Programa Avançado

Implementação de Políticas de Segurança Informática

tech universidade tecnológica

tech universidade tecnológica

Programa Avançado
Implementação de Políticas de Segurança Informática

- Modalidade: **online**
- Duração: **6 meses**
- Certificado: **TECH Universidade Tecnológica**
- Dedicação: **16h/semana**
- Horário: **no seu próprio ritmo**
- Provas: **online**

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

Índice

01

Apresentação

As empresas apostam na segurança dos equipamentos informáticos e da nuvem para evitar o roubo ou perda de dados valiosos, no entanto, negligenciam outros aspectos igualmente importantes da segurança em uma empresa, tais como a proteção de equipamentos físicos e ambientais. Neste programa 100% online, o profissional de TI se aprofundará no hardening dos sistemas com a implementação de métodos de segurança avançados para manter o controle de acesso e a autorização para cada usuário. Todos estes aspectos, com um conteúdo de qualidade baseado em resumos em vídeo, leituras específicas e casos práticos que permitirão a qualificação em uma área da ciência da computação que necessita de profissionais altamente qualificados.

Saiba mais sobre as principais tecnologias de identificação e autorização e implemente sistemas informáticos mais seguros através deste Programa Avançado"

O investimento em segurança informática é fundamental para empresas e instituições, no entanto, muitas se concentram em possíveis ataques cibernéticos externos e negligenciam o desenvolvimento de uma política adequada de segurança física e ambiental para controlar o acesso aos sistemas de TI. Neste Programa Avançado, o profissional de TI se aprofundará nos principais aspectos a serem considerados na prática desta tarefa, resultando não ser um fator fácil.

Ministrado por especialistas em segurança informática, este programa abordará a verificação do status de segurança de um sistema informático através de controles CIS, a análise de todos os sistemas de controle de acesso biométrico existentes, bem como sua implementação e a gestão de riscos. Além disso, analisaremos a implementação da criptografia em redes de comunicação com os protocolos atuais de maior utilização, tanto simétricos como assimétricos.

Da mesma forma, a autenticação e identificação terá um lugar importante neste programa, onde o profissional de TI desenvolverá uma PKI, conhecerá sua estrutura e sua utilização para proteger a rede através do uso de certificados digitais.

Trata-se de uma excelente oportunidade proporcionada pela TECH para especializar-se em um setor que requer profissionais com conhecimentos atualizados e inovadores na área de segurança informática. O modelo de ensino 100% online permitirá ao aluno conciliar a aprendizagem com outras atividades pessoais, considerando que somente será necessário um dispositivo com conexão à internet para acessar todos os conteúdos multimídia de qualidade.

Este **Programa Avançado de Implementação de Políticas de Segurança Informática** 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
- O conteúdo gráfico, esquemático e extremamente útil fornece informações técnicas e práticas sobre as disciplinas fundamentais para a prática profissional
- Exercícios práticos onde o processo de autoavaliação é realizado para melhorar a aprendizagem
- Destaque especial para as metodologias inovadoras
- 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

Atualize seus conhecimentos sobre segurança informática em caso de incêndios e terremotos. Matricule-se neste Programa Avançado”

Conheça os últimos avanços em impressões digitais, reconhecimento facial, íris e retina como medidas de segurança informática"

Aprofunda-se nos protocolos de comunicação segura e evite o roubo de dados de alto valor. Matricule-se já.

Domine de forma perfeita a ferramenta Secure Shell e evite vazamentos de informações das empresas.

A equipe de professores deste programa inclui profissionais da área, cuja experiência de trabalho é somada nesta capacitação, além de reconhecidos especialistas de 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 estrutura deste programa se concentra na Aprendizagem Baseada em Problemas, onde o profissional deverá tentar resolver as diferentes situações de prática profissional que surjam ao longo do curso acadêmico. Para isso, o profissional contará com a ajuda de um inovador sistema de vídeo interativo desenvolvido por destacados especialistas nesta área.

02

Objetivos

Ao concluir este Programa Avançado, o profissional de TI poderá implementar políticas de segurança em software e hardware ou examinar a biometria e os sistemas biométricos. Além disso, o aluno poderá aplicar várias técnicas de criptografia de rede, como TLS, VPN ou SSH e controlar as melhores ferramentas de monitoramento de sistemas atualmente disponíveis no mercado. A grande variedade de recursos e casos práticos proporcionará uma experiência de aprendizagem muito próxima da realidade a ser enfrentada no ambiente profissional.

Obtenha uma qualificação na área de segurança informática graças a este Programa Avançado. Matricule-se já"

Objetivos Gerais

- Aprofundar-se nos principais conceitos de segurança da informação
- Desenvolver as medidas necessárias para garantir boas práticas de segurança da informação
- Desenvolver as diferentes metodologias para realizar uma análise abrangente das ameaças
- Instalar e conhecer as diferentes ferramentas utilizadas no tratamento e prevenção de incidentes

Este programa lhe fornecerá as ferramentas necessárias para examinar a biometria e os sistemas biométricos em uma empresa"

Objetivos Específicos

Módulo 1. Implementação Prática de Políticas de Segurança em Software e Hardware

- Determinando o que é a autenticação e a identificação
- Analisar os diferentes métodos de autenticação que existem e sua implementação prática
- Implementar a política adequada de controle de acesso para software e sistemas
- Estabelecer as principais tecnologias de identificação atuais
- Desenvolver conhecimentos especializados sobre as diferentes metodologias que existem para o Hardening de sistemas

Módulo 2. Implementação de Políticas de Segurança Física e Ambiental na Empresa

- Analisar o termo área segura e perímetro seguro
- Analisar a biometria e os sistemas biométricos
- Implementar políticas de segurança sólidas para a segurança física
- Desenvolver os regulamentos atuais em áreas seguras de sistemas informáticos

Módulo 3. Políticas de Comunicação Segura na Empresa

- Proteger uma rede de comunicações através da partição da mesma
- Analisar os diferentes algoritmos de criptografia utilizados nas redes de comunicação
- Implementar diversas técnicas de criptografia na rede, tais como TLS, VPN ou SSH

Módulo 4. Ferramentas de Monitoramento em Políticas de Segurança de Sistemas de Informação

- Desenvolver o conceito de monitoramento e implementação de métricas
- Configurar os logs de auditoria em sistemas e monitorar redes
- Compilar as melhores ferramentas de monitoramento de sistemas atualmente disponíveis no mercado

03

Direção do curso

Este Programa Avançado dispõe de uma equipe docente com experiência na gestão web e segurança em redes e sistemas de serviços. Seu amplo conhecimento nesta área da informática foi fundamental para realizar sua seleção. Ao longo de seis meses deste programa, o aluno terá a garantia de ser orientado por professores com formação acadêmica e prática diária na aplicação de ferramentas, sistemas e protocolos de segurança nas empresas. Todos estes aspectos, com o objetivo de proporcionar uma aprendizagem de qualidade, permitindo que o profissional de TI avance nesta área.

Uma equipe de professores com ampla experiência em segurança de TI será sua garantia de sucesso neste processo de aprendizagem"

Direção

Sra. Sonia Fernández Sapena

- Formadora em Segurança Informática e Hacking Ético no Centro de Referência Nacional de Getafe, em Informática e Telecomunicações de Madrid
- Instrutora certificada E-Council
- Instrutora nas seguintes certificações: EXIN Ethical Hacking Foundation e EXIN Cyber & IT Security Foundation. Madrid
- Instrutor especializada credenciada pela CAM para os seguintes certificados de profissionalismo: Segurança Informática (IFCT0190), Gerenciamento de Redes de Voz e Dados (IFCM0310), Administração de Redes Departamentais (IFCT0410), Gerenciamento de Alarmes em Redes de Telecomunicações (IFCM0410), Operador de Redes de Voz e Dados (IFCM0110), e Administração de Serviços de Internet (IFCT0509)
- Colaboradora externa CSO/SSA (Chief Security Officer/Senior Security Architect) na Universidade das Ilhas Baleares
- Formada em Engenharia da Computação pela Universidade de Alcalá de Henares de Madrid
- Mestrado em DevOps: Docker and Kubernetes. Cas-Training
- Microsoft Azure Security Techonologies. E-Council

Professores

Sra. Rosa María López García

- Especialista em Informação Gerencial
- Professora do Linux Professional Institute
- Colaboradora na Academia Hacker Incibe
- Gerente de Talentos de Cibersegurança na Teamciberhack
- Gerente administrativo, contábil e financeiro da Integra2Transportes
- Auxiliar administrativo em recursos de compras no Centro Educacional Cardenal Marcelo Espínola
- Técnico Superior em Cibersegurança e Hacking Ético
- Membro da Patrulha Cibernética

Sr. Francisco Oropesiano Carrizosa

- Engenheiro informático
- Técnico em Microinformática, Redes e Segurança na Cas-Training
- Web Services Developer, CMS, e-Commerce, UI e UX na Fersa Reparaciones
- Gestor de serviços web, conteúdos, mail e DNS na Oropesia Web & Network
- Designer gráfico e de aplicações web na Xarxa Sakai Projectes
- Curso de Sistemas Informáticos pela Universidade de Alcalá de Henares
- Mestrado em DevOps: Docker and Kubernetes pela Cyber Business Center
- Técnico de Redes e Segurança Informática pela Universidade das Ilhas Baleares
- Especialista em Design Gráfico pela Universidade Politécnica de Madrid

04

Estrutura e conteúdo

A equipe de professores deste Programa Avançado desenvolveu um programa que integra todo o conhecimento sobre a implementação prática de políticas de segurança em software e hardware, dedicando um de seus módulos à abordagem detalhada de sistemas biométricos e da proteção contra fatores ambientais, tais como incêndio ou terremotos. Além disso, este plano de estudos concentra-se especialmente nas ferramentas de monitoramento do sistema e nos algoritmos criptográficos. O sistema *Relearning*, baseado na reiteração de conteúdos e os casos eminentemente práticos irão possibilitar uma aprendizagem sólida de forma simples.

Adapte a carga didática deste programa às suas necessidades. Acesse o conteúdo a qualquer hora e em qualquer lugar. Clique e matricule-se"

Módulo 1. Implementação Prática de Políticas de Segurança em Software e Hardware

1.1. Implementação Prática de Políticas de Segurança em Software e Hardware
- 1.1.1. Implementação da identificação e autorização
- 1.1.2. Implementação de técnicas de identificação
- 1.1.3. Medidas técnicas de autorização

1.2. Tecnologias de identificação e autorização
- 1.2.1. Identificador e OTP
- 1.2.2. *Token* USB ou cartão inteligente PKI
- 1.2.3. A chave "Defesa Confidencial"
- 1.2.4. O RFID ativo

1.3. Políticas de segurança no acesso a software e sistemas
- 1.3.1. Implementação de políticas de controle de acesso
- 1.3.2. Implementação de políticas de acesso às comunicações
- 1.3.3. Tipos de ferramentas de segurança para controle de acesso

1.4. Gestão de acesso de usuários
- 1.4.1. Gestão dos direitos de acesso
- 1.4.2. Segregação de papéis e funções de acesso
- 1.4.3. Implementação de direitos de acesso em sistemas

1.5. Controle de acesso a sistemas e aplicações
- 1.5.1. Regras de acesso mínimo
- 1.5.2. Tecnologias de login seguro
- 1.5.3. Políticas de segurança de senhas

1.6. Tecnologias de sistemas de identificação
- 1.6.1. Diretório ativo
- 1.6.2. OTP
- 1.6.3. PAP, CHAP
- 1.6.4. KERBEROS, DIAMETER, NTLM

1.7. Controles CIS para hardening de sistemas
- 1.7.1. Controles CIS básicos
- 1.7.2. Controles CIS fundamentais
- 1.7.3. Controles CIS organizacionais

1.8. Segurança operacional
- 1.8.1. Proteção contra códigos maliciosos
- 1.8.2. Cópias de segurança
- 1.8.3. Registro de atividade e supervisão

1.9. Gestão das vulnerabilidades técnicas
- 1.9.1. Vulnerabilidades técnicas
- 1.9.2. Gestão das vulnerabilidades técnicas
- 1.9.3. Restrições na instalação de software

1.10. Implementação de práticas de política de segurança
- 1.10.1. Vulnerabilidades lógicas
- 1.10.2. Implementação de políticas de defesa

Módulo 2. Implementação de Políticas de Segurança Física e Ambiental na Empresa

2.1. Áreas seguras
- 2.1.1. Perímetro de segurança física
- 2.1.2. Trabalho em áreas seguras
- 2.1.3. Segurança de escritórios, repartições e recursos

2.2. Controles físicos de entrada
- 2.2.1. Políticas de controle de acesso físico
- 2.2.2. Sistemas de controle de entrada física

2.3. Vulnerabilidades de acesso físico
- 2.3.1. Principais vulnerabilidades físicas
- 2.3.2. Implementação de medidas de salvaguardas

2.4. Sistemas biométricos fisiológicos
- 2.4.1. Impressão digital
- 2.4.2. Reconhecimento facial
- 2.4.3. Reconhecimento da íris e da retina
- 2.4.4. Outros sistemas biométricos fisiológicos

2.5. Sistemas biométricos de comportamento
- 2.5.1. Reconhecimento de assinaturas
- 2.5.2. Reconhecimento do escritor
- 2.5.3. Reconhecimento de voz
- 2.5.4. Outros sistemas biométricos de comportamentos

2.6. Gestão de riscos em biometria
- 2.6.1. Implementação de sistemas biométricos
- 2.6.2. Vulnerabilidades dos sistemas biométricos

2.7. Implementação de políticas em Hosts
- 2.7.1. Instalação de suprimentos e segurança de cabeamento
- 2.7.2. Localização dos equipamentos
- 2.7.3. Saída dos equipamentos fora das instalações
- 2.7.4. Equipamentos de informática desacompanhados e uma política transparente de banca

2.8. Proteção ambiental
- 2.8.1. Sistemas de proteção contra incêndios
- 2.8.2. Sistemas de proteção sísmica
- 2.8.3. Sistemas de proteção contra terremotos

2.9. Segurança no centro de processamento de dados
- 2.9.1. Portas de segurança
- 2.9.2. Sistemas de videovigilância (CCTV)
- 2.9.3. Controle de segurança

2.10. Regulamento Internacional de Segurança Física
- 2.10.1. IEC 62443-2-1 (europeia)
- 2.10.2. NERC CIP-005-5 (E UA)
- 2.10.3. NERC CIP-014-2 (E UA)

Módulo 3. Políticas de Comunicação Segura na Empresa

3.1. Gestão de segurança nas redes
- 3.1.1. Controle e monitoramento de rede
- 3.1.2. Segregação de redes
- 3.1.3. Sistemas de segurança em redes

3.2. Protocolos seguros de comunicação
- 3.2.1. Modelo TCP/IP
- 3.2.2. Protocolo IPSEC
- 3.2.3. Protocolo TLS

3.3. Protocolo TLS 1.3
- 3.3.1. Fases de um processo TLS 1.3
- 3.3.2. Protocolo Handshake
- 3.3.3. Protocolo de registro
- 3.3.4. Diferenças com TLS 1,2

3.4. Algoritmos criptográficos
- 3.4.1. Algoritmos criptográficos utilizados nas comunicações
- 3.4.2. *Cipher-suites*
- 3.4.3. Algoritmos criptográficos permitidos para TLS 1.3

3.5. Funções *Digest*
- 3.5.1. MD6
- 3.5.2. SHA

3.6. PKI. Infraestrutura de chave pública
- 3.6.1. PKI e suas entidades
- 3.6.2. Certificado digital
- 3.6.3. Tipos de certificados digitais

3.7. Comunicações de túneis e transporte
- 3.7.1. Comunicações em túneis
- 3.7.2. Comunicações em transporte
- 3.7.3. Implementação de túneis criptografados

3.8. SSH. *Secure Shell*
- 3.8.1. SSH. Cápsula segura
- 3.8.2. Funcionamento de SSH
- 3.8.3. Ferramentas SSH

3.9. Auditoria de sistemas criptográficos
- 3.9.1. Teste de integração
- 3.9.2. Teste de sistema criptográfico

3.10. Sistemas criptográficos
- 3.10.1. Vulnerabilidades de sistemas criptográficos
- 3.10.2. Salvaguardas na criptografia

Módulo 4. Ferramentas de Monitoramento em Políticas de Segurança de Sistemas de Informação

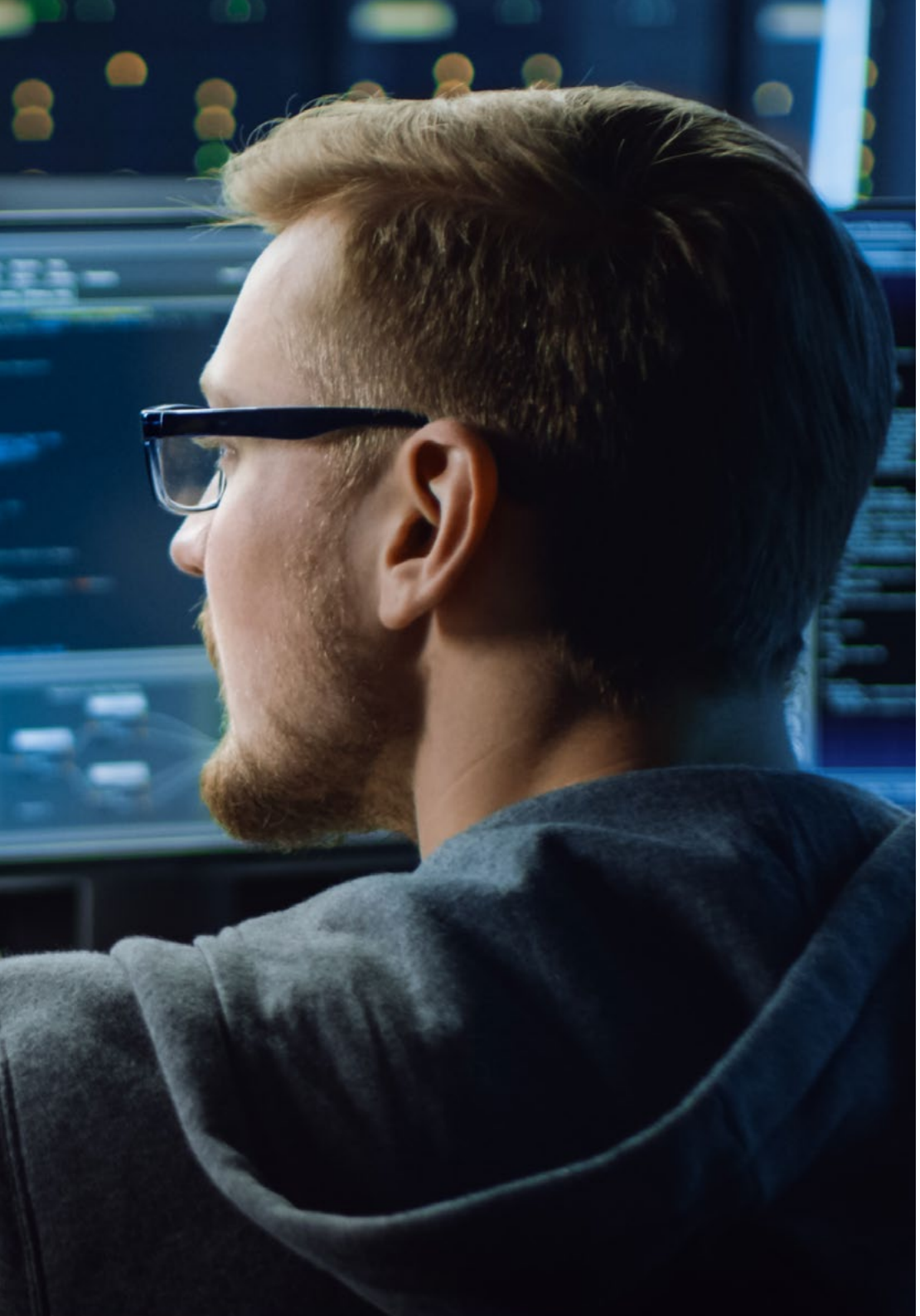
4.1. Políticas de monitoramento de sistemas da informação
- 4.1.1. Monitoramento de sistemas
- 4.1.2. Métricas
- 4.1.3. Tipos de métricas

4.2. Auditoria e registro em sistemas
- 4.2.1. Auditoria e registro em Windows
- 4.2.2. Auditoria e registro em Linux

4.3. Protocolo SNMP. *Simple Network Management Protocol*
- 4.3.1. Protocolo SNMP
- 4.3.2. Funcionamento de SNMP
- 4.3.3. Ferramentas SNMP

4.4. Monitoramento de redes
- 4.4.1. O monitoramento de redes em sistemas de controle
- 4.4.2. Ferramentas de monitoramento para sistemas de controle

4.5. Nagios. Sistema de monitoramento de redes
- 4.5.1. Nagios
- 4.5.2. Funcionamento do Nagios
- 4.5.3. Instalação do Nagios



4.6. Zabbix. Sistema de monitoramento de redes
- 4.6.1. Zabbix
- 4.6.2. Funcionamento do Zabbix
- 4.6.3. Instalação do Zabbix

4.7. Cacti. Sistema de monitoramento de redes
- 4.7.1. Cacti
- 4.7.2. Funcionamento de Cacti
- 4.7.3. Instalação de Cacti

4.8. Pandora. Sistema de monitoramento de redes
- 4.8.1. Pandora
- 4.8.2. Funcionamento de Pandora
- 4.8.3. Instalação de Pandora

4.9. SolarWinds. Sistema de monitoramento de redes
- 4.9.1. SolarWinds
- 4.9.2. Funcionamento do SolarWinds
- 4.9.3. Instalação de SolarWinds

4.10. Regulamento sobre monitoramento
- 4.10.1. Controles CIS sobre auditoria e registro
- 4.10.2. NIST 800-123 (EUA)

Os resumos interativos e os casos práticos desenvolvidos pela equipe docente lhe fornecerão o conteúdo necessário para avançar em sua carreira"

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

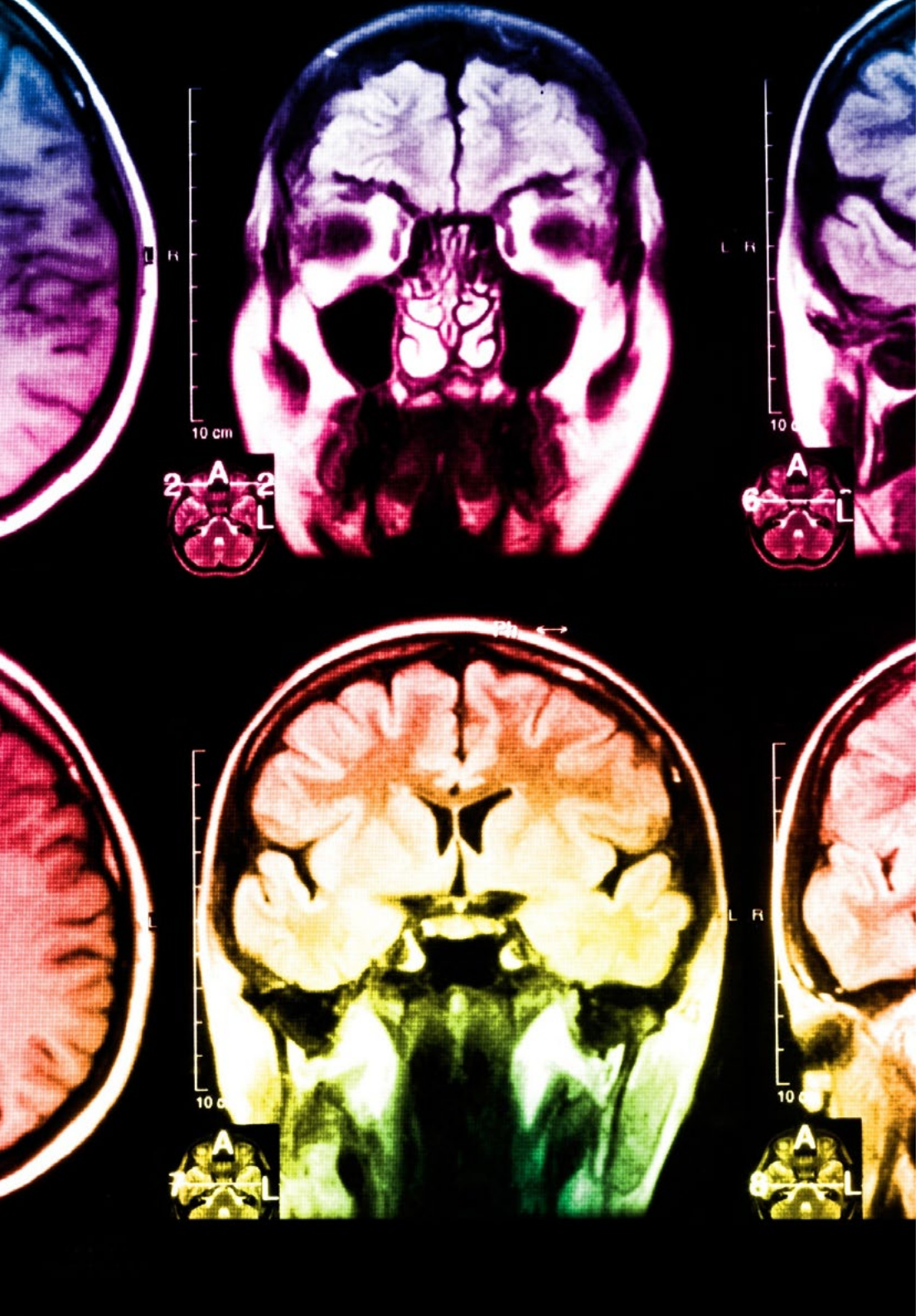
A TECH utiliza de maneira eficaz a metodologia do estudo de caso com um sistema de aprendizagem 100% online, baseado na repetição, combinando elementos didáticos diferentes em cada aula.

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.

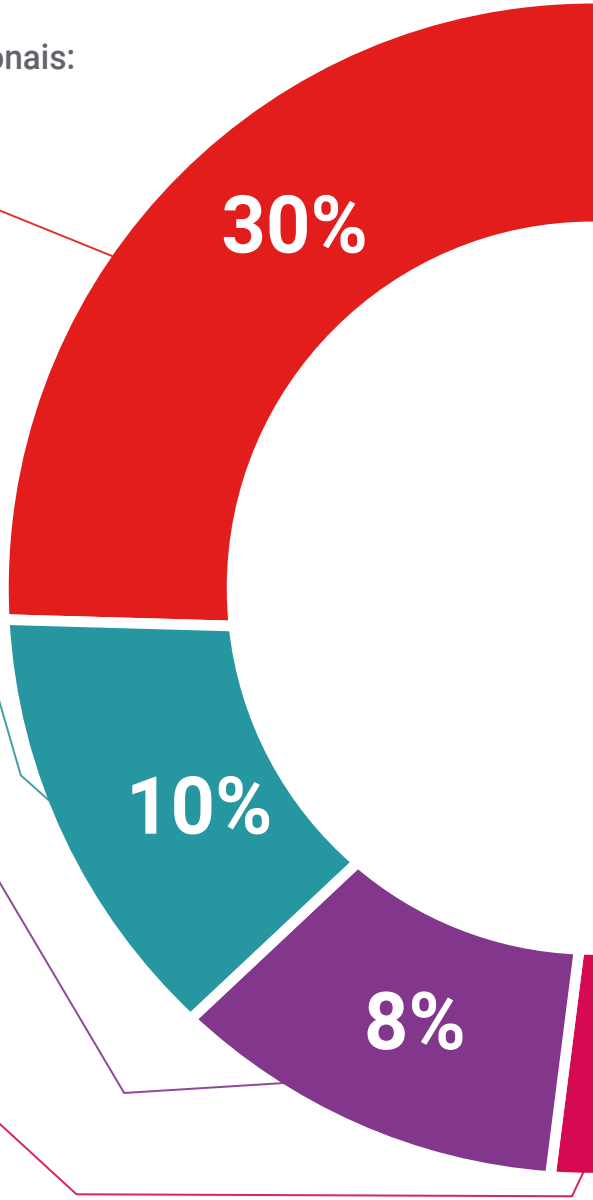
O "Learning from an expert" fortalece o conhecimento e a memória, além de gerar segurança para a tomada de decisões difíceis no futuro

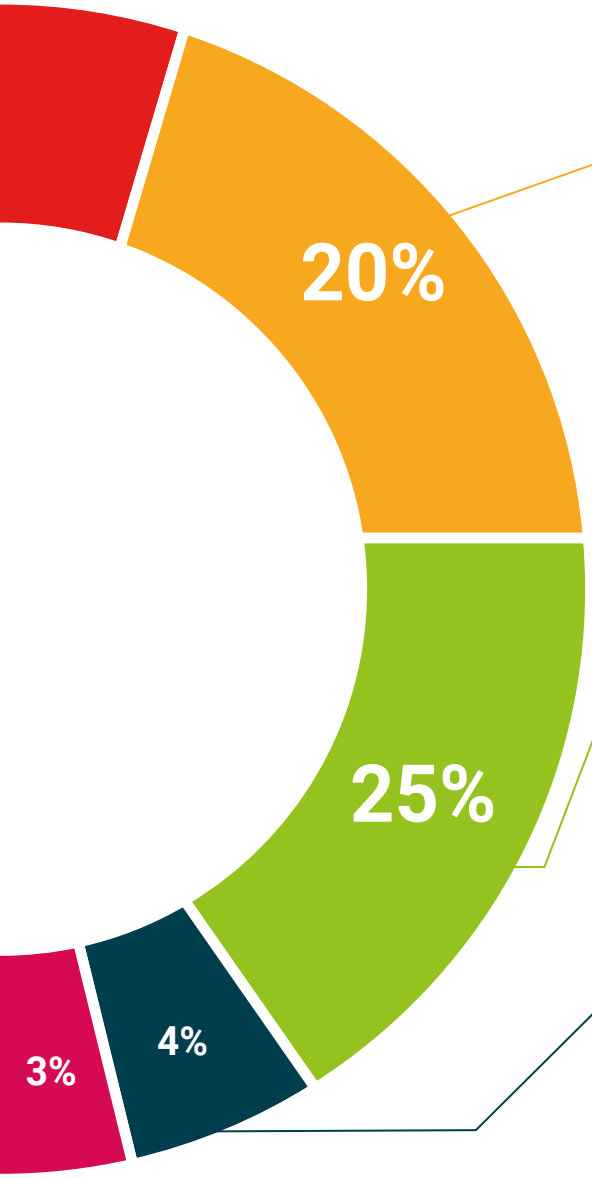
Práticas de habilidades e competências

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 Programa Avançado de Implementação de Políticas de Segurança Informática 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 Implementação de Políticas de Segurança Informática** conta com o conteúdo 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 Implementação de Políticas de Segurança Informática**

N.º de Horas Oficiais: **450h**


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

Implementação de Políticas de Segurança Informática

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
Implementação de Políticas de Segurança Informática

- Modalidade: **online**
- Duração: **6 meses**
- Certificado: **TECH Universidade Tecnológica**
- Dedicação: **16h/semana**
- Horário: **no seu próprio ritmo**
- Provas: **online**

Programa Avançado

Implementação de Políticas de Segurança Informática

tech universidade tecnológica