Programa Avançado
Cibersegurança Ofensiva

tech universidade tecnológica

tech universidade tecnológica

Programa Avançado
Cibersegurança Ofensiva

- 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-ofensiva

Índice

01

Apresentação

A cibersegurança é um aspecto essencial para que as instituições protejam seus ativos digitais, mantenham sua reputação social e se protejam contra a espionagem dos concorrentes. Por isso, cada vez mais empresas estão solicitando a incorporação de especialistas em TI em seus organogramas, a fim de evitar consequências que poderiam até mesmo afetar suas capacidades financeiras. Nesse contexto, esses especialistas precisam atualizar constantemente seus conhecimentos e habilidades para acompanhar as técnicas do crime cibernético. Por esse motivo, a TECH desenvolveu um Programa Avançado inovador, no qual as ameaças serão identificadas e mitigadas. Deve-se observar que todo o programa será ministrado em um modo 100% online, para garantir que os alunos tenham maior conveniência e flexibilidade.

Você aprenderá mais sobre o protocolo Kerberos e protegerá as informações em ambientes de rede”

Todos os dias, a mídia relata casos de hackers que prejudicam instituições ao acessar seus bancos de dados. As consequências desses ataques são graves, interrompendo as operações e impedindo o funcionamento eficaz das empresas. Na verdade, isso pode afetar diretamente sua economia, levando a multas por não conformidade com regulamentos e limitações de receita.

Nesse sentido, a TECH criou uma qualificação de ponta para detectar as técnicas de invasão mais utilizadas, bem como as melhores estratégias para lidar com elas. Sob a orientação de uma equipe de professores experientes, o programa de estudos estabelecerá as bases essenciais para entender como os hackers pensam. Além disso, fornecerá uma variedade de soluções, com o objetivo de fornecer infraestruturas seguras para a gestão de certificados digitais em uma rede corporativa.

Da mesma forma, os profissionais abordarão a preparação ideal de ambientes virtuais, graças à configuração de máquinas virtuais ou snapshots. Além disso, o malware será analisado, sondando as chamadas com o API Monitor e observando as solicitações de rede com o TCPView. Os alunos aprenderão conceitos teóricos em ambientes simulados, preparando-os para os desafios do mundo real na Cibersegurança Ofensiva. Por fim, será dada ênfase à ética e à responsabilidade social que devem caracterizar os especialistas nesse campo.

Para consolidar o domínio de todos esses conteúdos, o Programa Avançado aplica o inovador sistema 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. O programa também se baseia em materiais em vários formatos, como vídeos explicativos, resumos interativos e infográficos. Tudo isso em um conveniente modo 100% online, que permite que cada pessoa ajuste seu horário de acordo com suas responsabilidades e disponibilidade.

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

- O desenvolvimento de estudos de caso apresentados por especialistas em Cibersegurança Ofensiva
- O conteúdo gráfico, esquemático e eminentemente prático do plano de estudos fornece informações completas e práticas sobre as disciplinas que são essenciais para a prática profissional
- 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

Desenvolva suas habilidades como auditor ofensivo e embarque em um novo desafio profissional nas empresas digitais de maior prestígio”

Você alcançará seus objetivos por meio das ferramentas didáticas da TECH, incluindo vídeos explicativos e resumos interativos"

Quer se tornar um Big Bounty Hunter? Você poderá detectar qualquer vulnerabilidade na Internet graças a esse programa.

Em apenas 6 meses, você dominará a gestão de identidade no Azure AD. Matricule-se já!.

A equipe de professores deste programa inclui profissionais desta área, cuja experiência é somada a esta capacitação, além de reconhecidos especialistas de conceituadas sociedades científicas 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.

02

Objetivos

Esse programa oferece uma experiência educacional única, que se destaca por sua abordagem prática e inovadora da cibersegurança. Dessa forma, os alunos aprenderão sobre tudo, desde a análise de vulnerabilidades até técnicas avançadas de invasão. Nessa linha, serão fornecidas medidas ideais para avaliar e fortalecer os diferentes sistemas cibernéticos. Além disso, será dada ênfase às responsabilidades legais e éticas que os especialistas nesse campo devem adotar.

Reduza as ameaças de malware com a melhor universidade digital do mundo, de acordo com a Forbes"

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

Objetivos específicos

Módulo 1. Segurança ofensiva

- 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*

Módulo 2. Ataques a Redes e Sistemas Windows

- Desenvolver habilidades para identificar e avaliar vulnerabilidades específicas nos sistemas operacionais Windows
- Aprenda as táticas avançadas usadas pelos atacantes para se infiltrar e persistir em redes baseadas no Windows
- Adquirir habilidades em estratégias e ferramentas para atenuar ameaças específicas direcionadas aos sistemas operacionais Windows
- Familiarizar o aluno com as técnicas de análise forense aplicadas aos sistemas Windows, facilitando a identificação e a resposta a incidentes

- Aplicar o conhecimento teórico em ambientes simulados, participando de exercícios práticos para entender e combater ataques específicos a sistemas Windows
- Aprender estratégias específicas para proteger ambientes corporativos usando sistemas operacionais Windows, levando em consideração as complexidades das infraestruturas corporativas
- Desenvolver competências para avaliar e melhorar as configurações de segurança em sistemas Windows, garantindo a implementação de medidas eficazes
- Promover práticas éticas e legais na execução de ataques e testes em sistemas Windows, considerando os princípios éticos da cibersegurança
- Manter o aluno atualizado com as últimas tendências e ameaças em ataques a sistemas Windows, garantindo a relevância e a eficácia contínuas das habilidades adquiridas

Módulo 3. 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

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

03

Direção do curso

Em seu compromisso de oferecer excelência educacional, a TECH conta com um corpo docente de prestígio. Vale ressaltar que esses especialistas têm um extenso histórico profissional, tendo feito parte de renomadas empresas dedicadas à Cibersegurança Ofensiva. Por esse motivo, as atividades acadêmicas incluirão os recursos e as tecnologias mais avançados nesse campo. Além disso, será oferecida uma abordagem abrangente para atender às expectativas dos formandos de se especializarem em um campo que lhes proporcionará muitas oportunidades.

Você terá o apoio de um corpo docente de profissionais renomados de Cibersegurança Ofensiva”

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

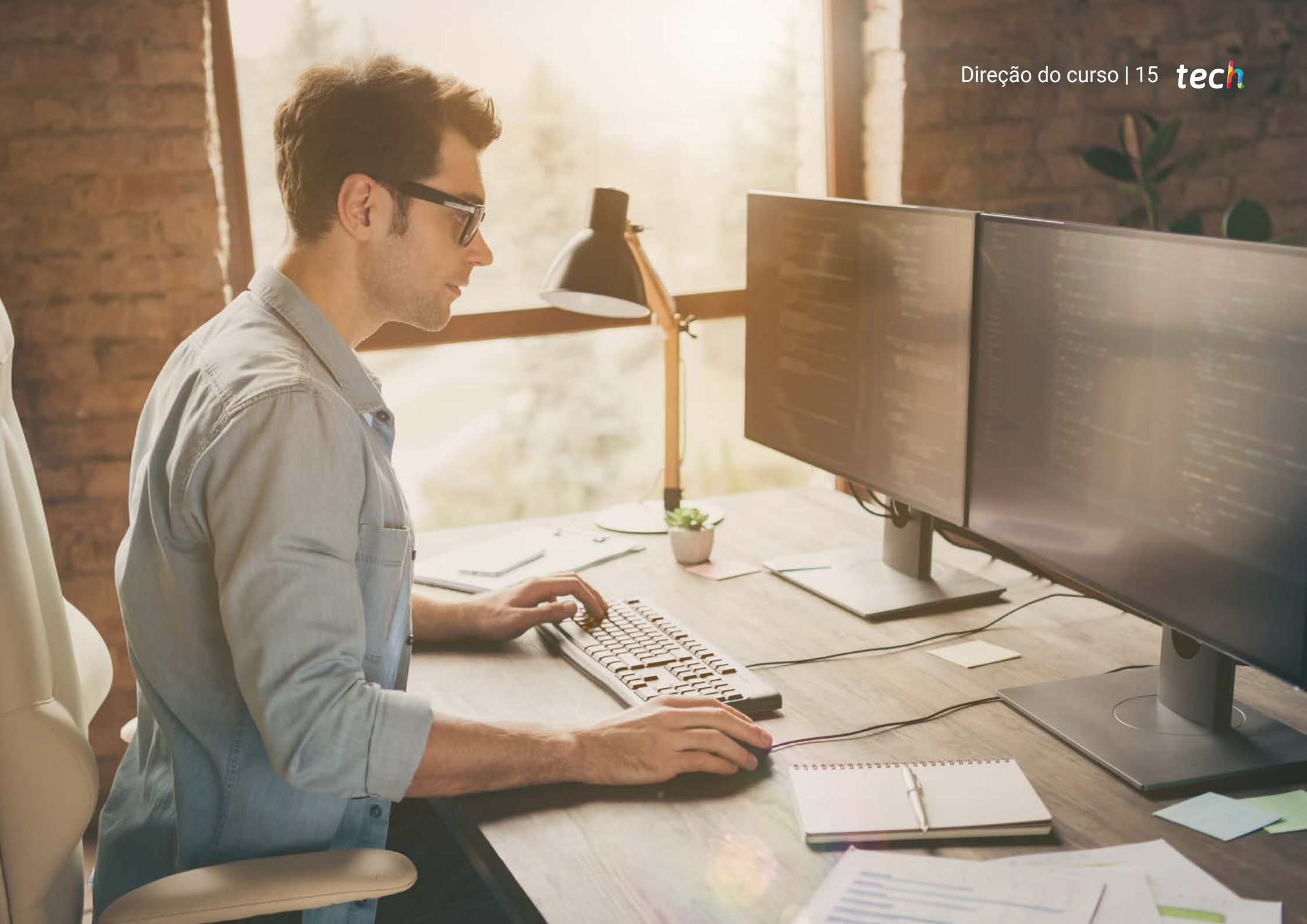
Professores

Sr. Yuba González Parrilla

- Coordenador da linha de segurança ofensiva e red team
- Especialista em gestão de projetos *Predictive* no Project Management Institute
- Especialista em *SmartDefense*
- Especialista em *Web Application Penetration Tester* no eLearnSecurity
- *Junior Penetration Tester* no eLearnSecurity
- Graduado em Engenharia da Computação pela Universidade Politécnica de Madri

Sr. Alejandro Gallego Sánchez

- Pentester no Grupo Oesia
- Consultor de Cibersegurança na Integración Tecnológica Empresarial, S.L
- Técnico Audiovisual na Ingeniería Audiovisual S.A
- Formado em Engenharia de Cibersegurança pela Universidade Rey Juan Carlos



04

Estrutura e conteúdo

Este programa está estruturado em 3 módulos: Segurança ofensiva, ataque a redes ou sistemas Windows, e análise e desenvolvimento de *Malware*. Ao longo do programa, será oferecida uma perspectiva prática sobre a detecção precoce de ameaças. Nesse sentido, a criatividade dos alunos será incentivada a superar os desafios por meio de soluções inovadoras. Além disso, a categorização das vulnerabilidades, entre as quais a CVE é uma das mais importantes. Além disso, investigará técnicas avançadas para a análise de *malware*, a fim de fortalecer a segurança em ambientes cibernéticos.

Você terá acesso a um sistema de aprendizado baseado na repetição, com ensino natural e progressivo ao longo de todo o programa de estudos"

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

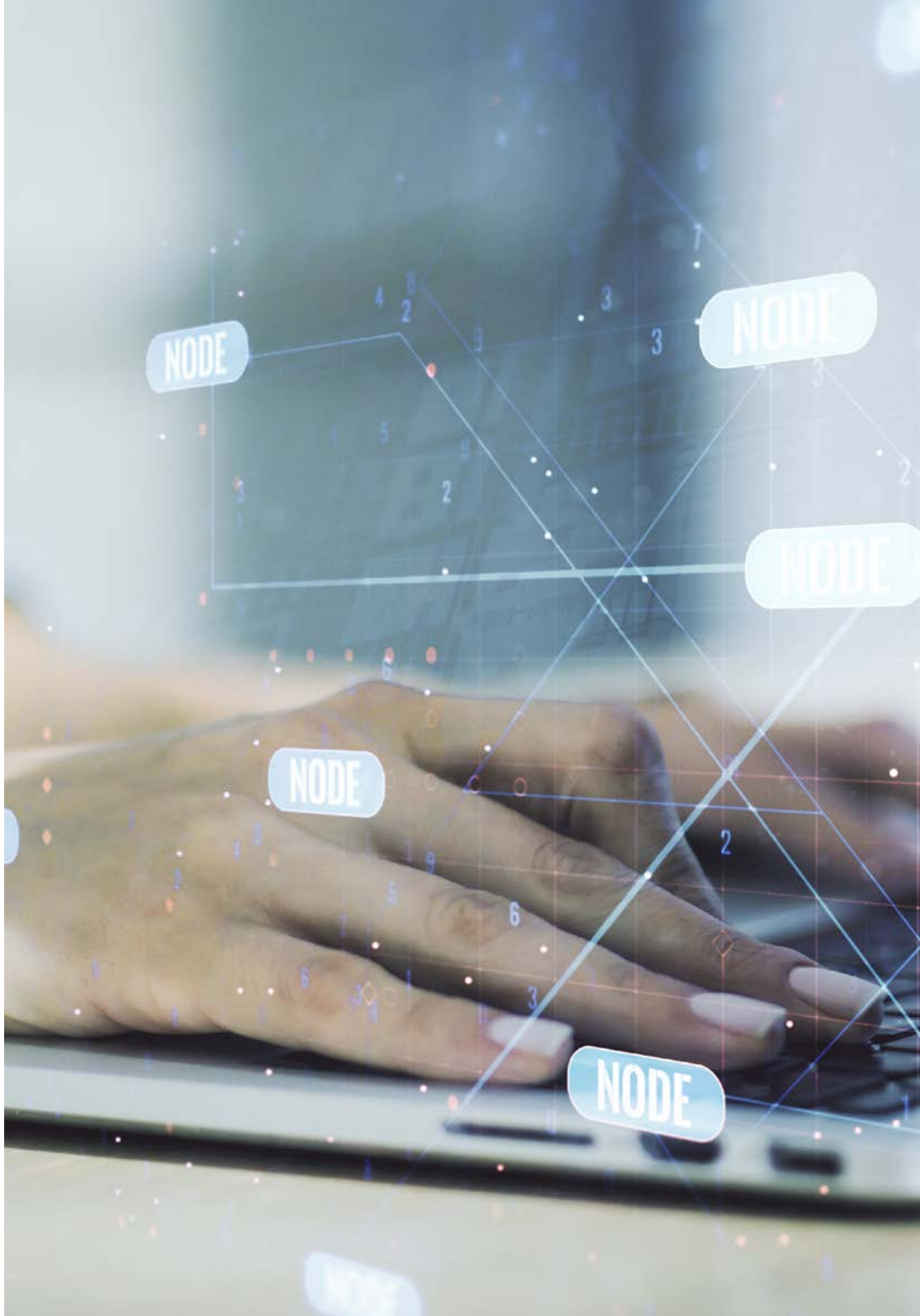
1.4. Metodologias de segurança ofensivas
- 1.4.1. PTES (*Penetration Testing Execution Standard*)
- 1.4.2. OWASP (*Open Web Application Security Project*)
- 1.4.3. *Cyber Security Kill Chain*

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 da pesquisa

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

Módulo 2. Ataques a Redes e Sistemas Windows

2.1. Windows e Diretório Ativo
- 2.1.1. História e evolução do Windows
- 2.1.2. Noções básicas sobre o Diretório Ativo
- 2.1.3. Funções e serviços do Diretório Ativo
- 2.1.4. Arquitetura geral do Diretório Ativo

2.2. Redes em ambientes de Diretório Ativo
- 2.2.1. Protocolos de rede no Windows
- 2.2.2. DNS e seu funcionamento no Diretório Ativo
- 2.2.3. Ferramentas de diagnóstico de rede
- 2.2.4. Implementação de redes no Diretório Ativo

2.3. Autenticação e autorização no Diretório Ativo
- 2.3.1. Processo e fluxo de autenticação
- 2.3.2. Tipos de credenciais
- 2.3.3. Armazenamento e gestão de credenciais
- 2.3.4. Segurança de autenticação

2.4. Permissões e políticas no Diretório Ativo
- 2.4.1. GPOs
- 2.4.2. Implementação e gestão de GPOs
- 2.4.3. Gestão de licençasno Diretório Ativo
- 2.4.4. Vulnerabilidades e mitigações em licenças

2.5. Noções básicas do Kerberos
- 2.5.1. O que é o Kerberos?
- 2.5.2. Componentes e funcionamento
- 2.5.3. Tickets no Kerberos
- 2.5.4. Kerberos no contexto do Diretório Ativo

2.6. Técnicas avançadas do Kerberos
- 2.6.1. Ataques comuns do Kerberos
- 2.6.2. Mitigações e proteções
- 2.6.3. Monitoramento de tráfego Kerberos
- 2.6.4. Ataques avançados do Kerberos

2.7. *Active Directory Certificate Services* (ADCS)
- 2.7.1. Noções básicas de PKI
- 2.7.2. Funções e componentes do ADCS
- 2.7.3. Configuração e implantação do ADCS
- 2.7.4. Segurança em ADCS

2.8. Ataques e defesas em Active Directori Certificate Services (ADCS)
- 2.8.1. Vulnerabilidades comuns no ADCS
- 2.8.2. Ataques e técnicas de exploração
- 2.8.3. Defesas e mitigações
- 2.8.4. Monitoramento e auditoria de ADCS

2.9. Auditoria do Diretório Ativo
- 2.9.1. Importância da auditoria no Diretório Ativo
- 2.9.2. Ferramentas de auditoria
- 2.9.3. Detecção de anomalias e comportamentos suspeitos
- 2.9.4. Resposta a incidentes e recuperação

2.10. Azure AD
- 2.10.1. Fundamentos do Azure AD
- 2.10.2. Sincronização com o diretório ativo local
- 2.10.3. Gestão de identidades no Azure AD
- 2.10.4. Integração com aplicativos e serviços

Módulo 3. Análise e Desenvolvimento de *Malware*

3.1. Análise e Desenvolvimento de *Malware*
- 3.1.1. História e evolução do *malware*
- 3.1.2. Classificação e tipos de *Malware*
- 3.1.3. Análises de *malware*
- 3.1.4. Desenvolvimento de *malware*

3.2. Preparação do ambiente
- 3.2.1. Configuração de máquina virtual e *Snapshots*
- 3.2.2. Ferramentas de análise de malware
- 3.2.3. Ferramentas de desenvolvimento de malware

3.3. Fundamentos do Windows
- 3.3.1. Formato do arquivo PE (*Portable Executable*)
- 3.3.2. Processos e *Threads*
- 3.3.3. Sistema de arquivos e registro
- 3.3.4. *Windows Defender*

3.4. Técnicas de *Malware* básicas
- 3.4.1. Geração de *shellcode*
- 3.4.2. Execução de *shellcode* no disco
- 3.4.3. Disco vs memória
- 3.4.4. Execução de *shellcode* na memória

3.5. Técnicas de *malware* intermediárias
- 3.5.1. Persistência no Windows
- 3.5.2. Pasta inicial
- 3.5.3. Chaves de registro
- 3.5.4. Protetores de tela

3.6. Técnicas de *malware* avançadas
- 3.6.1. Cifrado de *shellcode* (XOR)
- 3.6.2. Cifrado de *shellcode* (RSA)
- 3.6.3. Ofuscação de *strings*
- 3.6.4. Injeção de processos

3.7. Análise estática de ***malware***
- 3.7.1. Analisando *packers* com DIE (*Detect It Easy*)
- 3.7.2. Analisando seções com o PE-Bear
- 3.7.3. Descompilação com Ghidra

3.8. Análise dinâmica de ***malware***
- 3.8.1. Observando o comportamento com o Process Hacker
- 3.8.2. Análise de chamadas com o API Monitor
- 3.8.3. Análise de alterações no registro com o Regshot
- 3.8.4. Observação de solicitações de rede com o TCPView

3.9. Análise em .NET
- 3.9.1. Introdução ao .NET
- 3.9.2. Descompilação com o dnSpy
- 3.9.3. Depuração com o dnSpy
- 3.10. Analizando um malware real

3.10.1. Preparação do ambiente
- 3.10.2. Análise estática do *malware*
- 3.10.3. Análise dinâmica do *malware*
- 3.10.4. Criação de regras YARA

Não há cronogramas predefinidos ou cronogramas de avaliação. É assim que é essa capacitação da TECH!"

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

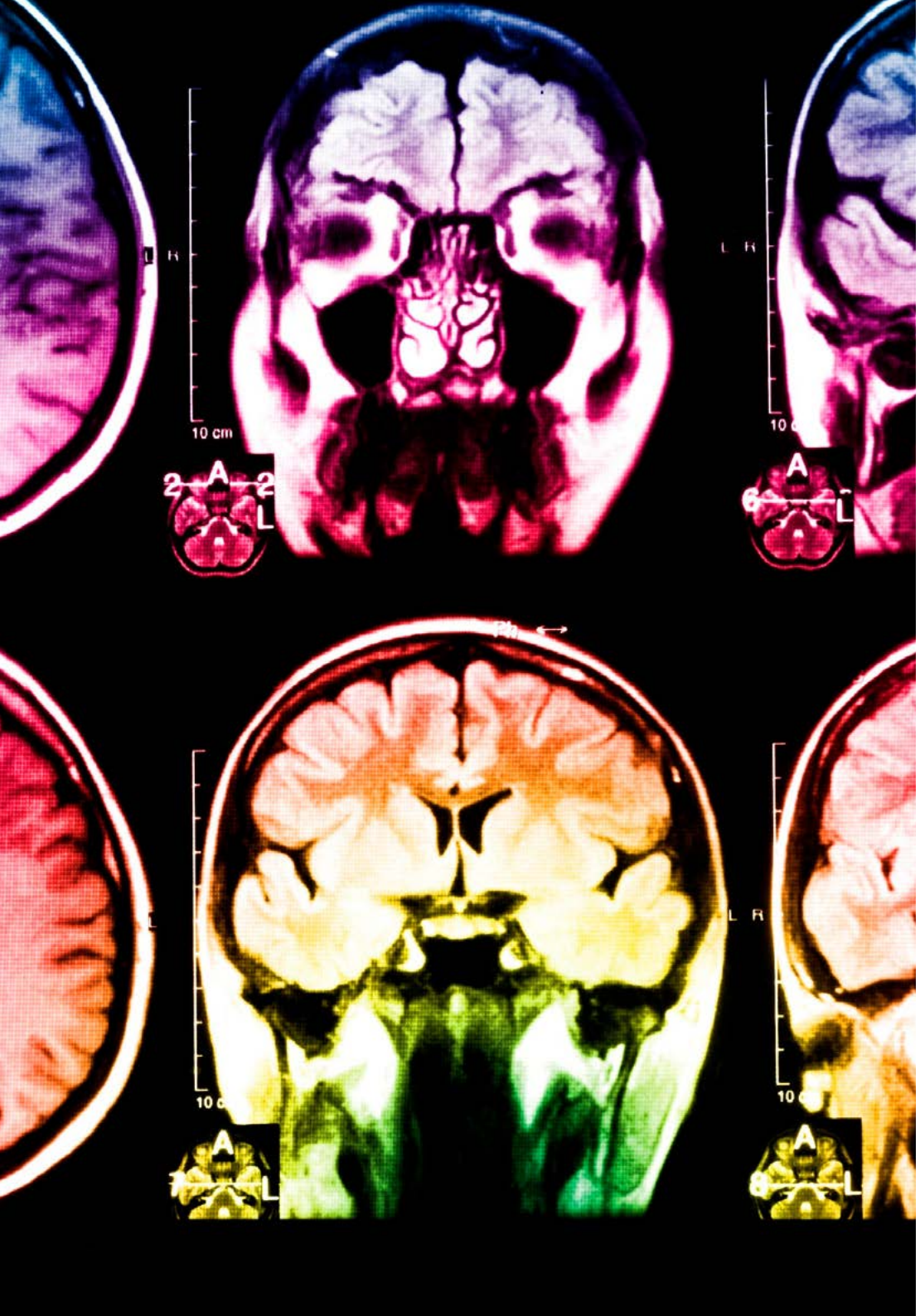
A TECH utiliza de maneira eficaz a metodologia do estudo de caso com um sistema de aprendizagem 100% online, baseado na repetição, combinando elementos didáticos diferentes em cada aula.

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.

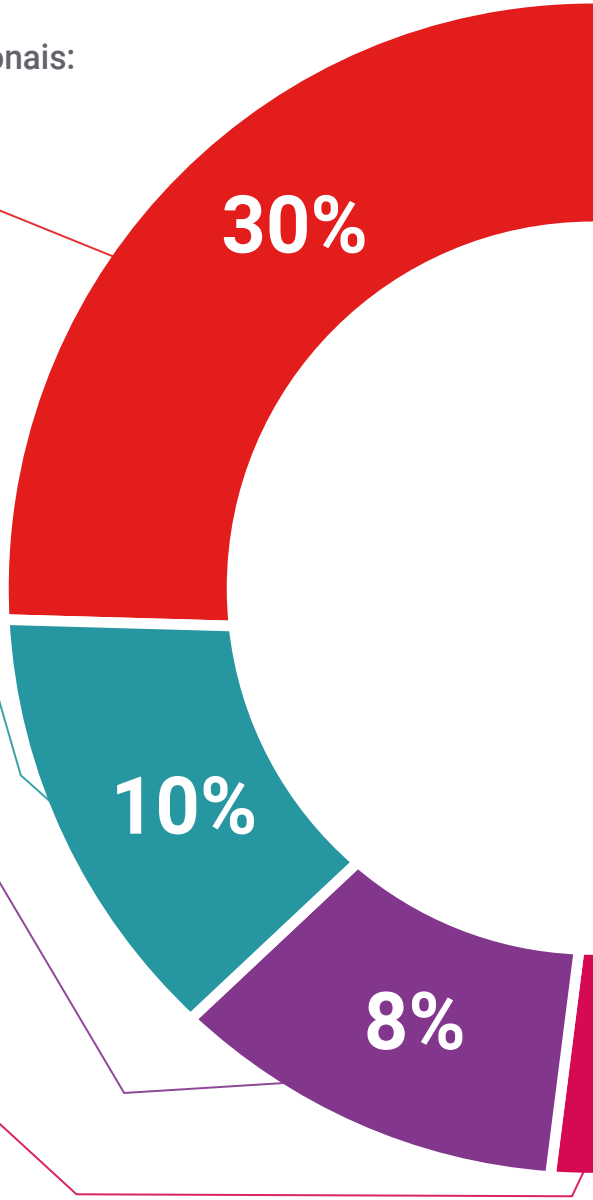
O "Learning from an expert" fortalece o conhecimento e a memória, além de gerar segurança para a tomada de decisões difíceis no futuro.

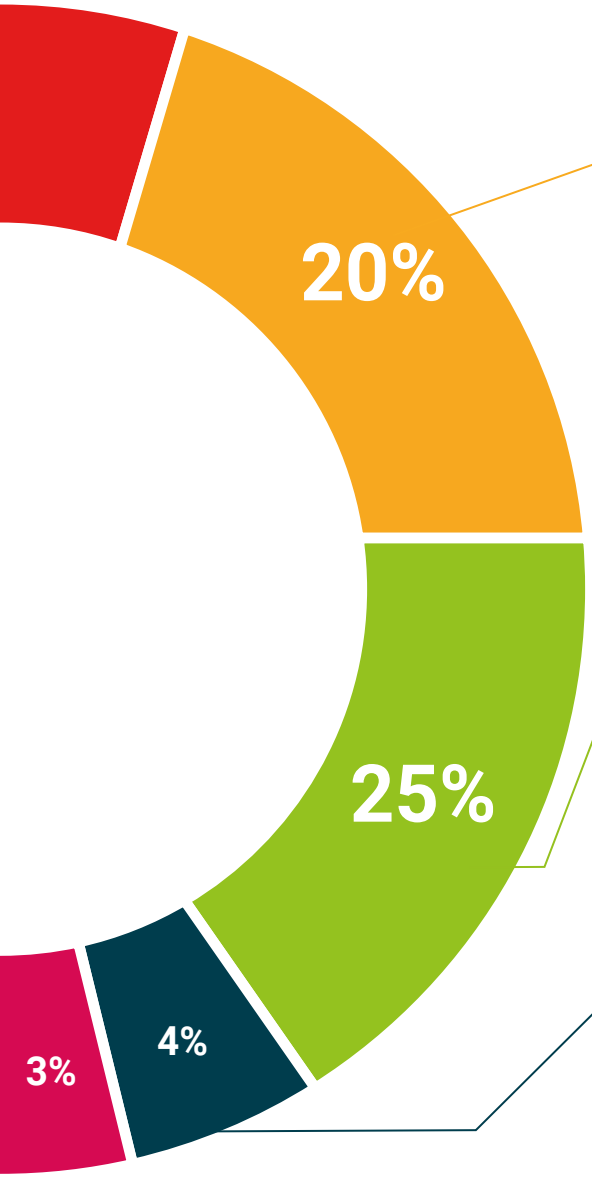
Práticas de habilidades e competências

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 Ofensiva 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 Cibersegurança Ofensiva** 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 Cibersegurança Ofensiva**

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

Cibersegurança Ofensiva

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 Ofensiva

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

Programa Avançado
Cibersegurança Ofensiva

tech universidade tecnológica