

# Programa Avançado

## Medidas de Defesa de Segurança Informática



## Programa Avançado Medidas de Defesa de Segurança Informática

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

Acesso ao site: [www.techtute.com/br/informatica/programa-avancado/programa-avancado-medidas-defensa-seguranca-informatica](http://www.techtute.com/br/informatica/programa-avancado/programa-avancado-medidas-defensa-seguranca-informatica)

# Índice

01

Apresentação

---

*pág. 4*

02

Objetivos

---

*pág. 8*

03

Direção do curso

---

*pág. 12*

04

Estrutura e conteúdo

---

*pág. 16*

05

Metodologia

---

*pág. 22*

06

Certificado

---

*pág. 30*

# 01

# Apresentação

Os setores financeiro, empresarial e turístico sofreram um aumento nos ataques de engenharia social que comprometem informações sensíveis e valiosas das próprias instituições e de seus clientes. Os ataques cibernéticos continuam representando um grande problema para as companhias, aumentando nos últimos anos o número de empregos criados para garantir a segurança informática. Em resposta a esta necessidade, este programa proporcionará ao profissional de TI uma qualificação na área de implantação de medidas de defesa de TI contra qualquer ataque. Uma equipe de professores especializados nesta área ministrará este programa em um formato 100% online, permitindo ao aluno adquirir uma aprendizagem atual e abrangente graças ao seu extenso conteúdo multimídia.



“

*Ofereça a melhor resposta em segurança informática e evite que as empresas caiam em engenharia social”*

A implementação de políticas de segurança informática representa um custo para as empresas, no entanto, estão dispostas a pagar por isso devido aos elevados prejuízos resultantes da invasão de seus sistemas, comprometendo seu bom funcionamento e o serviço que prestam a seus clientes. Um papel fundamental neste cenário é desempenhado pelos profissionais de TI.

Este Programa Avançado oferece ao aluno uma formação intensiva sobre as medidas de defesa da segurança informática, iniciando com uma análise das ameaças e depois classificando-as adequadamente a fim de descobrir onde uma empresa apresentará vulnerabilidades. Além disso, a equipe docente especializada neste campo fornecerá as ferramentas fundamentais para a realização de uma análise forense informatizada. Desta forma, será mostrada a detecção de incidentes através dos sistemas IDS/IPS e seu processamento no SIEM até o processo de notificação e escalonamento.

Com o objetivo de estar na vanguarda da defesa da segurança, o profissional de TI desenvolverá as técnicas para mitigar a negação de serviço, o *session hacking* e ataques a aplicações web. Todos estes aspectos, em uma modalidade de ensino 100% online, que permitirá ao aluno combinar suas atividades profissionais com um programa que oferece conteúdos multimídia inovadores. Somente será necessário um dispositivo com conexão à internet para acessar um plano de estudos que poderá estudá-lo ao seu próprio ritmo.

Este **Programa Avançado de Medidas de Defesa 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 eminentemente prático oferece informações técnicas e práticas sobre aquelas disciplinas que são essenciais para a prática profissional
- ◆ Exercícios práticos em que o processo de autoavaliação é realizado para melhorar a aprendizagem
- ◆ Destaque especial para as metodologias inovadoras
- ◆ Aulas teóricas, perguntas a 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



*Implemente eficazmente políticas de segurança contra Session Hijacking, Hacking Web Servers ou Mobile Platforms graças a este Programa Avançado”*

“

*Controle a norma ISO 27035 e cumpra os requisitos para uma gestão adequada de incidentes. Matricule-se agora neste Programa Avançado”*

O corpo docente do programa conta com profissionais do setor, que transferem toda a experiência adquirida ao longo de suas carreiras para esta capacitação, além de especialistas reconhecidos de instituições de referência e universidades de prestígio.

O conteúdo multimídia, desenvolvido com a mais recente tecnologia educacional, permitirá ao profissional uma aprendizagem contextualizada, ou seja, realizada através de um ambiente simulado, proporcionando uma capacitação imersiva e programada para praticar diante de situações reais.

A estrutura deste curso se concentra na Aprendizagem Baseada em Problemas, através da qual o profissional tentará resolver as diferentes situações de prática profissional que surgirem ao longo do curso. Para isso, contará com a ajuda de um inovador sistema de vídeo interativo realizado por especialistas reconhecidos.

*Avance em sua trajetória profissional com um programa que lhe permitirá aprofundar-se na análise e no controle das ameaças informáticas.*

*Você está a apenas um clique para matricular-se em um Programa Avançado que oferecerá mais oportunidades profissionais.*



# 02

# Objetivos

Este Programa Avançado proporcionará uma aprendizagem cujo objetivo é permitir ao profissional de TI obter uma qualificação especializada na área de segurança. Ao longo deste programa, o aluno aperfeiçoará suas habilidades na análise de ameaças, comparando diferentes metodologias de gestão que lhe permitirá selecionar a que melhor se adapte ao incidente. Também serão capacitados para implementar tecnicamente medidas para mitigar as principais ameaças para a empresa. Desta forma, o profissional de TI ganhará uma qualificação que lhe possibilitará avançar em seu ambiente laboral.





“

*Matricule-se agora. Atualize seus conhecimentos e descubra as últimas técnicas para evitar as principais ameaças informáticas em uma empresa”*



## 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

“

*Realize esta capacitação que lhe proporcionará as estratégias mais recentes e eficazes para administrar qualquer ataque cibernético”*





## Objetivos específicos

---

### **Módulo 1. Políticas de Segurança para Análise de Ameaças em Sistemas Informáticos**

- ◆ Analisando o significado das ameaças
- ◆ Determinar as fases da gestão preventiva de ameaças
- ◆ Comparar as diferentes metodologias de gestão de ameaças

### **Módulo 2. Políticas de Gestão de Incidentes de Segurança**

- ◆ Desenvolver conhecimentos específicos sobre como gerenciar incidentes causados por eventos de segurança informática
- ◆ Determinar o funcionamento de uma equipe de tratamento de incidentes de segurança
- ◆ Analisar as diferentes fases da gestão de eventos da segurança informática
- ◆ Examinar os protocolos padronizados para o manejo de incidentes de segurança

### **Módulo 3. Implementação Prática de Políticas de Segurança contra Ataques**

- ◆ Determinar os diferentes ataques reais ao nosso sistema de informação
- ◆ Avaliar as diferentes políticas de segurança para mitigar os ataques
- ◆ Implementar tecnicamente medidas para mitigar as principais ameaças

# 03

## Direção do curso

A TECH seleciona cuidadosamente todos os professores que ministram os programas de graduação. Este Programa Avançado conta com uma equipe docente altamente qualificada na área de segurança informática. Sua experiência como responsável pela segurança nesta área em entidades públicas e privadas, garantirá ao aluno um conhecimento privilegiado, proporcionando grande valor ao profissional que deseja conhecer em primeira mão as principais medidas adotadas neste campo, diante das principais ameaças sofridas. Desta forma, os casos práticos apresentados correspondem a situações reais que o aluno deverá enfrentar em seu ambiente de trabalho e que, portanto, irá ajudá-lo a crescer profissionalmente.



“

*Uma equipe de especialistas em segurança informática disponibilizará todo o seu conhecimento para ajudá-lo a avançar em sua carreira”*

## 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 Technologies. 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 da Computação
- ◆ 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 plano de estudos que abordará detalhadamente cada uma das fases do desenvolvimento de um plano de segurança voltado para as ameaças aos sistemas informáticos. Desta forma, analisaremos a auditoria de ameaças, sua categorização, a gestão de incidentes e as últimas ferramentas para a detecção de ameaças. Também contemplaremos as questões levantadas pela engenharia social nas empresas que são afetadas. Todos estes aspectos, com materiais multimídia atualizados que facilitarão a compreensão do conteúdo, além de um sistema *Relearning*, que possibilitará a aquisição de sólidos conhecimentos.





“

*Acesse uma aprendizagem 100% online e flexível, podendo avançar ao seu próprio ritmo. Concilie sua vida pessoal com um ensino de qualidade. Faça sua matrícula agora"*

## Módulo 1. Políticas de Segurança para Análise de Ameaças em Sistemas Informáticos

- 1.1. A gestão de ameaças nas políticas de segurança
  - 1.1.1. A gestão de riscos
  - 1.1.2. O risco na segurança
  - 1.1.3. Metodologias na gestão de ameaças
  - 1.1.4. Implantação de metodologias
- 1.2. Fases da gestão de ameaças
  - 1.2.1. Identificação
  - 1.2.2. Análise
  - 1.2.3. Localização
  - 1.2.4. Medidas de proteção
- 1.3. Sistemas de auditoria para localização de ameaças
  - 1.3.1. Classificação e fluxo de informações
  - 1.3.2. Análise de processos vulneráveis
- 1.4. Classificação de riscos
  - 1.4.1. Tipos de riscos
  - 1.4.2. Cálculo da probabilidade de ameaças
  - 1.4.3. Risco residual
- 1.5. Tratamento de risco
  - 1.5.1. Implementação de medidas de salvaguarda
  - 1.5.2. Transferir ou assumir
- 1.6. Controle de riscos
  - 1.6.1. Processo contínuo da gestão de riscos
  - 1.6.2. Implementação de métricas de segurança
  - 1.6.3. Modelo estratégico de métricas de segurança da informação
- 1.7. Metodologias práticas para análise e controle de ameaças
  - 1.7.1. Catálogo de ameaças
  - 1.7.2. Catálogo de medidas de controle
  - 1.7.3. Catálogo de salvaguardas
- 1.8. Norma ISO 27005
  - 1.8.1. Identificação de riscos
  - 1.8.2. Análise de risco
  - 1.8.3. Avaliação de risco



- 1.9. Matriz de risco, impacto e ameaças
  - 1.9.1. Dados, sistemas e pessoal
  - 1.9.2. Probabilidade de ameaça
  - 1.9.3. Magnitude do prejuízo
- 1.10. Planejamento de fases e processos na análise de ameaças
  - 1.10.1. Identificação de elementos críticos da organização
  - 1.10.2. Determinação de ameaças e impactos
  - 1.10.3. Análise de impacto e riscos
  - 1.10.4. Metodologias

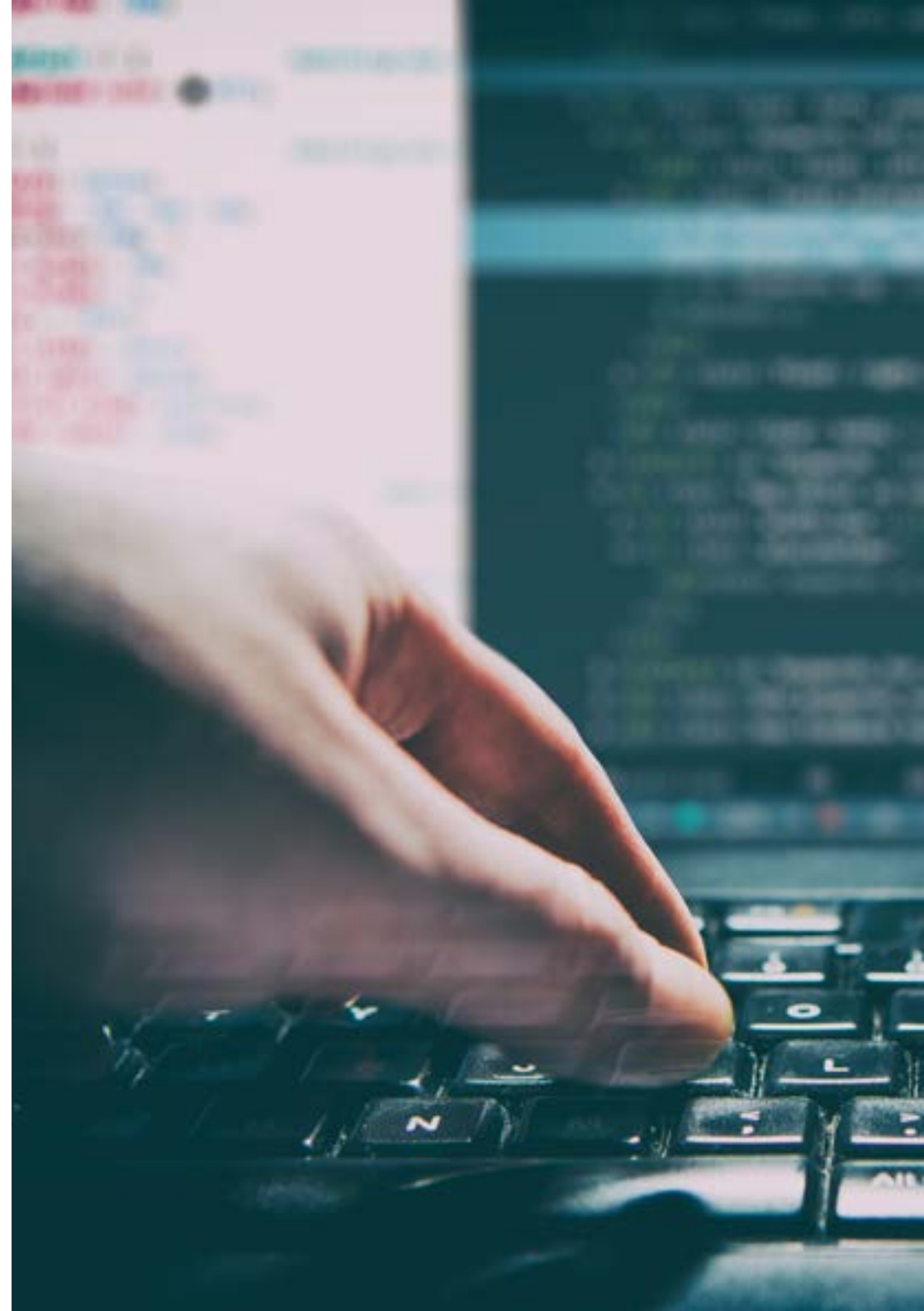
## Módulo 2. Políticas de Gestão de Incidentes de Segurança

- 2.1. Políticas de gestão de incidentes de segurança da informação e melhorias
  - 2.1.1. Gestão de incidências
  - 2.1.2. Responsabilidades e procedimentos
  - 2.1.3. Notificação de eventos
- 2.2. Sistemas de Detecção e Prevenção de Intrusão (IDS/IPS)
  - 2.2.1. Dados operacionais do sistema
  - 2.2.2. Tipos de sistemas de detecção de intrusão
  - 2.2.3. Critérios para a localização do IDS/IPS
- 2.3. Resposta a incidentes de segurança
  - 2.3.1. Procedimento de coleta de informações
  - 2.3.2. Processo de verificação de intrusão
  - 2.3.3. Organismos CERT
- 2.4. Processo de notificação e gestão de tentativas de intrusão
  - 2.4.1. Responsabilidades no processo de notificação
  - 2.4.2. Classificação dos incidentes
  - 2.4.3. Processo de resolução e recuperação
- 2.5. Análise forense como política de segurança
  - 2.5.1. Evidências voláteis e não voláteis
  - 2.5.2. Análise e coleta de evidências eletrônicas
    - 2.5.2.1. Análise de evidências eletrônicas
    - 2.5.2.2. Coleta de evidências eletrônicas

- 2.6. Ferramentas de Sistemas de Detecção e Prevenção de Intrusão (IDS/IPS)
  - 2.6.1. Snort
  - 2.6.2. Suricata
  - 2.6.3. SolarWinds
- 2.7. Ferramentas de centralização de eventos
  - 2.7.1. SIM
  - 2.7.2. SEM
  - 2.7.3. SIEM
- 2.8. Guia de Segurança CCN-STIC 817
  - 2.8.1. Gestão de incidentes cibernéticos
  - 2.8.2. Métricas e Indicadores
- 2.9. NIST/SP800-61
  - 2.9.1. Capacidade de resposta a incidentes de segurança informática
  - 2.9.2. Manejo de um incidente
  - 2.9.3. Coordenação e compartilhamento de informações
- 2.10. Norma ISO 27035
  - 2.10.1. Norma ISO 27035. Princípios da gestão de incidentes
  - 2.10.2. Diretrizes para a elaboração de um plano de gestão de incidentes
  - 2.10.3. Diretrizes de operações de resposta a incidentes

### Módulo 3. Implementação Prática de Políticas de Segurança contra Ataques

- 3.1. *System Hacking*
  - 3.1.1. Riscos e vulnerabilidades
  - 3.1.2. Contramedidas
- 3.2. DoS em serviços
  - 3.2.1. Riscos e vulnerabilidades
  - 3.2.2. Contramedidas
- 3.3. *Sessão Hijacking*
  - 3.3.1. O processo de Hijacking
  - 3.3.2. Contramedidas para *Hijacking*
- 3.4. Evasão do IDS, *Firewalls and Honeypots*
  - 3.4.1. Técnicas de prevenção
  - 3.4.2. Implementação de contramedidas



- 3.5. *Hacking Web Servers*
  - 3.5.1. Ataques a servidores web
  - 3.5.2. Implementação de medidas de defesa
- 3.6. *Hacking Web Applications*
  - 3.6.1. Ataques a aplicações web
  - 3.6.2. Implementação de medidas de defesa
- 3.7. *Hacking Wireless Networks*
  - 3.7.1. Vulnerabilidades em redes wifi
  - 3.7.2. Implementação de medidas de defesa
- 3.8. *Hacking Mobile Platforms*
  - 3.8.1. Vulnerabilidades de plataformas móveis
  - 3.8.2. Implementação de contramedidas
- 3.9. *Ramsonware*
  - 3.9.1. Vulnerabilidades que causam *Ramsonware*
  - 3.9.2. Implementação de contramedidas
- 3.10. Engenharia social
  - 3.10.1. Tipos de engenharia social
  - 3.10.2. Contramedidas à engenharia social

“ Os casos práticos e o conteúdo multimídia são as ferramentas mais eficazes deste Programa Avançado. Faça o download deste material desde o primeiro dia e avance 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.*





## 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”*

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

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.



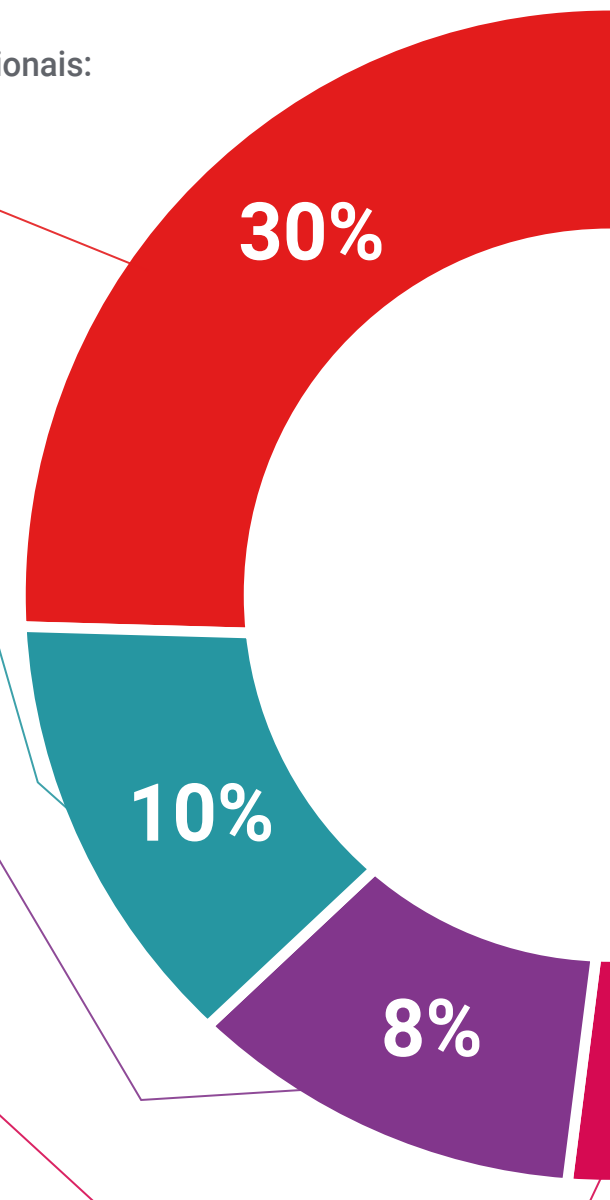
#### Práticas de habilidades e competências

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 Medidas de Defesa 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 o seu certificado sem sair de casa e sem burocracias”*

Este **Programa Avançado de Medidas de Defesa 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\* do **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 Medidas de Defesa de Segurança Informática**

Modalidade: **online**

Duração: **6 meses**



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



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

**tech** universidade  
tecnológica

Programa Avançado  
Medidas de Defesa de  
Segurança Informática

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

# Programa Avançado

## Medidas de Defesa de Segurança Informática