Curso

Análise e Desenvolvimento de Malware

tech universidade tecnológica

tech universidade tecnológica

Curso
Análise e Desenvolvimento de Malware

- Modalidade: **online**
- Duração: **6 semanas**
- Certificado: **TECH Universidade Tecnológica**
- Horário: **no seu próprio ritmo**
- Provas: **online**

Acesso ao site: www.techtitute.com/br/informatica/curso/analise-desenvolvimento-malware

Índice

01 Apresentação — *pág. 4*

02 Objetivos — *pág. 8*

03 Direção do curso — *pág. 12*

04 Estrutura e conteúdo — *pág. 16*

05 Metodologia — *pág. 20*

06 Certificado — *pág. 28*

01

Apresentação

Em um ambiente digital em que os ativos comerciais dependem de forma crítica da segurança cibernética, a ameaça constante de malware representa um desafio significativo. Nesse sentido, a proliferação de ataques maliciosos ressalta a urgência de contar com profissionais altamente capacitados nessa área. Nesse sentido, o plano de estudos aborda a necessidade imperativa de especialistas que não apenas compreendam a complexidade das ameaças digitais, mas também possam criar estratégias proativas para sua detecção e atenuação. Assim, os alunos aprenderão ferramentas essenciais para proteger a integridade dos sistemas em um ambiente de negócios cada vez mais digitalizado. Com a flexibilidade do modo 100% online, este curso garante a acessibilidade e a atualização contínua necessárias para enfrentar os desafios em constante mudança do ciberespaço.

Torne-se um especialista em malware com técnicas inovadoras de análise dinâmica graças a este exclusivo programa 100% online"

No cenário atual de cibersegurança, a sofisticação das ameaças cibernéticas atingiu níveis sem precedentes, gerando uma demanda crescente por profissionais especializados em análise e desenvolvimento de malware. A constante evolução das táticas maliciosas exige uma resposta igualmente dinâmica dos especialistas em cibersegurança. Nesse contexto, o atual programa universitário da TECH surge como uma solução abrangente para atender a essas necessidades. Projetado para fornecer aos alunos conhecimentos avançados, o plano de estudos abrange tudo, desde uma compreensão completa da natureza do malware até a avaliação de ferramentas antimalware. Essa abordagem abrangente prepara os profissionais para lidar com as ameaças atuais e futuras.

O programa de Análise e Desenvolvimento de Malware da TECH é um conjunto robusto de conhecimento que abrange várias dimensões do mundo do malware. Os alunos explorarão em profundidade as várias formas e alvos de malware, obtendo conhecimento avançado de sua natureza, funcionalidade e comportamento. O programa se aprofunda na análise forense aplicada a malware, fornecendo aos alunos as habilidades necessárias para identificar indicadores de comprometimento (IoC) e padrões de ataque, cruciais para a detecção precoce e a resposta eficaz a incidentes de segurança. Além disso, o plano de estudos se concentra no desenvolvimento de habilidades específicas para avaliar e selecionar ferramentas de segurança antimalware. Os alunos aprenderão a discernir a eficácia dessas ferramentas e sua adaptabilidade a ambientes específicos, o que é essencial para a implementação de estratégias de defesa eficazes.

Com uma abordagem inovadora e adaptável, esse programa universitário é uma proposta de capacitação exclusiva. A modalidade 100% online e a metodologia *Relearning* garantir uma experiência educacional flexível e eficiente, permitindo que os profissionais avancem em suas carreiras sem interrupções e se adaptem continuamente às demandas em constante mudança do campo da cibersegurança.

Este **Curso de Análise e Desenvolvimento de Malware** conta com o conteúdo mais completo e atualizado do mercado. Suas principais características são:

- O desenvolvimento de casos práticos apresentados por especialistas em Análise e Desenvolvimento de Malware
- Os conteúdos gráficos, esquemáticos e extremamente práticos fornece informação atualizada e prática sobre aquelas disciplinas essenciais para o exercício da profissão
- Contém exercícios práticos onde o processo de autoavaliação é realizado para melhorar o aprendizado
- Destaque especial para as metodologias inovadoras
- Lições teóricas, perguntas a especialistas, fóruns de discussão sobre temas controversos e trabalhos de reflexão individual
- Disponibilidade de acesso a todo o conteúdo a partir de qualquer dispositivo, fixo ou portátil, com conexão à Internet

Você dominará a análise de chamadas com API monkeys em apenas 6 semanas da melhor formação online”

Você aprenderá a gerar Shellcode na universidade mais bem avaliada do mundo por seus alunos, de acordo com a plataforma Trustpilot (4,9/5)"

Você terá acesso a um sistema de aprendizagem baseado na repetição, por meio de um ensino natural e progressivo ao longo de todo o programa.

Você se aprofundará na ofuscação de Strings e dará à sua carreira o impulso de que ela precisa!.

O programa de estudos inclui em seu corpo docente profissionais do setor que trazem a experiência de seu trabalho nesta capacitação, além de renomados especialistas de sociedades líderes e universidades de prestígio.

O conteúdo multimídia, desenvolvido com a mais recente tecnologia educacional, permitirá ao profissional uma aprendizagem contextualizada, ou seja, realizada através de um ambiente simulado, proporcionando uma capacitação imersiva e programada para praticar diante de situações reais.

A estrutura deste programa se concentra na Aprendizagem Baseada em Problemas, onde o profissional deverá tentar resolver as diferentes situações de prática profissional que surgirem ao longo do curso acadêmico. Para isso, contará com a ajuda de um inovador sistema de vídeo interativo realizado por especialistas reconhecidos.

02

Objetivos

O principal objetivo deste programa de estudos é permitir que os alunos dominem conhecimentos avançados sobre a natureza, a funcionalidade e o comportamento do malware. Ao longo do programa, os alunos se aprofundarão nas várias formas e alvos de malware, o que lhes permitirá analisar e desenvolver estratégias defensivas eficazes no campo da cibersegurança. Essa abordagem integral também busca capacitar profissionais capazes de enfrentar os desafios emergentes na detecção, análise e atenuação de ameaças de malware em ambientes digitais complexos. Além disso, o uso de uma metodologia 100% online torna o aprendizado mais flexível, dando a possibilidade de acessar o curso a qualquer hora e lugar.

Você alcançará seus objetivos graças às ferramentas didáticas da TECH, incluindo vídeos explicativos e resumos interativos"

Objetivos gerais

- Adquirir habilidades avançadas em testes de penetração e simulações de Red Team, abordando a identificação e a exploração de vulnerabilidades em sistemas e redes
- Desenvolver habilidades de liderança para coordenar equipes especializadas em cibersegurança ofensiva, otimizando a execução de projetos de Pentesting e Red Team
- Desenvolver habilidades na análise e no desenvolvimento de malware, compreendendo sua funcionalidade e aplicando estratégias defensivas e educacionais
- Aperfeiçoar as habilidades de comunicação produzindo relatórios técnicos e executivos detalhados, apresentando as descobertas de forma eficaz para públicos técnicos e executivos
- Promover a prática ética e responsável no campo da cibersegurança, considerando os princípios éticos e legais em todas as atividades

Deseja dar um grande salto de qualidade em sua carreira? Com a TECH, você adquirirá habilidades em análise forense aplicada ao malware"

Objetivos específicos

- Adquirir conhecimentos avançados sobre a natureza, a funcionalidade e o comportamento do malware, compreender suas várias formas e objetivos
- Desenvolver habilidades em análise forense aplicadas ao malware, permitindo a identificação de indicadores de comprometimento (IoC) e padrões de ataque
- Aprender estratégias para detecção e prevenção eficazes de malware, incluindo a implementação de soluções avançadas de segurança
- Familiarizar o aluno com o desenvolvimento de malware para fins educacionais e defensivos, permitindo uma compreensão completa das táticas usadas pelos atacantes
- Promover práticas éticas e legais na análise e no desenvolvimento de malware, garantindo a integridade e a responsabilidade em todas as atividades
- Aplicar o conhecimento teórico em ambientes simulados, participar de exercícios práticos para entender e combater ataques maliciosos
- Desenvolver habilidades para avaliar e selecionar ferramentas de segurança anti-malware, considerando sua eficácia e adaptabilidade a ambientes específicos
- Aprender a implementar uma atenuação eficaz contra ameaças mal-intencionadas, reduzindo o impacto e a disseminação de ameaças de malware em sistemas e redes
- Promover a colaboração eficaz com as equipes de segurança, integrando estratégias e esforços para proteger contra ameaças de Malware

03

Direção do curso

O programa de Análise e Desenvolvimento de Malware tem um corpo docente excepcionalmente qualificado. Para isso, a TECH selecionou especialistas com experiência e reconhecido prestígio em empresas líderes no setor de cibersegurança. Esse corpo docente, composto por profissionais de destaque, traz não apenas experiência prática em análise e desenvolvimento de malware, mas também seu compromisso com a formação de futuros especialistas, garantindo um ensino atualizado e alinhado com as demandas e os desafios atuais do campo da segurança cibernética.

Atualize-se sobre a configuração de máquinas virtuais e snapshots com os melhores especialistas da área. Inicie sua carreira com a TECH!"

Direção

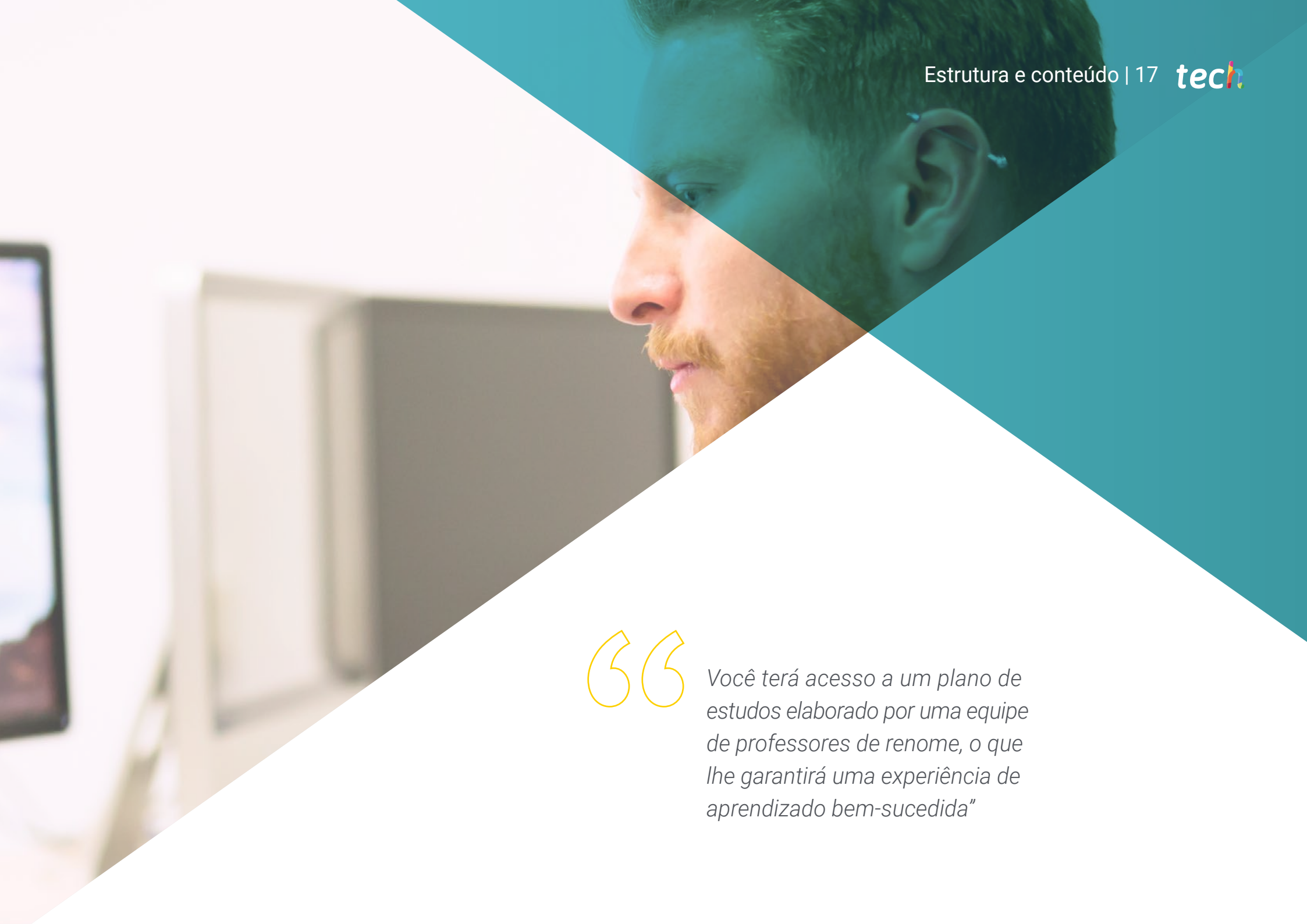
Sr. Carlos Gómez Pintado

- Gerente de cibersegurança e Red Team Cipherbit no Grupo Oesía
- Gestor *Advisor* & *Investor na* Wesson App
- Formado em Engenharia de Software e Tecnologias da Sociedade da Informação pela Universidade Politécnica de Madri
- Colaboração com instituições educacionais para o desenvolvimento de ciclos de formação de nível superior em cibersegurança

04

Estrutura e conteúdo

Esse programa universitário oferecerá aos alunos um aprofundamento no mundo do malware, com foco em seu desenvolvimento para fins educacionais e defensivos. Ao longo do curso, os alunos abordarão as complexidades do malware, permitindo uma compreensão detalhada das táticas empregadas pelos invasores. Nesse sentido, a abordagem equilibrada do plano de estudos não apenas promove a aquisição de conhecimentos avançados em análise de malware, mas também permite que os alunos desenvolvam estratégias defensivas essenciais no campo de segurança cibernética.



Você terá acesso a um plano de estudos elaborado por uma equipe de professores de renome, o que lhe garantirá uma experiência de aprendizado bem-sucedida"

Módulo 1. Análise e Desenvolvimento de Malware

1.1. Análise e Desenvolvimento de Malware
- 1.1.1. História e evolução do malware
- 1.1.2. Classificação e tipos de Malware
- 1.1.3. Análise de malware
- 1.1.4. Desenvolvimento de malware

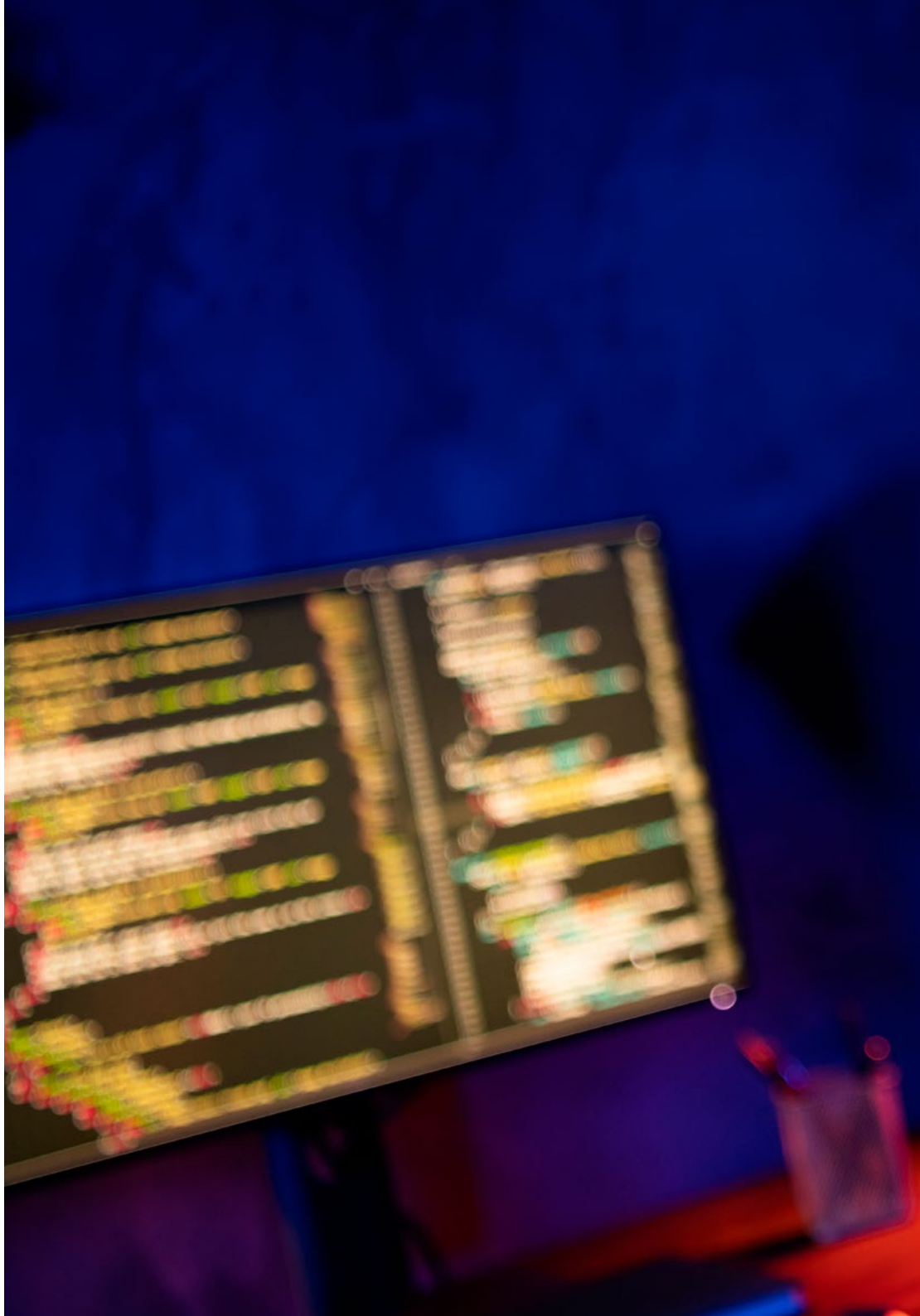
1.2. Preparação do ambiente
- 1.2.1. Configuração de máquina virtual e Snapshots
- 1.2.2. Ferramentas de análise de malware
- 1.2.3. Ferramentas de desenvolvimento de malware

1.3. Fundamentos do Windows
- 1.3.1. Formato do arquivo PE (Portable Executable)
- 1.3.2. Processos e Threads
- 1.3.3. Sistema de arquivos e registro
- 1.3.4. Windows Defender

1.4. Técnicas de Malware básicas
- 1.4.1. Geração de shellcode
- 1.4.2. Execução de shellcode no disco
- 1.4.3. Disco vs memória
- 1.4.4. Execução de shellcode na memória

1.5. Técnicas de malware intermediárias
- 1.5.1. Persistência no Windows
- 1.5.2. Pasta inicial
- 1.5.3. Chaves de registro
- 1.5.4. Protetores de tela

1.6. Técnicas de malware avançadas
- 1.6.1. Cifrado de shellcode (XOR)
- 1.6.2. Cifrado de shellcode (RSA)
- 1.6.3. Ofuscação de strings
- 1.6.4. Injeção de processos



1.7. Análise estática de malware
  1.7.1. Analisando packers com DIE (Detect It Easy)
  1.7.2. Analisando seções com o PE-Bear
  1.7.3. Descompilação com Ghidra
1.8. Análise dinâmica de malware
  1.8.1. Observando o comportamento com o Process Hacker
  1.8.2. Análise de chamadas com o API Monitor
  1.8.3. Análise de alterações no registro com o Regshot
  1.8.4. Observação de solicitações de rede com o TCPView
1.9. Análise em NET
  1.9.1. Introdução ao .NET
  1.9.2. Descompilação com o dnSpy
  1.9.3. Depuração com o dnSpy
1.10. Analizando um malware real
  1.10.1. Preparação do ambiente
  1.10.2. Análise estática do malware
  1.10.3. Análise dinâmica do malware
  1.10.4. Criação de regras YARA

Não perca a oportunidade de impulsionar sua carreira por meio desse programa inovador”

05

Metodologia

Este curso oferece uma maneira diferente de aprender. Nossa metodologia é desenvolvida através de um modo de aprendizagem cíclico: ***o Relearning***. Este sistema de ensino é utilizado, por exemplo, nas faculdades de medicina mais prestigiadas do mundo e foi considerado um dos mais eficazes pelas principais publicações científicas, como o ***New England Journal of Medicine.***

Descubra o Relearning, um sistema que abandona a aprendizagem linear convencional para realizá-la através de sistemas de ensino cíclicos: uma forma de aprendizagem que se mostrou extremamente eficaz, especialmente em disciplinas que requerem memorização"

Estudo de caso para contextualizar todo o conteúdo

Nosso programa oferece um método revolucionário para desenvolver as habilidades e o conhecimento. Nosso objetivo é fortalecer as competências em um contexto de mudança, competitivo e altamente exigente.

Com a TECH você irá experimentar uma forma de aprender que está revolucionando as bases das universidades tradicionais em todo o mundo"

Você terá acesso a um sistema de aprendizagem baseado na repetição, por meio de um ensino natural e progressivo ao longo de todo o programa.

Através de atividades de colaboração e casos reais, o aluno aprenderá a resolver situações complexas em ambientes reais de negócios.

Um método de aprendizagem inovador e diferente

Este curso da TECH é um programa de ensino intensivo, criado do zero, que propõe os desafios e decisões mais exigentes nesta área, em âmbito nacional ou internacional. Através desta metodologia, o crescimento pessoal e profissional é impulsionado em direção ao sucesso. O método do caso, técnica que constitui a base deste conteúdo, garante que a realidade econômica, social e profissional mais atual seja adotada.

> *Nosso programa prepara você para enfrentar novos desafios em ambientes incertos e alcançar o sucesso na sua carreira"*

O método do caso é o sistema de aprendizagem mais utilizado nas principais escolas de Informática do mundo, desde que elas existem. Desenvolvido em 1912 para que os estudantes de Direito não aprendessem a lei apenas com base no conteúdo teórico, o método do caso consistia em apresentar-lhes situações realmente complexas para que tomassem decisões conscientes e julgassem a melhor forma de resolvê-las. Em 1924 foi estabelecido como o método de ensino padrão em Harvard.

Em uma determinada situação, o que um profissional deveria fazer? Esta é a pergunta que abordamos no método do caso, um método de aprendizagem orientado para a ação. Ao longo do curso, os alunos vão se deparar com múltiplos casos reais. Terão que integrar todo o conhecimento, pesquisar, argumentar e defender suas ideias e decisões.

Metodologia Relearning

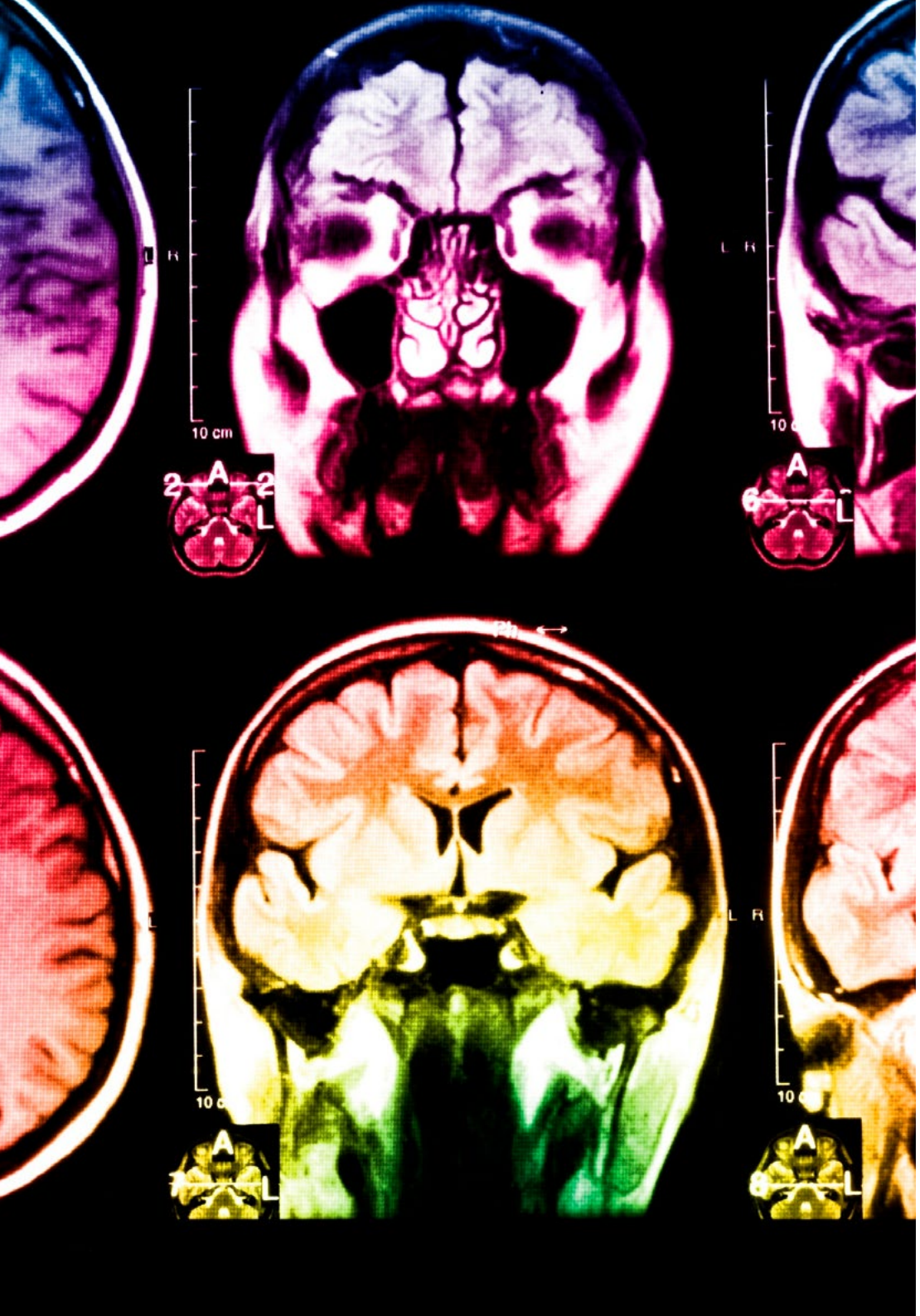
A TECH utiliza de maneira eficaz a metodologia do estudo de caso com um sistema de aprendizagem 100% online, baseado na repetição, combinando elementos didáticos diferentes em cada aula.

Potencializamos o Estudo de Caso com o melhor método de ensino 100% online: o Relearning.

Em 2019 alcançamos os melhores resultados de aprendizagem entre todas as universidades online do mundo.

Na TECH você aprenderá através de uma metodologia de vanguarda, desenvolvida para capacitar os profissionais do futuro. Este método, na vanguarda da pedagogia mundial, se chama Relearning.

Nossa universidade é uma das únicas que possui a licença para usar este método de sucesso. Em 2019 conseguimos melhorar os níveis de satisfação geral dos nossos alunos (qualidade de ensino, qualidade dos materiais, estrutura dos curso, objetivos, entre outros) com relação aos indicadores da melhor universidade online.



No nosso programa, a aprendizagem não é um processo linear, ela acontece em espiral (aprender, desaprender, esquecer e reaprender). Portanto, combinamos cada um desses elementos de forma concêntrica. Esta metodologia já capacitou mais de 650 mil universitários com um sucesso sem precedentes em campos tão diversos como a bioquímica, a genética, a cirurgia, o direito internacional, habilidades administrativas, ciência do esporte, filosofia, direito, engenharia, jornalismo, história, mercados e instrumentos financeiros. Tudo isso em um ambiente altamente exigente, com um corpo discente com um perfil socioeconômico médio-alto e uma média de idade de 43,5 anos.

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

A partir das últimas evidências científicas no campo da neurociência, sabemos como organizar informações, ideias, imagens, memórias, mas sabemos também que o lugar e o contexto onde aprendemos algo é fundamental para nossa capacidade de lembrá-lo e armazená-lo no hipocampo, para mantê-lo em nossa memória a longo prazo.

Desta forma, no que se denomina Neurocognitive context-dependent e-learning, os diferentes elementos do nosso programa estão ligados ao contexto onde o aluno desenvolve sua prática profissional.

Neste programa, oferecemos o melhor material educacional, preparado especialmente para os profissionais:

Material de estudo

Todo o conteúdo foi criado especialmente para o curso pelos especialistas que irão ministrá-lo, o que faz com que o desenvolvimento didático seja realmente específico e concreto.

Posteriormente, esse conteúdo é adaptado ao formato audiovisual, para criar o método de trabalho online da TECH. Tudo isso, com as técnicas mais inovadoras que proporcionam alta qualidade em todo o material que é colocado à disposição do aluno.

Masterclasses

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

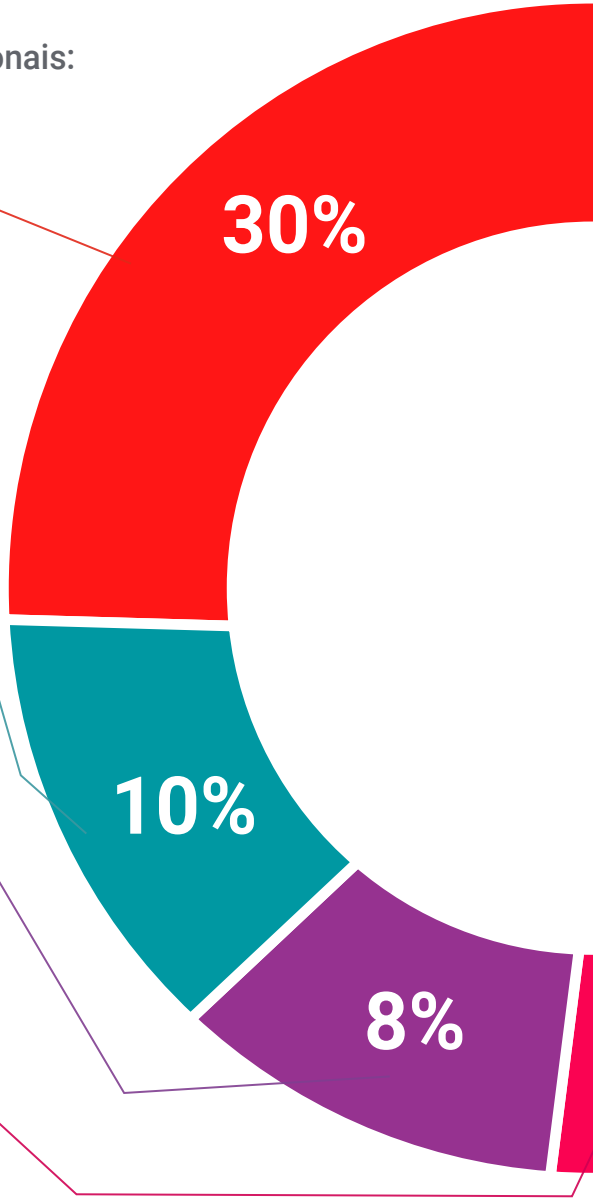
O "Learning from an expert" fortalece o conhecimento e a memória, além de gerar segurança para a tomada de decisões difíceis no futuro.

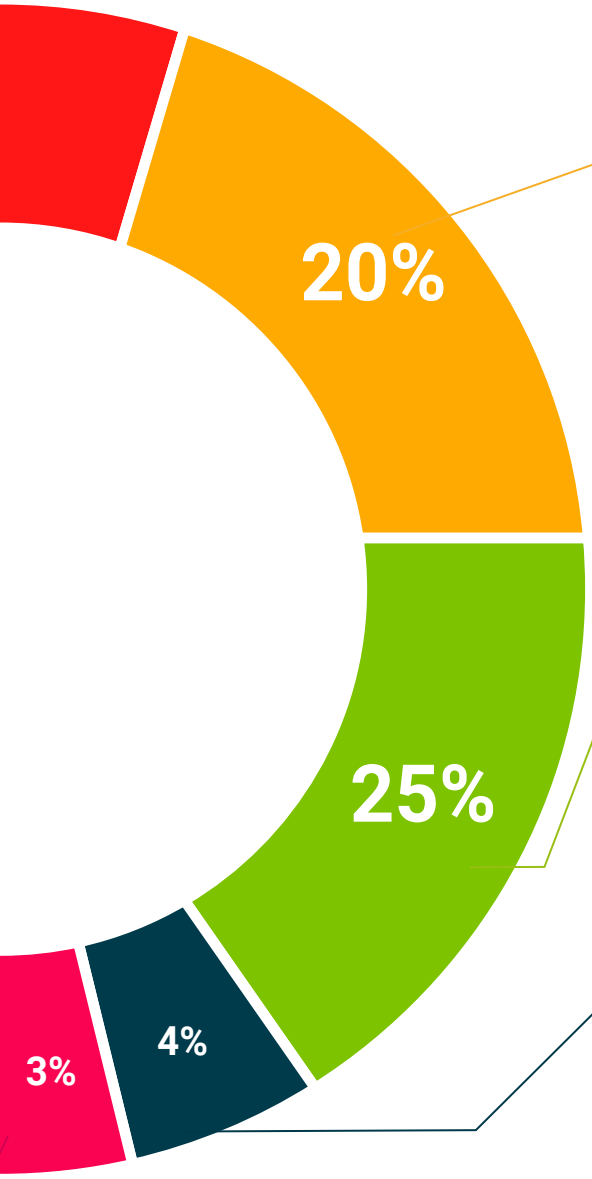
Práticas de habilidades e competências

Serão realizadas atividades para desenvolver competências e habilidades específicas em cada área temática. Práticas e dinâmicas para adquirir e ampliar as competências e habilidades que um especialista precisa desenvolver no contexto globalizado em que vivemos.

Leituras complementares

Artigos recentes, documentos de consenso e diretrizes internacionais, entre outros. Na biblioteca virtual da TECH o aluno terá acesso a tudo o que for necessário para complementar a sua capacitação.





Estudos de caso

Os alunos irão completar uma seleção dos melhores estudos de caso escolhidos especialmente para esta capacitação. Casos apresentados, analisados e orientados pelos melhores especialistas do cenário internacional.

Resumos interativos

A equipe da TECH apresenta o conteúdo de forma atraente e dinâmica através de pílulas multimídia que incluem áudios, vídeos, imagens, gráficos e mapas conceituais para consolidar o conhecimento.

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

Testing & Retesting

Avaliamos e reavaliamos periodicamente o conhecimento do aluno ao longo do programa, através de atividades e exercícios de avaliação e autoavaliação, para que possa comprovar que está alcançando seus objetivos.

06

Certificado

O Curso de Análise e Desenvolvimento de Malware garante, além da capacitação mais rigorosa e atualizada, acesso ao certificado do Curso emitido pela TECH Universidade Tecnológica.

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

Este **Curso de Análise e Desenvolvimento de Malware** conta com o conteúdo mais completo e atualizado do mercado.

Uma vez aprovadas as avaliações, o aluno receberá por correio o certificado* do **Curso** emitido pela **TECH Universidade Tecnológica.**

O certificado emitido pela **TECH Universidade Tecnológica** expressará a qualificação obtida no Curso, atendendo aos requisitos normalmente exigidos pelas bolsas de empregos, concursos públicos e avaliação de carreira profissional.

Título: **Curso de Análise e Desenvolvimento de Malware**

Modalidade: **online**

Duração: **6 semanas**


tech universidade tecnológica

Outorga o presente

CERTIFICADO

a

Sr./Sra. _____, com documento de identidade nº _____

por ter concluído e aprovado com sucesso o

CURSO

de

Análise e Desenvolvimento de Malware

Este é um curso próprio desta Universidade, com duração de 150 horas, com data de início dd/mm/aaaa e data final dd/mm/aaaaa.

A TECH é uma Instituição Privada de Ensino Superior reconhecida pelo Ministério da Educação Pública em 28 de junho de 2018.

Em 17 de junho de 2020

Ma.Tere Guevara Navarro
Reitora

código único TECH: AFWOR23S techtitute.com/titulos

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

tech universidade tecnológica

Curso
Análise e Desenvolvimento de Malware

- Modalidade: **online**
- Duração: **6 semanas**
- Certificado: **TECH Universidade Tecnológica**
- Horário: **no seu próprio ritmo**
- Provas: **online**

Curso

Análise e Desenvolvimento de Malware

tech universidade tecnológica