

Curso de Especialização

Segurança em TI



Curso de Especialização Segurança em TI

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

Acesso ao site: www.techtitute.com/pt/informatica/curso-especializacao/curso-especializacao-seguranca-ti

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

As tecnologias da informação são o presente e o futuro de numerosos processos sociais e empresariais. Portanto, atualmente, estas ferramentas são essenciais para a comunicação interpessoal, para efetuar compras e vendas ou para contactar clientes e fornecedores. A sua popularidade tornou-os omnipresentes, tornando-os um alvo cobiçado por aqueles que desejam explorar as suas vulnerabilidades. Neste contexto, o especialista em Segurança em TI tornou-se um perfil profissional muito procurado. Por este motivo, este Curso de Especialização foi cuidadosamente concebido para que os informáticos possam ficar a par de todos os aspetos da cibersegurança aplicados a estas tecnologias, melhorando imediatamente as suas perspetivas profissionais.



“

Esta qualificação permitir-lhe-á especializar-se em Segurança em TI, o que lhe dará acesso a grandes oportunidades de carreira numa área da informática que é cada vez mais procurada”

O novo contexto tecnológico exige que os profissionais se dediquem se adaptarem às transformações existentes na Segurança em TI. Assim, estas tecnologias da informação são omnipresentes e são utilizadas em todos os tipos de processos de âmbito empresarial e social. Consequentemente, existem inúmeros aspetos que correm o risco de serem expostos a vulnerabilidades exploráveis.

Esta situação é muito preocupante para as empresas, que veem como uma segurança inadequada pode pôr em perigo o seu negócio. A solução passa, portanto, pelo recrutamento de profissionais especializados nesta área, razão pela qual os especialistas em Segurança em TI são atualmente um dos perfis mais procurados e valorizados pelas empresas de diferentes áreas e setores.

Em resposta a esta procura, este Curso de Especialização é apresentado num formato 100% online, com um corpo docente de enorme prestígio internacional neste domínio da cibersegurança. Além disso, este Curso de Especialização apresenta os seus conteúdos em diferentes formatos multimédia: resumos interativos, vídeos, casos práticos, masterclasses, atividades práticas, etc. vídeos, casos práticos, masterclasses, atividades práticas, etc. Tudo com o objetivo de proporcionar aos profissionais uma maior proximidade com os últimos desenvolvimentos em matéria de segurança aplicada às tecnologias da informação.

Este **Curso de Especialização em Segurança em TI** 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
- ♦ Disponibilidade de acesso ao conteúdo a partir de qualquer dispositivo fixo ou portátil com ligação à Internet

“

Com este Curso de Especialização, poderá aprofundar os aspetos relevantes da segurança informática, tais como o desenvolvimento seguro das comunicações e da operação software”

“

A metodologia online da TECH permitir-lhe-á conciliar o seu trabalho com os seus estudos, uma vez que se adapta a todas as suas circunstâncias pessoais e profissionais”

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.

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.

O corpo docente deste Curso de Especialização é composto por profissionais em atividade que conhecem todos os desenvolvimentos mais recentes neste domínio da cibersegurança.

O seu perfil profissional melhorará após a conclusão deste Curso de Especialização, que é lecionado através de numerosos recursos multimédia.



02 Objetivos

O principal objetivo deste Curso de Especialização em Segurança em TI é oferecer aos profissionais as melhores ferramentas para se adaptarem ao novo contexto informático, transformado pelo processo de digitalização que se estendeu a todas as áreas da sociedade. Estará então na melhor posição para trabalhar como especialista em cibersegurança em qualquer empresa que pretenda proteger o seu negócio de novas ameaças informáticas.



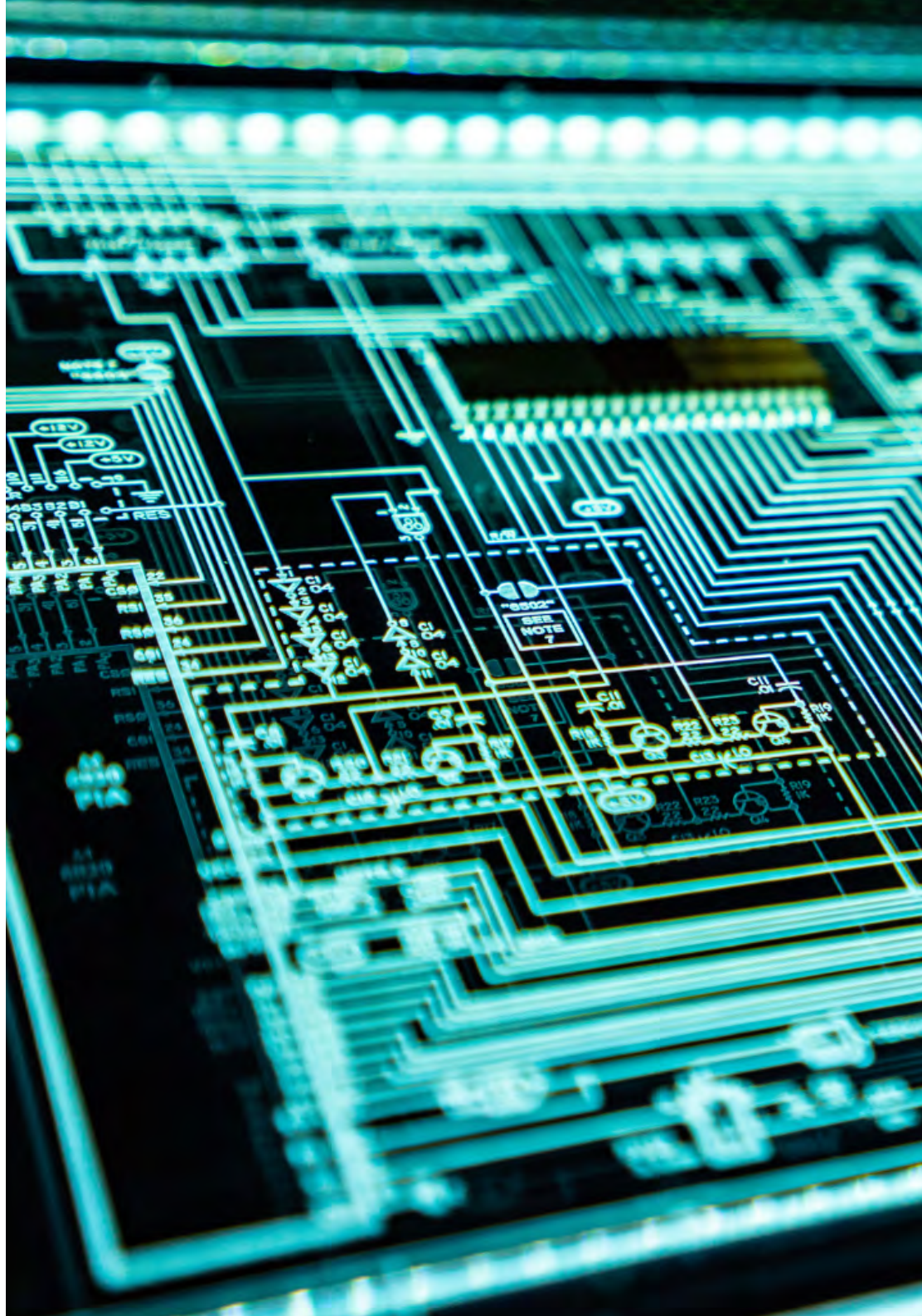
“

O objetivo da TECH é proporcionar-lhe os conhecimentos mais atualizados para que possa realizar o seu trabalho com as máximas garantias, tornando-o num profissional de referência no setor”



Objetivos gerais

- ◆ Gerar conhecimentos especializados sobre um sistema de informação, tipos e aspectos de segurança a ter em conta
- ◆ Identificar as vulnerabilidades de um sistema de informação
- ◆ Aplicar as medidas de segurança mais adequadas em função das ameaças
- ◆ Desenvolver a regulamentação legal e a tipificação do delito no ataque a um sistema de informação
- ◆ Determinar a política e o plano de segurança do sistema de informação de uma empresa, completando a conceção e implementação do plano de contingência
- ◆ Gerar um conhecimento especializado sobre o ecossistema de segurança Informática
- ◆ Avaliar o conhecimento em termos de cibersegurança
- ◆ Desenvolver as melhores práticas no desenvolvimento seguro
- ◆ Apresentar os riscos para as empresas de não terem um ambiente informático seguro
- ◆ Examinar o processo de desenho de uma estratégia de segurança ao implantar serviços empresariais em *Cloud*
- ◆ Identificar os âmbitos de segurança em *Cloud*
- ◆ Analisar os serviços e ferramentas em cada um dos domínios da segurança
- ◆ Avaliar as diferenças nas implementações concretas de diferentes fornecedores de *Cloud* pública





Objetivos específicos

Módulo 1 Segurança no desenho e desenvolvimento de sistemas

- ♦ Avaliar a segurança de um sistema de informação em todos os seus componentes e camadas
- ♦ Identificar os tipos de ameaças à segurança atuais e as suas tendências
- ♦ Estabelecer orientações de segurança definindo políticas e planos de segurança e contingência
- ♦ Analisar estratégias e ferramentas para garantir a integridade e segurança dos sistemas de informação
- ♦ Aplicar as técnicas e ferramentas específicas para cada tipo de ataque ou vulnerabilidade de segurança
- ♦ Proteger a informação sensível armazenada no sistema de informação
- ♦ Dispor do enquadramento legal e tipificação do crime, completando a visão com a tipificação do infrator e da sua vítima

Módulo 2 Segurança em comunicações e operação software

- ♦ Desenvolver conhecimento especializado em matéria de segurança física e lógica
- ♦ Demonstrar o conhecimento em comunicações e redes
- ♦ Identificar os principais ataques maliciosos
- ♦ Estabelecer um quadro de desenvolvimento seguro
- ♦ Demonstrar conhecer os principais regulamentos dos sistemas de gestão da segurança da informação
- ♦ Fundamentar o funcionamento de um centro de operações de cibersegurança
- ♦ Demonstrar a importância das práticas de cibersegurança para as catástrofes organizacionais

Módulo 3 Segurança em ambientes *Cloud*

- ♦ Identificar riscos de uma implantação de infraestrutura em *Cloud* pública
- ♦ Definir os requisitos de segurança
- ♦ Desenvolvimento de um plano de segurança para a implantação em *Cloud*
- ♦ Identificar os serviços *Cloud* a implementar para a execução de um plano de segurança
- ♦ Determinar as disposições operacionais necessárias para os mecanismos de prevenção
- ♦ Estabelecer as diretrizes para um sistema de *logging* e monitorização
- ♦ Propor ações de resposta a incidentes



Poderá progredir rapidamente a nível profissional, uma vez que os seus novos conhecimentos o tornarão um especialista muito procurado"

03

Direção do curso

A segurança das tecnologias da informação é uma área em constante evolução, que exige conhecimentos de última geração que só um profissional em atividade pode proporcionar. Por esta razão, a TECH empenhou-se em tornar especialistas de prestígio neste domínio responsáveis pelo ensino do Curso de Especialização, proporcionando ao estudante as melhores competências para se desenvolver eficazmente na conceção da proteção de qualquer empresa.





“

Este Curso de Especialização é o que precisa: terá ao seu alcance os melhores especialistas em Segurança em TI a nível internacional”

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. Javier Nogales Ávila

- ◆ Enterprise Cloud and sourcing senior consultant. Quint
- ◆ Cloud and Technology Consultant. Indra
- ◆ Associate Technology Consultant. Accenture
- ◆ Licenciado pela Universidade de Jaén e Universidade de Tecnologia e Economia de Budapeste (BME)
- ◆ Licenciatura em Engenharia de Organização Industrial

Dr. Antonio Gómez Rodríguez

- ◆ Engenheiro de Soluções Cloud na Oracle
- ◆ Diretor de Projetos em Sopra Group
- ◆ Diretor de Projetos em Everis
- ◆ Chefe de Projetos na Empresa Pública de Gestão de Programas Culturais Assessoria de Cultura da Andaluzia
- ◆ Analista de Sistemas de informação. Sopra Group
- ◆ Licenciado em Engenharia de Telecomunicações pela Universidade Politécnica da Catalunha
- ◆ Pós-graduação em Tecnologias e Sistemas de Informação, pelo Instituto Catalão de Tecnologia
- ◆ E-Business Mestrado pela Escola de Negócios La Salle

Dra. Lorena Jurado Jabonero

- ◆ Chefe de Segurança da Informação (CISO) no Grupo Pascual
- ◆ Licenciada em Engenharia Informática pela Universidade Alfonso X El Sabio
- ◆ Engenheira Técnico em Informática de Gestão pela Universidade Politécnica de Madrid
- ◆ Conhecimentos: ISO 27001, ISO 27701, ISO 22301, ISO 20000, RGD/LOPDGD, NIST CSF, CSA, ITIL, PCI, etc.

04

Estrutura e conteúdo

Para atingir os objetivos propostos, este Curso de Especialização em Segurança em TI foi dividido em três módulos especializados, que podem ser completados em 450 horas de aprendizagem. Assim, ao longo deste Curso de Especialização, o informático ficará a conhecer os últimos desenvolvimentos em segurança informática nas comunicações e operação software, a segurança em ambientes de *Cloud Computing*, a securitização de sistemas de armazenamento ou de sistemas de autorização, entre muitos outros aspetos relevantes nesta área.



“

Este Curso de Especialização permitir-lhe-á aplicar as melhores técnicas de análise forense aplicadas à Segurança em TI"

Módulo 1 Segurança no desenho e desenvolvimento de sistemas

- 1.1. Sistemas de informação
 - 1.1.1. O que é um sistema de informação
 - 1.1.2. Componentes de um sistema de informação
 - 1.1.3. Atividades de um sistema de informação
 - 1.1.4. Ciclo de vida de um sistema de informação
 - 1.1.5. Recursos de um sistema de Informação
- 1.2. Sistemas de informação. Tipologia
 - 1.2.1. Tipos dos sistemas de informação
 - 1.2.1.1. Empresarial
 - 1.2.1.2. Estratégicos
 - 1.2.1.3. De acordo com o âmbito da aplicação
 - 1.2.1.4. Específicos
 - 1.2.2. Sistemas de informação. Exemplos reais
 - 1.2.3. Evolução dos sistemas de informação: etapas
 - 1.2.4. Metodologia dos sistemas de informação
- 1.3. Segurança dos sistemas de informação. Implicações legais
 - 1.3.1. Acesso a Dados
 - 1.3.2. Ameaças de segurança: vulnerabilidades
 - 1.3.3. Implicações legais: delitos
 - 1.3.4. Procedimentos de manutenção de um sistema de informação
- 1.4. Segurança de um sistemas de informação. Protocolos de segurança
 - 1.4.1. Segurança de um sistema de informação
 - 1.4.1.1. Integração
 - 1.4.1.2. Confidencialidade
 - 1.4.1.3. Disponibilidade
 - 1.4.1.4. Autenticação
 - 1.4.2. Serviços de segurança
 - 1.4.3. Protocolos de segurança da informação. Tipologia
 - 1.4.4. Sensibilidade de um sistema de informação
- 1.5. Segurança num sistemas de informação. Medidas e sistemas de controlo de acesso
 - 1.5.1. Medidas de segurança
 - 1.5.2. Tipos de medidas de segurança
 - 1.5.2.1. Prevenção
 - 1.5.2.2. Detecção
 - 1.5.2.3. Correção
 - 1.5.3. Sistema de controlo de acesso. Tipologia
 - 1.5.4. Criptografia
- 1.6. Segurança em redes e internet
 - 1.6.1. *Firewalls*
 - 1.6.2. Identificação digital
 - 1.6.3. Vírus e worms
 - 1.6.4. *Hacking*
 - 1.6.5. Exemplos e casos reais
- 1.7. Crimes informáticos
 - 1.7.1. Crime informático
 - 1.7.2. Crimes informáticos. Tipologia
 - 1.7.3. Crime informático. Ataque. Tipologias
 - 1.7.4. O caso da Realidade Virtual
 - 1.7.5. Perfis de delinquentes e vítimas. Tipificação do crime
 - 1.7.6. Crimes informáticos. Exemplos e casos reais
- 1.8. Plano de segurança num sistema de informação
 - 1.8.1. Plano de segurança. Objetivos
 - 1.8.2. Plano de segurança. Planificação
 - 1.8.3. Plano de riscos Análises
 - 1.8.4. Políticas de segurança. Implementação na organização
 - 1.8.5. Plano de segurança. Implementação na organização
 - 1.8.6. Procedimentos de segurança. Tipos
 - 1.8.7. Planos de segurança. Exemplos

- 1.9. Plano de contingência
 - 1.9.1. Plano de contingência. Funções
 - 1.9.2. Plano de emergência: elementos e objetivos
 - 1.9.3. Plano de contingência na organização. Implementação
 - 1.9.4. Planos de contingência. Exemplos
- 1.10. Governança da segurança dos sistemas de informação
 - 1.10.1. Regulamentos legais
 - 1.10.2. Padrões
 - 1.10.3. Certificações
 - 1.10.4. Tecnologias

Módulo 2 Segurança em comunicações e operação software

- 2.1. Segurança informática em comunicações e operação software
 - 2.1.1. Segurança Informática
 - 2.1.2. Cibersegurança
 - 2.1.3. Segurança na nuvem
- 2.2. Segurança informática em comunicações e operação software. Tipologia
 - 2.2.1. Segurança física
 - 2.2.2. Segurança lógica
- 2.3. Segurança em comunicações
 - 2.3.1. Principais elementos
 - 2.3.2. Segurança de redes
 - 2.3.3. Melhores práticas
- 2.4. Ciberinteligência
 - 2.4.1. Engenharia social
 - 2.4.2. *Deep Web*
 - 2.4.3. *Phishing*
 - 2.4.4. *Malware*
- 2.5. Desenvolvimento seguro em comunicações e operação software
 - 2.5.1. Desenvolvimento seguro. Protocolo HTTP
 - 2.5.2. Desenvolvimento seguro. Ciclo de vida
 - 2.5.3. Desenvolvimento seguro. Segurança PHP
 - 2.5.4. Desenvolvimento seguro. Segurança NET
 - 2.5.5. Desenvolvimento seguro. Melhores práticas

- 2.6. Sistemas de gestão de segurança da informação em comunicações e operação software
 - 2.6.1. GDPR
 - 2.6.2. ISO 27021
 - 2.6.3. ISO 27017/ 18
- 2.7. Tecnologias SIEM
 - 2.7.1. Tecnologias SIEM
 - 2.7.2. Operativa de SOC
 - 2.7.3. SIEM *Vendors*
- 2.8. A função da segurança nas organizações
 - 2.8.1. Funções nas organizações
 - 2.8.2. Função dos especialistas IoT nas empresas
 - 2.8.3. Certificações reconhecidas no mercado
- 2.9. Análise forense
 - 2.9.1. Análise forense
 - 2.9.2. Análise forense. Metodologia
 - 2.9.3. Análise forense. Ferramentas e implantação
- 2.10. A cibersegurança na atualidade
 - 2.10.1. Principais ataques informáticos
 - 2.10.2. Previsões de empregabilidade
 - 2.10.3. Desafios

Módulo 3 Segurança em ambientes *Cloud*

- 3.1. Segurança em ambientes *Cloud Computing*
 - 3.1.1. Segurança em ambientes *Cloud Computing*
 - 3.1.2. Segurança em ambientes *Cloud Computing*. Ameaças e riscos segurança
 - 3.1.3. Segurança em ambientes *Cloud Computing*. Aspectos-chave de segurança
- 3.2. Tipos de infraestrutura *Cloud*
 - 3.2.1. Público
 - 3.2.2. Privado
 - 3.2.3. Híbrido

- 3.3. Modelo de gestão partilhada
 - 3.3.1. Elementos de segurança geridos por fornecedor
 - 3.3.2. Elementos geridos por cliente
 - 3.3.3. Definição da estratégia para a segurança
- 3.4. Mecanismos de prevenção
 - 3.4.1. Sistemas de gestão de autenticação
 - 3.4.2. Sistema de gestão de autorização: políticas de acesso
 - 3.4.3. Sistemas de gestão de chaves
- 3.5. Securitização de sistemas
 - 3.5.1. Securitização dos sistemas de armazenamento
 - 3.5.2. Proteção dos sistemas de base de dados
 - 3.5.3. Securitização de dados em trânsito
- 3.6. Proteção de infraestrutura
 - 3.6.1. Desenho e implementação de rede segura
 - 3.6.2. Segurança de recursos de computação
 - 3.6.3. Ferramentas e recursos para proteção de infraestrutura
- 3.7. Deteção as ameaças e ataques
 - 3.7.1. Sistemas de auditoria, *Logging* e monitorização
 - 3.7.2. Sistemas de eventos e alarmes
 - 3.7.3. Sistemas SIEM
- 3.8. Resposta a incidentes
 - 3.8.1. Plano de resposta a incidentes
 - 3.8.2. A continuidade do negócio
 - 3.8.3. Análise forense e remediação de incidentes da mesma natureza



- 3.9. Segurança em *Clouds* públicas
 - 3.9.1. AWS (Amazon Web Services)
 - 3.9.2. Microsoft Azure
 - 3.9.3. Google GCP
 - 3.9.4. Oracle Cloud
- 3.10. Normativa e cumprimento
 - 3.10.1. Cumprimento de normativas de segurança
 - 3.10.2. Gestão de risco
 - 3.10.3. Pessoas e processo nas organizações

“

O conteúdo mais completo e atualizado do mercado está agora ao seu alcance. Inscreva-se, não se vai arrepender"

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.

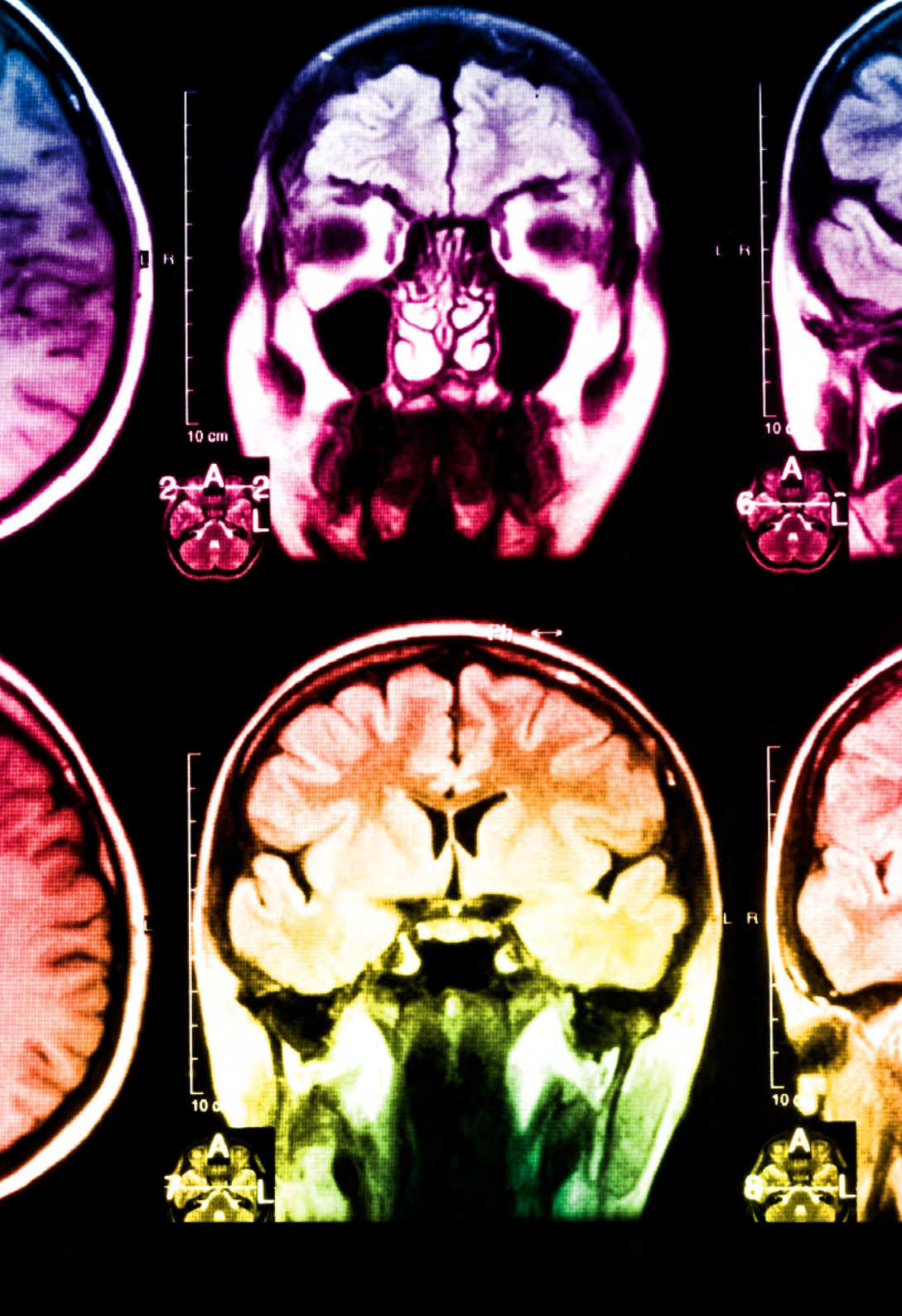


No nosso programa, a aprendizagem não é um processo linear, mas acontece numa espiral (aprender, desaprender, esquecer e reaprender). Portanto, cada um destes elementos é combinado de forma concêntrica. Esta metodologia formou mais de 650.000 licenciados com sucesso sem precedentes em áreas tão diversas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



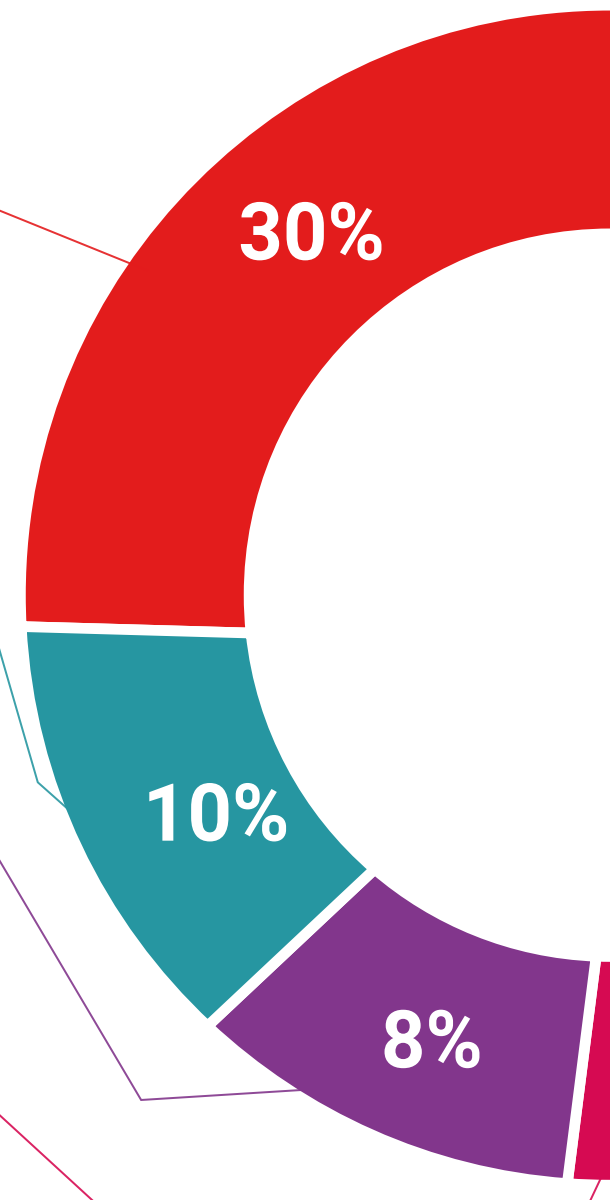
Práticas de aptidões e competências

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 em TI 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 em TI** 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 Segurança em TI**

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.

futuro
saúde confiança pessoas
informação orientadores
educação certificação ensino
garantia aprendizagem
instituições tecnologia
comunidade compreensão
atenção personalizada
conhecimento inovação
presente qualidade
desenvolvimento sustentabilidade

tech universidade
tecnológica

Curso de Especialização Segurança em TI

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

Curso de Especialização

Segurança em TI