Programa Avançado
Cibersegurança Red Team

tech universidade tecnológica

tech universidade tecnológica

Programa Avançado
Cibersegurança Red Team

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

Acesso ao site: www.techtitute.com/br/informatica/programa-avancado/programa-avancado-ciberseguranca-red-team

Índice

01

Apresentação

A cibersegurança tornou-se um pilar fundamental na era digital, enquanto a crescente interconexão dos sistemas intensificou a ameaça de ataques cibernéticos. A demanda por profissionais altamente qualificados nesse campo está mais evidente do que nunca, especialmente considerando o aumento exponencial do crime cibernético e dos ataques sofisticados. Nesse contexto, este programa é apresentado como uma resposta estratégica para equipar os profissionais com as habilidades necessárias para lidar com as ameaças cibernéticas. Durante o curso, os alunos estarão imersos em simulações avançadas de ameaças. A metodologia do plano de estudos 100% online oferece flexibilidade e acessibilidade, com uma ampla variedade de conteúdo multimídia e a aplicação do método *Relearning*.

Você contribuirá para melhorar a cibersegurança e evitará a ocorrência de crimes digitais graves. Não perca esta oportunidade e matricule-se já!"

No complexo cenário da cibersegurança, ter um especialista nessa área é uma necessidade absoluta para as organizações que buscam fortalecer suas defesas contra ameaças em constante evolução. Essa abordagem proativa, fundamental para aprimorar continuamente a postura de segurança, destaca a necessidade crítica de conhecimento especializado.

A implementação de medidas proativas é essencial, e a capacitação especializada da Red Team oferece aos profissionais a capacidade de antecipar, identificar e mitigar ativamente as vulnerabilidades em sistemas e redes. Neste Programa Avançado, o aluno adquirirá habilidades em testes de penetração e simulações, abordando a identificação e a exploração de vulnerabilidades. Nesse sentido, além de desenvolver habilidades técnicas avançadas, o programa também promoverá uma colaboração eficaz com as equipes de segurança, integrando estratégias contra ameaças de *malware*.

Além disso, os alunos adquirirão uma sólida compreensão dos princípios fundamentais da investigação forense digital (DFIR), aplicáveis na resolução de incidentes cibernéticos. Além disso, essa abordagem integral do plano de estudos garantirá que os profissionais estejam equipados com habilidades de ponta no campo da cibersegurança.

Essa formação acadêmica se distingue não apenas pelo conteúdo, mas também pela metodologia avançada. Ele estará disponível para os alunos totalmente online, oferecendo a flexibilidade necessária para que eles avancem em suas carreiras sem comprometer suas responsabilidades profissionais.

Além disso, a implementação do *Relearning*, consistente na repetição de conceitos-chave, é usado para fixar o conhecimento e facilitar o aprendizado eficaz. Essa combinação de acessibilidade e abordagem pedagógica robusta faz com que este Programa Avançado não seja apenas uma opção educacional avançada, mas também um importante impulsionador para aqueles que buscam se destacar no campo da Cibersegurança.

Este **Programa Avançado de Cibersegurança Red Team** conta com o conteúdo mais completo e atualizado do mercado. Suas principais características são:

- O desenvolvimento de estudos de caso apresentados por especialistas em Segurança Cibernética Red Team
- 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 se destacará em um setor de grande projeção graças a esse programa universitário exclusivo da TECH”

Você se aprofundará em relatórios forenses detalhados na universidade mais bem avaliada do mundo por seus alunos, de acordo com a plataforma Trustpilot (4,9/5)"

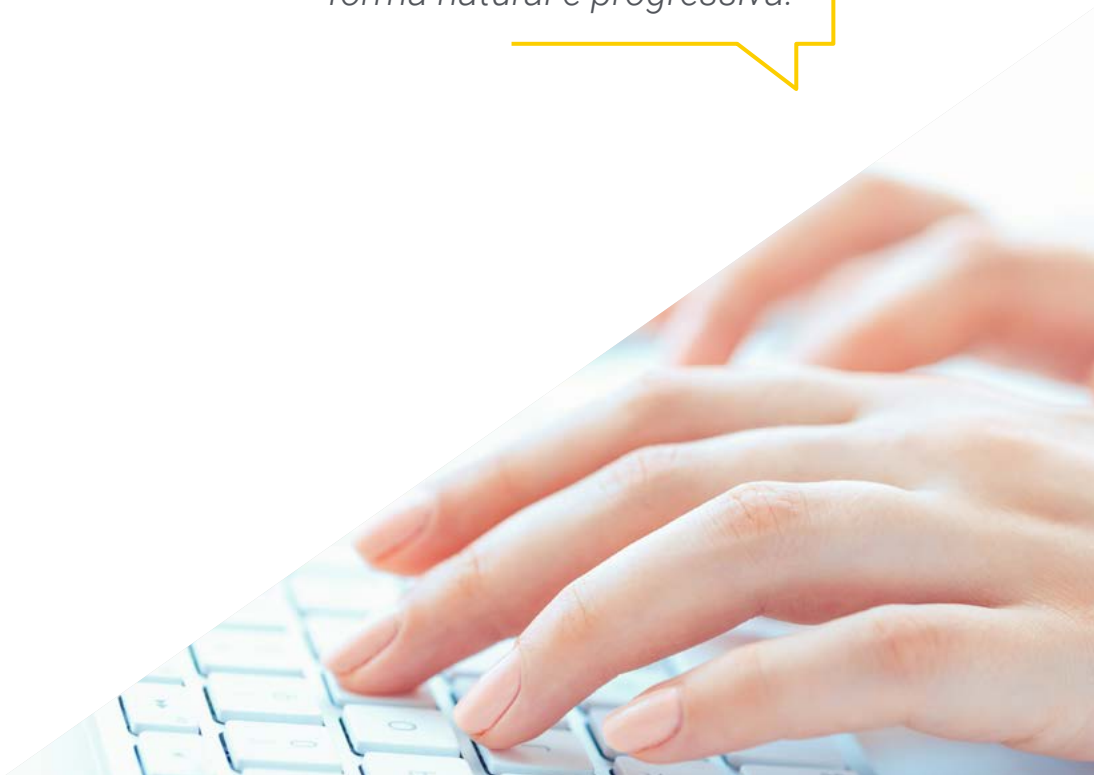
O corpo docente deste programa inclui profissionais da área que transferem a experiência do seu trabalho para esta capacitação, além de especialistas reconhecidos de sociedades científicas de referência e universidades de prestigio.

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.

Você desenvolverá habilidades para avaliar e selecionar ferramentas de segurança antimalware.

Esqueça a memorização! Com o sistema Relearning, você integrará os conceitos de forma natural e progressiva.



02

Objetivos

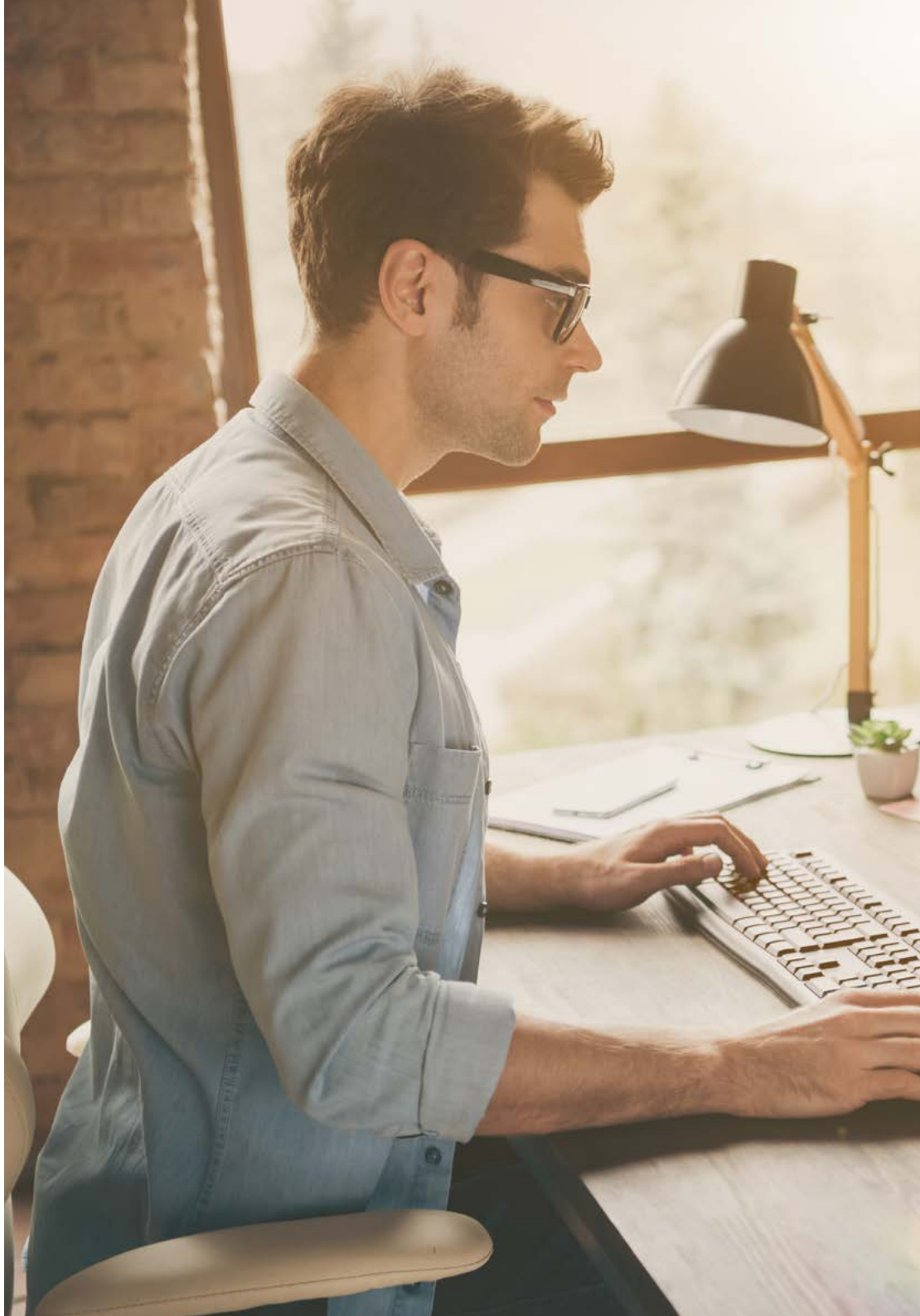
O Programa Avançado de Cibersegurança *Red Team* tem como principal objetivo capacitar os alunos no desenvolvimento de habilidades avançadas de simulação de ameaças. Durante todo o programa, os alunos estarão imersos na replicação de táticas, técnicas e procedimentos (TTPs) usados por agentes mal-intencionados. Nesse contexto, a abordagem especializada não apenas fortalecerá as habilidades técnicas dos profissionais, mas também os capacitará a enfrentar os desafios mundo real nesse campo. Além disso, o uso da metodologia *Relearning* facilitará a aprendizagem, fixando conceitos-chave com pouco esforço.

Você identificará os pontos fracos e as vulnerabilidades das infraestruturas cibernéticas das empresas. Alcance as suas metas com a TECH!"

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
- Manter os alunos atualizados com as tendências e tecnologias emergentes em cibersegurança

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



Objetivos específicos

Módulo 1. Análise e Desenvolvimento de Malware

- 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*
- Manter o aluno atualizado com as últimas tendências e técnicas usadas na análise e no desenvolvimento de *malware*, assegurando a relevância e a eficácia contínuas das habilidades adquiridas

Módulo 2. Fundamentos forenses e DFIR

- Adquirir uma sólida compreensão dos princípios fundamentais da Investigação Forense Digital (DFIR) e sua aplicação na resolução de incidentes cibernéticos
- Desenvolver habilidades na aquisição segura e forense de evidências digitais, garantindo a preservação da cadeia de custódia
- Aprender a realizar análise forense de sistemas de arquivos
- Familiarizar o aluno com técnicas avançadas para a análise de logs e registros, permitindo a reconstrução de eventos em ambientes digitais
- Aprender a aplicar metodologias de investigação forense digital na resolução de casos, desde a identificação até a documentação das descobertas
- Familiarizar o aluno com a análise de evidências digitais e a aplicação de técnicas forenses em *Pentesting*
- Desenvolver habilidades na preparação de relatórios forenses detalhados e claros, apresentando descobertas e conclusões de forma compreensível
- Promover a colaboração eficaz com as equipes de resposta a incidentes (IR), otimizando a coordenação na investigação e mitigação de ameaças
- Promover práticas éticas e legais em perícia digital, garantindo a adesão às normas de cibersegurança e aos padrões de conduta

Módulo 3. Exercícios de Red Team Avançados

- Desenvolver habilidades em simulação de ameaças avançadas, replicando táticas, técnicas e procedimentos (TTPs) usados por agentes mal-intencionados atraentes
- Aprender a identificar pontos fracos e vulnerabilidades na infraestrutura por meio de exercícios realistas de *Red Team*, fortalecendo a postura de segurança
- Familiarizar o aluno com técnicas avançadas de evasão de segurança, permitindo a avaliação da resistência da infraestrutura a ataques desejáveis
- Desenvolver habilidades eficazes de coordenação e colaboração entre os membros da equipe de *Red Team*, otimizando a execução de táticas e estratégias para avaliar de forma abrangente a segurança da organização
- Aprender a simular cenários de ameaças atuais, como ataques de *ransomware* ou campanhas avançadas de *phishing* para avaliar a capacidade da organização de responder a organização
- Familiarizar o aluno com as técnicas de análise pós-exercício, avaliando o desempenho da equipe de *Red Team* e extraindo as lições aprendidas para melhorias contínuas
- Desenvolver habilidades para avaliar a resiliência organizacional a ataques simulados, identificando áreas para aprimoramento de políticas e procedimentos
- Aprender a preparar relatórios detalhados que documentem as descobertas, as metodologias usadas e as recomendações derivadas de *Red Team* avançados
- Promover práticas éticas e legais na condução de exercícios de *Red Team*, assegurando a adesão às normas de cibersegurança e aos padrões éticos

03

Direção do curso

Para esse programa universitário, a TECH reuniu um corpo docente distinto, composto pelos melhores especialistas da área. Nesse sentido, cada membro da equipe de professores tem um histórico profissional extenso e reconhecido, formado em empresas líderes do setor de segurança cibernética. Cuidadosamente selecionados por sua experiência e conhecimento, esses profissionais não apenas garantirão a qualidade acadêmica do programa, mas também fornecerão uma perspectiva prática e atualizada, enriquecendo a formação dos participantes com insights valiosos de sua experiência real no ambiente do Red Team.

Mantenha-se atualizado com as mais recentes técnicas de criptografia Shellcode (XQR) dos principais especialistas em segurança cibernética. Inicie sua carreira com a TECH!"

Direção

Sr. Carlos Gómez Pintado

- Gerente de cibersegurança e Red Team Cipherbit no Grupo Oesía
- Gerente *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 de estudos proporcionará aos alunos uma imersão especializada em análise forense aplicada ao *malware*, destacando o desenvolvimento de habilidades essenciais para a identificação de indicadores de comprometimento (IoC) e padrões de ataque. Durante o curso, os alunos estarão imersos em metodologias avançadas, fornecendo-lhes as ferramentas e o conhecimento necessários para lidar com ameaças cibernéticas sofisticadas. Além disso, esse programa rigorosamente estruturado garantirá uma formação abrangente na área de *Red Team*, preparando os profissionais para analisar e combater estratégias complexas usadas por agentes mal-intencionados.

Você aprofundará seus conhecimentos sobre técnicas avançadas de pós-exploração e se posicionará como um excelente Red Teamer”

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. Análises 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*

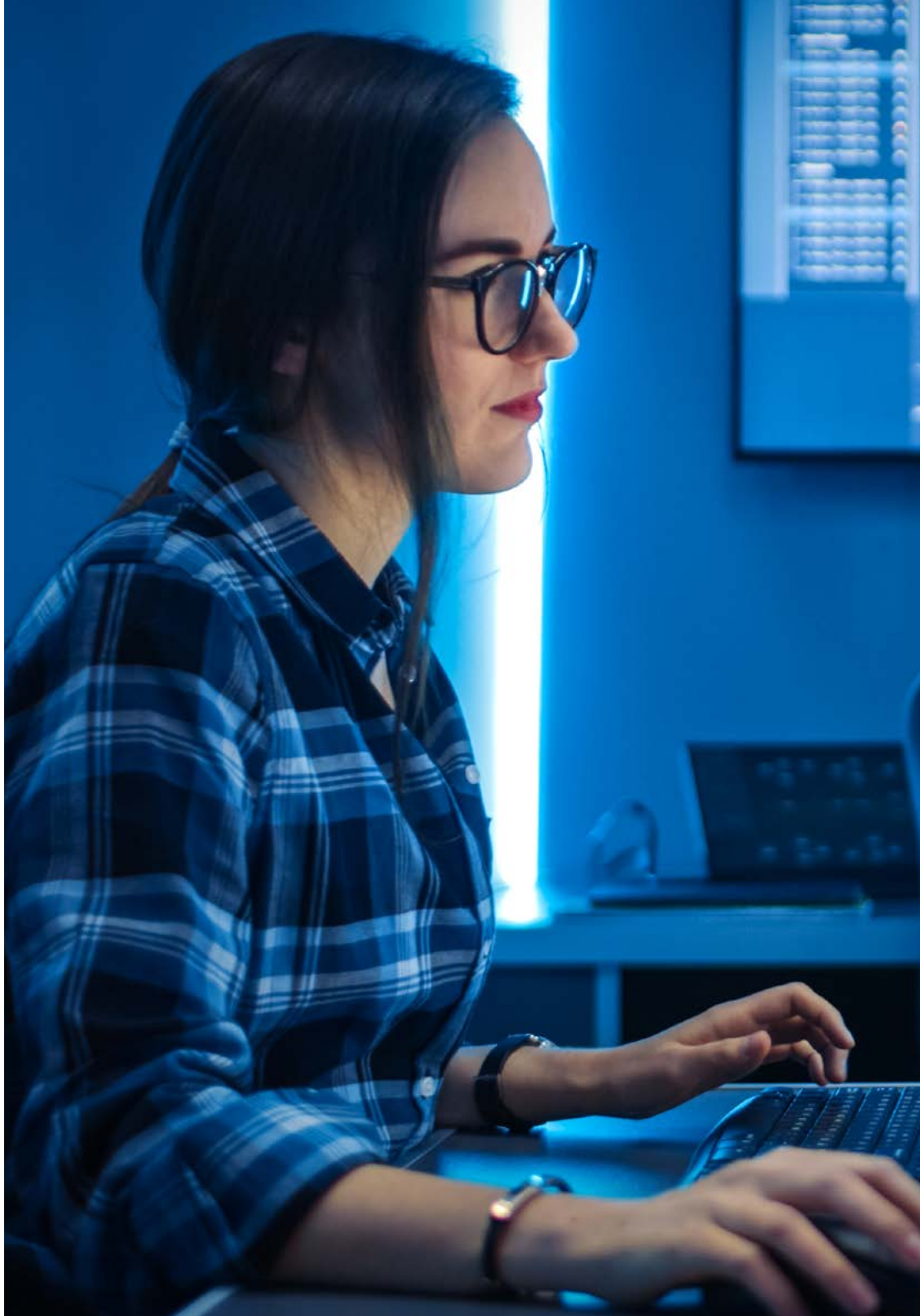
1.3. Fundamentos do Windows
- 1.3.1. Formato do arquivo PE (*Portable Executable*)
- 1.3.2. Processos e *Threads*
- 1.3.3. Sistema de arquivos e registro
- 1.3.4. *Windows Defender*

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

Módulo 2. Fundamentos forenses e DFIR

2.1. Forense digital
- 2.1.1. História e evolução da computação forense
- 2.1.2. Importância da computação forense na cibersegurança
- 2.1.3. História e evolução da computação forense

2.2. Fundamentos de informática forense
- 2.2.1. Cadeia de custódia e sua implementação
- 2.2.2. Tipos de evidência digital
- 2.2.3. Processos de aquisição de evidências

2.3. Sistemas de arquivos e estrutura de dados
- 2.3.1. Principais sistemas de arquivos
- 2.3.2. Métodos de ocultação de dados
- 2.3.3. Análise de metadados e atributos de arquivos

2.4. Análise de sistemas operacionais
- 2.4.1. Análise forense de sistemas Windows
- 2.4.2. Análise forense de sistemas Linux
- 2.4.3. Análise forense de sistemas macOS

2.5. Recuperação de dados e análise de disco
- 2.5.1. Recuperação de dados de mídias danificadas
- 2.5.2. Ferramentas de análise de disco
- 2.5.3. Interpretação de tabelas de alocação de arquivos

2.6. Análise de rede e tráfego
- 2.6.1. Captura e análise de pacotes de rede
- 2.6.2. Análise de registros de *firewall*
- 2.6.3. Detecção de intrusão de rede

2.7. *Malware* e análise de código malicioso
- 2.7.1. Classificação de *Malware* e suas características
- 2.7.2. Análise estática e dinâmica de *malware*
- 2.7.3. Técnicas de desmontagem e depuração

2.8. Análise de registros e eventos
- 2.8.1. Tipos de registros em sistemas e aplicativos
- 2.8.2. Interpretação de eventos relevantes
- 2.8.3. Ferramentas de análise de registros

2.9. Resposta a incidentes de segurança
- 2.9.1. Processo de resposta a incidentes
- 2.9.2. Criação de um plano de resposta a incidentes
- 2.9.3. Coordenação com equipes de segurança

2.10. Apresentação de evidências e questões legais
- 2.10.1. Regras de evidência digital no campo jurídico
- 2.10.2. Preparação de relatórios forenses
- 2.10.3. Comparecimento ao julgamento como testemunha especializada

Módulo 3. Exercícios de *Rede Team* Avançados

3.1. Técnicas avançadas de reconhecimento
- 3.1.1. Enumeração avançada de subdomínios
- 3.1.2. *Google Dorking* avançado
- 3.1.3. Redes Sociais e theHarvester

3.2. Campanhas de *phishing* avançadas
- 3.2.1. O que é *Reverse-Proxy Phishing*
- 3.2.2. *2FA Bypass* com Evilginx
- 3.2.3. Exfiltração de dados

3.3. Técnicas avançadas de persistência
- 3.3.1. *Golden Tickets*
- 3.3.2. *Silver Tickets*
- 3.3.3. Técnica *DCShadow*

3.4. Técnicas avançadas de evasão
- 3.4.1. *Bypass* de AMSI
- 3.4.2. Modificação de ferramentas existentes
- 3.4.3. Ofuscação de *Powershell*

3.5. Técnicas avançadas de movimento lateral
- 3.5.1. *Pass-the-Ticket* (PtT)
- 3.5.2. *Overpass-the-Hash (Pass-the-Key)*
- 3.5.3. NTLM Relay

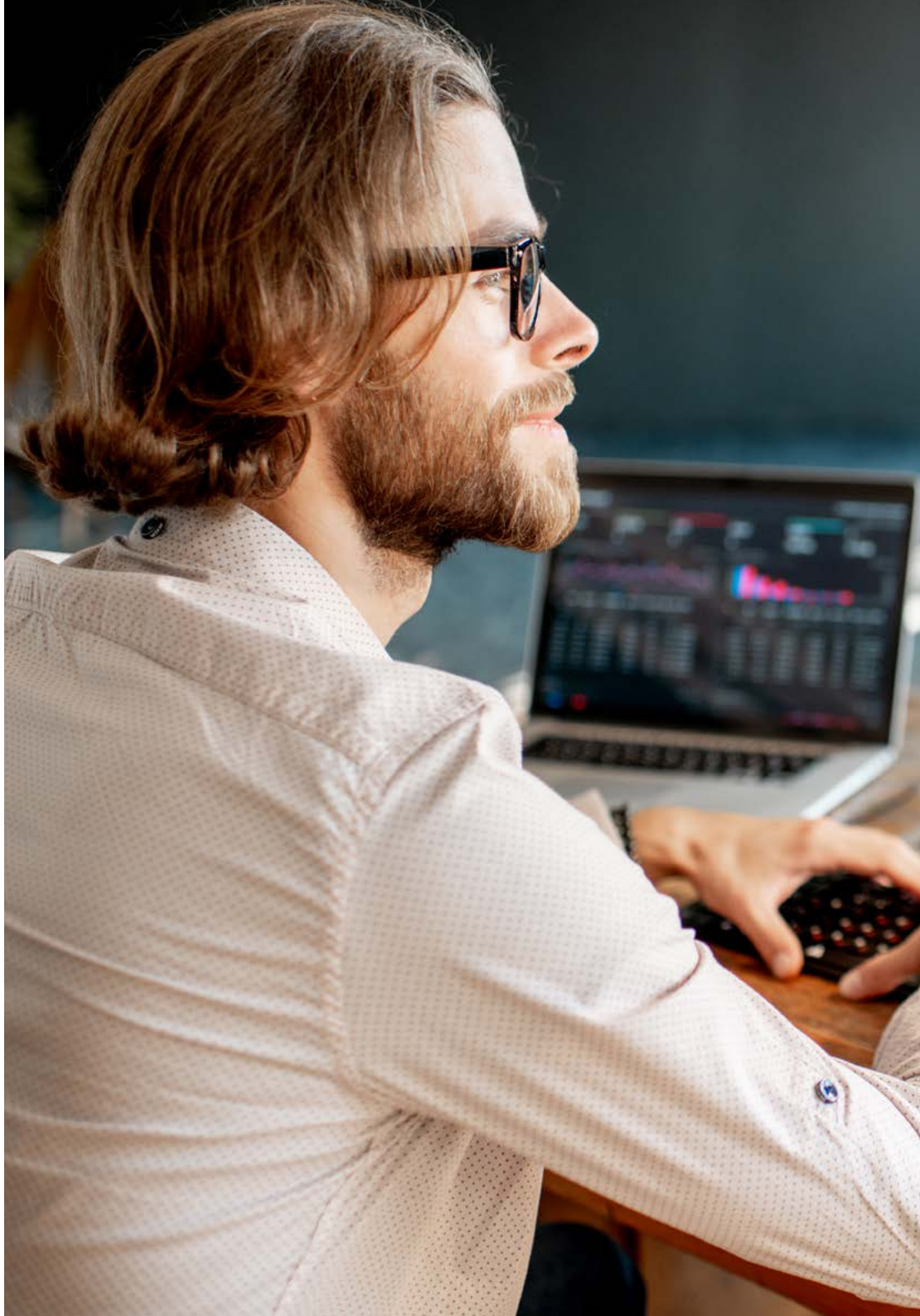
3.6. Técnicas avançadas de pós-exploração
- 3.6.1. *Dump* de LSASS
- 3.6.2. *Dump* de SAM
- 3.6.3. Ataque *DCSync*

3.7. Técnicas avançadas de *pivoting*
- 3.7.1. O que él *pivoting*
- 3.7.2. Túneis com SSH
- 3.7.3. *Pivoting* com Chisel

3.8. Intrusões físicas
- 3.8.1. Vigilância e reconhecimento
- 3.8.2. *Tailgating e Piggybacking*
- 3.8.3. *Lock-Picking*

3.9. Ataques Wi-Fi
- 3.9.1. Ataques a WPA/WPA2 PSK
- 3.9.2. Ataques de Rogue AP
- 3.9.3. Ataques a WPA2 *Enterprise*

3.10. Ataques RFID
- 3.10.1. Leitura de cartões RFID
- 3.10.2. Manuseio de cartões RFID
- 3.10.3. Criação de cartões clonados



Não perca esta oportunidade de impulsionar sua carreira por meio deste programa inovador. Torne-se um um especialista em cibersegurança!”

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

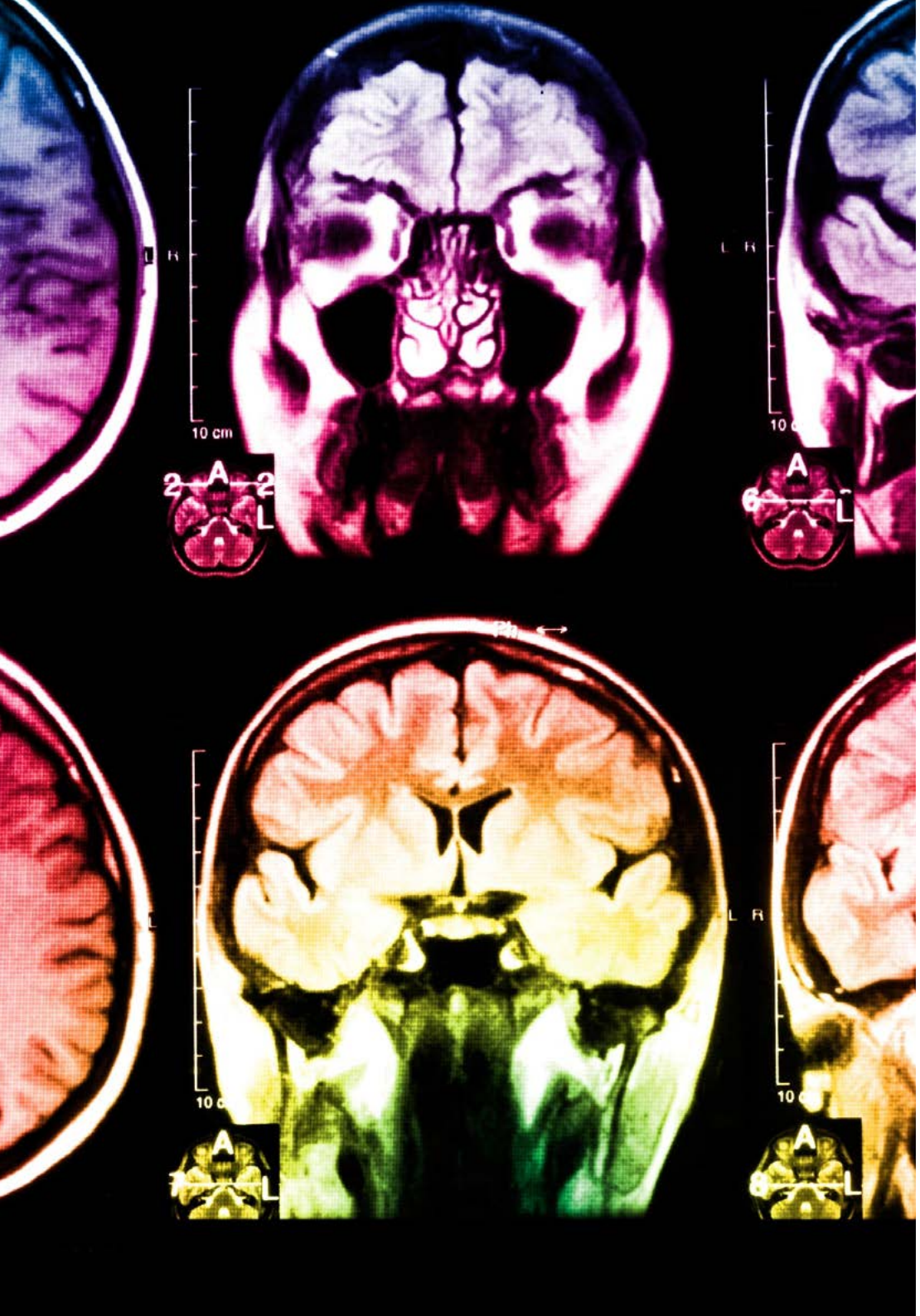
A TECH utiliza de maneira eficaz a metodologia do estudo de caso com um sistema de aprendizagem 100% online, baseado na repetição, combinando elementos didáticos diferentes em cada aula.

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.

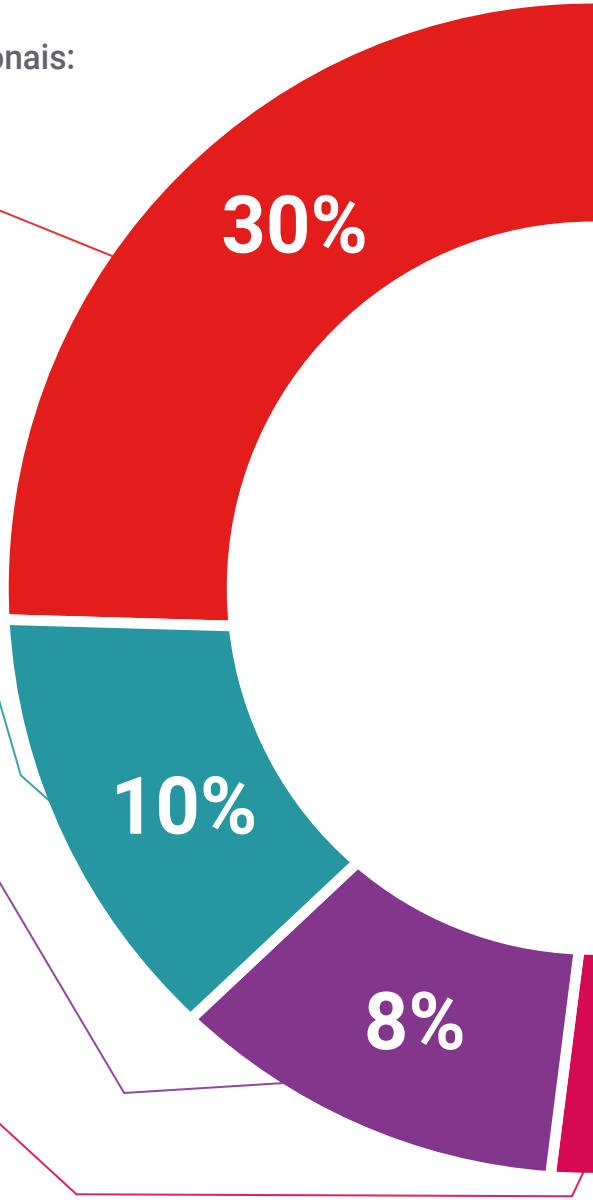
O "Learning from an expert" fortalece o conhecimento e a memória, além de gerar segurança para a tomada de decisões difíceis no futuro.

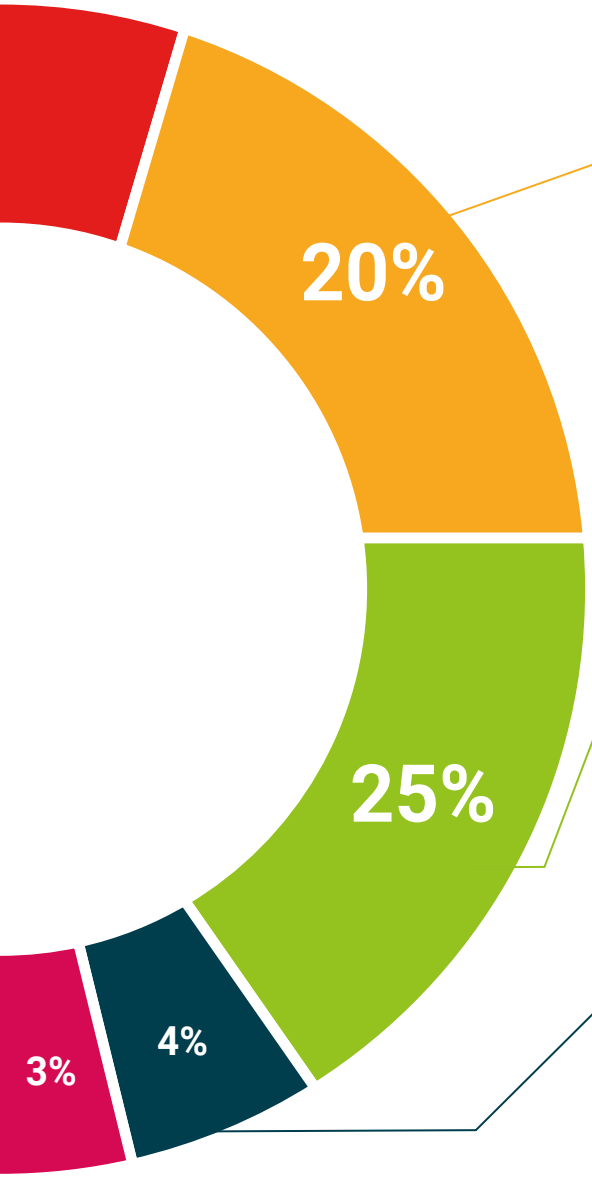
Práticas de habilidades e competências

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 Programa Avançado de Cibersegurança Red Team garante, além da capacitação mais rigorosa e atualizada, o acesso a um título de Programa Avançado 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 **Programa Avançado de Segurança Cibernética em Red Team** conta com o conteúdo mais completo e atualizado do mercado.

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

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

Título: **Programa Avançado de Segurança Cibernética em Red Team**

Modalidade: **online**

Duração: **6 meses**


tech universidade tecnológica

Outorga o presente

CERTIFICADO

a

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

por ter concluído e aprovado com sucesso o

PROGRAMA AVANÇADO

de

Segurança Cibernética em Red Team

Este é um curso próprio desta Universidade, com duração de 450 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

Programa Avançado
Cibersegurança Red Team

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

Programa Avançado
Cibersegurança Red Team

tech universidade tecnológica