Mestrado
Telemática

tech global university

tech global university

Mestrado

Telemática

- Modalidade: **online**
- Duração: **12 meses**
- Certificado: **TECH Global University**
- Créditos: **60 ECTS**
- Horário: **no seu próprio ritmo**
- Provas: **online**

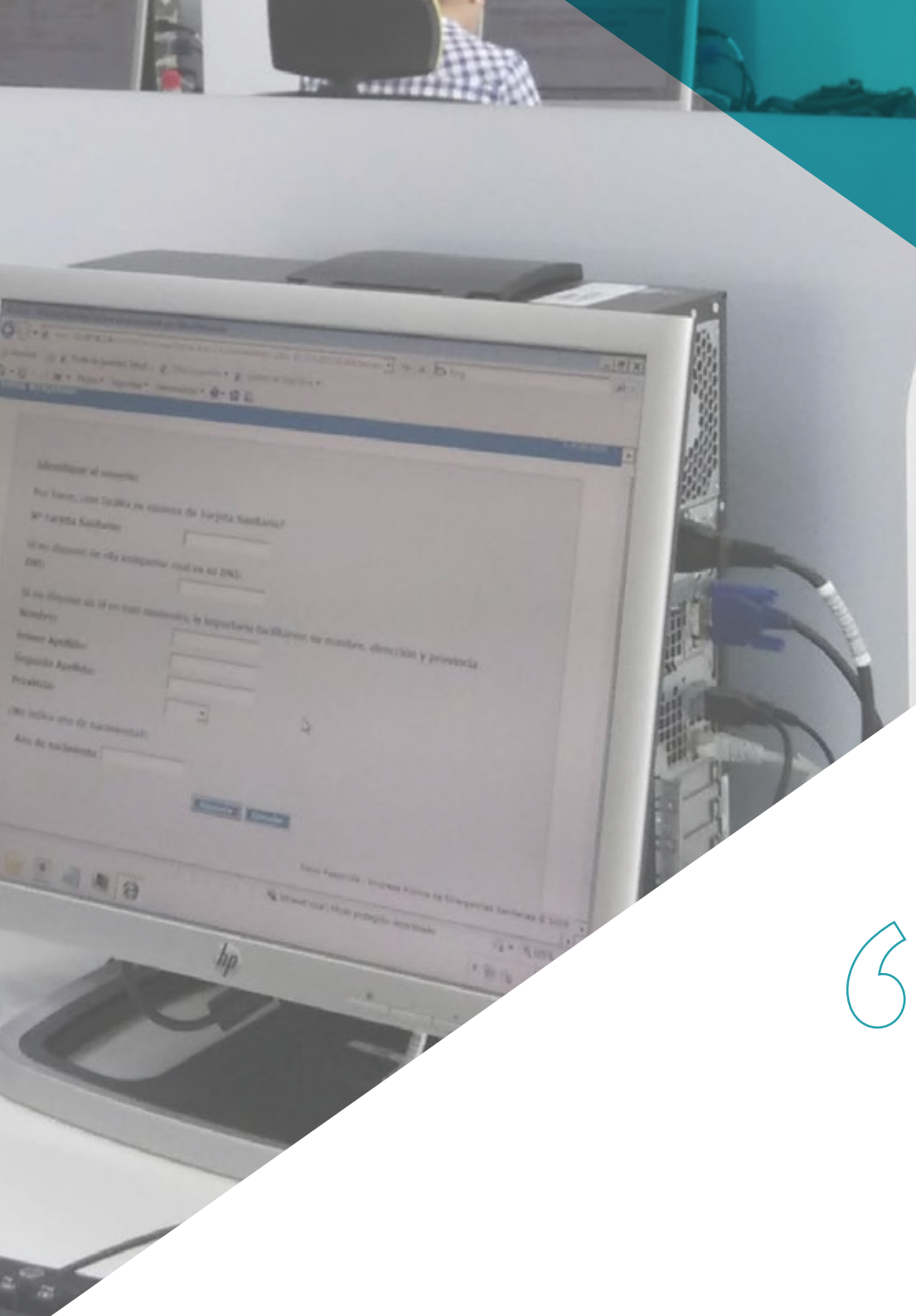
Acesso ao site: www.techtitute.com/br/informatica/mestrado/mestrado-telematica

Índice

01

Apresentação

A informática e a tecnologia da comunicação se combinam na Telemática para responder ao desenvolvimento e implantação de técnicas, processos, conhecimentos e dispositivos que permitam o envio e o recebimento eficientes de dados. Essa área de atuação e a constante incorporação de avanços tecnológicos exigem uma atualização permanente e muito abrangente. Este estudo proporcionará a atualização e capacitação que o profissional requer com um programa altamente qualificado e moderno. Trata-se de uma jornada de elevada qualidade que permitirá ao aluno avançar em sua profissão.



Completo, totalmente atualizado e adaptável à sua disponibilidade, este programa consiste em uma ferramenta de alta qualidade para o cientista da computação que busca ampliar suas competências"

Os avanços nas telecomunicações acontecem constantemente, considerando que esta é uma das áreas que mais cresce. 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.

O Mestrado em Telemática abordará todos os aspectos relacionados com esse campo. 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. Além disso, a equipe de professores deste programa selecionou cuidadosamente cada um dos temas dessa capacitação, oferecendo ao aluno uma oportunidade de estudo completa e conectada aos assuntos atuais.

Esse programa destina-se aos interessados em alcançar um nível mais elevado de conhecimentos em Telemática. O principal objetivo deste programa 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.

Tratando-se de um programa 100% online, o aluno não estará condicionado por horários fixos ou pela necessidade de deslocar-se para um local físico, podendo acessar os conteúdos a qualquer momento do dia, conciliando suas atividades profissionais ou pessoais com a vida acadêmica.

Este **Mestrado em Telemática** conta com o conteúdo mais completo e atualizado do mercado. Suas principais características são:

- O desenvolvimento de casos práticos apresentados por especialistas em Telemática
- O conteúdo gráfico, esquemático e extremamente útil fornece informações científicas e práticas sobre aquelas disciplinas indispensáveis para o exercício da profissão
- Contém exercícios práticos onde o processo de autoavaliação é realizado para melhorar o aprendizado
- Destaque especial para as metodologias inovadoras em Telemática
- Lições teóricas, perguntas aos especialistas, fóruns de discussão sobre temas controversos e trabalhos de reflexão individual
- Disponibilidade de acesso a todo o conteúdo a partir de qualquer dispositivo, fixo ou portátil, com conexão à Internet

Inclua em suas competências a capacidade de atuar nos diferentes campos da telemática, através de uma jornada didática que impulsionará seu crescimento profissional"

Este programa é o melhor investimento que você pode fazer na seleção de uma capacitação para atualizar seus conhecimentos em telemática"

O material didático utilizado para desenvolver seu estudo é um compêndio de alta qualidade que permitirá avançar de forma confortável e prática.

Este programa 100% online lhe permitirá conciliar seus estudos com suas atividades profissionais.

A equipe de professores deste programa inclui profissionais da área da informática de telecomunicações, cuja experiência é somada nesta capacitação, além de reconhecidos especialistas das principais instituições 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 plano de estudos se fundamenta na Aprendizagem Baseada em Problemas, onde o profissional deverá resolver as diferentes situações da prática profissional que surjam ao longo do programa acadêmico. Para isso, o profissional contará com a ajuda de um sistema inovador de vídeo interativo desenvolvido por especialistas em Telemática.

02

Objetivos

O Mestrado em Telemática tem como objetivo oferecer ao profissional de TI um estudo completo e atualizado de todas as áreas relacionadas à intervenção em Telemática, contando com a segurança e a qualidade de um programa elaborado com um critério de total excelência.

O objetivo deste programa consiste em proporcionar ao profissional uma abordagem completa dos conhecimentos teóricos e práticos necessários na área da Telemática"

Objetivo geral

- Capacitar o aluno na elaboração de aplicativos telemáticos, na análise de dados ou na execução de tarefas de segurança digital, entre outros aspectos

Uma oportunidade criada para os profissionais que buscam um curso intensivo e eficaz para avançar de forma significativa em sua profissão"

Objetivos Específicos

Módulo 1. Redes de Computadores

- Adquirir o conhecimento essencial de redes de computadores na Internet
- Compreender o funcionamento das diferentes camadas que definem um sistema em rede, tais como as camadas de aplicação, transporte, rede e ligação
- Compreender a composição das LANs, sua topologia e seus elementos de rede e interconexão
- Aprender o funcionamento do endereçamento IP e da subnetting
- Entender a estrutura das redes sem fio e móveis, incluindo a nova Rede 5G
- Conhecer os diferentes mecanismos de segurança de rede, assim como os diferentes protocolos de segurança da Internet

Módulo 2. Sistemas Distribuídos

- Dominar os princípios básicos dos sistemas distribuídos
- Aprender a caracterizar e classificar os sistemas distribuídos de acordo com uma série de parâmetros básicos
- Compreender os diferentes tipos de modelos utilizados em sistemas distribuídos
- Conhecer as arquiteturas atuais que implementam o conceito de sistemas de arquivos distribuídos
- Analisar os algoritmos de sincronização de processos e objetos, a definição de relógios lógicos e a consistência temporal das informações
- Compreender o sistema de nomes utilizado na internet, conhecido como DNS (System)
- Saber como funciona o endereçamento IP e a *subnetting*

Módulo 3. Segurança em Sistemas e Redes de Comunicação

- Ganhar uma perspectiva global sobre segurança, criptografia e análise clássica de criptografia
- Compreender os fundamentos da criptografia simétrica e da criptografia assimétrica, bem como seus principais algoritmos
- Analisar a natureza dos ataques de rede e os diferentes tipos de arquiteturas de segurança
- Compreender as diferentes técnicas de proteção do sistema e desenvolvimento seguro do código
- Compreender os componentes essenciais de ***botnets*** e spam, assim como malware e código malicioso
- Estabelecer as bases para a análise forense no mundo do software e das auditorias informáticas

Módulo 4. Redes Corporativas e Infraestruturas

- Dominar os aspectos avançados de interconexão de infraestruturas, essenciais no projeto e planejamento de redes de alta velocidade
- Conhecer as principais características e tecnologias de redes de transporte
- Compreender as arquiteturas clássicas de WAN, All-Ethernet, MPLS, VPN
- Analisar os aspectos fundamentais da evolução das redes para NGN (Next Generation Networks)
- Compreender os requisitos avançados de qualidade de serviço, roteamento e controle de congestionamento e confiabilidade
- Conhecer e saber como aplicar as normas internacionais de redes

Módulo 5. 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 6. Data Centers, Operação de Redes e Serviços

- Projetar, operar, gerenciar e manter as redes, serviços e conteúdos proporcionados através de um Data Center
- Conhecer todos os elementos essenciais que compõem um Data Center e as normas e certificações existentes
- Analisar o impacto econômico de uma infraestrutura de Data Center em termos de desempenho e eficiência
- Identificar em infraestruturas reais os elementos hardware de um Data Center
- Compreender as implicações de segurança das diferentes soluções de oferta de serviços por fornecedores de mercado
- Compreender o funcionamento do processo de virtualização
- Conhecer as vantagens, benefícios e modelos de adoção da nuvem (Cloud)

Módulo 7. Programação Avançada

- Aprofundar-se nos conhecimentos de programação, especialmente em relação à programação orientada a objetos, assim como nos diferentes tipos de relações entre as classes existentes
- Conhecer os diferentes padrões de projeto para problemas orientados a objetos
- Aprender sobre programação orientada a eventos e o desenvolvimento de Interfaces de usuário com Qt
- Adquirir os conhecimentos essenciais de programação concorrente, processos e linhas
- Aprender a gestionar o uso de linhas e sincronização, assim como a resolução de problemas comuns dentro da programação concorrente
- Entender a importância da documentação e das provas no desenvolvimento de software

Módulo 8. Engenharia de Sistemas e Serviços de Rede

- Dominar os conceitos fundamentais da engenharia de serviços
- Conhecer os princípios básicos da gestão da configuração de sistemas software em evolução
- Conhecer as tecnologias e ferramentas para a prestação de serviços telemáticos
- Conhecer diferentes estilos arquitetônicos de um sistema de software, compreender suas distinções e saber como escolher o mais adequado de acordo com as exigências do sistema
- Compreender os processos de validação e verificação e suas relações com outras fases do ciclo de vida
- Integrar sistemas de captação, representação, processamento, armazenamento, gestão e apresentação de informações multimídia para a construção de serviços de telecomunicação e aplicações telemáticas
- Conhecer os elementos comuns para o design detalhado de um sistema de software
- Adquirir habilidades de programação, simulação e validação de serviços, bem como em aplicações telemáticas, em rede e distribuídas
- Conhecer o processo e as atividades de transição, configuração, implantação e operação
- Compreender os processos de gestão, automação e otimização de redes

Módulo 9. 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

Módulo 10. Gestão de Projetos

- Conhecer os conceitos fundamentais da gestão de projetos e seu ciclo de vida
- Compreender as diferentes etapas do gerenciamento do projeto, tais como iniciação, planejamento, gerenciamento dos *stakeholders* e definição do escopo
- Aprender o desenvolvimento de cronograma para gerenciamento de tempo, desenvolvimento de orçamento e resposta a riscos
- Compreender o funcionamento da gestão da qualidade em projetos, incluindo planejamento, garantia, controle, conceitos estatísticos e ferramentas disponíveis
- Compreender o funcionamento dos processos de aquisição, execução, monitoramento, controle e encerramento de um projeto
- Adquirir os conhecimentos essenciais relacionados à responsabilidade profissional na gestão de projetos

03

Competências

Ao concluir as avaliações do Mestrado em Telemática, o aluno terá adquirido as competências necessárias para intervir de forma segura e atualizada nos diferentes campos de trabalho desenvolvidos pela Telemática. Trata-se de um processo de crescimento de competências que marcará a diferença em sua carreira profissional.

Adquira as competências de um especialista em telemática e atue nessa área com a visão de um profissional vanguardista"

Competência geral

- Desenvolver aplicativos de telemática e realizar tarefas de segurança digital

Especialize-se com os melhores profissionais e mantenha-se na liderança da intervenção profissional"

Competências específicas

- Conhecer toda a estrutura das redes de computadores
- Dominar os sistemas distribuídos e compreender como classificá-los
- Realizar tarefas de segurança em sistemas e redes de comunicação
- Aplicar os padrões internacionais para redes
- Dominar todos os procedimentos de segurança de TI
- Projetar e administrar data centers
- Realizar programações, identificar problemas e solucioná-los
- Conhecer todo o processo do design de sistemas
- Realizar auditorias em sistemas e melhorar cibersegurança
- Conhecer todas as etapas da gestão de projetos e seu ciclo de vida para saber como gerenciá-las

04

Estrutura e conteúdo

O conteúdo deste programa foi elaborado pelos melhores profissionais do setor de TI de telecomunicações. Trata-se de uma abordagem intensiva e completa que inclui todos os aspectos que o cientista da computação que atua na área da Telemática deverá dominar com desenvoltura, sendo desenvolvida de forma estruturada e eficiente para o aluno.

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

Módulo 1. Redes de Computadores

1.1. Redes de computadores na Internet
- 1.1.1. Redes e a Internet
- 1.1.2. Arquitetura do protocolo

1.2. A camada de aplicação
- 1.2.1. Modelo e protocolos
- 1.2.2. Serviços de FTP e SMTP
- 1.2.3. Serviço DNS
- 1.2.4. Modelo operacional HTTP
- 1.2.5. Formatos de mensagens HTTP
- 1.2.6. Interação com métodos avançados

1.3. A camada de transporte
- 1.3.1. Comunicação entre processos
- 1.3.2. Transporte orientado para a conexão: TCP e SCTP

1.4. A camada de rede
- 1.4.1. Comutação de circuitos e pacotes
- 1.4.2. O protocolo IP (v4 e v6)
- 1.4.3. Algoritmos de roteamento

1.5. A camada de ligação
- 1.5.1. Técnicas de detecção e correção de erros e camada de ligação
- 1.5.2. Links e protocolos de acesso múltiplo
- 1.5.3. Endereço de nível de link

1.6. Redes LAN
- 1.6.1. Topologias de rede
- 1.6.2. Elementos de rede e interconexão

1.7. Endereçamento IP
- 1.7.1. Endereçamento IP e *Subnetting*
- 1.7.2. Visão geral: uma solicitação HTTP

1.8. Redes sem fio e móveis
- 1.8.1. Redes e serviços móveis 2G, 3G e 4G
- 1.8.2. Redes 5G

1.9. Segurança de rede
- 1.9.1. Fundamentos da segurança das comunicações
- 1.9.2. Controle de acesso
- 1.9.3. Segurança do sistema
- 1.9.4. Fundamentos da criptografia
- 1.9.5. Assinatura digital

1.10. Protocolos de segurança na Internet
- 1.10.1. Segurança IP e redes privadas virtuais (VPN)
- 1.10.2. Segurança Web com SSL/TLS

Módulo 2. Sistemas Distribuídos

2.1. Introdução à computação distribuída
- 2.1.1. Conceitos básicos
- 2.1.2. Computação monolítica, distribuída, paralela e cooperativa
- 2.1.3. Vantagens, desvantagens e desafios dos sistemas distribuídos
- 2.1.4. Conceitos prévios sobre sistemas operacionais: processos e simultaneidade
- 2.1.5. Conceitos prévios sobre redes
- 2.1.6. Conceitos prévios sobre a engenharia de software
- 2.1.7. Organização deste manual

2.2. Paradigmas da computação distribuída e comunicação entre processos
- 2.2.1. Comunicação entre processos
- 2.2.2. Sincronização de eventos
  - 2.2.2.1. Cenário 1: envio síncrono e recepção síncrona
  - 2.2.2.2. Cenário 2: envio assíncrono e recepção síncrona
  - 2.2.2.3. Cenário 3: envio síncrono e recepção assíncrona
  - 2.2.2.4. Cenário 4: envio assíncrono e recepção assíncrona
- 2.2.3. Interbloqueios e temporizadores
- 2.2.4. Representação e codificação de dados
- 2.2.5. Classificação e descrição de paradigmas da computação distribuída
- 2.2.6. Java como ambiente de desenvolvimento de sistemas distribuídos

2.3. API de *Sockets*
- 2.3.1. API de soquetes, tipos e diferenças
- 2.3.2. Soquetes do tipo datagrama
- 2.3.3. Soquetes do tipo *Stream*
- 2.3.4. Solução de interbloqueios: temporizadores e eventos sem bloqueios
- 2.3.5. Segurança de *soquetes*

2.4 Paradigma de comunicações cliente-servidor
- 2.4.1. Características e conceitos fundamentais dos sistemas distribuídos do tipo cliente-servidor
- 2.4.2. Processo de design e implementação de um sistema cliente-servidor
- 2.4.3. Problemas de endereçamento sem conexão com clientes anônimos
- 2.4.4. Servidores iterativos e concorrentes
- 2.4.5. Informação do status e da sessão
  - 2.4.5.1. Informações da sessão
  - 2.4.5.2. Informações sobre o status global
- 2.4.6. Clientes complexos recebendo respostas assíncronas do lado do servidor
- 2.4.7. Servidores complexos atuando como intermediários entre vários clientes

2.5. Comunicação de grupo
- 2.5.1. Introdução ao multidifusão e usos comuns
- 2.5.2. Confiabilidade e ordenação em sistemas multidifusão
- 2.5.3. Implementação Java de sistemas multidifusão
- 2.5.4. Exemplo de uso de comunicação em grupo entre iguais
- 2.5.5. Implementações de multidifusão confiável
- 2.5.6. Multitransmissão a nível de aplicação

2.6. Objetos distribuídos
- 2.6.1. Introdução aos objetos distribuídos
- 2.6.2. Arquitetura de uma aplicação baseada em objetos distribuídos
- 2.6.3. Tecnologias de sistemas de objetos distribuídos
- 2.6.4. Camadas de software Java RMI no lado do cliente e no lado do servidor
- 2.6.5. API Java RMI para objetos distribuídos
- 2.6.6. Passos para construir uma aplicação RMI
- 2.6.7. Uso de *Callback* em RMI
- 2.6.8. Download dinâmico de cachês de objetos remotos e gestor de segurança RMI

2.7. Aplicações da Internet I: HTML, XML, HTTP
- 2.7.1. Introdução às aplicações da Internet I
- 2.7.2. Linguagem HTML
- 2.7.3. Linguagem XML
- 2.7.4. Protocolo de Internet HTTP
- 2.7.5. Uso de conteúdo dinâmico: gestão de formulários e CGI
- 2.7.6. Gestão de dados de status e sessão na internet

2.8. CORBA
- 2.8.1. Introdução ao CORBA
- 2.8.2. Arquitetura CORBA
- 2.8.3. Linguagem de descrição da interface em CORBA
- 2.8.4. Protocolos de interoperabilidade GIOP
- 2.8.5. Referências de objetos remotos IOR
- 2.8.6. Serviço de Nomeação CORBA
- 2.8.7. Exemplo em IDL Java
- 2.8.8. Etapas do design, compilação e execução em IDL Java

2.9. Aplicações da Internet II: Applets, Servlets e SOA
- 2.9.1. Introdução às aplicações da Internet II
- 2.9.2. Applets
- 2.9.3. Introdução aos Servlets
- 2.9.4. Servlets HTTP e seu funcionamento
- 2.9.5. Manutenção de informações de estado em Servlets
  - 2.9.5.1. Campos ocultos de formulários
  - 2.9.5.2. *Cookies*
  - 2.9.5.3. Variáveis de Servlet
  - 2.9.5.4. Objeto sessão
- 2.9.6. Serviços Web
- 2.9.7. Protocolo SOAP
- 2.9.8. Breve descrição da arquitetura REST

2.10. Paradigmas avançados
- 2.10.1. Introdução a paradigmas avançados
- 2.10.2. Paradigma MOM
- 2.10.3. Paradigma de agentes software móveis
- 2.10.4. Paradigma do espaço de objetos
- 2.10.5. Computação colaborativa
- 2.10.6. Tendências futuras na computação distribuída

Módulo 3. Segurança em Sistemas e Redes de Comunicação

3.1. Uma perspectiva global sobre segurança, criptografia e análises de criptografia clássica
- 3.1.1. Segurança informática: uma perspectiva histórica
- 3.1.2. Mas o que exatamente se entende por segurança?
- 3.1.3. História da criptografia
- 3.1.4. Criptores substitutos
- 3.1.5. Estudo de caso: a máquina Enigma

3.2. Criptografia simétrica
- 3.2.1. Introdução e terminologia básica
- 3.2.2. Criptografia simétrica
- 3.2.3. Modos de operação
- 3.2.4. DES
- 3.2.5. A nova norma AES
- 3.2.6. Criptografia em fluxo
- 3.2.7. Criptanálise

3.3. Criptografia assimétrica
- 3.3.1. Origens da criptografia de chave pública
- 3.3.2. Conceitos básicos e funcionamento
- 3.3.3. O algoritmo da RSA
- 3.3.4. Certificados digitais
- 3.3.5. Armazenamento e gerenciamento de chaves

3.4. Ataques de rede
- 3.4.1. Ameaças e ataques de rede
- 3.4.2. Enumeração
- 3.4.3. Intercepção de tráfego: *Sniffers*
- 3.4.4. Ataques de negação de serviço
- 3.4.5. Ataques de envenenamento por ARP

3.5. Arquiteturas de segurança
- 3.5.1. Arquiteturas tradicionais de segurança
- 3.5.2. Secure Socket Layer: SSL
- 3.5.3. Protocolo SSH
- 3.5.4. Redes Privadas Virtuais (VPN)
- 3.5.5. Mecanismos de proteção de unidades de armazenamento externas
- 3.5.6. Mecanismos de proteção do hardware

3.6. Técnicas de proteção do sistema e desenvolvimento de código seguro
- 3.6.1. Segurança em operações
- 3.6.2. Recursos e controles
- 3.6.3. Monitoramento
- 3.6.4. Sistemas de detecção de Intrusão
- 3.6.5. IDS de *Host*
- 3.6.6. Rede IDS
- 3.6.7. IDS baseado em assinatura
- 3.6.8. Sistemas de engodo
- 3.6.9. Princípios básicos de segurança no desenvolvimento de códigos
- 3.6.10. Gerenciamento de falhas
- 3.6.11. Inimigo Público Número 1: Estouros de búfer
- 3.6.12. Botões criptográficos

3.7. Botnets e *Spam*
- 3.7.1. Origem do problema
- 3.7.2. Processo Spam
- 3.7.3. Envio de spam
- 3.7.4. Refinamento das listas de correio
- 3.7.5. Técnicas de proteção
- 3.7.6. Serviço *Antispam* oferecido por terceiros
- 3.7.7. Estudos de caso
- 3.7.8. Spam exótico

3.8. Auditoria e ataques na Web
- 3.8.1. Coleta de informações
- 3.8.2. Técnicas de ataque
- 3.8.3. Ferramentas

3.9. Malwares e códigos maliciosos
- 3.9.1. O que é malware?
- 3.9.2. Tipos de malware
- 3.9.3. Vírus
- 3.9.4. Criptovírus
- 3.9.5. Minhocas
- 3.9.6. *Adware*
- 3.9.7. *Spyware*
- 3.9.8. *Hoaxes*
- 3.9.9. *Pishing*
- 3.9.10. Troyanos
- 3.9.11. A economia do malware
- 3.9.12. Possíveis soluções

3.10. Análise Forense
- 3.10.1. Coleta de provas
- 3.10.2. Análise das evidência
- 3.10.3. Técnicas antiforenses
- 3.10.4. Estudo de caso

Módulo 4. Redes Corporativas e Infraestruturas

4.1. Redes de transporte
- 4.1.1. Arquitetura funcional das redes de transporte
- 4.1.2. Interface de nó de rede em SDH
- 4.1.3. Elemento de rede
- 4.1.4. Qualidade e disponibilidade de rede
- 4.1.5. Gestão de redes de transporte
- 4.1.6. Evolução das redes de transporte

4.2. Arquiteturas WAN clássicas
- 4.2.1. Redes de área extensa WAN
- 4.2.2. Normas WAN
- 4.2.3. Encapsulamento WAN
- 4.2.4. Dispositivos WAN
  - 4.2.4.1. Router
  - 4.2.4.2. Modem
  - 4.2.4.3. *Switch*
  - 4.2.4.4. Servidores de comunicação
  - 4.2.4.5. *Gateway*
  - 4.2.4.6. *Firewall*
  - 4.2.4.7. *Proxy*
  - 4.2.4.8. NAT
- 4.2.5. Tipos de conexão
  - 4.2.5.1. Enlaces ponto a ponto
  - 4.2.5.2. Comutação de circuitos
  - 4.2.5.3. Comutação de pacotes
  - 4.2.5.4. Circuitos virtuais WAN

4.3. Redes baseadas em ATM
- 4.3.1. Introdução, características e modelo de camadas
- 4.3.2. Camada física de acesso ATM
  - 4.3.2.1. Subcamada dependente do meio físico PM
  - 4.3.2.2. Subcamada de convergência de transmissão, TC
- 4.3.3. Célula ATM
  - 4.3.3.1. Cabeçalho
  - 4.3.3.2. Conexão virtual
  - 4.3.3.3. Nó de Switching ATM
  - 4.3.3.4. Controle de fluxo (carregamento do enlace)
- 4.3.4. Adaptação de células AAL
  - 4.3.4.1. Tipos de serviços AAL

4.4. Modelos avançados de filas
- 4.4.1. Introdução
- 4.4.2. Fundamentos da teoria de filas
- 4.4.3. Teoria de filas de sistemas básicos
  - 4.4.3.1. Sistemas M/M/1, M/M/m e M/M/∞
  - 4.4.3.2. Sistemas M/M/1/k e M/M/m/m

4.4.4. Teoria de filas de sistemas avançados
4.4.4.1. Sistema M/G/1
4.4.4.2. Sistema M/G/1 com prioridades
4.4.4.3. Redes de filas
4.4.4.4. Modelagem de redes de comunicação
4.5. Qualidade de serviço em redes corporativas
4.5.1. Fundamentos
4.5.2. Fatores de QoS em redes convergentes
4.5.3. Conceitos de QoS
4.5.4. Políticas de QoS
4.5.5. Métodos para implementar a QoS
4.5.6. Modelos de QoS
4.5.7. Mecanismos para a implantação da DiffServ QoS
4.5.8. Exemplos de aplicação
4.6. Redes corporativas e infraestruturas All-Ethernet
4.6.1. Topologias da rede ethernet
4.6.1.1. Topologia em bus
4.6.1.2. Topologia em estrela
4.6.2. Formato de quadro ethernet e IEEE 802.3
4.6.3. Rede ethernet comutada
4.6.3.1. Redes virtuais VLAN
4.6.3.2. Agregação de portas
4.6.3.3. Redundância de conexões
4.6.3.4. Gestão da QoS
4.6.3.5. Funções de segurança
4.6.4. Fast Ethernet
4.6.5. Gigabit Ethernet
4.7. Infraestruturas MPLS
4.7.1. Introdução
4.7.2. MPLS
4.7.2.1. Histórico do MPLS e evolução
4.7.2.2. Arquitetura MPLS
4.7.2.3. Remessa de pacotes etiquetados
4.7.2.4. Protocolo de distribuição de etiquetas (LDP)

4.7.3. VPN MPLS
- 4.7.3.1. Definição de uma VPN
- 4.7.3.2. Modelos de VPN
- 4.7.3.3. Modelo de VPN MPLS
- 4.7.3.4. Arquitetura de VPN MPLS
- 4.7.3.5. *Virtual Routing Forwarding* (VRF)
- 4.7.3.6. RD
- 4.7.3.7. Route Target (RT)
- 4.7.3.8. Propagação de rota VPNv4 em uma VPN MPLS
- 4.7.3.9. Reenvio de pacotes em uma rede VPN MPLS
- 4.7.3.10. BGP
- 4.7.3.11. Comunidade estendida do BGP: RT
- 4.7.3.12. Transporte de etiquetas com BGP
- 4.7.3.13. Route Reflector (RR
- 4.7.3.14. Grupo RR
- 4.7.3.15. Seleção de rotas BGP
- 4.7.3.16. Reenvio de pacotes

4.7.4. Protocolos de *Routing* comuns em ambientes MPLS
- 4.7.4.1. Protocolos de Routing do tipo vetor distância
- 4.7.4.2. Protocolos de Routing de estado de enlace
- 4.7.4.3. OSPF
- 4.7.4.4. ISIS

4.8. Serviços de operadoras e VPN
- 4.8.1. Introdução
- 4.8.2. Requisitos básicos de uma VPN
- 4.8.3. Tipos de VPN
  - 4.8.3.1. VPN de acesso remoto
  - 4.8.3.2. VPN ponto a ponto
  - 4.8.3.3. VPN interna (over LAN)
- 4.8.4. Protocolos utilizados na VPN
- 4.8.5. Implementações e tipos de conexão

4.9. NGN (Next Generation Networks)
- 4.9.1. Introdução
- 4.9.2. Antecedentes
  - 4.9.2.1. Definição e características da rede NGN
  - 4.9.2.2. Migração para redes de nova geração
- 4.9.3. Arquitetura NGN
  - 4.9.3.1. Camada de conectividade primária
  - 4.9.3.2. Camada de acesso
  - 4.9.3.3. Camada de serviço
  - 4.9.3.4. Camada de gestão
- 4.9.4. IMS
- 4.9.5. Organizações de Padronização
- 4.9.6. Tendências regulatórias

4.10. Revisão das normas ITU e IETF
- 4.10.1. Introdução
- 4.10.2. Padronização
- 4.10.3. Algumas organizações padronizadas
- 4.10.4. Protocolos e Padrões de Camadas Físicas WAN
- 4.10.5. Exemplos de protocolos orientados ao meio

Módulo 5. Arquiteturas de Segurança

5.1. Princípios básicos de segurança informática
- 5.1.1. O que significa a segurança informática
- 5.1.2. Objetivos da segurança informática
- 5.1.3. Serviços de segurança informática
- 5.1.4. Consequências da falta de segurança
- 5.1.5. Princípio da defesa em segurança
- 5.1.6. Políticas, planos e procedimentos de segurança
  - 5.1.6.1. Gestão da conta do usuário
  - 5.1.6.2. Identificação e autenticação de usuários
  - 5.1.6.3. Autorização e controle de acesso lógico
  - 5.1.6.4. Monitoramento de servidores
  - 5.1.6.5. Proteção de dados
  - 5.1.6.6. Segurança em conexões remotas
- 5.1.7. A importância do fator humano

5.2. Padronização e certificação em segurança informática
- 5.2.1. Normas de segurança
  - 5.2.1.1. Propósitos dos padrões
  - 5.2.1.2. Órgãos responsáveis
- 5.2.2. Padrões dos EUA
  - 5.2.2.1. TCSEC
  - 5.2.2.2. Critérios Federais
  - 5.2.2.3. FISCAM
  - 5.2.2.4. NIST SP 800
- 5.2.3. Padrões europeus
  - 5.2.3.1. ITSEC
  - 5.2.3.2. ITSEM
  - 5.2.3.3. Agência Europeia de Segurança da Informação e Redes
- 5.2.4. Padrões internacionais
- 5.2.5. Processo de certificação

5.3. Ameaças à segurança informática: vulnerabilidades e Malware
- 5.3.1. Introdução
- 5.3.2. Vulnerabilidades dos sistemas
  - 5.3.2.1. Incidentes de segurança nas redes
  - 5.3.2.2. Causas das vulnerabilidades dos sistemas informáticos
  - 5.3.2.3. Tipos de vulnerabilidades
  - 5.3.2.4. Responsabilidades dos fabricantes de software
  - 5.3.2.5. Ferramentas para a avaliação de vulnerabilidades
- 5.3.3. Ameaças da segurança informática
  - 5.3.3.1. Classificação dos invasores nas redes
  - 5.3.3.2. Motivações dos atacantes
  - 5.3.3.3. Etapas de um ataque
  - 5.3.3.4. Tipos de ataques
- 5.3.4. Vírus de computador
  - 5.3.4.1. Características gerais
  - 5.3.4.2. Tipos de vírus

5.3.4.3. Danos causados por vírus
5.3.4.4. Como combater os vírus
5.4. Ciberterrorismo e resposta a incidentes
5.4.1. Introdução
5.4.2. A ameaça do ciberterrorismo e das guerras informáticas
5.4.3. Consequências de falhas e ataques às empresas
5.4.4. A espionagem em redes de computadores
5.5. Identificação de usuários e sistemas biométricos
5.5.1. Introdução à autenticação, autorização e registro de usuários
5.5.2. Modelo de segurança AAA
5.5.3. Controle de acesso
5.5.4. Identificação de usuários
5.5.5. Verificação de senhas
5.5.6. Autenticação com certificados digitais
5.5.7. Identificação remota de usuários
5.5.8. Início de sessão individual
5.5.9. Gestores de senhas
5.5.10. Sistemas biométricos
5.5.10.1. Características gerais
5.5.10.2. Tipos de sistemas biométricos
5.5.10.3. Implantação dos sistemas
5.6. Fundamentos de criptografia e protocolos criptográficos
5.6.1. Introdução à Criptografia
5.6.1.1. Criptografia, criptoanálise e criptologia
5.6.1.2. Funcionamento de um sistema criptográfico
5.6.1.3. História dos sistemas criptográficos
5.6.2. Criptanálise
5.6.3. Classificação dos sistemas criptográficos
5.6.4. Sistemas criptográficos simétricos e assimétricos
5.6.5. Autenticação com sistemas criptográficos
5.6.6. Assinatura eletrônica
5.6.6.1. O que é uma assinatura eletrônica?
5.6.6.2. Características da assinatura eletrônica
5.6.6.3. Autoridades de certificação
5.6.6.4. Certificados digitais
5.6.6.5. Sistemas confiáveis baseados em terceiros
5.6.6.6. Utilização da assinatura eletrônica
5.6.6.7. Identificação eletrônica
5.6.6.8. Fatura eletrônica
5.7. Ferramentas para a segurança em redes
5.7.1. O problema da segurança da conexão à internet
5.7.2. A segurança na rede externa
5.7.3. O papel dos servidores *Proxy*
5.7.4. O papel dos firewalls
5.7.5. Servidores de autenticação para conexões remotas
5.7.6. A análise dos registros de atividades
5.7.7. Sistemas de detecção de intrusos
5.7.8. As iscas
5.8. Segurança de redes privadas virtuais e sem fio
5.8.1. Segurança em redes privadas virtuais
5.8.1.1 O papel das VPNs
5.8.1.2 Protocolos para VPN
5.8.2. Segurança tradicional em redes sem fio
5.8.3. Possíveis ataques a redes sem fio
5.8.4. O protocolo WEP
5.8.5. Padrões para segurança de redes sem fio
5.8.6. Recomendações para reforçar a segurança
5.9. Segurança no uso dos serviços de internet
5.9.1. Navegação segura na web
5.9.1.1. O serviço www
5.9.1.2. Problemas de segurança em www
5.9.1.3. Recomendações de segurança
5.9.1.4. Proteção da privacidade na internet
5.9.2. Segurança do e-mail
5.9.2.1. Características do e-mail
5.9.2.2. Problemas de segurança no e-mail
5.9.2.3. Recomendações de segurança no e-mail

5.9.2.4. Serviços de e-mail avançados
5.9.2.5. Uso do e-mail pelos funcionários
5.9.3. O SPAM
5.9.4. O *Phising*
5.10. Controle de conteúdos
5.10.1. A distribuição de conteúdos pela internet
5.10.2. Medidas legais para combater o conteúdo ilícito
5.10.3. Filtragem, catalogação e bloqueio de conteúdos
5.10.4. Danos à imagem e à reputação

Módulo 6. Data Centers, Operação de Redes e Serviços

6.1. Data Center: conceitos básicos e componentes
6.1.1. Introdução
6.1.2. Conceitos básicos
6.1.2.1. Definição de um DC
6.1.2.2. Classificação e importância
6.1.2.3. Catástrofes e perdas
6.1.2.4. Tendência evolutiva
6.1.2.5. Custos de complexidade
6.1.2.6. Pilares e camadas de redundância
6.1.3. Filosofia de design
6.1.3.1. Objetivos
6.1.3.2. Seleção do local
6.1.3.3. Disponibilidade
6.1.3.4. Elementos críticos
6.1.3.5. Avaliação e análise de custos
6.1.3.6. Orçamento de TI
6.1.4. Componentes básicos
6.1.4.1. Piso técnico
6.1.4.2. Tipos de blocos
6.1.4.3. Considerações gerais
6.1.4.4. Tamanho do DC
6.1.4.5. *Racks*
6.1.4.6. Servidores e equipamentos de comunicação
6.1.4.7. Monitoramento
6.2. *Data Center*: sistemas de controle
6.2.1. Introdução
6.2.2. Fornecimento de energia
6.2.2.1. Rede elétrica
6.2.2.2. Potência elétrica
6.2.2.3. Estratégias de distribuição de eletricidade
6.2.2.4. UPS
6.2.2.5. Geradores
6.2.2.6. Problemas elétricos
6.2.3. Controle ambiental
6.2.3.1. Temperatura
6.2.3.2. Umidade
6.2.3.3. Ar-condicionado
6.2.3.4. Estimativa calórica
6.2.3.5. Estratégias de refrigeração
6.2.3.6. Design de corredor. Circulação do ar
6.2.3.7. Sensores e manutenção
6.2.4. Segurança e prevenção de incêndios
6.2.4.1. Segurança física
6.2.4.2. O fogo e sua classificação
6.2.4.3. Classificação e tipos de sistemas de extinção
6.3. *Data Centers*: design e organização
6.3.1. Introdução
6.3.2. Design de rede
6.3.2.1. Tipologia
6.3.2.2. Cabeamento estruturado
6.3.2.3. Backbone
6.3.2.4. Cabos de rede UTP e STP
6.3.2.5. Cabos de telefonia
6.3.2.6. Elementos terminais
6.3.2.7. Cabos de fibra ótica
6.3.2.8. Cabo coaxial

6.3.2.9. Transmissão sem fio
6.3.2.10. Recomendações e etiquetagem
6.3.3. Organização
6.3.3.1. Introdução
6.3.3.2. Medidas básicas
6.3.3.3. Estratégias para a gestão de cabos
6.3.3.4. Políticas e procedimentos
6.3.4. Gestão do DC
6.3.5. Padrões no *Data Center*
6.4. *Data Center*: modelos e continuidade de negócios
6.4.1. Introdução
6.4.2. Otimização
6.4.2.1. Técnicas de otimização
6.4.2.2. *Data Centers* ecológicos
6.4.2.3. Desafios atuais
6.4.2.4. *Data Centers* modulares
6.4.2.5. Housing
6.4.2.6. Consolidação de *Data Centers*
6.4.2.7. Monitoramento
6.4.3. Continuidade do negócio
6.4.3.1. BCP. Plano de continuidade de negócios. Pontos-chave
6.4.3.2. DR. Plano de recuperação em caso de desastre
6.4.3.3. Implementação de um DR
6.4.3.4. *Backup* e estratégias
6.4.3.5. *Data Center* de respaldo
6.4.4. Melhores práticas
6.4.4.1. Recomendações
6.4.4.2. Uso da metodologia ITIL
6.4.4.3. Métricas de disponibilidade
6.4.4.4. Controle ambiental
6.4.4.5. Gestão de riscos
6.4.4.6. Responsável do DC
6.4.4.7. Ferramentas
6.4.4.8. Dicas para implantação
6.4.4.9. Caracterização
6.5. *Cloud Computing*: introdução e conceitos básicos
6.5.1. Introdução
6.5.2. Conceitos básicos e terminologia
6.5.3. Objetivos e benefícios
6.5.3.1. Disponibilidade
6.5.3.2. Confiabilidade
6.5.3.3. Escalabilidade
6.5.4. Riscos e desafios
6.5.5. Funções. Provider. Consumer
6.5.6. Características do Cloud
6.5.7. Modelos de prestação de serviços
6.5.7.1. IaaS
6.5.7.2. PaaS
6.5.7.3. SaaS
6.5.8. Tipos de Cloud
6.5.8.1. Pública
6.5.8.2. Privada
6.5.9.3. Híbrida
6.5.9. Tecnologias habilitadoras de Cloud
6.5.9.1. Arquiteturas de redes
6.5.9.2. Redes de banda larga. Interconectividade
6.5.9.3. Tecnologias de Data Center
6.5.9.3.1. *Computing*
6.5.9.3.2. *Storage*
6.5.9.3.3. *Networking*
6.5.9.3.4. Alta disponibilidade
6.5.9.3.5. Sistemas de *Backup*
6.5.9.3.6. Balanceadores

6.5.9.4. Virtualização
6.5.9.5. Tecnologias Web
6.5.9.6. Tecnologia Multitenant
6.5.9.7. Tecnologia de serviços
6.5.9.8. Segurança Cloud
6.5.9.8.1. Condições e conceitos
6.5.9.8.2. Integridade, autenticação
6.5.9.8.3. Mecanismos de segurança
6.5.9.8.4. Ameaças à segurança
6.5.9.8.5. Ataques à segurança Cloud
6.5.9.8.6. Casos práticos

6.6. *Cloud Computing*: tecnologia e segurança na nuvem
6.6.1. Introdução
6.6.2. Mecanismo de Infraestrutura Cloud
6.6.2.1. Perímetro de rede
6.6.2.2. Armazenamento
6.6.2.3. Ambiente de servidores
6.6.2.4. Monitoramento Cloud
6.6.2.5. Alta disponibilidade
6.6.3. Mecanismos de segurança Cloud (parte I)
6.6.3.1. Automatização
6.6.3.2. Balanceadores de carga
6.6.3.3. Monitor de SLA
6.6.3.4. Mecanismos de pagamento por uso
6.6.4. Mecanismos de segurança Cloud (parte II)
6.6.4.1. Sistemas de rastreabilidade e auditoria
6.6.4.2. Sistemas de Failover
6.6.4.3. Hypervisor
6.6.4.4. Clustering
6.6.4.5. Sistemas Multitenant

6.7. *Cloud Computing*: infraestrutura. Mecanismos de controle e segurança
6.7.1. Introdução aos mecanismos de gestão Cloud
6.7.2. Sistemas de administração remota
6.7.3. Sistemas de gestão de recursos

6.7.4. Sistemas de gestão de acordos de nível de serviço
6.7.5. Sistemas de gestão de faturamento
6.7.6. Mecanismo de segurança Cloud
6.7.6.1. Criptografia
6.7.6.2. *Hashing*
6.7.6.3. Assinatura digital
6.7.6.4. PKI
6.7.6.5. Gestão de acessos e identidades
6.7.6.6. SSO
6.7.6.7. Grupos de segurança baseados em Cloud
6.7.6.8. Sistemas bastiões

6.8. *Cloud Computing*: arquiteturas Cloud
6.8.1. Introdução
6.8.2. Arquiteturas Cloud básicas
6.8.2.1. Arquiteturas de distribuição da carga de trabalho
6.8.2.2. Arquiteturas de uso de recursos
6.8.2.3. Arquiteturas Escaláveis
6.8.2.4. Arquiteturas de balanceamento de carga
6.8.2.5. Arquiteturas redundantes
6.8.2.6. Exemplos
6.8.3. Arquiteturas Cloud avançadas
6.8.3.1. Arquiteturas de cluster hipervisor
6.8.3.2. Arquiteturas virtuais de balanceamento de carga
6.8.3.3. Arquiteturas *Non-Stop*
6.8.3.4. Arquiteturas de alta disponibilidade
6.8.3.5. Arquiteturas Baremetal
6.8.3.6. Arquiteturas redundantes
6.8.3.7. Arquiteturas híbridas
6.8.4. Arquiteturas Cloud especializadas
6.8.4.1. Arquiteturas de acesso direto I/O
6.8.4.2. Arquiteturas de acesso direto LUN
6.8.4.3. Arquiteturas de redes elásticas
6.8.4.4. Arquiteturas SDDC

6.8.4.5. Arquiteturas especiais
6.8.4.6. Exemplos
6.9. *Cloud Computing*: modelos de prestação de serviços
6.9.1. Introdução
6.9.2. Prestação de serviços Cloud
6.9.3. Perspectiva do fornecedor de serviços
6.9.4. Perspectiva do consumidor destes serviços
6.9.5. Estudos de caso
6.10. *Cloud Computing*: modelos de contratação, métricas e fornecedores de serviços
6.10.1. Introdução aos modelos e métricas de faturamento
6.10.2. Modelos de faturamento
6.10.3. Métricas de pagamento por uso
6.10.4. Considerações sobre a gestão de custos
6.10.5. Introdução à métrica de qualidade de serviço e SLA
6.10.6. Métricas da qualidade do serviço
6.10.7. Métricas do desempenho do serviço
6.10.8. Métricas da escalabilidade do serviço
6.10.9. SLA do modelo de serviço
6.10.10. Estudos de caso

Módulo 7. Programação Avançada

7.1. Introdução à programação orientada a objetos
7.1.1. Introdução à programação orientada a objetos
7.1.2. Projeto de classes
7.1.3. Introdução à UML para modelagem de problemas
7.2. Relações entre classes
7.2.1. Abstração e herança
7.2.2. Conceitos avançados de herança
7.2.3. Polimorfismo
7.2.4. Composição e agregação
7.3. Introdução aos padrões de projeto para problemas orientados a objetos
7.3.1. O que são padrões de projeto?
7.3.2. Padrão Factory
7.3.3. Padrão Singleton
7.3.4. Padrão Observer
7.3.5. Padrão Composite
7.4. Exceções
7.4.1. O que são as exceções?
7.4.2. Captura e gestão de exceções
7.4.3. Lançamento de exceções
7.4.4. Criação de exceções
7.5. Interfaces de usuário
7.5.1. Introdução ao Qt
7.5.2. Posicionamento
7.5.3. O que são os eventos?
7.5.4. Eventos: definição e captura
7.5.5. Desenvolvimento de interfaces de usuário
7.6. Introdução à programação concorrente
7.6.1. Introdução à programação concorrente
7.6.2. O conceito de processo e linha
7.6.3. Interação entre processos ou linhas
7.6.4. As linhas em C++
7.6.5. Vantagens e desvantagens da programação concorrente
7.7. Gestão de linhas e sincronização
7.7.1. Ciclo de vida de uma linha
7.7.2. A classe Thread
7.7.3. Planejamento de linhas
7.7.4. Grupos de linhas
7.7.5. Linhas de tipo daemon
7.7.6. Sincronização
7.7.7. Mecanismos de bloqueio
7.7.8. Mecanismos de comunicação
7.7.9. Monitores
7.8. Problemas comuns dentro da programação concorrente
7.8.1. O problema dos produtores-consumidores

7.8.2. O problema dos leitores e escritores
7.8.3. O problema do jantar dos filósofos
7.9. Documentação e testes de software
7.9.1. Por que é importante documentar o software?
7.9.2. Documentação de projeto
7.9.3. Uso de ferramentas para documentação
7.10. Provas de software
7.10.1. Introdução às provas de software
7.10.2. Tipos de provas
7.10.3. Prova de unidade
7.10.4. Teste de integração
7.10.5. Prova de validação
7.10.6. Prova de sistema

Módulo 8. Engenharia de Sistemas e Serviços de Rede

8.1. Introdução à Engenharia de Sistemas e Serviços de Rede
8.1.1. Conceito de sistema informático e engenharia da computação
8.1.2. O software e suas características
8.1.2.1. Características do software
8.1.3. A evolução do software
8.1.3.1. O início do desenvolvimento de software
8.1.3.2. A crise do software
8.1.3.3. A Engenharia de Software
8.1.3.4. A tragédia do software
8.1.3.5. Novidades em software
8.1.4. Os mitos sobre software
8.1.5. Os novos desafios do software
8.1.6. Deontologia profissional em engenharia de software
8.1.7. SWEBOK. O conjunto de conhecimentos da engenharia de software
8.2. O processo de desenvolvimento
8.2.1. Processo de resolução de problemas
8.2.2. O processo de desenvolvimento de software
8.2.3. Processo de software vs. ciclo de vida
8.2.4. Ciclo de vida. Modelos de processo (tradicionais)
8.2.4.1. Modelo em cascata
8.2.4.2. Modelos baseados em prototipagem
8.2.4.3. Modelo de desenvolvimento incremental
8.2.4.4. Desenvolvimento rápido de aplicações (RAD)
8.2.4.5. Modelo em espiral
8.2.4.6. Processo unificado de desenvolvimento ou processo racional unificado (RUP)
8.2.4.7. Desenvolvimento de software baseado em componentes
8.2.5. O manifesto ágil. Os métodos ágeis
8.2.5.1. Extreme Programming (XP)
8.2.5.2. Scrum
8.2.5.3. Feature Driven Development (FDD)
8.2.6. Padrões do processo de software
8.2.7. Definição de um processo de software
8.2.8. Maturidade do processo de software
8.3. Planejamento e gestão de projetos ágeis
8.3.1. O que é Ágil?
8.3.1.1. História Ágil
8.3.1.2. Manifesto Ágil
8.3.2. Fundamentos ágeis
8.3.2.1. A mentalidade ágil
8.3.2.2. Adaptação ao Ágil
8.3.2.3. Ciclo de vida do desenvolvimento de produtos
8.3.2.4. O Triângulo de Ferro
8.3.2.5. Trabalhar com incerteza e volatilidade
8.3.2.6. Processos definidos e processos empíricos
8.3.2.7. Os mitos ágeis
8.3.3. O ambiente ágil
8.3.3.1. Modelo operacional
8.3.3.2. Funções ágeis

8.3.3.3. Técnicas ágeis
8.3.3.4. Práticas ágeis
8.3.4. Estruturas ágeis
8.3.4.1. e-Xtreme Programming (XP)
8.3.4.2. Scrum
8.3.4.3. Dynamic Systems Development Method (DSDM)
8.3.4.4. Agile Project Management
8.3.4.5. Kanban
8.3.4.6. Lean software Development
8.3.4.7. Lean Start-up
8.3.4.8. Scaled Agile Framework (SAFe)
8.4. Gestão de configuração e repositórios colaborativos
8.4.1. Conceitos básicos de gestão de configuração de software
8.4.1.1. O que é a gestão da configuração do software?
8.4.1.2. Configuração do software e elementos da configuração do software
8.4.1.3. Linhas de base
8.4.1.4. Versões, revisões, variantes e *releases*
8.4.2. Atividades de gestão da configuração
8.4.2.1. Identificação da configuração
8.4.2.2. Controle de mudança de configuração
8.4.2.3. Geração de relatórios de status
8.4.2.4. Auditoria da configuração
8.4.3. O plano de gestão da configuração
8.4.4. Ferramentas de gestão da configuração
8.4.5. A gestão da configuração na metodologia Métrica v.3
8.4.6. A gestão da configuração no SWEBOK
8.5. Teste de sistemas e serviços
8.5.1. Conceitos gerais das provas
8.5.1.1. Verificar e validar
8.5.1.2. Definição de prova
8.5.1.3. Princípios das provas
8.5.2. Abordagem das provas

8.5.2.1. Prova de caixa branca
8.5.2.2. Teste da caixa preta
8.5.3. Provas estáticas ou revisões
8.5.3.1. Revisões técnicas formais
8.5.3.2. *Walkthroughs*
8.5.3.3. Inspeções de código
8.5.4. Provas dinâmicas
8.5.4.1. Provas de unidade ou unitárias
8.5.4.2. Teste de integração
8.5.4.3. Provas de sistema
8.5.4.4. Provas de aceitação
8.5.4.5. Provas de regressão
8.5.5. Provas alfa e beta
8.5.6. O processo das provas
8.5.7. Erro, defeito e falha
8.5.8. Ferramentas de prova automática
8.5.8.1. Junit
8.5.8.2. LoadRunner
8.6. Modelagem e design de arquiteturas de rede
8.6.1. Introdução
8.6.2. Características dos sistemas
8.6.2.1. Descrição de cada sistema
8.6.2.2. Descrição e características dos serviços
8.6.2.3. Requisitos de operabilidade
8.6.3. Análise de requisitos
8.6.3.1. Requisitos do usuário
8.6.3.2. Requisitos de aplicações
8.6.3.3. Requisitos de rede
8.6.4. Design de arquiteturas de rede
8.6.4.1. Arquitetura de referência e componentes

8.6.4.2. Modelos de arquitetura
8.6.4.3. Arquiteturas de sistema e rede
8.7. Modelagem e design de sistemas distribuídos
8.7.1. Introdução
8.7.2. Arquitetura de endereçamento e *roteamento*
8.7.2.1. Estratégia de endereçamento
8.7.2.2. Estratégia de roteamento
8.7.2.3. Considerações do design
8.7.3. Conceitos de design de redes
8.7.4. Processos de design
8.8. Plataformas e ambientes de implantação
8.8.1. Introdução
8.8.2. Sistemas de computadores distribuídos
8.8.2.1. Conceitos básicos
8.8.2.2. Modelos de computação
8.8.2.3. Vantagens, desvantagens e desafios
8.8.2.4. Conceitos básicos do sistema operacional
8.8.3. Implantação de redes virtualizadas
8.8.3.1. A necessidade de uma mudança
8.8.3.2. Transformação das redes: de "tudo-IP" para a nuvem
8.8.3.3. Implantação de redes em cloud
8.8.4. Exemplo: arquitetura de rede em Azure
8.9. Benefícios E2E: atraso e largura de banda. QoS
8.9.1. Introdução
8.9.2. Análise de desempenho
8.9.3. QoS
8.9.4. Priorização e gestão do tráfego
8.9.5. Acordos de nível de serviço
8.9.6. Considerações do design
8.9.6.1. Avaliação de desempenho
8.9.6.2. Relações e interações
8.10. Automação e otimização da rede
8.10.1. Introdução
8.10.2. Gestão de rede
8.10.2.1. Protocolos de gestão e configuração
8.10.2.2. Arquiteturas de gestão de rede
8.10.3. Orquestração e automação
8.10.3.1. Arquitetura ONAP
8.10.3.2. Controladores e funções
8.10.3.3. Políticas
8.10.3.4. Inventário da rede
8.10.4. Otimização

Módulo 9. Auditoria de Sistemas de Informação

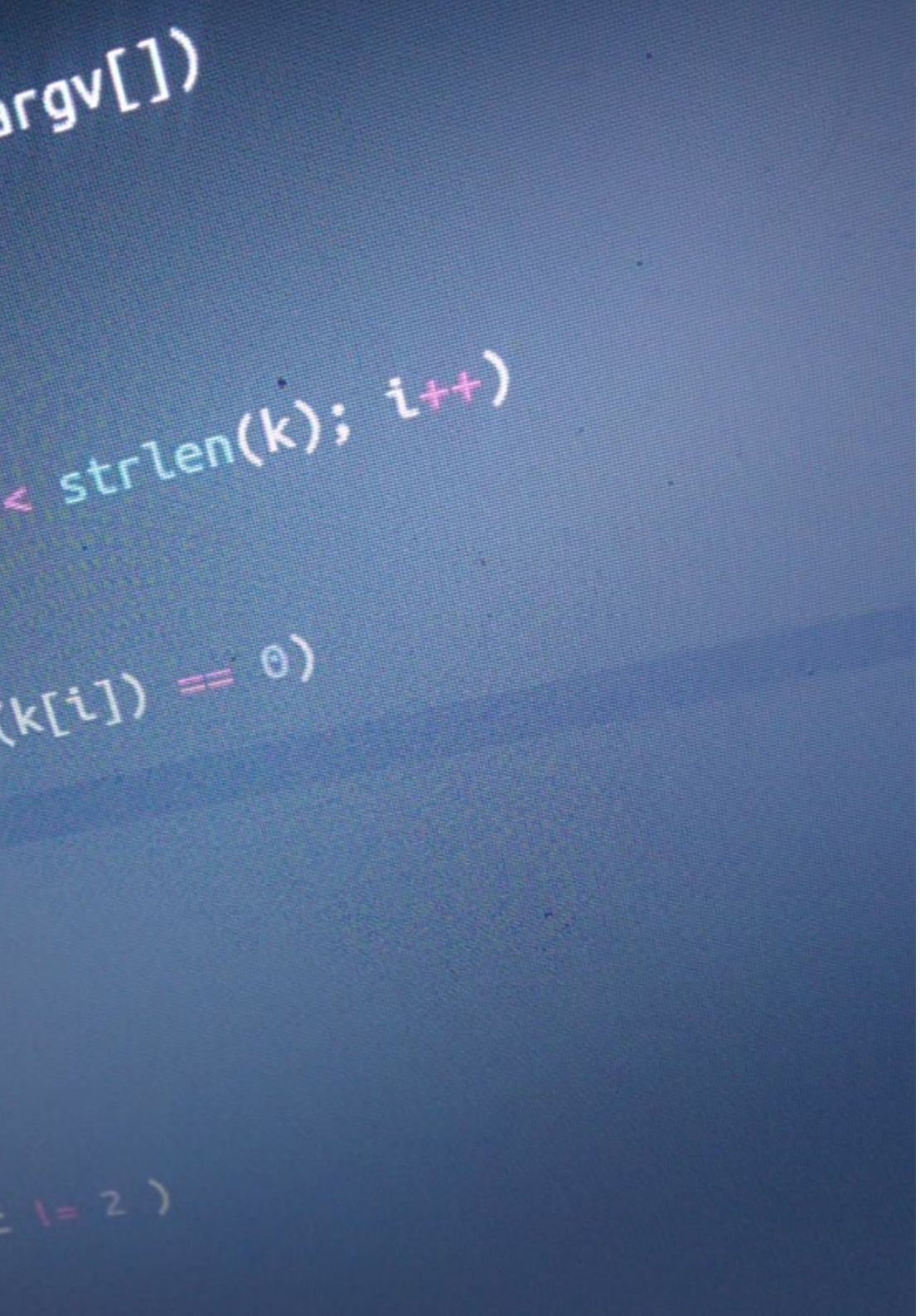
9.1. Auditoria de Sistemas de Informação. Normas de boas práticas
9.1.1. Introdução
9.1.2. Auditoria e COBIT
9.1.3. Auditoria de sistemas de gestão das TIC
9.1.4. Certificações
9.2. Conceitos e metodologias de auditoria de sistemas
9.2.1. Introdução
9.2.2. Metodologias de avaliação de sistemas: quantitativas e qualitativas
9.2.3. Metodologias de auditoria informática
9.2.4. O plano de auditoria
9.3. Contrato de auditoria
9.3.1. Natureza jurídica do contrato
9.3.2. Partes de um contrato de auditoria
9.3.3. Objeto do contrato de auditoria
9.3.4. O relatório de auditoria
9.4. Elementos organizacionais das auditorias
9.4.1. Introdução
9.4.2. Missão do departamento de auditoria
9.4.3. Planejamento das auditorias
9.4.4. Metodologia da auditoria de SI
9.5. Estrutura legal para auditorias
9.5.1. Proteção de dados pessoais
9.5.2. Proteção jurídica do software

9.5.3. Delitos tecnológicos
9.5.4. Contratação, assinatura e identificação eletrônica
9.6. Auditoria do outsourcing e estruturas de referência
9.6.1. Introdução
9.6.2. Conceitos básicos do outsourcing
9.6.3. Auditoria do outsourcing de TI
9.6.4. Estruturas: CMMI, ISO27001, ITIL
9.7. Auditoria de Segurança
9.7.1. Introdução
9.7.2. Segurança física e lógica
9.7.3. Segurança do ambiente
9.7.4. Planejamento e execução da auditoria de segurança física
9.8. Auditorias de redes e internet
9.8.1. Introdução
9.8.2. Vulnerabilidades em redes
9.8.3. Princípios e direitos na internet
9.8.4. Controles e processamento de dados
9.9. Auditoria de aplicações e sistemas informáticos
9.9.1. Introdução
9.9.2. Modelos de referência
9.9.3. Avaliação da qualidade das aplicações
9.9.4. Auditoria da organização e gestão da área de desenvolvimento e manutenção
9.10. Auditoria de dados pessoais
9.10.1. Introdução
9.10.2. Leis e regulamentos de proteção de dados
9.10.3. Desenvolvimento da auditoria
9.10.4. Infrações e sanções

Módulo 10. Gestão de Projetos

10.1. Conceitos fundamentais do gerenciamento de projetos e o ciclo de vida deles
10.1.1. O que é um projeto?
10.1.2. Metodologia comum
10.1.3. O que é gerenciamento de projetos?
10.1.4. O que é um plano de projetos?
10.1.5. Benefícios
10.1.6. Ciclo de vida do projeto
10.1.7. Grupos de processo ou ciclo de vida de gerenciamento de projetos
10.1.8. A relação entre grupos de processo e áreas de conhecimento
10.1.9. Relação entre o ciclo de vida do produto e do projeto
10.2. Início e planejamento
10.2.1. Da ideia ao projeto
10.2.2. Desenvolvimento da carta do projeto
10.2.3. Reunião de lançamento do projeto
10.2.4. Tarefas, conhecimentos e habilidades no processo inicial
10.2.5. O plano do projeto
10.2.6. Desenvolvimento do plano básico Passos
10.2.7. Tarefas, conhecimentos e habilidades no processo de planejamento
10.3. Gestão dos *Stakeholders* e do alcance
10.3.1. Identificação das partes interessadas
10.3.2. Desenvolver um plano para a gestão das partes interessadas
10.3.3. Gerenciamento do engajamento das partes interessadas
10.3.4. Monitoramento do engajamento das partes interessadas
10.3.5. O objetivo do projeto
10.3.6. A gestão de alcance e seu plano
10.3.7. Requisitos para a coleta
10.3.8. Definir a declaração do escopo
10.3.9. Criar o WBS (EDT)
10.3.10. Verificar e controlar o escopo
10.4. Desenvolvimento do cronograma
10.4.1. A gestão de Tempo e seu plano
10.4.2. Definir as atividades
10.4.3. Sequenciamento de atividades
10.4.4. Recursos estimados de atividades

10.4.5. Estimativa da duração as atividades
10.4.6. Desenvolvimento da cronologia e cálculo do caminho crítico
10.4.7. Controle do Cronograma
10.5. Desenvolvimento do orçamento e resposta aos riscos
10.5.1. Estimativa de custos
10.5.2. Desenvolver o orçamento e a curva S
10.5.3. Controle de custos e método do valor agregado
10.5.4. Os conceitos de risco
10.5.5. Como fazer uma análise de risco
10.5.6. Desenvolvimento do plano de resposta
10.6. Gestão da qualidade
10.6.1. Planejamento de qualidade
10.6.2. Garantia de qualidade
10.6.3. Controle de qualidade
10.6.4. Conceitos estatísticos básicos
10.6.5. Ferramentas de gerenciamento de Qualidade
10.7. Comunicação e recursos humanos
10.7.1. Planejamento da gestão das comunicações
10.7.2. Análise das exigências de comunicação
10.7.3. Tecnologia das comunicações
10.7.4. Modelos de comunicação
10.7.5. Métodos de comunicação
10.7.6. Plano de gestão de comunicações
10.7.7. Gerenciando as comunicações
10.7.8. Gestão de recursos humanos
10.7.9. Principais atores e seus papéis nos projetos
10.7.10. Tipos de organizações
10.7.11. Organização do projeto
10.7.12. A equipe de trabalho
10.8. Aquisições
10.8.1. O processo de Compras



10.8.2. Planejamento
10.8.3. Busca de fornecedores e solicitação de propostas
10.8.4. Adjudicação do contrato
10.8.5. Administração do contrato
10.8.6. Os contratos
10.8.7. Tipos de contratos
10.8.8. Negociação de contratos

10.9. Implementação, monitoramento, controle e fechamento
10.9.1. Grupos de Processo:
10.9.2. Implementação do projeto
10.9.3. Monitoramento e controle de projetos
10.9.4. Encerramento do projeto

10.10. Responsabilidade profissional
10.10.1. Responsabilidade profissional
10.10.2. Características da responsabilidade social e profissional
10.10.3. Código de ética do líder do projeto
10.10.4. Responsabilidades PMP®
10.10.5. Exemplos de responsabilidade
10.10.6. Benefícios da profissionalização

Um crescimento profissional e pessoal que será um grande impulso para sua competitividade"

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

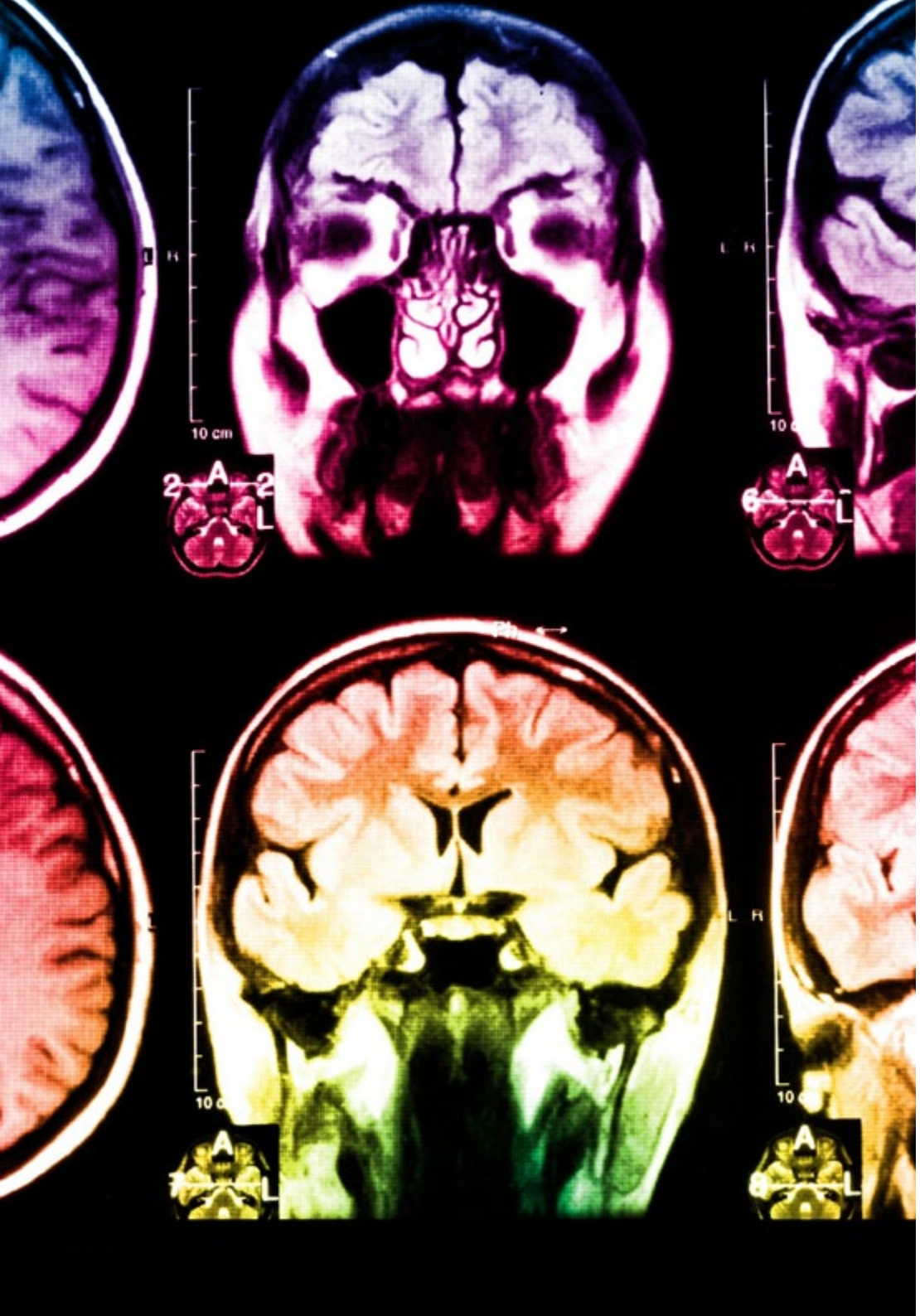
A TECH utiliza de maneira eficaz a metodologia do estudo de caso com um sistema de aprendizagem 100% online, baseado na repetição, combinando elementos didáticos diferentes em cada aula.

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.

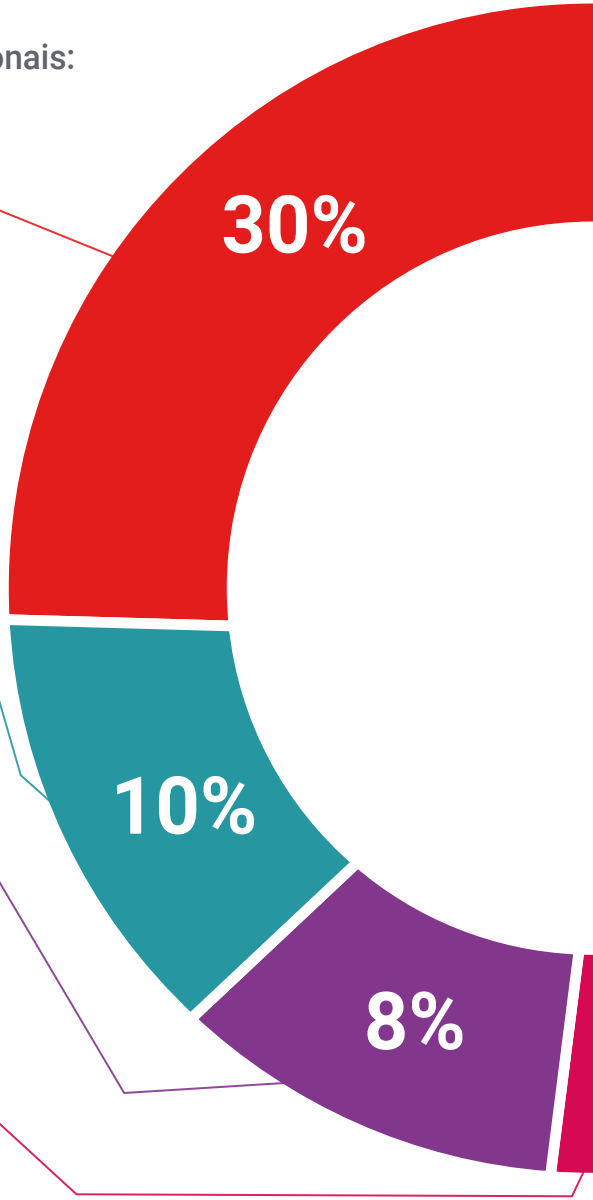
O "Learning from an expert" fortalece o conhecimento e a memória, além de gerar segurança para a tomada de decisões difíceis no futuro.

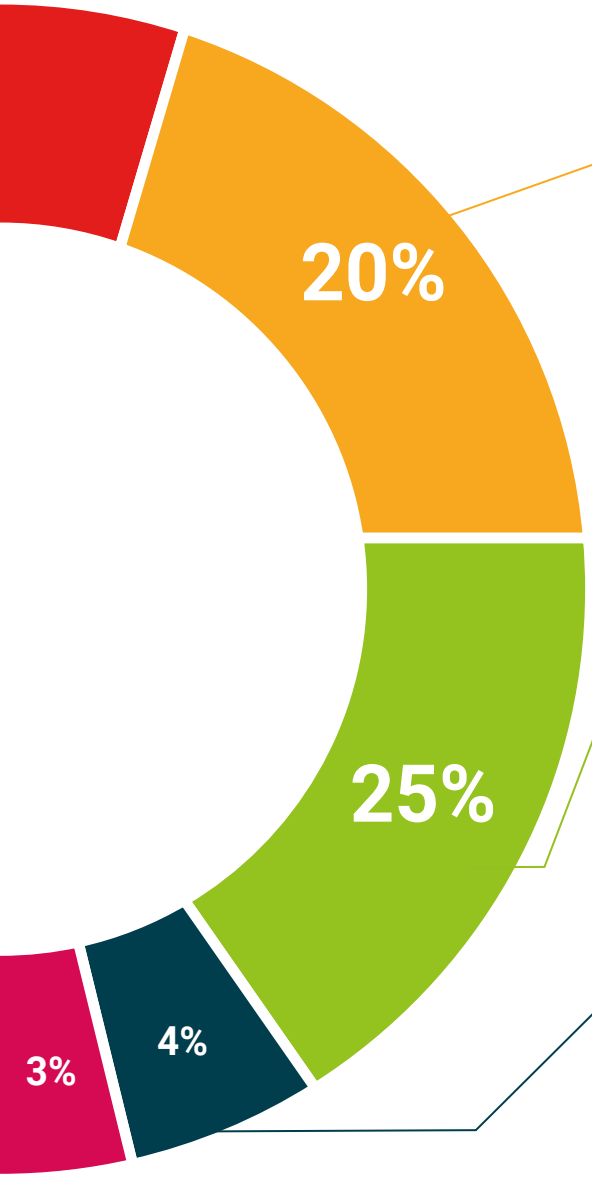
Práticas de habilidades e competências

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.

06

Certificado

O Mestrado em Telemática garante, além da capacitação mais rigorosa e atualizada, o acesso a um título de Mestrado emitido pela TECH Global University.

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

Este programa permitirá a obtenção do certificado próprio de **Mestrado em Telemática** reconhecido pela **TECH Global University**, a maior universidade digital do mundo.

A **TECH Global University**, é uma Universidade Europeia Oficial reconhecida publicamente pelo Governo de Andorra ***(boletim oficial)***. Andorra faz parte do Espaço Europeu de Educação Superior (EEES) desde 2003. O EEES é uma iniciativa promovida pela União Europeia com o objetivo de organizar o modelo de formação internacional e harmonizar os sistemas de ensino superior dos países membros desse espaço. O projeto promove valores comuns, a implementação de ferramentas conjuntas e o fortalecimento de seus mecanismos de garantia de qualidade para fomentar a colaboração e a mobilidade entre alunos, pesquisadores e acadêmicos.

Esse título próprio da **TECH Global University**, é um programa europeu de formação contínua e atualização profissional que garante a aquisição de competências em sua área de conhecimento, conferindo um alto valor curricular ao aluno que conclui o programa.

Título: **Mestrado em Telemática**

Modalidade: **online**

Duração: **12 meses**

Créditos: **60 ECTS**


tech global university

O Sr. _____, com documento de identidade _____, aprovou satisfatoriamente e obteve o certificado próprio do:

Mestrado em Telemática

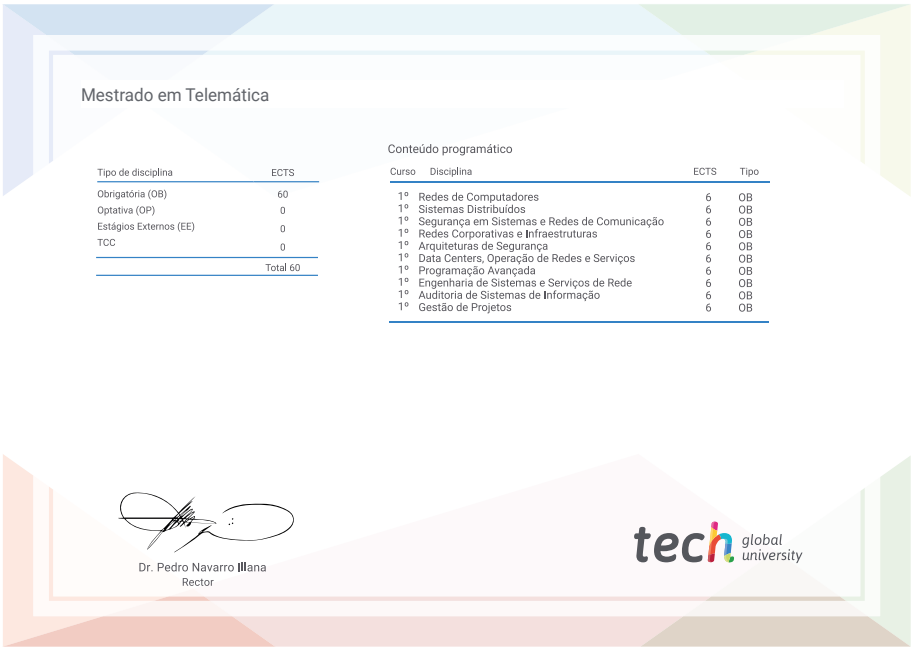
Trata-se de um título próprio com duração de 1.800 horas, o equivalente a 60 ECTS, com data de início dd/mm/aaaa e data final dd/mm/aaaa.

A TECH Global University é uma universidade oficialmente reconhecida pelo Governo de Andorra em 31 de janeiro de 2024, que pertence ao Espaço Europeu de Educação Superior (EEES).

Em Andorra la Vella, 28 de fevereiro de 2024

Dr. Pedro Navarro Illana
Rector

código único TECH: AFWOR23S techtitute.com/titulos


Mestrado em Telemática

Tipo de disciplina	ECTS
Obrigatória (OB)	60
Optativa (OP)	0
Estágios Externos (EE)	0
TCC	0
	Total 60

Conteúdo programático

Curso	Disciplina	ECTS	Tipo
1º	Redes de Computadores	6	OB
1º	Sistemas Distribuídos	6	OB
1º	Segurança em Sistemas e Redes de Comunicação	6	OB
1º	Redes Corporativas e Infraestruturas	6	OB
1º	Arquiteturas de Segurança	6	OB
1º	Data Centers, Operação de Redes e Serviços	6	OB
1º	Programação Avançada	6	OB
1º	Engenharia de Sistemas e Serviços de Rede	6	OB
1º	Auditoria de Sistemas de Informação	6	OB
1º	Gestão de Projetos	6	OB

Dr. Pedro Navarro Illana
Rector

tech global university

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

tech global university

Mestrado

Telemática

- Modalidade: **online**
- Duração: **12 meses**
- Certificado: **TECH Global University**
- Créditos: **60 ECTS**
- Horário: **no seu próprio ritmo**
- Provas: **online**

Mestrado
Telemática

tech global university