Programa Avançado
Hacking Web Avançado

tech universidade tecnológica

tech universidade tecnológica

Programa Avançado
Hacking Web Avançado

- 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-hacking-web-avancado**

Índice

01

Apresentação

À medida que as instituições se expandem digitalmente, elas estão usando cada vez mais a tecnologia para armazenar dados confidenciais. Assim, o *Hacking* Avançado se torna uma séria ameaça para as instituições. Se os *hackers* acessar seus sites, as consequências podem ser terríveis, variando de roubo de identidade a fraude financeira e chantagem. Portanto, é importante que as empresas tenham especialistas em medidas de segurança avançadas, para a implementação de medidas como *firewalls*.

Em resposta a isso, a TECH está lançando um programa inovador para ajudar os alunos a dominar as técnicas mais eficazes de cibersegurança. Além disso, ele é baseado em uma modalidade 100% online, garantindo conveniência e flexibilidade de horário.

Graças a este programa avançado, você transformará qualquer empresa em um ambiente seguro, livre de ameaças cibernéticas"

Os especialistas em TI são um intangível valioso para as organizações atuais. Um dos principais motivos é o fato de que as auditorias regulares ajudam a identificar e solucionar antecipadamente as possíveis vulnerabilidades. Dessa forma, eles estão antecipando crimes que podem ser cometidos por *hackers*, enquanto transforma ambientes virtuais em zonas seguras.

Dessa forma, os usuários têm a garantia de poder navegar com segurança e liberdade em sua rede e comprar seus produtos e serviços. Entretanto, em vista do aumento dessas práticas, os cientistas da computação enfrentam o desafio de atualizar constantemente seus conhecimentos, implementando as técnicas mais revolucionárias para lidar com elas.

Nesse contexto, a TECH desenvolveu o Programa Avançado de *Hacking Web* Avançado mais completo do mercado acadêmico. Com esse programa, os alunos estarão na vanguarda da cibersegurança e terão uma ampla variedade de táticas para proteger informações restritas. Além disso, as estratégias de exploração de vulnerabilidades sofisticadas serão exploradas em profundidade.

O profissional também se concentrará na implementação de medidas de segurança eficazes, como sistemas de detecção de intrusão. A ênfase também será colocada no *switching* para interconectar os equipamentos de todas as seções do organograma na mesma rede. Ele também fornecerá as ferramentas para a elaboração de relatórios técnicos e executivos. Nesse sentido, o relatório abordará como expor dados confidenciais, concentrando-se nos clientes. Por fim, serão exploradas várias metodologias para medir a segurança operacional real.

Para reforçar o domínio dos conteúdos, esta capacitação aplica o sistema inovador *Relearning*, que promove a assimilação de conceitos complexos por meio da reiteração natural e progressiva dos mesmos. Da mesma forma, o programa é apoiado por materiais em vários formatos, como infográficos ou vídeos explicativos. Tudo isso em um conveniente modo 100% online, que permite que cada pessoa ajuste seu horário de acordo com suas responsabilidades.

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

- O desenvolvimento de estudos de caso apresentados por especialistas em Hacking Web Avançado
- 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

> *Você decifrará senhas armazenadas em computadores e se antecipará a ataques de hackers"*

Você explorará o modelo OSI e entenderá os processos de comunicação em sistemas em rede. E em apenas 6 meses!"

Você se aprofundará nas vulnerabilidades do DOM e evitará ataques avançados com as estratégias mais eficazes.

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

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.

02

Objetivos

Este programa de estudos se aprofundará em técnicas avançadas de hacking direcionadas a serviços da Web, permitindo que os profissionais implementem as estratégias mais eficazes antes da ocorrência de ataques de hacking. Para isso, os princípios fundamentais do projeto de rede serão analisados e os pontos fracos comuns serão identificados. Como resultado, os alunos formados oferecerão as soluções mais inovadoras e se destacarão em um setor digital que avança a passos largos.

Você deseja proteger a rede e os dados transmitidos por ela? Domine o switching 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

Você aplicará as medidas de segurança mais eficazes e evitará vulnerabilidades, como a autenticação quebrada. Matricule-se já!"

Objetivos específicos

Módulo 1. Hacking Web Avançado

- Desenvolver habilidades para identificar e avaliar vulnerabilidades em aplicativos da Web, incluindo injeções de SQL, XSS e outros vetores de ataque comuns
- Aprender como realizar testes de segurança em aplicativos modernos da Web
- Adquirir habilidades em técnicas avançadas de hacking na Web, explorando estratégias para contornar medidas de segurança e explorar vulnerabilidades sofisticadas
- Familiarizar o aluno com a avaliação da segurança em APIs e serviços da Web, identificando possíveis vulnerabilidades e reforçando a segurança em interfaces de programação
- Desenvolver habilidades para implementar medidas eficazes de atenuação em aplicativos da Web, reduzindo a exposição a ataques e reforçando a segurança
- Participar de simulações práticas para avaliar a segurança em ambientes complexos da Web, aplicando o conhecimento em situações do mundo real
- Desenvolver competências na formulação de estratégias de defesa eficazes para proteger os aplicativos da Web contra ameaças cibernéticas
- Aprender a alinhar as práticas avançadas de hacking na Web com as regulamentações e os padrões de segurança relevantes, garantindo a adesão a estruturas legais e éticas
- Promover a colaboração eficaz entre as equipes de desenvolvimento e segurança

Módulo 2. Arquitetura e Segurança em Redes

- Adquirir conhecimentos avançados de arquitetura de rede, incluindo topologias, protocolos e componentes principais
- Desenvolver habilidades para identificar e avaliar vulnerabilidades específicas em infraestruturas de rede, considerando as possíveis ameaças
- Aprender como implementar medidas eficazes de segurança de rede, incluindo firewalls, sistemas de detecção de intrusão (IDS) e segmentação de rede
- Familiarizar o aluno com as tecnologias de rede emergentes, como a rede definida por software (SDN), e entender seu impacto sobre a segurança
- Desenvolver habilidades para proteger as comunicações em redes, incluindo proteção contra ameaças, como ataques de sniffing e ataques de intermediários
- Aprender como avaliar e aprimorar as configurações de segurança em ambientes de rede corporativa, garantindo a proteção adequada
- Desenvolver habilidades para implementar medidas eficazes de atenuação contra ameaças às redes corporativas, desde ataques internos até ameaças externas
- Promover a colaboração eficaz com as equipes de segurança, integrando estratégias e esforços para proteger a infraestrutura de rede
- Promover práticas éticas e legais na implementação de medidas de segurança de rede, garantindo a adesão a princípios éticos em todas as atividades

Módulo 3. Relatório técnico e executivo

- Desenvolver habilidades para produzir relatórios técnicos detalhados, apresentando de forma clara e abrangente as descobertas, as metodologias usadas e as recomendações
- Aprender a se comunicar de forma eficaz com públicos técnicos, usando linguagem precisa e apropriada para transmitir informações técnicas complexas
- Desenvolver habilidades para formular recomendações práticas e acionáveis destinadas a atenuar as vulnerabilidades e melhorar a postura de segurança
- Aprender a avaliar o impacto potencial das vulnerabilidades identificadas, considerando aspectos técnicos, operacionais e estratégicos
- Familiarizar o aluno com as práticas recomendadas para relatórios executivos, adaptando informações técnicas para públicos não técnicos
- Desenvolver competências para alinhar as conclusões e recomendações com os objetivos estratégicos e operacionais da organização
- Aprender a usar ferramentas de visualização de dados para representar graficamente as informações contidas nos relatórios, facilitando a compreensão
- Promover a inclusão de informações relevantes sobre a conformidade com regulamentos e padrões nos relatórios, garantindo a adesão aos requisitos legais
- Promover a colaboração eficaz entre as equipes técnicas e executivas, garantindo a compreensão e o apoio às ações de melhoria propostas no relatório

03

Direção do curso

Com o objetivo de oferecer excelência educacional, a TECH reuniu uma equipe de professores com ampla experiência profissional em cibersegurança. Com mais de 13 anos de experiência, esses especialistas oferecerão a abordagem mais abrangente e as ferramentas mais recentes para desenvolver ambientes virtuais seguros. Dessa forma, os alunos terão as garantias necessárias para se especializarem em um setor digital que oferece várias oportunidades.

Você vai se aprofundar nos limites do Pentester com o apoio da melhor equipe de professores. Suas atividades serão 100% legais!"

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

Professores

Sr. Marcelino Siles Rubia

- Cibersecurity Engineer
- Engenharia de Cibersegurança na Universidade Rey Juan Carlos
- Conhecimentos Programação Competitiva, *Hacking Web*, *Active Directory* e *Malware Development*
- Vencedor do concurso AdaByron

Sr. Pablo Redondo Castro

- Pentester no Grupo Oesia
- Engenheiro de cibersegurança, Universidade Rey Juan Carlos, Madri
- Ampla experiência como *Cibersecurity Evaluator Traineev*
- Ele acumula experiência de ensino, ministrando capacitações relacionadas a torneios de Capture The Flag

04

Estrutura e conteúdo

Esse programa é composto por 3 módulos abrangentes: *Hacking Web* Avançado; Arquitetura e segurança de rede; e Relatórios técnicos e executivos. Com o apoio de professores veteranos, táticas avançadas para proteger redes corporativas serão abordadas por meio da implementação de *firewalls*. Também será desenvolvida a detecção de intrusão, incluindo HHTP *Request Smuggling*. Será discutida a importância de ter VLANs para separar o tráfego de dados no mesmo ambiente virtual e será analisado o processo de geração de relatórios para apresentar relatórios precisos e detalhados.

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"

Módulo 1. Hacking Web Avançado

1.1. Funcionamento de um site
- 1.1.1. O URL e suas partes
- 1.1.2. Métodos HTTP
- 1.1.3. Os cabeçalhos
- 1.1.4. Como visualizar solicitações da Web com o Burp Suite

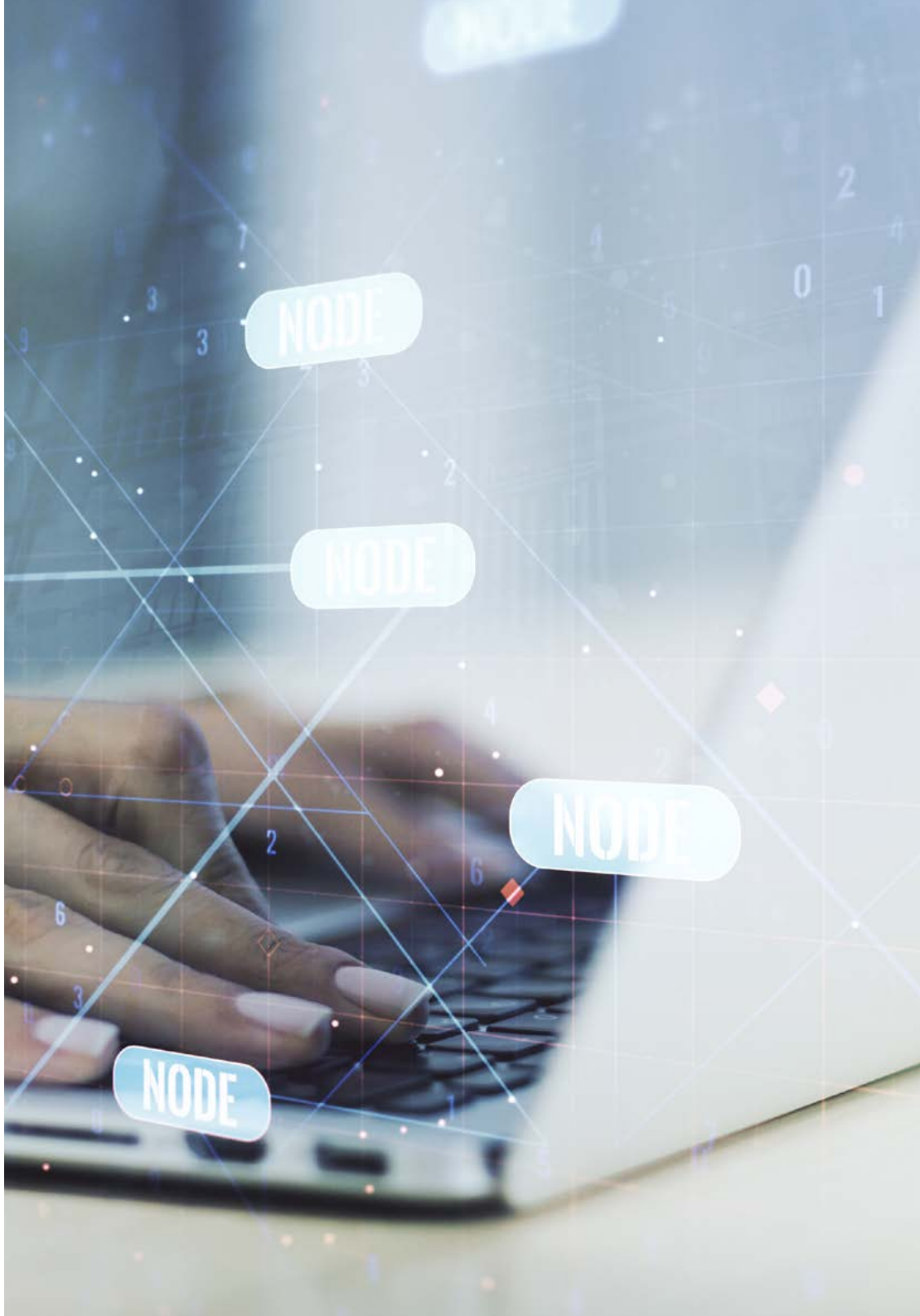
1.2. Sessões
- 1.2.1. Os *cookies*
- 1.2.2. *Tokens* JWT
- 1.2.3. Ataques de sequestro de sessão
- 1.2.4. Ataques a JWT

1.3. *Cross Site Scripting* (XSS)
- 1.3.1. O que é um XSS
- 1.3.2. Tipos de XSS
- 1.3.3. Exploração de um XSS
- 1.3.4. Introdução ao *XSLeaks*

1.4. Injeções de banco de dados
- 1.4.1. O que é um *SQL Injection*
- 1.4.2. Extração de informações com *SQLi*
- 1.4.3. *SQLi Blind, Time-Based e Error-Based*
- 1.4.4. Injeções de NoSQLi

1.5. Path Traversal e Local File Inclusion
- 1.5.1. O que são e suas diferenças
- 1.5.2. Filtros comuns e como contorná-los
- 1.5.3. *Log Poisoning*
- 1.5.4. LFIs em PHP

1.6. *Broken Authentication*
- 1.6.1. *User Enumeration*
- 1.6.2. *Password Bruteforce*
- 1.6.3. *2FA Bypass*
- 1.6.4. *Cookies* com informações sensíveis e modificáveis



1.7. *Remote Command Execution*
- 1.7.1. *Command Injection*
- 1.7.2. *Blind Command Injection*
- 1.7.3. *Insecure Deserialization* PHP
- 1.7.4. *Insecure Deserialization* Java

1.8. *File Uploads*
- 1.8.1. RCE mediante *webshells*
- 1.8.2. XSS em uploads de arquivos
- 1.8.3. XML *External Entity* (XXE) *Injection*
- 1.8.4. *Path traversal* em uploads de arquivos

1.9. *Broken Acess Control*
- 1.9.1. Acesso aos painéis sem restrição
- 1.9.2. *Insecure Direct Object References* (IDOR)
- 1.9.3. *Bypass* de filtros
- 1.9.4. Métodos de autorização insuficientes

1.10. Vulnerabilidades do DOM e ataques mais avançados
- 1.10.1. *Regex Denial of Service*
- 1.10.2. DOM *Clobbering*
- 1.10.3. *Prototype Pollution*
- 1.10.4. HTTP *Request Smuggling*

Módulo 2. Arquitetura e Segurança em Redes

2.1. Redes de computadores
- 2.1.1. Conceitos básicos Protocolos LAN, WAN, CP, CC
- 2.1.2. Modelo OSI TCP/IP
- 2.1.3. *Switching:* Conceitos básicos
- 2.1.4. *Routing:* Conceitos básicos

2.2. *Switching:*
- 2.2.1. Introdução às VLANs
- 2.2.2. STP
- 2.2.3. *EtherChannel*
- 2.2.4. Ataques à camada 2

2.3. VLAN´s
- 2.3.1. Importância das VLANs
- 2.3.2. Vulnerabilidades em VLANs
- 2.3.3. Ataques comuns a VLANs
- 2.3.4. Mitigações

2.4. *Routing*
- 2.4.1. Endereçamento IP - IPv4 e IPv6
- 2.4.2. Roteamento: Conceitos fundamentais
- 2.4.3. Roteamento estático
- 2.4.4. Roteamento dinâmico: Introdução

2.5. Protocolos IGP
- 2.5.1. RIP
- 2.5.2. OSPF
- 2.5.3. RIP vs OSPF
- 2.5.4. Análise das necessidades de topologia

2.6. Proteção do perímetro
- 2.6.1. DMZs
- 2.6.2. *Firewalls*
- 2.6.3. Arquiteturas comuns
- 2.6.4. Zero Trust Network Access

2.7. IDS e IPS
- 2.7.1. Características
- 2.7.2. Implementação
- 2.7.3. SIEM e SIEM CLOUDS
- 2.7.4. Detecção baseada em *HoneyPots*

2.8. TLS e VPN´s
- 2.8.1. SSL/ TLS
- 2.8.2. TLS: Ataques comuns
- 2.8.3. VPNs com TLS
- 2.8.4. VPNs com IPSEC

2.9. Segurança em redes sem fio
- 2.9.1. Introdução às redes sem fio
- 2.9.2. Protocolos
- 2.9.3. Elementos fundamentais
- 2.9.4. Ataques comuns

2.10. Redes empresariais e como lidar com elas
- 2.10.1. Segmentação lógica
- 2.10.2. Segmentação física
- 2.10.3. Controle de acesso
- 2.10.4. Outras considerações

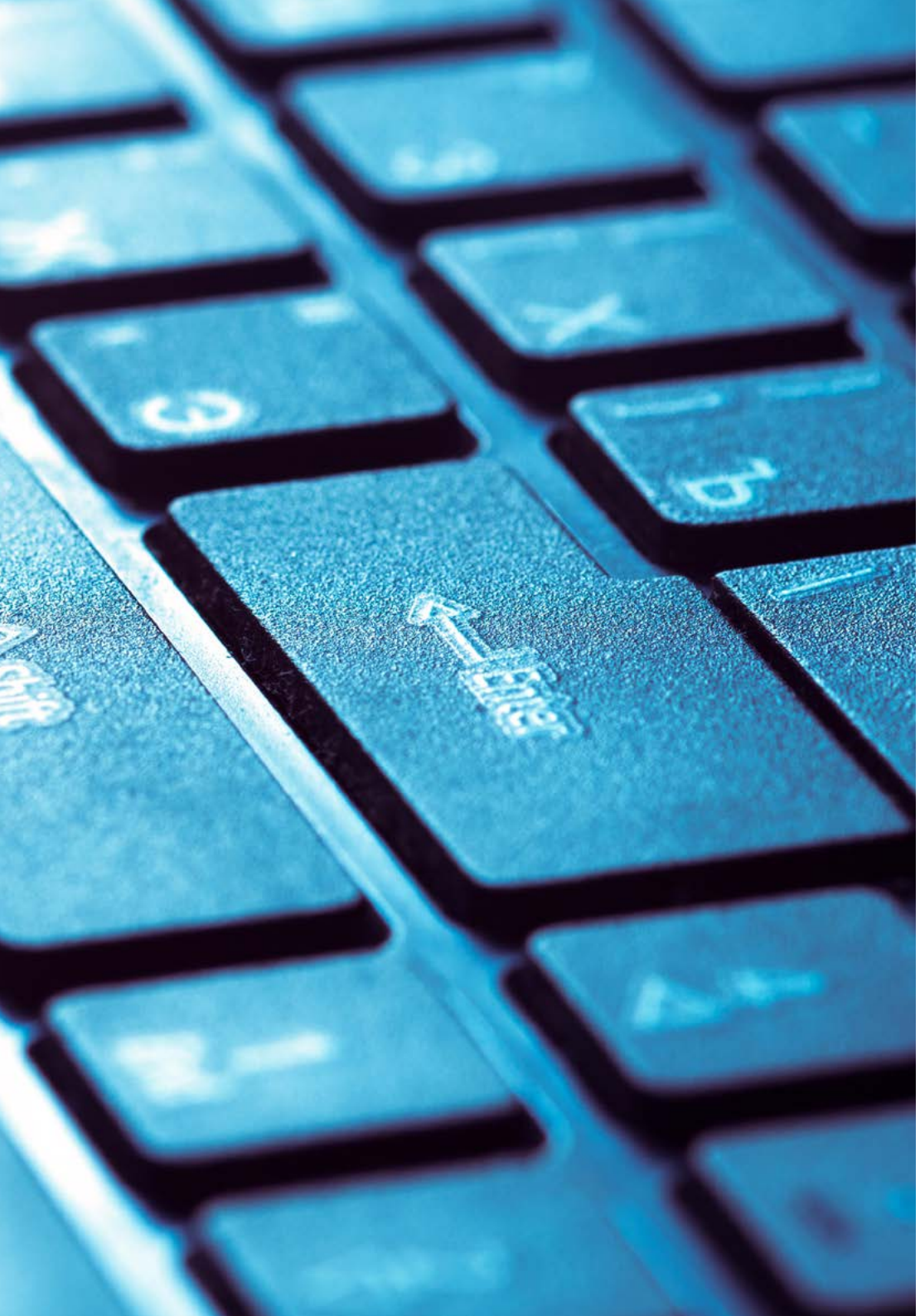
Módulo 3. Relatório técnico e executivo

3.1. Processo de relatório
- 3.1.1. Estrutura de um relatório
- 3.1.2. Processo de relatório
- 3.1.3. Conceitos fundamentais
- 3.1.4. Executivo x Técnico

3.2. Guias
- 3.2.1. Introdução
- 3.2.2. Tipos de guias
- 3.2.3. Guias nacionais
- 3.2.4. Casos de uso

3.3. Metodologias
- 3.3.1. Avaliação
- 3.3.2. *Pentesting*
- 3.3.3. Revisão de metodologias comuns
- 3.3.4. Introdução às metodologias nacionais

3.4. Abordagem técnica para a fase de relatório
- 3.4.1. Entendendo os limites do *pentester*
- 3.4.2. Uso e dicas de linguagem
- 3.4.3. Apresentação de informações
- 3.4.4. Erros mais comuns



3.5. Abordagem executiva para a fase de relatório
- 3.5.1. Ajustando o relatório ao contexto
- 3.5.2. Uso e dicas de linguagem
- 3.5.3. Padronização
- 3.5.4. Erros mais comuns

3.6. OSSTMM
- 3.6.1. Entendendo a metodologia
- 3.6.2. Reconhecimento
- 3.6.3. Documentação
- 3.6.4. Elaboração do relatório

3.7. LINCE
- 3.7.1. Entendendo a metodologia
- 3.7.2. Reconhecimento
- 3.7.3. Documentação
- 3.7.4. Elaboração do relatório

3.8. Relatório de vulnerabilidades
- 3.8.1. Conceitos fundamentais
- 3.8.2. Quantificação do escopo
- 3.8.3. Vulnerabilidades e evidências
- 3.8.4. Erros mais comuns

3.9. Focando o relatório no cliente
- 3.9.1. Importância da evidência do trabalho
- 3.9.2. Soluções e mitigações
- 3.9.3. Dados sensíveis e relevantes
- 3.9.4. Exemplos práticos e casos

3.10. Reportando *retakes*
- 3.10.1. Conceitos fundamentais
- 3.10.2. Compreensão das informações legadas
- 3.10.3. Verificação de erros
- 3.10.4. Adicionando informações

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

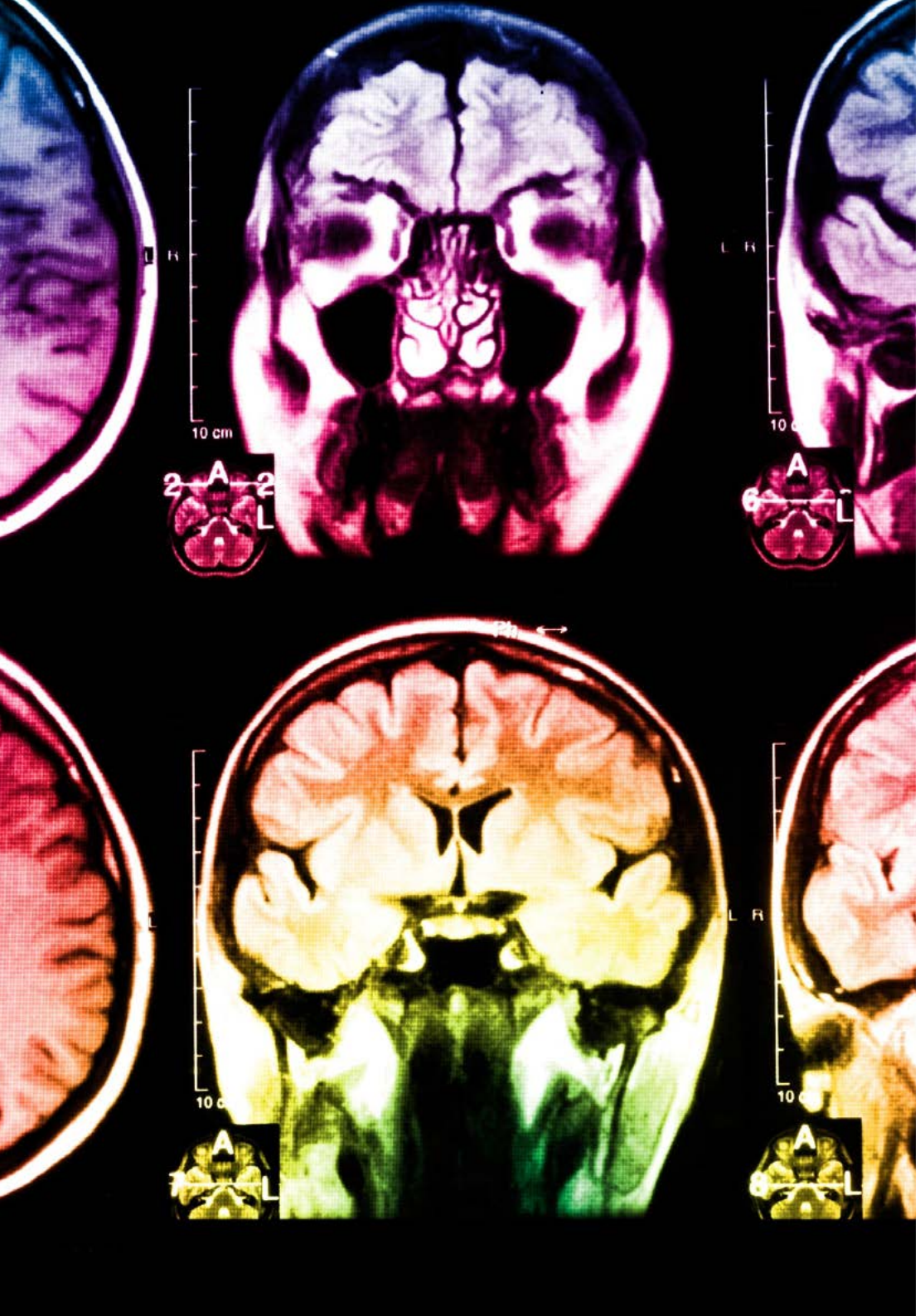
A TECH utiliza de maneira eficaz a metodologia do estudo de caso com um sistema de aprendizagem 100% online, baseado na repetição, combinando elementos didáticos diferentes em cada aula.

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.

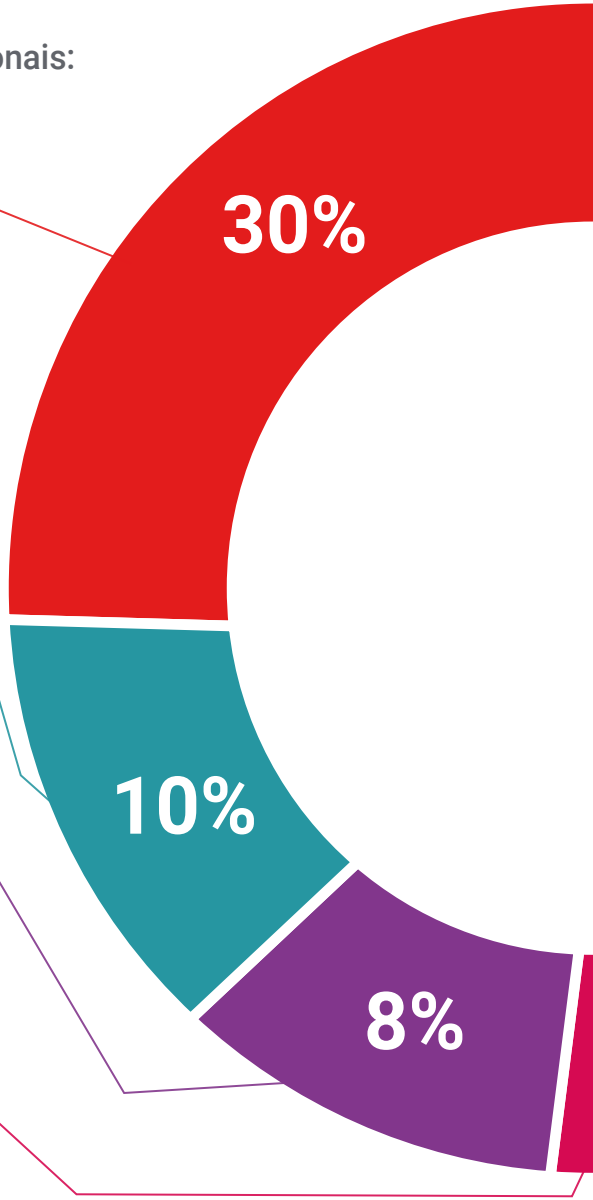
O "Learning from an expert" fortalece o conhecimento e a memória, além de gerar segurança para a tomada de decisões difíceis no futuro.

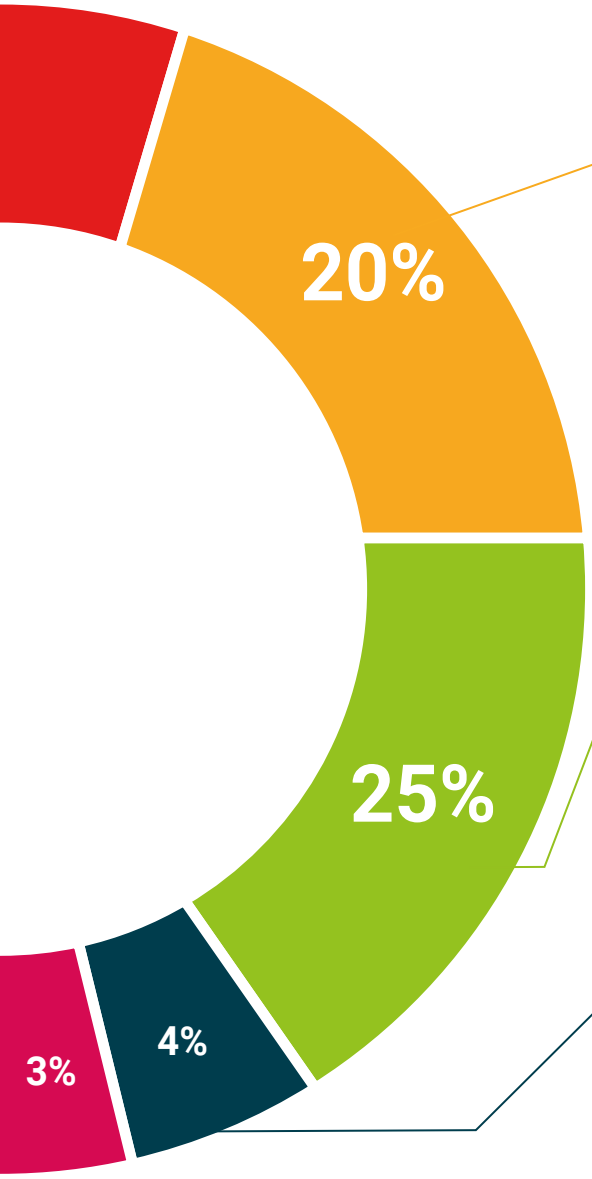
Práticas de habilidades e competências

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 Hacking Web Avançado 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 Hacking Web Avançado** 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 Hacking Web Avançado**

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

Hacking Web Avançado

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
Hacking Web Avançado

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

Programa Avançado
Hacking Web Avançado

tech universidade tecnológica