

Curso

Gestão de Equipes de Pentesting



**tech** universidade  
tecnológica

## Curso Gestão de Equipes de Pentesting

- » 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/gestao-equipes-pentestin](http://www.techtitute.com/br/informatica/curso/gestao-equipes-pentestin)

# 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

A gestão das equipes de pentesting é uma questão fundamental para as instituições. A razão para isso é que ele permite o uso máximo dos recursos humanos e tecnológicos disponíveis, realizando testes de penetração. Assim, as empresas estão exigindo cada vez mais a incorporação de especialistas em cibersegurança para identificar e resolver problemas de forma otimizada. Em vista do aumento do *hacking* informático, esses profissionais devem atualizar seus conhecimentos habitualmente e aplicar as ferramentas mais modernas com o objetivo de prevenir ataques cibernéticos. Por esse motivo, a TECH está lançando um programa inovador para que os alunos implementem as táticas mais avançadas em *pentesting*. Além disso, este programa é baseado em uma modalidade 100% online, garantindo assim a conveniência e a flexibilidade dos alunos.



```
// Begin Actor overrides
virtual void PostInitializeComponents() override;
virtual void Tick(float DeltaSeconds) override;
virtual void ReceiveHit(class UPawn* Instigator, class UDamageType* DamageType, const FVector& Location, const FHitResult& HitResult) override;
virtual void FellOutOfWorld(const class UDamageType* DamageType) override;
// End Actor overrides

// Begin Pawn overrides
virtual void SetupPlayerInputComponent(class UInputComponent* InputComponent) override;
virtual float TakeDamage(float Damage, struct FDamageEvent const& Event, class AActor* Instigator, class UDamageType* DamageType) override;
virtual void TurnOff() override;
// End Pawn overrides

/** Identifies if pawn is in its dying state.
 * @see UPROPERTY(VisibleAnywhere, BlueprintReadWrite)
 */
uint32 bIsDying:1;

/** replicating death on client
 * @see UFUNCTION()
 */
void OnRep_Dying();

/** Returns true if the pawn is in its dying state.
 * @see UFUNCTION()
 */
virtual bool IsDying() const;

```

“

Apresente o mais poderoso arsenal de auditoria ofensiva por meio de 150 horas do melhor ensino digital”

Graças às auditorias realizadas por especialistas em gestão de equipes, as entidades ficam cientes de seus possíveis obstáculos, riscos e problemas antes que seja tarde demais. Nesse sentido, os pentesters facilitam a comunicação entre os membros da equipe, permitindo que eles compartilhem conhecimento e informações. Além disso, os recursos são monitorados e as estratégias de controle são aplicadas para atingir os objetivos definidos pelas organizações (tanto de curto quanto de longo prazo).

Ciente dessa realidade, a TECH desenvolveu uma formação pioneira que abrange desde a análise de vulnerabilidades até técnicas avançadas de intrusão. O programa se concentrará em uma série de metodologias ofensivas voltadas para a segurança, entre as quais se destaca a Cyber Security Kill Chain. Além disso, ele incentivará a criatividade por meio da técnica de think outside the box e, assim, promoverá soluções inovadoras para se diferenciar das demais. Ele também explorará as diferentes funções do *pentesting*, enfatizando a necessidade de uma pesquisa aprofundada. Além disso, se aprofundará na ferramenta Metasploit, com o objetivo de realizar ataques simulados de forma controlada. Por fim, ele descreverá os principais desafios que afetam a segurança ofensiva e incentivará que eles sejam transformados em oportunidades para que os alunos demonstrem todo o seu potencial e engenhosidade.

Deve-se observar que, para reforçar o domínio dos conteúdos, este programa de ensino aplica o sistema de última geração *Relearning*. A TECH é pioneira no uso desse modelo de ensino, que promove a assimilação de conceitos complexos por meio da reiteração natural e progressiva dos mesmos. Nessa linha, o programa também se baseia em materiais de vários formatos, como infográficos, resumos interativos e vídeos explicativos. Tudo isso em um conveniente modo 100% online, que permite que os alunos ajustem seus horários de acordo com suas responsabilidades e circunstâncias pessoais.

Este **Curso de Gestão de Equipes de Pentesting** conta com o conteúdo mais completo e atualizado do mercado. Suas principais características são:

- O desenvolvimento de estudos de casos práticos apresentados por especialistas em Gestão de Equipes de Pentesting
- 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 deseja avançar profissionalmente na sua carreira? Torne-se um especialista em Inteligência de Código Aberto com esta capacitação”*

“

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

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 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.

*Você aprofundará suas habilidades de pesquisa para realizar a pesquisa mais abrangente e se diferenciar dos demais.*

*Domine o programa Metasploit na melhor universidade digital do mundo, de acordo com a Forbes.*



# 02

## Objetivos

O projeto deste programa proporcionará um aprofundamento nas táticas e técnicas empregadas pelos profissionais de segurança ofensiva. Nessa linha, o foco será o desenvolvimento de habilidades e estratégias de teste de penetração para explorar vulnerabilidades em sistemas e redes. Isso proporcionará um conhecimento sólido de como conduzir avaliações de segurança de maneira eficaz e ética. Os alunos participarão de sessões práticas para aprender conceitos teóricos em ambientes simulados, preparando-os para enfrentar os desafios do mundo real no *Red Team*.



“

*Deseja implementar as medidas de segurança ofensivas mais inovadoras? Tudo graças a este programa de 6 semanas “*



## 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.



*Durante seu processo de aprendizagem, você terá o apoio dos melhores profissionais em Cibersegurança”*





## Objetivos específicos

---

- ♦ Familiarizar o aluno com as metodologias de teste de penetração, incluindo as principais fases, como coleta de informações, análise de vulnerabilidade, exploração e documentação
- ♦ Desenvolver habilidades práticas no uso de ferramentas especializadas de pentesting para identificar e avaliar vulnerabilidades em sistemas e redes
- ♦ Estudar e compreender as táticas, técnicas e procedimentos usados por agentes mal-intencionados, permitindo a identificação e a simulação de ameaças
- ♦ Aplicar os conhecimentos teóricos em cenários práticos e simulações, enfrentando desafios reais, a fim de fortalecer as habilidades de Pentesting
- ♦ Desenvolver habilidades eficazes de documentação, criando relatórios detalhados que reflitam as descobertas, as metodologias usadas e as recomendações para o aperfeiçoamento da segurança
- ♦ Praticar a colaboração eficaz em equipes de segurança ofensiva, otimizando a coordenação e a execução de atividades de pentesting

# 03

## Direção do curso

Em seu compromisso de oferecer uma educação da mais alta qualidade, a TECH tem uma equipe de professores de excelência. Esses especialistas são caracterizados por seu profundo conhecimento de cibersegurança e, ao mesmo tempo, por terem uma ampla experiência profissional. Portanto, este curso acadêmico oferece aos alunos as melhores ferramentas e táticas para adquirir várias habilidades durante o curso. Assim, os alunos têm as garantias de que precisam para se especializar em um setor digital que oferece inúmeras oportunidades de emprego.



“

*Você terá acesso a um sistema de aprendizado baseado na repetição, com um sistema de ensino natural e progressivo durante todo o programa de estudos”*

## 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 Madrid
- ♦ Colaboração com instituições educacionais para o desenvolvimento de **ciclos de formação de nível superior** em cibersegurança

## Professores

### Sr. Sergio Mora Navas

- ♦ Consultor de Cibersegurança no Grupo Oesía
- ♦ Engenheiro em Cibersegurança pela Universidad Rey Juan Carlos
- ♦ Engenheiro da Computação pela Universidade de Burgos



# 04

# Estrutura e conteúdo

Este programa é abordado a partir de uma perspectiva teórico-prática, com um corpo docente experiente que se aprofunda na análise das estratégias mais eficazes em segurança ofensiva. Para obter uma compreensão abrangente de como os agentes mal-intencionados operam, a categorização de vulnerabilidades (CAPEC, CVSS etc.) é explorada em profundidade. Além disso, é dada ênfase ao uso de scripts com o objetivo de executar scripts que automatizam tarefas em um sistema de computador, principalmente JavaScript. Também aborda os princípios da ética *hacker* a fim de compreender as implicações e consequências legais que podem surgir durante as atividades. Para isso, são analisados estudos de casos reais em que a ética da cibersegurança foi aplicada.

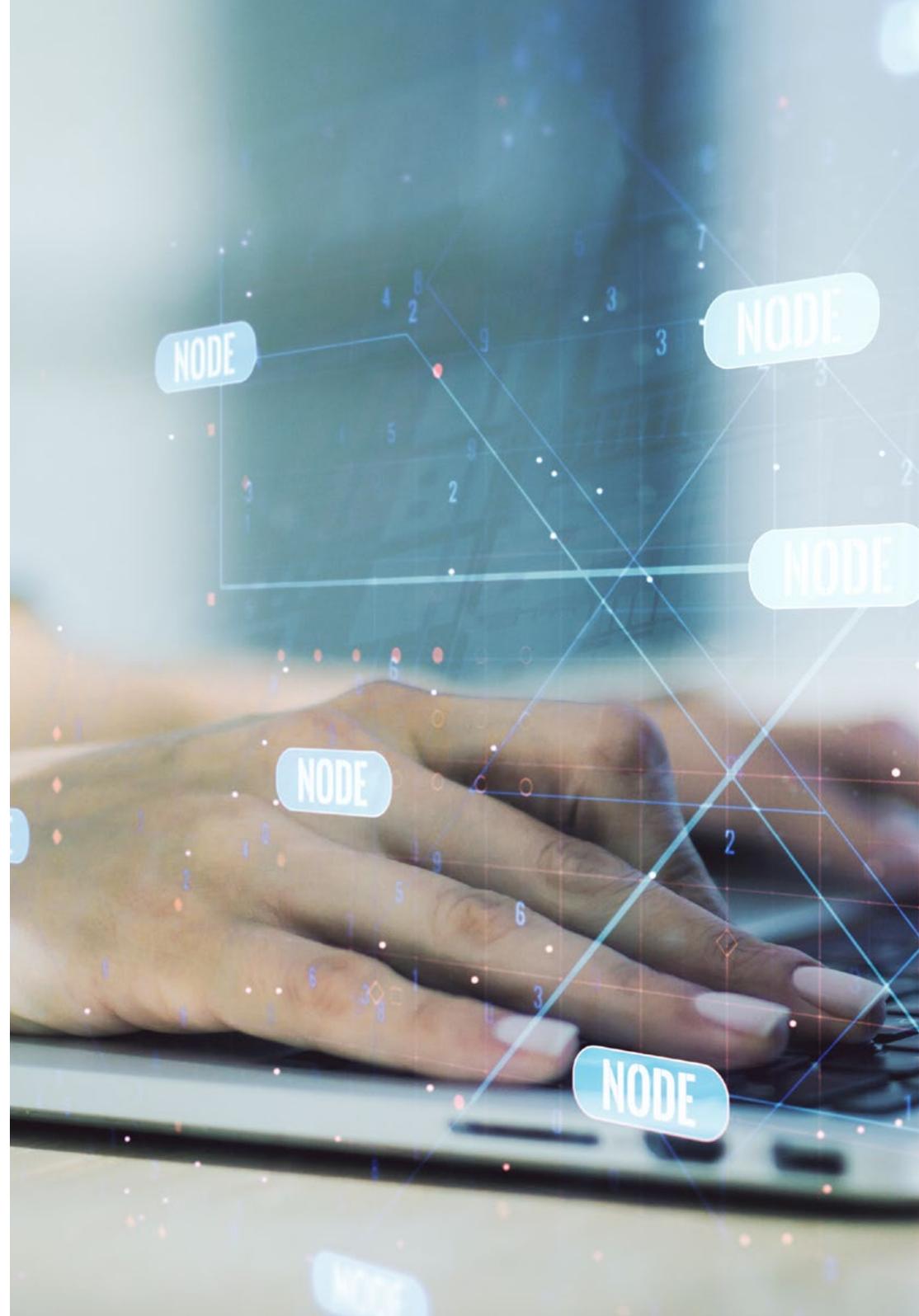


“

*Sem horários pré-estabelecidos ou cronogramas de avaliação: é disso que se trata o programa da TECH”*

## Módulo 1. Segurança ofensiva

- 1.1. Definição e contexto
  - 1.1.1. Conceitos fundamentais de segurança ofensiva
  - 1.1.2. A importância da cibersegurança na atualidade
  - 1.1.3. Desafios e oportunidades na segurança ofensiva
- 1.2. Fundamentos da cibersegurança
  - 1.2.1. Desafios iniciais e evolução das ameaças
  - 1.2.2. Marcos tecnológicos e seu impacto na cibersegurança
  - 1.2.3. Cibersegurança na era moderna
- 1.3. Base da segurança ofensiva
  - 1.3.1. Principais conceitos e terminologia
  - 1.3.2. Think Outside the Box
  - 1.3.3. Diferenças entre hacking ofensivo e defensivo
- 1.4. Metodologias de segurança ofensivas
  - 1.4.1. PTES (Penetration Testing Execution Standard)
  - 1.4.2. OWASP (Open Web Application Security Project)
  - 1.4.3. Cyber Security Kill Chain
- 1.5. Funções e responsabilidades na segurança ofensiva
  - 1.5.1. Principais perfis
  - 1.5.2. Bug Bounty Hunters
  - 1.5.3. Researching a arte de pesquisar
- 1.6. Arsenal do auditor ofensivo
  - 1.6.1. Sistemas operacionais de Hacking
  - 1.6.2. Introdução ao C2
  - 1.6.3. Metasploit: Fundamentos e uso
  - 1.6.4. Recursos úteis
- 1.7. OSINT Inteligência em Fontes Abertas
  - 1.7.1. Fundamentos da OSINT
  - 1.7.2. Técnicas e ferramentas de OSINT
  - 1.7.3. Aplicativos OSINT em segurança ofensiva



- 1.8. Scripting Introdução à automatização
  - 1.8.1. Fundamentos de scripting
  - 1.8.2. Scripting em Bash
  - 1.8.3. Scripting em Python
- 1.9. Categorização de vulnerabilidades
  - 1.9.1. CVE (Common Vulnerabilities and Exposure)
  - 1.9.2. CWE (Common Weakness Enumeration)
  - 1.9.3. CAPEC (Common Attack Pattern Enumeration and Classification)
  - 1.9.4. CVSS (Common Vulnerability Scoring System)
  - 1.9.5. MITRE ATT & CK
- 1.10. Ética e hacking
  - 1.10.1. Princípios de ética hacker
  - 1.10.2. A linha entre hacking ético e hacking malicioso
  - 1.10.3. Implicações e consequências legais
  - 1.10.4. Estudos de caso: Situações éticas na cibersegurança



*Tenha acesso a uma biblioteca repleta de recursos multimídia em diferentes formatos audiovisuais”*

# 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

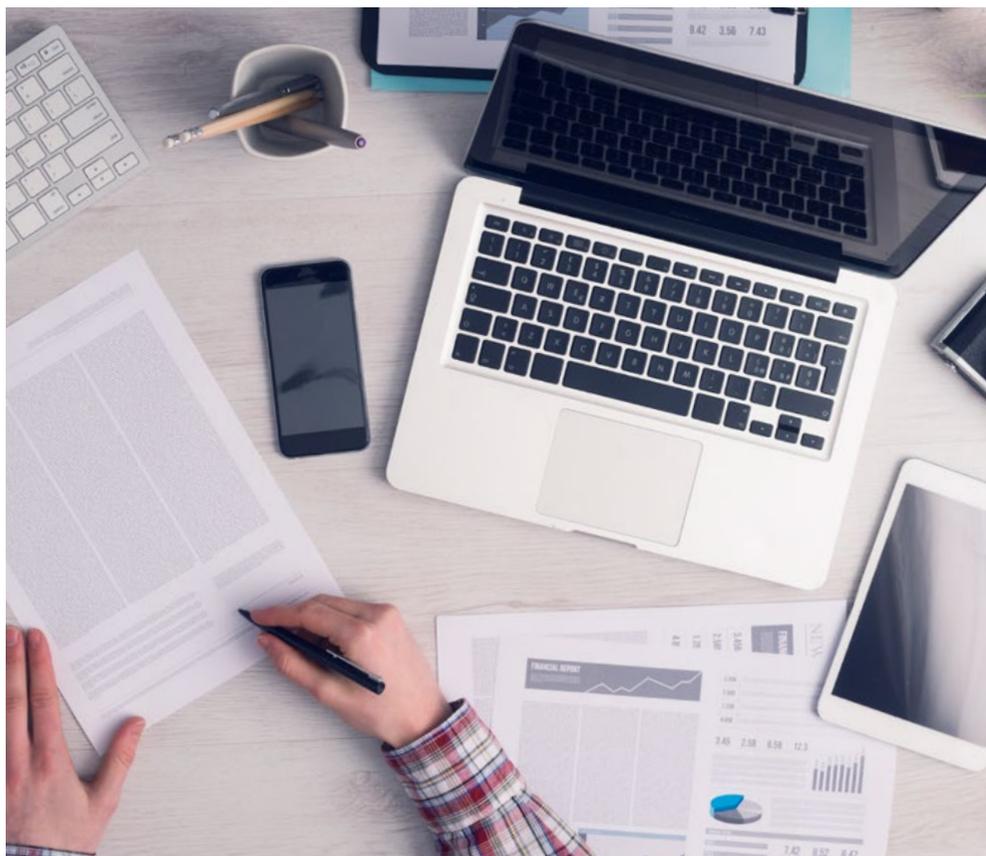
Nosso programa oferece um método revolucionário para desenvolver as habilidades e o conhecimento. Nosso objetivo é fortalecer as competências em um contexto de mudança, competitivo e altamente exigente.

“

*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.



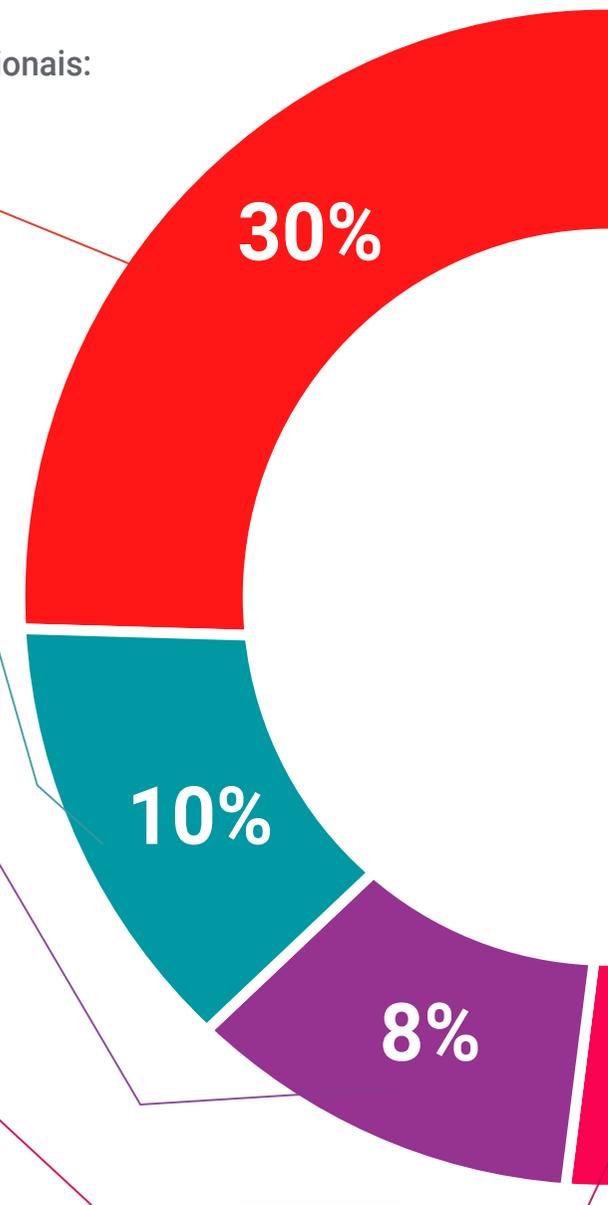
#### Práticas de habilidades e competências

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 Gestão de Equipes de Pentesting 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 Gestão de Equipes de Pentesting** 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 Gestão de Equipes de Pentesting**

Modalidade: **online**

Duração: **6 semanas**



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

futuro  
saúde confiança pessoas  
informação orientadores  
educação certificação ensino  
garantia aprendizagem  
instituições tecnologia  
comunidade compreensão  
atenção personalizada  
conhecimento inovação  
presente qualidade  
desenvolvimento sustentabilidade

**tech** universidade  
tecnológica

Curso  
Gestão de Equipes de  
Pentesting

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

Curso

Gestão de Equipes de Pentesting

