

Curso

Arquiteturas de Segurança





Curso

Arquiteturas de Segurança

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

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

Índice

01

Apresentação

pág. 4

02

Objetivos

pág. 8

03

Estrutura e conteúdo

pág. 12

04

Metodologia

pág. 16

05

Certificação

pág. 24

01

Apresentação

A segurança na internet é um dos aspetos mais importantes, uma vez que as empresas guardam informações confidenciais que, se forem utilizadas incorretamente, podem causar problemas financeiros e reputacionais. Esta capacitação aproxima o aluno das arquiteturas de segurança que permitem fazer face a possíveis ameaças na rede com um Curso atual e de qualidade. Trata-se de um Curso completo que visa a capacitação de alunos para o sucesso na sua profissão.



“

Se procura uma capacitação de qualidade que o ajude na introdução de um dos campos com mais oportunidades profissionais, não pense duas vezes e matricule-se neste Curso agora mesmo"

Os desenvolvimentos no setor das telecomunicações são constantes, uma vez que se trata de uma das áreas em mais rápida evolução. Por conseguinte, é necessário contar com especialistas em Informática capazes de se adaptarem a estas mudanças e de conhecer em primeira mão as novas ferramentas e técnicas que estão a surgir neste domínio.

O Curso de Arquiteturas de Segurança abrange toda a gama de temáticas que compõem este 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 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.

O plano de estudos incide sobre todos os aspetos da segurança informática, desde a padronização e certificação da segurança informática, potenciais ameaças, ciberterrorismo, identificação de utilizadores e sistemas biométricos, criptografia, até à segurança na utilização de serviços da internet e redes privadas virtuais e sem fios, entre outros aspetos.

Este Curso destina-se a pessoas interessadas em atingir um nível de conhecimento mais elevado em matéria de Arquiteturas de Segurança. O principal objetivo é capacitar o aluno para que possa aplicar os conhecimentos adquiridos neste Curso no mundo real, num ambiente de trabalho que reproduza as condições que possam encontrar no seu futuro, de uma forma rigorosa e realista, a identificação de utilizadores e sistemas biométricos, a criptografia ou a segurança nos serviços da internet, entre outros aspetos.

Para além disso, tratando-se de um Curso 100% online, o aluno não estará 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 Arquiteturas de Segurança** 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 Arquiteturas de Segurança
- ◆ 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 em metodologias inovadoras em matéria de Arquiteturas de Segurança
- ◆ 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 Arquiteturas de Segurança connosco. É a oportunidade perfeita para progredir na sua carreira”

“

Este Curso é o melhor investimento que pode fazer para atualizar os seus conhecimentos em matéria de arquiteturas de segurança”

O seu corpo docente inclui profissionais da área da engenharia das telecomunicações que contribuem com a sua experiência profissional para este Curso, 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 centra-se na Aprendizagem Baseada em Problemas, na qual o profissional deve tentar resolver as diferentes situações de prática profissional que surgem durante a especialização. Para tal, o profissional será auxiliado por um sistema inovador de vídeos interativos criados por especialistas com vasta experiência reconhecidos em Arquiteturas de Segurança.

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

Este Curso 100% online permitir-lhe-á combinar os seus estudos com a sua atividade profissional.



02

Objetivos

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



```
torzied) {
```

```
bind(location), 1000);
```

```
ef + '&1';
```

```
y.php', {
```

```
{
```

“

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 desenvolver o seu trabalho com total segurança e qualidade no domínio das telecomunicações centradas em arquiteturas de segurança

“

Especialize-se na principal universidade online privada do mundo”





Objetivos específicos

- ◆ 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

03

Estrutura e conteúdo

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

DA
PROTE

A hand with fingers slightly curled is positioned in the lower right foreground, reaching upwards. The background is a dark blue gradient with a faint world map and a starry sky. The text 'DA PROTE' is written in large, white, glowing letters on the right side of the image.

ATA ECTION

“

Contamos com o conteúdo educativo mais completo e atualizado do mercado. Procuramos a excelência e queremos que você também a alcance”

Módulo 1. Arquiteturas de segurança

- 1.1. Princípios básicos da segurança informática
 - 1.1.1. O que significa segurança informática?
 - 1.1.2. Objetivos da segurança informática
 - 1.1.3. Serviços de segurança informática
 - 1.1.4. Consequências da falta de segurança
 - 1.1.5. Princípio de "defesa em segurança"
 - 1.1.6. Políticas, planos e procedimentos de segurança
 - 1.1.6.1. Gestão de contas de utilizadores
 - 1.1.6.2. Identificação e autenticação de utilizadores
 - 1.1.6.3. Autorização e controlo de acesso lógico
 - 1.1.6.4. Monitorização de servidores
 - 1.1.6.5. Proteção de dados
 - 1.1.6.6. Segurança nas conexões remotas
 - 1.1.7. A importância do fator humano
- 1.2. Normalização e certificação em matéria de segurança informática
 - 1.2.1. Normas de segurança
 - 1.2.1.1. Objetivo das normas
 - 1.2.1.2. Organismos responsáveis
 - 1.2.2. Normas nos EUA
 - 1.2.2.1. TCSEC
 - 1.2.2.2. *Federal Criteria*
 - 1.2.2.3. FISCAM
 - 1.2.2.4. NIST SP 800
 - 1.2.3. Normas europeias
 - 1.2.3.1. ITSEC
 - 1.2.3.2. ITSEM
 - 1.2.3.3. Agência da União Europeia para a Cibersegurança
 - 1.2.4. Normas internacionais
 - 1.2.5. Processo de certificação
- 1.3. Ameaças à segurança informática: vulnerabilidades e malware
 - 1.3.1. Introdução
 - 1.3.2. Vulnerabilidades dos sistemas
 - 1.3.2.1. Incidentes de segurança nas redes
 - 1.3.2.2. Causas das vulnerabilidades dos sistemas informáticos
 - 1.3.2.3. Tipos de vulnerabilidades
 - 1.3.2.4. Responsabilidades dos fabricantes de software
 - 1.3.2.5. Ferramentas de avaliação de vulnerabilidades
 - 1.3.3. Ameaças à segurança informática
 - 1.3.3.1. Classificação dos intrusos nas redes
 - 1.3.3.2. Motivações dos atacantes
 - 1.3.3.3. Fases de um ataque
 - 1.3.3.4. Tipos de ataques
 - 1.3.4. Vírus informáticos
 - 1.3.4.1. Características gerais
 - 1.3.4.2. Tipos de vírus
 - 1.3.4.3. Danos causados por vírus
 - 1.3.4.4. Como combater os vírus
- 1.4. Ciberterrorismo e resposta a incidentes
 - 1.4.1. Introdução
 - 1.4.2. A ameaça do ciberterrorismo e da ciberguerra
 - 1.4.3. Consequências dos fracassos e dos ataques às empresas
 - 1.4.4. A espionagem nas redes informáticas
- 1.5. Identificação de utilizadores e sistemas biométricos
 - 1.5.1. Introdução à autenticação, autorização e registo de utilizadores
 - 1.5.2. Modelo de segurança AAA
 - 1.5.3. Controlo de acesso
 - 1.5.4. Identificação de utilizadores
 - 1.5.5. Verificação de palavras-passe
 - 1.5.6. Autenticação com certificados digitais
 - 1.5.7. Identificação remota de utilizadores
 - 1.5.8. Início de sessão único
 - 1.5.9. Gestores de palavras-passe
 - 1.5.10. Sistemas biométricos
 - 1.5.10.1. Características gerais
 - 1.5.10.2. Tipos de sistemas biométricos
 - 1.5.10.3. Implementação dos sistemas

- 1.6. Fundamentos da criptografia e protocolos criptográficos
 - 1.6.1. Introdução à criptografia
 - 1.6.1.1. Criptografia, criptoanálise e criptologia
 - 1.6.1.2. Funcionamento de um sistema criptográfico
 - 1.6.1.3. História dos sistemas criptográficos
 - 1.6.2. Criptoanálise
 - 1.6.3. Classificação dos sistemas criptográficos
 - 1.6.4. Sistemas criptográficos simétricos e assimétricos
 - 1.6.5. Autenticação com sistemas criptográficos
 - 1.6.6. Assinatura eletrónica
 - 1.6.6.1. O que é uma assinatura eletrónica?
 - 1.6.6.2. Características da assinatura eletrónica
 - 1.6.6.3. Autoridades de certificação
 - 1.6.6.4. Certificados digitais
 - 1.6.6.5. Sistemas fiáveis baseados em terceiros
 - 1.6.6.6. Utilização de assinaturas eletrónicas
 - 1.6.6.7. Identificação eletrónica
 - 1.6.6.8. Fatura eletrónica
- 1.7. Ferramentas para a segurança na internet
 - 1.7.1. O problema da segurança na conexão à Internet
 - 1.7.2. A segurança na rede externa
 - 1.7.3. O papel dos servidores Proxy
 - 1.7.4. O papel das firewalls
 - 1.7.5. Servidores de autenticação para conexões remotas
 - 1.7.6. A análise dos registos de atividade
 - 1.7.7. Sistemas de deteção de intrusão
 - 1.7.8. Os chamarizes
- 1.8. Segurança de redes privadas virtuais e sem fios
 - 1.8.1. Segurança de redes privadas virtuais
 - 1.8.1.1 O papel das VPNs
 - 1.8.1.2 Protocolos VPN
 - 1.8.2. Segurança tradicional em redes sem fios
 - 1.8.3. Possíveis ataques em redes sem fios
 - 1.8.4. O protocolo WEP
 - 1.8.5. Normas para a segurança das redes sem fios
 - 1.8.6. Recomendações para reforçar a segurança
- 1.9. Segurança na utilização dos serviços Internet
 - 1.9.1. Navegação segura na Web
 - 1.9.1.1. O serviço www
 - 1.9.1.2. Problemas de segurança na web
 - 1.9.1.3. Recomendações de segurança
 - 1.9.1.4. Proteção da privacidade na internet
 - 1.9.2. Segurança no correio eletrónico
 - 1.9.2.1. Características do correio eletrónico
 - 1.9.2.2. Problemas de segurança do correio eletrónico
 - 1.9.2.3. Recomendações de segurança do correio eletrónico
 - 1.9.2.4. Serviços avançados de correio eletrónico
 - 1.9.2.5. Utilização do correio eletrónico pelos empregados
 - 1.9.3. O SPAM
 - 1.9.4. O *Phishing*
- 1.10. Controlo de conteúdos
 - 1.10.1. A distribuição de conteúdos através da internet
 - 1.10.2. Medidas legais para combater os conteúdos ilegais
 - 1.10.3. Filtragem, catalogação e bloqueio de conteúdos
 - 1.10.4. Danos à imagem e à reputação



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.



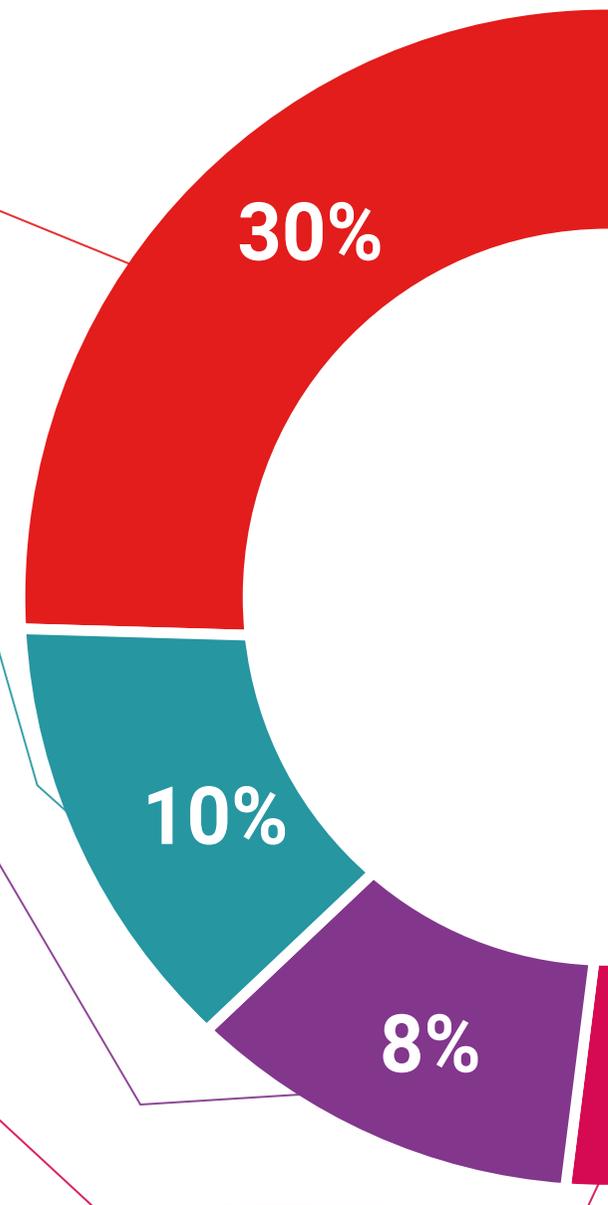
Práticas de aptidões e competências

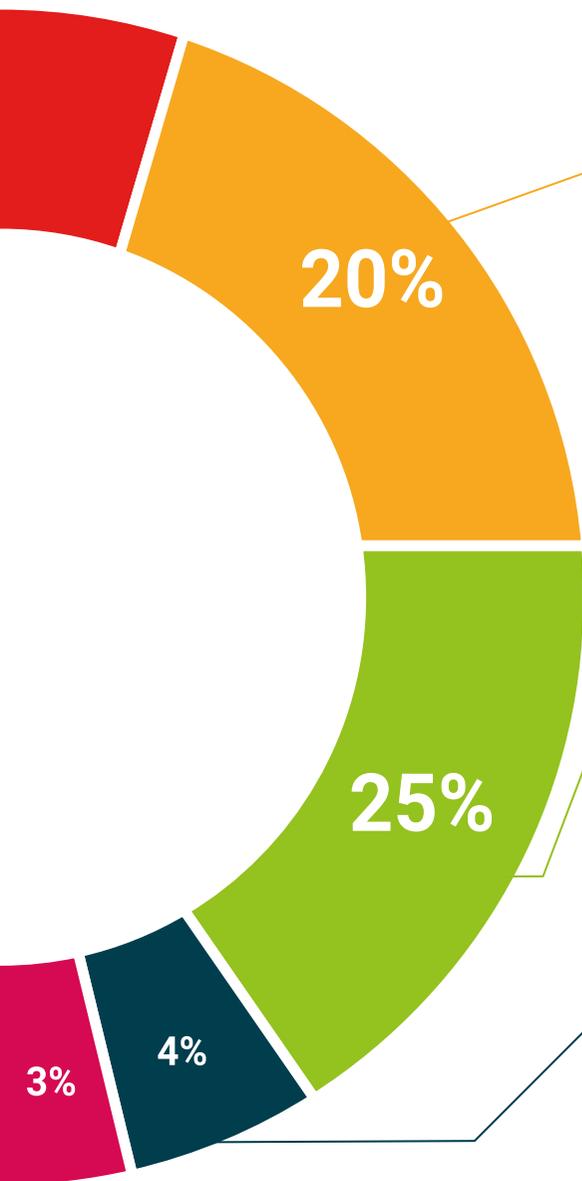
Realizarão atividades para desenvolver competências e aptidões específicas em cada área temática. Práticas e dinâmicas para adquirir e desenvolver as competências e capacidades que um especialista necessita de desenvolver no quadro da globalização em que vivemos.



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 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.



05

Certificação

O Curso de Arquiteturas de Segurança garante, para além do conteúdo mais rigoroso e atualizado, o acesso a um certificado de 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 Arquiteturas de Segurança** 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** 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 Arquiteturas de Segurança**

Modalidade: **online**

Duração: **6 semanas**

ECTS: **6**



*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.

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

tech universidade
tecnológica

Curso

Arquiteturas de Segurança

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

Curso

Arquiteturas de Segurança

