Curso
Criptografia Avançada

tech universidade tecnológica

tech universidade tecnológica

Curso

Criptografia Avançada

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

Acesso ao site: **www.techtitute.com/pt/informatica/curso/criptografia-avancada**

Índice

01 Apresentação — *pág. 4*

02 Objetivos — *pág. 8*

03 Direção do curso — *pág. 12*

04 Estrutura e conteúdo — *pág. 16*

05 Metodologia — *pág. 20*

06 Certificação — *pág. 28*

01

Apresentação

A criptografia tem vindo a ganhar importância nos últimos anos. Não só é uma disciplina essencial na encriptação de senhas e dados, como também é um elemento central num novo domínio tecnológico que está a sofrer um grande crescimento: a *Blockchain*. É por isso que as empresas do setor digital e do desenvolvimento de aplicações e outras ferramentas informáticas procuram especialistas com competências criptográficas avançadas. Assim, este Curso oferece aos profissionais um estudo completo e aprofundado desta área, preparando-os para responder aos desafios atuais e futuros da cibersegurança. Tudo isto se baseia numa metodologia de ensino online com a qual pode conciliar o seu trabalho e os seus estudos de uma forma confortável e simples.

A criptografia é essencial para a cibersegurança das empresas e para tecnologias como a Blockchain. Por isso, este Curso prepará-lo-á intensivamente para evoluir profissionalmente neste importante domínio informático"

A importância crescente da cibersegurança levou a um enorme impulso na criptografia. Esta disciplina permite codificar, cifrar e encriptar todos os tipos de dados, quer se trate de informações sensíveis da empresa, de transações ou de senhas de acesso. É, por isso, essencial no atual mundo digital. Além disso, o surgimento de outras áreas como a *Blockchain* ou a inteligência artificial deu-lhe um impulso extra, tornando-o num setor com uma elevada procura de profissionais especializados.

Este Curso de Criptografia Avançada oferece, assim, a possibilidade de explorar este campo, preparando o informático para responder a todos os desafios atuais e futuros nesta área. Ao longo deste Curso, o profissional aprofundará temas como a esteganografia e a estegoanálise, a combinação de cifras de bloco, a criptografia assimétrica e os algoritmos quânticos.

Baseado num ensino 100% online, este Curso permitirá ao informático progredir profissionalmente graças aos seus conteúdos modernos e ao seu corpo docente, composto por especialistas em criptografia que estão a par dos últimos desenvolvimentos nesta área e das suas novas aplicações práticas.

Este **Curso de Criptografia Avançada** conta com o conteúdo educacional mais completo e atualizado do mercado. As suas principais características são:

- O desenvolvimento de casos práticos apresentados por especialistas em Informática Cibersegurança
- O conteúdo gráfico, esquemático e eminentemente prático fornece informações científicas e práticas sobre as disciplinas que são essenciais para a prática profissional
- Exercícios práticos em que o processo de autoavaliação pode ser utilizado para melhorar a aprendizagem
- A sua ênfase especial em metodologias inovadoras
- Palestras teóricas, perguntas ao especialista, fóruns de discussão sobre questões controversas e atividades de reflexão individual.
- A disponibilidade de acesso ao conteúdo a partir de qualquer dispositivo fixo ou portátil com ligação à Internet

Conheça as mais recentes aplicações da criptografia graças a este Curso, que é lecionado através de uma metodologia 100% online"

Poderá aprender mais sobre as melhores técnicas criptográficas através de numerosos recursos multimédia: atividades práticas, resumos multimédia, masterclasses, etc"

As empresas tecnológicas necessitam de especialistas em Criptografia Avançada e este Curso prepará-lo-á para melhorar profissionalmente.

O sistema de aprendizagem da TECH permitir-lhe-á continuar a desenvolver a sua carreira profissional sem interrupções ou horários fixos.

O pessoal docente do Curso inclui profissionais do setor que trazem para esta capacitação a experiência do seu trabalho, bem como especialistas reconhecidos de sociedades líderes e universidades de prestígio.

Graças ao seu conteúdo multimédia, desenvolvido com a mais recente tecnologia educativa, o profissional terá acesso a uma aprendizagem situada e contextual, isto é, um ambiente de simulação que proporcionará uma educação imersiva, programada para praticar em situações reais.

A conceção desta qualificação centra-se na Aprendizagem Baseada em Problemas, através da qual o especialista deve tentar resolver as diferentes situações da prática profissional que surgem ao longo do Curso. Para tal, contará com a ajuda de um sistema inovador de vídeo interativo desenvolvido por especialistas reconhecidos.

02

Objetivos

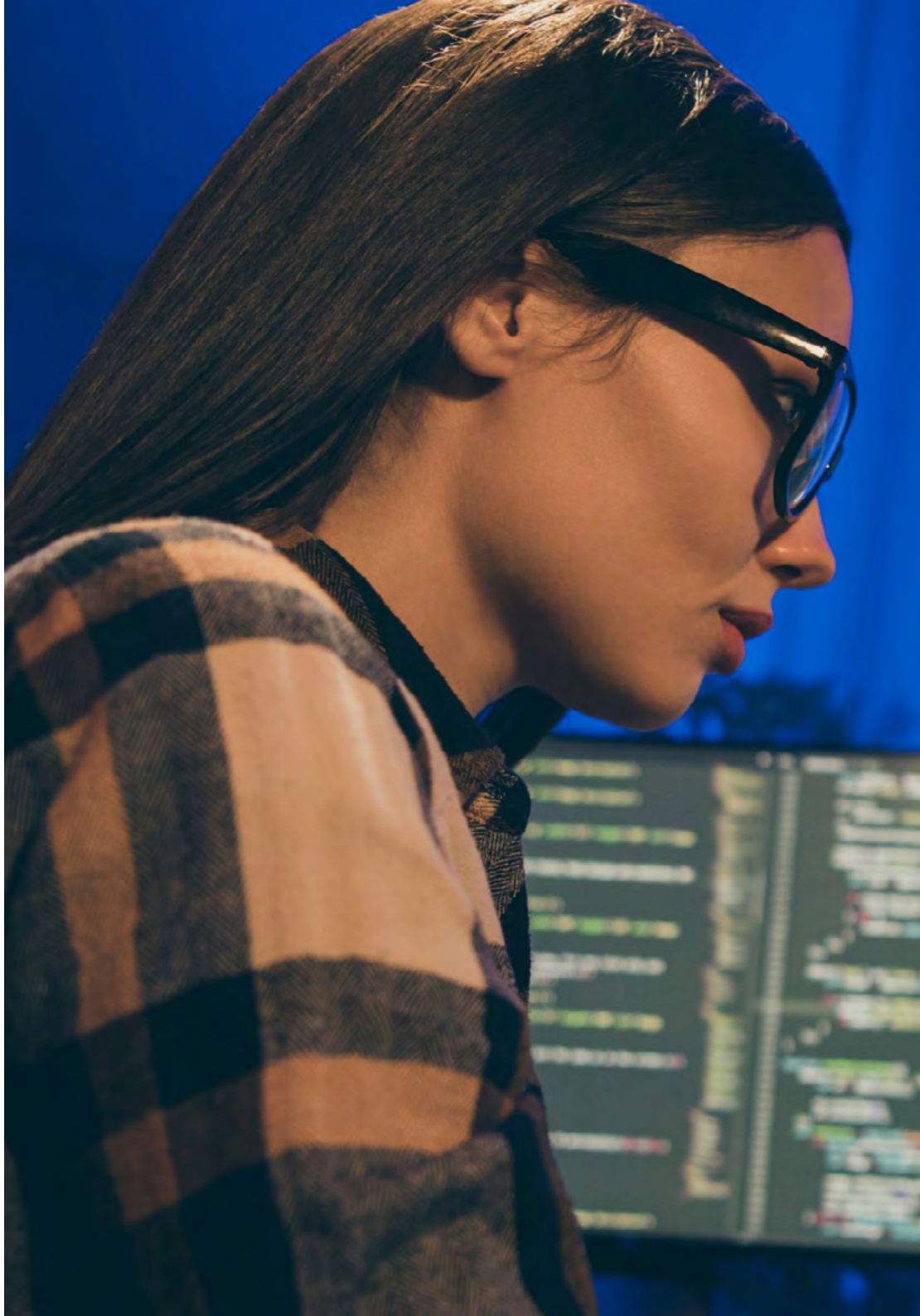
O principal objetivo deste Curso de Criptografia Avançada é transmitir ao profissional os melhores métodos criptográficos, bem como as novas aplicações desta importante disciplina. Assim, tornar-se-á um informático especializado em criptografia capaz de resolver diferentes problemas, seja ao nível da segurança das senhas de acesso a um determinado sistema ou em tecnologias emergentes como a *Blockchain*. Isto prepará-lo-á para trabalhar em diferentes domínios e alargará as suas perspetivas profissionais.

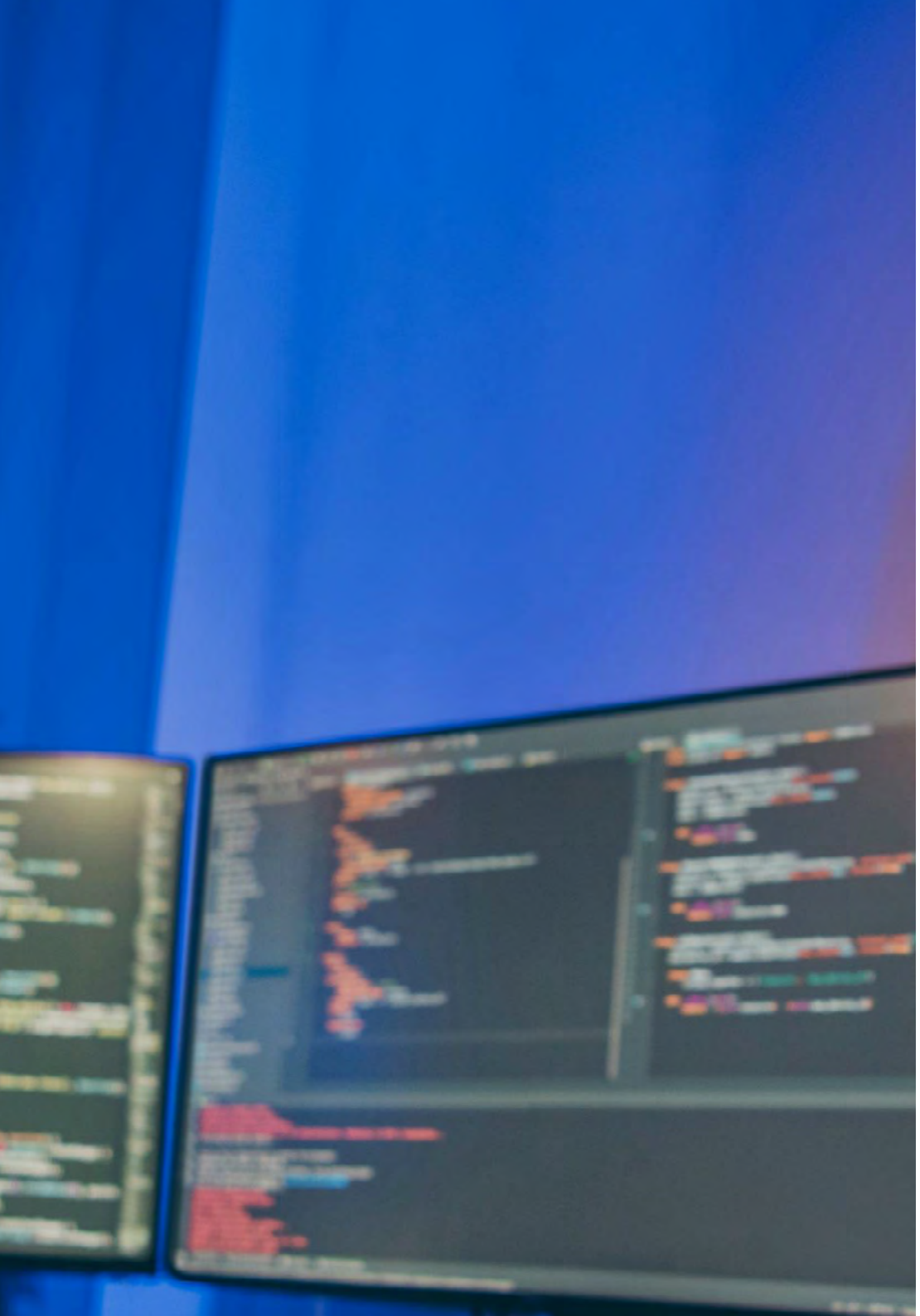
Alcance todos os seus objetivos profissionais ao especializar-se em Criptografia Avançada graças a este Curso"

Objetivos gerais

- Examinar a ciência da criptologia e a relação com os seus ramos: criptografia, criptoanálise, esteganografia e estegoanálise
- Analisar os tipos de criptografia de acordo com o tipo de algoritmo e de acordo com a sua utilização
- Compilar Sistemas de gestão de chaves
- Avaliar as diferentes aplicações práticas
- Examinar os certificados digitais
- Examinar a Infraestrutura de Chave Pública (PKI)
- Analisar as últimas tendências e desafios

A criptografia será essencial para o seu futuro profissional: inscreva-se agora e prepare-se para importantes oportunidades na área da cibersegurança"





Objetivos específicos

- Compilar as operações fundamentais (XOR, grandes números, substituição e transposição) e os vários componentes (funções One-Way, Hash, geradores de números aleatórios)
- Analisar as técnicas criptográficas
- Desenvolver os diferentes algoritmos criptográficos
- Demonstrar a utilização de assinaturas digitais e a sua aplicação nos certificados digitais
- Avaliar os sistemas de gestão de chaves e a importância da longitude das chaves criptográficas
- Examinar algoritmos de derivação de chaves
- Analisar o ciclo de vida das chaves
- Avaliação dos modos de cifragem de blocos e cifragem de fluxo
- Determinar os geradores de números pseudoaleatórios
- Desenvolver casos reais de aplicações criptográficas, tais como Kerberos, PGP ou cartões inteligentes
- Examinar associações e organismos relacionados, tais como ISO, NIST ou NCSC
- Determinar os desafios na criptografia da computação quântica

03

Direção do curso

A criptografia é um domínio muito complexo para o qual se pretende a melhor preparação. O surgimento de novos setores tecnológicos, para os quais a criptografia é um elemento básico, levou a um crescimento exponencial neste campo, e a sua enorme dificuldade exige o acompanhamento de especialistas para compreender os seus pormenores. Por este motivo, a TECH reuniu um corpo docente de grande prestígio que acompanhará o aluno ao longo de todo o processo de aprendizagem, garantindo que todos os elementos-chave da criptografia atual sejam assimilados de forma ágil e simples.

O corpo docente da TECH orientá-lo-á para que as 150 horas de aprendizagem deste Curso sejam eficazes e o promovam profissionalmente"

Direção

Sr. Olalla Bonal, Martín

- Client Technical Specialist Blockchain na IBM
- Blockchain Technical Specialist na IBM SPGI
- Arquiteto *Blockchain*
- Arquiteto de Infraestruturas na Banca
- Gestão de projetos e implementação de soluções
- Técnico em Eletrónica Digital
- Docente: Formação Hyperledger Fabric a empresas
- Docente: Formação Blockchain indicada para negócios em empresas

Professores

Dr. Ortega Esteban, Octavio

- Programador de Aplicações Informáticas e Desenvolvimento Web
- Web Designer e de APPS para clientes, CRDS para a investigação do Instituto de Saúde Carlos III, lojas online, aplicações Android, etc.
- Docente de Segurança Informática
- Licenciado em Psicologia pela Universidade Oberta de Catalunya
- Técnico Superior Universitário em Análise, Design e Soluções de Software
- Técnico Superior Universitário em Programação Avançada

A nossa equipa pedagógica fornecer-lhe-á todos os seus conhecimentos para que esteja a par das últimas informações sobre a matéria"

04

Estrutura e conteúdo

O Curso de Criptografia Avançada foi pensado para responder à procura atual de especialistas nesta disciplina, e o seu módulo específico ajudará os profissionais a aprofundar aspetos relevantes da cibersegurança, como a criptografia assimétrica, os certificados digitais, os protocolos de telefonia móvel, a proteção de algoritmos contra a computação quântica ou a distribuição quântica de senhas. Tudo isto através de 150 horas de aprendizagem oferecidas ao longo de seis semanas.

O Curso mais atualizado de Criptografia Avançada prepará-lo-á para conhecer todas as ferramentas para proteger os algoritmos contra a computação quântica"

Módulo 1 Criptografia em IT

1.1. Criptografia
- 1.1.1. Criptografia
- 1.1.2. Fundamentos matemáticos

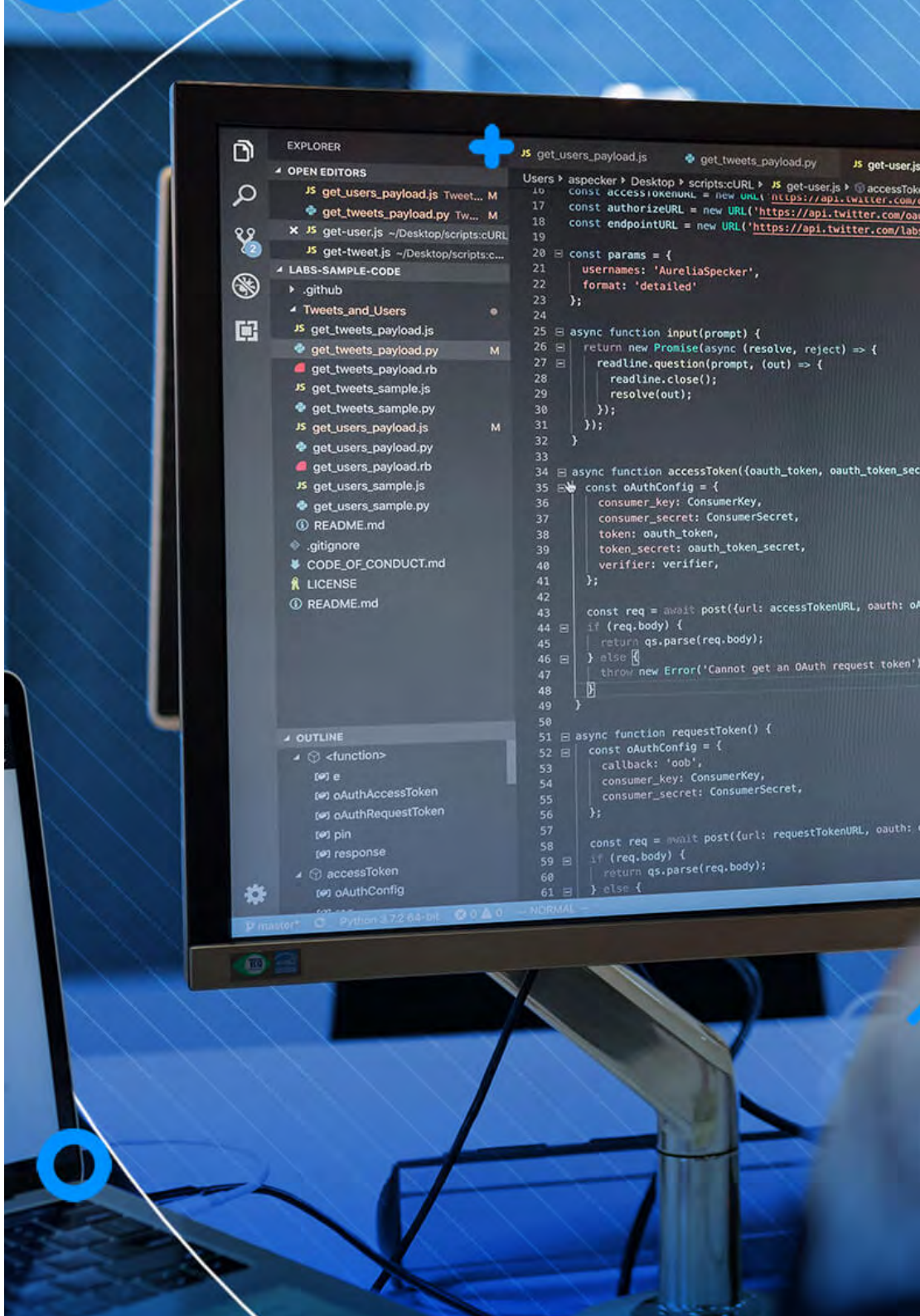
1.2. Criptologia
- 1.2.1. Criptologia
- 1.2.2. Criptoanálise
- 1.2.3. Criptoanálise

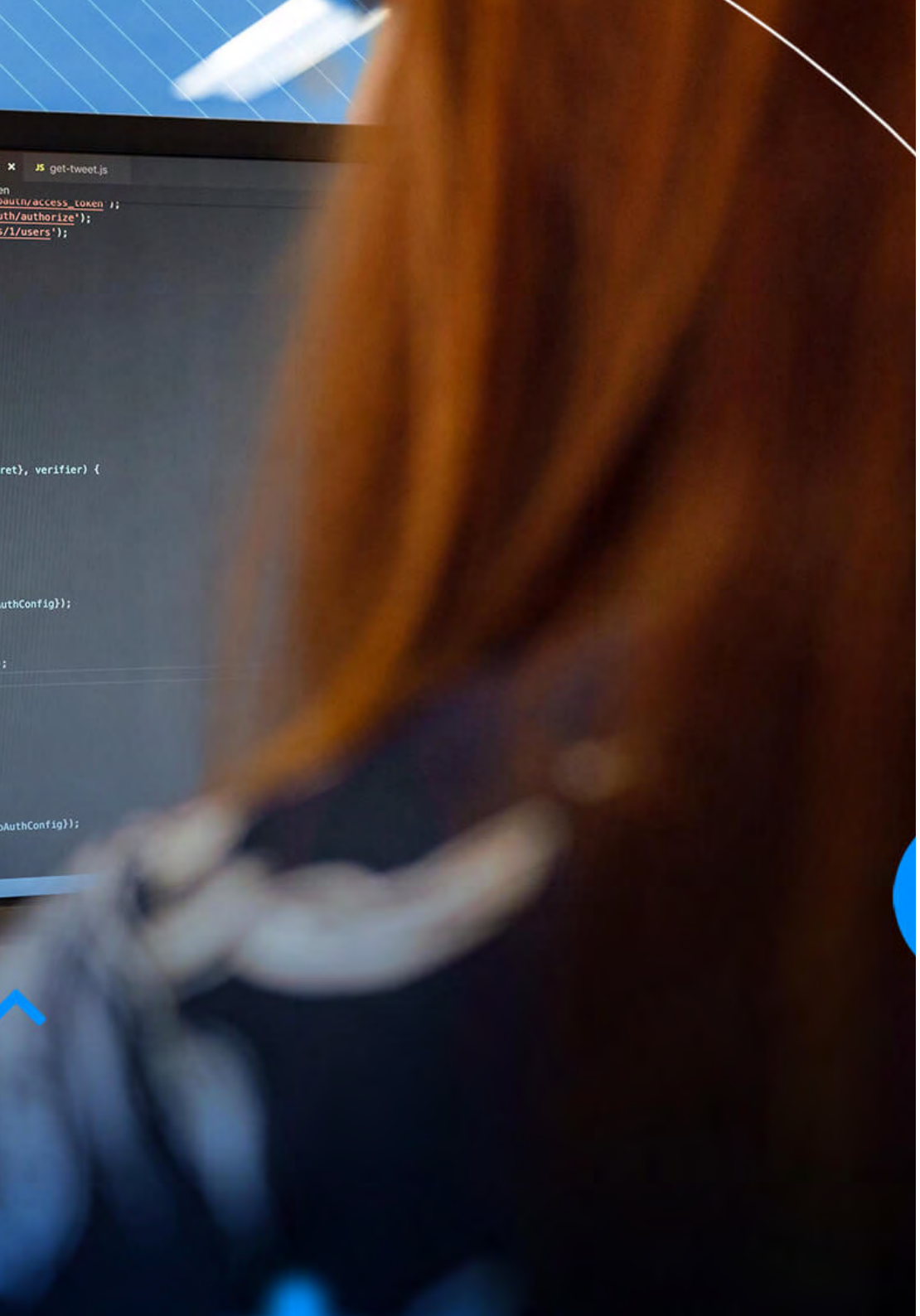
1.3. Protocolos criptográficos
- 1.3.1. Blocos básicos
- 1.3.2. Protocolos básicos
- 1.3.3. Protocolos intermédios
- 1.3.4. Protocolos avançados
- 1.3.5. Protocolos esotéricos

1.4. Técnicas criptográficas
- 1.4.1. Longitude de chaves
- 1.4.2. Gestão de chaves
- 1.4.3. Tipos de algoritmos
- 1.4.4. Funções resumo. Hash
- 1.4.5. Geradores de números pseudoaleatórios
- 1.4.6. Uso de algoritmos

1.5. Criptografia simétrica
- 1.5.1. Cifras de bloco
- 1.5.2. DES (*Data Encryption Standard*)
- 1.5.3. Algoritmo RC4
- 1.5.4. AES (*Advanced Encryption Standard*)
- 1.5.5. Combinação de cifras de bloco
- 1.5.6. Derivação de chaves

1.6. Criptografia assimétrica
- 1.6.1. Diffie-Hellman
- 1.6.2. DSA (*Digital Signature Algorithm*)
- 1.6.3. RSA (Rivest, Shamir e Adleman)
- 1.6.4. Curva elíptica
- 1.6.5. Criptografia assimétrica Tipologia





1.7. Certificados digitais
  1.7.1. Assinatura digital
  1.7.2. Certificados X509
  1.7.3. Infraestrutura de chave pública (PKI)
1.8. Implementações
  1.8.1. Kerberos
  1.8.2. IBM CCA
  1.8.3. *Pretty Good Privacy* (PGP)
  1.8.4. ISO *Authentication Framework*
  1.8.5. SSL e TLS
  1.8.6. Cartões inteligentes em meios de pagamento (EMV)
  1.8.7. Protocolos de telefonia móvel
  1.8.8. *Blockchain*
1.9. Processamento de dados em tempo real
  1.9.1. Esteganografia
  1.9.2. Estegoanálise
  1.9.3. Aplicações e usos
1.10. Criptografia quântica
  1.10.1. Algoritmos quânticos
  1.10.2. Proteção de algoritmos frente à computação quântica
  1.10.3. Distribuição de chave quântica

Este Curso tem tudo: um corpo docente de alto nível, uma metodologia flexível que se adapta ao profissional e o mais completo conteúdo em criptografia e cibersegurança"

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

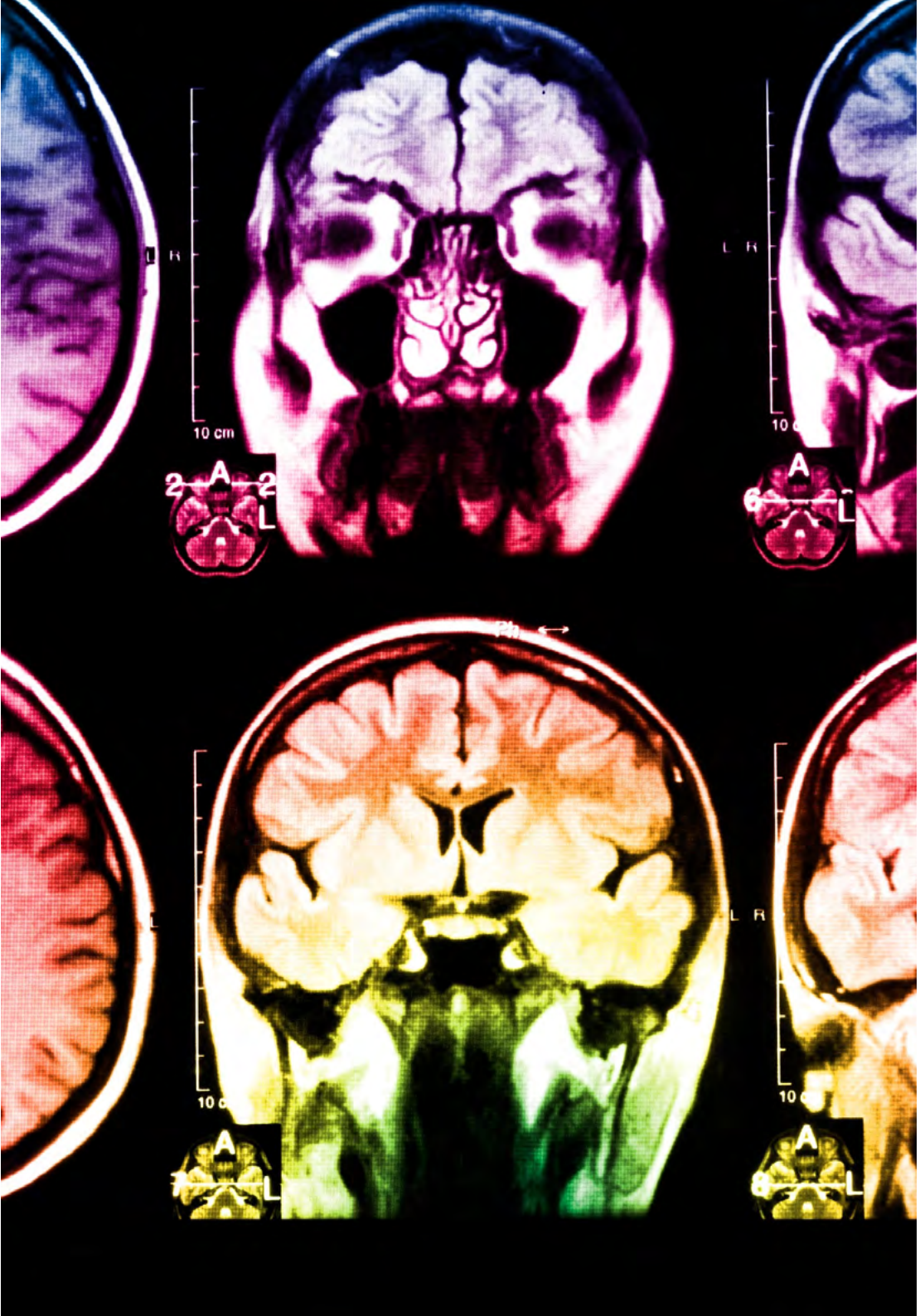
A TECH combina eficazmente a metodologia do Estudo de Caso com um sistema de aprendizagem 100% online baseado na repetição, que combina elementos didáticos diferentes em cada lição.

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.

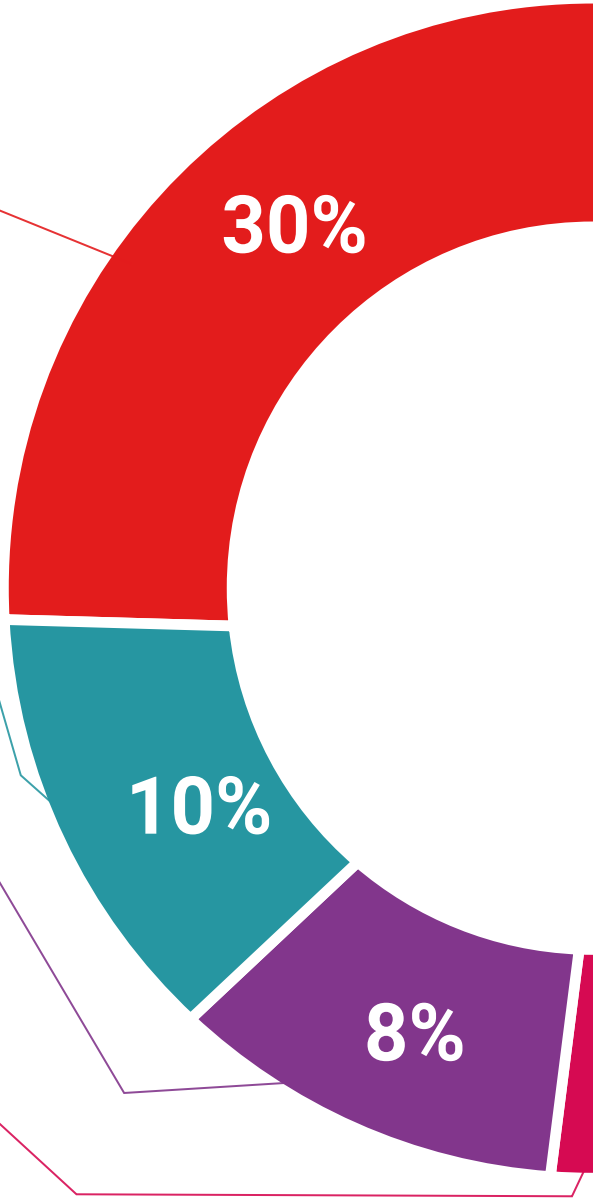
O denominado Learning from an Expert constrói conhecimento e memória, e gera confiança em futuras decisões difíceis.

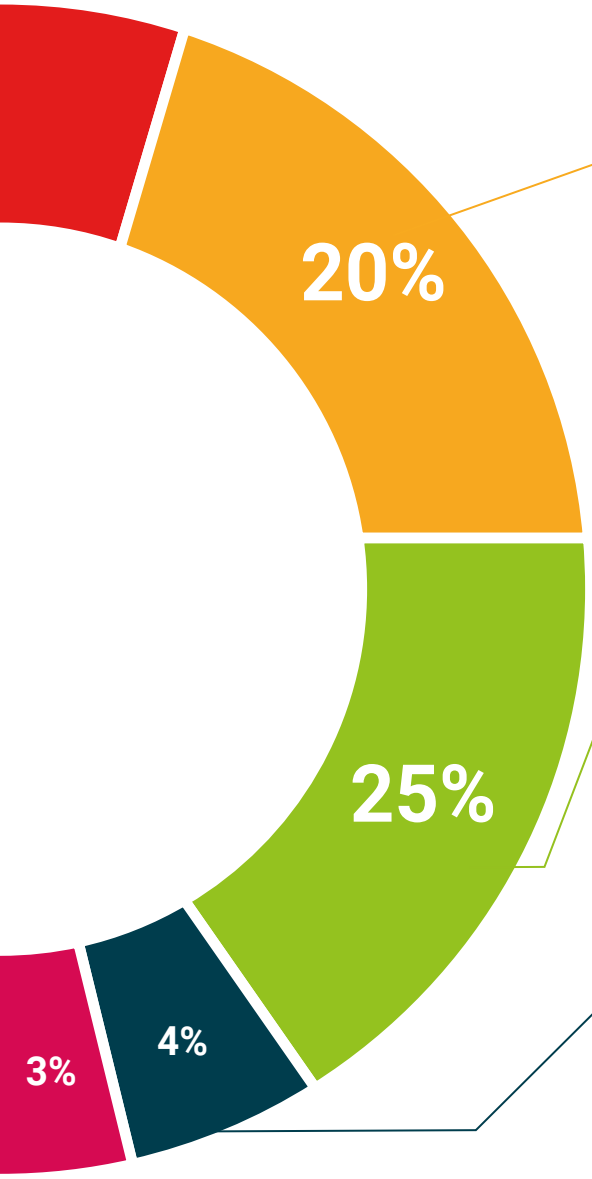
Práticas de aptidões e competências

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 Criptografia Avançada garante, para além de um conteúdo mais rigoroso e atualizado, o acesso a um 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 Criptografia Avançada** 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.**

Este certificado contribui significativamente para o desenvolvimento da capacitação continuada dos profissionais e proporciona um importante valor para a sua capacitação universitária, sendo 100% válido e atendendo aos requisitos normalmente exigidos pelas bolsas de emprego, concursos públicos e avaliação de carreiras profissionais.

Certificação: **Curso de Criptografia Avançada**

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

Criptografia Avançada

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

código único TECH: AFWOR23S techtitute.com/titulos

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

tech universidade tecnológica

Curso

Criptografia Avançada

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

Curso

Criptografia Avançada

tech universidade tecnológica