Curso de Especialização

Segurança Informática para Comunicações

tech universidade tecnológica

tech universidade tecnológica

Curso de Especialização

Segurança Informática para Comunicações

- Modalidade: **online**
- Duração: **6 meses**
- 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-informatica-comunicacoes

Índice

01 Apresentação *pág. 4*

02 Objetivos *pág. 8*

03 Estrutura e conteúdo *pág. 12*

04 Metodologia *pág. 20*

05 Certificação *pág. 28*

01

Apresentação

A utilização não autorizada e indevida da internet é um dos principais problemas que os utilizadores podem enfrentar. É essencial levar a cabo ações de segurança informática, uma vez que uma grande quantidade de informação privada e confidencial circula através da internet. Este Curso de Especialização aproxima os alunos do campo da segurança informática para comunicações com um conteúdo atual e de qualidade. Trata-se de um Curso de Especialização completo que visa a capacitação de alunos para o sucesso na sua profissão.

Se procura um Curso de Especialização de qualidade que o ajude a especializar-se num dos campos com mais oportunidades profissionais, esta é a sua melhor opção"

Os avanços nas telecomunicações são constantes, sendo este uma das áreas com mais rápida evolução, pelo que é necessário contar com especialistas em informática capazes de se adaptarem a estas mudanças e de conhecerem em primeira mão as novas ferramentas e técnicas que vão surgindo neste contexto.

Dentro desta área, a segurança informática tem de ser um dos aspetos com que as empresas devem ter mais cuidado, uma vez que toda a sua informação está na internet, e o acesso descontrolado de um utilizador para realizar tarefas ilícitas pode ser um problema grave para a organização, tanto a nível financeiro como reputacional.

O Curso de Especialização em Segurança Informática para Comunicações aborda toda a gama de questões envolvidas neste campo. O seu estudo tem uma clara vantagem sobre outras capacitações que se concentram em blocos específicos, o que impede o aluno de conhecer a inter-relação com outras áreas incluídas no campo multidisciplinar das telecomunicações. Para além disso, o corpo docente deste Curso de Especialização fez uma seleção cuidadosa de cada um dos temas desta capacitação de forma a oferecer ao aluno a oportunidade de estudo mais completa possível e sempre atual.

Este Curso de Especialização destina-se a pessoas interessadas em atingir um nível de conhecimento mais elevado sobre Segurança Informática para Comunicações. O principal objetivo é a especialização dos alunos para que possam aplicar os conhecimentos adquiridos neste Curso de Especialização no mundo real, num ambiente de trabalho que reproduza as condições que possam encontrar no seu futuro, de uma forma rigorosa e realista.

Para além disso, tratando-se de um Curso de Especialização 100% online, o aluno não está condicionado a horários fixos nem à necessidade de se deslocar a um local físico, podendo aceder aos conteúdos em qualquer altura do dia, equilibrando o seu trabalho ou vida pessoal com a sua vida académica.

Este **Curso de Especialização em Segurança Informática para Comunicações** conta com o conteúdo educativo mais completo e atualizado do mercado. As suas principais características são:

- O desenvolvimento de casos práticos apresentados por especialistas em segurança informática
- O conteúdo gráfico, esquemático e eminentemente prático fornece informações científicas e práticas sobre as disciplinas que são essenciais para a prática profissional
- Exercícios práticos onde o processo de autoavaliação pode ser levado a cabo para melhorar a aprendizagem
- O seu foco especial nas metodologias inovadoras em segurança informática para comunicações
- 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

Não perca a oportunidade de frequentar este Curso de Especialização em Segurança Informática para Comunicações connosco. É a oportunidade perfeita para progredir na sua carreira profissional"

Este Curso de Especialização é o melhor investimento que pode fazer de forma a atualizar os seus conhecimentos em segurança informática para comunicações"

O seu corpo docente inclui profissionais da área da informática das telecomunicações que contribuem com a sua experiência profissional para este Curso de Especialização, bem como especialistas reconhecidos de empresas líderes 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 qualificação. Para tal, o profissional será auxiliado por um sistema inovador de vídeos interativos criados por especialistas reconhecidos com vasta experiência em segurança informática para comunicações.

Esta capacitação conta com o melhor material didático, o que lhe permitirá realizar um estudo contextual que facilitará a sua aprendizagem.

Este Curso de Especialização 100% online permitir-lhe-á combinar os seus estudos com a sua atividade profissional. É você que escolhe onde e quando quer estudar.

02

Objetivos

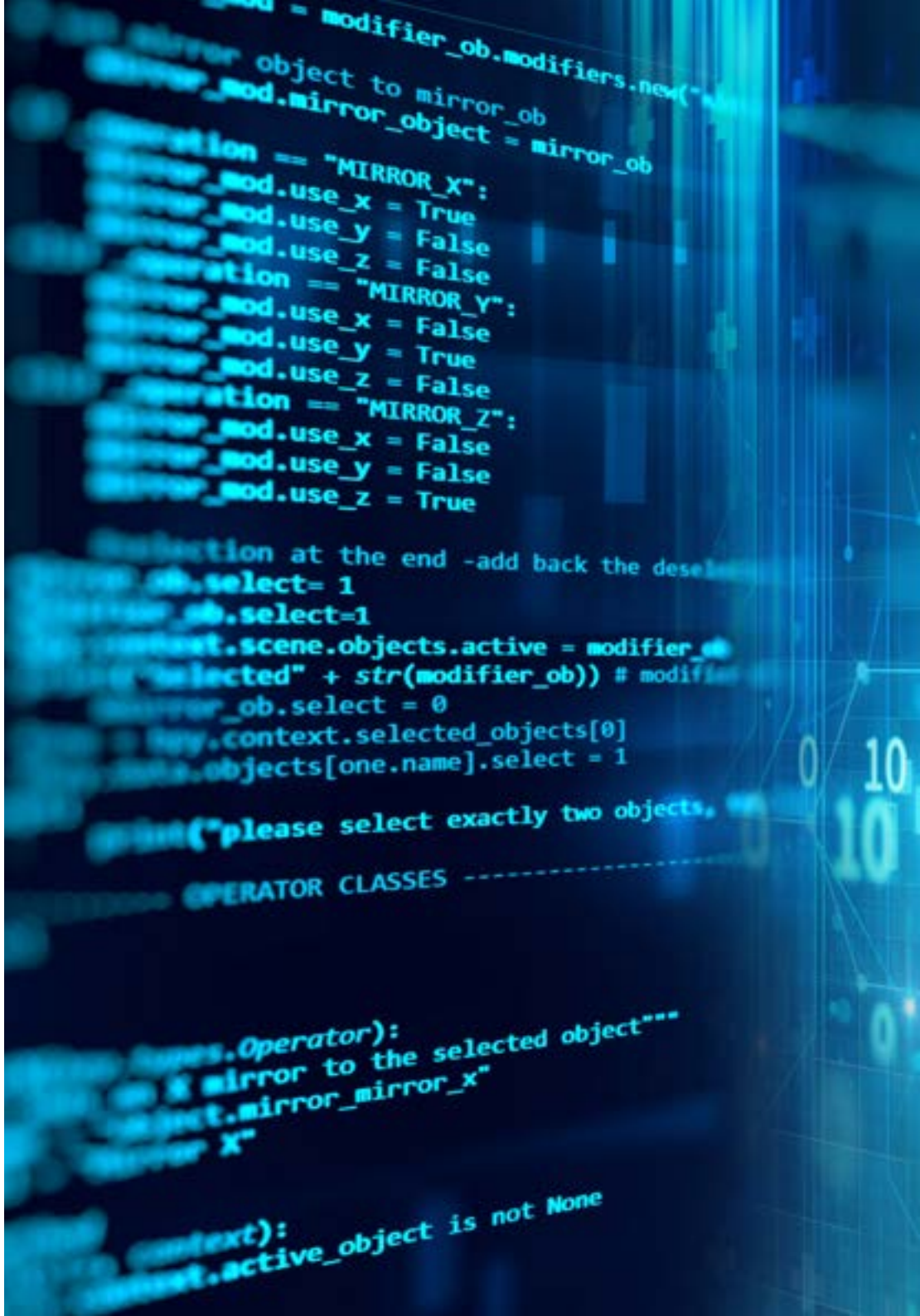
O Curso de Especialização em Segurança Informática para Comunicações tem como objetivo facilitar o desempenho dos profissionais nesta área para que possam adquirir conhecimentos sobre as suas principais novidades.

O nosso objetivo é que se torne no melhor profissional do seu setor. E para isso contamos com a melhor metodologia e com o melhor plano de estudos"

Objetivo geral

- Capacitar o aluno para poder trabalhar com total segurança e qualidade no domínio da segurança informática para comunicações

Especialize-se na principal universidade online privada do mundo"



Objetivos específicos

Módulo 1. Segurança nos sistemas e redes de comunicação

- Conhecer e saber aplicar os fundamentos da programação na internet, sistemas e serviços de telecomunicações
- Dominar as normas e regulamentos dos protocolos e redes dos organismos internacionais de normalização
- Compreender os conceitos de criptografia simétrica e assimétrica, assinatura digital, funções hash e segurança de cada nível de uma arquitetura de comunicações
- Compreender os diferentes mecanismos e protocolos de segurança baseados no controlo do acesso: autenticação e defesa perimetral
- Compreender o funcionamento das ameaças técnicas e humanas à segurança das redes e sistemas de telecomunicação
- Classificar adequadamente os diferentes serviços de segurança para redes e sistemas de acordo com os ativos que protegem
- Aplicar sistemas de gestão de redes e serviços para a configuração, exploração, controlo e tarifação de redes e serviços de telecomunicações
- Saber gerir a segurança das redes e serviços de telecomunicações através da implementação de túneis, firewalls, protocolos de encriptação e autenticação e mecanismos de proteção de conteúdos
- Ser capaz de compreender e aplicar as principais técnicas de programação segura

Módulo 2. Arquiteturas de segurança

- Compreender os princípios básicos da segurança informática
- Dominar as normas de segurança informática e os processos de certificação
- Analisar os fundamentos organizacionais e criptográficos em que se baseiam as tecnologias de segurança
- Identificar as principais ameaças e vulnerabilidades dos diferentes elementos envolvidos nas TIC, bem como as suas causas
- Conhecer aprofundadamente as ferramentas de segurança das redes e das suas funções específicas
- Saber aplicar as tecnologias que compõem uma arquitetura de segurança das TIC, nas suas diferentes perspetivas

Módulo 3. Auditoria de sistemas de informação

- Dominar os principais conceitos, normas e metodologias de auditoria de sistemas
- Conhecer os elementos organizacionais e o quadro jurídico das auditorias
- Obter um guia de referência para a conceção de novos sistemas de controlo informático interno
- Compreender e identificar os riscos associados ao desenvolvimento tecnológico
- Detetar de que forma os diferentes sistemas de informação satisfazem ou não os requisitos de segurança pretendidos
- Ser capaz de levar a cabo um processo de melhoria contínua da cibersegurança

03

Estrutura e conteúdo

A estrutura do Curso de Especialização foi concebida pelos melhores profissionais do setor da engenharia de telecomunicações com vasta experiência e prestígio reconhecido na profissão.

Dispomos do conteúdo educativo mais completo e atualizado do mercado. Procuramos a excelência e queremos que você também a alcance"

Módulo 1. Segurança em Sistemas e Redes de Comunicação

1.1. Uma perspetiva global sobre segurança, criptografia e criptanálises clássicas
- 1.1.1. Segurança informática: uma perspetiva histórica
- 1.1.2. Mas o que se entende exatamente por segurança?
- 1.1.3. História da Criptografia
- 1.1.4. Encriptadores de substituição
- 1.1.5. Estudo de caso: a máquina Enigma

1.2. Criptografia simétrica
- 1.2.1. Introdução e terminologia básica
- 1.2.2. Encriptação simétrica
- 1.2.3. Modos de funcionamento
- 1.2.4. DES
- 1.2.5. A nova norma AES
- 1.2.6. Criptografia em fluxo
- 1.2.7. Criptoanálise

1.3. Criptografia assimétrica
- 1.3.1. Origens da criptografia de chave pública
- 1.3.2. Conceitos básicos e funcionamento
- 1.3.3. O algoritmo RSA
- 1.3.4. Certificados digitais
- 1.3.5. Armazenamento e gestão de chaves

1.4. Ataques em redes
- 1.4.1. Ameaças e ataques de rede
- 1.4.2. Enumeração
- 1.4.3. Interceção do tráfego: *sniffers*
- 1.4.4. Ataques de negação de serviço
- 1.4.5. Ataques de envenenamento por ARP

1.5. Arquiteturas de segurança
- 1.5.1. Arquiteturas de segurança tradicional
- 1.5.2. *Secure Socket Layer*: SSL
- 1.5.3. Protocolo SSH
- 1.5.4. Redes Privadas Virtuais (VPNs)
- 1.5.5. Mecanismos de proteção de unidades de armazenamento externas
- 1.5.6. Mecanismos de proteção do hardware

1.6. Técnicas de proteção do sistema e desenvolvimento de código seguro
- 1.6.1. Segurança em operações
- 1.6.2. Recursos e controlos
- 1.6.3. Observação
- 1.6.4. Sistemas de deteção de intrusão
- 1.6.5. Anfitrião IDS
- 1.6.6. IDS de rede
- 1.6.7. IDS baseado na assinatura
- 1.6.8. Sistemas de engodo
- 1.6.9. Princípios básicos de segurança no desenvolvimento de códigos
- 1.6.10. Gestão de avarias
- 1.6.11. Inimigo Público Número 1: Buffer Overflow
- 1.6.12. Fundos criptográficos

1.7. Botnets e spam
- 1.7.1. Origem do problema
- 1.7.2. Processo de Spam
- 1.7.3. Envio de spam
- 1.7.4. Refinar listas de correio
- 1.7.5. Técnicas de proteção
- 1.7.6. Serviço antispam oferecidos por terceiros
- 1.7.7. Casos de estudo
- 1.7.8. Spam exótico

1.8. Auditoria e ataques na Web
- 1.8.1. Recolha de informação
- 1.8.2. Técnicas de ataque
- 1.8.3. Ferramentas

1.9. Malware e código malicioso
- 1.9.1. O que é o *malware*?
- 1.9.2. Tipos de *malware*
- 1.9.3. Vírus
- 1.9.4. Criptovírus
- 1.9.5. Worms
- 1.9.6. *Adware*
- 1.9.7. *Spyware*
- 1.9.8. *Hoaxes*
- 1.9.9. *Pishing*
- 1.9.10. Trojans
- 1.9.11. A economia do *malware*
- 1.9.12. Possíveis soluções

1.10. Análise forense
- 1.10.1. Recolha de provas
- 1.10.2. Análise das provas
- 1.10.3. Técnicas antiforenses
- 1.10.4. Casos de estudo prático

Módulo 2. Arquiteturas de Segurança

2.1. Princípios básicos da segurança informática
- 2.1.1. O que significa segurança informática?
- 2.1.2. Objetivos da segurança informática
- 2.1.3. Serviços de segurança informática
- 2.1.4. Consequências da falta de segurança
- 2.1.5. Princípio de "defesa em segurança"
- 2.1.6. Políticas, planos e procedimentos de segurança
  - 2.1.6.1. Gestão de contas de utilizadores
  - 2.1.6.2. Identificação e autenticação de utilizadores
  - 2.1.6.3. Autorização e controlo de acesso lógico
  - 2.1.6.4. Monitorização de servidores
  - 2.1.6.5. Proteção de dados
  - 2.1.6.6. Segurança nas conexões remotas
- 2.1.7. A importância do fator humano

2.2. Normalização e certificação em matéria de segurança informática
- 2.2.1. Normas de segurança
  - 2.2.1.1. Objetivo das normas
  - 2.2.1.2. Organismos responsáveis
- 2.2.2. Normas nos EUA
  - 2.2.2.1. TCSEC
  - 2.2.2.2. Federal Criteria
  - 2.2.2.3. FISCAM
  - 2.2.2.4. NIST SP 800
- 2.2.3. Normas europeias
  - 2.2.3.1. ITSEC
  - 2.2.3.2. ITSEM
  - 2.2.3.3. Agência da União Europeia para a Cibersegurança
- 2.2.4. Normas internacionais
- 2.2.5. Processo de certificação

2.3. Ameaças à segurança informática: vulnerabilidades e *malware*
- 2.3.1. Introdução
- 2.3.2. Vulnerabilidades dos sistemas
  - 2.3.2.1. Incidentes de segurança nas redes
  - 2.3.2.2. Causas das vulnerabilidades dos sistemas informáticos
  - 2.3.2.3. Tipos de vulnerabilidades
  - 2.3.2.4. Responsabilidades dos fabricantes de software
  - 2.3.2.5. Ferramentas de avaliação de vulnerabilidades
- 2.3.3. Ameaças à segurança informática
  - 2.3.3.1. Classificação dos intrusos nas redes
  - 2.3.3.2. Motivações dos atacantes
  - 2.3.3.3. Fases de um ataque
  - 2.3.3.4. Tipos de ataques
- 2.3.4. Vírus informáticos
  - 2.3.4.1. Características gerais
  - 2.3.4.2. Tipos de vírus
  - 2.3.4.3. Danos causados por vírus
  - 2.3.4.4. Como combater os vírus

2.4. Ciberterrorismo e resposta a incidentes
- 2.4.1. Introdução
- 2.4.2. A ameaça do ciberterrorismo e da ciberguerra
- 2.4.3. Consequências dos fracassos e dos ataques às empresas
- 2.4.4. A espionagem nas redes informáticas

2.5. Identificação de utilizadores e sistemas biométricos
- 2.5.1. Introdução à autenticação, autorização e registo de utilizadores
- 2.5.2. Modelo de segurança AAA
- 2.5.3. Controlo de acesso
- 2.5.4. Identificação de utilizadores
- 2.5.5. Verificação de palavras-passe
- 2.5.6. Autenticação com certificados digitais
- 2.5.7. Identificação remota de utilizadores
- 2.5.8. Início de sessão único
- 2.5.9. Gestores de palavras-passe

2.5.10. Sistemas biométricos
2.5.10.1. Características gerais
2.5.10.2. Tipos de sistemas biométricos
2.5.10.3. Implementação dos sistemas
2.6. Fundamentos da criptografia e protocolos criptográficos
2.6.1. Introdução à criptografia
2.6.1.1. Criptografia, criptoanálise e criptologia
2.6.1.2. Funcionamento de um sistema criptográfico
2.6.1.3. História dos sistemas criptográficos
2.6.2. Criptoanálise
2.6.3. Classificação dos sistemas criptográficos
2.6.4. Sistemas criptográficos simétricos e assimétricos
2.6.5. Autenticação com sistemas criptográficos
2.6.6. Assinatura eletrónica
2.6.6.1. O que é uma assinatura eletrónica?
2.6.6.2. Características da assinatura eletrónica
2.6.6.3. Autoridades de certificação
2.6.6.4. Certificados digitais
2.6.6.5. Sistemas fiáveis baseados em terceiros
2.6.6.6. Utilização de assinaturas eletrónicas
2.6.6.7. Identificação eletrónica
2.6.6.8. Fatura eletrónica
2.7. Ferramentas para a segurança na internet
2.7.1. O problema da segurança na conexão à Internet
2.7.2. A segurança na rede externa
2.7.3. O papel dos servidores Proxy
2.7.4. O papel das firewalls
2.7.5. Servidores de autenticação para conexões remotas
2.7.6. A análise dos registos de atividade
2.7.7. Sistemas de deteção de intrusão
2.7.8. Os chamarizes
2.8. Segurança de redes privadas virtuais e sem fios
2.8.1. Segurança de redes privadas virtuais
2.8.1.1 O papel das VPNs
2.8.1.2 Protocolos VPN
2.8.2. Segurança tradicional em redes sem fios
2.8.3. Possíveis ataques em redes sem fios
2.8.4. O protocolo WEP
2.8.5. Normas para a segurança das redes sem fios
2.8.6. Recomendações para reforçar a segurança
2.9. Segurança na utilização dos serviços Internet
2.9.1. Navegação segura na Web
2.9.1.1. O serviço www
2.9.1.2. Problemas de segurança na web
2.9.1.3. Recomendações de segurança
2.9.1.4. Proteção da privacidade na internet
2.9.2. Segurança no correio eletrónico
2.9.2.1. Características do correio eletrónico
2.9.2.2. Problemas de segurança do correio eletrónico
2.9.2.3. Recomendações de segurança do correio eletrónico
2.9.2.4. Serviços avançados de correio eletrónico
2.9.2.5. Utilização do correio eletrónico pelos empregados
2.9.3. O SPAM
2.9.4. O *phishing*
2.10. Controlo de conteúdos
2.10.1. A distribuição de conteúdos através da internet
2.10.2. Medidas legais para combater os conteúdos ilegais
2.10.3. Filtragem, catalogação e bloqueio de conteúdos
2.10.4. Danos à imagem e à reputação

Módulo 3. Auditoria de sistemas de informação

3.1. Auditoria de sistemas de informação. Regras de boas práticas
- 3.1.1. Introdução
- 3.1.2. Auditoria e COBIT
- 3.1.3. Auditorias dos sistemas de gestão nas TIC
- 3.1.4. Certificações

3.2. Conceitos e metodologias da auditoria de sistemas
- 3.2.1. Introdução
- 3.2.2. Metodologias de avaliação de sistemas: quantitativas e qualitativas
- 3.2.3. Metodologias da auditoria informática
- 3.2.4. O plano de auditoria

3.3. Contrato de auditoria
- 3.3.1. Natureza jurídica do contrato
- 3.3.2. Partes de um contrato de auditoria
- 3.3.3. Objeto do contrato de auditoria
- 3.3.4. O relatório de auditoria

3.4. Elementos organizacionais das auditorias
- 3.4.1. Introdução
- 3.4.2. Missão do departamento de auditoria
- 3.4.3. Planeamento das auditorias
- 3.4.4. Metodologia da auditoria de SI

3.5. Quadro jurídico das auditorias
- 3.5.1. A proteção de dados pessoais de carácter pessoal
- 3.5.2. Proteção jurídica do software
- 3.5.3. Crimes tecnológicos
- 3.5.4. Contratação, assinatura e identificação eletrónica

3.6. Auditoria da subcontratação e dos quadros de referência
- 3.6.1. Introdução
- 3.6.2. Conceitos básicos da subcontratação
- 3.6.3. Auditoria da subcontratação nas TI
- 3.6.4. Quadros de referência: CMMI, ISO27001, ITIL

3.7. Auditoria de segurança
- 3.7.1. Introdução
- 3.7.2. Segurança física e lógica
- 3.7.3. Segurança do ambiente
- 3.7.4. Planeamento e execução da auditoria de segurança física

3.8. Gestão de redes e internet
- 3.8.1. Introdução
- 3.8.2. Vulnerabilidades nas redes
- 3.8.3. Princípios e direitos na Internet
- 3.8.4. Controlo e tratamento dos dados

3.9. Auditoria de aplicações e sistemas informáticos
- 3.9.1. Introdução
- 3.9.2. Modelos de referência
- 3.9.3. Avaliação da qualidade das aplicações
- 3.9.4. Auditoria da organização e da gestão da área do desenvolvimento e manutenção

3.10. Auditoria de dados pessoais
- 3.10.1. Introdução
- 3.10.2. Leis e regulamentos de proteção de dados
- 3.10.3. Desenvolvimento da auditoria
- 3.10.4. Infrações e sanções

Esta capacitação permitir-lhe-á progredir na sua carreira de forma cómoda"

04

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

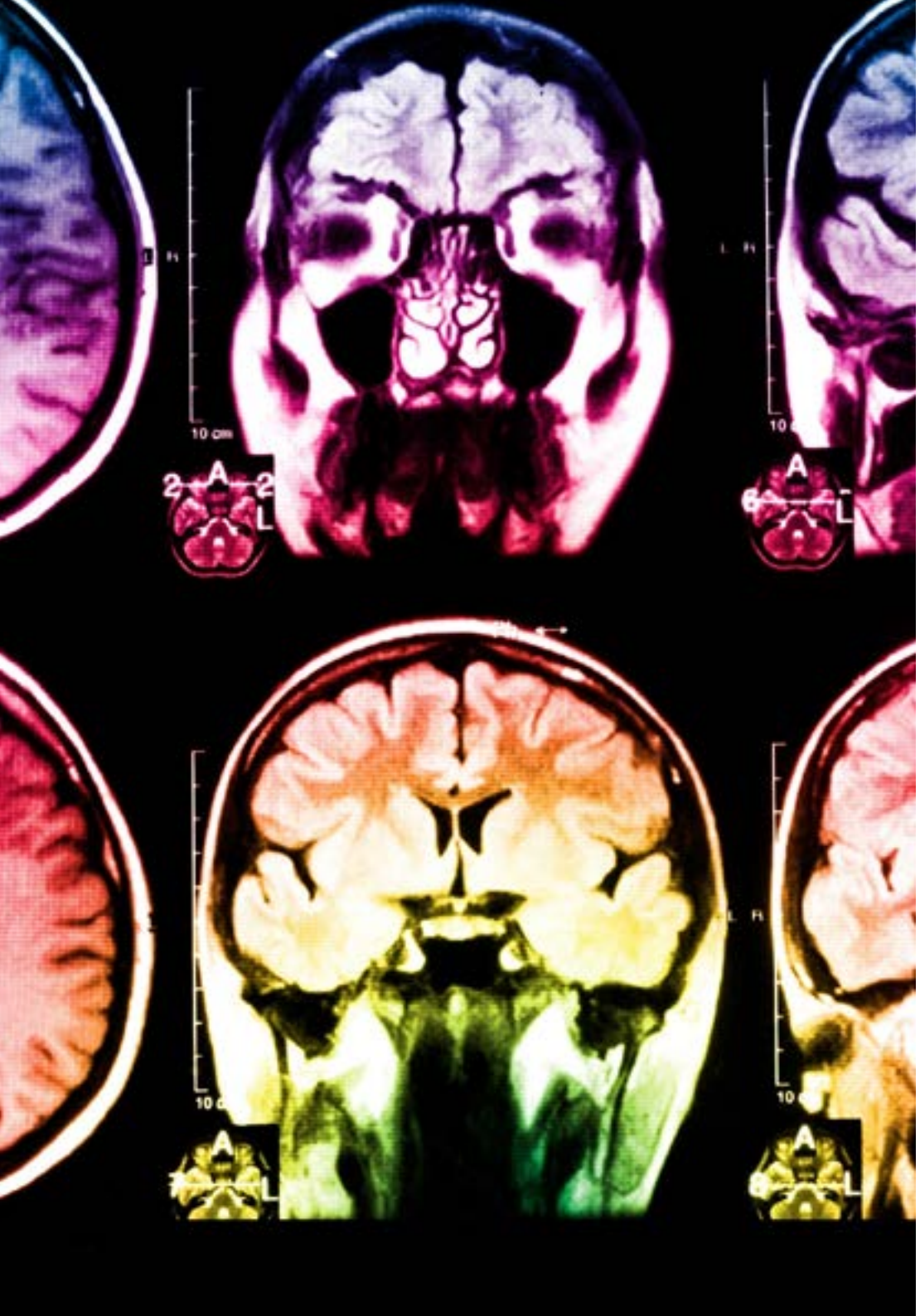
A TECH combina eficazmente a metodologia do Estudo de Caso com um sistema de aprendizagem 100% online baseado na repetição, que combina elementos didáticos diferentes em cada lição.

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.

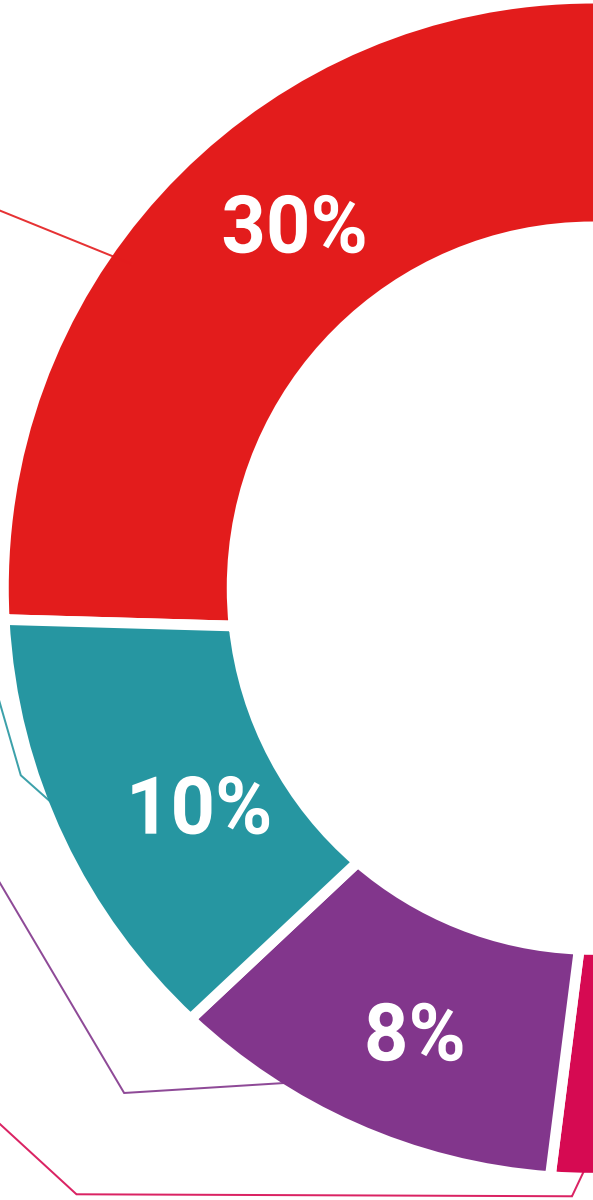
O denominado Learning from an Expert constrói conhecimento e memória, e gera confiança em futuras decisões difíceis.

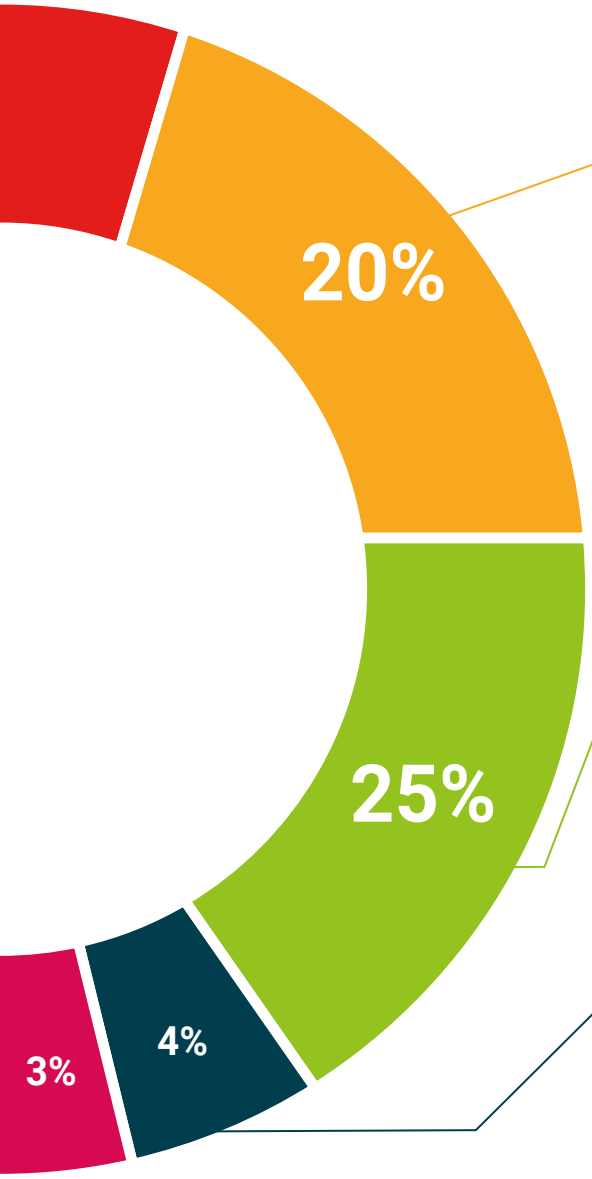
Práticas de aptidões e competências

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.

05

Certificação

O Curso de Especialização em Segurança Informática para Comunicações 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 Segurança Informática para Comunicações** 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 Informática para Comunicações**

Modalidade: **online**

Duração: **6 messes**

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

Segurança Informática para Comunicações

Este é um certificado atribuído por esta Universidade, reconhecido por 18 ECTS e equivalente a 600 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

Segurança Informática para Comunicações

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

Curso de Especialização

Segurança Informática para Comunicações

tech universidade tecnológica