Curso

Fundamentos Forenses e DFIR

tech universidade tecnológica

tech universidade tecnológica

Curso
Fundamentos Forenses e DFIR

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

Acesso ao site **www.techtitute.com/br/informatica/curso/fundamentos-forenses-dfir**

Índice

01

Apresentação

Com o avanço das novas tecnologias, como os sistemas de computador, as instituições têm uma presença cada vez maior na Internet. No entanto, com o aumento dos ataques cibernéticos, as empresas estão expostas a vários contratempos. Nesse sentido, se os hackers obtiverem acesso às suas redes, eles poderão excluir dados confidenciais e até mesmo exigir dinheiro de resgate em troca da liberação dos sistemas bloqueados. Portanto, é importante que as empresas tenham especialistas em Fundamentos Forenses para detectar violações de segurança e reduzir ao máximo o impacto delas. Em resposta a essa necessidade, a TECH está lançando um programa inovador para implementar técnicas avançadas para a análise de evidências digitais. Além disso, ele é ministrado 100% online, garantindo a conveniência dos alunos.

Deseja analisar os registros de firewall e, assim, detectar invasões de rede? Consiga isso em 150 horas, graças a esta capacitação"

As empresas estão percebendo cada vez mais a importância de ter especialistas em TI de segurança cibernética em sua organização. Os benefícios disso incluem a proteção de seus ativos digitais e a investigação forense para determinar as causas e a extensão de possíveis incidentes. Por sua vez, esses profissionais também coletam informações que podem ser usadas como prova em tribunais e para processar criminosos cibernéticos. Nesse sentido, eles até ajudam as organizações a cumprir as normas de segurança de dados e os requisitos de notificação de violação de segurança.

Diante dessa situação, a TECH está desenvolvendo uma capacitação de última geração para que os alunos possam evitar ataques de hackers implementando as estratégias mais adequadas. O itinerário acadêmico se aprofundará nos processos de aquisição de provas, com base na cadeia de custódia. Dessa forma, os alunos atuarão como laboratórios forenses de informática e resolverão incidentes que afetam as organizações. O programa também abordará a análise de pacotes de rede e, portanto, os alunos realizarão registros de *firewall*. O malware também será fornecido para a execução de técnicas de desmontagem.
Assim os alunos aplicarão as metodologias DFIR e liberarão sua criatividade para oferecer as soluções comerciais mais inovadoras.

Além disso, para consolidar o domínio dos conteúdos, este programa de estudos aplica o sistema *Relearning*. Vale ressaltar que a TECH é pioneira no uso desse modelo de ensino, que promove a assimilação de conceitos complexos por meio da reiteração natural e progressiva dos mesmos. Nessa linha, o programa também se baseia em materiais de vários formatos, como resumos interativos ou vídeos explicativos. Tudo isso em um conveniente modo 100% online, que permite que os alunos ajustem seus horários de acordo com suas responsabilidades.

Este **Curso de Fundamentos Forenses e DFIR** conta com o conteúdo mais completo e atualizado do mercado. Suas principais características são:

- O desenvolvimento de casos práticos apresentados por especialistas em Fundamentos Forenses e DFIR
- Os conteúdos gráficos, esquemáticos e extremamente práticos fornece informação atualizada e prática sobre aquelas disciplinas essenciais 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
- Lições 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

Você criará planos de resposta a incidentes na melhor universidade digital do mundo, de acordo com a Forbes"

Você alcançará seus objetivos graças às ferramentas didáticas da TECH, incluindo vídeos explicativos e resumos interativos"

Precisa recuperar dados de uma mídia danificada? A TECH lhe fornece as melhores ferramentas para conseguir isso.

Você produzirá relatórios forenses com os quais poderá aparecer como testemunha especializada em casos judiciais importantes.

O corpo docente deste programa inclui profissionais da área que transferem a experiência do seu trabalho para esta capacitação, além de especialistas reconhecidos de sociedades científicas de referência e universidades de prestigio.

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 programa se concentra na Aprendizagem Baseada em Problemas, onde o profissional deverá tentar resolver as diferentes situações de prática profissional que surgirem ao longo do curso acadêmico. Para isso, contará com a ajuda de um inovador sistema de vídeo interativo realizado por especialistas reconhecidos.

02

Objetivos

O desenvolvimento desse programa explorará técnicas avançadas de coleta e análise de evidências digitais, abordando casos de violações de segurança. Dessa forma, os alunos aprenderão mais sobre análise de arquivos, bem como sobre a preservação da cadeia de custódia. Além disso, os alunos examinarão as táticas mais benéficas para minimizar o impacto de possíveis incidentes cibernéticos.

Esqueça a memorização! Com o sistema Relearning, você integrará os conceitos de forma natural e progressiva.

Objetivos gerais

- Adquirir habilidades avançadas em testes de penetração e simulações de Red Team, abordando a identificação e a exploração de vulnerabilidades em sistemas e redes
- Desenvolver habilidades de liderança para coordenar equipes especializadas em cibersegurança ofensiva, otimizando a execução de projetos de Pentesting e Red Team.
- Desenvolver habilidades na análise e no desenvolvimento de malware, compreendendo sua funcionalidade e aplicando estratégias defensivas e educacionais.
- Aperfeiçoar as habilidades de comunicação produzindo relatórios técnicos e executivos detalhados, apresentando as descobertas de forma eficaz para públicos técnicos e executivos.
- Promover a prática ética e responsável no campo da cibersegurança, considerando os princípios éticos e legais em todas as atividades.
- Manter os alunos atualizados com as tendências e tecnologias emergentes em cibersegurança.

Você contará com o apoio de um corpo docente formado por profissionais Cibersegurança Industrial"

Objetivos específicos

Módulo 1. Fundamentos Forenses e DFIR

- Adquirir uma sólida compreensão dos princípios fundamentais da Investigação Forense Digital (DFIR) e sua aplicação na resolução de incidentes cibernéticos
- Desenvolver habilidades na aquisição segura e forense de evidências digitais, garantindo a preservação da cadeia de custódia
- Aprender a realizar análise forense de sistemas de arquivos
- Familiarizar o aluno com técnicas avançadas de registro e análise de registros, permitindo a reconstrução de eventos em ambientes digitais
- Aprender a aplicar metodologias de investigação forense digital na solução de casos, desde a identificação até a documentação das descobertas
- Familiarizar o aluno com a análise de evidências digitais e a aplicação de técnicas forenses em ambientes de pentesting
- Desenvolver habilidades na preparação de relatórios forenses detalhados e claros, apresentando descobertas e conclusões de forma compreensível
- Promover a colaboração eficaz com as equipes de resposta a incidentes (IR), otimizando a coordenação na investigação e mitigação de ameaças
- Promover práticas éticas e legais em forense digital, garantindo a adesão a regulamentos e padrões de conduta de segurança cibernética

03

Direção do curso

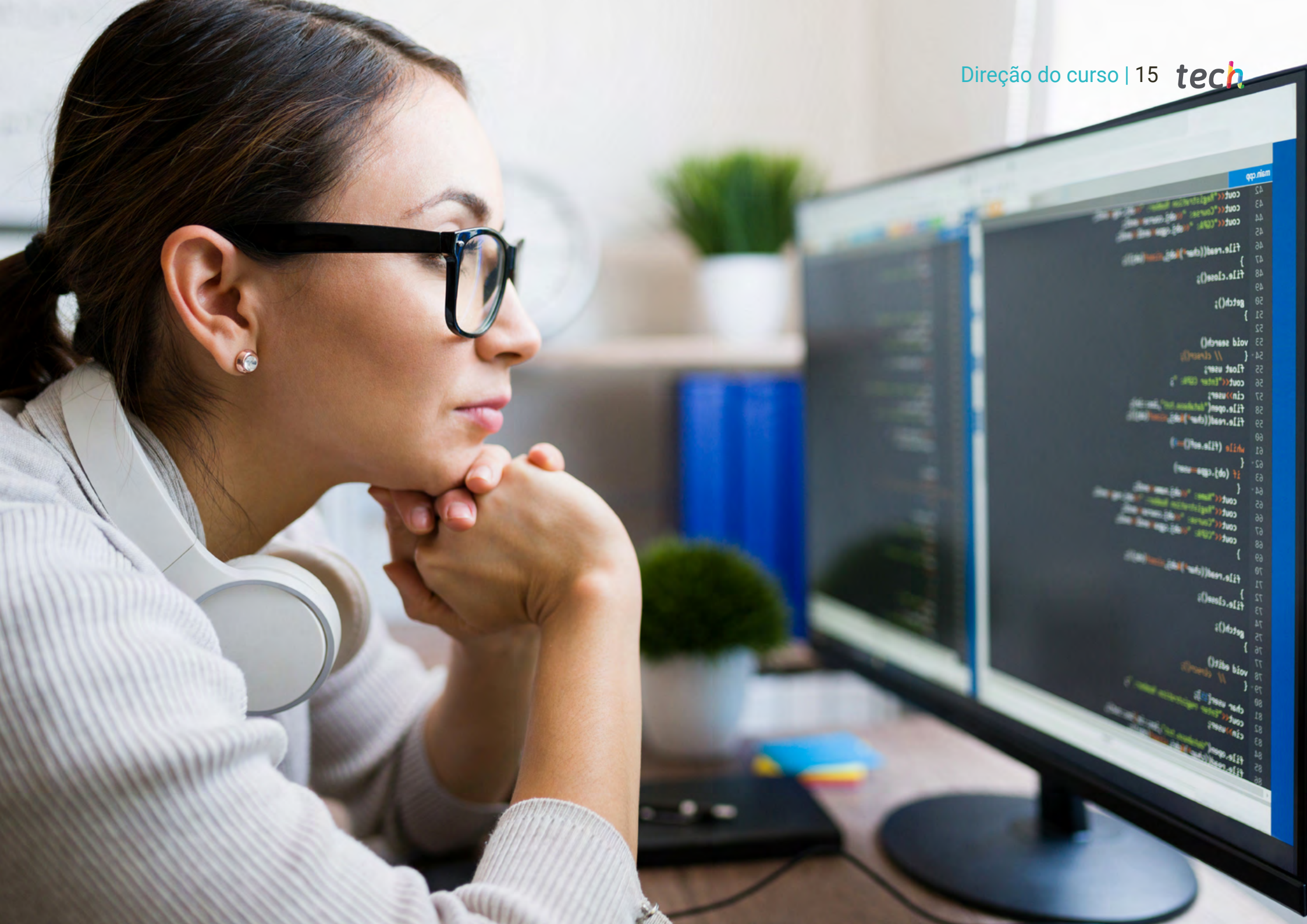
Em seu compromisso de oferecer uma educação baseada na excelência, a TECH conta com profissionais de prestígio internacional. Esses profissionais de segurança cibernética têm uma ampla experiência em segurança cibernética, portanto, essa capacitação oferece as ferramentas mais eficazes para que os alunos adquiram habilidades essenciais de investigação forense digital e resposta a incidentes. Dessa forma, os alunos têm as garantias de que precisam para se especializar em um setor digital que oferece inúmeras oportunidades de emprego.

Tenha acesso a uma biblioteca repleta de recursos multimídia em diferentes formatos audiovisuais"

Direção

Sr. Carlos Gómez Pintado

- Gerente de cibersegurança e Red Team Cipherbit no Grupo Oesía
- Gestor *Advisor & Investor* na Wesson App
- Formado em Engenharia de Software e Tecnologias da Sociedade da Informação pela Universidade Politécnica de Madri
- Colaboração com instituições educacionais para o desenvolvimento de **ciclos de formação de nível superior** em cibersegurança



04

Estrutura e conteúdo

O plano de estudos abrangerá simulações destinadas a responder imediatamente a incidentes cibernéticos, reduzir seus efeitos e restaurar a normalidade operacional. Além disso, o percurso acadêmico aprofunda a análise dos sistemas operacionais mais importantes (Windows, Linux e maCos) para permitir que os alunos recuperem dados de mídias danificadas. A análise de malware para identificar códigos maliciosos e, assim, evitar que as organizações sejam afetadas por vírus, como worms ou cavalos de Troia, também será mais desenvolvida. Dessa forma, os alunos adquirirão um conhecimento sólido de forense digital.

Tenha acesso a uma biblioteca repleta de recursos multimídia em diferentes formatos audiovisuais"

Módulo 1. Fundamentos Forenses e DFIR

1.1. Forense digital
- 1.1.1. História e evolução da computação forense
- 1.1.2. Importância da computação forense na cibersegurança
- 1.1.3. História e evolução da computação forense

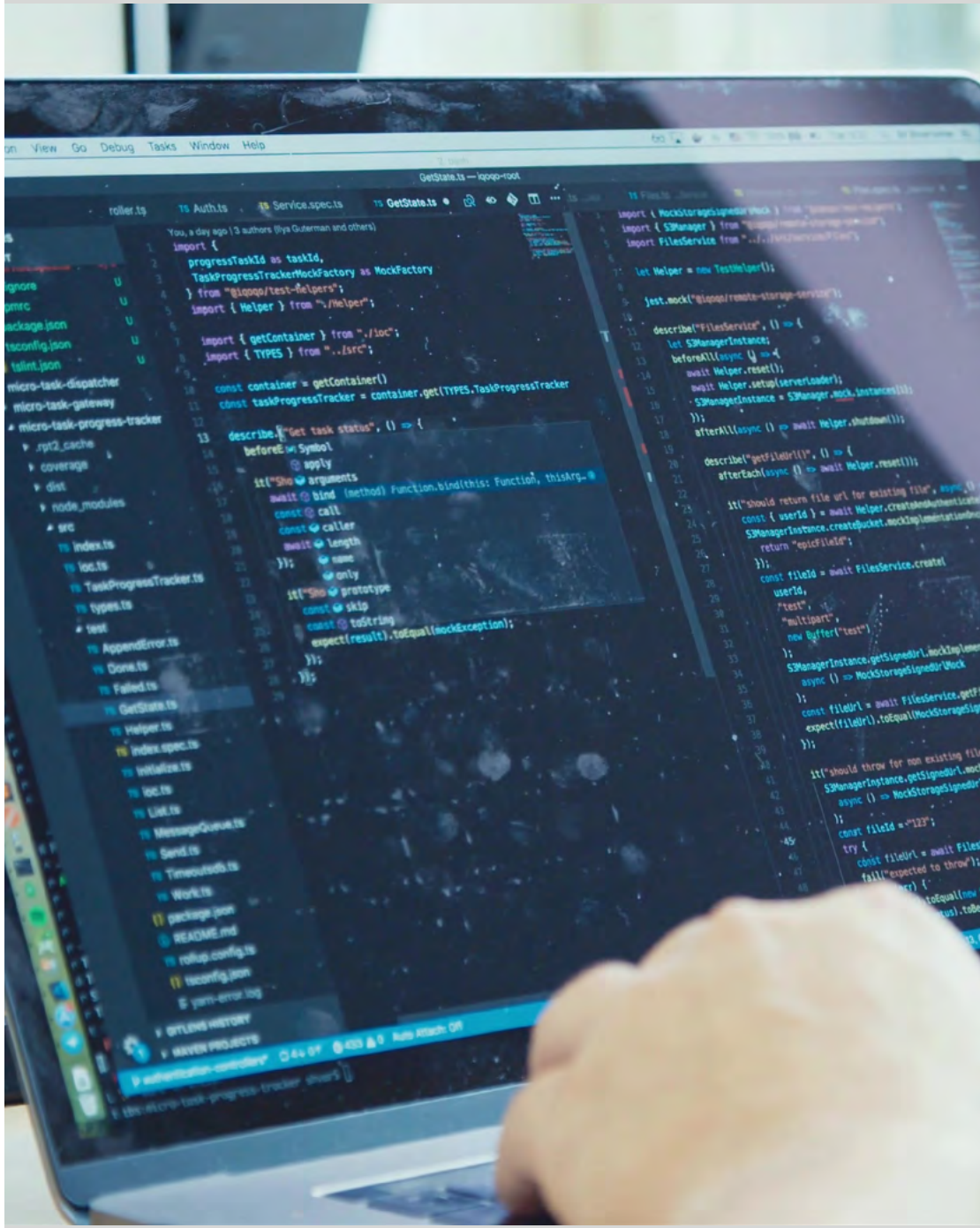
1.2. Fundamentos de informática Forense
- 1.2.1. Cadeia de custódia e sua implementação
- 1.2.2. Tipos de evidência digital
- 1.2.3. Processos de aquisição de evidências

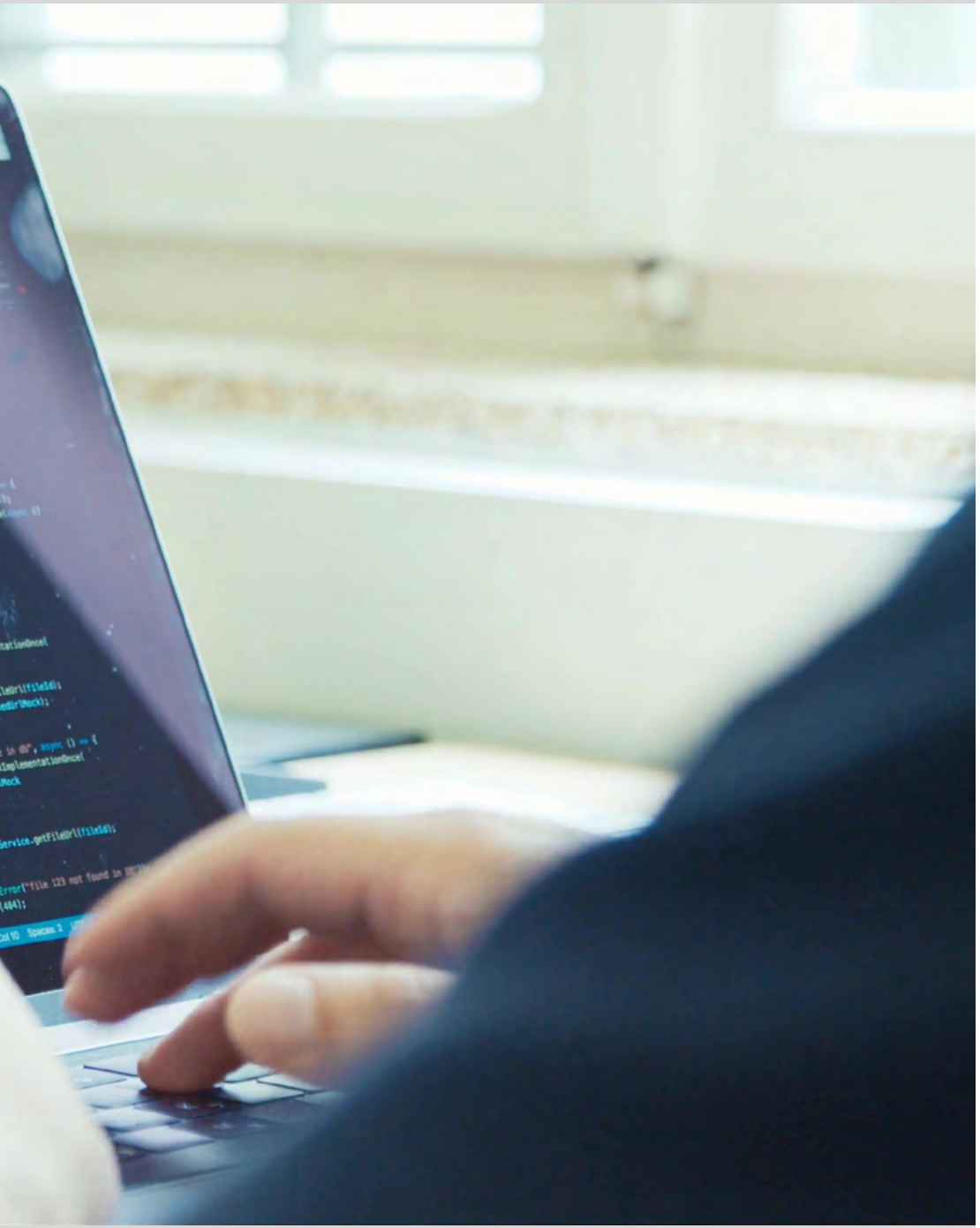
1.3. Sistemas de arquivos e estrutura de dados
- 1.3.1. Principais sistemas de arquivos
- 1.3.2. Métodos de ocultação de dados
- 1.3.3. Análise de metadados e atributos de arquivos

1.4. Análise de sistemas operacionais
- 1.4.1. Análise forense de sistemas Windows
- 1.4.2. Análise forense de sistemas Linux
- 1.4.3. Análise forense de sistemas macOS

1.5. Recuperação de dados e análise de disco
- 1.5.1. Recuperação de dados de mídias danificadas
- 1.5.2. Ferramentas de análise de disco
- 1.5.3. Interpretação de tabelas de alocação de arquivos

1.6. Análise de rede e tráfego
- 1.6.1. Captura e análise de pacotes de rede
- 1.6.2. Análise de registros de firewall
- 1.6.3. Detecção de intrusão de rede





1.7. Análise de malware e código malicioso
- 1.7.1. Classificação de Malware e suas características
- 1.7.2. Análise estática e dinâmica de malware
- 1.7.3. Técnicas de desmontagem e depuração

1.8. Análise de registros e eventos
- 1.8.1. Tipos de registros em sistemas e aplicativos
- 1.8.2. Interpretação de eventos relevantes
- 1.8.3. Ferramentas de análise de registros

1.9. Responder a incidentes de segurança
- 1.9.1. Processo de resposta a incidentes
- 1.9.2. Criação de um plano de resposta a incidentes
- 1.9.3. Coordenação com equipes de segurança

1.10. Apresentação de evidências e aspectos legais
- 1.10.1. Regras de evidência digital no campo jurídico
- 1.10.2. Preparação de relatórios forenses
- 1.10.3. Comparecimento ao julgamento como testemunha especializada

Tenha acesso a uma biblioteca repleta de recursos multimídia em diferentes formatos audiovisuais"

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

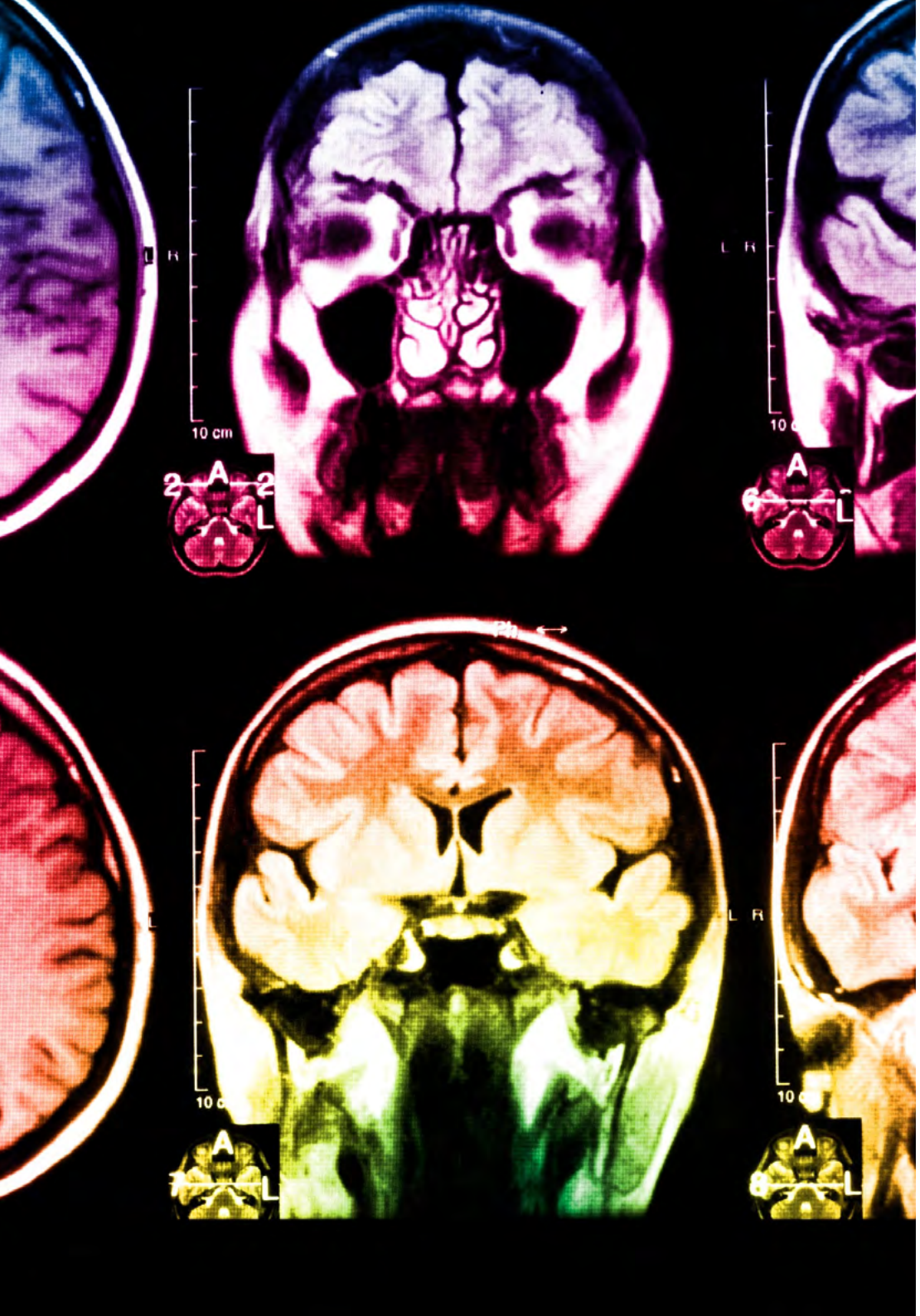
A TECH utiliza de maneira eficaz a metodologia do estudo de caso com um sistema de aprendizagem 100% online, baseado na repetição, combinando elementos didáticos diferentes em cada aula.

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.

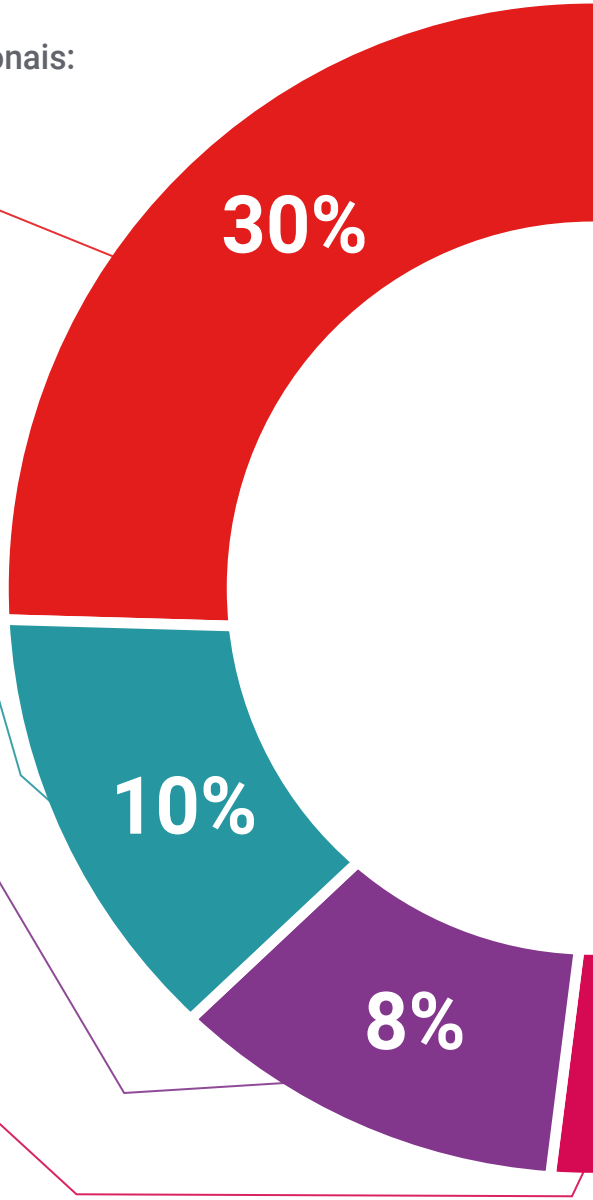
O "Learning from an expert" fortalece o conhecimento e a memória, além de gerar segurança para a tomada de decisões difíceis no futuro.

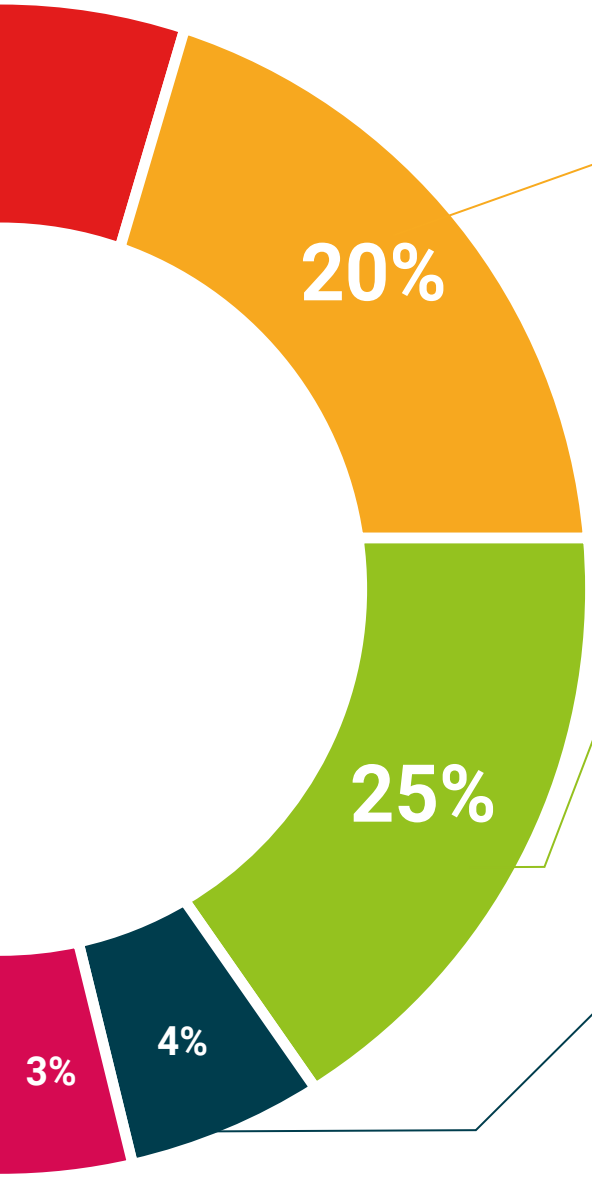
Práticas de habilidades e competências

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 Curso de Fundamentos Forenses e DFIR garante, além da capacitação mais rigorosa e atualizada, acesso ao certificado do Curso 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 **Curso de Fundamentos Forenses e DFIR** conta com o conteúdo mais completo e atualizado do mercado.

Uma vez aprovadas as avaliações, o aluno receberá por correio o certificado* do **Curso** emitido pela **TECH Universidade Tecnológica.**

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

Título: **Curso de Fundamentos Forenses e DFIR**

Modalidade: **online**

Duração: **6 semanas**


tech universidade tecnológica

Outorga o presente

CERTIFICADO

a

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

por ter concluído e aprovado com sucesso o

CURSO

de

Fundamentos Forenses e DFIR

Este é um curso próprio desta Universidade, com duração de 150 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

Curso
Fundamentos Forenses e DFIR

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

Curso

Fundamentos Forenses e DFIR

tech universidade tecnológica