradores convidados excepcionais: profissionais com um passado desportivo distinto que oferecem os seus conhecimentos sobre os temas mais relevantes.

Líderes em empregabilidade

A TECH conseguiu tornar-se a universidade líder em empregabilidade. 99% dos seus estudantes conseguem um emprego na área académica que estudaram, no prazo de um ano após a conclusão de qualquer um dos programas da universidade. Um número semelhante consegue uma melhoria imediata da sua carreira. Tudo isto graças a uma metodologia de estudo que baseia a sua eficácia na aquisição de competências práticas, absolutamente necessárias para o desenvolvimento profissional.

Google Partner Premier

O gigante tecnológico americano atribuiu à TECH o distintivo Google Partner Premier. Este prémio, que só está disponível para 3% das empresas no mundo, destaca a experiência eficaz, flexível e adaptada que esta universidade proporciona aos estudantes. O reconhecimento não só acredita o máximo rigor, desempenho e investimento nas infra-estruturas digitais da TECH, mas também coloca esta universidade como uma das empresas de tecnologia mais avançadas do mundo.

A universidade mais bem classificada pelos seus alunos

Os alunos posicionaram a TECH como a universidade mais bem avaliada do mundo nos principais portais de opinião, destacando a sua classificação máxima de 4,9 em 5, obtida a partir de mais de 1.000 avaliações. Estes resultados consolidam a TECH como uma instituição universitária de referência internacional, refletindo a excelência e o impacto positivo do seu modelo educativo"

03

Plano de estudos

O programa deste Curso de Especialização oferece uma visão completa dos principais desafios e soluções para a proteção dos sistemas digitais. Através de três módulos abrangentes, os cientistas informáticos cobrirão tudo, desde os fundamentos da cibersegurança até à implementação de modelos preditivos e sistemas avançados de deteção de intrusões. Com uma abordagem prática e ferramentas inovadoras como o ChatGPT, este programa universitário fornece as competências necessárias para antecipar, identificar e responder às ciberameaças mais complexas do ambiente digital atual.

Irá especializar-se na gestão de incidentes e na resposta automatizada, reforçando a sua capacidade de agir rapidamente face a ameaças como o Ransomware"

Módulo 1. Cibersegurança e análise de ameaças modernas com ChatGPT

1.1. Introdução à Cibersegurança: ameaças atuais e o papel da Inteligência Artificial
- 1.1.1. Definição e conceitos básicos de Cibersegurança
- 1.1.2. Tipos de ameaças cibernéticas modernas
- 1.1.3. Papel da Inteligência Artificial na evolução da Cibersegurança

1.2. Confidencialidade, integridade e disponibilidade (CIA) na era da Inteligência Artificial
- 1.2.1. Fundamentos do modelo CIA em Cibersegurança
- 1.2.2. Princípios de segurança aplicados no contexto da Inteligência Artificial
- 1.2.3. Desafios e considerações do CIA em sistemas impulsionados por Inteligência Artificial

1.3. Uso do ChatGPT para análise de riscos e cenários de ameaça
- 1.3.1. Fundamentos da análise de riscos em Cibersegurança
- 1.3.2. Capacidade do ChatGPT para identificar e avaliar cenários de ameaça
- 1.3.3. Benefícios e limitações da análise de riscos com Inteligência Artificial

1.4. ChatGPT na deteção de vulnerabilidades críticas
- 1.4.1. Princípios da deteção de vulnerabilidades em sistemas de informação
- 1.4.2. Funcionalidades do ChatGPT para apoiar na deteção de vulnerabilidades
- 1.4.3. Considerações éticas e de segurança ao usar Inteligência Artificial na deteção de falhas

1.5. Análisis de *malware* e *ransomware* assistida por Inteligência Artificial
- 1.5.1. Princípios básicos da análise de *malware* e *ransomware*
- 1.5.2. Técnicas de Inteligência Artificial aplicadas na identificação de código malicioso
- 1.5.3. Desafios técnicos e operacionais na análise de *malware* assistida por Inteligência Artificial

1.6. Identificação de ataques comuns com Inteligência Artificial: *phishing,* engenharia social e exploração
- 1.6.1. Classificação dos ataques: *phishing*, engenharia social e exploração
- 1.6.2. Técnicas de Inteligência Artificial para a identificação e análise de ataques comuns
- 1.6.3. Dificuldades e limitações dos modelos de Inteligência Artificial na deteção de ataques

1.7. ChatGPT na capacitação e simulação de ameaças cibernéticas
- 1.7.1. Fundamentos da simulação de ameaças para formação em Cibersegurança
- 1.7.2. Capacidades do ChatGPT para desenhar cenários de simulação
- 1.7.3. Benefícios da simulação de ameaças como ferramenta de capacitação

1.8. Políticas de segurança cibernética com recomendações de Inteligência Artificial
- 1.8.1. Princípios para a formulação de políticas de segurança cibernética
- 1.8.2. Papel da Inteligência Artificial na geração de recomendações de segurança
- 1.8.3. Componentes chave em políticas de segurança orientadas para Inteligência Artificial

1.9. Segurança em dispositivos IoT e o papel da Inteligência Artificial
- 1.9.1. Fundamentos da segurança na Internet das Coisas (IoT)
- 1.9.2. Capacidades da Inteligência Artificial para mitigar vulnerabilidades em dispositivos IoT
- 1.9.3. Desafios e considerações específicas de Inteligência Artificial para a segurança de IoT

1.10. Avaliação de ameaças e respostas assistidas por ferramentas de Inteligência Artificial
- 1.10.1. Princípios de avaliação de ameaças em Cibersegurança
- 1.10.2. Características das respostas automatizadas através de Inteligência Artificial
- 1.10.3. Fatores críticos na eficácia das respostas cibernéticas com Inteligência Artificial

Módulo 2. Deteção e prevenção de intrusões usando modelos de Inteligência Artificial Generativa

2.1. Fundamentos de sistemas IDS/IPS e o papel da Inteligência Artificial
- 2.1.1. Definição e princípios básicos dos sistemas IDS e IPS
- 2.1.2. Principais tipos e configurações de IDS/IPS
- 2.1.3. Contribuição da Inteligência Artificial na evolução dos sistemas de deteção e prevenção

2.2. Uso de Gemini para detecção de anomalias em redes
- 2.2.1. Conceitos e tipos de anomalias no tráfego de rede
- 2.2.2. Características de Gemini para a análise de dados de rede
- 2.2.3. Benefícios da deteção de anomalias na prevenção de intrusões

2.3. Gemini e a identificação de padrões de intrusão
- 2.3.1. Princípios de identificação e classificação de padrões de intrusão
- 2.3.2. Técnicas de Inteligência Artificial aplicadas na deteção de padrões de ameaças
- 2.3.3. Tipos de padrões e comportamentos anômalos em segurança de redes

2.4. Aplicação de modelos generativos na simulação de ataques
- 2.4.1. Fundamentos dos modelos generativos em Inteligência Artificial
- 2.4.2. Uso de modelos generativos para recriar cenários de ataque
- 2.4.3. Vantagens e limitações na simulação de ataques por meio de Inteligência Artificial generativa

2.5. *Clustering* e classificação de eventos usando Inteligência Artificial
- 2.5.1. Fundamentos do *clustering* e classificação na detecção de intrusões
- 2.5.2. Algoritmos comuns de *clustering* aplicados em Cibersegurança
- 2.5.3. Papel da Inteligência Artificial na melhoria dos métodos de classificação de eventos

2.6. Gemini na geração de perfis de comportamento
- 2.6.1. Conceitos de perfilamento de usuários e dispositivos
- 2.6.2. Aplicação de modelos generativos na criação de perfis
- 2.6.3. Vantagens dos perfis de comportamento na deteção de ameaças

2.7. Análise de *Big Data* para prevenção de intrusões
- 2.7.1. Importância do *Big Data* na deteção de padrões de segurança
- 2.7.2. Métodos de processamento de grandes volumes de dados em Cibersegurança
- 2.7.3. Aplicações de Inteligência Artificial na análise e prevenção baseadas em *Big Data*

2.8. Redução de dados e seleção de características relevantes com Inteligência Artificial
- 2.8.1. Princípios de redução de dimensionalidade em grandes volumes de dados
- 2.8.2. Seleção de características para melhorar a eficiência da análise de Inteligência Artificial
- 2.8.3. Técnicas de redução de dados aplicadas em Cibersegurança

2.9. Avaliação de modelos de Inteligência Artificial na detecção de intrusos
- 2.9.1. Critérios de avaliação de modelos de Inteligência Artificial em Cibersegurança
- 2.9.2. Indicadores de desempenho e precisão dos modelos
- 2.9.3. Importância da validação e avaliação constante na Inteligência Artificial

2.10. Implementação de um sistema de detecção de intrusos potenciado com Inteligência Artificial generativa
- 2.10.1. Conceitos básicos de implementação de sistemas de detecção de intrusos
- 2.10.2. Integração de Inteligência Artificial generativa nos sistemas IDS/IPS
- 2.10.3. Aspetos chave para a configuração e manutenção de sistemas baseados em Inteligência Artificial

Módulo 3. Modelos preditivos de defesa proativa em Cibersegurança usando ChatGPT

3.1. Análise preditiva em Cibersegurança: técnicas e aplicações com Inteligência Artificial
- 3.1.1. Conceitos básicos de análise preditiva em segurança
- 3.1.2. Técnicas de predição no âmbito da Cibersegurança
- 3.1.3. Aplicação da Inteligência Artificial na antecipação de ciberameaças

3.2. Modelos de regressão e classificação com suporte de ChatGPT
- 3.2.1. Princípios de regressão e classificação na predição de ameaças
- 3.2.2. Tipos de modelos de classificação em Cibersegurança
- 3.2.3. Assistência do ChatGPT na interpretação de modelos preditivos

3.3. Identificação de ameaças emergentes com predições de ChatGPT
- 3.3.1. Conceitos de deteção de ameaças emergentes
- 3.3.2. Técnicas de identificação de novos padrões de ataque
- 3.3.3. Limitações e precauções na predição de novas ameaças

3.4. Redes neuronais para antecipação de ataques cibernéticos
- 3.4.1. Fundamentos de redes neuronais aplicadas em Cibersegurança
- 3.4.2. Arquiteturas comuns para deteção e predição de ataques
- 3.4.3. Desafios na implementação de redes neuronais em defesa cibernética

3.5. Uso de ChatGPT para simulações de cenários de ameaça
- 3.5.1. Conceitos básicos de simulação de ameaças em Cibersegurança
- 3.5.2. Capacidades do ChatGPT para desenvolver simulações preditivas
- 3.5.3. Fatores a considerar no design de cenários simulados

3.6. Algoritmos de aprendizagem por reforço para otimização de defesas
- 3.6.1. Introdução à aprendizagem por reforço em Cibersegurança
- 3.6.2. Algoritmos de reforço aplicados a estratégias de defesa
- 3.6.3. Benefícios e desafios da aprendizagem por reforço em ambientes de Cibersegurança

3.7. Simulação de ameaças e respostas com ChatGPT
- 3.7.1. Princípios de simulação de ameaças e sua relevância em ciberdefesa
- 3.7.2. Respostas automatizadas e otimizadas perante ataques simulados
- 3.7.3. Benefícios da simulação para melhorar a preparação cibernética

3.8. Avaliação de precisão e efetividade em modelos preditivos de Inteligência Artificial
- 3.8.1. Indicadores chave para a avaliação de modelos preditivos
- 3.8.2. Metodologias de avaliação de precisão em modelos de Cibersegurança
- 3.8.3. Fatores críticos na efetividade dos modelos de Inteligência Artificial em Cibersegurança

3.9. Inteligência Artificial na gestão de incidentes e respostas automatizadas
- 3.9.1. Fundamentos da gestão de incidentes em Cibersegurança
- 3.9.2. Papel da Inteligência Artificial na tomada de decisões em tempo real
- 3.9.3. Desafios e oportunidades na automatização de respostas

3.10. Criação de um sistema de defesa preditivo com suporte de ChatGPT
- 3.10.1. Princípios de design de sistemas de defesa proativa
- 3.10.2. Integração de modelos preditivos em ambientes de Cibersegurança
- 3.10.3. Componentes chave para um sistema de defesa preditivo baseado em Inteligência Artificial

Aprofundará a integração de modelos computacionais avançados nos sistemas IDS/IPS, levando a proteção das redes digitais para o nível seguinte"

04

Objetivos de ensino

Com esta titulação universitária da TECH, os cientistas informáticos desenvolverão as competências necessárias para liderar estratégias de cibersegurança em ambientes tecnológicos avançados. Através de uma abordagem prática, adquirirão competências essenciais para implementar sistemas de deteção, analisar riscos e conceber defesas proativas baseadas em IA, consolidando a sua capacidade de proteger as infraestruturas digitais e responder eficazmente às ciberameaças emergentes.

Desenvolverá competências avançadas em deteção de intrusões e análise preditiva para liderar estratégias de defesa proativas em ambientes digitais”

Objetivos gerais

- Analisar as principais ciberameaças modernas e a sua evolução no contexto da Inteligência Artificial
- Identificar padrões anómalos em sistemas digitais utilizando ferramentas avançadas de Inteligência Artificial
- Desenvolver estratégias de deteção e prevenção de intrusões utilizando modelos generativos e preditivos
- Implementar sistemas de defesa proactivos baseados em técnicas de análise preditiva e de aprendizagem automática
- Conceber simulações de ciberataques para avaliar as vulnerabilidades e otimizar as defesas
- Aplicar algoritmos de Inteligência Artificial na gestão de incidentes e respostas automatizadas
- Otimizar a segurança dos dispositivos ligados através da atenuação dos riscos específicos da Internet das Coisas
- Avaliar a eficácia e a precisão dos modelos de Inteligência Artificial aplicados à cibersegurança
- Desenvolver políticas de cibersegurança com base em recomendações baseadas em IA
- Promover a utilização ética e responsável da Inteligência Artificial na proteção de sistemas e dados

Objetivos específicos

Módulo 1. Cibersegurança e análise de ameaças modernas com ChatGPT

- Compreender os conceitos fundamentais de Cibersegurança, incluindo as ameaças modernas e o modelo CIA
- Utilizar o ChatGPT para a análise de riscos, deteção de vulnerabilidades e simulação de cenários de ameaça
- Desenvolver habilidades para desenhar políticas de segurança cibernética eficazes e proteger dispositivos IoT através de Inteligência Artificial
- Implementar estratégias avançadas de gestão de ameaças utilizando Inteligência Artificial generativa para antecipar possíveis ataques
- Avaliar o impacto das ameaças modernas em infraestruturas críticas através de técnicas de simulação assistida por Inteligência Artificial
- Desenhar soluções personalizadas para a proteção de redes corporativas, baseadas em ferramentas avançadas de Inteligência Artificial

Módulo 2. Deteção e prevenção de intrusões usando modelos de Inteligência Artificial Generativa

- Dominar as técnicas de deteção de anomalias e padrões de intrusão com ferramentas como Gemini
- Aplicar modelos generativos para simular ataques cibernéticos e melhorar a prevenção de intrusões
- Implementar sistemas IDS/IPS avançados otimizados com Inteligência Artificial, desenvolvendo perfis de comportamento e analisando Big Data em tempo real
- Desenhar arquiteturas de segurança integradas com Inteligência Artificial para a proteção de ambientes multiusuário e sistemas distribuídos
- Utilizar modelos generativos para antecipar ataques dirigidos e elaborar contramedidas em tempo real
- Integrar análise preditiva em sistemas de deteção para a gestão dinâmica de ameaças emergentes

Módulo 3. Modelos preditivos de defesa proativa em Cibersegurança usando ChatGPT

- Desenhar modelos preditivos avançados baseados em redes neuronais e aprendizagem por reforço
- Implementar simulações de cenários de ameaça para treinar equipas e melhorar a preparação para incidentes
- Avaliar e optimizar sistemas de defesa proativa, integrando Inteligência Artificial generativa na tomada de decisões e automatização de respostas
- Desenvolver *frameworks* de defesa preditiva adaptáveis a infraestruturas críticas e sistemas empresariais
- Utilizar análise preditiva para identificar vulnerabilidades emergentes antes que sejam exploradas
- Integrar Inteligência Artificial generativa em processos de tomada de decisões estratégicas para a melhoria contínua de sistemas defensivos

05

Oportunidades de carreira

Este programa universitário abre as portas a inúmeras oportunidades num setor em constante crescimento. Graças às competências adquiridas ao longo deste curso académico, os profissionais poderão trabalhar em funções-chave como Analista de Cibersegurança, Especialista em Deteção de Ameaças, Consultor de Sistemas de Defesa Proactiva ou Especialista em Proteção de Infra-estruturas Digitais. Além disso, o seu foco na Inteligência Artificial aplicada permite-lhe liderar projetos inovadores em ambientes empresariais, governamentais e tecnológicos avançados.

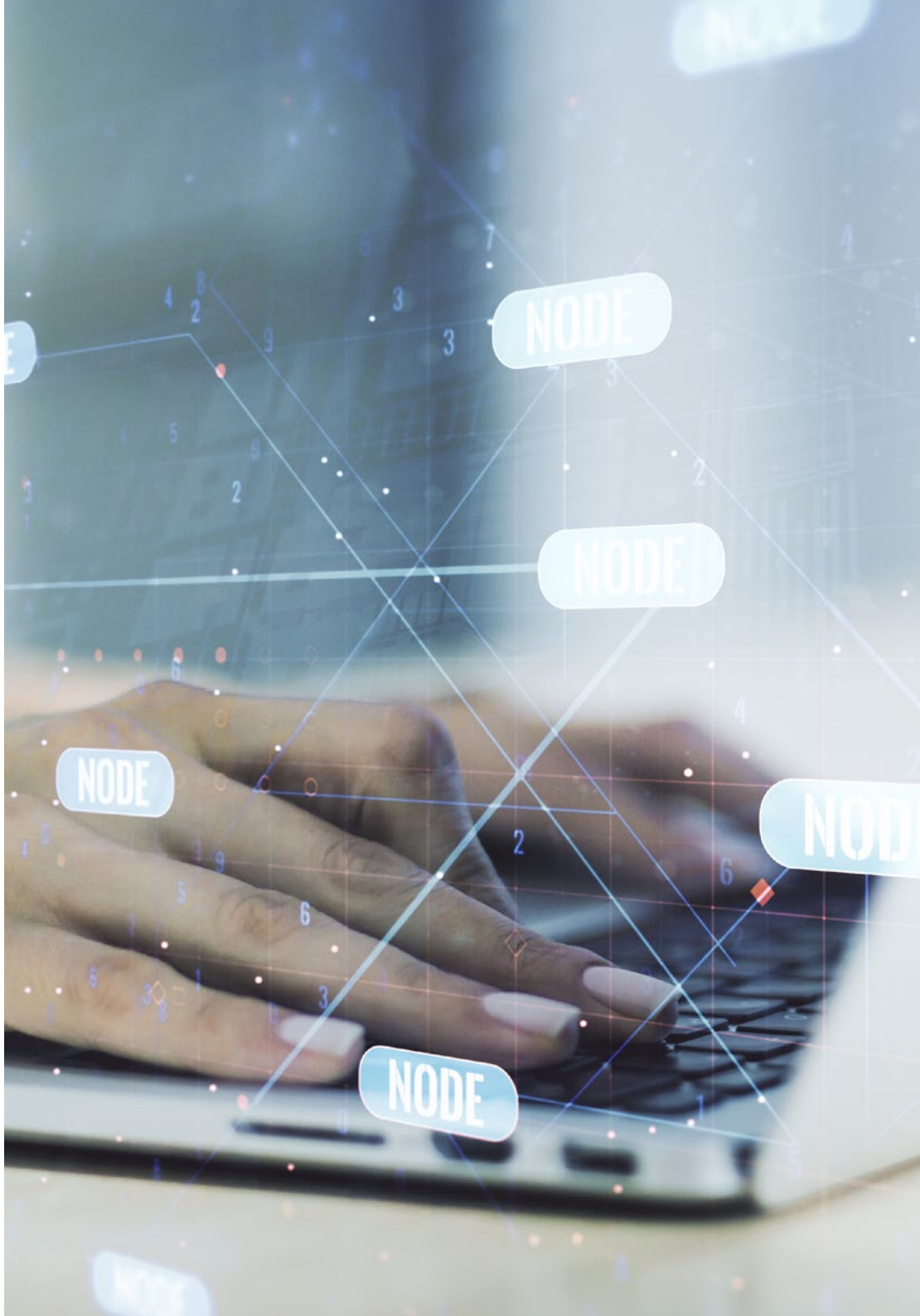
Poderá aceder a funções estratégicas como Especialista em Análise Preditiva de Ameaças Cibernéticas ou Auditor de Vulnerabilidades em Ambientes Digitais"

Perfil dos nossos alunos

O aluno deste Curso de Especialização da TECH será um profissional altamente qualificado para enfrentar os desafios da segurança digital na atualidade. Com competências avançadas na utilização da Inteligência Artificial, estará preparado para conceber estratégias de defesa, implementar sistemas de deteção de ameaças e gerir incidentes em tempo real. O seu domínio de ferramentas inovadoras e a sua abordagem ética posicioná-lo-ão como um perito capaz de proteger infra-estruturas críticas e liderar projetos em ambientes tecnológicos complexos.

Irá liderar projetos de cibersegurança com uma perspetiva inovadora e orientada para os resultados.

- **Adaptabilidade tecnológica:** Capacidade de incorporar eficazmente novas ferramentas, técnicas e metodologias baseadas na Inteligência Artificial, adaptando-se rapidamente aos avanços tecnológicos e aplicando-os em ambientes de trabalho diversificados com elevados padrões de exigência
- **Comunicação efetiva:** Competência para exprimir ideias, resultados e estratégias de forma clara e estruturada, adaptando a linguagem técnica para ser compreendida tanto por equipas multidisciplinares como por audiências não tecnológicas
- **Gestão de projetos:** Capacidade para planear, organizar e coordenar projetos de cibersegurança, supervisionando a implementação de soluções e assegurando o cumprimento de prazos, recursos e objetivos estratégicos em contextos dinâmicos e em mudança
- **Colaboração interdisciplinar:** Capacidade de trabalhar eficazmente com equipas diversificadas, integrando conhecimentos e perspectivas de áreas como a cibersegurança, a inteligência artificial, a tecnologia e a gestão empresarial, a fim de atingir objetivos comuns e gerar soluções integradas



Após realizar a qualificação poderá desempenhar os seus conhecimentos e competências nos seguintes cargos:

1. **Analista de cibersegurança especializado em Inteligência Artificial:** Responsável pela identificação de vulnerabilidades e ameaças em sistemas digitais, utilizando ferramentas avançadas de Inteligência Artificial para proteger redes e dados críticos.
2. **Especialista em Deteção de Intrusão de Sistemas:** Responsável pela implementação e gerir sistemas de deteção de intrusão alimentados por Inteligência Artificial para impedir o acesso não autorizado a infra-estruturas digitais.
3. **Consultor de Segurança de Dispositivos Ligados:** Responsável pela atenuação dos riscos associados aos dispositivos da Internet das Coisas, garantindo a sua segurança em ambientes empresariais e domésticos.
4. **Especialista em Análise Preditiva de Ameaças Cibernéticas:** Centra-se na antecipação de potenciais ataques através da aplicação de técnicas de modelação preditiva e de aprendizagem automática.
5. **Analista de Resposta a Incidentes de Inteligência Artificial:** Responsável de gerir e automatizar a resposta a incidentes cibernéticos utilizando ferramentas de Inteligência Artificial.
6. **Auditor de Vulnerabilidades Assistido por Inteligência Artificial:** Responsável de avaliar sistemas digitais para detetar falhas de segurança e propor soluções eficazes com o apoio de ferramentas de Inteligência Artificial.

Irá liderar projetos de cibersegurança com ênfase na integração de sistemas inteligentes para garantir uma proteção abrangente de dados e redes"

06

Metodologia de estudo

A TECH é a primeira universidade do mundo a unir a metodologia dos ***case studies*** com o ***Relearning***, um sistema de aprendizado 100% online baseado na repetição guiada.

Essa estratégia de ensino inovadora foi projetada para oferecer aos profissionais a oportunidade de atualizar conhecimentos e desenvolver habilidades de forma intensiva e rigorosa. Um modelo de aprendizagem que coloca o aluno no centro do processo acadêmico e lhe dá o papel principal, adaptando-se às suas necessidades e deixando de lado as metodologias mais convencionais.

A TECH prepara você para enfrentar novos desafios em ambientes incertos e alcançar o sucesso em sua carreira"

O aluno: a prioridade de todos os programas da TECH

Na metodologia de estudo da TECH, o aluno é o protagonista absoluto. As ferramentas pedagógicas de cada programa foram selecionadas levando-se em conta as demandas de tempo, disponibilidade e rigor acadêmico que, atualmente, os alunos, bem como os empregos mais competitivos do mercado, exigem.

Com o modelo educacional assíncrono da TECH, é o aluno quem escolhe quanto tempo passa estudando, como decide estabelecer suas rotinas e tudo isso no conforto do dispositivo eletrônico de sua escolha. O aluno não precisa assistir às aulas presenciais, que muitas vezes não poderá comparecer. As atividades de aprendizado serão realizadas de acordo com sua conveniência. O aluno sempre poderá decidir quando e de onde estudar.

Na TECH, o aluno NÃO terá aulas ao vivo (das quais poderá nunca participar)"

Os programas de ensino mais abrangentes do mundo

A TECH se caracteriza por oferecer os programas acadêmicos mais completos no ambiente universitário. Essa abrangência é obtida por meio da criação de programas de estudo que cobrem não apenas o conhecimento essencial, mas também as últimas inovações em cada área.

Por serem constantemente atualizados, esses programas permitem que os alunos acompanhem as mudanças do mercado e adquiram as habilidades mais valorizadas pelos empregadores. Dessa forma, os alunos da TECH recebem uma preparação abrangente que lhes dá uma vantagem competitiva significativa para avançar em suas carreiras.

Além disso, eles podem fazer isso de qualquer dispositivo, PC, tablet ou smartphone.

> *O modelo da TECH é assíncrono, portanto, você poderá estudar com seu PC, tablet ou smartphone onde quiser, quando quiser e pelo tempo que quiser"*

Case studies ou Método de caso

O método de casos tem sido o sistema de aprendizado mais amplamente utilizado pelas melhores escolas de negócios do mundo. Desenvolvido em 1912 para que os estudantes de direito não aprendessem a lei apenas com base no conteúdo teórico, sua função também era apresentar a eles situações complexas da vida real. Assim, eles poderiam tomar decisões informadas e fazer julgamentos de valor sobre como resolvê-los. Em 1924 foi estabelecido como o método de ensino padrão em Harvard.

Com esse modelo de ensino, é o próprio aluno que desenvolve sua competência profissional por meio de estratégias como o *Learning by doing* ou o *Design Thinking*, usados por outras instituições renomadas, como Yale ou Stanford.

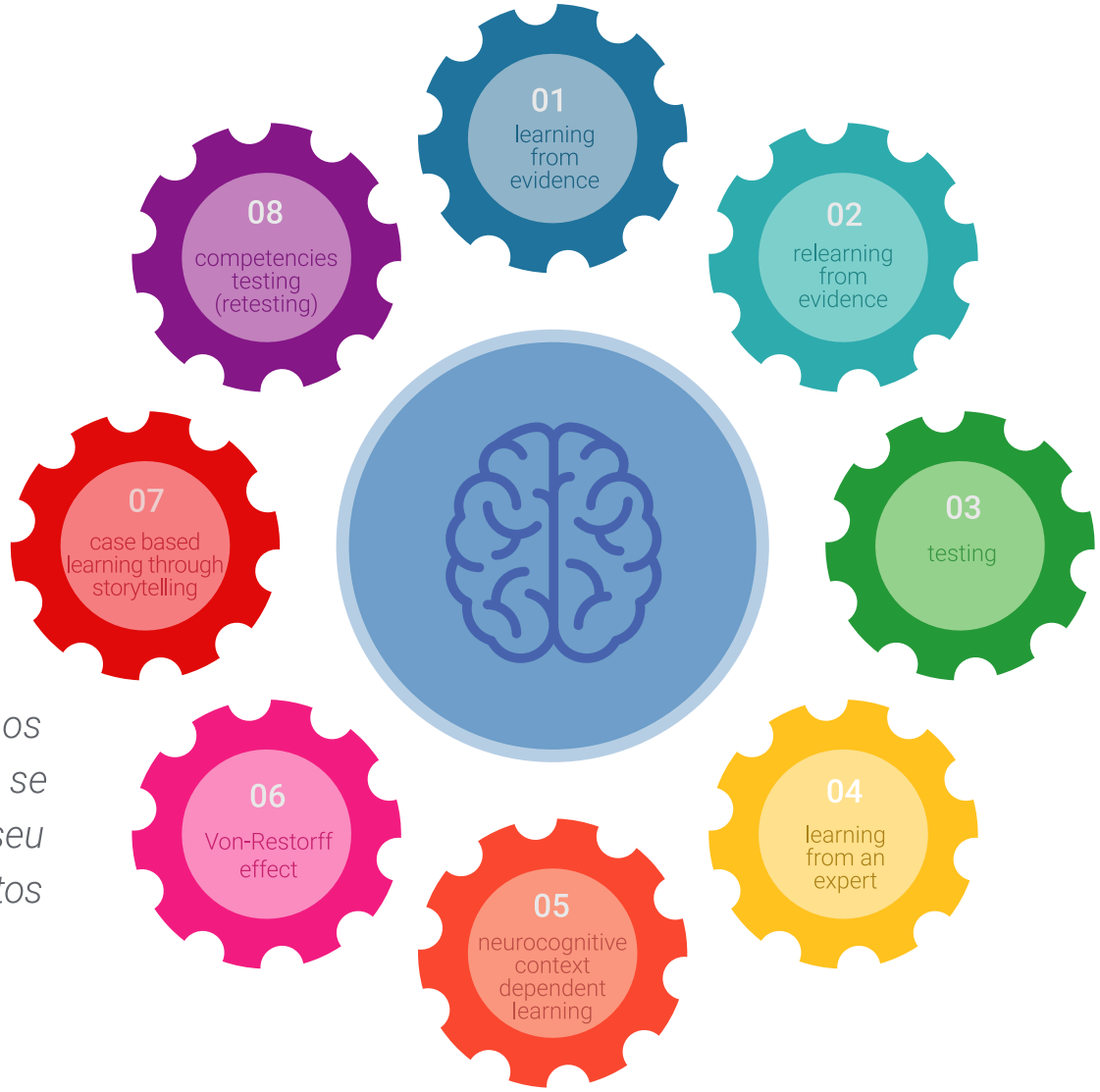
Esse método orientado para a ação será aplicado em toda a trajetória acadêmica do aluno com a TECH. Dessa forma, o aluno será confrontado com várias situações da vida real e terá de integrar conhecimentos, pesquisar, argumentar e defender suas ideias e decisões. A premissa era responder à pergunta sobre como eles agiriam diante de eventos específicos de complexidade em seu trabalho diário.

Método *Relearning*

Na TECH os *case studies* são alimentados pelo melhor método de ensino 100% online: o *Relearning*.

Esse método rompe com as técnicas tradicionais de ensino para colocar o aluno no centro da equação, fornecendo o melhor conteúdo em diferentes formatos. Dessa forma, consegue revisar e reiterar os principais conceitos de cada matéria e aprender a aplicá-los em um ambiente real.

Na mesma linha, e de acordo com várias pesquisas científicas, a repetição é a melhor maneira de aprender. Portanto, a TECH oferece entre 8 e 16 repetições de cada conceito-chave dentro da mesma lição, apresentadas de uma forma diferente, a fim de garantir que o conhecimento seja totalmente incorporado durante o processo de estudo.



O Relearning permitirá uma aprendizagem com menos esforço e mais desempenho, fazendo com que você se envolva mais em sua especialização, desenvolvendo seu espírito crítico e sua capacidade de defender argumentos e contrastar opiniões: uma equação de sucesso.

Um Campus Virtual 100% online com os melhores recursos didáticos

Para aplicar sua metodologia de forma eficaz, a TECH se concentra em fornecer aos alunos materiais didáticos em diferentes formatos: textos, vídeos interativos, ilustrações e mapas de conhecimento, entre outros. Todos eles são projetados por professores qualificados que concentram seu trabalho na combinação de casos reais com a resolução de situações complexas por meio de simulação, o estudo de contextos aplicados a cada carreira profissional e o aprendizado baseado na repetição, por meio de áudios, apresentações, animações, imagens etc.

As evidências científicas mais recentes no campo da neurociência apontam para importância de levar em conta o local e o contexto em que o conteúdo é acessado antes de iniciar um novo processo de aprendizagem. A capacidade de ajustar essas variáveis de forma personalizada ajuda as pessoas a lembrar e armazenar o conhecimento no hipocampo para retenção a longo prazo. Trata-se de um modelo chamado *Neurocognitive context-dependent e-learning* que é aplicado conscientemente nesse curso universitário.

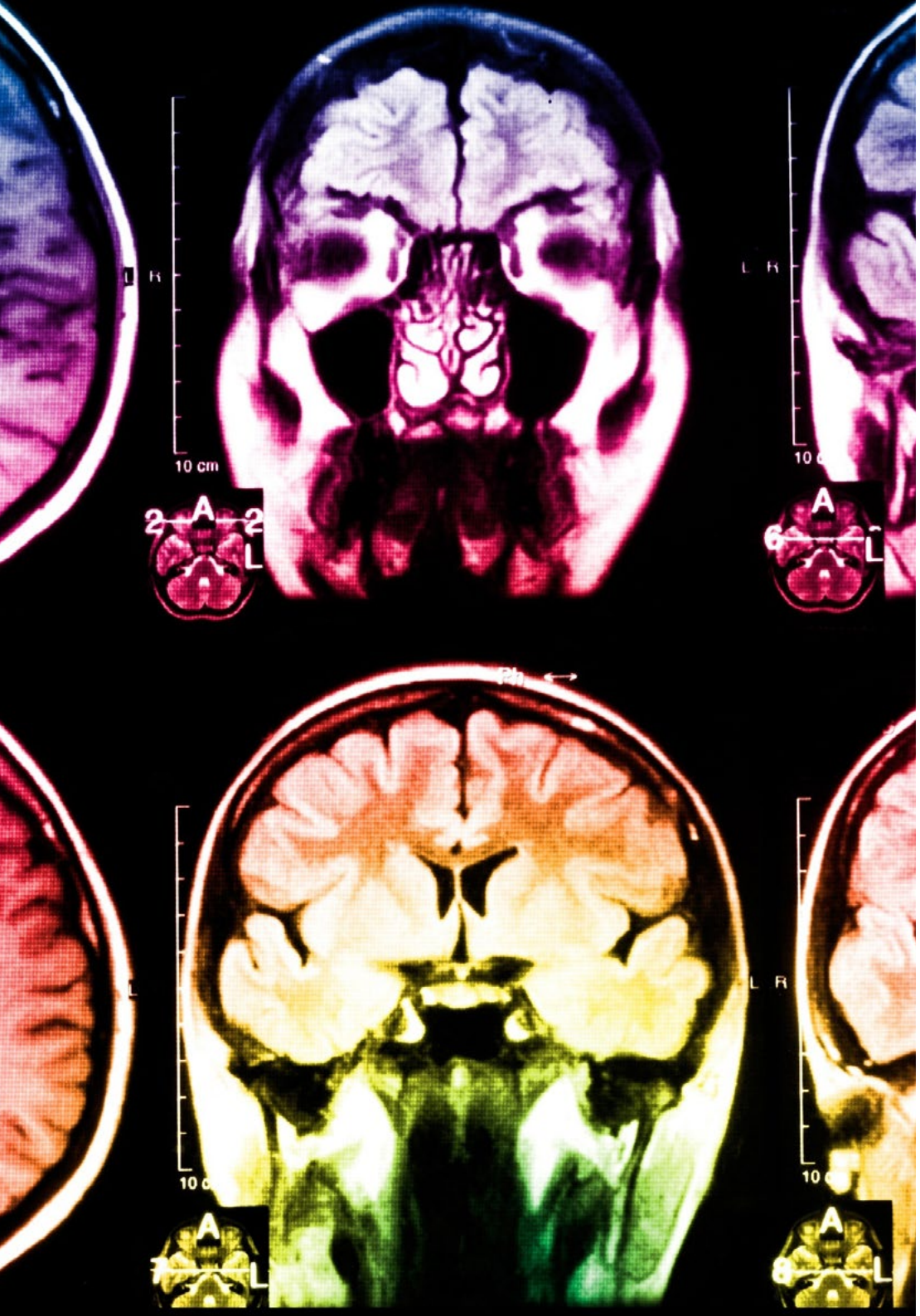
Por outro lado, também para favorecer ao máximo o contato entre mentor e mentorado, é oferecida uma ampla variedade de possibilidades de comunicação, tanto em tempo real quanto em diferido (mensagens internas, fóruns de discussão, serviço telefônico, contato por e-mail com a secretaria técnica, bate-papo, videoconferência etc.).

Da mesma forma, esse Campus Virtual muito completo permitirá que os alunos da TECH organizem seus horários de estudo de acordo com sua disponibilidade pessoal ou obrigações de trabalho. Dessa forma, eles terão um controle global dos conteúdos acadêmicos e de suas ferramentas didáticas, em função de sua atualização profissional acelerada.

> *O modo de estudo online deste programa permitirá que você organize seu tempo e ritmo de aprendizado, adaptando-o à sua agenda"*

A eficácia do método é justificada por quatro conquistas fundamentais:

1. Os alunos que seguem este método não só assimilam os conceitos, mas também desenvolvem a capacidade intelectual através de exercícios de avaliação de situações reais e de aplicação de conhecimentos.
2. A aprendizagem se consolida nas habilidades práticas, permitindo ao aluno integrar melhor o conhecimento à prática clínica.
3. A assimilação de ideias e conceitos se torna mais fácil e eficiente, graças à abordagem de situações decorrentes da realidade.
4. A sensação de eficiência do esforço investido se torna um estímulo muito importante para os alunos, o que se traduz em um maior interesse pela aprendizagem e um aumento no tempo dedicado ao curso.



A metodologia universitária mais bem avaliada por seus alunos

Os resultados desse modelo acadêmico inovador podem ser vistos nos níveis gerais de satisfação dos alunos da TECH.

A avaliação dos estudantes sobre a qualidade do ensino, a qualidade dos materiais, a estrutura e os objetivos dos cursos é excelente. Não é de surpreender que a instituição se tenha tornado a universidade mais bem classificada pelos seus estudantes de acordo com o índice Global Score, obtendo uma classificação de 4,9 em 5.

Acesse o conteúdo do estudo de qualquer dispositivo com conexão à Internet (computador, tablet, smartphone) graças ao fato da TECH estar na vanguarda da tecnologia e do ensino.

Você poderá aprender com as vantagens do acesso a ambientes de aprendizagem simulados e com a abordagem de aprendizagem por observação, ou seja, aprender com um especialista.

Assim, os melhores materiais educacionais, cuidadosamente preparados, estarão disponíveis neste programa:

Material de estudo

O conteúdo didático foi elaborado especialmente para este curso pelos especialistas que irão ministrá-lo, o que permite que o desenvolvimento didático seja realmente específico e concreto.

Posteriormente, esse conteúdo é adaptado ao formato audiovisual, para criar o método de trabalho online, com as técnicas mais recentes que nos permitem lhe oferecer a melhor qualidade em cada uma das peças que colocaremos a seu serviço.

Práticas de aptidões e competências

Serão realizadas atividades para desenvolver as habilidades e competências específicas em cada área temática. Práticas e dinâmicas para adquirir e desenvolver as competências e habilidades que um especialista precisa desenvolver no âmbito da globalização.

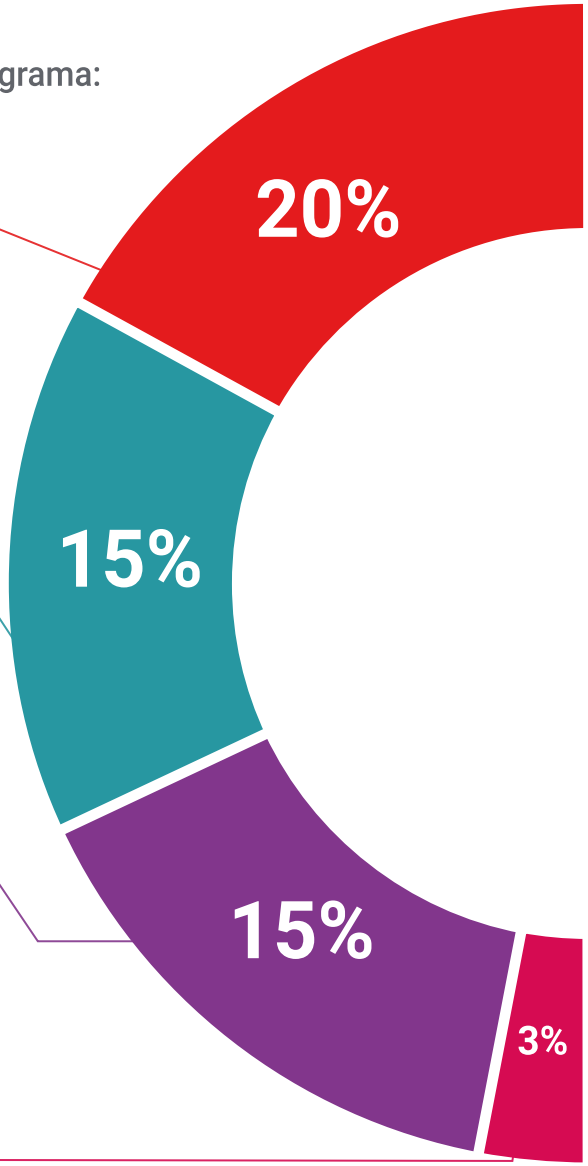
Resumos interativos

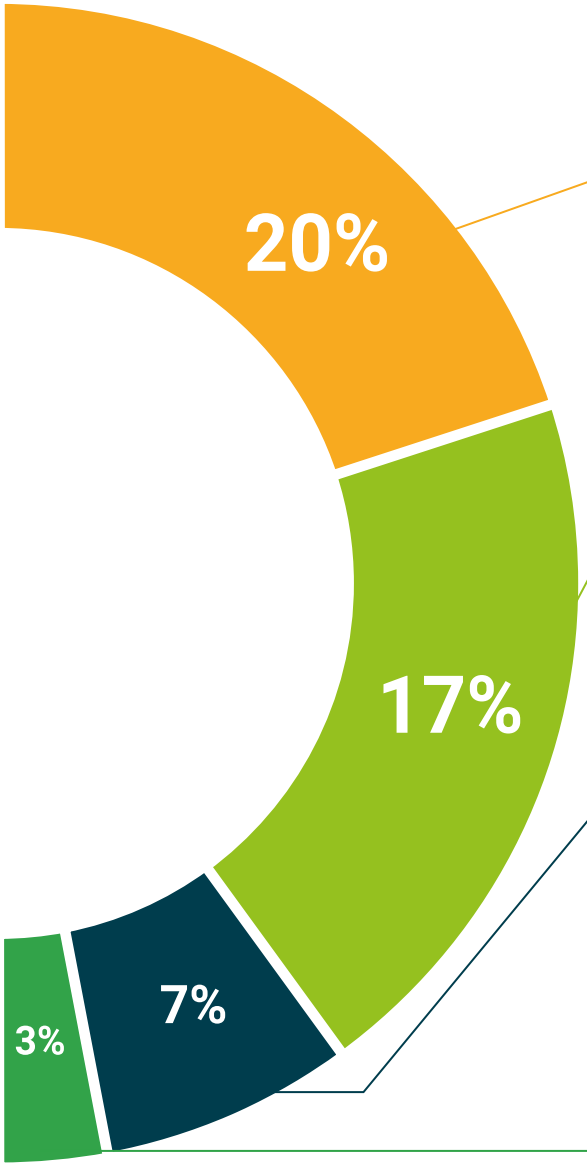
Apresentamos os conteúdos de forma atraente e dinâmica em pílulas multimídia que incluem áudio, vídeos, imagens, diagramas e mapas conceituais com o objetivo de reforçar o conhecimento.

Este sistema exclusivo de capacitação por meio da apresentação de conteúdo multimídia foi premiado pela Microsoft como "Caso de sucesso na Europa"

Leituras complementares

Artigos recentes, documentos científicos, guias internacionais, entre outros. Na biblioteca virtual do estudante você terá acesso a tudo o que for necessário para completar sua capacitação.





Case Studies

Você concluirá uma seleção dos melhores *case studies* da disciplina. Casos apresentados, analisados e orientados pelos melhores especialistas no cenário internacional.

Testing & Retesting

Avaliamos e reavaliamos periodicamente seus conhecimentos ao longo de todo o programa. Fazemos isso em 3 dos 4 níveis da Pirâmide de Miller.

Masterclasses

Há evidências científicas sobre a utilidade da observação de terceiros especialistas.

O *Learning from an expert* fortalece o conhecimento e a memória, e aumenta nossa confiança para tomar decisões difíceis no futuro.

Guias rápidos de ação

A TECH oferece o conteúdo mais relevante do curso em formato de fichas de trabalho ou guias rápidos de ação. Uma forma sintetizada, prática e eficaz de ajudar os alunos a progredirem na aprendizagem.

07

Corpo docente

A equipa docente selecionada pela TECH para este programa universitário é composta por especialistas de renome em Cibersegurança e Inteligência Artificial com uma vasta experiência profissional e académica. A sua experiência vai desde a implementação de sistemas avançados de deteção de ameaças até à conceção de estratégias proactivas para proteger as infra-estruturas digitais. Além disso, a sua abordagem prática e os seus conhecimentos atualizados garantem um ensino de elevada qualidade, destinado a resolver os verdadeiros desafios do ambiente tecnológico atual.

Terá à sua disposição uma equipa docente de prestígio, com uma longa carreira profissional, constituída por especialistas na proteção de sistemas digitais e no desenvolvimento de estratégias de defesa inovadoras"

Direção

Dr. Peralta Martín-Palomino, Arturo

- CEO e CTO, Prometeus Global Solutions
- CTO em Korporate Technologies
- CTO em AI Shepherds GmbH
- Consultor e Assessor Empresarial Estratégico na Alliance Medical
- Diretor de Design e Desenvolvimento na DocPath
- Doutoramento em Engenharia Informática pela Universidade de Castilla-La Mancha
- Doutoramento em Economia, Empresas e Finanças pela Universidade Camilo José Cela
- Doutoramento em Psicologia pela Universidade de Castilla-La Mancha
- Mestrado em Executive MBA pela Universidade Isabel I
- Mestrado em Gestão Comercial e de Marketing pela Universidade Isabel I
- Mestrado Especialista em Big Data pela Formação Hadoop
- Mestrado em Tecnologias Avançadas de Informação da Universidade de Castilla-La Mancha
- Membro: Grupo de Investigação SMILE

Professores

Sr. Del Rey Sánchez, Alejandro

- Responsável pela implementação de programas para melhorar a atenção tática em emergências
- Licenciatura em Engenharia de Organização Industrial
- Certificação em *Big Data* e *Business Analytics*
- Certificação em Microsoft Excel Avançado, VBA, KPI e DAX
- Certificação em CIS Sistemas de Telecomunicações e Informação

Aproveite a oportunidade para conhecer os últimos avanços nesta área e aplicá-los na sua prática diária"

08

Certificação

O Curso de Especialização em Análise e Deteção de Ameaças de Cibersegurança com Inteligência Artificial garante, além da formação mais rigorosa e atualizada, o acesso a um certificado de Curso de Especialização emitido pela TECH Global University.

Conclua este programa de estudos com sucesso e receba seu certificado sem sair de casa e sem burocracias”

Este programa permitirá a obtenção do certificado próprio de **Curso de Especialização em Análise e Deteção de Ameaças de Cibersegurança com Inteligência Artificial** reconhecido pela TECH Global University, a maior universidade digital do mundo.

A **TECH Global University,** é uma Universidade Europeia Oficial reconhecida publicamente pelo Governo de Andorra ***(bollettino ufficiale)***. Andorra faz parte do Espaço Europeu de Educação Superior (EEES) desde 2003. O EEES é uma iniciativa promovida pela União Europeia com o objetivo de organizar o modelo de formação internacional e harmonizar os sistemas de ensino superior dos países membros desse espaço. O projeto promove valores comuns, a implementação de ferramentas conjuntas e o fortalecimento dos seus mecanismos de garantia de qualidade para fomentar a colaboração e a mobilidade entre alunos, investigadores e académicos.

Esse título próprio da **TECH Global University**, é um programa europeu de formação contínua e atualização profissional que garante a aquisição de competências na sua área de conhecimento, conferindo um alto valor curricular ao aluno que conclui o programa.

A TECH é membro da Society for the Study of Artificial Intelligence and Simulation of Behavior (AISB), a maior organização dedicada à investigação e desenvolvimento em Inteligência Artificial na Europa. Ao fazer parte dos seus membros, a TECH oferece aos estudantes um grande número de pesquisas a nível de doutoramento, conferências online, masterclasses e acesso a uma rede de professores e profissionais que contribuirão continuamente para o desenvolvimento profissional do estudante através de apoio e acompanhamento contínuos.

TECH é membro da:


tech global university

Sr./Sra. _____, com o documento de identidade nº _____, foi aprovado satisfatoriamente e obteve o certificado de:

Curso de Especialização em Análise e Deteção de Ameaças de Cibersegurança com Inteligência Artificial

Trata-se de um título próprio com duração de 540 horas, o equivalente a 18 ECTS, com data de início dd/ mm/aaaa e data final dd/mm/aaaa.

A TECH Global University é uma universidade oficialmente reconhecida pelo Governo de Andorra em 31 de janeiro de 2024, que pertence ao Espaço Europeu de Educação Superior (EEES).

Andorra la Vella, 28 de fevereiro de 2024

Dr. Pedro Navarro Illana
Reitor

código único TECH: BBADCEADBECB99D techtitute.com/titulos

Título: **Curso de Especialização em Análise e Deteção de Ameaças de Cibersegurança com Inteligência Artificial**

Modalidade: **online**

Duração: **6 meses**

Acreditação: **18 ECTS**

*Apostila de Haia: Caso o aluno solicite que o seu certificado seja apostilado, a TECH Global University providenciará a obtenção do mesmo a um custo adicional.

tech global university

Curso de Especialização

Análise e Deteção de Ameaças de Cibersegurança com Inteligência Artificial

- Modalidade: **online**
- Duração: **6 meses**
- Certificação: **TECH Global University**
- Acreditação: **18 ECTS**
- Horário: **ao seu próprio ritmo**
- Exames: **online**

Curso de Especialização

Análise e Deteção de Ameaças de Cibersegurança com Inteligência Artificial

TECH é membro da:

tech global university