Curso de Especialização
Cibersegurança Corretiva e Perícia Forense

tech universidade tecnológica

tech universidade tecnológica

Curso de Especialização
Cibersegurança Corretiva e Perícia Forense

- Modalidade: **online**
- Duração: **6 meses**
- Certificação: **TECH Universidade Tecnológica**
- Acreditação: **18 ECTS**
- Horário: **ao seu próprio ritmo**
- Exames: **online**

Acesso ao site: www.techtitute.com/pt/informatica/curso-especializacao/curso-especializacao-ciberseguranca-corretiva-pericia-forense

Índice

01
Apresentação
pág. 4

02
Objetivos
pág. 8

03
Direção do curso
pág. 12

04
Estrutura e conteúdo
pág. 18

05
Metodologia
pág. 24

06
Certificação
pág. 32

01

Apresentação

Num mundo que muda e evolui todos os dias, com tecnologias que surgem e são adotadas rapidamente sem estarem maduras, temos de estar preparados para enfrentar muitos desafios e prever o impacto que terão na sociedade. Este Curso de Especialização forma engenheiros informáticos para investigarem um incidente de cibersegurança após a sua ocorrência, fornecendo-lhes os conhecimentos e os mecanismos para obterem, analisarem e comunicarem as suas conclusões, a partir do momento em que um cientista forense encontra um cenário e decide, de forma não destrutiva, adquirir as provas, necessita de diretrizes para relacionar os dados obtidos de diferentes fontes e chegar a conclusões irrefutáveis.

Adquirir a capacidade de dar as chaves de um incidente de cibersegurança com os conhecimentos mais atualizados em matéria de perícia forense nesta matéria"

No ambiente informático existem diferentes motivações que levam à aplicação de diferentes técnicas de engenharia inversa para compreender e saber o suficiente sobre um software, um protocolo de comunicação ou um algoritmo.

Uma das aplicações mais conhecidas da engenharia inversa é a análise de *malware* que, através de diferentes técnicas como o *sandboxing*, permite compreender e aprender sobre o software malicioso em estudo e, com isso, o desenvolvimento de software capaz de o detetar e neutralizar, como no caso do software antivírus que funciona por assinaturas.

Por vezes, a vulnerabilidade não está no código-fonte, mas é introduzida pelo compilador que gera o código de máquina. O conhecimento da engenharia inversa e, por conseguinte, da forma como obtemos o código de máquina permitir-nos-á detetar essas vulnerabilidades.

É necessário conhecer os diferentes cenários, compreender as diferentes tecnologias e ser capaz de as explicar em diferentes línguas, consoante o público-alvo do relatório específico. O número de crimes diferentes com que um perito forense terá de lidar significa que ele ou ela precisa de perícia, perspicácia e serenidade para levar a cabo esta tarefa extremamente importante, uma vez que o veredicto de um julgamento pode depender do seu correto desempenho.

Os profissionais deste setor precisam de ter uma visão ampla e periférica para detetar não só os benefícios destas tecnologias, mas também as suas possíveis desvantagens. Este Curso de Especialização prepara para compreender o que está para vir, como pode afetar as profissões atuais, como são exercidas e o que pode acontecer num futuro por vezes incerto.

Este **Curso de Especialização em Cibersegurança Corretiva e Perícia Forense** conta com o conteúdo educativo mais completo e atualizado do mercado. As suas principais características são:

- O desenvolvimento de casos práticos apresentados por especialistas
- 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

Compreenda os fundamentos e o modus operandi do malware como base para a criação de vias de atuação altamente eficazes"

Com uma abordagem totalmente centrada na prática, este Curso de Especialização irá aumentar as suas competências ao nível de um especialista"

Uma aprendizagem que lhe permitirá trabalhar como perito forense em cibersegurança na área jurídica.

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

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

02

Objetivos

Este Curso de Especialização reforça a capacidade de intervenção dos alunos 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.

Uma aprendizagem intensiva em Cibersegurança Corretiva e Perícia Forense que lhe permitirá alargar o seu campo de trabalho numa área cheia de possibilidades de emprego"

Objetivos gerais

- Analisar a engenharia inversa e as suas diferentes técnicas
- Examinar diferentes arquiteturas e a forma como afetam a engenharia inversa
- Determinar em que condições devem ser utilizadas as diferentes técnicas de engenharia inversa
- Aplicar a engenharia inversa ao ambiente de cibersegurança
- Recolher todas as provas e dados existentes para levar a cabo um relatório forense
- Analisar os dados e correlacioná-los adequadamente
- Preservar as provas para elaborar um relatório forense
- Apresentar devidamente o relatório forense
- Analisar o estado atual e futuro da segurança informática
- Analisar os riscos das novas tecnologias emergentes
- Compilar as diferentes tecnologias em relação à segurança informática

Objetivos específicos

Módulo 1. Engenharia inversa

- Analisar as fases de um compilador
- Examinar a arquitetura de processadores x86 e a arquitetura de processadores ARM
- Determinar os diferentes tipos de análise
- Aplicar *sandboxing* em diferentes ambientes
- Desenvolver as diferentes técnicas de análise de *malware*
- Estabelecer as ferramentas orientadas para a análise de *malware*

Módulo 2. Análise forense

- Identificar os diferentes elementos que revelam um crime
- Gerar conhecimentos especializados para obter dados de diferentes meios de comunicação antes que estes se percam
- Recuperar dados eliminados intencionalmente
- Analisar os registos dos sistemas
- Determinar como são duplicados os dados de modo a não alterar os originais
- Fundamentar as provas para que sejam consistentes
- Gerar um relatório sólido e sem falhas
- Apresentar as conclusões de forma coerente
- Estabelecer como defender o relatório perante a autoridade competente
- Concretizar estratégias para um teletrabalho seguro

Módulo 3. Desafios atuais e futuros em matéria de segurança informática

- Examinar a utilização de criptomoedas, o impacto na economia e na segurança
- Analisar a situação dos utilizadores e o grau de iliteracia digital
- Determinar o âmbito de utilização da *blockchain*
- Apresentar alternativas ao IPv4 no endereçamento de redes
- Desenvolver estratégias para educar a população na utilização correta das tecnologias
- Gerar conhecimentos especializados para enfrentar novos desafios de segurança e evitar a usurpação de identidade
- Concretizar estratégias para um teletrabalho seguro

Adquira a competência necessária para preparar e apresentar um relatório exaustivo e de qualidade à autoridade competente"

03

Direção do curso

Os professores que lecionam este Curso de Especialização 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 deles, o Curso de Especialização oferece a visão mais direta e imediata das características reais da intervenção neste domínio, alcançando uma visão contextual de máximo interesse.

Os especialistas em cibersegurança acompanhá-lo-ão em cada fase do estudo e dar-lhe-ão uma visão mais realista deste trabalho"

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

Professores

Sr. Jesús Serrano Redondo

- Programador FrontEnd Júnior e Técnico de Cibersegurança Júnior
- Programador FrontEnd na Telefónica, Madrid
- Programador FrontEnd. Best Pro Consulting SL, Madrid
- Instalador de equipamentos e serviços de telecomunicações. Grupo Zener, Castilla y León
- Instalador de equipamentos e serviços de telecomunicações. Lican Comunicaciones SL, Castilla y León
- Certificado em Segurança Informática. CFTIC Getafe, Madrid
- Técnico superior: Sistemas de telecomunicações e Informáticos. IES Trinidad Arroyo, Palencia
- Técnico superior: Instalações Eletrotécnicas de MT e BT. IES Trinidad Arroyo, Palencia
- Formação em engenharia inversa, estenografia, encriptação. Academia Hacker Incibe (Talentos Incibe)

Um percurso de crescimento profissional estimulante concebido para o manter interessado e motivado durante toda a capacitação"

04

Estrutura e conteúdo

Este Curso de Especialização é uma análise completa de todos e cada um das áreas de conhecimento que o profissional envolvido em cibersegurança deve conhecer no domínio da cibersegurança corretiva e da perícia forense. 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 Especialização de alta intensidade e qualidade criado para capacitar os melhores do setor.

Todos os conceitos da Cibersegurança Corretiva e Perícia Forense desenvolvidos de forma estruturada numa abordagem de estudo centrada na eficiência"

Módulo 1. Engenharia Inversa

1.1. Compiladores
- 1.1.1. Tipos de códigos
- 1.1.2. Fases de um compilador
- 1.1.3. Tabela de símbolos
- 1.1.4. Gestor de erros
- 1.1.5. Compilador GCC

1.2. Tipos de análise em compiladores
- 1.2.1. Análise lexical
  - 1.2.1.1. Terminologia
  - 1.2.1.2. Componentes léxicos
  - 1.2.1.3. Analisador léxico LEX
- 1.2.2. Análise sintática
  - 1.2.2.1. Gramáticas livres de contexto
  - 1.2.2.2. Tipos de análise sintática
    - 1.2.2.2.1. Análise descendente
    - 1.2.2.2.2. Análise ascendente
  - 1.2.2.3. Árvores sintáticas e derivações
  - 1.2.2.4. Tipos de analisadores sintáticos
    - 1.2.2.4.1. Analisadores LR (*Left To Right*)
    - 1.2.2.4.2. Analisadores LALR
- 1.2.3. Análise semântica
  - 1.2.3.1. Gramáticas de atributos
  - 1.2.3.2. S-atribuídas
  - 1.2.3.3. L-atribuídas

1.3. Estruturas de dados de montagem
- 1.3.1. Variáveis
- 1.3.2. Matrizes
- 1.3.3. Indicadores
- 1.3.4. Estruturas
- 1.3.5. Objetos

1.4. Estruturas de código de montagem
- 1.4.1. Estruturas de seleção
  - 1.4.1.1. If, else if, Else
  - 1.4.1.2. *Switch*
- 1.4.2. Estruturas de iteração
  - 1.4.2.1. *For*
  - 1.4.2.2. *While*
  - 1.4.2.3. Utilização do *break*
- 1.4.3. Funções

1.5. Arquitetura hardware x86
- 1.5.1. Arquitetura de processadores x86
- 1.5.2. Estruturas de dados em x86
- 1.5.3. Estruturas de código em x86

1.6. Arquitetura hardware ARM
- 1.6.1. Arquitetura de processadores ARM
- 1.6.2. Estruturas de dados em ARM
- 1.6.3. Estruturas de código em ARM

1.7. Análise de código estático
- 1.7.1. Desmontadores
- 1.7.2. IDA
- 1.7.3. Reconstrutores de código

1.8. Análise de código dinâmico
- 1.8.1. Análise comportamental
  - 1.8.1.1. Comunicações
  - 1.8.1.2. Monitorização
- 1.8.2. Depuradores de código em Linux
- 1.8.3. Depuradores de código em Windows

1.9. *Sandbox*
- 1.9.1. Arquitetura de uma *Sandbox*
- 1.9.2. Evasão de uma *Sandbox*
- 1.9.3. Técnicas de deteção
- 1.9.4. Técnicas de evasão
- 1.9.5. Contramedidas
- 1.9.6. *Sandbox* em Linux
- 1.9.7. *Sandbox* em Windows
- 1.9.8. *Sandbox* em MacOS
- 1.9.9. *Sandbox* em Android

1.10. Análise de *malwares*
- 1.10.1. Métodos de análise de *malware*
- 1.10.2. Técnicas de ofuscação de *malware*
  - 1.10.2.1. Ofuscação de executáveis
  - 1.10.2.2. Restrição de ambientes de execução
- 1.10.3. Ferramentas de análise de *malware*

Módulo 2. Análise forense

2.1. Aquisição de dados e duplicação
- 2.1.1. Aquisição de dados voláteis
  - 2.1.1.1. Informação do sistema
  - 2.1.1.2. Informação da rede
  - 2.1.1.3. Ordem de volatilidade
- 2.1.2. Aquisição de dados estáticos
  - 2.1.2.1. Criação de uma imagem duplicada
  - 2.1.2.2. Preparação de um documento para a cadeia de custódia
- 2.1.3. Métodos de validação dos dados adquiridos
  - 2.1.3.1. Métodos para Linux
  - 2.1.3.2. Métodos para Windows

2.2. Avaliação e derrota de técnicas antiforenses
- 2.2.1. Objetivos das técnicas antiforenses
- 2.2.2. Eliminação de dados
  - 2.2.2.1. Eliminação de dados e ficheiros
  - 2.2.2.2. Recuperação de ficheiros
  - 2.2.2.3. Recuperação de partições eliminadas
- 2.2.3. Proteção por palavra-passe
- 2.2.4. Esteganografia
- 2.2.5. Limpeza segura de dispositivos
- 2.2.6. Encriptação

2.3. Análise forense do sistema operativo
- 2.3.1. Análise forense de Windows
- 2.3.2. Análise forense de Linux
- 2.3.3. Análise forense de Mac

2.4. Análise forense da rede
- 2.4.1. Análise dos registos
- 2.4.2. Correlação de dados
- 2.4.3. Investigação da rede
- 2.4.4. Passos a seguir na análise forense da rede

2.5. Análise forense web
- 2.5.1. Investigação dos ataques Web
- 2.5.2. Deteção de ataques
- 2.5.3. Localização de endereços IP

2.6. Análise forense de bases de dados
- 2.6.1. Análise forense em MSSQL
- 2.6.2. Análise forense em MySQL
- 2.6.3. Análise forense em PostgreSQL
- 2.6.4. Análise forense em MongoDB

2.7. Análise forense na Cloud
- 2.7.1. Tipos de crimes na Cloud
  - 2.7.1.1. Cloud como sujeito
  - 2.7.1.2. Cloud como objeto
  - 2.7.1.3. Cloud como ferramenta
- 2.7.2. Desafios da análise forense na Cloud
- 2.7.3. Investigação dos serviços de armazenamento na Cloud
- 2.7.4. Ferramentas de análise forense na Cloud

2.8. Investigação de crimes por correio eletrónico
- 2.8.1. Sistemas de correio eletrónico
  - 2.8.1.1. Clientes de correio eletrónico
  - 2.8.1.2. Servidor de correio eletrónico
  - 2.8.1.3. Servidor SMTP
  - 2.8.1.4. Servidor POP3
  - 2.8.1.5. Servidor IMAP4
- 2.8.2. Crimes de correio eletrónico
- 2.8.3. Mensagem de correio eletrónico
  - 2.8.3.1. Cabeçalhos padrão
  - 2.8.3.2. Cabeçalhos estendidos
- 2.8.4. Etapas da investigação destes crimes
- 2.8.5. Ferramentas forenses para correio eletrónico

2.9. Análise forense de dispositivos móveis
- 2.9.1. Redes celulares
  - 2.9.1.1. Tipos de Redes
  - 2.9.1.2. Conteúdo do CR
- 2.9.2. *Subscriber Identity Module* (SIM)
- 2.9.3. Aquisição lógica
- 2.9.4. Aquisição física
- 2.9.5. Aquisição do sistema de ficheiros

2.10. Redação e apresentação de relatórios forenses
- 2.10.1. Aspetos importantes de um relatório forense
- 2.10.2. Classificação e tipos de relatórios
- 2.10.3. Guia para a redação de um relatório
- 2.10.4. Apresentação do relatório
  - 2.10.4.1. Preparação prévia para testemunhar
  - 2.10.4.2. Deposição
  - 2.10.4.3. Lidar com os meios

Módulo 3. Desafios atuais e futuros da segurança informática

3.1. Tecnologia *blockchain*
- 3.1.1. Âmbitos de aplicação
- 3.1.2. Garantia de confidencialidade
- 3.1.3. Garantia de não repúdio

3.2. Moeda digital
- 3.2.1. Bitcoins
- 3.2.2. Criptomoedas
- 3.2.3. Mineração de criptomoedas
- 3.2.4. Esquemas de pirâmide
- 3.2.5. Outros potenciais crimes e problemas

3.3. *Deepfake*
- 3.3.1. Impacto nos meios de comunicação
- 3.3.2. Perigos para a sociedade
- 3.3.3. Mecanismos de deteção

3.4. O futuro da inteligência artificial
- 3.4.1. Inteligência artificial e computação cognitiva
- 3.4.2. Utilizações para simplificar o serviço ao cliente

3.5. Privacidade digital
- 3.5.1. Direitos dos dados na internet
- 3.5.2. Utilização dos dados na internet
- 3.5.3. Gestão da privacidade e da identidade digital

3.6. Ciberconflitos, cibercriminosos e ciberataques
- 3.6.1. O impacto da cibersegurança nos conflitos internacionais
- 3.6.2. Consequências dos ciberataques para a população em geral
- 3.6.3. Tipos de cibercriminosos. Medidas de proteção

3.7. Teletrabalho
- 3.7.1. Revolução do teletrabalho durante e após a COVID-19
- 3.7.2. Obstáculos de acesso
- 3.7.3. Variação da superfície de ataque
- 3.7.4. Necessidades dos colaboradores

3.8. Tecnologias *wireless* emergentes
- 3.8.1. WPA3
- 3.8.2. 5G
- 3.8.3. Ondas milimétricas
- 3.8.4. Tendência do "*Get Smart*" em vez de "*Get more*"

3.9. Endereçamento futuro em redes
- 3.9.1. Problemas atuais com o endereçamento IP
- 3.9.2. IPv6
- 3.9.3. IPv4+
- 3.9.4. Vantagens do IPv4+ em relação ao IPv4
- 3.9.5. Vantagens do IPv6 em relação ao IPv4

3.10. O desafio da sensibilização para a educação precoce e contínua da população
- 3.10.1. Estratégias governamentais atuais
- 3.10.2. Resistência da população à aprendizagem
- 3.10.3. Planos de formação a serem adotados pelas empresas

Um Curso de Especialização de alto impacto para as suas competências que lhe permitirá intervir eficazmente na Cibersegurança Corretiva e Perícia Forense com recursos de ponta"

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

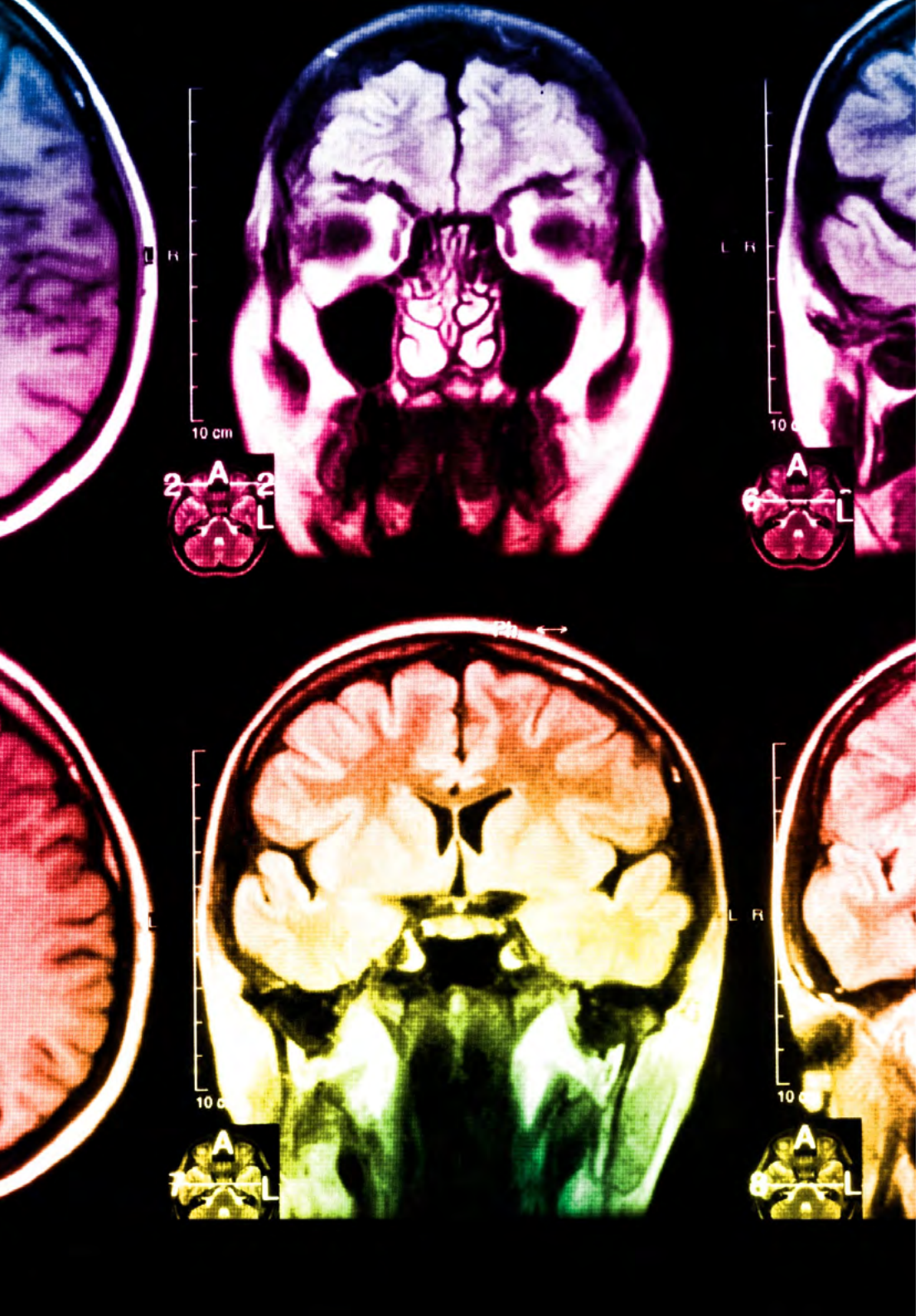
A TECH combina eficazmente a metodologia do Estudo de Caso com um sistema de aprendizagem 100% online baseado na repetição, que combina elementos didáticos diferentes em cada lição.

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.

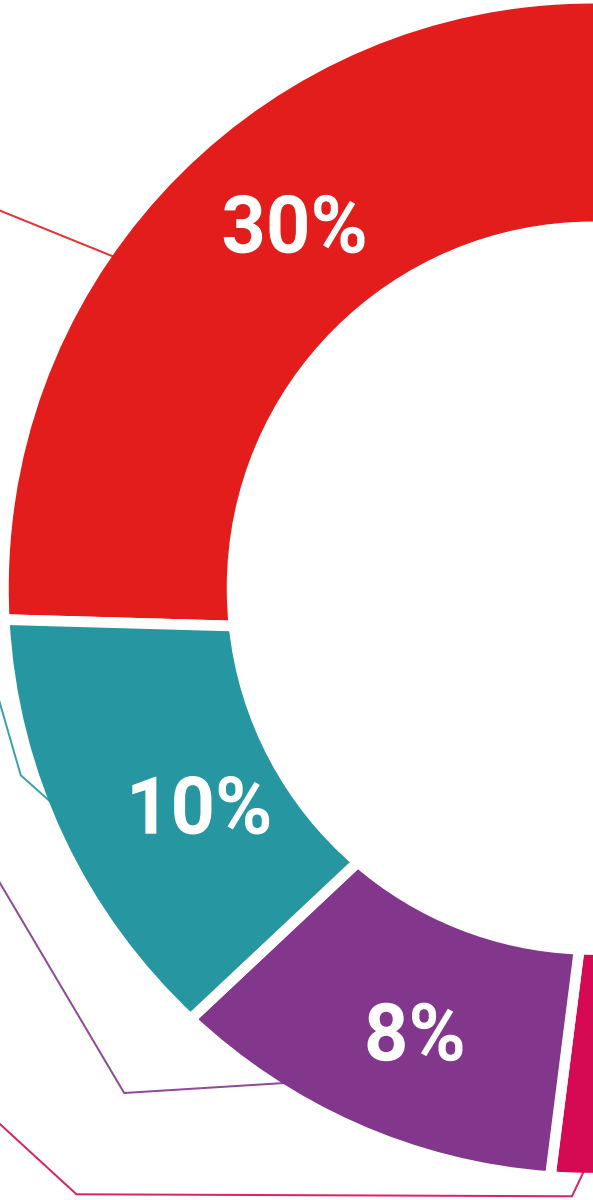
O denominado Learning from an Expert constrói conhecimento e memória, e gera confiança em futuras decisões difíceis.

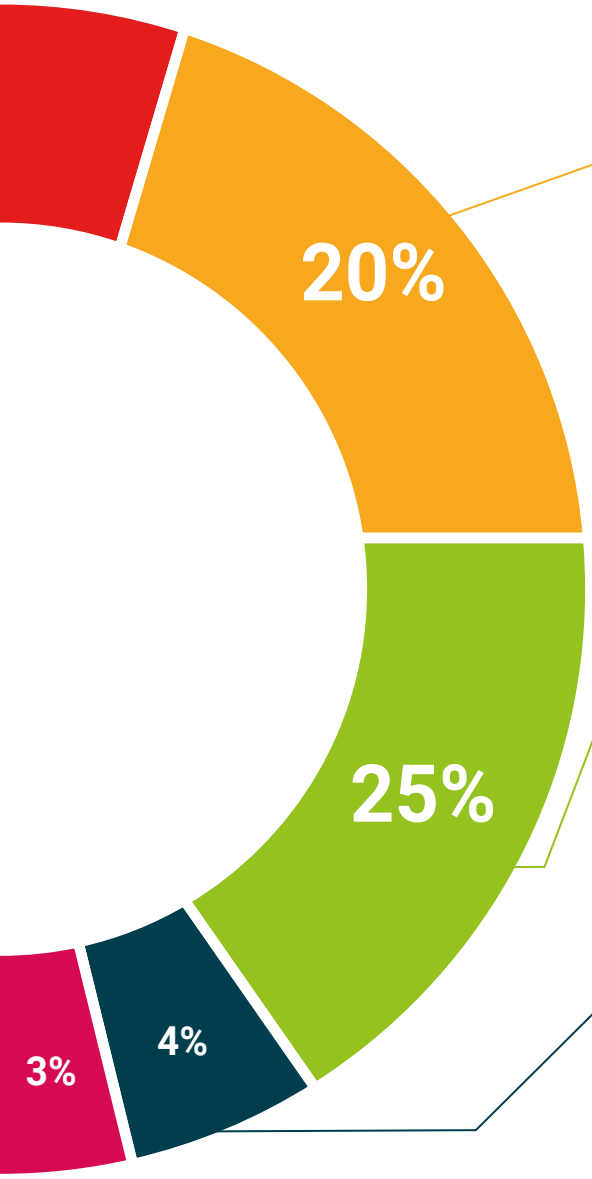
Práticas de aptidões e competências

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 Especialização em Cibersegurança Corretiva e Perícia Forense garante, para além do conteúdo mais rigoroso e atualizado, o acesso a um certificado de Curso de Especialização 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 Especialização em Cibersegurança Corretiva e Perícia Forense** 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 de Especialização** 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 Especialização em Cibersegurança Corretiva e Perícia Forense**

Modalidade: **online**

Duração: **6 meses**

ECTS: **18 ECTS**

tech universidade tecnológica

Concede o presente

CERTIFICADO

a

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

Por ter completado e certificado com sucesso o

CURSO DE ESPECIALIZAÇÃO

em

Cibersegurança Corretiva e Perícia Forense

Este é um certificado atribuído por esta Universidade, reconhecido por 18 ECTS e equivalente a 450 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

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 de Especialização
Cibersegurança Corretiva e Perícia Forense

- Modalidade: **online**
- Duração: **6 meses**
- Certificação: **TECH Universidade Tecnológica**
- Acreditação: **18 ECTS**
- Horário: **ao seu próprio ritmo**
- Exames: **online**

Curso de Especialização
Cibersegurança Corretiva e Perícia Forense

tech universidade tecnológica