Curso
Hacking Ético

tech universidade tecnológica

tech universidade tecnológica

Curso
Hacking Ético

- Modalidade: **online**
- Duração: **6 semanas**
- Certificação: **TECH Universidade Tecnológica**
- Acreditação: **6 ECTS**
- Horário: **ao seu próprio ritmo**
- Exames: **online**

Acesso ao site: **www.techtitute.com/pt/informatica/curso/hacking-etico**

Índice

01

Apresentação

A ciberproteção tornou-se numa prioridade para os indivíduos e empresas. Quanto mais inovadoras e desenvolvidas forem as funcionalidades dos dispositivos, mais sofisticadas e perigosas serão as ameaças aos mesmos e, consequentemente, aos dados dos seus utilizadores. A criação de ferramentas que se adaptem às alterações da ameaça implica a utilização de tecnologias, *hacking* e abordagens que proporcionem uma cobertura de segurança adequada. Este Curso é a forma mais completa e de maior qualidade no mercado do ensino online para obter a capacitação mais completa neste domínio.

Aprenda a detetar vulnerabilidades num sistema através da realização de ataques preventivos que demonstrem violações e obtenha dados valiosos sobre cibersegurança"

Atualmente, nenhuma empresa está livre de sofrer um ciberataque e, portanto, de sofrer as várias consequências que este acarreta. Independentemente do tamanho da mesma, está exposta a roubos de informação, chantagem, sabotagem, etc.

É necessário realizar um estudo de vulnerabilidade e determinar a superfície de ataque, pelo que cada vez mais serão efetuados estudos periódicos da vulnerabilidade e de riscos. Cada empresa terá de verificar se cumpre as regras e a legislação do país onde está localizada e estar ciente dos danos causados, tanto monetários como outros danos imateriais, por exemplo, à sua reputação.

Este módulo apresenta as diferentes ferramentas e metodologias para responder a esta necessidade e, por conseguinte, fornece um conjunto abrangente de conhecimentos especializados para realizar este trabalho.

Este **Curso de Hacking Ético** conta com o conteúdo educativo mais completo e atualizado do mercado. As suas principais características são:

- O desenvolvimento de casos práticos apresentados por especialistas em cibersegurança
- Os conteúdos gráficos, esquemáticos e eminentemente práticos fornecem informações científicas e práticas sobre as disciplinas essenciais para a prática profissional
- Os exercícios práticos em que o processo de autoavaliação pode ser utilizado para melhorar a aprendizagem
- A sua ênfase especial nas metodologias inovadoras
- As lições teóricas, perguntas a especialistas, fóruns de discussão sobre questões controversas e atividades de reflexão individual
- A disponibilidade de acesso aos conteúdos a partir de qualquer dispositivo fixo ou portátil com ligação à Internet

As formas mais inovadoras e eficientes de criar sistemas de proteção que garantam a cibersegurança dos dispositivos"

Estude com este Curso centrado na prática, aumentando as suas competências até ao nível de um especialista"

Conheça as principais ameaças e as ferramentas mais inovadoras e atualizadas na luta contra os ciberataques através deste Curso excecional.

Um processo de alta capacitação criado para ser acessível e flexível, com a mais interessante metodologia de ensino online.

O corpo docente do Curso inclui profissionais do setor que trazem a sua experiência profissional para esta capacitação, para além de especialistas reconhecidos de sociedades de referência e universidades de prestígio.

Os seus conteúdos multimédia, desenvolvidos com a mais recente tecnologia educativa, permitirão ao profissional uma aprendizagem situada e contextual, ou seja, um ambiente simulado que proporcionará uma capacitação imersiva programada para praticar em situações reais.

A estrutura deste Curso centra-se na Aprendizagem Baseada em Problemas, na qual o profissional deve tentar resolver as diferentes situações de prática profissional que surgem durante o Curso. Para tal, contará com a ajuda de um sistema inovador de vídeos interativos criados por especialistas reconhecidos.

02

Objetivos

O Curso de Hacking Ético dá aos alunos a capacidade de trabalhar neste domínio de forma rápida e fácil. Com objetivos realistas e de grande interesse, este processo de estudo foi concebido para conduzir progressivamente os alunos à aquisição dos conhecimentos teóricos e práticos necessários para intervir com qualidade e para desenvolver competências transversais que lhes permitam enfrentar situações complexas, elaborando respostas ajustadas e precisas.

A aprendizagem mais completa sobre o hacking ético como ferramenta de deteção de vulnerabilidades num processo de altíssima qualidade"

Objetivos gerais

- Analisar os diferentes sistemas existentes
- Avaliar a informação obtida e desenvolver mecanismos de prevenção e *hacking*
- Estabelecer prioridades para o estudo e resolução de vulnerabilidades
- Demonstrar que um sistema é vulnerável, atacá-lo preventivamente e resolver esses problemas

Objetivos específicos

- Analisar os métodos IOSINT
- Recolher informações disponíveis nos meios de comunicação social públicos
- Fazer scan das redes para obter informação de modo ativo

A pensar no aluno, este Curso implementa os sistemas de apoio ao estudo mais interessantes do momento"

03

Direção do curso

Os professores que lecionam este Curso foram selecionados pela sua competência excecional neste campo. Combinam conhecimentos técnicos e práticos com experiência de ensino, oferecendo aos alunos um apoio de primeira classe para atingirem os seus objetivos. Através destes, o Curso oferece a visão mais direta e imediata das características reais da intervenção neste domínio, alcançando uma visão contextual de máximo interesse.

Os professores especialistas em Hacking Ético dar-lhe-ão a visão ampla e contextual de que necessita para trabalhar com precisão em cibersegurança"

Diretor Convidado Internacional

O Doutor Frederic Lemieux é reconhecido internacionalmente como um especialista inovador e líder inspirador nos domínios da **Inteligência**, **Segurança Nacional**, **Segurança Interna**, **Cibersegurança e Tecnologias Disruptivas**. A sua dedicação constante e contributos relevantes para a investigação e educação posicionam-no como uma figura-chave na promoção da segurança e na compreensão das tecnologias emergentes atualmente. Durante a sua carreira profissional, concebeu e liderou programas académicos de vanguarda em várias instituições de renome, como a **Universidade de Montreal**, a **Universidade George Washington** e a **Universidade de Georgetown**.

Ao longo da sua vasta carreira, publicou vários livros importantes, todos relacionados com a **informação criminal**, **o policiamento**, **as ciberameaças e a segurança internacional**. Também contribuiu significativamente para o domínio da cibersegurança, publicando inúmeros artigos em revistas académicas sobre o controlo da criminalidade durante grandes catástrofes, a luta contra o terrorismo, as agências de informação e a cooperação policial. Além disso, foi orador de painel e orador principal em várias conferências nacionais e internacionais, estabelecendo-se como uma referência no domínio académico e profissional.

O Doutor Lemieux desempenhou funções editoriais e de avaliação em várias organizações académicas, privadas e governamentais, o que reflete a sua influência e o seu compromisso com a excelência na sua área de especialização. Como tal, a sua prestigiada carreira académica levou-o a desempenhar as funções de Professor de Estágios e Diretor do Corpo Docente dos programas MPS em **Inteligência Aplicada**, **Gestão de Riscos de Cibersegurança**, **Gestão Tecnológica e Gestão de Tecnologias da Informação** na **Universidade de Georgetown**.

Doutor Lemieux, Frederic

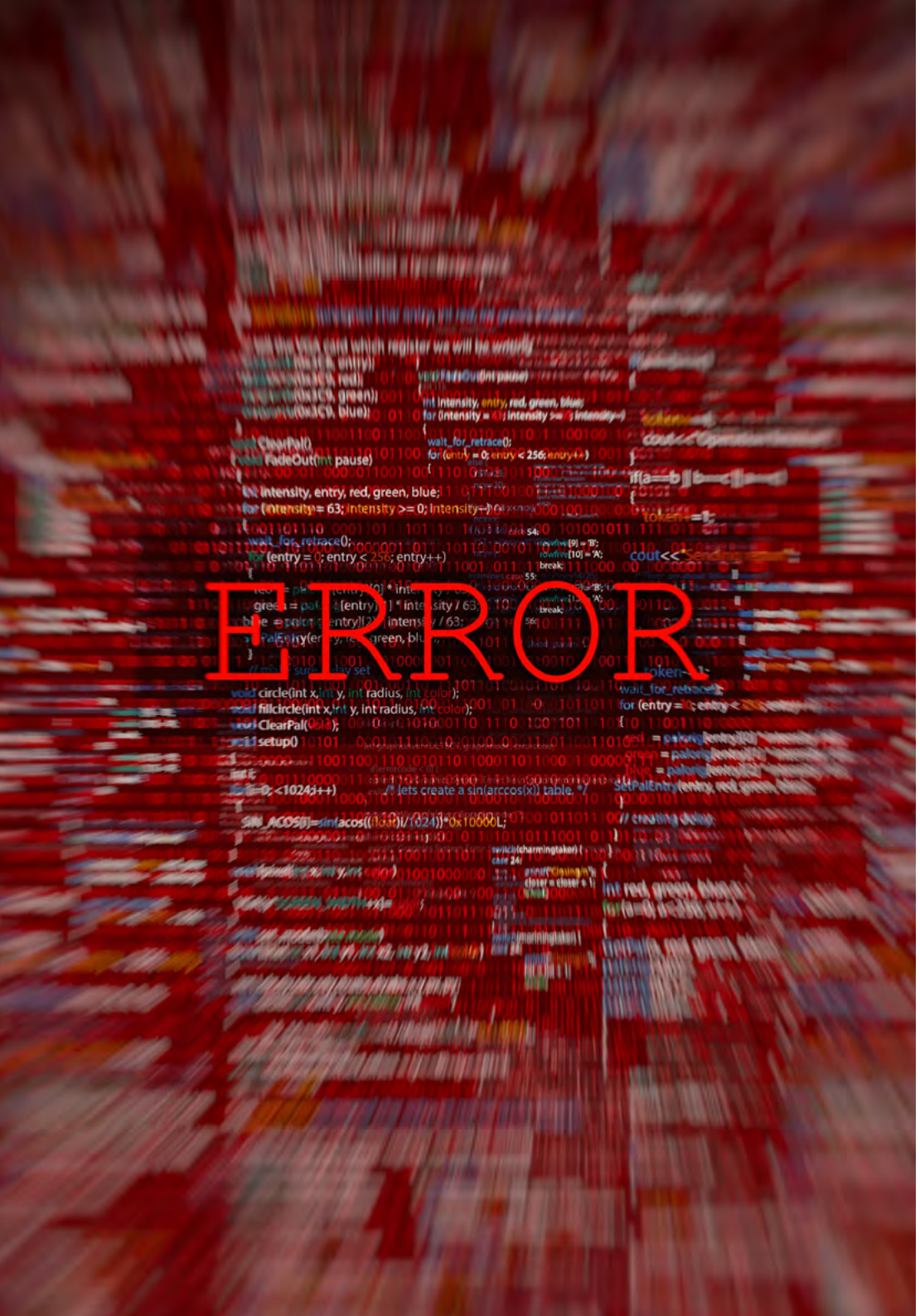
- Investigador em Inteligência, Cibersegurança e Tecnologias Disruptivas, na Universidade de Georgetown
- Diretor do Mestrado em Information Technology Management na Universidade de Georgetown
- Diretor do Mestrado em Technology Management na Universidad de Georgetown
- Diretor do Mestrado em Cybersecurity Risk Management na Universidad de Georgetown
- Diretor do Mestrado em Applied Intelligence na Universidad de Georgetown
- Professor de Estágios na Universidade de Georgetown
- Doutoramento em Criminologia pela School of Criminology, na Universidade de Montreal
- Licenciatura em Sociologia, Minor Degree em Psicologia, pela Universidade de Laval
- Membro de:
  - New Program Roundtable Committee, pela Universidade de Georgetown

Graças à TECH, poderá aprender com os melhores profissionais do mundo"

Direção

Dra. Sonia Fernández Sapena

- Formadora em Segurança Informática e Hacking Ético. Centro de Referencia Nacional de Getafe en Informática y Telecomunicaciones. Madrid
- Instrutora certificada E-Council. Madrid
- Formadora nas seguintes certificações: EXIN Ethical Hacking Foundation e EXIN Cyber & IT Security Foundation. Madrid
- Formadora especializada certificada pela CAM para os seguintes certificados de profissionalização: Segurança Informática (IFCT0190), Gestão de Redes de Voz e Dados (IFCM0310), Administração de Redes Departamentais (IFCT0410), Gestão de Alarmes em Redes de Telecomunicações (IFCM0410), Operador de Redes de Voz e Dados (IFCM0110), e Administração de Serviços de Internet (IFCT0509)
- Colaboradora externa CSO/SSA (Chief Security Officer/Senior Security Architect). Universidade de las Islas Baleares
- Engenheira informática. Universidade de Alcalá de Henares. Madrid
- Mestrado em DevOps: Docker and Kubernetes. Cas-Training. Madrid
- Microsoft Azure Security Technologies. E-Council. Madrid

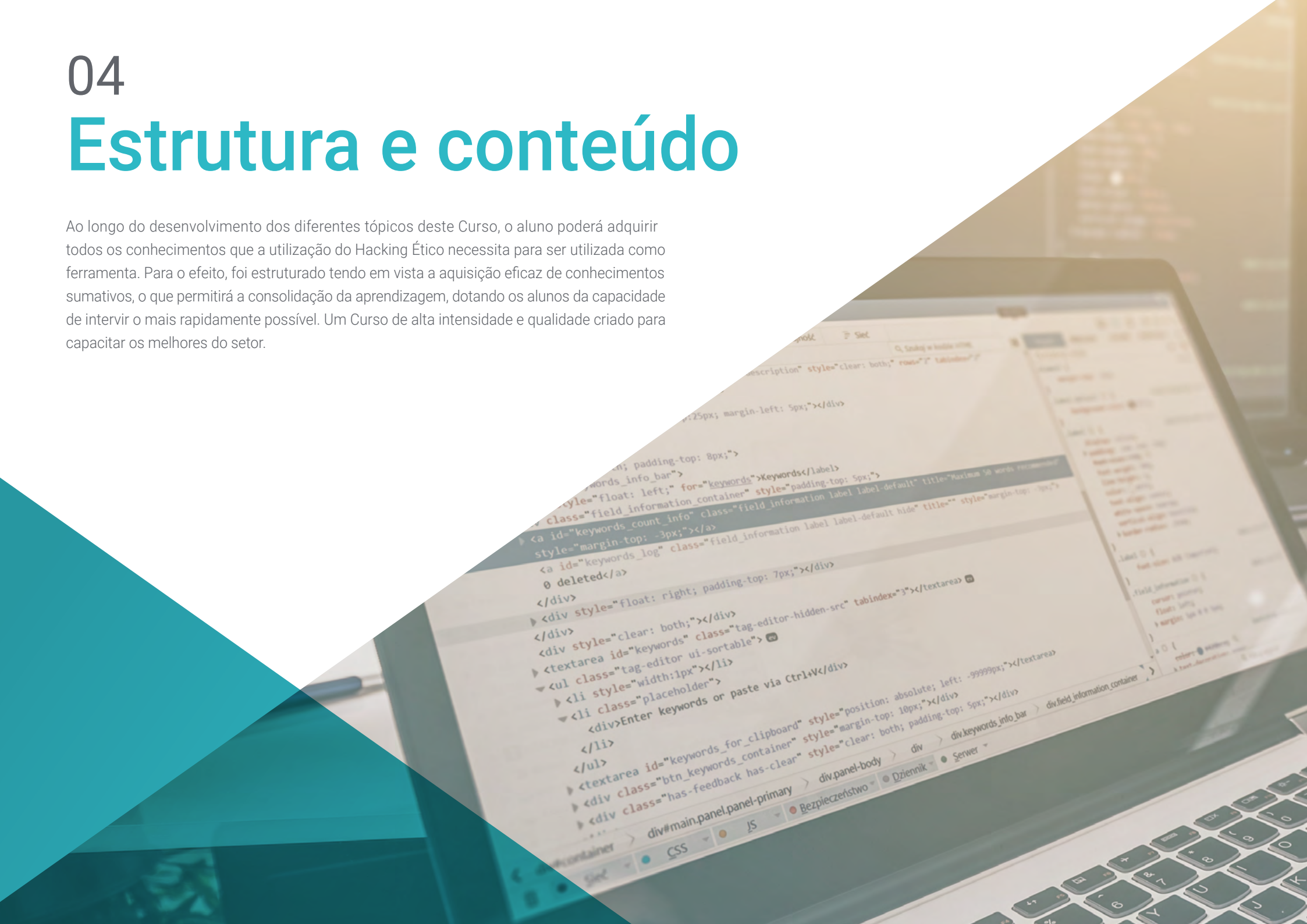


Desenvolva a sua educação com os melhores especialistas na matéria"

04

Estrutura e conteúdo

Ao longo do desenvolvimento dos diferentes tópicos deste Curso, o aluno poderá adquirir todos os conhecimentos que a utilização do Hacking Ético necessita para ser utilizada como ferramenta. Para o efeito, foi estruturado tendo em vista a aquisição eficaz de conhecimentos sumativos, o que permitirá a consolidação da aprendizagem, dotando os alunos da capacidade de intervir o mais rapidamente possível. Um Curso de alta intensidade e qualidade criado para capacitar os melhores do setor.



Um Curso desenvolvido de forma estruturada através de uma abordagem de estudo centrada na eficiência"

Módulo 1. Hacking Ético

1.1. Ambiente de trabalho
- 1.1.1. Distribuições Linux
  - 1.1.1.1. Kali Linux - Offensive Security
  - 1.1.1.2. Parrot OS
  - 1.1.1.3. Ubuntu
- 1.1.2. Sistemas de virtualização
- 1.1.3. Sandbox
- 1.1.4. Implementação de laboratórios

1.2. Metodologias
- 1.2.1. OSSTMM
- 1.2.2. OWASP
- 1.2.3. NIST
- 1.2.4. PTES
- 1.2.5. ISSAF

1.3. Footprinting
- 1.3.1. Inteligência de fontes abertas (OSINT)
- 1.3.2. Pesquisa de violações e vulnerabilidades de dados
- 1.3.3. Utilização de ferramentas passivas

1.4. Análise de redes
- 1.4.1. Ferramentas de análise
  - 1.4.1.1. Nmap
  - 1.4.1.2. Hping3
  - 1.4.1.3. Outras ferramentas de análise
- 1.4.2. Técnicas de análise
- 1.4.3. Técnicas de evasão de *firewall* e IDS
- 1.4.4. Banner *grabbing*
- 1.4.5. Diagramas de rede

1.5. Enumeração
- 1.5.1. Enumeração SMTP
- 1.5.2. Enumeração DNS
- 1.5.3. Enumeração de NetBIOS e Samba
- 1.5.4. Enumeração de LDAP
- 1.5.5. Enumeração de SNMP
- 1.5.6. Outras técnicas de enumeração

1.6. Análise de vulnerabilidade
- 1.6.1. Soluções de análise de vulnerabilidades
  - 1.6.1.1. Qualys
  - 1.6.1.2. Nessus
  - 1.6.1.3. CFI LanGuard
- 1.6.2. Sistemas de avaliação de vulnerabilidades
  - 1.6.2.1. CVSS
  - 1.6.2.2. CVE
  - 1.6.2.3. NVD

1.7. Ataques a redes sem fios
- 1.7.1. Metodologia de *hacking* em redes sem fios
  - 1.7.1.1. Wifi *discovery*
  - 1.7.1.2. Análise de tráfego
  - 1.7.1.3. Ataques do *aircrack*
    - 1.7.1.3.1. Ataques WEP
    - 1.7.1.3.2. Ataques WPA/WPA2
  - 1.7.1.4. Ataques de Evil Twin
  - 1.7.1.5. Ataques ao WPS
  - 1.7.1.6. *Jamming*
- 1.7.2. Ferramentas para a segurança sem fios

1.8. Hacking de servidores Web
- 1.8.1. *Cross site scripting*
- 1.8.2. CSRF
- 1.8.3. *Session hijacking*
- 1.8.4. SQL *injection*

1.9. Exploração de vulnerabilidades
- 1.9.1. Utilização de *exploits* conhecidos
- 1.9.2. Utilização de *metasploits*
- 1.9.3. Utilização de *malwares*
  - 1.9.3.1. Definição e alcance
  - 1.9.3.2. Geração de *malware*
  - 1.9.3.3. Contorno de antivírus

1.10. Persistência
- 1.10.1. Instalação de *rootkits*
- 1.10.2. Utilização de Ncat
- 1.10.3. Utilização de tarefas programadas para *backdoors*
- 1.10.4. Criação de utilizadores
- 1.10.5. Deteção de HIDS

Tudo o que um profissional de cibersegurança precisa de saber está organizado num plano de estudos abrangente que irá progressivamente e de forma constante aumentar as suas competências até ao mais alto nível”

05

Metodologia

Este programa de capacitação oferece uma forma diferente de aprendizagem. A nossa metodologia é desenvolvida através de um modo de aprendizagem cíclico: ***o Relearning***. Este sistema de ensino é utilizado, por exemplo, nas escolas médicas mais prestigiadas do mundo e tem sido considerado um dos mais eficazes pelas principais publicações, tais como a ***New England Journal of Medicine.***

Descubra o Relearning, um sistema que abandona a aprendizagem linear convencional para o levar através de sistemas de ensino cíclicos: uma forma de aprendizagem que provou ser extremamente eficaz, especialmente em disciplinas que requerem memorização"

Estudo de Caso para contextualizar todo o conteúdo

O nosso programa oferece um método revolucionário de desenvolvimento de competências e conhecimentos. O nosso objetivo é reforçar as competências num contexto de mudança, competitivo e altamente exigente.

Com a TECH pode experimentar uma forma de aprendizagem que abala as fundações das universidades tradicionais de todo o mundo"

Terá acesso a um sistema de aprendizagem baseado na repetição, com ensino natural e progressivo ao longo de todo o programa de estudos.

O estudante aprenderá, através de atividades de colaboração e casos reais, a resolução de situações complexas em ambientes empresariais reais.

Um método de aprendizagem inovador e diferente

Este programa da TECH é um programa de ensino intensivo, criado de raiz, que propõe os desafios e decisões mais exigentes neste campo, tanto a nível nacional como internacional. Graças a esta metodologia, o crescimento pessoal e profissional é impulsionado, dando um passo decisivo para o sucesso. O método do caso, a técnica que constitui a base deste conteúdo, assegura que a realidade económica, social e profissional mais atual é seguida.

> *"O nosso programa prepara-o para enfrentar novos desafios em ambientes incertos e alcançar o sucesso na sua carreira"*

O método do caso tem sido o sistema de aprendizagem mais amplamente utilizado nas principais escolas de informática do mundo desde que existem. Desenvolvido em 1912 para que os estudantes de direito não só aprendessem o direito com base no conteúdo teórico, o método do caso consistia em apresentar-lhes situações verdadeiramente complexas, a fim de tomarem decisões informadas e valorizarem juízos sobre a forma de as resolver. Em 1924 foi estabelecido como um método de ensino padrão em Harvard.

Numa dada situação, o que deve fazer um profissional? Esta é a questão que enfrentamos no método do caso, um método de aprendizagem orientado para a ação. Ao longo do programa, os estudantes serão confrontados com múltiplos casos da vida real. Terão de integrar todo o seu conhecimento, investigar, argumentar e defender as suas ideias e decisões.

Relearning Methodology

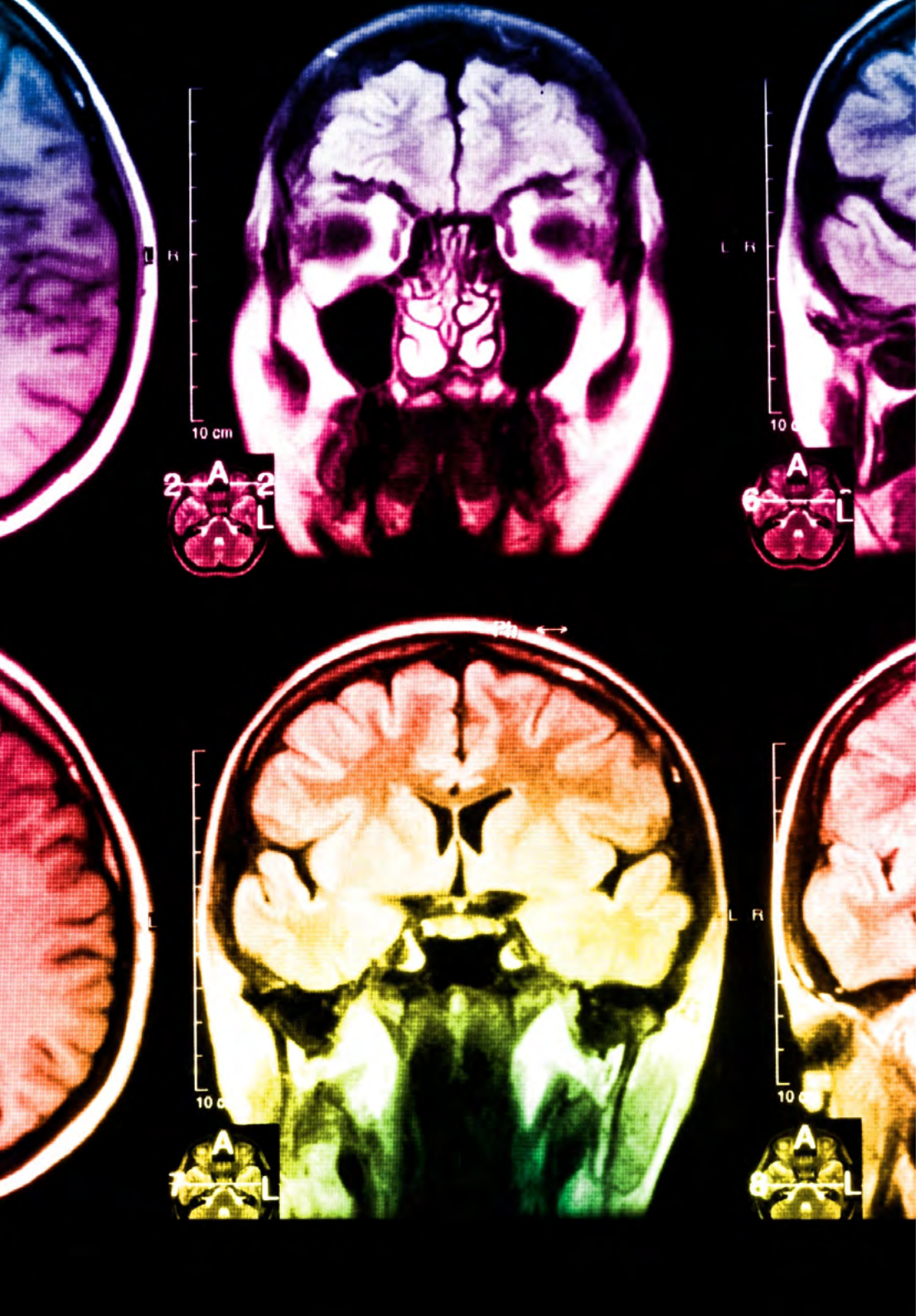
A TECH combina eficazmente a metodologia do Estudo de Caso com um sistema de aprendizagem 100% online baseado na repetição, que combina elementos didáticos diferentes em cada lição.

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

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

Na TECH aprende- com uma metodologia de vanguarda concebida para formar os gestores do futuro. Este método, na vanguarda da pedagogia mundial, chama-se Relearning.

A nossa universidade é a única universidade de língua espanhola licenciada para utilizar este método de sucesso. Em 2019, conseguimos melhorar os níveis globais de satisfação dos nossos estudantes (qualidade de ensino, qualidade dos materiais, estrutura dos cursos, objetivos...) no que diz respeito aos indicadores da melhor universidade online do mundo.



No nosso programa, a aprendizagem não é um processo linear, mas acontece numa espiral (aprender, desaprender, esquecer e reaprender). Portanto, cada um destes elementos é combinado de forma concêntrica. Esta metodologia formou mais de 650.000 licenciados com sucesso sem precedentes em áreas tão diversas como a bioquímica, genética, cirurgia, direito internacional, capacidades de gestão, ciência do desporto, filosofia, direito, engenharia, jornalismo, história, mercados e instrumentos financeiros. Tudo isto num ambiente altamente exigente, com um corpo estudantil universitário com um elevado perfil socioeconómico e uma idade média de 43,5 anos.

O Relearning permitir-lhe-á aprender com menos esforço e mais desempenho, envolvendo-o mais na sua capacitação, desenvolvendo um espírito crítico, defendendo argumentos e opiniões contrastantes: uma equação direta ao sucesso.

A partir das últimas provas científicas no campo da neurociência, não só sabemos como organizar informação, ideias, imagens e memórias, mas sabemos que o lugar e o contexto em que aprendemos algo é fundamental para a nossa capacidade de o recordar e armazenar no hipocampo, para o reter na nossa memória a longo prazo.

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

Este programa oferece o melhor material educativo, cuidadosamente preparado para profissionais:

Material de estudo

Todos os conteúdos didáticos são criados pelos especialistas que irão ensinar o curso, especificamente para o curso, para que o desenvolvimento didático seja realmente específico e concreto.

Estes conteúdos são depois aplicados ao formato audiovisual, para criar o método de trabalho online da TECH. Tudo isto, com as mais recentes técnicas que oferecem peças de alta-qualidade em cada um dos materiais que são colocados à disposição do aluno.

Masterclasses

Existem provas científicas sobre a utilidade da observação por terceiros especializada.

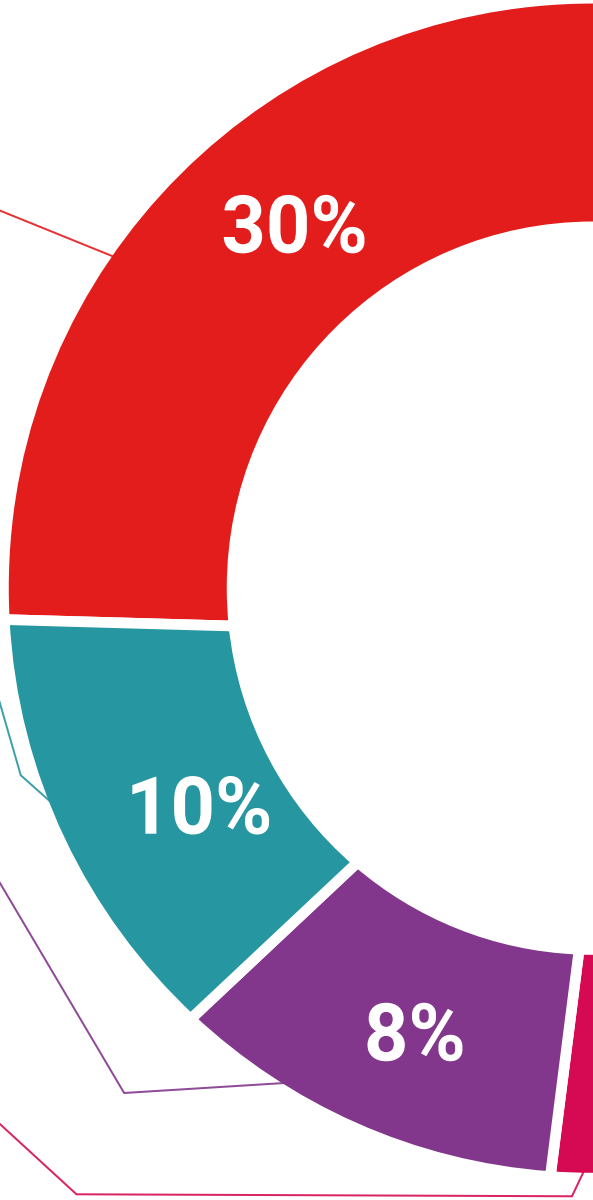
O denominado Learning from an Expert constrói conhecimento e memória, e gera confiança em futuras decisões difíceis.

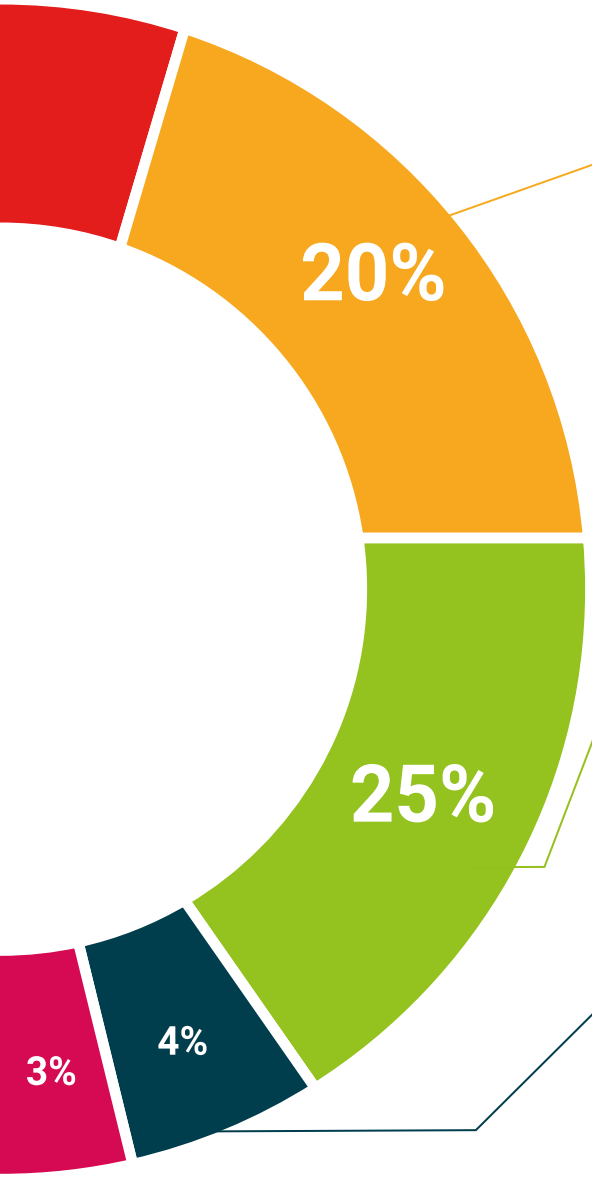
Práticas de aptidões e competências

Realizarão atividades para desenvolver competências e aptidões específicas em cada área temática. Práticas e dinâmicas para adquirir e desenvolver as competências e capacidades que um especialista necessita de desenvolver no quadro da globalização 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 necessita para completar a sua capacitação.





Case studies

Completarão uma seleção dos melhores estudos de casos escolhidos especificamente para esta situação. Casos apresentados, analisados e instruídos pelos melhores especialistas na cena internacional.

Resumos interativos

A equipa da TECH apresenta os conteúdos de uma forma atrativa e dinâmica em comprimidos multimédia que incluem áudios, vídeos, imagens, diagramas e mapas concetuais a fim de reforçar o conhecimento.

Este sistema educativo único para a apresentação de conteúdos multimédia foi premiado pela Microsoft como uma "História de Sucesso Europeu".

Testing & Retesting

Os conhecimentos do aluno são periodicamente avaliados e reavaliados ao longo de todo o programa, através de atividades e exercícios de avaliação e auto-avaliação, para que o aluno possa verificar como está a atingir os seus objetivos.

06

Certificação

O Curso de Hacking Ético garante, para além do conteúdo mais rigoroso e atualizado, o acesso a um certificado de Curso emitido pela TECH Universidade Tecnológica.

Conclua este plano de estudos com sucesso e receba o seu certificado sem sair de casa e sem burocracias"

Este **Curso de Hacking Ético** conta com o conteúdo educacional mais completo e atualizado do mercado.

Uma vez aprovadas as avaliações, o aluno receberá por correio, com aviso de receção, o certificado* correspondente ao título de **Curso** emitido pela **TECH Universidade Tecnológica.**

O certificado emitido pela TECH Universidade Tecnológica expressará a qualificação obtida no Mestrado Próprio, atendendo aos requisitos normalmente exigidos pelas bolsas de emprego, concursos públicos e avaliação de carreiras profissionais.

Certificação: **Curso de Hacking Ético**

Modalidade: **online**

Duração: **6 semanas**

ECTS: **6**


tech universidade tecnológica

Concede o presente

CERTIFICADO

a

Sr./Sra. _____, com o documento de identificação nº_____

Por ter completado e acreditado com sucesso o

CURSO

de

Hacking Ético

Este é um certificado concedido por esta Universidade, reconhecido por 6 ECTS e equivalente a 150 horas, com data de início a dd/mm/aaaaa e data de conclusão a dd/mm/aaaaa.

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

A 17 de junho de 2020

Prof. Dra. Tere Guevara Navarro
Reitora

Esta qualificação deve ser sempre acompanhada por um certificado universitário emitido pela autoridade competente para a prática profissional em cada país.

código único TECH: AFWOR23S techtitute.com/titulos

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

tech universidade tecnológica

Curso
Hacking Ético

- Modalidade: **online**
- Duração: **6 semanas**
- Certificação: **TECH Universidade Tecnológica**
- Acreditação: **6 ECTS**
- Horário: **ao seu próprio ritmo**
- Exames: **online**

Curso
Hacking Ético

tech universidade tecnológica