Curso de Especialização

Segurança na Engenharia de Software

tech universidade tecnológica

tech universidade tecnológica

Curso de Especialização

Segurança na Engenharia de Software

- Modalidade: **online**
- Duração: **6 meses**
- Certificação: **TECH Universidade Tecnológica**
- Qualificação: **24 ECTS**
- Carga horária: **16horas/semana**
- Horário: **ao seu ritmo**
- Exames: **online**

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

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

Esta capacitação de alto nível vai permitir ao aluno ficará a conhecer o processo de segurança da informação, as suas implicações na confidencialidade, integridade, disponibilidade e custos económicos, bem como compreender os problemas relacionados com a segurança do software, as suas vulnerabilidades e a sua classificação.

Com esta qualificação de elevado rigor científico, o profissional adquirirá os conhecimentos necessários para o controlo interno informático e para avaliar e detetar vulnerabilidades nas aplicações online.

Especialize-se em Sistemas Informáticos sob a orientação de profissionais com uma vasta experiência no setor"

Esta capacitação abrangente em Segurança na Engenharia de Software permitirá aos profissionais da indústria das Tecnologias de Informação aprofundar e formar-se nos processos de gestão e monitorização de software de qualidade e seguro, que satisfaça requisitos pré-definidos.

Este Curso de Especialização especializa o estudante em Segurança na Engenharia de Software, a fim de lhe fornecer os conhecimentos e as ferramentas necessárias para a conceção e o controlo de sistemas complexos que respondem a problemas de forma fiável.

O principal objetivo desta capacitação é que o aluno adquira a capacidade de incorporar melhorias qualitativas substanciais, fornecendo novas soluções para problemas específicos. Pretende ainda formar profissionais capazes de utilizar uma abordagem sistemática e quantificável no desenvolvimento e manutenção de software, de modo a que obtenham também um conhecimento profundo da programação informática, implementação e planeamento de sistemas informáticos, numa perspetiva prática e adaptada à realidade atual.

Com esta capacitação, contará com os recursos didáticos mais avançados e terá a oportunidade de realizar um programa de ensino que reúne os conhecimentos mais aprofundados na área, onde um grupo de professores com elevado rigor científico e ampla experiência internacional lhe proporcionará a informação mais completa e atualizada sobre os últimos avanços e técnicas em engenharia de software e sistemas de informação.

O plano de estudos abrange os principais tópicos da atualidade em Segurança na Engenharia de Software, de tal forma que quem os dominar estará preparado para trabalhar nesta área. Portanto, não é apenas mais um certificado, mas uma verdadeira ferramenta de aprendizagem que aborda os temas da especialidade de maneira atualizada, objetiva e criteriosa, com base na informação de ponta atual.

Deve-se notar que, sendo um Curso de Especialização 100% online, o estudante não está condicionado por horários fixos ou pela necessidade de se deslocar para outro local físico, mas pode aceder aos conteúdos em qualquer altura do dia, conciliando a sua vida profissional ou pessoal com a vida académica.

Se pretende diferenciar-se e ser capaz de conceber e desenvolver projetos complexos de engenharia de sistemas, esta é a qualificação certa para si.

Este **Curso de Especialização em Segurança na Engenharia de Software** 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 Segurança na Engenharia de Software
- Os conteúdos gráficos, esquemáticos e predominantemente práticos com que está concebido fornecem informações científicas e práticas sobre as disciplinas que são essenciais para a prática profissional
- Os exercícios práticos onde o processo de autoavaliação pode ser efetuado a fim de melhorar a aprendizagem
- O seu foco especial em metodologias inovadoras em Segurança na Engenharia de Software
- As aulas teóricas, perguntas ao especialista, fóruns de discussão sobre temas controversos e atividades de reflexão individual
- A disponibilidade de acesso aos conteúdos a partir de qualquer dispositivo fixo ou portátil com ligação à Internet

A conclusão deste Curso de Especialização colocará os profissionais da Segurança na Engenharia de Software na vanguarda dos mais recentes desenvolvimentos no setor"

Este Curso de Especialização é o melhor investimento que pode fazer ao selecionar uma capacitação de atualização no domínio da Segurança na Engenharia]de Software. *Oferecemos-lhe qualidade e acesso gratuito ao conteúdo"*

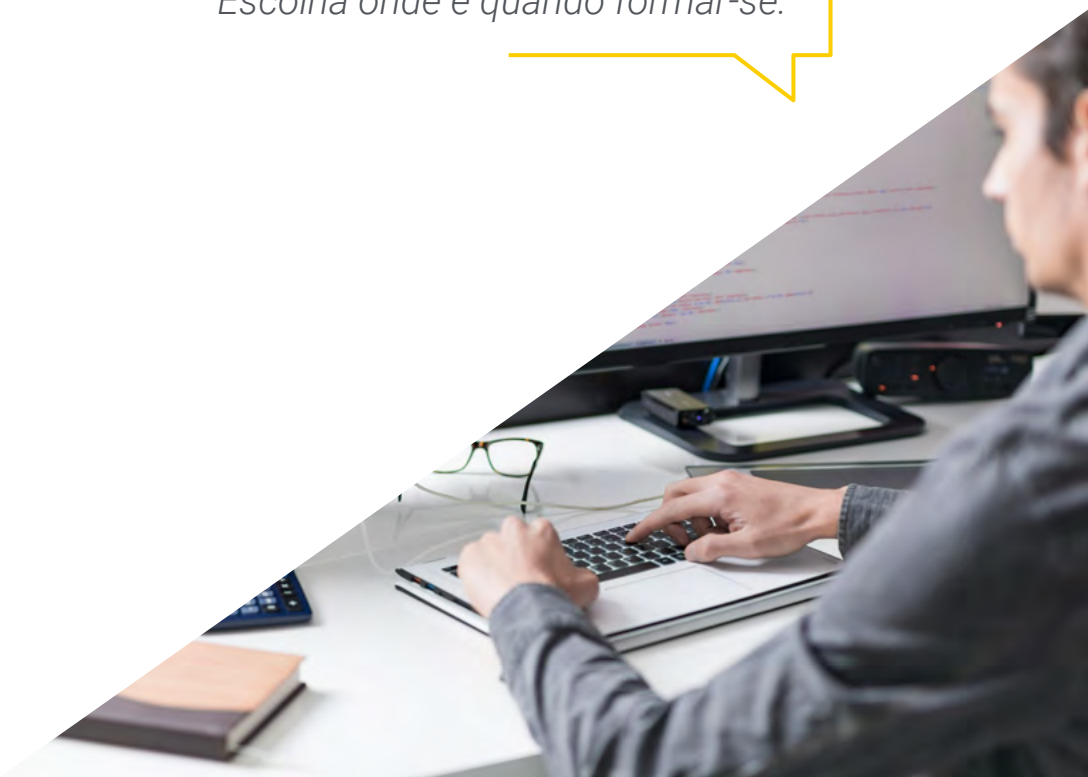
Esta capacitação conta com o melhor material didático, o que lhe permitirá realizar um estudo contextual que facilitará a sua aprendizagem.

Este Curso de Especialização 100% online permitir-lhe-á combinar os seus estudos com o seu trabalho profissional. Escolha onde e quando formar-se.

O seu corpo docente inclui profissionais do setor da Segurança na Engenharia de Software que trazem a sua experiência profissional para esta capacitação, bem como especialistas reconhecidos de empresas de referência e universidades de prestígio.

O seu conteúdo multimédia, desenvolvido com a mais recente tecnologia educacional, irá permitir que o profissional tenha acesso a uma aprendizagem situada e contextual, isto é, um ambiente de simulação que proporcionará uma capacitação imersiva, programada para praticar em situações reais.

A conceção desta especialização foca-se na Aprendizagem Baseada em Problemas, através da qual o profissional deverá tentar resolver as diferentes situações da atividade profissional que surgem ao longo do Curso de Especialização. Para tal, o profissional poderá contar com o apoio de um sistema inovador de vídeo interativo desenvolvido por especialistas reconhecidos e com vasta experiência em Segurança na Engenharia de Software.



02

Objetivos

O Curso de Especialização em Segurança na Engenharia de Software tem como objetivo facilitar o desempenho do profissional para que este possa adquirir e conhecer as principais novidades neste campo, o que lhe permitirá exercer a sua profissão com a máxima qualidade e profissionalismo.

O nosso objetivo é que se torne o melhor profissional do seu setor. E para isso temos a melhor metodologia e conteúdo"

Objetivos gerais

- Adquirir novos conhecimentos em Segurança na Engenharia de Software
- Adquirir novas competências em termos de novas tecnologias, os últimos desenvolvimentos de software
- Tratar os dados gerados nas atividades de engenharia de software

Melhorar as suas competências no campo da Segurança na Engenharia de Software permitir-lhe-á ser mais competitivo. Continue a sua aprendizagem e dê um impulso à sua carreira"

Objetivos específicos

Módulo 1. Gestão da segurança

- Conhecer o processo de segurança da informação, as suas implicações em termos de confidencialidade, integridade, disponibilidade e custos económicos
- Aprender o uso de boas práticas de segurança na gestão de serviços de tecnologias da informação
- Adquirir os conhecimentos para a correta certificação dos processos de segurança
- Compreender os mecanismos e métodos de autenticação para o controlo de acesso, bem como o processo de auditoria de acessos
- Compreender os programas de gestão de segurança, gestão de riscos e conceção de políticas de segurança
- Conhecer os planos de continuidade de negócios, as suas fases e o processo de manutenção
- Conhecer os procedimentos para a correta proteção da empresa através das redes DMZ, a utilização de sistemas de deteção de intrusão e outras metodologias

Módulo 2. Segurança do software

- Compreender os problemas relacionados com a segurança do software, as suas vulnerabilidades e como são classificadas
- Conhecer os princípios de design, metodologias e normas de segurança de software
- Compreender a aplicação da segurança nas diferentes fases do ciclo de vida do software
- Adquirir os conhecimentos necessários para uma codificação segura do Software e as suas técnicas de validação
- Assimilar metodologias e processos para garantir a segurança durante o desenvolvimento e prestação de serviços na cloud
- Compreender as bases da criptologia e as diferentes técnicas de encriptação que existem atualmente

Módulo 3. Auditoria de segurança

- Adquirir os conhecimentos necessários para a correta execução do processo de auditoria e controlo interno informático
- Compreender os processos a realizar para a auditoria de segurança de sistemas e redes
- Compreender as diferentes ferramentas de apoio, metodologias e análise subsequente durante a auditoria de segurança da Internet e dos dispositivos móveis
- Aprender as propriedades e os fatores de influência que condicionam os riscos empresariais e determinam a correta implementação de uma gestão adequada dos riscos
- Conhecer as medidas de mitigação de riscos, bem como as metodologias de implementação de um Sistema de Gestão de Segurança da Informação e os regulamentos e normas a serem utilizados
- Compreender os procedimentos para a realização da auditoria de segurança, a sua rastreabilidade e a apresentação de resultados

Módulo 4. Segurança das aplicações online

- Adquirir os conhecimentos necessários para avaliar e detetar as vulnerabilidades das aplicações online
- Compreender as políticas e normas de segurança a serem aplicadas às aplicações online
- Conhecer os procedimentos a utilizar durante o desenvolvimento de aplicações web e a sua subsequente validação através de análises e testes de segurança
- Aprender as medidas de segurança para a implementação e produção de aplicações Web
- Compreender os conceitos, funções e tecnologias a aplicar na segurança dos serviços web, bem como os testes de segurança e as medidas de proteção
- Assimilar os procedimentos para a realização do hacking ético, análise de malware e forense
- Conhecer as medidas de mitigação e contenção de incidentes em serviços Web
- Adquirir conhecimentos para a implementação de técnicas de boas práticas para o desenvolvimento e implementação de aplicações online, bem como os erros mais comuns

03

Direção do curso

Este programa académico conta com o corpo docente mais especializado do mercado educativo atual. São especialistas seleccionados pela TECH para desenvolver todo o itinerário. Desta forma, com base na sua própria experiência e nas mais recentes evidências, conceberam os conteúdos mais actuais que oferecem uma garantia de qualidade numa matéria tão relevante.

A TECH oferece-lhe o corpo docente mais especializado na área de estudo. Inscreva-se já e desfrute da qualidade que merece".

Diretor Internacional Convidado

Darren Pulsipher é um arquiteto de software altamente experiente, um inovador com uma destacada trajetória internacional no desenvolvimento de software e firmware. De fato, possui habilidades altamente desenvolvidas em comunicação, gestão de projetos e negócios, o que tem-lhe permitido liderar importantes iniciativas a nível global.

Assim, ocupou altos cargos de grande responsabilidade ao longo de sua carreira, como o de Arquiteto Chefe de Soluções para o Setor Público na Intel Corporation, onde promoveu negócios modernos, processos e tecnologias para clientes, parceiros e usuários do setor público. Além disso, fundou a Yoly Inc., onde também se desempenhou como CEO, trabalhando para desenvolver uma ferramenta de agregação e diagnóstico de redes sociais baseada em Software Como Serviço (SaaS), utilizando para isso tecnologias de Big Data e Web 2.0.

Adicionalmente, exerceu em outras empresas, como Diretor Sénior de Engenharia na Dell Technologies, onde dirigiu a Unidade de Negócios de Big Data na Nuvem, liderando equipas nos Estados Unidos e na China para a gestão de projetos de grande envergadura e a reestruturação de divisões empresariais para sua integração bem-sucedida. Igualmente, trabalhou como Diretor de Tecnologias da Informação (Chief Information Officer) na XanGo, onde gerenciou projetos como suporte de Help Desk, suporte de produção e desenvolvimento de soluções.

Entre as múltiplas especialidades nas quais é especialista, destacam-se a tecnologia Edge to Cloud, a cibersegurança, a Inteligência Artificial Generativa, o desenvolvimento de software, a tecnologia de redes, o desenvolvimento nativo na nuvem e o ecossistema de contêineres. Conhecimentos que compartilhou através do pódcast e boletim semanal "Embracing Digital Transformation", que ele mesmo produziu e apresentou, ajudando as organizações a navegar com sucesso na transformação digital, aproveitando as pessoas, os processos e tecnologia.

Sr. Pulsipher, Darren

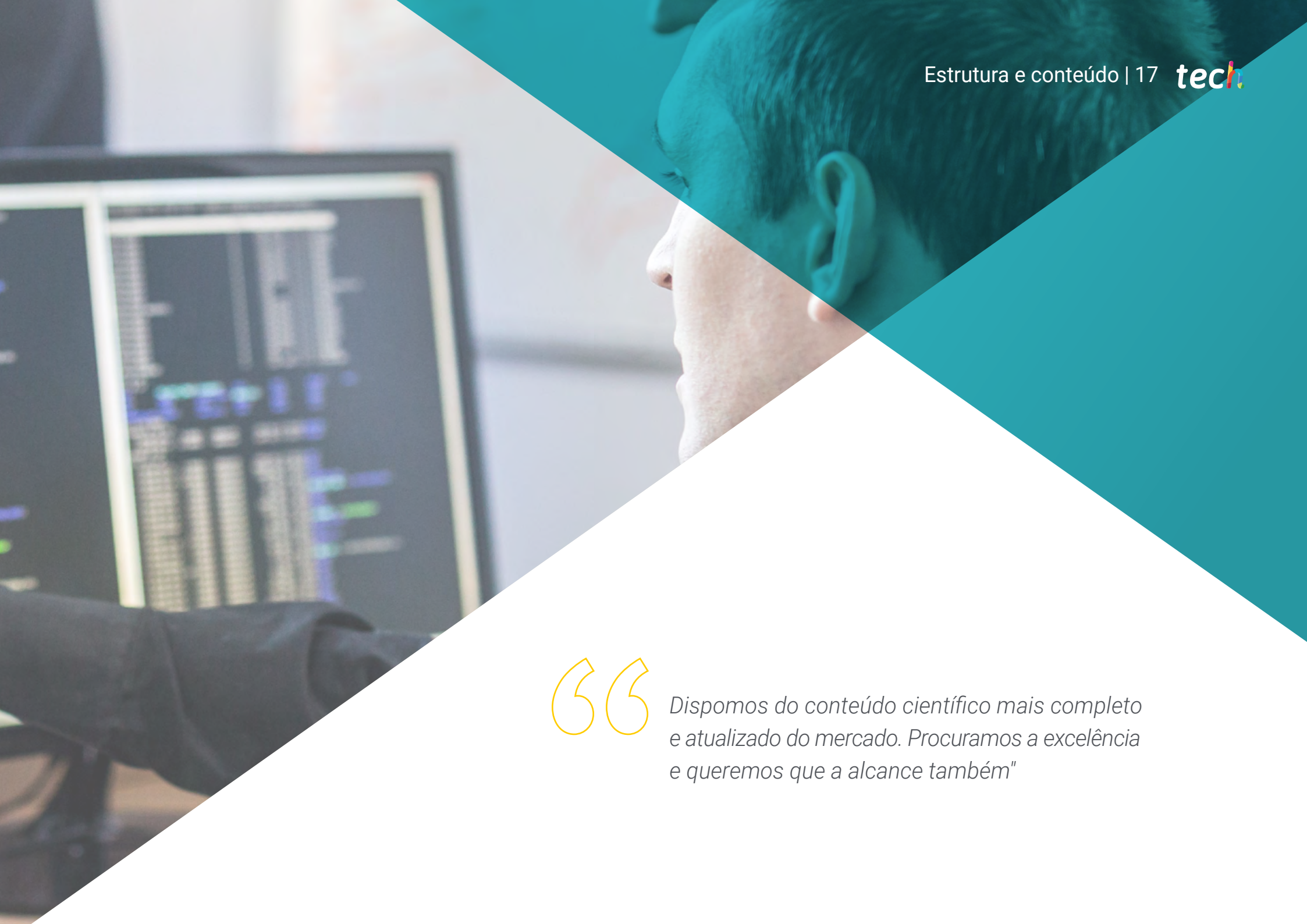
- Arquiteto Chefe de Soluções para o Setor Público na Intel, Califórnia, Estados Unidos
- Apresentador e Produtor de "Embracing Digital Transformation", Califórnia
- Fundador e CEO na Yoly Inc., Arkansas
- Diretor Sénior de Engenharia na Dell Technologies, Arkansas
- Diretor de Tecnologias da Informação (Chief Information Officer) na XanGo, Utah
- Arquiteto Sénior na Cadence Design Systems, Califórnia
- Gerente Sénior de Processos de Projetos na Lucent Technologies, Califórnia
- Engenheiro de Software na Cemax-Icon, Califórnia
- Engenheiro de Software na ISG Technologies, Canadá
- MBA em Gestão de Tecnologia pela Universidade de Phoenix
- Licenciatura em Ciências da Computação e Engenharia Elétrica pela Universidade Brigham Young

Graças à TECH, poderá aprender com os melhores profissionais do mundo"

04

Estrutura e conteúdo

A estrutura dos conteúdos foi desenvolvida pelos melhores profissionais do setor da Segurança na Engenharia de Software, com ampla experiência e reconhecido prestígio na profissão, e conscientes dos benefícios que a última tecnologia educacional pode trazer ao ensino superior.



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

Módulo 1. Gestão da segurança

1.1. A segurança da informação
- 1.1.1. Introdução
- 1.1.2. A segurança da informação implica confidencialidade, integridade e disponibilidade
- 1.1.3. A segurança é um assunto económico
- 1.1.4. A segurança é um processo
- 1.1.5. A classificação da informação
- 1.1.6. A segurança da informação implica a gestão de riscos
- 1.1.7. A segurança é articulada com controlos de segurança
- 1.1.8. A segurança é tanto física como lógica
- 1.1.9. A segurança envolve pessoas

1.2. O profissional da segurança da informação
- 1.2.1. Introdução
- 1.2.2. A segurança da informação como profissão
- 1.2.3. As certificações (ISC)2
- 1.2.4. A norma ISO 27001
- 1.2.5. Boas práticas de segurança na gestão de serviços TI
- 1.2.6. Modelos de maturidade para a segurança da informação
- 1.2.7. Outras certificações, normas e recursos profissionais

1.3. Controlo de acessos
- 1.3.1. Introdução
- 1.3.2. Requisitos de controlo de acessos
- 1.3.3. Mecanismos de autenticação
- 1.3.4. Métodos de autorização
- 1.3.5. Contabilidade e auditoria de acessos
- 1.3.6. Tecnologias «Triple A»

1.4. Programas, processos e políticas de segurança da informação
- 1.4.1. Introdução
- 1.4.2. Programa de gestão da segurança
- 1.4.3. A gestão de riscos
- 1.4.4. Conceção de políticas de segurança

1.5. Planos de continuidade de negócio
- 1.5.1. Introdução às PCN
- 1.5.2. Fase I e II
- 1.5.3. Fase III e IV
- 1.5.4. Manutenção do PCN

1.6. Procedimentos para a correta proteção da empresa
- 1.6.1. Redes DMZ
- 1.6.2. Sistemas de deteção de intrusos
- 1.6.3. Listas de controlo de acessos
- 1.6.4. Aprender com o atacante: *Honeypot*

1.7. Arquitetura de segurança. Prevenção
- 1.7.1. Visão geral. Atividades e modelo de camadas
- 1.7.2. Defesa perimetral (*firewalls*, WAFs, IPS, etc.)
- 1.7.3. Defesa do ponto final (equipamento, servidores e serviços)

1.8. Arquitetura de segurança. Deteção
- 1.8.1. Visão geral deteção e supervisão
- 1.8.2. *Logs*, rutura de tráfico encriptado, gravação e *Siems*
- 1.8.3. Alertas e inteligência

1.9. Arquitetura de segurança. Reação
- 1.9.1. Reação. Produtos, serviços e recursos
- 1.9.2. Gestão de incidentes
- 1.9.3. CERTS e CSIRTs

1.10. Arquitetura de segurança. Recuperação
- 1.10.1. Resiliência, conceitos, requisitos de negócio e normas
- 1.10.2. Soluções IT de resiliência
- 1.10.3. Gestão e governação das crises

Módulo 2. Segurança no software

2.1. Problemas de segurança do software
- 2.1.1. Introdução ao problema da segurança no software
- 2.1.2. Vulnerabilidades e a sua classificação
- 2.1.3. Propriedades software seguro
- 2.1.4. Referências

2.2. Princípios de conceção de segurança do software
- 2.2.1. Introdução
- 2.2.2. Princípios de conceção de segurança do software
- 2.2.3. Tipos de S-SDLC
- 2.2.4. Segurança do software nas fases do S-SDLC
- 2.2.5. Metodologias e normas
- 2.2.6. Referências

2.3. Segurança no ciclo de vida do software nas fases de requisitos e conceção
- 2.3.1. Introdução
- 2.3.2. Modelação de ataques
- 2.3.3. Casos de abuso
- 2.3.4. Engenharia de requisitos de segurança
- 2.3.5. Análise de risco. Arquitetónico
- 2.3.6. Padrões de design
- 2.3.7. Referências

2.4. Segurança no ciclo de vida do software nas fases de codificação, provas e operação
- 2.4.1. Introdução
- 2.4.2. Provas de segurança baseadas no risco
- 2.4.3. Revisão de código
- 2.4.4. Teste de penetração
- 2.4.5. Operações de segurança
- 2.4.6. Revisão externa
- 2.4.7. Referências

2.5. Codificação segura aplicações I
- 2.5.1. Introdução
- 2.5.2. Práticas de codificação segura
- 2.5.3. Manipulação e validação de entradas
- 2.5.4. Sobrecarga de memória
- 2.5.5. Referências

2.6. Codificação segura aplicações II
- 2.6.1. Introdução
- 2.6.2. *Integers overflows*, erros de truncagem e problemas com conversões de tipo entre números inteiros
- 2.6.3. Erros e exceções
- 2.6.4. Privacidade e confidencialidade
- 2.6.5. Programas privilegiados
- 2.6.6. Referências

2.7. Segurança no desenvolvimento e na cloud
- 2.7.1. Segurança no desenvolvimento; metodologia e prática
- 2.7.2. Modelos PaaS, IaaS, PaaS e SaaS
- 2.7.3. Segurança na cloud e para serviços na cloud

2.8. Encriptação
- 2.8.1. Fundamentos de criptologia
- 2.8.2. Encriptação simétrica e assimétrica
- 2.8.3. Encriptação em repouso e em trânsito

2.9. Automatização e orquestração de segurança (SOAR)
- 2.9.1. Complexidade do tratamento manual; necessidade de automatizar tarefas
- 2.9.2. Produtos e serviços
- 2.9.3. Arquitetura SOAR

2.10. Segurança no teletrabalho
- 2.10.1. Necessidade e cenários
- 2.10.2. Produtos e serviços
- 2.10.3. Segurança no teletrabalho

Módulo 3. Auditoria de segurança

3.1. Introdução aos sistemas de informação e a sua auditoria
- 3.1.1. Introdução aos sistemas de informação e o papel da auditoria informática
- 3.1.2. Definições de auditoria informática e de controlo interno informático
- 3.1.3. Funções e objetivos da auditoria informática
- 3.1.4. Diferenças entre controlo interno e auditoria informática

3.2. Controlos internos dos sistemas de informação
- 3.2.1. Organograma funcional de um centro de processamento de dados
- 3.2.2. Classificação dos controlos dos sistemas de informação
- 3.2.3. A Regra de Ouro

3.3. O processo e as fases da auditoria de sistemas de informação
- 3.3.1. Avaliação de riscos (EDR) e outras metodologias de auditoria informática
- 3.3.2. Execução de uma auditoria de Sistemas de Informação. Fases de auditoria
- 3.3.3. Competências fundamentais do auditor de Sistemas de Informação

3.4. Auditoria técnica de segurança em sistemas e redes
- 3.4.1. Auditorias técnicas de segurança. Teste de intrusão. Conceitos prévios
- 3.4.2. Auditorias de segurança em sistemas. Ferramentas de apoio
- 3.4.3. Auditorias de segurança em redes. Ferramentas de apoio

3.5. Auditoria técnica da segurança da Internet e dos dispositivos móveis
- 3.5.1. Auditoria da segurança da Internet. Ferramentas de apoio
- 3.5.2. Auditoria de segurança em dispositivos móveis. Ferramentas de apoio
- 3.5.3. Anexo 1. Estrutura de relatório executivo e relatório técnico
- 3.5.4. Anexo 2. Inventário de ferramentas
- 3.5.5. Anexo 3. Metodologias

3.6. Sistema de gestão de segurança da informação
- 3.6.1. Segurança dos SI: propriedades e fatores de influência
- 3.6.2. Riscos empresariais e gestão de riscos: implementação de controlos
- 3.6.3. SG da Segurança da Informação (SGSI): conceito e fatores críticos de sucesso
- 3.6.4. SGSI-Modelo PDCA
- 3.6.5. SGSI ISO-IEC 27001: contexto da organização
- 3.6.6. Anexo 4. Contexto da organização
- 3.6.7. Anexo 5. Liderança
- 3.6.8. Anexo 6. Planificação
- 3.6.9. Anexo 7. Suporte
- 3.6.10. Anexo 8. Operação
- 3.6.11. Anexo 9. Avaliação do desempenho
- 3.6.12. Anexo 10. Melhoria
- 3.6.13. Anexo ao ISO 27001/ISO-IEC 27002: objetivos e controlos
- 3.6.14. Auditoria do SGSI

3.7. Realização da auditoria
- 3.7.1. Procedimentos
- 3.7.2. Técnicas

3.8. Rastreabilidade
- 3.8.1. Metodologias
- 3.8.2. Análise

3.9. Custódia
- 3.9.1. Técnicas
- 3.9.2. Resultados

3.10. Relatórios e apresentação de provas
- 3.10.1. Tipos de relatórios
- 3.10.2. Análises dos dados
- 3.10.3. Apresentação das provas

Módulo 4. Segurança em aplicações online

4.1. Vulnerabilidades e problemas de segurança nas aplicações online
- 4.1.1. Introdução à segurança nas aplicações online
- 4.1.2. Vulnerabilidades de segurança na conceção das aplicações web
- 4.1.3. Vulnerabilidades de segurança na implementação das aplicações web
- 4.1.4. Vulnerabilidades de segurança na implantação de aplicações Web
- 4.1.5. Listas oficiais de vulnerabilidades de segurança

4.2. Políticas e normas para a segurança das aplicações online
- 4.2.1. Pilares para a segurança das aplicações online
- 4.2.2. Políticas de segurança
- 4.2.3. Sistema de gestão de segurança da informação
- 4.2.4. Ciclo de vida do desenvolvimento seguro de Software
- 4.2.5. Padrões para a segurança das aplicações

4.3. Segurança na conceção das aplicações web
- 4.3.1. Introdução à segurança das aplicações web
- 4.3.2. Segurança na conceção das aplicações web

4.4. Teste da segurança e proteção online das aplicações web
- 4.4.1. Análise e teste da segurança das aplicações web
- 4.4.2. Segurança na implantação e produção das aplicações web

4.5. Segurança dos serviços web
- 4.5.1. Introdução à segurança dos serviços web
- 4.5.2. Funções e tecnologias da segurança dos serviços web

4.6. Teste da segurança e proteção online dos serviços web
- 4.6.1. Avaliação da segurança dos serviços web
- 4.6.2. Proteção online. *Firewalls e gateways* XML

4.7. *Hacking* ético, *malware e forensic*
- 4.7.1. *Hacking* ético
- 4.7.2. Análise de *Malware*
- 4.7.3. Análise forense

4.8. Resolução de incidentes para serviços web
- 4.8.1. Monitorização
- 4.8.2. Ferramentas de medição de desempenho
- 4.8.3. Medidas de contenção
- 4.8.4. Análise da causa-raíz
- 4.8.5. Gestão proativa de problemas

4.9. Boas práticas para garantir a segurança nas aplicações
- 4.9.1. Manual de boas práticas no desenvolvimento das aplicações online
- 4.9.2. Manual de boas práticas na implementação das aplicações online

4.10. Erros comuns que prejudicam a segurança das aplicações
- 4.10.1. Erros comuns no desenvolvimento
- 4.10.2. Erros comuns na hospedagem
- 4.10.3. Erros comuns na produção

Uma capacitação abrangente e multidisciplinar que lhe permitirá destacar-se na sua carreira, seguindo os últimos avanços no campo da Gestão e Auditoria de Segurança do Software"

05

Metodologia

Este programa de capacitação oferece uma forma diferente de aprendizagem. A nossa metodologia é desenvolvida através de um modo de aprendizagem cíclico: ***o Relearning***. Este sistema de ensino é utilizado, por exemplo, nas escolas médicas mais prestigiadas do mundo e tem sido considerado um dos mais eficazes pelas principais publicações, tais como a ***New England Journal of Medicine.***

Descubra o Relearning, um sistema que abandona a aprendizagem linear convencional para o levar através de sistemas de ensino cíclicos: uma forma de aprendizagem que provou ser extremamente eficaz, especialmente em disciplinas que requerem memorização"

Estudo de Caso para contextualizar todo o conteúdo

O nosso programa oferece um método revolucionário de desenvolvimento de competências e conhecimentos. O nosso objetivo é reforçar as competências num contexto de mudança, competitivo e altamente exigente.

Com a TECH pode experimentar uma forma de aprendizagem que abala as fundações das universidades tradicionais de todo o mundo"

Terá acesso a um sistema de aprendizagem baseado na repetição, com ensino natural e progressivo ao longo de todo o programa de estudos.

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

Um método de aprendizagem inovador e diferente

Este programa da TECH é um programa de ensino intensivo, criado de raiz, que propõe os desafios e decisões mais exigentes neste campo, tanto a nível nacional como internacional. Graças a esta metodologia, o crescimento pessoal e profissional é impulsionado, dando um passo decisivo para o sucesso. O método do caso, a técnica que constitui a base deste conteúdo, assegura que a realidade económica, social e profissional mais atual é seguida.

> *"O nosso programa prepara-o para enfrentar novos desafios em ambientes incertos e alcançar o sucesso na sua carreira"*

O método do caso tem sido o sistema de aprendizagem mais amplamente utilizado nas principais escolas de informática do mundo desde que existem. Desenvolvido em 1912 para que os estudantes de direito não só aprendessem o direito com base no conteúdo teórico, o método do caso consistia em apresentar-lhes situações verdadeiramente complexas, a fim de tomarem decisões informadas e valorizarem juízos sobre a forma de as resolver. Em 1924 foi estabelecido como um método de ensino padrão em Harvard.

Numa dada situação, o que deve fazer um profissional? Esta é a questão que enfrentamos no método do caso, um método de aprendizagem orientado para a ação. Ao longo do programa, os estudantes serão confrontados com múltiplos casos da vida real. Terão de integrar todo o seu conhecimento, investigar, argumentar e defender as suas ideias e decisões.

Relearning Methodology

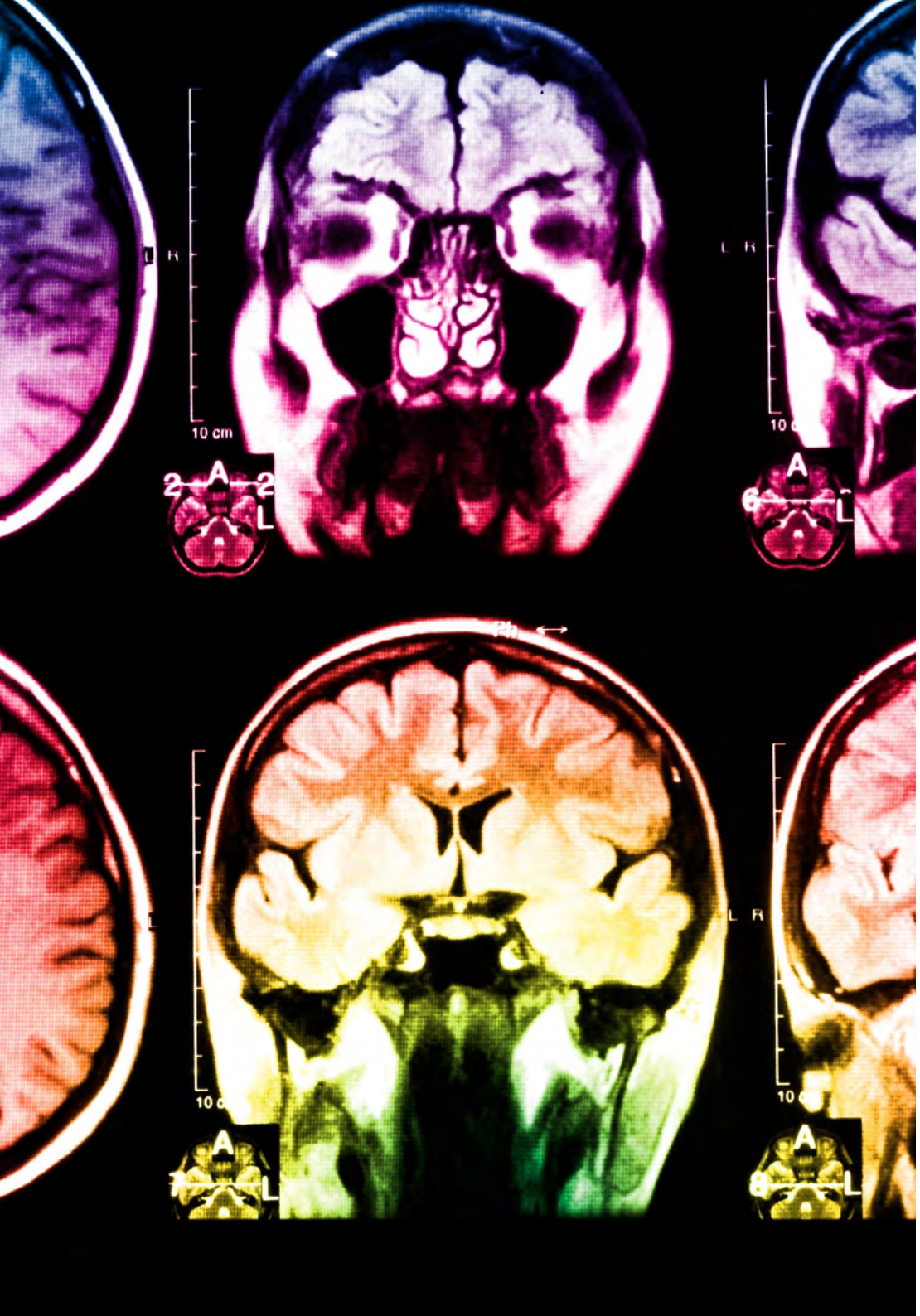
A TECH combina eficazmente a metodologia do Estudo de Caso com um sistema de aprendizagem 100% online baseado na repetição, que combina elementos didáticos diferentes em cada lição.

Melhoramos o Estudo de Caso com o melhor método de ensino 100% online: o Relearning.

Em 2019 obtivemos os melhores resultados de aprendizagem de todas as universidades online do mundo.

Na TECH aprende- com uma metodologia de vanguarda concebida para formar os gestores do futuro. Este método, na vanguarda da pedagogia mundial, chama-se Relearning.

A nossa universidade é a única universidade de língua espanhola licenciada para utilizar este método de sucesso. Em 2019, conseguimos melhorar os níveis globais de satisfação dos nossos estudantes (qualidade de ensino, qualidade dos materiais, estrutura dos cursos, objetivos...) no que diz respeito aos indicadores da melhor universidade online do mundo.



No nosso programa, a aprendizagem não é um processo linear, mas acontece numa espiral (aprender, desaprender, esquecer e reaprender). Portanto, cada um destes elementos é combinado de forma concêntrica. Esta metodologia formou mais de 650.000 licenciados com sucesso sem precedentes em áreas tão diversas como a bioquímica, genética, cirurgia, direito internacional, capacidades de gestão, ciência do desporto, filosofia, direito, engenharia, jornalismo, história, mercados e instrumentos financeiros. Tudo isto num ambiente altamente exigente, com um corpo estudantil universitário com um elevado perfil socioeconómico e uma idade média de 43,5 anos.

O Relearning permitir-lhe-á aprender com menos esforço e mais desempenho, envolvendo-o mais na sua capacitação, desenvolvendo um espírito crítico, defendendo argumentos e opiniões contrastantes: uma equação direta ao sucesso.

A partir das últimas provas científicas no campo da neurociência, não só sabemos como organizar informação, ideias, imagens e memórias, mas sabemos que o lugar e o contexto em que aprendemos algo é fundamental para a nossa capacidade de o recordar e armazenar no hipocampo, para o reter na nossa memória a longo prazo.

Desta forma, e no que se chama Neurocognitive context-dependent e-learning, os diferentes elementos do nosso programa estão ligados ao contexto em que o participante desenvolve a sua prática profissional.

Este programa oferece o melhor material educativo, cuidadosamente preparado para profissionais:

Material de estudo

Todos os conteúdos didáticos são criados pelos especialistas que irão ensinar o curso, especificamente para o curso, para que o desenvolvimento didático seja realmente específico e concreto.

Estes conteúdos são depois aplicados ao formato audiovisual, para criar o método de trabalho online da TECH. Tudo isto, com as mais recentes técnicas que oferecem peças de alta-qualidade em cada um dos materiais que são colocados à disposição do aluno.

Masterclasses

Existem provas científicas sobre a utilidade da observação por terceiros especializada.

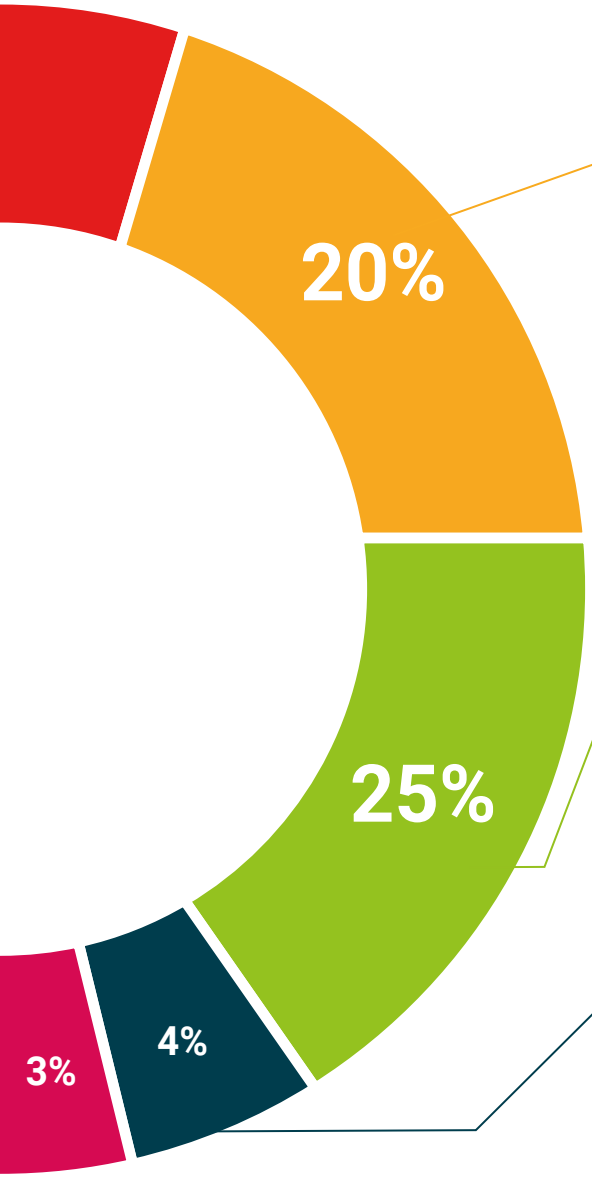
O denominado Learning from an Expert constrói conhecimento e memória, e gera confiança em futuras decisões difíceis.

Práticas de aptidões e competências

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

Leituras complementares

Artigos recentes, documentos de consenso e diretrizes internacionais, entre outros. Na biblioteca virtual da TECH o aluno terá acesso a tudo o que necessita para completar a sua capacitação.



Case studies

Completarão uma seleção dos melhores estudos de casos escolhidos especificamente para esta situação. Casos apresentados, analisados e instruídos pelos melhores especialistas na cena internacional.

Resumos interativos

A equipa da TECH apresenta os conteúdos de uma forma atrativa e dinâmica em comprimidos multimédia que incluem áudios, vídeos, imagens, diagramas e mapas concetuais a fim de reforçar o conhecimento.

Este sistema educativo único para a apresentação de conteúdos multimédia foi premiado pela Microsoft como uma "História de Sucesso Europeu".

Testing & Retesting

Os conhecimentos do aluno são periodicamente avaliados e reavaliados ao longo de todo o programa, através de atividades e exercícios de avaliação e auto-avaliação, para que o aluno possa verificar como está a atingir os seus objetivos.

06

Certificação

O Curso de Especialização em Segurança na Engenharia de Software garante, para além de um conteúdo mais rigoroso e atualizado, o acesso a um 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 na Engenharia de Software** 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 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 na Engenharia de Software**

ECTS**: 24**

Carga horária: **600 horas**

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 na Engenharia de Software

Este é um certificado atribuído por esta Universidade, reconhecido por 24 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 EDUCATION providenciará a obtenção do mesmo com um custo adicional.

tech universidade tecnológica

Curso de Especialização

Segurança na Engenharia de Software

- Modalidade: **online**
- Duração: **6 meses**
- Certificação: **TECH Universidade Tecnológica**
- Qualificação: **24 ECTS**
- Carga horária: **16horas/semana**
- Horário: **ao seu ritmo**
- Exames: **online**

Curso de Especialização

Segurança na Engenharia de Software

tech universidade tecnológica