Programa Avançado
Segurança Informática para Comunicações

tech universidade tecnológica

tech universidade tecnológica

Programa Avançado
Segurança Informática para Comunicações

- Modalidade: **online**
- Duração: **6 meses**
- Certificado: **TECH Universidade Tecnológica**
- Horário: **no seu próprio ritmo**
- Provas: **online**

Acesso ao site: www.techtitute.com/br/informatica/programa-avancado/programa-avancado-seguranca-informatica-comunicacoes

Índice

01

Apresentação

O uso não autorizado e indevido de redes é um dos principais problemas que os usuários podem enfrentar. A realização de ações de segurança informática é fundamental, pois uma grande quantidade de informações privadas e confidenciais circula pela internet. Este Programa Avançado permite um maior conhecimento da área de segurança informática para as comunicações, através de um plano de estudos atualizado e de alta qualidade. Trata-se de uma capacitação abrangente que visa preparar o aluno para o sucesso em sua profissão.

Se você está à procura de uma capacitação de qualidade para especializar-se em uma das áreas com mais oportunidades profissionais, esta é a sua melhor opção"

Os avanços nas telecomunicações são constantes, uma vez que esta é uma das áreas de maior evolução. Por isso, é necessário contar com especialistas em informática que se adaptem a estas mudanças e tenham conhecimento das novas ferramentas e técnicas que estão surgindo neste campo.

A segurança informática deverá ser um dos aspectos mais importantes para as empresas, uma vez que toda sua informação está em rede, e o acesso descontrolado por um usuário para realizar tarefas ilegais poderá representar uma séria ameaça para a companhia, seja em termos financeiros ou de imagem.

O Programa Avançado de Segurança Informática para Comunicações abordará todos os aspectos relacionados a esta área. Este plano de estudos apresenta uma clara vantagem em relação aos demais programas que se concentram em módulos específicos, impossibilitando o aluno de conhecer as interrelações com outras áreas presentes no âmbito multidisciplinar das telecomunicações. A equipe de professores deste programa selecionou cuidadosamente cada um dos temas desta capacitação, oferecendo ao aluno uma oportunidade de estudo completa e conectada aos temas atuais.

Este programa é destinado aos interessados em alcançar um nível mais elevado de conhecimento em Segurança Informática para Comunicações. O principal objetivo deste Programa Avançado é capacitar o aluno para aplicar os conhecimentos adquiridos em situações reais, reproduzindo as condições que poderá enfrentar futuramente, de uma maneira rigorosa e realista.

Além disso, por ser um Programa Avançado 100% online, o aluno não estará condicionado por horários fixos ou pela necessidade de deslocar-se para um local físico, podendo acessar o conteúdo a qualquer momento do dia, equilibrando seu trabalho ou vida pessoal com sua vida acadêmica.

Este **Programa Avançado de Segurança Informática para Comunicações** conta com o conteúdo mais completo e atualizado do mercado.. Suas principais características são:

- O desenvolvimento de casos práticos apresentados por especialistas em Segurança Informática
- Seu conteúdo gráfico, esquemático e eminentemente prático, fornece informações científicas e práticas sobre as disciplinas fundamentais para a prática profissional
- Exercícios práticos onde o processo de autoavaliação pode ser usado para melhorar a aprendizagem
- Destaque especial para as metodologias inovadoras em Segurança Informática para Comunicações
- Lições teóricas, perguntas aos especialistas, fóruns de discussão sobre temas controversos e trabalhos individuais de reflexão
- Disponibilidade de acesso a todo o conteúdo desde qualquer dispositivo fixo ou portátil com conexão à internet

Aproveite a chance de realizar este Programa Avançado de Segurança Informática para Comunicações com a TECH! Esta é a oportunidade perfeita para impulsionar sua carreira”

Este Programa Avançado representa o melhor investimento na seleção de um programa de atualização dos seus conhecimentos em Segurança Informática para Comunicações"

O corpo docente inclui profissionais da área de informática nas telecomunicações, que trazem a experiência do seu trabalho para esta capacitação, assim como conceituados especialistas de empresas líderes e universidades de prestígio.

Através do seu conteúdo multimídia, desenvolvido com a mais recente tecnologia educacional, o profissional poderá ter uma aprendizagem situada e contextual, ou seja, em um ambiente simulado que proporcionará uma capacitação imersiva planejada para praticar diante de situações reais.

A proposta deste programa enfatiza a Aprendizagem Baseada em Problemas, onde o profissional deverá resolver as diferentes situações da prática profissional que surgirem ao longo do curso. Para isso, o profissional contará com a ajuda de um sistema inovador de vídeo interativo desenvolvido por especialistas em Segurança Informática para Comunicações

Esta capacitação possui o melhor material didático que lhe permitirá realizar um estudo contextual, facilitando a sua aprendizagem.

Este Programa Avançado 100% online lhe permitirá conciliar seus estudos com o seu trabalho. Você escolhe onde e quando realizará sua capacitação.

02

Objetivos

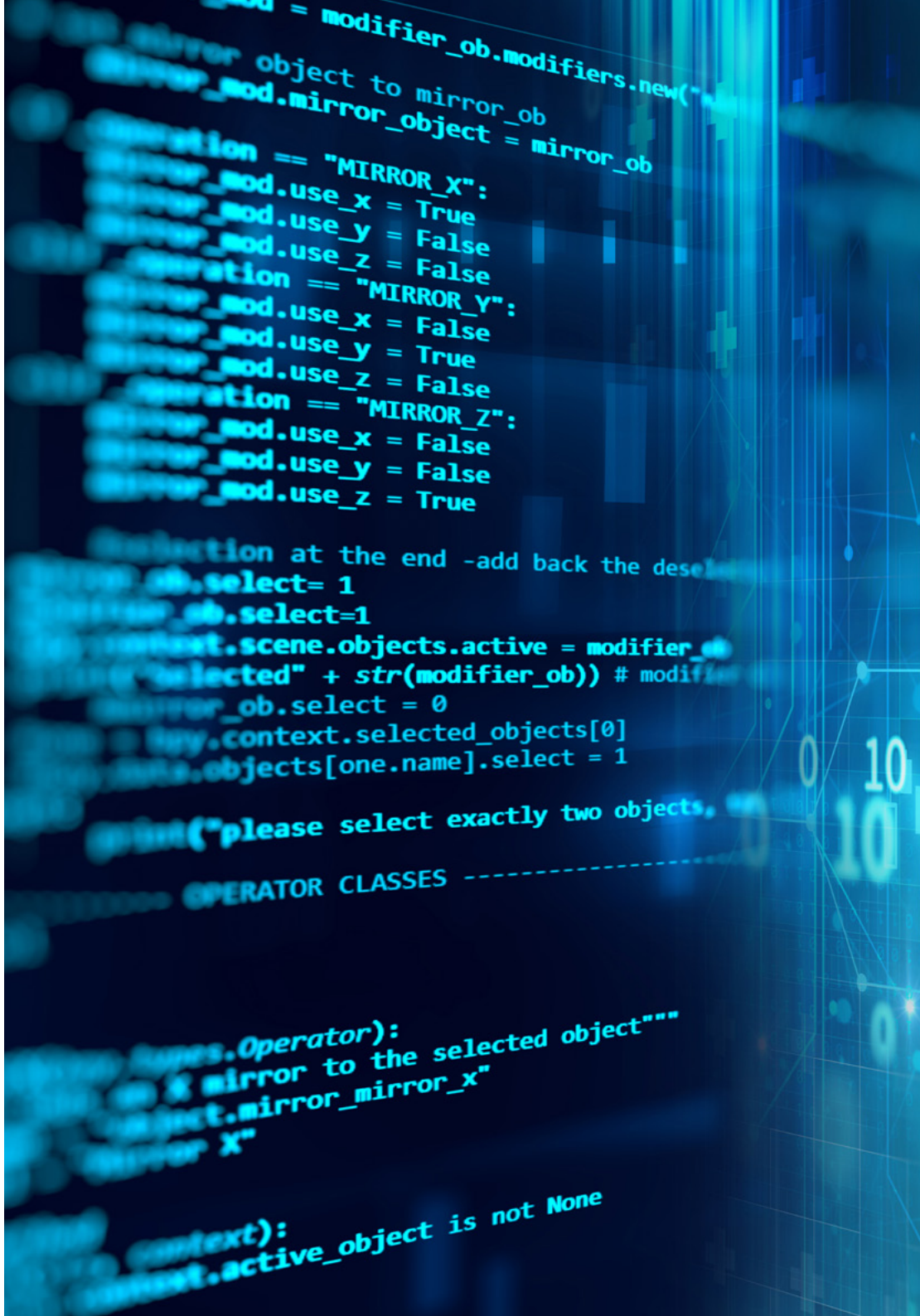
O Programa Avançado de Segurança Informática para Comunicações visa facilitar o desempenho dos profissionais desta área, proporcionando as informações sobre os principais avanços neste setor.

Nosso objetivo é que você se torne o melhor profissional em sua área. Para isso, temos a melhor metodologia e conteúdo"

Objetivo geral

- Capacitar o aluno para atuar com total segurança e qualidade na área de segurança informática para comunicações

Capacite-se na maior universidade online privada do mundo”



Objetivos Específicos

Módulo 1. Segurança em Sistemas e Redes de Comunicação

- Conhecer e aplicar os fundamentos da programação em redes, sistemas e serviços de telecomunicação
- Dominar as normas e regulamentos de protocolos e redes de organismos internacionais de normalização
- Compreender os conceitos de criptografia simétrica e assimétrica, assinatura digital, funções hash e securitização de cada nível de uma arquitetura de comunicação
- Compreender os diferentes mecanismos e protocolos de segurança baseados no controle de acesso: autenticação e defesa do perímetro
- Conhecer 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 nas redes e serviços de telecomunicações os sistemas de gestão de rede e serviços para a configuração, operação, supervisão e tarifação dos mesmos
- Gerenciar a segurança das redes e serviços de telecomunicações implementando túneis, firewalls, protocolos de criptografia e autenticação, e mecanismos de proteção de conteúdo
- Compreender e aplicar as principais técnicas de programação segura

Módulo 2. Arquiteturas de Segurança

- Compreender os princípios básicos da segurança informática
- Dominar os padrões de segurança informática e os processos de certificação
- Analisar os fundamentos organizacionais e criptográficos sobre os quais se baseiam as tecnologias de segurança
- Identificar as principais ameaças e vulnerabilidades dos diferentes elementos envolvidos nas TICs, assim como suas causas
- Conhecer detalhadamente as ferramentas para a segurança da rede e suas funções específicas
- Saber aplicar as tecnologias que compõem uma arquitetura de segurança das TIC, em suas diferentes perspectivas

Módulo 3. Auditoria de Sistemas de Informação

- Dominar os principais conceitos, normas e metodologias de auditoria de sistemas
- Conhecer os elementos organizacionais e a estrutura legal das auditorias
- Obter um guia de referência para o projeto de novos sistemas de controle interno de TI
- Compreender e identificar os riscos associados ao desenvolvimento tecnológico
- Detectar de que forma os diferentes sistemas de informação cumprem ou não com os requisitos de segurança desejados
- Realizar um processo de melhoria contínua de cibersegurança

03

Estrutura e conteúdo

Este conteúdo foi desenvolvido pelos melhores profissionais da área de engenharia de telecomunicações, com ampla experiência e reconhecido prestígio na profissão.

Contamos com o conteúdo mais completo e atualizado do mercado. Buscamos a excelência e queremos que você também possa alcançá-la"

Módulo 1. Segurança em Sistemas e Redes de Comunicação

1.1. Uma perspectiva global sobre segurança, criptografia e análises de criptografia clássica
- 1.1.1. Segurança informática: uma perspectiva histórica
- 1.1.2. Mas o que exatamente se entende por segurança?
- 1.1.3. História da criptografia
- 1.1.4. Criptores substitutos
- 1.1.5. Estudo de caso: a máquina Enigma

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

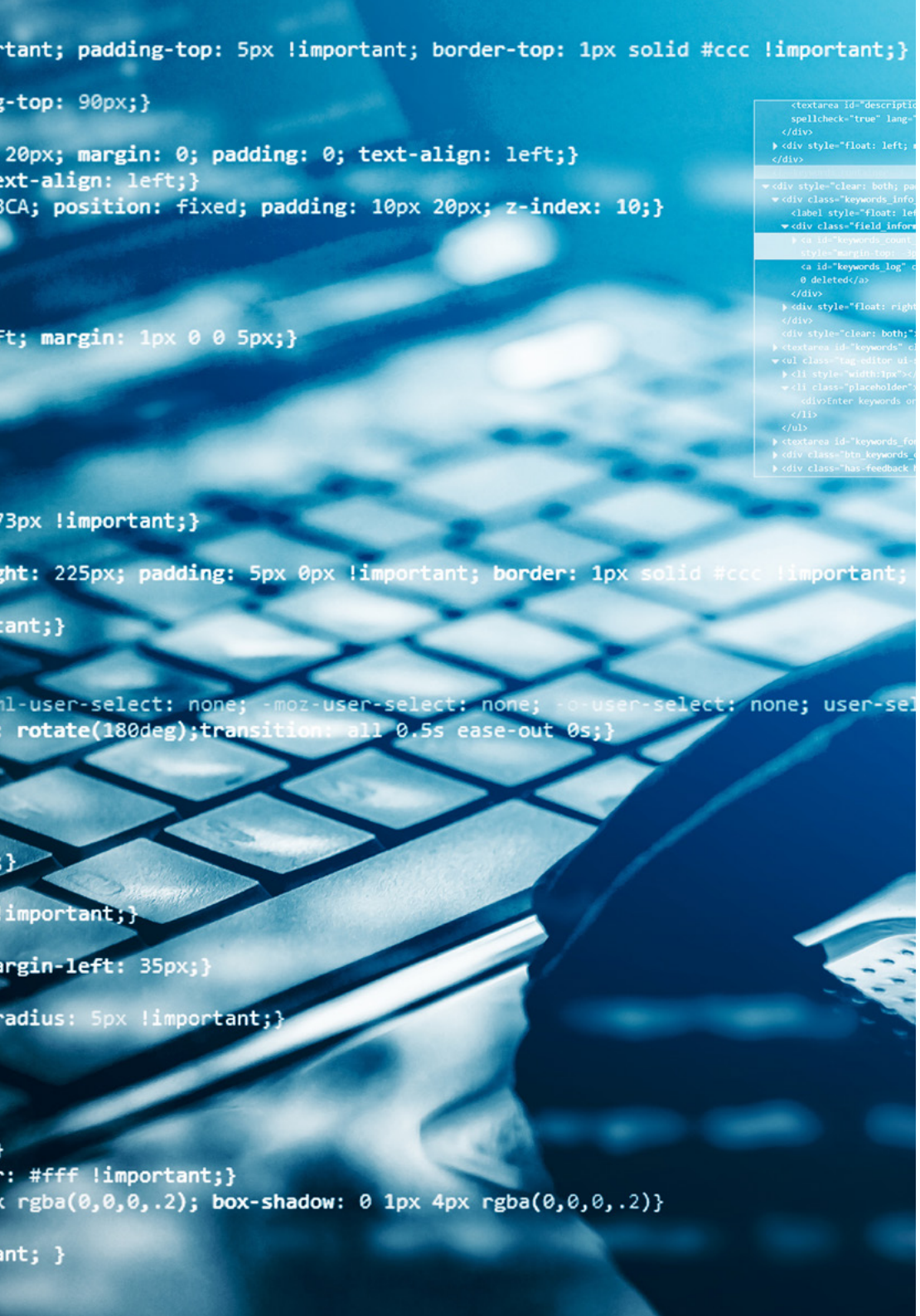
1.3. Criptografia assimétrica
- 1.3.1. Origens da criptografia de chave pública
- 1.3.2. Conceitos básicos e funcionamento
- 1.3.3. O algoritmo da RSA
- 1.3.4. Certificados digitais
- 1.3.5. Armazenamento e gerenciamento de chaves

1.4. Ataques de rede
- 1.4.1. Ameaças e ataques de rede
- 1.4.2. Enumeração
- 1.4.3. Intercepção de 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 tradicionais de segurança
- 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 controles
- 1.6.3. Monitoramento
- 1.6.4. Sistemas de detecção de Intrusão
- 1.6.5. IDS de host
- 1.6.6. Rede IDS
- 1.6.7. IDS baseado em assinatura
- 1.6.8. Sistemas de engodo
- 1.6.9. Princípios básicos de segurança no desenvolvimento de códigos
- 1.6.10. Gerenciamento de falhas
- 1.6.11. Inimigo Público Número 1: Estouros de búfer
- 1.6.12. Botões criptográficos

1.7. Botnets e spam
- 1.7.1. Origem do problema
- 1.7.2. Processo Spam
- 1.7.3. Envio de spam
- 1.7.4. Refinamento das listas de correio
- 1.7.5. Técnicas de proteção
- 1.7.6. Serviço Antispam oferecido por terceiros
- 1.7.7. Estudos de caso
- 1.7.8. Spam exótico



1.8. Auditoria e ataques na Web
- 1.8.1. Coleta de informações
- 1.8.2. Técnicas de ataque
- 1.8.3. Ferramentas

1.9. Malware e códigos maliciosos
- 1.9.1. O que é um *Malware*?
- 1.9.2. Tipos de *Malware*
- 1.9.3. Vírus
- 1.9.4. Criptovírus
- 1.9.5. Minhocas
- 1.9.6. *Adware*
- 1.9.7. *Spyware*
- 1.9.8. *Hoaxes*
- 1.9.9. *Pishing*
- 1.9.10. Troyanos
- 1.9.11. A economia do *malware*
- 1.9.12. Possíveis soluções

1.10. Análise Forense
- 1.10.1. Coleta de provas
- 1.10.2. Análise das evidência
- 1.10.3. Técnicas antiforenses
- 1.10.4. Estudo de caso

Módulo 2. Arquiteturas de Segurança

2.1. Princípios básicos de segurança informática
- 2.1.1. O que significa a 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 da "defesa em segurança"
- 2.1.6. Políticas, planos e procedimentos de segurança
  - 2.1.6.1. Gestão da conta do usuário
  - 2.1.6.2. Identificação e autenticação de usuários
  - 2.1.6.3. Autorização e controle de acesso lógico
  - 2.1.6.4. Monitoramento de servidores
  - 2.1.6.5. Proteção de dados
  - 2.1.6.6. Segurança em conexões remotas
- 2.1.7. A importância do fator humano

2.2. Padronização e certificação em segurança informática
- 2.2.1. Padrões de segurança
  - 2.2.1.1. Propósitos dos padrões
  - 2.2.1.2. Órgãos responsáveis
- 2.2.2. Padrões dos EUA
  - 2.2.2.1. TCSEC
  - 2.2.2.2. Critérios Federais
  - 2.2.2.3. FISCAM
  - 2.2.2.4. NIST SP 800
- 2.2.3. Padrões europeus
  - 2.2.3.1. ITSEC
  - 2.2.3.2. ITSEM
  - 2.2.3.3. Agência Européia de Segurança da Informação e Redes
- 2.2.4. Padrões 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 para a avaliação de vulnerabilidades
- 2.3.3. Ameaças da segurança informática
  - 2.3.3.1. Classificação dos invasores nas redes
  - 2.3.3.2. Motivações dos atacantes
  - 2.3.3.3. Etapas de um ataque
  - 2.3.3.4. Tipos de ataques
- 2.3.4. Vírus de computador
  - 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 das guerras informáticas
- 2.4.3. Consequências de falhas e ataques às empresas
- 2.4.4. A espionagem em redes de computadores

2.5. Identificação de usuários e sistemas biométricos
- 2.5.1. Introdução à autenticação, autorização e registro de usuários
- 2.5.2. Modelo de segurança AAA
- 2.5.3. Controle de acesso
- 2.5.4. Identificação de usuários
- 2.5.5. Verificação de senhas

2.5.6. Autenticação com certificados digitais
2.5.7. Identificação remota de usuários
2.5.8. Inicío de sessão individual
2.5.9. Gestores de senhas
2.5.10. Sistemas biométricos
2.5.10.1. Características gerais
2.5.10.2. Tipos de sistemas biométricos
2.5.10.3. Implantação dos sistemas
2.6. Fundamentos de 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 eletrônica
2.6.6.1. O que é uma assinatura eletrônica?
2.6.6.2. Características da assinatura eletrônica
2.6.6.3. Autoridades de certificação
2.6.6.4. Certificados digitais
2.6.6.5. Sistemas confiáveis baseados em terceiros
2.6.6.6. Utilização da assinatura eletrônica
2.6.6.7. Identificação eletrônica
2.6.6.8. Fatura eletrônica
2.7. Ferramentas para a segurança em redes
2.7.1. O problema da segurança da conexão à internet
2.7.2. A segurança na rede externa
2.7.3. O papel dos servidores Proxy
2.7.4. O papel dos firewalls
2.7.5. Servidores de autenticação para conexões remotas
2.7.6. A análise dos registros de atividades
2.7.7. Sistemas de detecção de intrusos
2.7.8. As iscas
2.8. Segurança de redes privadas virtuais e sem fio
2.8.1. Segurança em redes privadas virtuais
O papel das VPNs
Protocolos para VPNs
2.8.2. Segurança tradicional em redes sem fio
2.8.3. Possíveis ataques a redes sem fio
2.8.4. O protocolo WEP
2.8.5. Padrões para segurança de redes sem fio
2.8.6. Recomendações para reforçar a segurança
2.9. Segurança no uso dos serviços de internet
2.9.1. Navegação segura na web
2.9.1.1. O serviço www
2.9.1.2. Problemas de segurança em www
2.9.1.3. Recomendações de segurança
2.9.1.4. Proteção da privacidade na internet
2.9.2. Segurança do e-mail
2.9.2.1. Características do e-mail
2.9.2.2. Problemas de segurança no e-mail
2.9.2.3. Recomendações de segurança no e-mail
2.9.2.4. Serviços de e-mail avançados
2.9.2.5. Uso do e-mail pelos funcionários
2.9.3. O SPAM
2.9.4. O *phising*
2.10. Controle de conteúdos
2.10.1. A distribuição de conteúdos pela internet
2.10.2. Medidas legais para combater o conteúdo ilícito
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. Normas de boas práticas
- 3.1.1. Introdução
- 3.1.2. Auditoria e COBIT
- 3.1.3. Auditoria de sistemas de gestão das TIC
- 3.1.4. Certificações

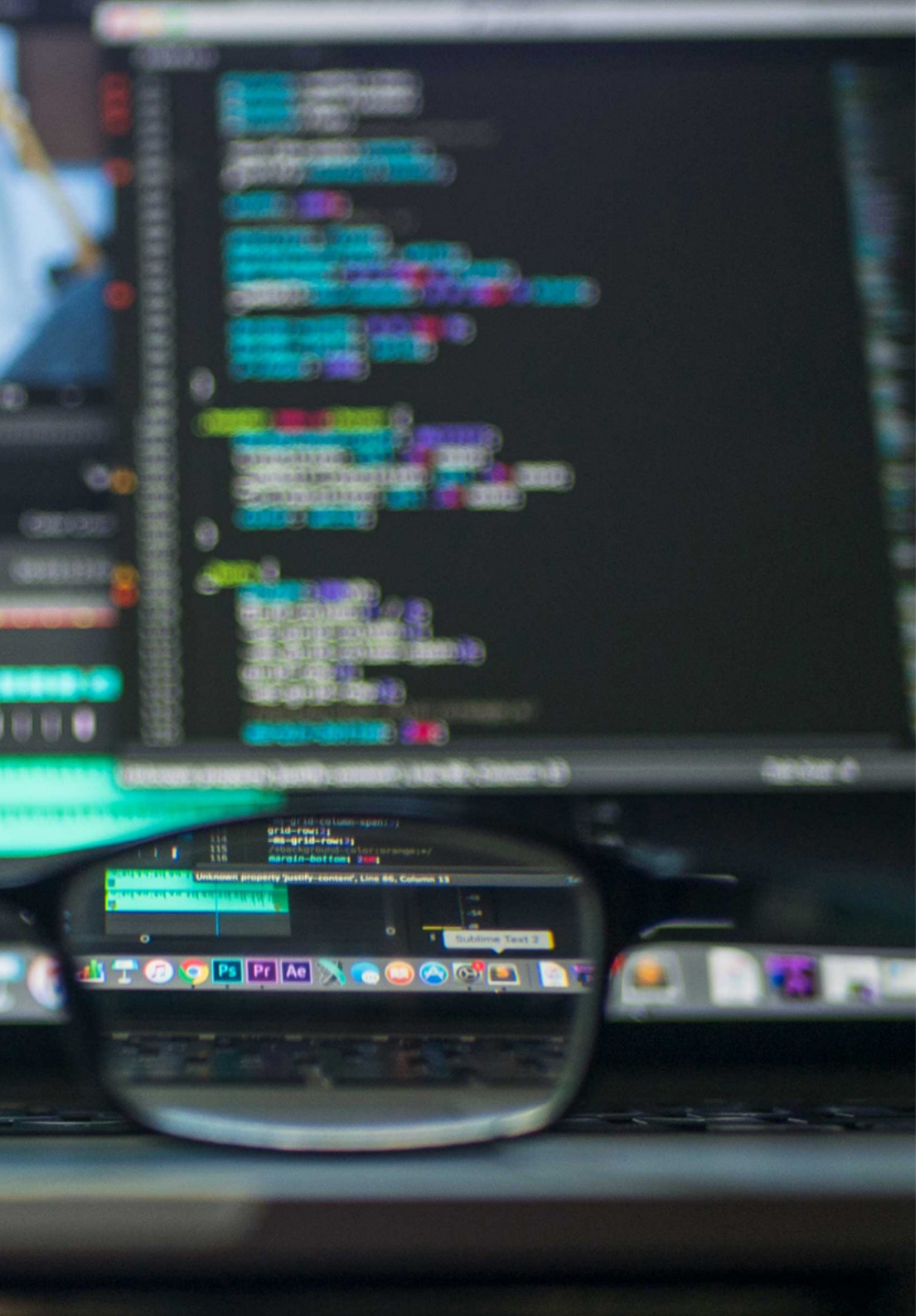
3.2. Conceitos e metodologias de auditoria de sistemas
- 3.2.1. Introdução
- 3.2.2. Metodologias de avaliação de sistemas: quantitativas e qualitativas
- 3.2.3. Metodologias de auditoria informática
- 3.2.4. O plano de auditoria

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. Planejamento das auditorias
- 3.4.4. Metodologia da auditoria de SI

3.5. Estrutura legal para auditorias
- 3.5.1. Proteção de dados pessoais
- 3.5.2. Proteção jurídica do software
- 3.5.3. Delitos tecnológicos
- 3.5.4. Contratação, assinatura e identificação eletrônica

3.6. Auditoria do *Outsourcing* e estruturas de referência
- 3.6.1. Introdução
- 3.6.2. Conceitos básicos do *Outsourcing*
- 3.6.3. Auditoria do *Outsourcing* de TI
- 3.6.4. Estruturas: 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. Planejamento e execução da auditoria de segurança física

3.8. Auditorias de redes e internet
- 3.8.1. Introdução
- 3.8.2. Vulnerabilidades em redes
- 3.8.3. Princípios e direitos na internet
- 3.8.4. Controles e processamento de 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 gestão da área de 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 lhe permitirá avançar em sua carreira de maneira prática e satisfatória"

05

Metodologia

Este curso oferece uma maneira diferente de aprender. Nossa metodologia é desenvolvida através de um modo de aprendizagem cíclico: ***o Relearning***. Este sistema de ensino é utilizado, por exemplo, nas faculdades de medicina mais prestigiadas do mundo e foi considerado um dos mais eficazes pelas principais publicações científicas, como o ***New England Journal of Medicine.***

Descubra o Relearning, um sistema que abandona a aprendizagem linear convencional para realizá-la através de sistemas de ensino cíclicos: uma forma de aprendizagem que se mostrou extremamente eficaz, especialmente em disciplinas que requerem memorização"

Estudo de caso para contextualizar todo o conteúdo

Nosso programa oferece um método revolucionário para desenvolver as habilidades e o conhecimento. Nosso objetivo é fortalecer as competências em um contexto de mudança, competitivo e altamente exigente.

Com a TECH você irá experimentar uma forma de aprender que está revolucionando as bases das universidades tradicionais em todo o mundo"

Você terá acesso a um sistema de aprendizagem baseado na repetição, por meio de um ensino natural e progressivo ao longo de todo o programa.

Através de atividades de colaboração e casos reais, o aluno aprenderá a resolver situações complexas em ambientes reais de negócios.

Um método de aprendizagem inovador e diferente

Este curso da TECH é um programa de ensino intensivo, criado do zero, que propõe os desafios e decisões mais exigentes nesta área, em âmbito nacional ou internacional. Através desta metodologia, o crescimento pessoal e profissional é impulsionado em direção ao sucesso. O método do caso, técnica que constitui a base deste conteúdo, garante que a realidade econômica, social e profissional mais atual seja adotada.

> *Nosso programa prepara você para enfrentar novos desafios em ambientes incertos e alcançar o sucesso na sua carreira"*

O método do caso é o sistema de aprendizagem mais utilizado nas principais escolas de Informática do mundo, desde que elas existem. Desenvolvido em 1912 para que os estudantes de Direito não aprendessem a lei apenas com base no conteúdo teórico, o método do caso consistia em apresentar-lhes situações realmente complexas para que tomassem decisões conscientes e julgassem a melhor forma de resolvê-las. Em 1924 foi estabelecido como o método de ensino padrão em Harvard.

Em uma determinada situação, o que um profissional deveria fazer? Esta é a pergunta que abordamos no método do caso, um método de aprendizagem orientado para a ação. Ao longo do curso, os alunos vão se deparar com múltiplos casos reais. Terão que integrar todo o conhecimento, pesquisar, argumentar e defender suas ideias e decisões.

Metodologia Relearning

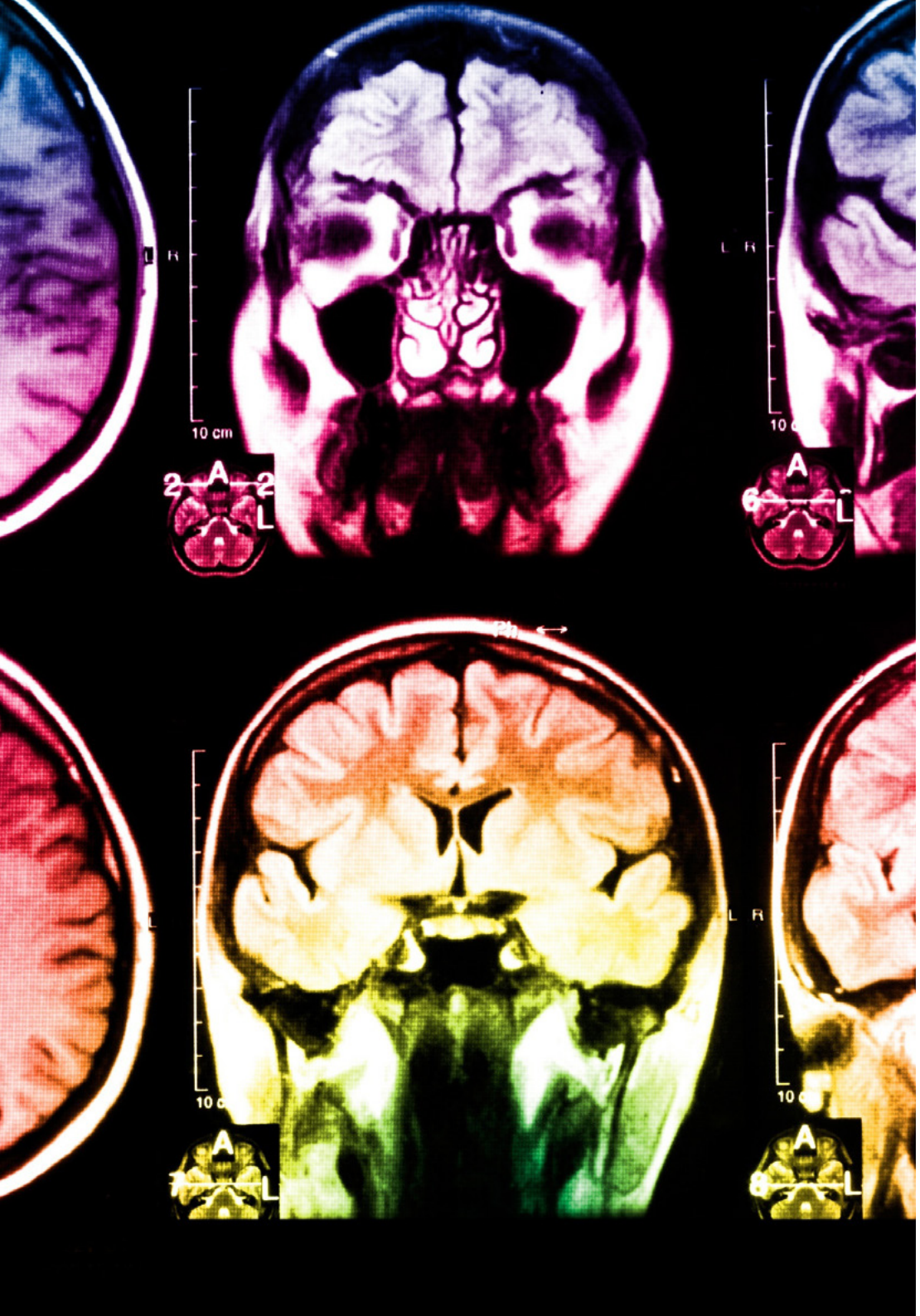
A TECH utiliza de maneira eficaz a metodologia do estudo de caso com um sistema de aprendizagem 100% online, baseado na repetição, combinando elementos didáticos diferentes em cada aula.

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

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

Na TECH você aprenderá através de uma metodologia de vanguarda, desenvolvida para capacitar os profissionais do futuro. Este método, na vanguarda da pedagogia mundial, se chama Relearning.

Nossa universidade é uma das únicas que possui a licença para usar este método de sucesso. Em 2019 conseguimos melhorar os níveis de satisfação geral dos nossos alunos (qualidade de ensino, qualidade dos materiais, estrutura dos curso, objetivos, entre outros) com relação aos indicadores da melhor universidade online.



No nosso programa, a aprendizagem não é um processo linear, ela acontece em espiral (aprender, desaprender, esquecer e reaprender). Portanto, combinamos cada um desses elementos de forma concêntrica. Esta metodologia já capacitou mais de 650 mil universitários com um sucesso sem precedentes em campos tão diversos como a bioquímica, a genética, a cirurgia, o direito internacional, habilidades administrativas, ciência do esporte, filosofia, direito, engenharia, jornalismo, história, mercados e instrumentos financeiros. Tudo isso em um ambiente altamente exigente, com um corpo discente com um perfil socioeconômico médio-alto e uma média de idade de 43,5 anos.

O Relearning permitirá uma aprendizagem com menos esforço e mais desempenho, fazendo com que você se envolva mais em sua especialização, desenvolvendo o espírito crítico e sua capacidade de defender argumentos e contrastar opiniões: uma equação de sucesso.

A partir das últimas evidências científicas no campo da neurociência, sabemos como organizar informações, ideias, imagens, memórias, mas sabemos também que o lugar e o contexto onde aprendemos algo é fundamental para nossa capacidade de lembrá-lo e armazená-lo no hipocampo, para mantê-lo em nossa memória a longo prazo.

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

Neste programa, oferecemos o melhor material educacional, preparado especialmente para os profissionais:

Material de estudo

Todo o conteúdo foi criado especialmente para o curso pelos especialistas que irão ministrá-lo, o que faz com que o desenvolvimento didático seja realmente específico e concreto.

Posteriormente, esse conteúdo é adaptado ao formato audiovisual, para criar o método de trabalho online da TECH. Tudo isso, com as técnicas mais inovadoras que proporcionam alta qualidade em todo o material que é colocado à disposição do aluno.

Masterclasses

Há evidências científicas sobre a utilidade da observação de terceiros especialistas.

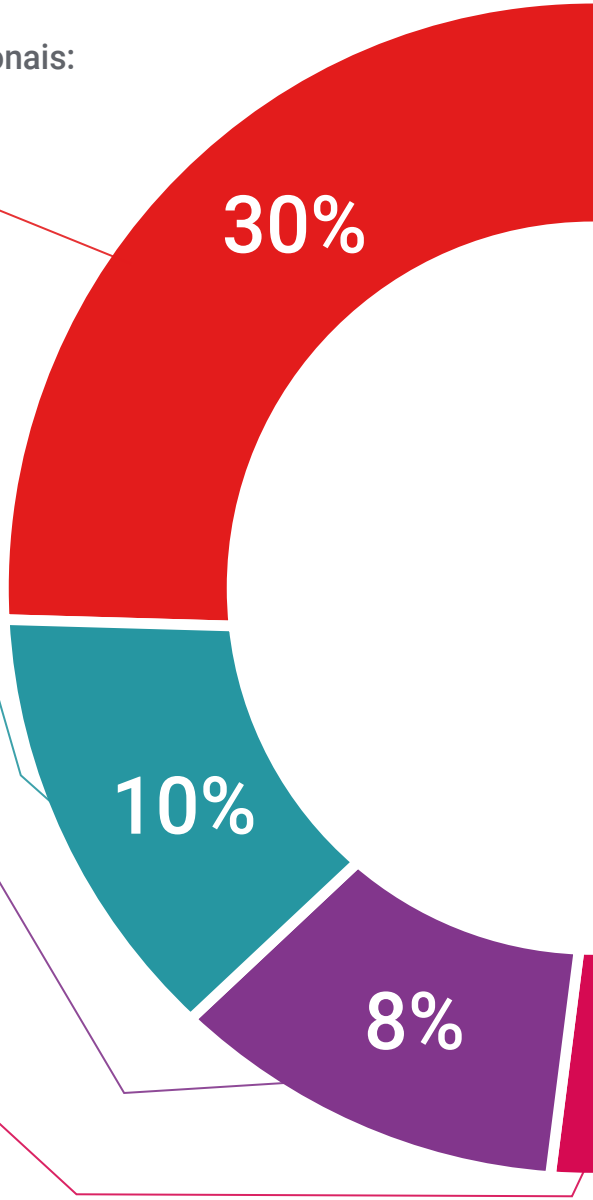
O "Learning from an expert" fortalece o conhecimento e a memória, além de gerar segurança para a tomada de decisões difíceis no futuro.

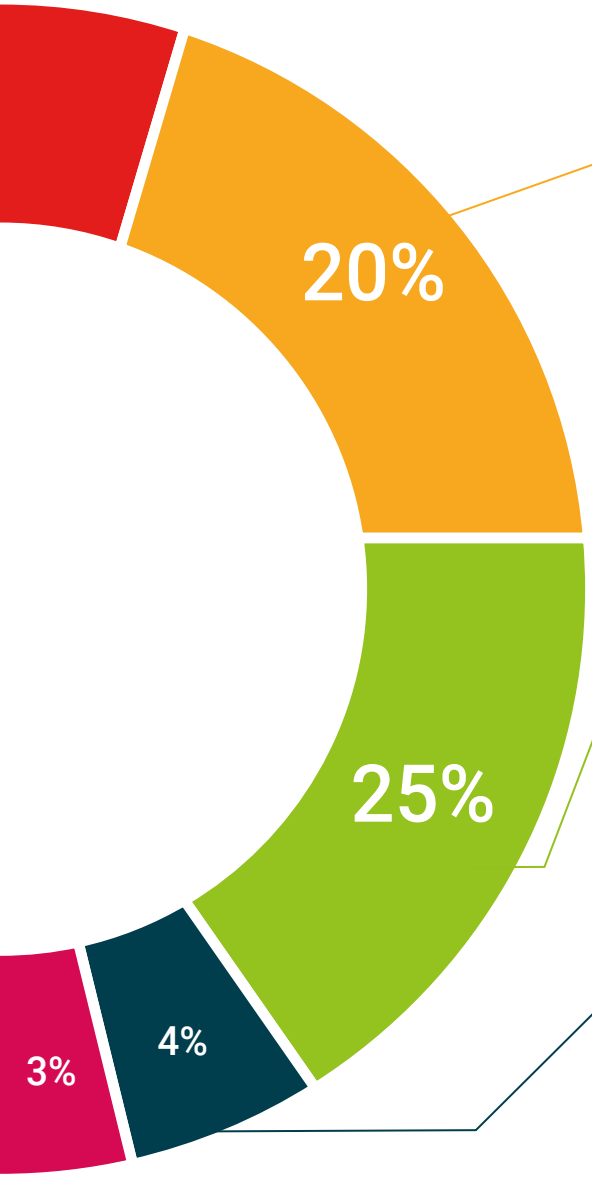
Práticas de habilidades e competências

Serão realizadas atividades para desenvolver competências e habilidades específicas em cada área temática. Práticas e dinâmicas para adquirir e ampliar as competências e habilidades que um especialista precisa desenvolver no contexto globalizado 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 for necessário para complementar a sua capacitação.





Estudos de caso

Os alunos irão completar uma seleção dos melhores estudos de caso escolhidos especialmente para esta capacitação. Casos apresentados, analisados e orientados pelos melhores especialistas do cenário internacional.

Resumos interativos

A equipe da TECH apresenta o conteúdo de forma atraente e dinâmica através de pílulas multimídia que incluem áudios, vídeos, imagens, gráficos e mapas conceituais para consolidar o conhecimento.

Este sistema exclusivo de capacitação por meio da apresentação de conteúdo multimídia foi premiado pela Microsoft como "Caso de sucesso na Europa".

Testing & Retesting

Avaliamos e reavaliamos periodicamente o conhecimento do aluno ao longo do programa, através de atividades e exercícios de avaliação e autoavaliação, para que possa comprovar que está alcançando seus objetivos.

05

Certificado

O Programa Avançado de Segurança Informática para Comunicações garante, além da capacitação mais rigorosa e atualizada, o acesso a um título de Programa Avançado emitido pela TECH Universidade Tecnológica.

Conclua este programa de estudos com sucesso e receba seu certificado sem sair de casa e sem burocracias”

Este **Programa Avançado de Segurança Informática para Comunicações** conta com o conteúdo científico mais completo e atualizado do mercado.

Uma vez aprovadas as avaliações, o aluno receberá por correio o certificado* correspondente ao título de **Programa Avançado** emitido pela **TECH Universidade Tecnológica.**

O certificado emitido pela **TECH Universidade Tecnológica** expressará a qualificação obtida no Programa Avançado, atendendo aos requisitos normalmente exigidos pelas bolsas de empregos, concursos públicos e avaliação de carreira profissional.

Título: **Programa Avançado de Segurança Informática para Comunicações**

Modalidade: **online**

Duração: **6 meses**


tech universidade tecnológica

Outorga o presente

CERTIFICADO

a

Sr./Sra. _____, com documento de identidade nº _____

por ter concluído e aprovado com sucesso o

PROGRAMA AVANÇADO

de

Segurança Informática para Comunicações

Este é um curso próprio desta Universidade, com duração de 450 horas, com data de início dd/mm/aaaa e data final dd/mm/aaaa.

A TECH é uma Instituição Privada de Ensino Superior reconhecida pelo Ministério da Educação Pública em 28 de junho de 2018.

Em 17 de junho de 2020

Ma.Tere Guevara Navarro
Reitora

código único TECH: AFWOR23S techtitute.com/titulos

*Apostila de Haia. Caso o aluno solicite que seu certificado seja apostilado, a TECH EDUCATION providenciará a obtenção do mesmo a um custo adicional.

tech universidade tecnológica

Programa Avançado
Segurança Informática para Comunicações

- Modalidade: **online**
- Duração: **6 meses**
- Certificado: **TECH Universidade Tecnológica**
- Horário: **no seu próprio ritmo**
- Provas: **online**

Programa Avançado

Segurança Informática para Comunicações

tech universidade tecnológica