

Curso de Especialização Segurança e Criptografia



Curso de Especialização Segurança e Criptografia

- » Modalidade: online
- » Duração: 24 semanas
- » Certificação: TECH Universidade Tecnológica
- » Créditos: 18 ECTS
- » Horário: ao seu próprio ritmo
- » Exames: online

Acesso ao site: www.techtute.com/pt/informatica/curso-especializacao/curso-especializacao-seguranca-criptografia

Índice

01

Apresentação

pág. 4

02

Objetivos

pág. 8

03

Direção do curso

pág. 12

04

Estrutura e conteúdo

pág. 16

05

Metodologia

pág. 22

06

Certificação

pág. 30

01

Apresentação

Uma das áreas mais importantes da cibersegurança atual é a criptografia. Este campo permite proteger todo o tipos de informação através do processo de encriptação, utilizando ferramentas como os algoritmos. Todo o tipo de empresas necessita de proteger os seus dados, pelo que procuram profissionais especializados nesta área que possam fornecer os padrões de segurança de que necessitam. Este Curso de Especialização, o mais sofisticado em criptografia simétrica, cifras de bloco, algoritmos quânticos ou tecnologia *Blockchain*. Tudo isto baseando-se numa metodologia de ensino 100% online que permitirá ao profissional conciliar os estudos com o trabalho, uma vez que é compatível com as suas circunstâncias pessoais.



“

Graças a este Curso de Especialização, conhecerá os melhores métodos de criptografia para proteger os dados dos seus clientes e empregadores”

A criptografia é uma disciplina em crescimento para a qual são cada vez mais procurados profissionais. Este campo permite proteger todo o tipo de dados digitais e pode ser aplicado em contextos bancários, em lojas online, bases de dados de todo o tipo e é essencial na *Blockchain*. Assim, especializar-se nesta área é indispensável para os atuais profissionais da informática.

Imensas empresas, não só as tecnológicas, necessitam de especialistas em criptografia para proporcionar uma maior segurança à sua informação e este Curso de Especialização dá resposta a essa necessidade. Ao longo de três módulos e 450 horas de aprendizagem, o informático irá explorar questões como os fundamentos matemáticos da criptografia, a metodologia de análise e gestão de riscos dos sistemas de informação ou a proteção de algoritmos frente à computação quântica.

O profissional poderá estudar esta disciplina através de uma metodologia 100% online, especialmente concebida para que o aluno possa conciliar o seu trabalho com os estudos. Além disso, terá também à sua disposição um corpo docente de grande prestígio na área da criptografia, que irá lecionar este Curso de Especialização através de numerosos recursos multimédia.

Este **Curso de Especialização em Segurança e Criptografia** 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



A criptografia é essencial para empresas como o Facebook, o Paypal ou a Amazon, e a tecnologia Blockchain deu-lhe um enorme impulso, de modo que a especialização nesta área pode conduzir a inúmeras oportunidades profissionais”

“

Utilizando os melhores materiais multimédia e acompanhado por um corpo docente constituído por profissionais em atividade, conhecerá todas as ferramentas da criptografia aplicada à segurança informática”

O pessoal docente da especialização 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 de Especialização. Para tal, contará com a ajuda de um sistema inovador de vídeo interativo desenvolvido por especialistas reconhecidos.

A criptografia é o grande domínio informático da atualidade: este Curso de Especialização permitir-lhe-á especializar-se neste domínio com o melhor ensino online do mercado.

Com este Curso de Especialização, aprofundará aspetos da criptografia, como a proteção de algoritmos contra a computação quântica.



02

Objetivos

O principal objetivo deste Curso de Especialização em Segurança e Criptografia é oferecer aos profissionais os últimos desenvolvimentos nesta área da cibersegurança, para que, após a sua conclusão, possam trabalhar em qualquer empresa que necessite de um especialista neste domínio. Para tal, a TECH oferece-lhe os conteúdos mais completos e atuais, o sistema de ensino mais flexível e professores de grande prestígio no domínio da criptografia.



“

Esta qualificação permitir-lhe-á atingir todos os seus objetivos profissionais, tornando-o num grande especialista em criptografia”



Objetivos gerais

- ♦ Analisar e desenvolver o conceito de risco, incerteza dentro do ambiente em que vivemos
- ♦ Examinar o modelo de gestão de riscos com base na norma ISO 31.000
- ♦ Aplicar a metodologia MAGERIT para fazer evoluir o modelo e levá-lo um nível mais avançado
- ♦ Conceber novas metodologias próprias de gestão de riscos, com base no conceito de *Agile Risk Management*
- ♦ Identificar, analisar, avaliar e abordar os riscos enfrentados partir de uma nova perspectiva empresarial baseada num modelo *Risk-Driven* ou “movido pelo risco” não só para sobreviver no seu próprio ambiente, mas também para promover a sua própria contribuição de valor
- ♦ Maximizar as oportunidades apresentadas e eliminar a exposição a todos os potenciais riscos a partir do próprio desenho
- ♦ 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
- ♦ Determinar os elementos básicos de um Plano de Continuidade de Negócio (PCN) utilizando como base as orientações da norma ISO-22301
- ♦ Examinar os riscos decorrentes da inexistência de um Plano de Continuidade de Negócio (PCN)
- ♦ Analisar os critérios de sucesso de um PCN e a sua integração na gestão de riscos global de uma empresa
- ♦ Definir as fases de implementação de um Plano de Continuidade de Negócio



Não espere mais: a evolução profissional que procurava está neste Curso de Especialização”



Objetivos específicos

Módulo 1 Análise de Riscos e Ambiente de Segurança IT

- ♦ Examinar, com uma visão holística, o ambiente em que nos movemos
- ♦ Identificar os principais riscos e oportunidades que podem afetar a realização dos nossos objetivos
- ♦ Analisar os riscos com base nas melhores práticas à nossa disposição
- ♦ Avaliar o impacto potencial de tais riscos e oportunidades
- ♦ Desenvolver técnicas que nos permitam lidar com os riscos e oportunidades de uma forma que maximize a nossa contribuição de valor
- ♦ Examinar em profundidade as diferentes técnicas de transferência de riscos, assim como de valor
- ♦ Gerar valor a partir da concepção de modelos próprios para a gestão ágil de riscos
- ♦ Examinar os resultados para propor melhorias contínuas na gestão de projetos e processos com base em modelos de gestão orientados para o risco o *Risk-Driven*
- ♦ Inovar e transformar dados gerais em informação relevante para a tomada de decisões com base no risco

Módulo 2 Criptografia em IT

- ♦ 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

Módulo 3 Plano de continuidade do negócio associado à segurança

- ♦ Apresentar os elementos-chave de cada fase e analisar as características do Plano de Continuidade de Negócio (PCN)
- ♦ Fundamentar a necessidade de um Plano de Continuidade para o Negócio
- ♦ Determinar os mapas de sucesso e de risco para cada fase do Plano de Continuidade de Negócio
- ♦ Especificar como é estabelecido um Plano de Ação para a implementação
- ♦ Avaliar a integridade de um Plano de Continuidade de Negócio (PCN)
- ♦ Desenvolver um plano para a implementação bem sucedida de um Plano de Continuidade de Negócio

03

Direção do curso

Este Curso de Especialização conta com os melhores especialistas profissionalmente ativos na área da criptografia para lecionar os seus três módulos. Assim, o corpo docente deste Curso de Especialização é um dos seus grandes pontos fortes, pois inclui especialistas de grande prestígio neste domínio, que transmitirão ao aluno todas as ferramentas para poder trabalhar utilizando as melhores técnicas e ferramentas de encriptação.



“

Um corpo docente constituído por profissionais em atividade na área da criptografia irão orientá-lo durante todo o processo de aprendizagem”

Direção



Dr. Martín Olalla Bonal

- ♦ Client Technical Specialist Blockchain na IBM
- ♦ 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. Félix Gonzalo Alonso

- ♦ Diretor-Geral e fundador da Smart REM Solutions
- ♦ Sócio Fundador e Responsável pela Engenharia de Riscos e Inovação. Dynargy
- ♦ Gerente e Sócio Fundador Risknova (Gabinete Pericial Especializado em Tecnologia)
- ♦ Licenciado em Engenharia de Organização Industrial pela Universidade Pontifícia de Comillas ICAI
- ♦ Licenciado em Engenharia Técnica Industrial especializado em Eletrónica Industrial pela Universidade Pontifícia de Comillas ICAI
- ♦ Mestrado em Gestão de Seguros pelo ICEA (Instituto para la Colaboración entre Entidades Aseguradoras)

Dr. Juan Luis Gozalo Fernández

- ◆ Engenheiro Informático
- ◆ Professor Associado em DevOps e em Blockchain em UNIR
- ◆ Ex-Diretor Blockchain DevOps em Alastria
- ◆ Diretor Desenvolvimento Aplicação Móvel Tinkerlink em Cronos Telecom
- ◆ Diretor Informático em Banco Santander
- ◆ Diretor Tecnologia Gestão de Serviço IT em Barclays Bank Espanha
- ◆ Licenciado em Engenharia Superior Informático pela Universidade Nacional de Educação à Distância (UNED)

Dr. Octavio Ortega

- ◆ 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

04

Estrutura e conteúdo

Este Curso de Especialização em Segurança e Criptografia desenvolve-se ao longo de seis meses, em 450 horas de aprendizagem. Além disso, foi estruturado em três módulos, com os quais o informático irá explorar questões como a metodologia de análise e gestão do risco dos sistemas de informação, o desenvolvimento de mapas de risco informático com base em metodologias ágeis, a inteligência artificial aplicada à gestão do risco ou a criptografia aplicada à *Blockchain*.



“

*Com este Curso de Especialização
terá acesso aos conteúdos mais
inovadores na esteganografia”*

Módulo 1 Análise de riscos e ambiente de segurança IT

- 1.1. Análise do ambiente
 - 1.1.1. Análise da situação conjuntural
 - 1.1.1.1. Ambientes VUCA
 - 1.1.1.1.1. Volátil
 - 1.1.1.1.2. Incerto
 - 1.1.1.1.3. Complexo
 - 1.1.1.1.4. Ambíguo
 - 1.1.1.2. Ambientes BANI
 - 1.1.1.2.1. Frágil
 - 1.1.1.2.2. Ansioso
 - 1.1.1.2.3. Não linear
 - 1.1.1.2.4. Incompreensível
 - 1.1.2. Análise do ambiente geral. PESTEL
 - 1.1.2.1. Político
 - 1.1.2.2. Económico
 - 1.1.2.3. Social
 - 1.1.2.4. Tecnológico
 - 1.1.2.5. Ecológico/Ambiental
 - 1.1.2.6. Legal
 - 1.1.3. Análise da situação interna. SWOT
 - 1.1.3.1. Objetivos
 - 1.1.3.2. Ameaças
 - 1.1.3.3. Oportunidades
 - 1.1.3.4. Pontos fortes
- 1.2. Riscos e incerteza
 - 1.2.1. Risco
 - 1.2.2. Gestão de riscos
 - 1.2.3. Normas de gestão de riscos
- 1.3. Diretrizes para a gestão de riscos ISO 31.000:2018
 - 1.3.1. Objeto
 - 1.3.2. Princípios
 - 1.3.3. Quadro de referência
 - 1.3.4. Processo
- 1.4. Metodologia de Análise e Gestão de Riscos dos Sistemas de Informação (MAGERIT)
 - 1.4.1. Metodologia MAGERIT
 - 1.4.1.1. Objetivos
 - 1.4.1.2. Método
 - 1.4.1.3. Elementos
 - 1.4.1.4. Técnicas
 - 1.4.1.5. Ferramentas disponíveis (PILAR)
- 1.5. Transferência do risco cibernético
 - 1.5.1. Transferência de riscos
 - 1.5.2. Riscos cibernéticos Tipologia
 - 1.5.3. Seguros de riscos cibernéticos
- 1.6. Metodologias ágeis para a gestão de riscos
 - 1.6.1. Metodologias ágeis
 - 1.6.2. Scrum para a gestão do risco
 - 1.6.3. *Agile Risk Management*
- 1.7. Tecnologias para a gestão do risco
 - 1.7.1. Inteligência artificial aplicada à gestão de riscos
 - 1.7.2. *Blockchain* e criptografia. Métodos de preservação do valor
 - 1.7.3. Computação quântica Oportunidade ou ameaça
- 1.8. Elaboração de mapas de riscos informáticos baseados em metodologias ágeis
 - 1.8.1. Representação da probabilidade e impacto em ambientes ágeis
 - 1.8.2. O risco como ameaça do valor
 - 1.8.3. Re-evolução na gestão de projetos e processos ágeis baseados em KRIs

- 1.9. *Risk Driven* na gestão de riscos
 - 1.9.1. *Risk Driven*
 - 1.9.2. *Risk Driven* na gestão de riscos
 - 1.9.3. Desenvolvimento de um modelo de gestão empresarial impulsionado pelo risco
- 1.10. Inovação e transformação digital na gestão de risco informáticos
 - 1.10.1. A gestão de riscos ágeis como fonte de inovação empresarial
 - 1.10.2. Transformação de dados em informação útil para a tomada de decisões
 - 1.10.3. Visão holística da empresa através do risco

Módulo 2 Criptografia em IT

- 2.1. Criptografia
 - 2.1.1. Criptografia
 - 2.1.2. Fundamentos matemáticos
- 2.2. Criptologia
 - 2.2.1. Criptologia
 - 2.2.2. Criptoanálise
 - 2.2.3. Criptoanálise
- 2.3. Protocolos criptográficos
 - 2.3.1. Blocos básicos
 - 2.3.2. Protocolos básicos
 - 2.3.3. Protocolos intermédios
 - 2.3.4. Protocolos avançados
 - 2.3.5. Protocolos esotéricos
- 2.4. Técnicas criptográficas
 - 2.4.1. Longitude de chaves
 - 2.4.2. Gestão de chaves
 - 2.4.3. Tipos de algoritmos
 - 2.4.4. Funções resumo. *Hash*
 - 2.4.5. Geradores de números pseudoaleatórios
 - 2.4.6. Uso de algoritmos
- 2.5. Criptografia simétrica
 - 2.5.1. Cifras de bloco
 - 2.5.2. DES (*Data Encryption Standard*)
 - 2.5.3. Algoritmo RC4
 - 2.5.4. AES (*Advanced Encryption Standard*)
 - 2.5.5. Combinação de cifras de bloco
 - 2.5.6. Derivação de chaves
- 2.6. Criptografia assimétrica
 - 2.6.1. Diffie-Hellman
 - 2.6.2. DSA (*Digital Signature Algorithm*)
 - 2.6.3. RSA (Rivest, Shamir e Adleman)
 - 2.6.4. Curva elíptica
 - 2.6.5. Criptografia assimétrica Tipologia
- 2.7. Certificados digitais
 - 2.7.1. Assinatura digital
 - 2.7.2. Certificados X509
 - 2.7.3. Infraestrutura de chave pública (PKI)
- 2.8. Implementações
 - 2.8.1. Kerberos
 - 2.8.2. IBM CCA
 - 2.8.3. *Pretty Good Privacy* (PGP)
 - 2.8.4. *ISO Authentication Framework*
 - 2.8.5. SSL e TLS
 - 2.8.6. Cartões inteligentes em meios de pagamento (EMV)
 - 2.8.7. Protocolos de telefonia móvel
 - 2.8.8. *Blockchain*
- 2.9. Esteganografia
 - 2.9.1. Esteganografia
 - 2.9.2. Estegoanálise
 - 2.9.3. Aplicações e usos

- 2.10. Criptografia quântica
 - 2.10.1. Algoritmos quânticos
 - 2.10.2. Proteção de algoritmos frente à computação quântica
 - 2.10.3. Distribuição de chave quântica

Módulo 3 Plano de continuidade do negócio associado à segurança

- 3.1. Planos de Continuidade de Negócio
 - 3.1.1. Os Planos de Continuidade de Negócio (PCN)
 - 3.1.2. Plano de Continuidade de Negócio (PCN). Questões-chave
 - 3.1.3. Plano de Continuidade de Negócio (PCN) para a avaliação da empresa
- 3.2. Métricas num Plano de Continuidade de Negócio (PCN)
 - 3.2.1. *Recovery Time Objective* (RTO) e *Recovery Point Objective* (RPO)
 - 3.2.2. Tempo Máximo Tolerável (MTD)
 - 3.2.3. Níveis Mínimos de Recuperação (ROL)
 - 3.2.4. Ponto de Recuperação Objetivo (RPO)
- 3.3. Projetos de continuidade. Tipologia
 - 3.3.1. Plano de Continuidade de Negócio (PCN)
 - 3.3.2. Plano de continuidade de TIC (PCTIC)
 - 3.3.3. Plano de recuperação em caso de desastres (PRD)
- 3.4. Gestão de riscos associada ao PCN
 - 3.4.1. Análise de impacto no negócio
 - 3.4.2. Benefícios da implementação de um PCN
 - 3.4.3. Mentalidade baseada em riscos
- 3.5. Ciclo de vida de um plano de continuidade de negócio
 - 3.5.1. Fase 1: Análise da Organização
 - 3.5.2. Fase 2: Determinação da estratégia de continuidade
 - 3.5.3. Fase 3: Resposta à contingência
 - 3.5.4. Fase 4: Prova, manutenção e revisão



- 3.6. Fase de análise da organização de um PCN
 - 3.6.1. Identificação de processos no âmbito do PCN
 - 3.6.2. Identificação de áreas críticas do negócio
 - 3.6.3. Identificação de dependências entre áreas e processos
 - 3.6.4. Determinação do MTD adequado
 - 3.6.5. Documentos a entregar Criação de um plano
- 3.7. Fase de determinação da estratégia de continuidade num PCN
 - 3.7.1. Funções na fase de determinação da estratégia
 - 3.7.2. Tarefas da fase de determinação da estratégia
 - 3.7.3. Documentos a entregar
- 3.8. Fase de resposta à contingência num PCN
 - 3.8.1. Funções na fase de resposta
 - 3.8.2. Tarefas nesta fase
 - 3.8.3. Documentos a entregar
- 3.9. Fase de testes, manutenção e revisão de um PCN
 - 3.9.1. Funções na fase de testes, manutenção e revisão
 - 3.9.2. Tarefas na fase de testes, manutenção e revisão
 - 3.9.3. Documentos a entregar
- 3.10. Normas ISO associadas aos Planos de Continuidade de Negócio (PCN)
 - 3.10.1. ISO 22301:2019
 - 3.10.2. ISO 22313:2020
 - 3.10.3. Outras normas ISO e internacionais relacionadas



*Empresas de todos os setores vão
querer contar consigo para proteger
os seus dados mais valiosos"*

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.



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

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.

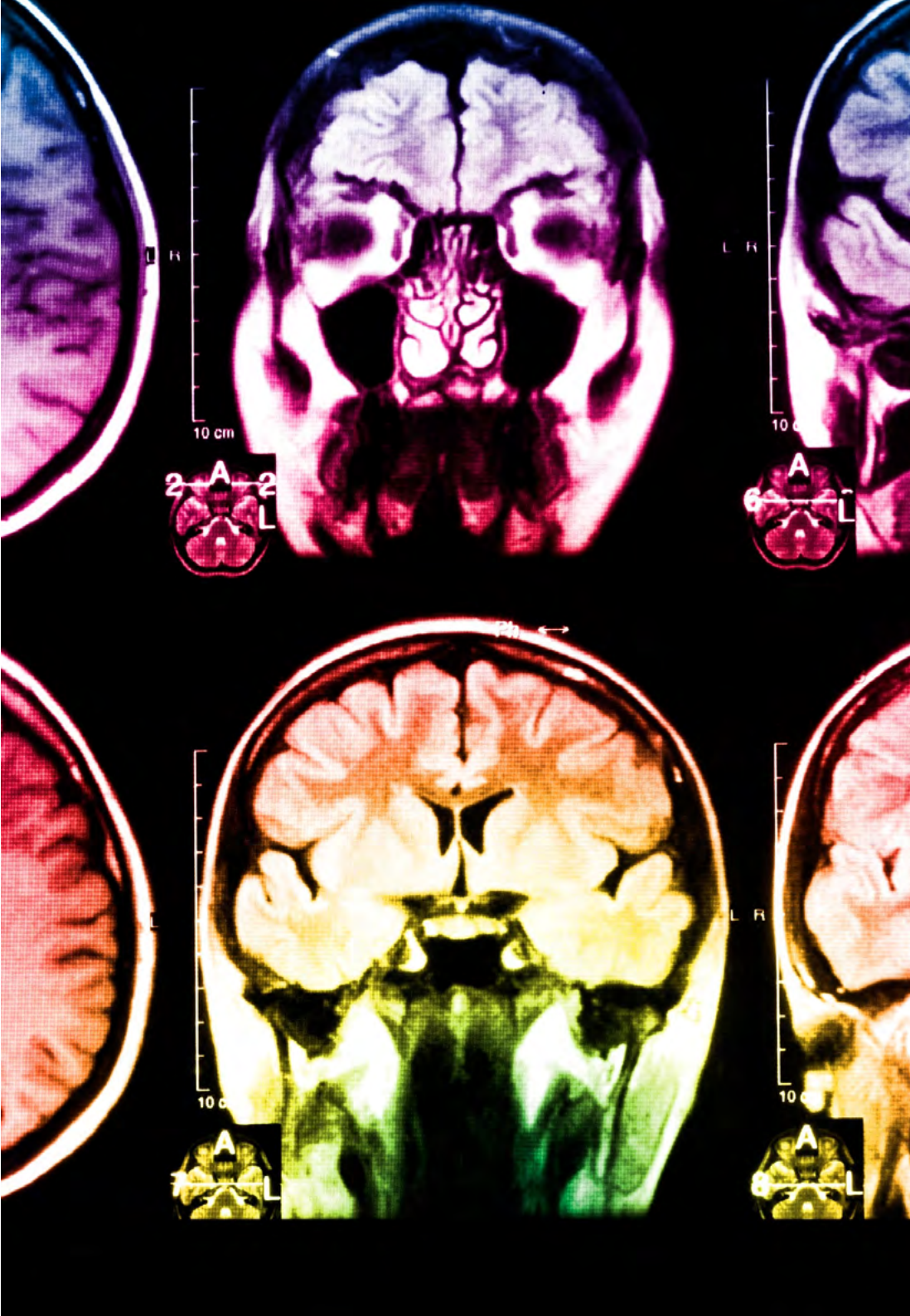


No nosso programa, a aprendizagem não é um processo linear, mas acontece numa espiral (aprender, desaprender, esquecer e reaprender). Portanto, cada um destes elementos é combinado de forma concêntrica. Esta metodologia formou mais de 650.000 licenciados com sucesso sem precedentes em áreas tão diversas 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.



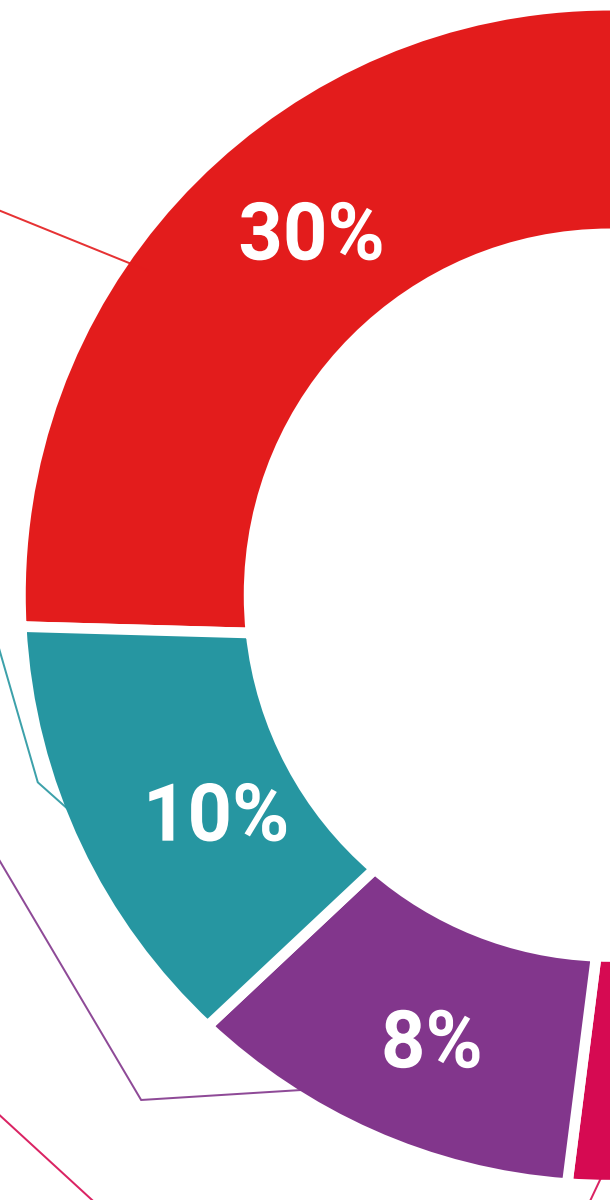
Práticas de aptidões e competências

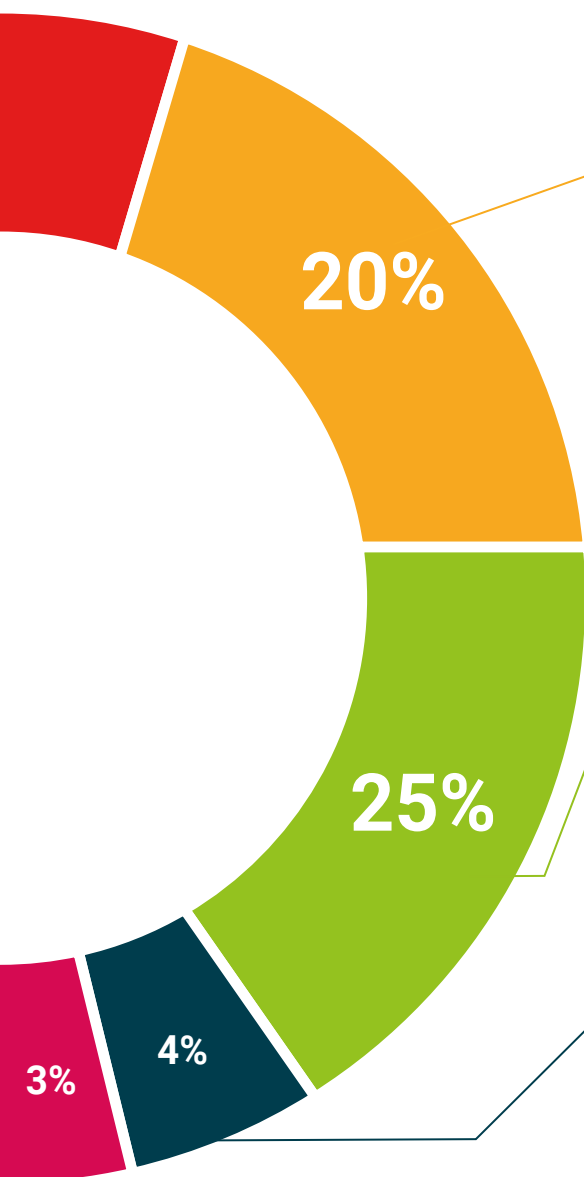
Realizarão atividades para desenvolver competências e aptidões específicas em cada área temática. Práticas e dinâmicas para adquirir e desenvolver as competências e capacidades que um especialista necessita de desenvolver no quadro da globalização em que vivemos.



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 conceituais 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 Segurança e Criptografia garante, 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 Segurança e Criptografia** conta com o conteúdo educacional mais completo e atualizado do mercado

Uma vez aprovadas as avaliações, o aluno receberá por correio, com aviso de recepção, 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 Curso de Especialização, atendendo aos requisitos normalmente exigidos pelas bolsas de emprego, concursos públicos e avaliação de carreiras profissionais.

Certificação: **Curso de Especialização em Segurança e Criptografia**

ECTS: **18**

Carga horária: **450 horas**



*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.



Curso de Especialização Segurança e Criptografia

- » Modalidade: online
- » Duração: 24 semanas
- » Certificação: TECH Universidade Tecnológica
- » Créditos: 18 ECTS
- » Horário: ao seu próprio ritmo
- » Exames: online

Curso de Especialização Segurança e Criptografia