Mestrado Próprio

Inteligência Artificial na Cibersegurança

TECH é membro da:

tech global university

tech global university

Mestrado Próprio
Inteligência Artificial na Cibersegurança

- Modalidade: **online**
- Duração: **12 meses**
- Certificação: **TECH Global University**
- Acreditação: **90 ECTS**
- Horário: **ao seu próprio ritmo**
- Exames: **online**

Acesso ao site: www.techtitute.com/pt/informatica/mestrado-proprio/mestrado-proprio-inteligencia-artificial-ciberseguranca

Índice

01

Apresentação do programa

A Inteligência Artificial aplicada à Cibersegurança é um setor em plena expansão devido ao aumento das ameaças digitais e à necessidade de respostas proativas e eficazes. Neste âmbito, os sistemas inteligentes não só permitem automatizar processos repetitivos, como também analisar grandes volumes de dados para identificar padrões anómalos, antecipar ataques e reforçar sistemas de proteção. Por essa razão, a TECH elaborou uma exaustiva qualificação universitária que prepara os informáticos para enfrentar os desafios atuais em Cibersegurança, oferecendo-lhes as ferramentas necessárias para antecipar as ameaças futuras, liderar iniciativas tecnológicas e garantir a proteção de infraestruturas críticas a nível global. Tudo isso, através de um itinerário académico 100% online ministrado pelos melhores especialistas do setor.

Com este inovador programa universitário 100% online, dominará as técnicas mais avançadas de Criptografia moderna e desenhará sistemas de proteção robustos para garantir a privacidade e autenticidade dos dados"

A Inteligência Artificial e a Cibersegurança são dois pilares fundamentais na era digital. Enquanto a primeira foca-se no desenvolvimento de sistemas capazes de simular processos cognitivos humanos, a Cibersegurança encarrega-se de proteger os sistemas informáticos e os dados de ataques maliciosos. A combinação de ambas disciplinas permite criar soluções avançadas que não só detetam e mitigam ameaças em tempo real, como também antecipam possíveis vulnerabilidades, garantindo assim um ambiente digital mais seguro. Este contexto impulsiona a necessidade de profissionais altamente qualificados que dominem tanto os fundamentos da Inteligência Artificial como as suas aplicações específicas na defesa cibernética.

A partir dessas exigências surge o Mestrado Próprio em Inteligência Artificial em Cibersegurança da TECH, um programa estruturado em 20 módulos exaustivos que abordam desde os fundamentos da Inteligência Artificial e a gestão de dados até ao aprendizado profundo, redes neuronais convolucionais e aplicação de modelos gerativos em Cibersegurança. Além disso, aprofunda-se na deteção de ameaças, análise forense digital e criptografia moderna, utilizando ferramentas como TensorFlow e modelos avançados de Inteligência Artificial para responder aos desafios de um ambiente digital em constante evolução. Desta forma, este percurso académico permite aos informáticos antecipar as ameaças emergentes e liderar estratégias de segurança em ambientes complexos.

Quanto à metodologia desta titulação universitária, a TECH oferece um ambiente 100% online que permite aos profissionais planejar de forma individual os seus horários e ritmo de estudo. Além disso, emprega o seu inovador sistema de *Relearning*, que facilita a assimilação progressiva de conceitos-chave através da reiteração contextualizada e do aprendizado ativo. Nesta mesma linha, os alunos apenas precisarão de um dispositivo eletrónico com ligação à internet para aceder ao Campus Virtual. Lá poderão acessar uma vasta biblioteca de recursos multimédia, como resumos interativos, vídeos explicativos ou leituras especializadas baseadas nas últimas evidências.

Este **Mestrado Próprio em Inteligência Artificial na Cibersegurança** conta com o conteúdo educativo mais completo e atualizado do mercado. As suas principais características são:

- O desenvolvimento de casos práticos apresentados por especialistas em Inteligência Artificial, Cibersegurança e tecnologias avanças
- Os conteúdos gráficos, esquemáticos e eminentemente práticos com os quais o curso foi concebido reúnem informação científica e prática sobre as disciplinas indispensáveis para o exercício profissional
- Os exercícios práticos onde o processo de autoavaliação pode ser efetuado 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

Profundizará na forma como a Inteligência Artificial transforma a Cibersegurança com ferramentas como Redes Neuronais e modelos gerativos aplicados à deteção e prevenção de ameaças"

Otimizará a sua tomada de decisões estratégicas mediante a análise preditiva e o uso de modelos avançados na gestão de ataques cibernéticos”

Terá à sua disposição os recursos multimédia mais vanguardistas, desde resumos interativos até vídeos explicativos e leituras especializadas.

Liderará projetos em setores chave, como a proteção de infraestruturas e a gestão de sistemas conectados da Internet das Coisas.

O programa inclui no seu corpo docente profissionais do setor que compartilham nesta formação a experiência do seu trabalho, além de reconhecidos especialistas de sociedades de referência e universidades de prestígio.

O seu conteúdo multimédia, elaborado com a última tecnologia educativa, permitirá ao profissional um aprendizado situado e contextual, ou seja, um ambiente simulado que proporcionará uma capacitação imersiva programada para se treinar 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

Plano de estudos

O programa deste Mestrado Próprio aborda tanto os fundamentos da Inteligência Artificial como as suas aplicações específicas no campo da Cibersegurança. Ao longo deste percurso académico, os informáticos aprofundarão temas chave como a algoritmia, a mineração de dados e o processamento da linguagem natural. Também explorarão as redes neuronais avançadas e sistemas inteligentes aplicados à análise forense, bem como a deteção de intrusões e defesa proativa, o que lhes permitirá adquirir as ferramentas necessárias para desenvolver soluções inovadoras frente a ameaças digitais.

Com a metodologia Relearning, da qual a TECH é pioneira, especializar-se-á no uso de Sistemas Bioinspirados e Aprendizagem Profunda para abordar problemas complexos na proteção digital"

Módulo 1. Fundamentos da Inteligência Artificial

1.1. História da Inteligência Artificial
- 1.1.1. Quando se começa a falar de inteligência artificial?
- 1.1.2. Referências no cinema
- 1.1.3. Importância da inteligência artificial
- 1.1.4. Tecnologias que viabilizam e apoiam a inteligência artificial

1.2. Inteligência Artificial em jogos
- 1.2.1. Teoria dos jogos
- 1.2.2. *Minimax* e poda Alfa-Beta
- 1.2.3. Simulação: Monte Carlo

1.3. Redes neuronais
- 1.3.1. Fundamentos teológicos
- 1.3.2. Modelo computacional
- 1.3.3. Redes neuronais supervisionadas e não supervisionadas
- 1.3.4. Perceptron simples
- 1.3.5. Perceptron multicamadas

1.4. Algoritmos genéticos
- 1.4.1. História
- 1.4.2. Base biológica
- 1.4.3. Codificação de problemas
- 1.4.4. Criação da população inicial
- 1.4.5. Algoritmo principal e operadores genéticos
- 1.4.6. Avaliação dos indivíduos: Fitness

1.5. Tesauros, vocabulários, taxonomias
- 1.5.1. Vocabulários
- 1.5.2. Taxonomias
- 1.5.3. Tesaurus
- 1.5.4. Ontologias
- 1.5.5. Representação do conhecimento: web semântica

1.6. Web semântica
- 1.6.1. Especificações: RDF, RDFS e OWL
- 1.6.2. Inferência/razoabilidade
- 1.6.3. *Linked Data*

1.7. Sistemas periciais e DSS
- 1.7.1. Sistemas periciais
- 1.7.2. Sistema de apoio à decisão

1.8. *Chatbots* e assistentes virtuais
- 1.8.1. Tipos de assistentes: assistentes de voz e texto
- 1.8.2. Partes fundamentais para o desenvolvimento de um assistente: *Intenções*, entidades e fluxo de diálogo
- 1.8.3. Integração: Web, *Slack*, Whatsapp, Facebook
- 1.8.4. Ferramentas para o desenvolvimento dos assistentes: *Dialog Flow, Watson Assistant*

1.9. Estratégia de implementação de IA

1.10. Futuro da inteligência artificial
- 1.10.1. Compreendemos como detetar as emoções através de algoritmos
- 1.10.2. Criação de uma personalidade: linguagem, expressões e conteúdo
- 1.10.3. Tendências da Inteligência Artificial
- 1.10.4. Reflexão

Módulo 2. Tipos e ciclo de vida do dado

2.1. A Estatística
- 2.1.1. Estatística: estatística descritiva, inferências estatísticas
- 2.1.2. População, amostra indivíduo
- 2.1.3. Variáveis: Definição de medição

2.2. Tipos de dados estatísticos
- 2.2.1. De acordo com o tipo
  - 2.2.1.1. Quantitativos: dados contínuos e dados discretos
  - 2.2.1.2. Qualitativo: dados binomiais, dados nominais, dados ordinais
- 2.2.2. De acordo com a sua forma
  - 2.2.2.1. Numérico
  - 2.2.2.2. Texto
  - 2.2.2.3. Lógico
- 2.2.3. De acordo com a sua fonte
  - 2.2.3.1. Primários
  - 2.2.3.2. Secundários

2.3. Ciclo de vida dos dados
- 2.3.1. Etapas do ciclo
- 2.3.2. Marcos do ciclo
- 2.3.3. Princípios FAIR

2.4. Etapas iniciais do ciclo
- 2.4.1. Definição de metas
- 2.4.2. Determinação de recursos necessários
- 2.4.3. Diagrama de Gantt
- 2.4.4. Estrutura de dados

2.5. Recolha de dados
- 2.5.1. Metodologia de recolha
- 2.5.2. Ferramentas de recolha
- 2.5.3. Canais de recolha

2.6. Limpeza de dados
- 2.6.1. Fases de limpeza de dados
- 2.6.2. Qualidade dos dados
- 2.6.3. Manipulação de dados (com R)

2.7. Análise de dados, interpretação e avaliação dos resultados
- 2.7.1. Medidas estatísticas
- 2.7.2. Indicadores de relação
- 2.7.3. Extração de dados

2.8. Armazém de dados (*Datawarehouse*)
- 2.8.1. Elementos incluídos
- 2.8.2. Design
- 2.8.3. Aspetos a considerar

2.9. Disponibilidade dos dados
- 2.9.1. Acesso
- 2.9.2. Utilidade
- 2.9.3. Segurança

2.10. Aspetos regulamentares
- 2.10.1. Lei da Proteção de Dados
- 2.10.2. Boas práticas
- 2.10.3. Outros aspetos regulamentares

Módulo 3. O dado na Inteligência Artificial

3.1. Ciência de dados
- 3.1.1. A ciência de dados
- 3.1.2. Ferramentas avançadas para o cientista de dados

3.2. Dados, informação e conhecimento
- 3.2.1. Dados, informação e conhecimento
- 3.2.2. Tipos de dados
- 3.2.3. Fontes de dados

3.3. Dos dados à informação
- 3.3.1. Análise de Dados
- 3.3.2. Tipos de análise
- 3.3.3. Extração de informação de um *Dataset*

3.4. Extração de informação através da visualização
- 3.4.1. A visualização como ferramenta de análise
- 3.4.2. Métodos de visualização
- 3.4.3. Visualização de um conjunto de dados

3.5. Qualidade dos dados
- 3.5.1. Dados de qualidade
- 3.5.2. Limpeza de dados
- 3.5.3. Pré-processamento básico de dados

3.6. *Dataset*
- 3.6.1. Enriquecimento do *Dataset*
- 3.6.2. A maldição da dimensionalidade
- 3.6.3. Modificação do nosso conjunto de dados

3.7. Desequilíbrio
- 3.7.1. Desequilíbrio de classes
- 3.7.2. Técnicas de mitigação do desequilíbrio
- 3.7.3. Equilíbrio de um *Dataset*

3.8. Modelos não supervisionados
- 3.8.1. Modelo não supervisionado
- 3.8.2. Métodos
- 3.8.3. Classificação com modelos não supervisionados

3.9. Modelos supervisionados
- 3.9.1. Modelo supervisionado
- 3.9.2. Métodos
- 3.9.3. Classificação com modelos supervisionados

3.10. Ferramentas e boas práticas
- 3.10.1. Boas práticas para um cientista de dados
- 3.10.2. O melhor modelo
- 3.10.3. Ferramentas úteis

Módulo 4. Exploração de dados. Seleção, pré-processamento e transformação

4.1. A inferência estatística
- 4.1.1. Estatística descritiva vs Inferência estatística
- 4.1.2. Procedimentos paramétricos
- 4.1.3. Procedimentos não paramétricos

4.2. Análise exploratória
- 4.2.1. Análise descritiva
- 4.2.2. Visualização
- 4.2.3. Preparação de dados

4.3. Preparação de dados
- 4.3.1. Integração e limpeza de dados
- 4.3.2. Normalização de dados
- 4.3.3. Transformando atributos

4.4. Os valores perdidos
- 4.4.1. Tratamento de valores perdidos
- 4.4.2. Métodos de imputação de máxima verosimilhança
- 4.4.3. Imputação de valores perdidos utilizando a aprendizagem automática

4.5. O ruído dos dados
- 4.5.1. Classes de ruído e atributos
- 4.5.2. Filtragem de ruído
- 4.5.3. O efeito do ruído

4.6. A maldição da dimensionalidade
- 4.6.1. *Oversampling*
- 4.6.2. *Undersampling*
- 4.6.3. Redução de dados multidimensionais

4.7. De atributos contínuos a discretos
- 4.7.1. Dados contínuos versus dados discretos
- 4.7.2. Processo de discretização

4.8. Os dados
- 4.8.1. Seleção de dados
- 4.8.2. Perspetivas e critérios de seleção
- 4.8.3. Métodos de seleção

4.9. Seleção de instâncias
- 4.9.1. Métodos para a seleção de instâncias
- 4.9.2. Seleção de protótipos
- 4.9.3. Métodos avançados para a seleção de instâncias

4.10. Pré-processamento de dados em ambientes *Big Data*

Módulo 5. Algoritmo e complexidade na Inteligência Artificial

5.1. Introdução às estratégias de desenho do algoritmos
- 5.1.1. Recursividade
- 5.1.2. Divide e conquista
- 5.1.3. Outras estratégias

5.2. Eficiência e análise dos algoritmos
- 5.2.1. Medidas de eficiência
- 5.2.2. Medir o tamanho da entrada
- 5.2.3. Medir o tempo de execução
- 5.2.4. Caso pior, melhor e médio
- 5.2.5. Notação assintótica
- 5.2.6. Critérios de Análise matemática de algoritmos não recursivos
- 5.2.7. Análise matemática de algoritmos recursivos
- 5.2.8. Análise empírica de algoritmos

5.3. Algoritmos de ordenação
- 5.3.1. Conceito de ordenação
- 5.3.2. Ordenação da bolha
- 5.3.3. Ordenação por seleção
- 5.3.4. Ordenação por inserção
- 5.3.5. Ordenação por mistura (*Merge_Sort*)
- 5.3.6. Ordenação rápida (*Quicksort*)

5.4. Algoritmos com árvores
- 5.4.1. Conceito de árvore
- 5.4.2. Árvores binários
- 5.4.3. Caminhos de árvore
- 5.4.4. Representar expressões
- 5.4.5. Árvores binários ordenadas
- 5.4.6. Árvores binárias equilibradas

5.5. Algoritmos com *Heaps*
- 5.5.1. Os *Heaps*
- 5.5.2. O algoritmo *Heapsort*
- 5.5.3. As filas de prioridade

5.6. Algoritmos com Grafos
- 5.6.1. Representação
- 5.6.2. Caminho de largura
- 5.6.3. Caminho de profundidade
- 5.6.4. Ordenação topológica

5.7. Algoritmos *Greedy*
- 5.7.1. A estratégia *Greedy*
- 5.7.2. Elementos da estratégia *Greedy*
- 5.7.3. Câmbio de moedas
- 5.7.4. Problema do viajante
- 5.7.5. Problema da mochila

5.8. Pesquisa de caminhos mínimos
- 5.8.1. O problema do caminho mínimo
- 5.8.2. Arcos negativos e ciclos
- 5.8.3. Algoritmo de Dijkstra

5.9. Algoritmos *Greedy* sobre Grafos
- 5.9.1. A árvore de extensão mínima
- 5.9.2. O algoritmo de Prim
- 5.9.3. O algoritmo Kruskal
- 5.9.4. Análise de complexidade

5.10. *Backtracking*
- 5.10.1. O *Backtracking*
- 5.10.2. Técnicas alternativas

Módulo 6. Sistemas inteligentes

6.1. Teoria dos agentes
- 6.1.1. História do conceito
- 6.1.2. Definição de agente
- 6.1.3. Agentes na Inteligência Artificial
- 6.1.4. Agentes em Engenharia de Software

6.2. Arquiteturas de agentes
- 6.2.1. O processo de argumentação de um agente
- 6.2.2. Agentes reativos
- 6.2.3. Agentes dedutivos
- 6.2.4. Agentes híbridos
- 6.2.5. Comparação

6.3. Informação e conhecimento
- 6.3.1. Distinção entre dados, informação e conhecimento
- 6.3.2. Avaliação qualidade dos dados
- 6.3.3. Métodos de recolha de dados
- 6.3.4. Métodos de aquisição de dados
- 6.3.5. Métodos de aquisição de conhecimento

6.4. Representação do conhecimento
- 6.4.1. A importância da representação do conhecimento
- 6.4.2. Definição da representação do conhecimento através das suas funções
- 6.4.3. Caraterísticas de uma representação do conhecimento

6.5. Ontologias
- 6.5.1. Introdução aos metadados
- 6.5.2. Conceito filosófico de ontologia
- 6.5.3. Conceito informático de ontologia
- 6.5.4. Ontologias de domínio e ontologias de nível superior
- 6.5.5. Como construir uma ontologia?

6.6. Linguagens para ontologias e Software para a criação de ontologias
- 6.6.1. Triples RDF, *Turtle* e N
- 6.6.2. RDF *Schema*
- 6.6.3. OWL
- 6.6.4. SPARQL
- 6.6.5. Introdução às diferentes ferramentas de criação de ontologias
- 6.6.6. Instalação e utilização do *Protégé*

6.7. A web semântica
- 6.7.1. O estado atual e futuro da web semântica
- 6.7.2. Aplicações da web semântica

6.8. Outros modelos representação do conhecimento
- 6.8.1. Vocabulários
- 6.8.2. Visão global
- 6.8.3. Taxonomias
- 6.8.4. Tesaurus
- 6.8.5. Folksonomias
- 6.8.6. Comparação
- 6.8.7. Mapas mentais

6.9. Avaliação e integração das representações do conhecimento
- 6.9.1. Lógica de ordem zero
- 6.9.2. Lógica de primeira ordem
- 6.9.3. Lógica descritiva
- 6.9.4. Relação entre diferentes tipos de lógica
- 6.9.5. *Prolog*: programação baseada na lógica de primeira ordem

6.10. Raciocinadores semânticos, sistemas baseados no conhecimento e Sistemas Periciais
- 6.10.1. Conceito de raciocinador
- 6.10.2. Aplicações de um raciocinador
- 6.10.3. Sistemas baseados no conhecimento
- 6.10.4. MYCIN, história dos Sistemas Periciais
- 6.10.5. Elementos e Arquitetura dos Sistemas Periciais
- 6.10.6. Criação de Sistemas Periciais

Módulo 7. Aprendizagem automática e mineração de dados

7.1. Introdução aos processos de descoberta de conhecimentos e aos conceitos básicos da aprendizagem automática
- 7.1.1. Conceitos-chave dos processos de descoberta do conhecimento
- 7.1.2. Perspetiva histórica dos processos de descoberta do conhecimento
- 7.1.3. Etapas dos processos de descoberta do conhecimento
- 7.1.4. Técnicas utilizadas nos processos de descoberta do conhecimento
- 7.1.5. Caraterísticas dos bons modelos de aprendizagem automática
- 7.1.6. Tipos de informação sobre aprendizagem automática
- 7.1.7. Conceitos básicos de aprendizagem
- 7.1.8. Conceitos básicos de aprendizagem não supervisionado

7.2. Exploração e pré-processamento de dados
- 7.2.1. Tratamento de dados
- 7.2.2. Tratamento de dados no fluxo de análise de dados
- 7.2.3. Tipos de dados
- 7.2.4. Transformação de dados
- 7.2.5. Visualização e exploração de variáveis contínuas
- 7.2.6. Visualização e exploração de variáveis categóricas
- 7.2.7. Medidas de correlação
- 7.2.8. Representações gráficas mais comuns
- 7.2.9. Introdução à análise multivariada e à redução da dimensionalidade

7.3. Árvore de decisão
- 7.3.1. Algoritmo ID
- 7.3.2. Algoritmo C
- 7.3.3. Excesso de treino e poda
- 7.3.4. Análise de resultados

7.4. Avaliação dos classificadores
- 7.4.1. Matrizes de confusão
- 7.4.2. Matrizes de avaliação numérica
- 7.4.3. Estatística Kappa
- 7.4.4. A curva ROC

7.5. Regras de classificação
- 7.5.1. Medidas de avaliação das regras
- 7.5.2. Introdução à representação gráfica
- 7.5.3. Algoritmo de sobreposição sequencial

7.6. Redes neurais
- 7.6.1. Conceitos básicos
- 7.6.2. Redes neuronais simples
- 7.6.3. Algoritmo de *Backpropagation*
- 7.6.4. Introdução às redes neuronais recorrentes

7.7. Métodos bayesianos
- 7.7.1. Conceitos básicos de probabilidade
- 7.7.2. Teorema de Bayes
- 7.7.3. Naive Bayes
- 7.7.4. Introdução às redes bayesianas

7.8. Modelos de regressão e modelos de resposta contínua
- 7.8.1. Regressão linear simples
- 7.8.2. Regressão linear múltipla
- 7.8.3. Regressão logística
- 7.8.4. Árvores de regressão
- 7.8.5. Introdução às máquinas de suporte vetorial (SVM)
- 7.8.6. Medidas de adequação

7.9. *Clustering*
- 7.9.1. Conceitos básicos
- 7.9.2. *Clustering* hierárquico
- 7.9.3. Métodos probabilísticos
- 7.9.4. Algoritmo EM
- 7.9.5. Método *B-Cubed*
- 7.9.6. Métodos implícitos

7.10. Mineração de texto e processamento linguagem natural(PLN)
- 7.10.1. Conceitos básicos
- 7.10.2. Criação do corpus
- 7.10.3. Análise descritiva
- 7.10.4. Introdução à análise de sentimentos

Módulo 8. As redes neuronais, a base da *Deep Learning*

8.1. Aprendizagem Profunda
- 8.1.1. Tipos de aprendizagem profunda
- 8.1.2. Aplicações da aprendizagem profunda
- 8.1.3. Vantagens e desvantagens da aprendizagem profunda

8.2. Operações
- 8.2.1. Adição
- 8.2.2. Produto
- 8.2.3. Transferência

8.3. Camadas
- 8.3.1. Camada de entrada
- 8.3.2. Camada oculta
- 8.3.3. Camada de saída

8.4. Ligação de Camadas e Operações
- 8.4.1. Design de arquiteturas
- 8.4.2. Conexão entre camadas
- 8.4.3. Propagação para a frente

8.5. Construção da primeira rede neuronal
- 8.5.1. Design da rede
- 8.5.2. Estabelecer os pesos
- 8.5.3. Treino da rede

8.6. Treinador e Otimizador
- 8.6.1. Seleção do otimizador
- 8.6.2. Estabelecimento de uma função de perda
- 8.6.3. Estabelecimento de uma métrica

8.7. Aplicação dos Princípios das Redes Neuronais
- 8.7.1. Funções de ativação
- 8.7.2. Propagação para trás
- 8.7.3. Ajuste dos parâmetros

8.8. Dos neurónios biológicos aos neurónios artificiais
- 8.8.1. Funcionamento de um neurónio biológico
- 8.8.2. Transferência de conhecimentos para os neurónios artificiais
- 8.8.3. Estabelecer de relações entre os dois

8.9. Implementação do MLP (Perceptron Multicamadas) com o Keras
- 8.9.1. Definição da estrutura da rede
- 8.9.2. Compilação do modelo
- 8.9.3. Treino do modelo

8.10. Hiperparâmetros de *Fine tuning* de Redes Neuronais
- 8.10.1. Seleção da função de ativação
- 8.10.2. Estabelecer a *Learning* rate
- 8.10.3. Ajuste dos pesos

Módulo 9. Treino de redes neuronais profundas

9.1. Problemas de Gradientes
- 9.1.1. Técnicas de otimização de gradiente
- 9.1.2. Gradientes Estocásticos
- 9.1.3. Técnicas de inicialização de pesos

9.2. Reutilização de camadas pré-treinadas
- 9.2.1. Treino de transferência de aprendizagem
- 9.2.2. Extração de caraterísticas
- 9.2.3. Aprendizagem profunda

9.3. Otimizadores
- 9.3.1. Otimizadores estocásticos de gradiente descendente
- 9.3.2. Otimizadores Adam e *RMSprop*
- 9.3.3. Otimizadores de momento

9.4. Programação da taxa de aprendizagem
- 9.4.1. Controlo de taxa sobre aprendizagem automática
- 9.4.2. Ciclos de aprendizagem
- 9.4.3. Termos de suavização

9.5. Sobreajuste
- 9.5.1. Validação cruzada
- 9.5.2. Regularização
- 9.5.3. Métricas de avaliação

9.6. Orientações práticas
- 9.6.1. Design do modelo
- 9.6.2. Seleção de métricas e parâmetros de avaliação
- 9.6.3. Teste de hipóteses

9.7. *Transfer Learning*
- 9.7.1. Treino de transferência de aprendizagem
- 9.7.2. Extração de caraterísticas
- 9.7.3. Aprendizagem profunda

9.8. *Data Augmentation*
- 9.8.1. Transformações de imagem
- 9.8.2. Geração de dados sintéticos
- 9.8.3. Transformação de texto

9.9. Aplicação Prática de *Transfer Learning*
- 9.9.1. Treino de transferência de aprendizagem
- 9.9.2. Extração de caraterísticas
- 9.9.3. Aprendizagem profunda

9.10. Regularização
- 9.10.1. L e L
- 9.10.2. Regularização por entropia máxima
- 9.10.3. *Dropout*

Módulo 10. Personalização de Modelos e treino com *TensorFlow*

10.1. *TensorFlow*
- 10.1.1. Uso da biblioteca *TensorFlow*
- 10.1.2. Treino de modelos com o *TensorFlow*
- 10.1.3. Operações de gráfico no *TensorFlow*

10.2. *TensorFlow* e NumPy
- 10.2.1. Ambiente computacional NumPy para *TensorFlow*
- 10.2.2. Utilização das arrays NumPy com o *TensorFlow*
- 10.2.3. Operações NumPy para o TensorFlow gráficos do *TensorFlow*

10.3. Personalização de modelos e algoritmos de treino
- 10.3.1. Construir modelos personalizados com o *TensorFlow*
- 10.3.2. Gestão dos parâmetros de treino
- 10.3.3. Utilização de técnicas de otimização para o treino

10.4. Funções e gráficos do *TensorFlow*
- 10.4.1. Funções com o *TensorFlow*
- 10.4.2. Utilização de gráficos para treino de modelos
- 10.4.3. Otimização de gráficos com operações do *TensorFlow*

10.5. Carga de conjuntos de dados com o *TensorFlow*
- 10.5.1. Carga de conjuntos de dados com o *TensorFlow*
- 10.5.2. Pré-processamento de dados com o *TensorFlow*
- 10.5.3. Utilizar de ferramentas do *TensorFlow* para a manipulação de dados

10.6. A API *tfdata*
- 10.6.1. Utilização da API *tfdata* para o processamento de dados
- 10.6.2. Construção de fluxo de dados com *tfdata*
- 10.6.3. Utilização da API *tfdata* para o treino de modelos

10.7. O formato *TFRecord*
- 10.7.1. Utilização da API *TFRecord* para a serialização de dados
- 10.7.2. Carregar arquivos *TFRecord* com *TensorFlow*
- 10.7.3. Utilização de arquivos *TFRecord* para o treino de modelos

10.8. Camadas de pré-processamento do Keras
- 10.8.1. Utilização da API de pré-processamento do Keras
- 10.8.2. Construção de *pipelined* de pré-processamento com o Keras
- 10.8.3. Utilização da API de pré-processamento do Keras para o treino de modelos

10.9. O projeto *TensorFlow Datasets*
- 10.9.1. Utilização de *TensorFlow Datasets* para o carregamento de dados
- 10.9.2. Pré-processamento de dados com *TensorFlow Datasets*
- 10.9.3. Uso de *TensorFlow Datasets* para o treino de modelos

10.10. Construção de uma Aplicação de Deep *Learning* com *TensorFlow*
- 10.10.1. Aplicação Prática
- 10.10.2. Construção de uma aplicação de Deep *Learning* com *TensorFlow*
- 10.10.3. Treino de um modelo com o *TensorFlow*
- 10.10.4. Utilizar a aplicação para previsão de resultados

Módulo 11. *Deep Computer Vision* com Redes Neuronais Convolucionais

11.1. A Arquitetura *Visual Cortex*
- 11.1.1. Funções do córtex visual
- 11.1.2. Teoria da visão computacional
- 11.1.3. Modelos de processamento de imagens

11.2. Camadas convolucionais
- 11.2.1. Reutilização de pesos na convolução
- 11.2.2. Convolução D
- 11.2.3. Funções de ativação

11.3. Camadas de agrupamento e implementação de camadas de agrupamento
- 11.3.1. *Pooling* e *Striding*
- 11.3.2. *Flattening*
- 11.3.3. Tipos de *Pooling*

11.4. Arquitetura CNN
- 11.4.1. Arquitetura VGG
- 11.4.2. Arquitetura *AlexNet*
- 11.4.3. Arquitetura *ResNet*

11.5. Implementação de uma CNN ResNet- usando Keras
- 11.5.1. Inicialização de pesos
- 11.5.2. Definição da camada de entrada
- 11.5.3. Definição da saída

11.6. Utilização de modelos pré-treinados do Keras
- 11.6.1. Caraterísticas dos modelos pré-treinados
- 11.6.2. Usos dos modelos pré-treinados
- 11.6.3. Vantagens dos modelos pré-treinados

11.7. Modelos pré-treinados para a aprendizagem por transferência
- 11.7.1. A Aprendizagem por transferência
- 11.7.2. Processo de aprendizagem por transferência
- 11.7.3. Vantagens do aprendizagem por transferência

11.8. Classificação e Localização em *Deep Computer Vision*
- 11.8.1. Classificação de imagens
- 11.8.2. Localização de objetos em imagens
- 11.8.3. Detenção de objetos

11.9. Deteção e seguimento de objetos
- 11.9.1. Métodos de deteção de objetos
- 11.9.2. Algoritmos de seguimento de objetos
- 11.9.3. Técnicas de seguimento e localização

11.10. Segmentação semântica
- 11.10.1. Aprendizagem profunda para a segmentação semântica
- 11.10.1. Deteção de bordas
- 11.10.1. Métodos de segmentação baseado sem regras

Módulo 12. Processamento de linguagem natural (PLN) com Redes Neurais Recorrentes (RNN) e Atenção

12.1. Geração de texto utilizando RNN
- 12.1.1. Treino de uma RNN para geração de texto
- 12.1.2. Geração de linguagem natural com RNN
- 12.1.3. Aplicações de geração de texto com RNN

12.2. Criação de conjuntos de dados de treino
- 12.2.1. Preparação dos dados para o treino de uma RNN
- 12.2.2. Armazenamento do conjunto de dados de treino
- 12.2.3. Limpeza e transformação dos dados
- 12.2.4. Análise de Sentimento

12.3. Classificação da opiniões com RNN
- 12.3.1. Deteção de temas nos comentários
- 12.3.2. Análise de sentimento com algoritmos de aprendizagem profunda

12.4. Rede codificadora-descodificadora para a tradução automática neural
- 12.4.1. Treino de uma RNN para a tradução automática
- 12.4.2. Utilização de uma rede *encoder-decoder* para a tradução automática
- 12.4.3. Melhoria da precisão da tradução automática com RNNs

12.5. Mecanismos de atenção
- 12.5.1. Implementação de mecanismos de atenção em RNN
- 12.5.2. Utilização de mecanismos de atenção para melhorar a precisão dos modelos
- 12.5.3. Vantagens dos mecanismos de atenção nas redes neuronais

12.6. Modelos *Transformers*
- 12.6.1. Uso de modelos *Transformers* no processamento de linguagem natural
- 12.6.2. Aplicação de modelos *Transformers* na visão
- 12.6.3. Vantagens dos modelos *Transformers*

12.7. *Transformers* para a visão
- 12.7.1. Utilização de modelos *Transformers* para a visão
- 12.7.2. Pré-processamento de dados de imagem
- 12.7.3. Treino de modelos *Transformers* para visão

12.8. Biblioteca de *Transformers* de *Hugging Face*
- 12.8.1. Utilização da biblioteca *Transformers* de *Hugging Face*
- 12.8.2. Aplicação da biblioteca de *Transformers* de *Hugging Face*
- 12.8.3. Vantagens da biblioteca *Transformers* de *Hugging Face*

12.9. Outras Bibliotecas de *Transformers*. Comparação
- 12.9.1. Comparação entre as diferentes bibliotecas de *Transformers*
- 12.9.2. Uso das outras bibliotecas de *Transformers*
- 12.9.3. Vantagens das outras bibliotecas de *Transformers*

12.10. Desenvolvimento de uma aplicação de PLN com RNN e Atenção. Aplicação Prática
- 12.10.1. Desenvolvimento de uma aplicação de processamento de linguagem natural com RNN e atenção
- 12.10.2. Utilização de RNN, mecanismos de atenção e modelos *Transformers* na aplicação
- 12.10.3. Avaliação da aplicação prática

Módulo 13. *Autoencoders, GANs,* e modelos de difusão

13.1. Representação de dados eficientes
- 13.1.1. Redução da dimensionalidade
- 13.1.2. Aprendizagem profunda
- 13.1.3. Representações compatas

13.2. Realização da PCA com um codificador automático linear incompleto
- 13.2.1. Processo de treino
- 13.2.2. Implementação em Python
- 13.2.3. Utilização de dados de teste

13.3. Codificadores automáticos empilhados
- 13.3.1. Redes neuronais profundas
- 13.3.2. Construção de arquiteturas de codificação
- 13.3.3. Utilização da regularização

13.4. Autoencodificadores convolucionais
- 13.4.1. Design do modelo convolucionais
- 13.4.2. Treino do modelo convolucionais
- 13.4.3. Avaliação dos resultados

13.5. Redução do ruído dos codificadores automáticos
- 13.5.1. Aplicação de filtros
- 13.5.2. Design de modelos de codificação
- 13.5.3. Utilização de técnicas de regularização

13.6. Codificadores automáticos dispersos
- 13.6.1. Aumento da eficiência da codificação
- 13.6.2. Minimizar o número de parâmetros
- 13.6.3. Utilização de técnicas de regularização

13.7. Codificadores automáticos variacionais
- 13.7.1. Utilização da otimização variacional
- 13.7.2. Aprendizagem profunda não supervisionada
- 13.7.3. Representações latentes profundas

13.8. Geração de imagens MNIST de moda
- 13.8.1. Reconhecimento de padrões
- 13.8.2. Geração de imagens
- 13.8.3. Treino de redes neuronais profundas

13.9. Redes generativas antagónicas e modelos de difusão
- 13.9.1. Geração de conteúdos a partir de imagens
- 13.9.2. Modelação de distribuições de dados
- 13.9.3. Utilização de redes contraditórias

13.10. Implementação dos Modelos
- 13.10.1. Aplicação Prática
- 13.10.2. Implementação dos modelos
- 13.10.3. Utilização de dados reais
- 13.10.4. Avaliação dos resultados

Módulo 14. Computação bioinspirada

14.1. Introdução à computação bioinspirada
- 14.1.1. Introdução à computação bioinspirada

14.2. Algoritmos de inspiração social
- 14.2.1. Computação bioinspirada baseada em colónias de formigas
- 14.2.2. Variantes dos algoritmos de colónias de formigas
- 14.2.3. Computação baseada em nuvens de partículas

14.3. Algoritmos genéticos
- 14.3.1. Estrutura geral
- 14.3.2. Implementações dos principais operadores

14.4. Estratégias de exploração do espaço para algoritmos genéticos
- 14.4.1. Algoritmo CHC
- 14.4.2. Problemas multimodais

14.5. Modelos de computação evolutiva
- 14.5.1. Estratégias evolutivas
- 14.5.2. Programação evolutiva
- 14.5.3. Algoritmos baseados em evolução diferencial

14.6. Modelos de computação evolutiva (II)
- 14.6.1. Modelos de evolução baseados na estimativa das distribuições (EDA)
- 14.6.2. Programação genética

14.7. Programação evolutiva aplicada a problemas de aprendizagem
- 14.7.1. A aprendizagem baseada em regras
- 14.7.2. Métodos evolutivos em problemas de seleção de exemplos

14.8. Problemas multiobjetivo
- 14.8.1. Conceito de dominância
- 14.8.2. Aplicação de algoritmos evolutivos a problemas multiobjetivos

14.9. Redes neuronais (I)
- 14.9.1. Introdução às redes neuronais
- 14.9.2. Exemplo prático com redes neuronais

14.10. Redes neuronais (II)
- 14.10.1. Casos de utilização de redes neuronais na investigação médica
- 14.10.2. Casos de utilização de redes neuronais na economia
- 14.10.3. Casos de utilização de redes neuronais na visão artificial

Módulo 15. Inteligência Artificial: estratégias e aplicações

15.1. Serviços financeiros
- 15.1.1. As implicações da Inteligência Artificial nos serviços financeiros Oportunidades e desafios
- 15.1.2. Casos de utilização
- 15.1.3. Riscos potenciais relacionados com a utilização da Inteligência Artificial
- 15.1.4. Potenciais desenvolvimentos/utilizações futuras da Inteligência Artificial

15.2. Implicações da inteligência artificial no serviço de saúde
- 15.2.1. Implicações da Inteligência Artificial no setor da saúde. Oportunidades e desafios
- 15.2.2. Casos de utilização

15.3. Riscos relacionados com a utilização da inteligência artificial nos serviços de saúde
- 15.3.1. Riscos potenciais relacionados com a utilização da Inteligência Artificial
- 15.3.2. Potenciais desenvolvimentos/utilizações futuras da Inteligência Artificial

15.4. *Retail*
- 15.4.1. Implicações da Inteligência Artificial no *Retail* Oportunidades e desafios
- 15.4.2. Casos de utilização
- 15.4.3. Riscos potenciais relacionados com a utilização da Inteligência Artificial
- 15.4.4. Potenciais desenvolvimentos/utilizações futuras da Inteligência Artificial

15.5. Indústrias
- 15.5.1. Implicações da Inteligência Artificial na Indústria Oportunidades e desafios
- 15.5.2. Casos de utilização

15.6. Riscos potenciais relacionados com a utilização da Inteligência Artificial na indústria
- 15.6.1. Casos de utilização
- 15.6.2. Riscos potenciais relacionados com a utilização da Inteligência Artificial
- 15.6.3. Potenciais desenvolvimentos/utilizações futuras da Inteligência Artificial

15.7. Administração pública
- 15.7.1. Implicações da Inteligência Artificial na Administração pública Oportunidades e desafios
- 15.7.2. Casos de utilização
- 15.7.3. Riscos potenciais relacionados com a utilização da Inteligência Artificial
- 15.7.4. Potenciais desenvolvimentos/utilizações futuras da Inteligência Artificial

15.8. Educação
- 15.8.1. Implicações da Inteligência Artificial na educação. Oportunidades e desafios
- 15.8.2. Casos de utilização
- 15.8.3. Riscos potenciais relacionados com a utilização da Inteligência Artificial
- 15.8.4. Potenciais desenvolvimentos/utilizações futuras da Inteligência Artificial

15.9. Silvicultura e agricultura
- 15.9.1. Implicações da Inteligência Artificial para a silvicultura e a agricultura. Oportunidades e desafios
- 15.9.2. Casos de utilização
- 15.9.3. Riscos potenciais relacionados com a utilização da Inteligência Artificial
- 15.9.4. Potenciais desenvolvimentos/utilizações futuras da Inteligência Artificial

15.10. Recursos Humanos
- 15.10.1. Implicações da Inteligência Artificial nos Recursos Humanos Oportunidades e desafios
- 15.10.2. Casos de utilização
- 15.10.3. Riscos potenciais relacionados com a utilização da Inteligência Artificial
- 15.10.4. Potenciais desenvolvimentos/utilizações futuras da Inteligência Artificial

Módulo 16. Cibersegurança e análise de ameaças modernas com ChatGPT

16.1. Introdução à Cibersegurança: ameaças atuais e o papel da Inteligência Artificial
- 16.1.1. Definição e conceitos básicos de Cibersegurança
- 16.1.2. Tipos de ameaças cibernéticas modernas
- 16.1.3. Papel da Inteligência Artificial na evolução da Cibersegurança

16.2. Confidencialidade, integridade e disponibilidade (CIA) na era da Inteligência Artificial
- 16.2.1. Fundamentos do modelo CIA em Cibersegurança
- 16.2.2. Princípios de segurança aplicados no contexto da Inteligência Artificial
- 16.2.3. Desafios e considerações do CIA em sistemas impulsionados por Inteligência Artificial

16.3. Uso do ChatGPT para análise de riscos e cenários de ameaça
- 16.3.1. Fundamentos da análise de riscos em Cibersegurança
- 16.3.2. Capacidade do ChatGPT para identificar e avaliar cenários de ameaça
- 16.3.3. Benefícios e limitações da análise de riscos com Inteligência Artificial

16.4. ChatGPT na deteção de vulnerabilidades críticas
- 16.4.1. Princípios da deteção de vulnerabilidades em sistemas de informação
- 16.4.2. Funcionalidades do ChatGPT para apoiar na deteção de vulnerabilidades
- 16.4.3. Considerações éticas e de segurança ao usar Inteligência Artificial na deteção de falhas

16.5. Análisis de *malware* e *ransomware* assistida por Inteligência Artificial
- 16.5.1. Princípios básicos da análise de *malware* e *ransomware*
- 16.5.2. Técnicas de Inteligência Artificial aplicadas na identificação de código malicioso
- 16.5.3. Desafios técnicos e operacionais na análise de *malware* assistida por Inteligência Artificial

16.6. Identificação de ataques comuns com Inteligência Artificial: *phishing*,, engenharia social e exploração
- 16.6.1. Classificação de ataques: phishing, engenharia social e exploração
- 16.6.2. Técnicas de Inteligência Artificial para a identificação e análise de ataques comuns
- 16.6.3. Dificuldades e limitações dos modelos de Inteligência Artificial na deteção de ataques

16.7. ChatGPT na capacitação e simulação de ameaças cibernéticas
- 16.7.1. Fundamentos da simulação de ameaças para formação em Cibersegurança
- 16.7.2. Capacidades do ChatGPT para desenhar cenários de simulação
- 16.7.3. Benefícios da simulação de ameaças como ferramenta de capacitação

16.8. Políticas de segurança cibernética com recomendações de Inteligência Artificial
- 16.8.1. Princípios para a formulação de políticas de segurança cibernética
- 16.8.2. Papel da Inteligência Artificial na geração de recomendações de segurança
- 16.8.3. Componentes chave em políticas de segurança orientadas para Inteligência Artificial

16.9. Segurança em dispositivos IoT e o papel da Inteligência Artificial
- 16.9.1. Fundamentos da segurança na Internet das Coisas (IoT)
- 16.9.2. Capacidades da Inteligência Artificial para mitigar vulnerabilidades em dispositivos IoT
- 16.9.3. Desafios e considerações específicas de Inteligência Artificial para a segurança de IoT

16.10. Avaliação de ameaças e respostas assistidas por ferramentas de Inteligência Artificial
- 16.10.1. Princípios de avaliação de ameaças em Cibersegurança
- 16.10.2. Características das respostas automatizadas através de Inteligência Artificial
- 16.10.3. Fatores críticos na eficácia das respostas cibernéticas com Inteligência Artificial

Módulo 17. Deteção e prevenção de intrusões usando modelos de Inteligência Artificial Generativa

17.1. Fundamentos de sistemas IDS/IPS e o papel da Inteligência Artificial
- 17.1.1. Definição e princípios básicos dos sistemas IDS e IPS
- 17.1.2. Principais tipos e configurações de IDS/IPS
- 17.1.3. Contribuição da Inteligência Artificial na evolução dos sistemas de deteção e prevenção

17.2. Uso de Gemini para detecção de anomalias em redes
- 17.2.1. Conceitos e tipos de anomalias no tráfego de rede
- 17.2.2. Características de Gemini para a análise de dados de rede
- 17.2.3. Benefícios da deteção de anomalias na prevenção de intrusões

17.3. Gemini e a identificação de padrões de intrusão
- 17.3.1. Princípios de identificação e classificação de padrões de intrusão
- 17.3.2. Técnicas de Inteligência Artificial aplicadas na deteção de padrões de ameaças
- 17.3.3. Tipos de padrões e comportamentos anômalos em segurança de redes

17.4. Aplicação de modelos generativos na simulação de ataques
- 17.4.1. Fundamentos dos modelos generativos em Inteligência Artificial
- 17.4.2. Uso de modelos generativos para recriar cenários de ataque
- 17.4.3. Vantagens e limitações na simulação de ataques por meio de Inteligência Artificial generativa

17.5. *Clustering* e classificação de eventos usando Inteligência Artificial
- 17.5.1. Fundamentos do *clustering* e classificação na detecção de intrusões
- 17.5.2. Algoritmos comuns de *clustering* aplicados em Cibersegurança
- 17.5.3. Papel da Inteligência Artificial na melhoria dos métodos de classificação de eventos

17.6. Gemini na geração de perfis de comportamento
- 17.6.1. Conceitos de perfilamento de usuários e dispositivos
- 17.6.2. Aplicação de modelos generativos na criação de perfis
- 17.6.3. Vantagens dos perfis de comportamento na deteção de ameaças

17.7. Análise de *Big Data* para a prevenção de intrusões
- 17.7.1. Importância do *Big Data* na deteção de padrões de segurança
- 17.7.2. Métodos de processamento de grandes volumes de dados em Cibersegurança
- 17.7.3. Aplicações de Inteligência Artificial na análise e prevenção baseadas em *Big Data*

17.8. Redução de dados e seleção de características relevantes com Inteligência Artificial
- 17.8.1. Princípios de redução de dimensionalidade em grandes volumes de dados
- 17.8.2. Seleção de características para melhorar a eficiência da análise de Inteligência Artificial
- 17.8.3. Técnicas de redução de dados aplicadas em Cibersegurança

17.9. Avaliação de modelos de Inteligência Artificial na detecção de intrusos
- 17.9.1. Critérios de avaliação de modelos de Inteligência Artificial em Cibersegurança
- 17.9.2. Indicadores de desempenho e precisão dos modelos
- 17.9.3. Importância da validação e avaliação constante na Inteligência Artificial

17.10. Implementação de um sistema de detecção de intrusos potenciado com Inteligência Artificial generativa
- 17.10.1. Conceitos básicos de implementação de sistemas de detecção de intrusos
- 17.10.2. Integração de Inteligência Artificial generativa nos sistemas IDS/IPS
- 17.10.3. Aspetos chave para a configuração e manutenção de sistemas baseados em Inteligência Artificial

Módulo 18. Criptografia moderna com assistência do ChatGPT na proteção de dados

18.1. Princípios básicos de criptografia com aplicações de Inteligência Artificial
- 18.1.1. Conceitos fundamentais de criptografia: confidencialidade e autenticidade
- 18.1.2. Principais algoritmos criptográficos e sua relevância atual
- 18.1.3. Papel da Inteligência Artificial na modernização da criptografia

18.2. ChatGPT no ensino e prática de criptografia simétrica e assimétrica
- 18.2.1. Introdução à criptografia simétrica e assimétrica
- 18.2.2. Comparação entre cifra simétrica e assimétrica
- 18.2.3. Uso do ChatGPT no aprendizado de métodos criptográficos

18.3. Criptografia avançada (AES, RSA) e recomendações geradas por Inteligência Artificial
- 18.3.1. Fundamentos dos algoritmos AES e RSA na criptografia de dados
- 18.3.2. Forças e fraquezas desses algoritmos no contexto atual
- 18.3.3. Geração de recomendações de segurança em criptografia avançada com Inteligência Artificial

18.4. Inteligência Artificial na gestão e autenticação de chaves
- 18.4.1. Princípios de gestão de chaves criptográficas
- 18.4.2. Importância da autenticação segura de chaves
- 18.4.3. Aplicação da Inteligência Artificial para otimizar processos de gestão e autenticação

18.5. Algoritmos de *hashing* e ChatGPT na avaliação de integridade
- 18.5.1. Conceitos básicos e aplicações dos algoritmos de *hashing*
- 18.5.2. Funções de hash na verificação de integridade de dados
- 18.5.3. Análise e verificação da integridade de dados com a ajuda do ChatGPT

18.6. ChatGPT na deteção de padrões de cifragem anómalos
- 18.6.1. Introdução à deteção de padrões anómalos em criptografia
- 18.6.2. Capacidade do ChatGPT para identificar irregularidades em dados cifrados
- 18.6.3. Limitações dos modelos de linguagem na deteção de cifragem anómala

18.7. Introdução à criptografia pós-quântica com simulações de Inteligência Artificial
- 18.7.1. Fundamentos da criptografia pós-quântica e sua importância
- 18.7.2. Principais algoritmos pós-quânticos em investigação
- 18.7.3. Uso da Inteligência Artificial em simulações para o estudo da criptografia pós-quântica

18.8. *Blockchain* e ChatGPT na verificação de transações seguras
- 18.8.1. Conceitos básicos de *blockchain* e sua estrutura de segurança
- 18.8.2. Papel da criptografia na integridade do *blockchain*
- 18.8.3. Aplicação do ChatGPT para explicar e analisar transações seguras

18.9. Proteção de privacidade e aprendizado federado
- 18.9.1. Definição e princípios do aprendizado federado
- 18.9.2. Importância da privacidade no aprendizado descentralizado
- 18.9.3. Benefícios e desafios do aprendizado federado para a segurança dos dados

18.10. Desenvolvimento de um sistema de criptografia baseado em Inteligência Artificial generativa
- 18.10.1. Princípios básicos na criação de sistemas de criptografia
- 18.10.2. Vantagens da Inteligência Artificial generativa no design de sistemas de cifragem
- 18.10.3. Componentes e requisitos de um sistema de criptografia assistido por Inteligência Artificial

Módulo 19. Análise forense digital e resposta a incidentes assistida pela Inteligência Artificial

19.1. Processos forenses com ChatGPT para a identificação de evidências
- 19.1.1. Conceitos básicos de análise forense em ambientes digitais
- 19.1.2. Etapas de identificação e recolha de evidências
- 19.1.3. Papel do ChatGPT no apoio à identificação forense

19.2. Gemini e ChatGPT na identificação e extração de dados
- 19.2.1. Fundamentos da extração de dados para análise forense
- 19.2.2. Técnicas de identificação de dados relevantes
- 19.2.3. Contribuição da Inteligência Artificial na automação do processo de extração

19.3. Análise de *logs* e correlação de eventos com Inteligência Artificial
- 19.3.1. Importância dos *logs* na análise de incidentes
- 19.3.2. Técnicas de correlação de eventos para reconstruir incidentes
- 19.3.3. Uso de Inteligência Artificial para identificar padrões na correlação de logs

19.4. Recuperação de dados e restauração de sistemas utilizando Inteligência Artificial
- 19.4.1. Princípios da recuperação de dados e sua importância na forense digital
- 19.4.2. Técnicas de restauração de sistemas comprometidos
- 19.4.3. Aplicação da Inteligência Artificial para melhorar os processos de recuperação e restauração

19.5. *Machine Learning* para deteção e reconstrução de incidentes
- 19.5.1. Introdução ao *Machine Learning* na deteção de incidentes
- 19.5.2. Técnicas de reconstrução de incidentes com modelos de Inteligência Artificial
- 19.5.3. Considerações éticas e práticas na deteção de eventos

19.6. Reconstrução de incidentes e simulação com ChatGPT
- 19.6.1. Fundamentos da reconstrução de incidentes em análise forense
- 19.6.2. Capacidade do ChatGPT para criar simulações de incidentes
- 19.6.3. Limitações e desafios na simulação de incidentes complexos

19.7. Deteção de atividades maliciosas em dispositivos móveis
- 19.7.1. Características e desafios na análise forense de dispositivos móveis
- 19.7.2. Principais atividades maliciosas em ambientes móveis
- 19.7.3. Aplicação da Inteligência Artificial para identificar ameaças em dispositivos móveis

19.8. Resposta automatizada a incidentes com fluxos de trabalho de Inteligência Artificial
- 19.8.1. Princípios de resposta a incidentes em cibersegurança
- 19.8.2. Importância da automação na resposta rápida a incidentes
- 19.8.3. Benefícios dos fluxos de trabalho assistidos por Inteligência Artificial na mitigação

19.9. Ética e transparência na análise forense com Inteligência Artificial generativa
- 19.9.1. Princípios éticos no uso de Inteligência Artificial em análise forense
- 19.9.2. Transparência e explicabilidade de modelos generativos em forense
- 19.9.3. Considerações sobre privacidade e responsabilidade na análise

19.10. Laboratório de análise forense e recriação de incidentes com ChatGPT e Gemini
- 19.10.1. Estrutura e objetivos de um laboratório de análise forense
- 19.10.2. Benefícios de ambientes controlados para a prática forense
- 19.10.3. Componentes chave para a criação de um laboratório de simulação

Módulo 20. Modelos preditivos de defesa proativa em Cibersegurança usando ChatGPT

20.1. Análise preditiva em Cibersegurança: técnicas e aplicações com Inteligência Artificial
- 20.1.1. Conceitos básicos de análise preditiva em segurança
- 20.1.2. Técnicas de predição no âmbito da Cibersegurança
- 20.1.3. Aplicação da Inteligência Artificial na antecipação de ciberameaças

20.2. Modelos de regressão e classificação com suporte de ChatGPT
- 20.2.1. Princípios de regressão e classificação na predição de ameaças
- 20.2.2. Tipos de modelos de classificação em Cibersegurança
- 20.2.3. Assistência do ChatGPT na interpretação de modelos preditivos

20.3. Identificação de ameaças emergentes com predições de ChatGPT
- 20.3.1. Conceitos de deteção de ameaças emergentes
- 20.3.2. Técnicas de identificação de novos padrões de ataque
- 20.3.3. Limitações e precauções na predição de novas ameaças

20.4. Redes neuronais para antecipação de ataques cibernéticos
- 20.4.1. Fundamentos de redes neuronais aplicadas em Cibersegurança
- 20.4.2. Arquiteturas comuns para deteção e predição de ataques
- 20.4.3. Desafios na implementação de redes neuronais em defesa cibernética

20.5. Uso de ChatGPT para simulações de cenários de ameaça
- 20.5.1. Conceitos básicos de simulação de ameaças em Cibersegurança
- 20.5.2. Capacidades do ChatGPT para desenvolver simulações preditivas
- 20.5.3. Fatores a considerar no design de cenários simulados

20.6. Algoritmos de aprendizagem por reforço para otimização de defesas
- 20.6.1. Introdução à aprendizagem por reforço em Cibersegurança
- 20.6.2. Algoritmos de reforço aplicados a estratégias de defesa
- 20.6.3. Benefícios e desafios da aprendizagem por reforço em ambientes de Cibersegurança

20.7. Simulação de ameaças e respostas com ChatGPT
- 20.7.1. Princípios de simulação de ameaças e sua relevância em ciberdefesa
- 20.7.2. Respostas automatizadas e otimizadas perante ataques simulados
- 20.7.3. Benefícios da simulação para melhorar a preparação cibernética

20.8. Avaliação de precisão e efetividade em modelos preditivos de Inteligência Artificial
- 20.8.1. Indicadores chave para a avaliação de modelos preditivos
- 20.8.2. Metodologias de avaliação de precisão em modelos de Cibersegurança
- 20.8.3. Fatores críticos na efetividade dos modelos de Inteligência Artificial em Cibersegurança

20.9. Inteligência Artificial na gestão de incidentes e respostas automatizadas
- 20.9.1. Fundamentos da gestão de incidentes em Cibersegurança
- 20.9.2. Papel da Inteligência Artificial na tomada de decisões em tempo real
- 20.9.3. Desafios e oportunidades na automatização de respostas

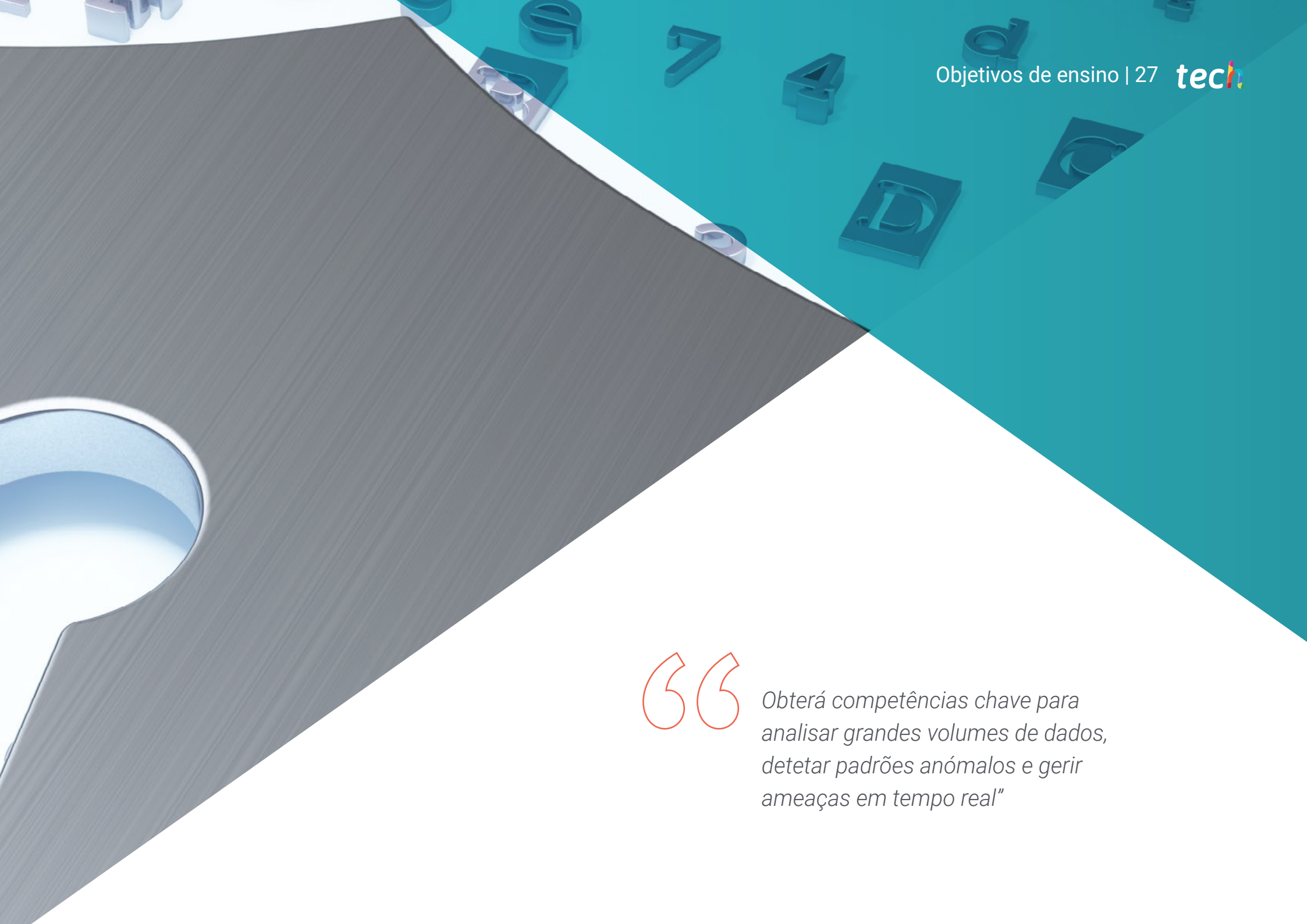
20.10. Criação de um sistema de defesa preditivo com suporte de ChatGPT
- 20.10.1. Princípios de design de sistemas de defesa proativa
- 20.10.2. Integração de modelos preditivos em ambientes de Cibersegurança
- 20.10.3. Componentes chave para um sistema de defesa preditivo baseado em Inteligência Artificial

Ahondará na integração do ChatGPT na análise de riscos e na resposta automatizada a incidentes, para gerir ambientes digitais de alta complexidade com precisão"

03

Objetivos de ensino

Este programa da TECH tem como objetivo principal dotar o profissional das competências necessárias para liderar projetos de Cibersegurança apoiados em Inteligência Artificial. Graças a este percurso académico, os informáticos poderão desenhar modelos preditivos, implementar algoritmos avançados e desenvolver estratégias eficazes para a proteção tanto de sistemas como de dados. Além disso, adquirirão competências para a deteção proativa de ameaças, a análise forense digital e a otimização de recursos tecnológicos em ambientes de alta complexidade.



Obterá competências chave para analisar grandes volumes de dados, detetar padrões anómalos e gerir ameaças em tempo real”

Objetivos gerais

- Dominar os princípios fundamentais da Inteligência Artificial e sua aplicação em Cibersegurança
- Analisar o ciclo de vida dos dados e seu impacto na implementação de sistemas inteligentes
- Desenhar modelos avançados de aprendizagem automática para a deteção e mitigação de ameaças
- Implementar redes neuronais profundas e sistemas de aprendizagem profunda em projetos de Cibersegurança
- Aplicar técnicas de mineração de dados e processamento de linguagem natural na análise de riscos
- Desenvolver estratégias baseadas em Inteligência Artificial para a proteção proativa de infraestruturas críticas
- Integrar sistemas inteligentes bioinspirados para a resolução de problemas complexos em ambientes digitais
- Otimizar algoritmos e ferramentas como TensorFlow para personalizar soluções de segurança
- Implementar métodos de análise forense digital assistidos por Inteligência Artificial
- Desenhar soluções inovadoras em criptografia moderna para garantir a integridade dos dados
- Avaliar a eficácia dos modelos preditivos e generativos aplicados à defesa cibernética
- Fomentar a inovação no desenvolvimento de ferramentas baseadas em Inteligência Artificial para abordar as ameaças emergentes

Objetivos específicos

Módulo 1. Fundamentos da Inteligência Artificial

- Analisar a evolução histórica da Inteligência Artificial, desde o seu início até ao seu estado atual, identificando os principais marcos e desenvolvimentos
- Compreender o funcionamento das redes neuronais e a sua aplicação em modelos de aprendizagem em Inteligência Artificial
- Estudar os princípios e aplicações dos algoritmos genéticos, analisando a sua utilidade na resolução de problemas complexos
- Analisar a importância dos thesauri, vocabulários e taxonomias na estruturação e processamento de dados para sistemas de Inteligência Artificial

Módulo 2. Tipos e ciclo de vida do dado

- Identificar e classificar os diferentes tipos de dados estatísticos, desde os quantitativos aos qualitativos
- Analisar o ciclo de vida dos dados, desde a sua geração até à sua eliminação, identificando as principais etapas
- Explorar as fases iniciais do ciclo de vida dos dados, destacando a importância do planeamento e da estrutura dos dados
- Estudar os processos de recolha de dados, incluindo a metodologia, as ferramentas e os canais de recolha
- Explorar o conceito de *Datawarehouse* (Armazém de Dados), com ênfase nos elementos que o inytegram e na sua conceção
- Analisar os aspetos regulamentares relacionados com a gestão de dados, cumprindo as normas de privacidade e segurança, bem como as boas práticas

Módulo 3. O dado na Inteligência Artificial

- Dominar os fundamentos da ciência dos dados, abrangendo ferramentas, tipos e fontes de análise de informações
- Explorar o processo de transformação de dados em informação utilizando técnicas de mineração e visualização de dados
- Estudar a estrutura e caraterísticas dos *datasets*, compreendendo a sua importância na preparação e utilização de dados para modelos de Inteligência Artificial
- Utilizar ferramentas específicas e boas práticas no tratamento e processamento de dados, garantindo eficiência e qualidade na implementação de Inteligência Artificial

Módulo 4. Mineria de dados. Seleção, pré-processamento e transformação

- Dominar técnicas de inferência estatística para compreender e aplicar métodos estatísticos na mineração de dados
- Realizar análises exploratórias pormenorizadas de conjuntos de dados para identificar padrões, anomalias e tendências relevantes
- Desenvolver competências para a preparação de dados, incluindo a sua limpeza, integração e formatação para utilização na mineração de dados
- Implementar estratégias eficazes para tratar valores em falta em conjuntos de dados, aplicando métodos de imputação ou eliminação sensíveis ao contexto
- Identificar e atenuar o ruído nos dados, utilizando técnicas de filtragem e suavização para melhorar a qualidade do conjunto de dados
- Abordar o preprocesamento de dados em ambientes *Big Data*

Módulo 5. Algoritmo e complexidade na Inteligência Artificial

- Introduzir estratégias de conceção de algoritmos, proporcionando uma compreensão sólida das abordagens fundamentais para a resolução de problemas
- Estudar e aplicar algoritmos de ordenação, compreendendo o seu desempenho e comparando a sua eficiência em diferentes contextos
- Investigar algoritmos com *Heaps*, analisando a sua implementação e utilidade na manipulação eficiente de dados
- Analisar algoritmos baseados em grafos, explorando a sua aplicação na representação e resolução de problemas que envolvam relações complexas
- Estudar algoritmos *Greedy,* compreendendo a sua lógica e aplicações na resolução de problemas de otimização
- Investigar e aplicar a técnica de *backtracking* na resolução sistemática de problemas, analisando a sua eficácia numa variedade de cenários

Módulo 6. Sistemas inteligentes

- Explorar a teoria dos agentes, compreendendo os conceitos fundamentais do seu funcionamento e da sua aplicação em Inteligência Artificial e engenharia de *Software*
- Analisar o conceito de web semântica e o seu impacto na organização e recuperação de informação em ambientes digitais
- Avaliar e comparar diferentes representações do conhecimento, integrando-as para melhorar a eficiência e a precisão dos sistemas inteligentes
- Estudar raciocinadores semânticos, sistemas baseados no conhecimento e sistemas periciais, compreendendo a sua funcionalidade e aplicações na tomada de decisões inteligentes

Módulo 7. Aprendizagem automática e mineração de dados

- Introduzir processos de descoberta de conhecimentos e os conceitos fundamentais da aprendizagem automática
- Avaliar classificadores utilizando técnicas específicas para medir o seu desempenho e exatidão na classificação de dados
- Estudar as redes neuronais, compreendendo o seu funcionamento e arquitetura para resolver problemas complexos de aprendizagem automática
- Explorar os métodos bayesianos e a sua aplicação na aprendizagem automática, incluindo redes e classificadores bayesianos
- Analisar modelos de regressão e de resposta contínua para prever valores numéricos a partir de dados
- Explorar a extração de texto e o processamento de linguagem natural (PLN), compreendendo como as técnicas de aprendizagem automática são aplicadas para analisar e compreender texto

Módulo 8. As redes neuronais, a base da *Deep Learning*

- Dominar os fundamentos da Aprendizagem Profunda, compreendendo o seu papel essencial na *Deep Learning*
- Explorar as operações fundamentais nas redes neuronais e compreender a sua aplicação na construção de modelos
- Analisar as diferentes camadas utilizadas nas redes neuronais e aprender a selecioná-las adequadamente
- Compreender a ligação eficaz de camadas e operações para conceber arquiteturas de redes neuronais complexas e eficientes
- Explorar a ligação entre neurónios biológicos e artificiais para uma compreensão mais profunda da conceção de modelos
- Afinar hiperparâmetros para o *Fine Tuning* de redes neuronais, melhorando o seu desempenho em tarefas específicas

Módulo 9. Treino de redes neuronais profundas

- Resolver problemas relacionados com gradientes na formação de redes neuronais profundas
- Aplicar diretrizes práticas para garantir o treino eficiente e eficaz de redes neuronais profundas
- Implementar *Transfer Learning* como uma técnica avançada para melhorar o desempenho do modelo em tarefas específicas
- Explorar e aplicar técnicas de *Data Augmentation* para enriquecer conjuntos de dados e melhorar a generalização do modelo
- Desenvolver aplicações práticas utilizando a *Transfer Learning* para resolver problemas do mundo real
- Compreender e aplicar técnicas de regularização para melhorar a generalização e evitar o sobreajuste em redes neuronais profundas

Módulo 10. Personalização de modelos e treino com *TensorFlow*

- Dominar os fundamentos do *TensorFlow* e a sua integração com o NumPy para um tratamento e computação eficientes dos dados
- Personalizar modelos e algoritmos de treino utilizando as capacidades avançadas do *TensorFlow*
- Implementar o formato TFRecord para armazenar e aceder a grandes conjuntos de dados *TensorFlow*
- Utilizar camadas de pré-processamento do Keras para facilitar a construção de modelos personalizados
- Explore o projeto *TensorFlow Datasets* para acessar conjuntos de dados predefinidos e melhorar a eficiência do desenvolvimento
- Desenvolver uma aplicação de *Deep Learning* com *TensorFlow*, integrando os conhecimentos adquiridos no módulo

Módulo 11. *Deep Computer Vision* com Redes Neuronais Convolucionais

- Compreender a arquitetura do córtex visual e a sua relevância para a *Deep Computer Vision*
- Explorar e aplicar camadas convolucionais para extrair caraterísticas-chave de imagens
- Implementar camadas de agrupamento e sua utilização em modelos de *Deep Computer Vision* com o Keras
- Analisar várias arquiteturas de Redes Neurais Convolucionais (CNN) e a sua aplicabilidade em diferentes contextos
- Desenvolver e implementar uma CNN ResNet utilizando a biblioteca Keras para melhorar a eficiência e o desempenho do modelo
- Utilizar modelos Keras pré-treinados para tirar partido da aprendizagem por transferência para tarefas específicas
- Abordar estratégias de deteção e seguimento de objetos utilizando Redes Neuronais Convolucionais.
- Implementar técnicas de segmentação semântica para compreender e classificar objetos em imagens de forma detalhada

Módulo 12. Processamento de linguagem natural (PLN) com Redes Neurais Recorrentes (RNN) e Atenção

- Desenvolver competências na geração de textos utilizando Redes Neuronais Recorrentes (RNN)
- Aplicar RNN na classificação de opiniões para análise de sentimentos em textos
- Compreender e aplicar mecanismos de atenção em modelos de processamento de linguagem natural
- Analisar e utilizar modelos *Transformers* em tarefas específicas de PNL
- Aprofundar na a aplicação de modelos *Transformers* no contexto do processamento de imagens e da visão computacional
- Familiarizar-se com a biblioteca *Transformers* de *Hugging Face* para a implementação eficiente de modelos avançados.
- Comparar diferentes bibliotecas de *Transformers* para avaliar a sua aptidão em tarefas específicass
- Desenvolver uma aplicação prática de PLN que integre RNN e mecanismos de atenção para resolver problemas do mundo real

Módulo 13. *Autoencoders, GANs,* e modelos de difusão

- Desenvolver representações de dados eficientes utilizando *Autoencoders, GANs* e Modelos de Difusão
- Realizar PCA utilizando um codificador automático linear incompleto para otimizar a representação dos dados
- Aprofundar e aplicar autoencodificadores convolucionais para representações visuais eficientes de dados
- Gerar imagens de moda a partir do conjunto de dados MNIST utilizando Autoencoders
- Compreender o conceito de Redes Generativas Antagónicas (*GANs*) e Modelos de Difusão
- Implementar e comparar o desempenho de modelos de difusão e *GANs* na geração de dados

Módulo 14. Computação bioinspirada

- Introduzir os conceitos fundamentais da computação bioinspirada
- Analisar os algoritmos de adaptação social como uma abordagem-chave para a computação bio-inspirada
- Examinar modelos de computação evolutiva no contexto da otimização
- Abordar a complexidade de problemas multi-objetivo no âmbito da computação bioinspirada
- Explorar a aplicação de redes neuronais no domínio da computação bioinspirada
- Aprofundar a implementação e a utilidade das redes neuronais na computação bioinspirada

Módulo 15. Inteligência Artificial Estratégias e aplicações

- Desenvolver estratégias para a implementação da Inteligência Artificial nos serviços financeiros
- Analisar as implicações da inteligência artificial na prestação de serviços de saúde
- Identificar e avaliar os riscos associados à utilização da inteligência Inteligência Artificial no setor da saúde
- Avaliar os riscos potenciais vinculados ao uso de Inteligência Artificial na indústria
- Aplicar técnicas de inteligência artificial na indústria para melhorar a produtividade
- Conceber soluções de inteligência artificial para otimizar os processos na administração pública
- Avaliar a implementação de tecnologias de Inteligência Artificial no setor educativo
- Aplicar técnicas de Inteligência Artificial na silvicultura e agricultura para melhorar a produtividade

Módulo 16. 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 17. Deteção e prevenção de intrusões usando modelos de Inteligência Artificial Generativa

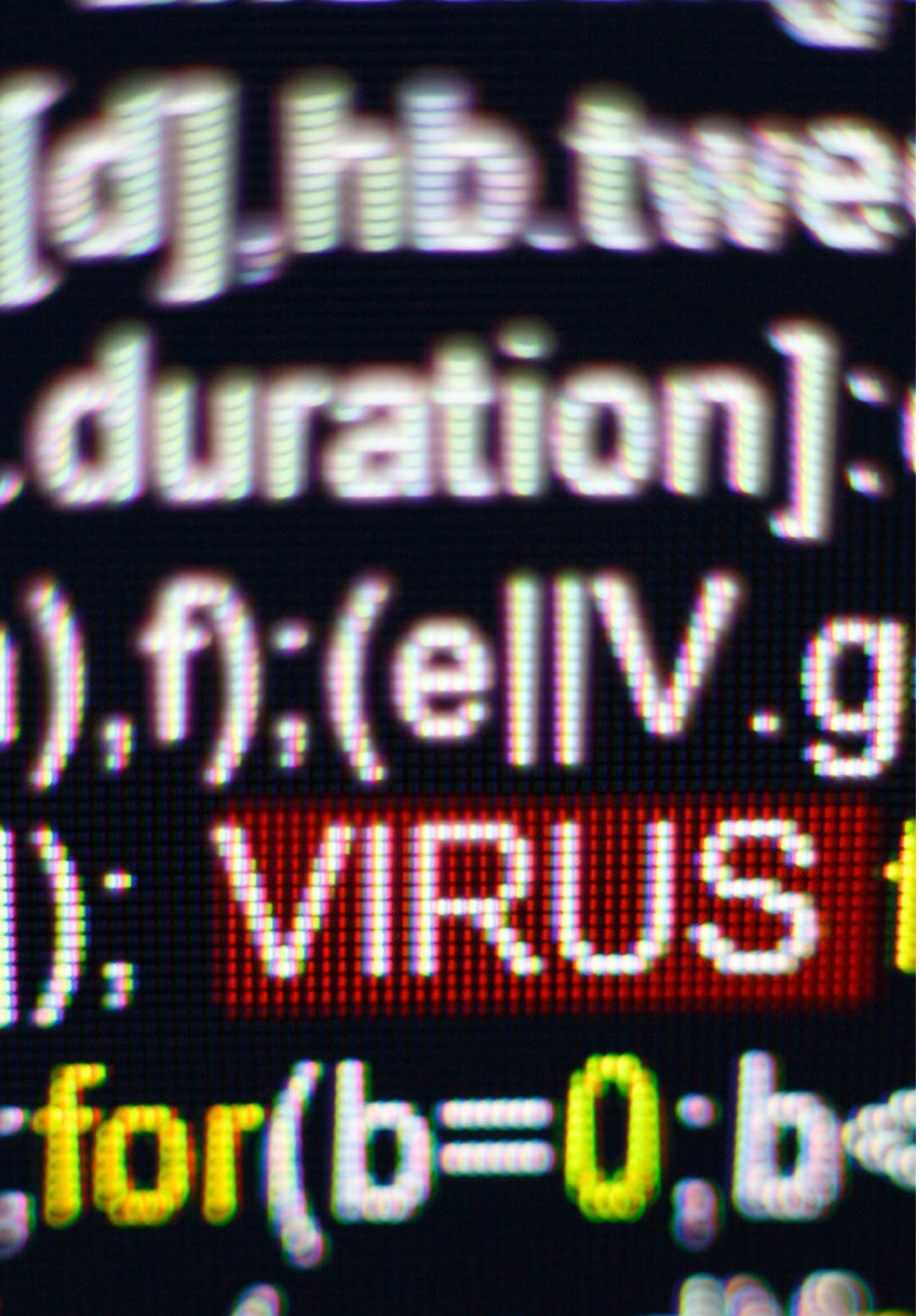
- Dominar as técnicas de deteção de anomalias e padrões de intrusão com ferramentas como Gemini
- Aplicar modelos generativos para simular ataques cibernéticos e melhorar a prevenção de intrusões
- Implementar sistemas IDS/IPS avançados otimizados com Inteligência Artificial, desenvolvendo perfis de 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 18. Criptografia moderna com assistência de ChatGPT na proteção de dados

- Dominar os fundamentos da criptografia avançada, incluindo algoritmos como AES, RSA e pós-quânticos
- Utilizar o ChatGPT para ensinar, praticar e otimizar métodos criptográficos
- Desenhar e gerir sistemas de encriptação assistidos por Inteligência Artificial, garantindo a privacidade e a autenticidade dos dados
- Avaliar a resistência de algoritmos criptográficos frente a cenários de ataques simulados com Inteligência Artificial generativa
- Desenvolver estratégias de cifrado e decifrado otimizadas para proteger infraestruturas críticas e dados sensíveis
- Implementar soluções de criptografia pós-quântica para mitigar riscos futuros em sistemas baseados em Inteligência Artificial

Módulo 19. Análise forense digital e resposta a incidentes assistida pela Inteligência Artificial

- Aprender a identificar, extrair e analisar evidências digitais com o apoio de ferramentas de Inteligência Artificial
- Utilizar Inteligência Artificial para automatizar a recuperação de dados e reconstrução de incidentes de segurança
- Desenhar e praticar fluxos de trabalho de resposta automatizada, assegurando rapidez e eficácia na mitigação de incidentes



- Integrar ferramentas de análise forense avançadas para a investigação de ciberataques complexos
- Desenvolver técnicas de reconstrução de eventos baseadas em Inteligência Artificial para auditorias pós-incidente
- Criar protocolos automatizados de resposta a incidentes, priorizando a continuidade operacional e a mitigação de danos

Módulo 20. 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

04

Oportunidades de carreira

Com as competências e conhecimentos adquiridos através desta qualificação universitária, os informáticos poderão aceder a um amplo leque de oportunidades laborais em setores chave como a Segurança Informática, a Análise de Riscos e a Gestão de Infraestruturas Críticas. Desta forma, estarão habilitados para desempenhar papéis estratégicos na deteção de ameaças, no design de modelos preditivos e na proteção avançada de dados, posicionando-os como referências em um campo altamente demandado.

O seu perfil profissional permitirá-lhe desempenhar-se como Consultor de Cibersegurança, assessorando organizações sobre a integração de soluções tecnológicas avançadas"

Perfil dos nossos alunos

O estudante deste programa será um profissional especializado na integração de Inteligência Artificial e Cibersegurança para desenhar soluções inovadoras face a ameaças digitais. Possuirá um conhecimento profundo de ferramentas avançadas, modelos preditivos e criptografia moderna, destacando-se pela sua capacidade de implementar estratégias eficazes na proteção de dados e sistemas críticos. Este perfil combina excelência técnica e visão prática, assegurando a sua contribuição na transformação do ambiente digital.

Ampliará os seus horizontes profissionais com um enfoque especializado, dominando métodos sofisticados como a Mineração de Dados, o Deep Learning e a Análise Forense Digital.

- **Pensamento crítico e resolução de problemas:** Capacidade para analisar situações complexas de várias perspetivas para identificar padrões em ameaças digitais e desenhar soluções inovadoras através da utilização de Inteligência Artificial que abordem desafios tecnológicos de forma precisa e adaptativa.
- **Tomada de decisões baseada em dados:** Habilidade para interpretar grandes volumes de dados e aplicar modelos preditivos que fundamentem estratégias em tempo real, assegurando ações orientadas para mitigar riscos de forma eficiente.
- **Adaptabilidade tecnológica:** Competência para integrar rapidamente novas ferramentas, tecnologias e metodologias de Inteligência Artificial na prática profissional, respondendo de forma ágil às mudanças no panorama digital e às novas formas de ataque cibernético.
- **Gestão ética e responsável:** Compreensão profunda dos aspetos legais e éticos relacionados com a proteção de dados e o uso de Inteligência Artificial, atuando de forma ética e alinhada com as regulamentações internacionais para garantir o uso responsável das tecnologias em Cibersegurança.

Após a realização do Mestrado Próprio, poderá aplicar os seus conhecimentos e habilidades nos seguintes cargos:

1. **Analista de Segurança Cibernética com Inteligência Artificial:** Responsável por identificar, prevenir e mitigar ameaças digitais utilizando modelos avançados de Inteligência Artificial para a proteção de sistemas críticos.
2. **Analista Forense Digital com Inteligência Artificial:** Responsável por identificar, extrair e analisar provas digitais utilizando tecnologias avançadas de Inteligência Artificial.
3. **Consultor em Defesa Digital Proativa:** Consultor especializado no desenvolvimento de estratégias de segurança baseadas em Inteligência Artificial para antecipar ameaças emergentes em ambientes empresariais.
4. **Especialista em Análise Forense Digital com Inteligência Artificial:** Responsável por investigar e reconstruir incidentes de cibersegurança utilizando ferramentas de Inteligência Artificial para extrair e analisar provas digitais.
5. **Designer de Modelos Preditivos de Cibersegurança:** Focado no desenvolvimento e implementação de sistemas baseados em aprendizagem automática e redes neuronais para antecipar vulnerabilidades.
6. **Coordenador de Segurança em Infraestruturas Críticas:** Responsável por supervisionar a implementação de soluções de cibersegurança baseadas em Inteligência Artificial em setores estratégicos, como energia, transporte ou finanças.
7. **Gestor de Riscos Cibernéticos com Inteligência Artificial:** Responsável por liderar o planeamento e execução de estratégias para identificar e minimizar riscos cibernéticos utilizando Inteligência Artificial.
8. **Responsável por Criptografia Pós-Quântica:** especialista em desenhar sistemas de criptografia robustos baseados em algoritmos resistentes a computadores quânticos, assegurando a proteção de dados a longo prazo.
9. **Administrador de Sistemas de Deteção de Intrusões com Inteligência Artificial Generativa:** Responsável por configurar e otimizar ferramentas de segurança automatizadas que utilizam Inteligência Artificial generativa para detectar e responder a ameaças.
10. **Auditor de Segurança Digital Assistido por Inteligência Artificial:** Responsável por avaliar e certificar sistemas de segurança digital utilizando ferramentas avançadas de análise assistida por Inteligência Artificial.

05

Metodologia do estudo

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

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

A TECH prepara-o para enfrentar novos desafios em ambientes incertos e alcançar o sucesso na 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 tendo em conta as exigências de tempo, disponibilidade e rigor académico que, atualmente, os estudantes de hoje, bem como os empregos mais competitivos do mercado.

Com o modelo educativo assíncrono da TECH, é o aluno que escolhe quanto tempo passa a estudar, como decide estabelecer as suas rotinas e tudo isto a partir do conforto do dispositivo eletrónico da sua escolha. O estudante não tem de assistir às aulas presenciais, que muitas vezes não pode frequentar. As atividades de aprendizagem serão realizadas de acordo com a sua conveniência. Poderá sempre decidir quando e de onde estudar.

Na TECH NÃO terá aulas ao vivo (às quais nunca poderá assistir)"

Os programas de estudo mais completos a nível internacional

A TECH caracteriza-se por oferecer os programas académicos mais completos no meio universitário. Esta abrangência é conseguida através da criação de programas de estudo que cobrem não só os conhecimentos essenciais, mas também as últimas inovações em cada área.

Ao serem constantemente atualizados, estes programas permitem que os estudantes acompanhem as mudanças do mercado e adquiram as competências mais valorizadas pelos empregadores. Deste modo, os programas da TECH recebem uma preparação completa que lhes confere uma vantagem competitiva significativa para progredirem nas suas carreiras.

E, além disso, podem fazê-lo a partir de qualquer dispositivo, PC, tablet ou smartphone.

> *O modelo da TECH é assíncrono, pelo que pode estudar com o seu PC, tablet ou smartphone onde quiser, quando quiser, durante o tempo que quiser"*

Case studies ou Método do caso

O método do caso tem sido o sistema de aprendizagem mais utilizado pelas melhores escolas de gestão do mundo. Criada em 1912 para que os estudantes de direito não aprendessem apenas o direito com base em conteúdos teóricos, a sua função era também apresentar-lhes situações complexas da vida real. Poderão então tomar decisões informadas e fazer juízos de valor sobre a forma de os resolver. Em 1924 foi estabelecido como um método de ensino padrão em Harvard.

Com este modelo de ensino, é o próprio aluno que constrói a sua competência profissional através de estratégias como o *Learning by doing* ou o *Design Thinking*, utilizadas por outras instituições de renome, como Yale ou Stanford.

Este método orientado para a ação será aplicado ao longo de todo o curso académico do estudante com a TECH. Desta forma, será confrontado com múltiplas situações da vida real e terá de integrar conhecimentos, pesquisar, argumentar e defender as suas ideias e decisões. A premissa era responder à questão de saber como agiriam quando confrontados com acontecimentos específicos de complexidade no seu trabalho quotidiano.

Método *Relearning*

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

Este método rompe com as técnicas tradicionais de ensino para colocar o aluno no centro da equação, fornecendo os melhores conteúdos em diferentes formatos. Desta forma, consegue rever e reiterar os conceitos-chave de cada disciplina e aprender a aplicá-los num ambiente real.

Na mesma linha, e de acordo com múltiplas investigações científicas, a repetição é a melhor forma de aprender. Por conseguinte, a TECH oferece entre 8 e 16 repetições de cada conceito-chave na mesma aula, apresentadas de forma diferente, a fim de garantir que o conhecimento seja totalmente incorporado durante o processo de estudo.

O Relearning permitir-lhe-á aprender com menos esforço e maior desempenho, envolvendo-o mais na sua especialização, desenvolvendo um espírito crítico, a defesa de argumentos e o confronto de opiniões: uma equação que o leva diretamente ao sucesso.

Um Campus Virtual 100% online com os melhores recursos didáticos

Para aplicar eficazmente a sua metodologia, a TECH concentra-se em fornecer aos licenciados materiais didáticos em diferentes formatos: textos, vídeos interativos, ilustrações e mapas de conhecimento, entre outros. Todos eles são concebidos por professores qualificados que centram o seu trabalho na combinação de casos reais com a resolução de situações complexas através da simulação, o estudo de contextos aplicados a cada carreira profissional e a aprendizagem baseada na repetição, através de áudios, apresentações, animações, imagens, etc.

Os últimos dados científicos no domínio da neurociência apontam para a importância de ter em conta o local e o contexto em que o conteúdo é acedido antes de iniciar um novo processo de aprendizagem. A possibilidade de ajustar estas variáveis de forma personalizada ajuda as pessoas a recordar e a armazenar conhecimentos no hipocampo para retenção a longo prazo. Trata-se de um modelo denominado *Neurocognitive context-dependent e-learning* que é conscientemente aplicado neste curso universitário.

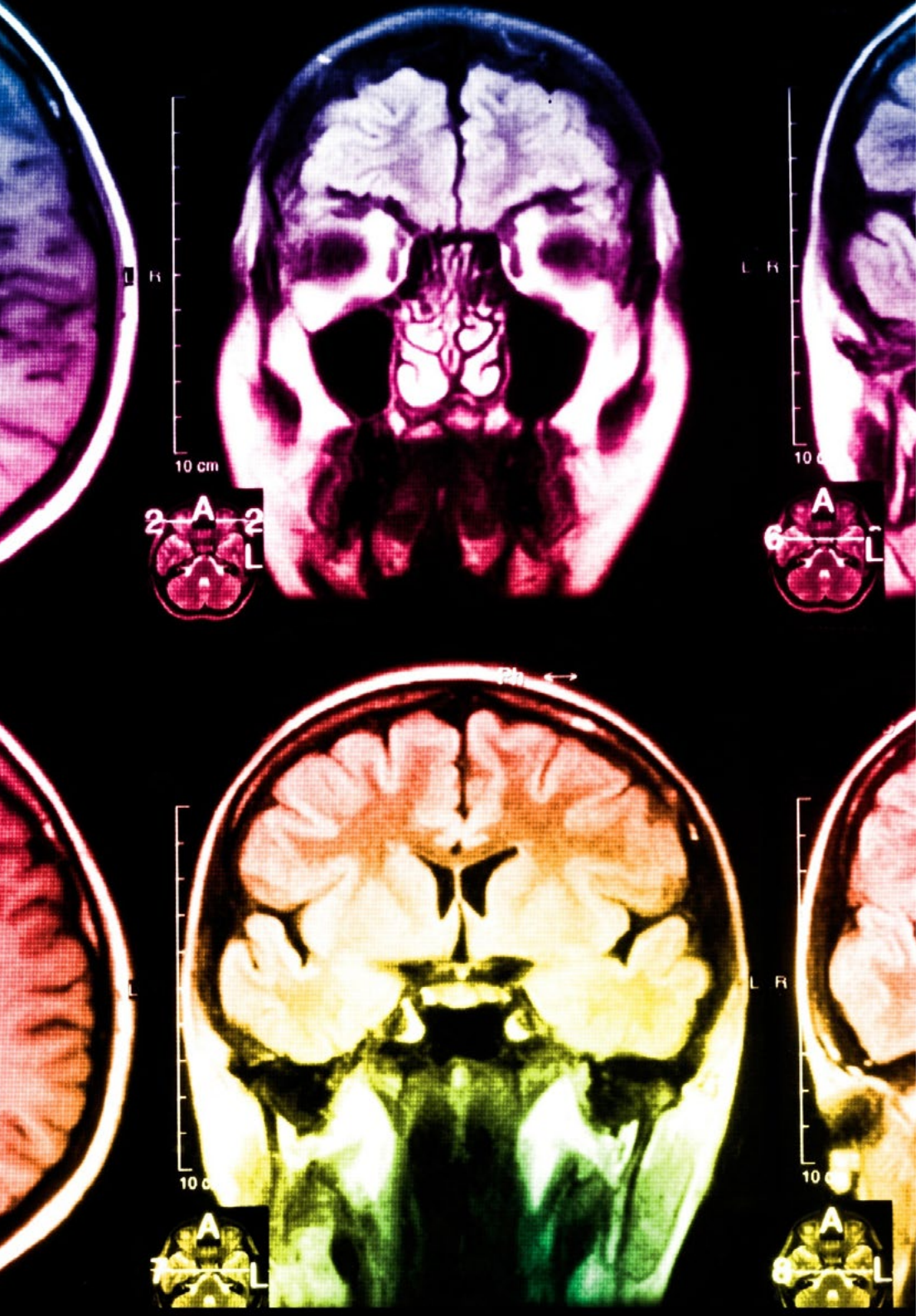
Por outro lado, também com o objetivo de favorecer ao máximo o contato mentor-mentorando, é disponibilizada uma vasta gama de possibilidades de comunicação, tanto em tempo real como em diferido (mensagens internas, fóruns de discussão, serviço telefónico, contacto por correio eletrónico com o secretariado técnico, chat, videoconferência, etc.).

Da mesma forma, este Campus Virtual muito completo permitirá aos estudantes da TECH organizar os seus horários de estudo em função da sua disponibilidade pessoal ou das suas obrigações profissionais. Desta forma, terão um controlo global dos conteúdos académicos e das suas ferramentas didácticas, em função da sua atualização profissional acelerada.

> *O modo de estudo online deste programa permitir-lhe-á organizar o seu tempo e ritmo de aprendizagem, adaptando-o ao seu horário"*

A eficácia do método justifica-se com quatro resultados fundamentais:

1. Os alunos que seguem este método não só conseguem a assimilação de conceitos, como também o desenvolvimento da sua capacidade mental, através de exercícios que avaliam situações reais e a aplicação de conhecimentos.
2. A aprendizagem traduz-se solidamente em competências práticas que permitem ao aluno uma melhor integração do conhecimento na prática diária.
3. A assimilação de ideias e conceitos é facilitada e mais eficiente, graças à utilização de situações que surgiram a partir da realidade.
4. O sentimento de eficiência do esforço investido torna-se um estímulo muito importante para os alunos, o que se traduz num maior interesse pela aprendizagem e num aumento da dedicação ao Curso.



A metodologia universitária mais bem classificada pelos seus alunos

Os resultados deste modelo académico inovador estão patentes nos níveis de satisfação global 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..

Aceder aos conteúdos de estudo a partir de qualquer dispositivo com ligação à Internet (computador, tablet, smartphone) graças ao fato de a TECH estar na vanguarda da tecnologia e do ensino.

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 didáticos, cuidadosamente preparados, estarão disponíveis neste programa:

Material de estudo

Todos os conteúdos didáticos são criados especificamente para o curso, pelos especialistas que o irão lecionar, de modo a que o desenvolvimento didático seja realmente específico e concreto.

Estes conteúdos são então aplicados ao formato audiovisual que criará a nossa forma de trabalhar online, com as mais recentes técnicas que nos permitem oferecer-lhe a maior qualidade em cada uma das peças que colocaremos ao seu serviço.

Estágios de aptidões e competências

Realizarão atividades para desenvolver competências e aptidões específicas em cada área temática. Práticas e dinâmicas para adquirir e desenvolver as competências e capacidades que um especialista deve desenvolver no quadro da globalização.

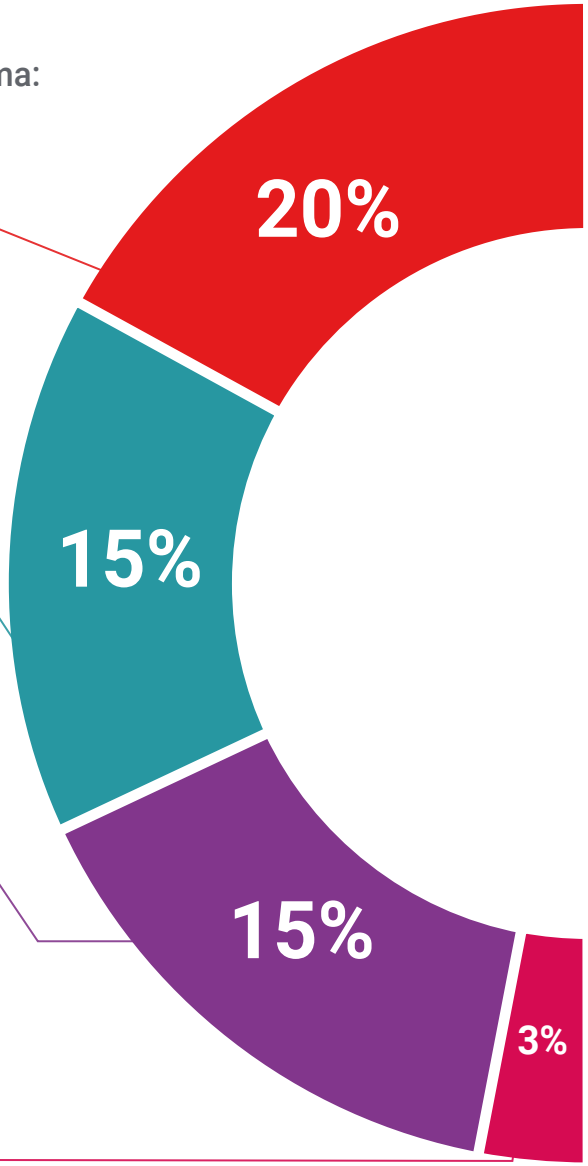
Resumos interativos

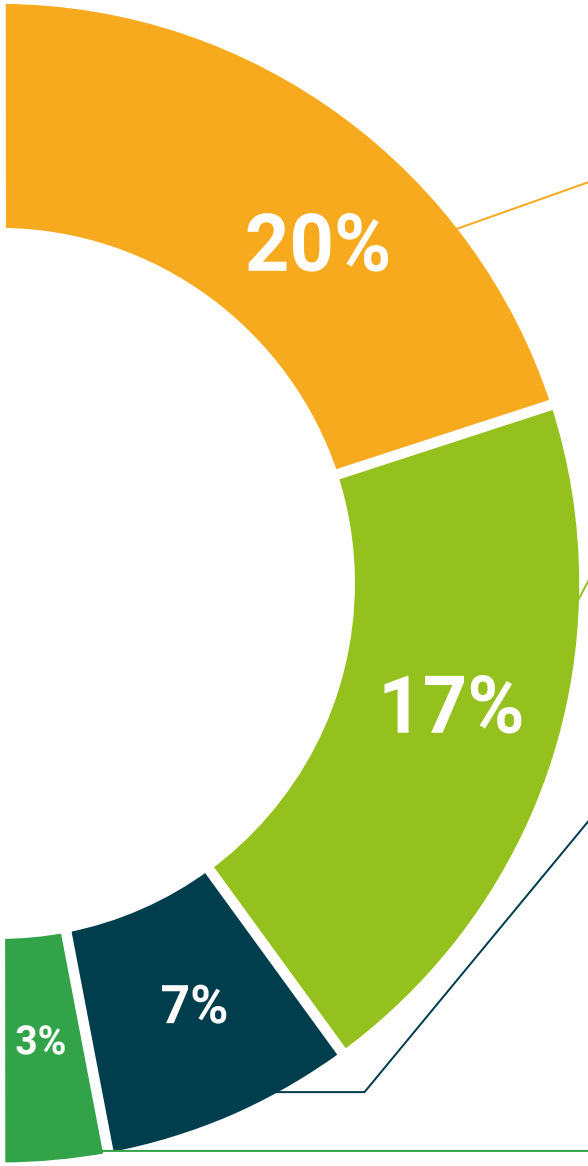
Apresentamos os conteúdos de forma atrativa e dinâmica em ficheiros multimédia que incluem áudio, vídeos, imagens, diagramas e mapas conceptuais a fim de reforçar o conhecimento.

Este sistema educativo único para a apresentação de conteúdos multimédia foi galardoado pela Microsoft como uma "Caso de sucesso na Europa"

Leituras complementares

Artigos recentes, documentos de consenso, diretrizes internacionais... Na nossa biblioteca virtual, terá acesso a tudo o que precisa para completar a sua formação.





Case Studies

Será realizada uma seleção dos melhores *case studies* na área;
Casos apresentados, analisados e instruídos pelos melhores especialistas do panorama internacional.

Testing & Retesting

Avaliamos e reavaliamos periodicamente os seus conhecimentos ao longo de todo o programa. Fazemo-lo em 3 dos 4 níveis da Pirâmide de Miller.

Masterclasses

Existe evidência científica acerca da utilidade da observação por especialistas terceiros.

O que se designa de *Learning from an expert* fortalece o conhecimento e a memória, e cria a confiança em futuras decisões difíceis.

Guias práticos

A TECH oferece os conteúdos mais relevantes do curso sob a forma de fichas de trabalho ou de guias de ação rápida. Uma forma sintética, prática e eficaz de ajudar o aluno a progredir na sua aprendizagem.

06

Corpo docente

O corpo docente deste programa da TECH é integrado por especialistas de renome internacional nas áreas de Inteligência Artificial e cibersegurança. Com trajetórias sólidas tanto na investigação como na implementação de soluções tecnológicas avançadas, estes profissionais trazem uma abordagem prática e estratégica ao desenvolvimento de competências-chave no setor. A sua experiência abrange desde a direção de projetos inovadores até a colaboração com líderes da indústria, garantindo uma visão atualizada e aplicada às exigências tecnológicas mais desafiantes.

Beneficiar-se-á tanto da experiência como do percurso académico de profissionais reconhecidos com uma sólida reputação em Cibersegurança e Aprendizagem Profunda"

Direção

Dr. Arturo Peralta Martín-Palomino

- 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 de: Grupo de Investigação SMILE

Professores

Sr. Alejandro Del Rey Sánchez

- 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"

07

Certificação

O Mestrado Próprio em Inteligência Artificial na Cibersegurança garante, além da formação mais rigorosa e atualizada, o acesso a um certificado de Mestrado Próprio 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 **Mestrado Próprio em Inteligência Artificial na Cibersegurança** 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:

Título: **Mestrado Próprio em Inteligência Artificial na Cibersegurança**

Modalidade: **online**

Duração: **12 meses**

Acreditação: **90 ECTS**

tech global university

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

Mestrado Próprio em Inteligência Artificial na Cibersegurança

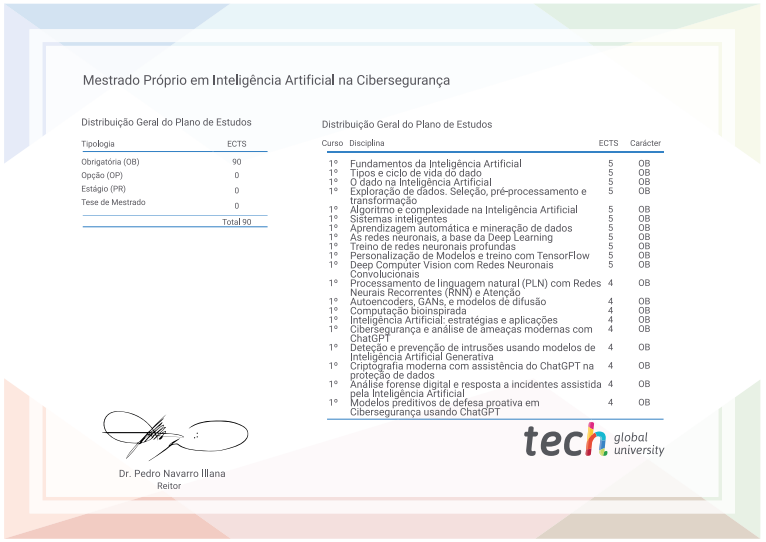
Trata-se de um título próprio com duração de 2.700 horas, o equivalente a 90 ECTS, com data de início dd/mm/aaaa e data final dd/mm/aaaa.

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: BBADCEA0BECB990 techtitute.com/titulos



Mestrado Próprio em Inteligência Artificial na Cibersegurança

Distribuição Geral do Plano de Estudos

Tipologia	ECTS
Obrigatória (OB)	90
Opção (OP)	0
Estágio (PR)	0
Tese de Mestrado	0
	Total 90

Distribuição Geral do Plano de Estudos

Curso	Disciplina	ECTS	Carácter
1º	Fundamentos da Inteligência Artificial	5	OB
1º	Tipos e ciclo de vida do dado	5	OB
1º	O dado na Inteligência Artificial	5	OB
1º	Exploração de dados. Seleção, pré-processamento e transformação	5	OB
1º	Algoritmo e complexidade na Inteligência Artificial	5	OB
1º	Sistemas inteligentes	5	OB
1º	Aprendizagem automática e mineração de dados	5	OB
1º	As redes neuronais, a base da Deep Learning	5	OB
1º	Treino de redes neuronais profundas	5	OB
1º	Personalização de Modelos e treino com TensorFlow	5	OB
1º	Deep Computer Vision com Redes Neuronais Convolucionais	5	OB
1º	Processamento de linguagem natural (PLN) com Redes Neurais Recorrentes (RNN) e Atenção	4	OB
1º	Autoencoders, GANs, e modelos de difusão	4	OB
1º	Computação bioinspirada	4	OB
1º	Inteligência Artificial: estratégias e aplicações	4	OB
1º	Cibersegurança e análise de ameaças modernas com ChatGPT	4	OB
1º	Deteção e prevenção de intrusões usando modelos de Inteligência Artificial Generativa	4	OB
1º	Criptografia moderna com assistência do ChatGPT na proteção de dados	4	OB
1º	Análise forense digital e resposta a incidentes assistida pela Inteligência Artificial	4	OB
1º	Modelos preditivos de defesa proativa em Cibersegurança usando ChatGPT	4	OB

Dr. Pedro Navarro Illana
Reitor

tech global university

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

tech global university

Mestrado Próprio
Inteligência Artificial na Cibersegurança

- Modalidade: **online**
- Duração: **12 meses**
- Certificação: **TECH Global University**
- Acreditação: **90 ECTS**
- Horário: **ao seu próprio ritmo**
- Exames: **online**

Mestrado Próprio
Inteligência Artificial na Cibersegurança

TECH é membro da:

tech global university