Mestrado Próprio

Gestão de Cibersegurança (CISO, Chief Information Security Officer)

tech universidade tecnológica

tech universidade tecnológica

Mestrado Próprio

Gestão de Cibersegurança (CISO, Chief Information Security Officer)

- Modalidade: **Online**
- Duração: **12 meses**
- Certificação: **TECH Universidade Tecnológica**
- Créditos: **60 ECTS**
- Horário: **Ao seu ritmo**
- Exames: **Online**

Acesso ao site: www.techtitute.com/pt/informatica/mestrado-proprio/mestrado-proprio-gestao-ciberseguranca-ciso-chief-information-security-officer

Índice

01 Apresentação — *pág. 4*

02 Objetivos — *pág. 8*

03 Competências — *pág. 14*

04 Direção do curso — *pág. 18*

05 Estrutura e conteúdo — *pág. 24*

06 Metodologia — *pág. 38*

07 Certificação — *pág. 46*

01

Apresentação

À medida que a tecnologia avança, o mesmo acontece com as ameaças, que aperfeiçoam as suas técnicas de ataque. Por outras palavras, as possibilidades e vias que os cibercriminosos têm para atingir os seus objetivos crescem. É neste contexto que a TECH apresenta uma capacitação com a qual os profissionais poderão atualizar-se, aprendendo de uma forma abrangente a proteger e a assegurar a segurança em vários ambientes digitais. Tudo isto através de uma metodologia revolucionária, o Relearning, e num formato cómodo e totalmente online, que permitirá ao aluno adquirir competências sem um timing pré-estabelecido. Desta forma, após a conclusão deste Mestrado Próprio, o profissional obterá as aptidões e competências necessárias para exercer eficazmente o cargo de Chief Information Security Officer, um cargo de gestão de topo de alto prestígio e com grandes perspetivas de crescimento e expansão.

À medida que a tecnologia e a conectividade avançam, o mesmo acontece com o número e forma de potenciais ameaças. É por isso que é crucial que os futuros Chief Information Security Officer atualizem os seus conhecimentos para oferecer soluções mais adaptadas às idiossincrasias da empresa"

Não é segredo que nos encontramos em plena era da informação e comunicação, uma vez que estamos todos ligados tanto em casa como em ambientes empresariais. Assim, temos acesso a uma infinidade de informações com um simples clique, com uma simples pesquisa em qualquer um dos motores à nossa disposição, seja a partir de um smartphone, de um computador pessoal ou de trabalho. Neste contexto, "tempo é dinheiro", mas a informação também o é.

À medida que a tecnologia avança para o cidadão e trabalhador comum, o mesmo acontece com as ameaças e técnicas de ataque. Quanto mais novas funcionalidades existirem e quanto mais comunicarmos, mais aumenta a superfície de ataque. Por outras palavras, as possibilidades e vias que os cibercriminosos têm para atingir os seus objetivos crescem.

Perante este contexto preocupante, a TECH lança este Mestrado Próprio em Gestão da Cibersegurança (CISO, Chief Information Security Officer), que foi desenvolvido por uma equipa com diferentes perfis profissionais especializados em diferentes setores, que combinam a experiência profissional internacional no setor privado em I&D&I e uma vasta experiência de ensino. Por conseguinte, não só estão atualizados em relação a todas as tecnologias, como também têm uma perspetiva das necessidades futuras do setor e apresentam-nas de forma didática.

O Mestrado Próprio engloba as diferentes disciplinas nucleares na área da cibersegurança, cuidadosamente selecionadas para cobrir com rigor um amplo espectro de tecnologias aplicáveis em diferentes áreas de trabalho. Mas também tratará de outro ramo de matérias que normalmente escasseiam no catálogo académico de outras instituições e que alimentarão profundamente o currículo do profissional. Desta forma, e graças aos conhecimentos transversais oferecidos pela TECH com este Mestrado Próprio, o aluno adquirirá as competências para trabalhar como gestor na área da cibersegurança (Chief Information Security Officer), aumentando assim as suas perspetivas de crescimento pessoal e profissional.

Este **Mestrado Próprio em Gestão de Cibersegurança (CISO, Chief Information Security Officer)** conta com o conteúdo educativo completo e atualizado do mercado. As suas principais características são:

- O desenvolvimento de casos práticos apresentados por especialistas em cibersegurança
- Os conteúdos gráficos, esquemáticos e essencialmente práticos fornecem informações científicas e práticas sobre as disciplinas essenciais para a atividade profissional
- Os exercícios práticos em que o processo de autoavaliação pode ser utilizado para melhorar a aprendizagem
- A sua ênfase especial nas metodologias inovadoras
- As lições teóricas, perguntas a especialistas, fóruns de discussão sobre questões controversas e atividades de reflexão individual
- A disponibilidade de acesso aos conteúdos a partir de qualquer dispositivo fixo ou portátil com ligação à Internet

Prepare-se para exercer, como Chief Information Security Officer, um perfil-chave na empresa devido ao seu papel de protetor da segurança informática"

Destaque-se num setor em crescimento e torne-se num especialista em cibersegurança com este Mestrado Próprio da TECH. É o mais completo do mercado"

As formas como as pessoas trocam informações estão a evoluir rapidamente. Isto exige novas formas de ciberproteção para os profissionais.

Um Mestrado Próprio 100% online com uma abordagem essencialmente prática que lançará as bases para o seu crescimento profissional.

O corpo docente do Mestrado Próprio inclui profissionais do setor que trazem a sua experiência profissional para esta capacitação, para além de especialistas reconhecidos de sociedades de referência e universidades de prestígio.

Os seus conteúdos multimédia, desenvolvidos com a mais recente tecnologia educativa, permitirão ao profissional uma aprendizagem situada e contextual, ou seja, um ambiente simulado que proporcionará uma capacitação imersiva programada para praticar em situações reais.

A estrutura deste Mestrado Próprio centra-se na Aprendizagem Baseada em Problemas, na qual o profissional deve tentar resolver as diferentes situações de prática profissional que surgem durante a especialização. Para tal, contará com a ajuda de um sistema inovador de vídeos interativos criados por especialistas reconhecidos.

02

Objetivos

Tendo plena consciência da relevância da cibersegurança para as empresas, a TECH desenvolveu este Mestrado Próprio que visa nutrir e atualizar os conhecimentos dos profissionais na deteção, proteção e prevenção do cibercrime. Desta forma, o aluno tornar-se-á num ator fundamental no cuidado dos dados e da informação, minimizando a possibilidade dos criminosos tirarem partido das falhas de segurança existentes. Uma competência profissional que na TECH, em apenas 12 meses, o profissional poderá adquirir.

Esta é uma oportunidade única para realizar os seus sonhos e objetivos e tornar-se num especialista em cibersegurança"

Objetivos gerais

- Analisar o papel do analista de cibersegurança
- Aprofundar a compreensão da engenharia social e dos seus métodos
- Analisar as metodologias OSINT, HUMINT, OWASP, PTEC, OSSTM e OWISAM
- Efetuar análises de risco e compreender os indicadores de risco
- Determinar a utilização adequada do anonimato e de redes como a TOR, a I2P e a Freenet
- Gerar conhecimentos especializados para efetuar uma auditoria de segurança
- Desenvolver políticas de utilização adequadas
- Analisar os sistemas de deteção e prevenção das ameaças mais importantes
- Avaliar os novos sistemas de deteção de ameaças e a sua evolução em relação às soluções mais tradicionais
- Analisar as principais plataformas móveis atuais, as suas características e utilização
- Identificar, analisar e avaliar os riscos de segurança das partes do projeto IoT
- Avaliar a informação obtida e desenvolver mecanismos de prevenção e *hacking*
- Aplicar a engenharia inversa ao ambiente de cibersegurança
- Especificar os testes a realizar ao software desenvolvido
- Recolher todas as provas e dados existentes para levar a cabo um relatório forense
- Apresentar devidamente o relatório forense
- Analisar o estado atual e futuro da segurança informática
- Analisar os riscos das novas tecnologias emergentes
- Compilar as diferentes tecnologias em relação à segurança informática

Objetivos específicos

Módulo 1. Ciberinteligência e Cibersegurança

- Desenvolver as metodologias utilizadas em matéria de cibersegurança
- Examinar o ciclo de inteligência e estabelecer a sua aplicação na ciberinteligência
- Determinar o papel do analista de informações e os obstáculos à atividade de evacuação
- Analisar as metodologias OSINT, OWISAM, OSSTM, PTES e OWASP
- Estabelecer as ferramentas mais comuns para a produção de informações
- Efetuar uma análise de risco e compreender as métricas utilizadas
- Concretizar as opções de anonimato e a utilização de redes como TOR, I2P, Freenet
- Detalhar os regulamentos vigentes em cibersegurança

Módulo 2. Segurança do Host

- Executar as políticas de *backup* de dados pessoais e profissionais
- Apreciar as diferentes ferramentas para fornecer soluções para problemas específicos de segurança
- Estabelecer mecanismos para manter o sistema atualizado
- Analisar o equipamento para detetar intrusos
- Determinar as regras de acesso ao sistema
- Analisar e classificar o correio para evitar fraudes
- Gerar listas de softwares permitidos

Módulo 3. Segurança da Rede (Perimetral)

- Analisar as arquiteturas de rede atuais para identificar o perímetro a proteger
- Desenvolver as configurações específicas de *firewall* e Linux para mitigar os ataques mais comuns
- Compilar as soluções mais utilizadas, como o Snort e o Suricata, bem como a sua configuração
- Examinar as diferentes camadas adicionais fornecidas pelas *firewalls* de nova geração e as funcionalidades de rede em ambientes de *Cloud*
- Identificar ferramentas de proteção da rede e demonstrar por que razão são fundamentais para uma defesa de múltiplas camadas

Módulo 4. Segurança de Smartphones

- Examinar os diferentes vetores de ataque para evitar tornar-se um alvo fácil
- Determinar os principais tipos de ataque e *malware* a que os utilizadores de dispositivos móveis estão expostos
- Analisar os dispositivos mais recentes para estabelecer uma configuração mais segura
- Especificar os principais passos para efetuar um teste de penetração nas plataformas iOS e Android
- Desenvolver conhecimentos especializados sobre diferentes ferramentas de proteção e segurança
- Estabelecer as melhores práticas em programação orientada a dispositivos móveis

Módulo 5. Segurança da IoT

- Analisar as principais arquiteturas de IoT
- Examinar as tecnologias de conectividade
- Desenvolver os principais protocolos de aplicação
- Especificar os diferentes tipos de dispositivos existentes
- Avaliar os níveis de risco e as vulnerabilidades conhecidas
- Desenvolver políticas de utilização segura
- Estabelecer condições de utilização adequadas para estes dispositivos

Módulo 6. Hacking Ético

- Análise dos métodos OSINT
- Recolher informações disponíveis nos meios de comunicação social públicos
- Fazer scan das redes para obter informação de modo ativo
- Desenvolver laboratórios de teste
- Analisar as ferramentas para o desempenho do *pentesting*
- Catalogar e avaliar as diferentes vulnerabilidades dos sistemas
- Especificar as diferentes metodologias de *hacking*

Módulo 7. Engenharia Inversa

- Analisar as fases de um compilador
- Examinar a arquitetura de processadores x86 e a arquitetura de processadores ARM
- Determinar os diferentes tipos de análise
- Aplicar *sandboxing* em diferentes ambientes
- Desenvolver as diferentes técnicas de análise de *malware*
- Estabelecer as ferramentas orientadas para a análise de *malware*

Módulo 8. Desenvolvimento Seguro

- Estabelecer os requisitos necessários para o correto funcionamento de uma aplicação de forma segura
- Examinar ficheiros de registo para compreender as mensagens de erro
- Analisar os diferentes eventos e decidir o que mostrar ao utilizador e o que guardar nos registos
- Gerar um código de qualidade limpo e facilmente verificável
- Avaliar a documentação adequada para cada fase do desenvolvimento

- Especificar o comportamento do servidor para otimizar o sistema
- Desenvolver código modular, reutilizável e de fácil manutenção

Módulo 9. Análise Forense

- Identificar os diferentes elementos que revelam um crime
- Gerar conhecimentos especializados para obter dados de diferentes meios de comunicação antes que estes se percam
- Recuperação de dados eliminados intencionalmente
- Analisar os registos dos sistemas
- Determinar como são duplicados os dados de modo a não alterar os originais
- Fundamentar as provas para que sejam consistentes
- Gerar um relatório sólido e sem falhas
- Apresentar as conclusões de forma coerente
- Estabelecer como defender o relatório perante a autoridade competente
- Concretizar estratégias para um teletrabalho seguro

Módulo 10. Desafios Atuais e Futuros em Matéria de Segurança Informática

- Analisar a utilização de criptomoedas, o impacto na economia e na segurança
- Analisar a situação dos utilizadores e o nível de iliteracia digital
- Determinar o âmbito de utilização de *blockchain*
- Apresentar alternativas ao IPv4 no endereçamento de redes
- Desenvolver estratégias para formar a população na utilização correta das tecnologias
- Gerar conhecimentos especializados para enfrentar novos desafios de segurança e evitar a usurpação de identidade
- Concretizar estratégias para um teletrabalho seguro

03

Competências

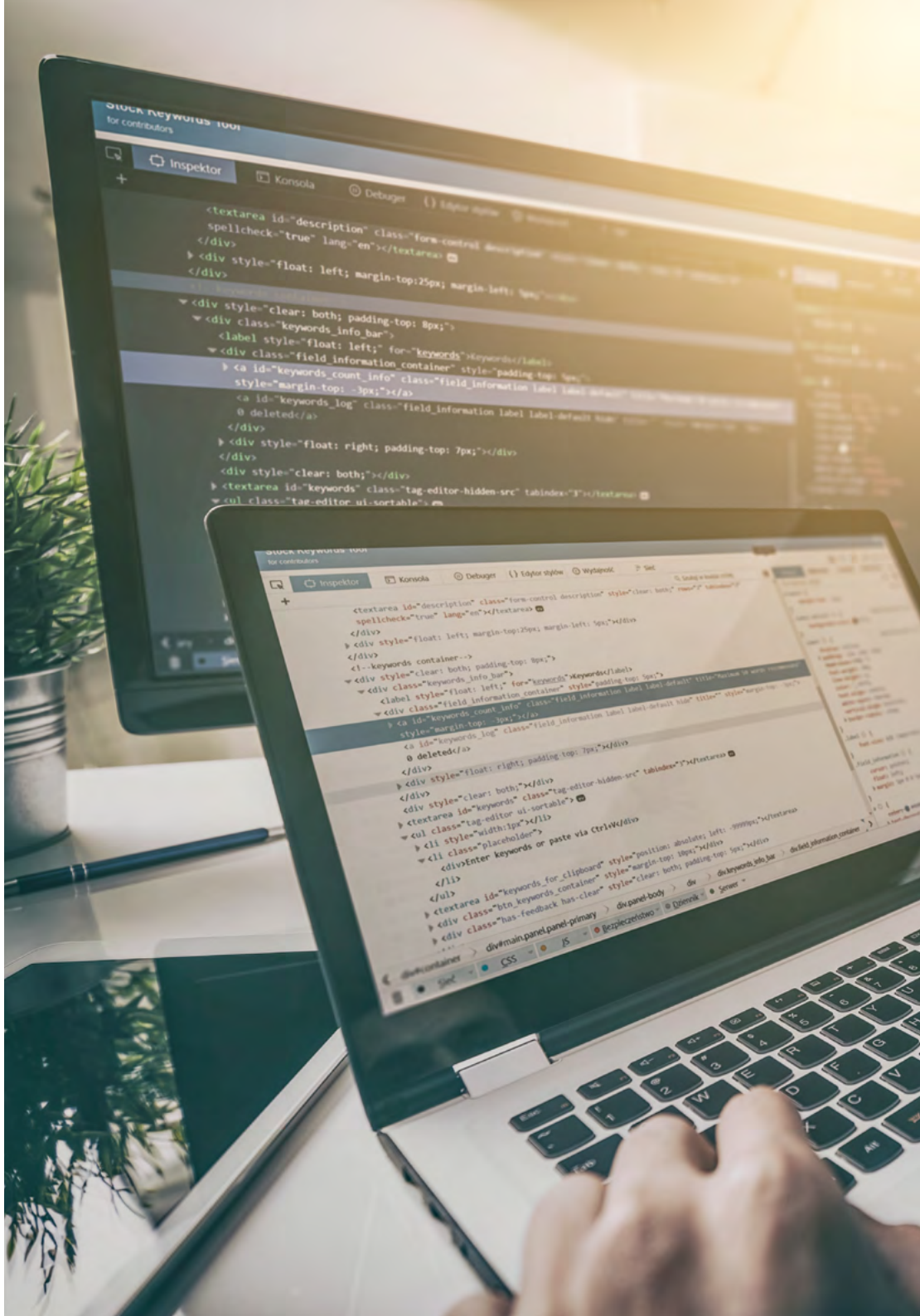
Após a conclusão do processo de avaliação deste Mestrado Próprio, o profissional terá adquirido uma série de conhecimentos, ferramentas e competências que lhe permitirão trabalhar neste setor com maiores garantias de sucesso. Desta forma, o aluno não só se tornará num especialista em cibersegurança, como também contribuirá positivamente para a redução da cibercriminalidade através da criação de uma rede mais segura e mais forte para todos. Chegar a cargos de gestão sénior como Chief Information Security Officer.

O setor da cibersegurança exige uma atualização constante dos conhecimentos. Com capacitações como esta, o profissional consegue-o de forma rápida e eficaz"

Competências gerais

- Conhecer as metodologias utilizadas em matéria de cibersegurança
- Saber avaliar cada tipo de ameaça para oferecer uma solução ótima em cada caso
- Ser capaz de gerar soluções inteligentes e completas para automatizar o comportamento em caso de incidentes
- Avaliar os riscos associados às vulnerabilidades, tanto fora como dentro da empresa
- Compreender a evolução e o impacto da IoT ao longo do tempo
- Ser capaz de demonstrar que um sistema é vulnerável, atacá-lo de forma pró-ativa e resolver esses problemas
- Saber aplicar *sandboxing* em diferentes ambientes
- Conhecer as diretrizes que um bom programador deve seguir para cumprir os requisitos de segurança necessários

Melhorar as suas competências num serviço para todos irá impulsionar a sua carreira e vida pessoal"



Competências específicas

- Saber conduzir operações de segurança defensiva
- Ter uma perceção profunda e especializada sobre segurança informática
- Possuir conhecimentos especializados no domínio da cibersegurança e ciberinteligência
- Ter um conhecimento profundo de aspetos fundamentais como o ciclo de inteligência, fontes de inteligência, engenharia social, metodologia OSINT, HUMINT, anonimização, análise de riscos e metodologias existentes (OWASP, OWISAM, OSSTM e PTES)
- Compreender a importância de conceber uma defesa de várias camadas, também conhecida como "Defense in Depth", abrangendo todos os aspetos de uma rede empresarial, onde alguns dos conceitos e sistemas que serão discutidos também podem ser utilizados e aplicados num ambiente doméstico
- Aplicar processos de segurança para smartphones e dispositivos portáteis
- Conhecer os meios para levar a cabo o chamado *hacking* ético e proteger uma empresa de um ataque cibernético
- Ser capaz de investigar um incidente de cibersegurança
- Conhecer as diferentes técnicas de ataque e defesa disponíveis
- Analisar o papel do Analista de Cibersegurança
- Compreender como funciona a engenharia social e os seus métodos

04

Direção do curso

O Mestrado Próprio em Gestão de Cibersegurança (CISO, Chief Information Security Officer) foi desenvolvido por uma equipa de pessoas com diferentes perfis profissionais especializados em diferentes setores, que combinam a experiência profissional internacional no setor privado em I&D&I e uma vasta experiência docente. Por conseguinte, não só estão atualizados em relação a todas as tecnologias, como também têm uma perspetiva das necessidades futuras do setor e apresentam-nas de forma didática. Desta forma, o profissional tem a certeza de aprender com os melhores do setor com a garantia de possuir os conhecimentos mais atualizados.

Durante o Mestrado Próprio, será acompanhado por uma série de profissionais especializados que tornarão a sua experiência educativa única"

Diretor Convidado Internacional

O Doutor Frederic Lemieux é reconhecido internacionalmente como um especialista inovador e líder inspirador nos domínios da **Inteligência**, **Segurança Nacional**, **Segurança Interna**, **Cibersegurança e Tecnologias Disruptivas**. A sua dedicação constante e contributos relevantes para a investigação e educação posicionam-no como uma figura-chave na promoção da segurança e na compreensão das tecnologias emergentes atualmente. Durante a sua carreira profissional, concebeu e liderou programas académicos de vanguarda em várias instituições de renome, como a **Universidade de Montreal**, a **Universidade George Washington** e a **Universidade de Georgetown**.

Ao longo da sua vasta carreira, publicou vários livros importantes, todos relacionados com a **informação criminal**, **o policiamento**, **as ciberameaças e a segurança internacional**. Também contribuiu significativamente para o domínio da cibersegurança, publicando inúmeros artigos em revistas académicas sobre o controlo da criminalidade durante grandes catástrofes, a luta contra o terrorismo, as agências de informação e a cooperação policial. Além disso, foi orador de painel e orador principal em várias conferências nacionais e internacionais, estabelecendo-se como uma referência no domínio académico e profissional.

O Doutor Lemieux desempenhou funções editoriais e de avaliação em várias organizações académicas, privadas e governamentais, o que reflete a sua influência e o seu compromisso com a excelência na sua área de especialização. Como tal, a sua prestigiada carreira académica levou-o a desempenhar as funções de Professor de Estágios e Diretor do Corpo Docente dos programas MPS em **Inteligência Aplicada**, **Gestão de Riscos de Cibersegurança**, **Gestão Tecnológica e Gestão de Tecnologias da Informação** na **Universidade de Georgetown**.

Doutor Lemieux, Frederic

- Investigador em Inteligência, Cibersegurança e Tecnologias Disruptivas, na Universidade de Georgetown
- Diretor do Mestrado em Information Technology Management na Universidade de Georgetown
- Diretor do Mestrado em Technology Management na Universidad de Georgetown
- Diretor do Mestrado em Cybersecurity Risk Management na Universidad de Georgetown
- Diretor do Mestrado em Applied Intelligence na Universidad de Georgetown
- Professor de Estágios na Universidade de Georgetown
- Doutoramento em Criminologia pela School of Criminology, na Universidade de Montreal
- Licenciatura em Sociologia, Minor Degree em Psicologia, pela Universidade de Laval
- Membro de:
  - New Program Roundtable Committee, pela Universidade de Georgetown

Graças à TECH, poderá aprender com os melhores profissionais do mundo"

Direção

Dra. Sonia Fernández Sapena

- Formadora em Segurança Informática e Hacking Ético no Centro de Referencia Nacional en Informática y Telecomunicaciones
- Instrutora certificada no E-Council
- Formadora nas seguintes certificações: EXIN Ethical Hacking Foundation e EXIN Cyber & IT Security Foundation, Madrid
- Formadora especializada certificada pela CAM para os seguintes certificados de profissionalização: Segurança Informática (IFCT0190), Gestão de Redes de Voz e Dados (IFCM0310), Administração de Redes Departamentais (IFCT0410), Gestão 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 de las Islas Baleares
- Engenheira Informática pela Universidade de Alcalá de Henares de Madrid
- Mestrado em DevOps: Docker e Kubernetes pela CAS Training
- Microsoft Azure Security Technologies, E-Council

Professores

Dr. Jesús Serrano Redondo

- Programador Web e Técnico de Cibersegurança
- Programador Web na Roams, Palencia
- Programador FrontEnd na Telefónica, Madrid
- Programador FrontEnd na Best Pro Consulting SL, Madrid
- Instalador de equipamentos e serviços de telecomunicações no Grupo Zener, Castilla y León
- Instalador de equipamentos e serviços de telecomunicações na Lican Comunicaciones SL, Castilla y León
- Certificado em Segurança Informática pelo CFTIC Getafe, Madrid
- Técnico Superior: Sistemas de Telecomunicações e Informáticos na IES Trinidad Arroyo, Palencia
- Técnico Superior: Instalações Eletrotécnicas de MT e BT na IES Trinidad Arroyo, Palencia
- Formação em Engenharia Inversa, Estenografia, Encriptação na Academia Hacker Incibe (Talentos Incibe)

Dr. Álvaro Jiménez Ramos

- Analista de Cibersegurança
- Analista Sénior de Segurança na The Workshop
- Analista de Cibersegurança L1 na Axians
- Analista de Cibersegurança L2 na Axians
- Analista de Cibersegurança na SACYR S.A.
- Licenciatura em Engenharia Telemática pela Universidade Politécnica de Madrid
- Mestrado em Cibersegurança e Hacking Ético pelo CICE
- Curso Superior em Cibersegurança pela Deusto Formación

Dra. Victoria Alicia Marcos Sbarbaro

- Programadora de Aplicações Móveis Android Nativas na B60, UK
- Programadora Analista para a gestão, coordenação e documentação de um ambiente virtualizado de alarmes de segurança
- Programadora Analista de aplicações Java para caixas multibanco
- Profissional de Programação de Software para aplicação de validação de assinaturas e gestão de documentos
- Técnica de Sistemas para a migração de equipamentos e para a gestão, manutenção e formação de dispositivos móveis PDAs
- Engenharia Técnica em Informática de Sistemas pela Universidade Oberta de Cataluña
- Mestrado em Segurança Informática e Hacking Ético Oficial EC- Council e CompTIA pela Escola Profissional de Nuevas Tecnologías CICE

Dr. Jon Peralta Alonso

- Consultor Sénior - Proteção de Dados e Cibersegurança, Altia
- Advogado/Consultor Jurídico na Arriaga Asociados Asesoramiento Jurídico y Económico, S.L. Consultor Jurídico/Estagiário Escritório profissional: Oscar Padura
- Licenciatura em Direito, Universidade Pública del País Vasco
- Mestrado em Delegado de Proteção de Dados pela EIS Innovative School
- Mestrado em Advocacia pela Universidade Pública del País Vasco
- Mestrado de Especialidade em Prática Processual Civil pela Universidade Internacional Isabel I de Castilla
- Professor no Mestrado em Proteção de Dados Pessoais, Cibersegurança e Direito das TIC

Dr. José Francisco Catalá Barba

- Técnico de Eletrónica Especialista em Cibersegurança
- Programador de aplicações para dispositivos móveis
- Técnico de Eletrónica, Chefia Intermédia no Ministério da Defesa Espanhol
- Técnico de Eletrónica na fábrica da Ford em Almusafes, Valência

Uma experiência de capacitação única, fundamental e decisiva para impulsionar o seu desenvolvimento profissional"

05

Estrutura e conteúdo

Para garantir que o aluno adquira os conhecimentos mais rigorosos e de vanguarda em matéria de cibersegurança, a TECH concebeu uma série de materiais que reúnem as últimas atualizações da profissão. Estes conteúdos foram concebidos por um grupo de especialistas na matéria, pelo que estão adaptados às necessidades atuais dos postos de trabalho oferecidos no setor. Uma oportunidade única e altamente profissional que catapultará os alunos para o sucesso no seu desenvolvimento profissional.

Um plano de estudos de alto nível, concebido por e para profissionais de alto nível. Vai perder esta oportunidade?"

Módulo 1. Ciberinteligência e Cibersegurança

1.1. Ciberinteligência
- 1.1.1. Ciberinteligência
  - 1.1.1.1. A inteligência
    - 1.1.1.1.1. Ciclo de inteligência
  - 1.1.1.2. Ciberinteligência
  - 1.1.1.3. Ciberinteligência e Cibersegurança
- 1.1.2. O analista de inteligência
  - 1.1.2.1. O papel do analista de inteligência
  - 1.1.2.2. Os preconceitos do analista de inteligência na atividade de avaliação

1.2. Cibersegurança
- 1.2.1. As camadas de segurança
- 1.2.2. Identificação das ciberameaças
  - 1.2.2.1. Ameaças externas
  - 1.2.2.2. Ameaças internas
- 1.2.3. Ações adversas
  - 1.2.3.1. Engenharia social
  - 1.2.3.2. Métodos mais utilizados

1.3. Técnicas e ferramentas de inteligência
- 1.3.1. OSINT
- 1.3.2. SOCMINT
- 1.3.3. Humit
- 1.3.4. Distribuições Linux e ferramentas
- 1.3.5. OWISAM
- 1.3.6. OWASP
- 1.3.7. PTES
- 1.3.8. OSSTMM

1.4. Metodologias de avaliação
- 1.4.1. A análise de inteligência
- 1.4.2. Técnicas de organização da informação adquirida
- 1.4.3. Fiabilidade e credibilidade das fontes de informação
- 1.4.4. Metodologias de análise
- 1.4.5. Análise dos resultados da inteligência

1.5. Auditorias e documentação
- 1.5.1. A auditoria na segurança informática
- 1.5.2. Documentação e autorizações de auditoria
- 1.5.3. Tipos de auditoria
- 1.5.4. Relatórios de conclusão
  - 1.5.4.1. Relatório técnico
  - 1.5.4.2. Relatório executivo

1.6. O anonimato na Internet
- 1.6.1. Utilização do anonimato
- 1.6.2. Técnicas de anonimato (Proxy, VPN)
- 1.6.3. Redes TOR, Freenet e IP2

1.7. Ameaças e tipos de segurança
- 1.7.1. Tipos de ameaças
- 1.7.2. Segurança física
- 1.7.3. Segurança na Internet
- 1.7.4. Segurança lógica
- 1.7.5. Segurança em aplicações Web
- 1.7.6. Segurança em dispositivos móveis

1.8. Regulamentos e *compliance*
- 1.8.1. RGPD
- 1.8.3. Família ISO 27000
- 1.8.4. Quadro de cibersegurança do NIST
- 1.8.5. PIC
- 1.8.6. ISO 27032
- 1.8.7. Regulamentos Cloud
- 1.8.8. SOX
- 1.8.9. PCI

1.9. Análise de riscos e métricas
- 1.9.1. Âmbito dos riscos
- 1.9.2. Os ativos
- 1.9.3. As ameaças
- 1.9.4. As vulnerabilidades
- 1.9.5. Avaliação do risco
- 1.9.6. Tratamento do risco

1.10. Organismos importantes em matéria de cibersegurança
- 1.10.1. NIST
- 1.10.2. ENISA
- 1.10.4. OEA
- 1.10.5. UNASUR PROSUR

Módulo 2. Segurança do Host

2.1. Cópias de segurança
- 2.1.1. Estratégias para as cópias de segurança
- 2.1.2. Ferramentas para Windows
- 2.1.3. Ferramentas para Linux
- 2.1.4. Ferramentas para macOS

2.2. Antivírus do utilizador
- 2.2.1. Tipos de antivírus
- 2.2.2. Antivírus para Windows
- 2.2.3. Antivírus para Linux
- 2.2.4. Antivírus para macOS
- 2.2.5. Antivírus para smartphones

2.3. Detetores de intrusos HIDS
- 2.3.1. Métodos de deteção de intrusos
- 2.3.2. Sagan
- 2.3.3. Aide
- 2.3.4. *Rkhunter*

2.4. *Firewall* local
- 2.4.1. *Firewalls* para Windows
- 2.4.2. *Firewalls* para Linux
- 2.4.3. *Firewalls* para macOS

2.5. Gestores de palavras-passe
- 2.5.1. Password
- 2.5.2. *LastPass*
- 2.5.3. *KeePass*
- 2.5.4. *Sticky Password*
- 2.5.5. RoboForm

2.6. Detetores de *phishing*
- 2.6.1. Deteção de *phishing* manual
- 2.6.2. Ferramentas *antiphishing*

2.7. *Spyware*
- 2.7.1. Mecanismos de prevenção
- 2.7.2. Ferramentas *antispyware*

2.8. Rastreadores
- 2.8.1. Medidas de proteção do sistema
- 2.8.2. Ferramentas antirrastreamento

2.9. *EDR - Endpoint Detection and Response*
- 2.9.1. Comportamento do sistema EDR
- 2.9.2. Diferenças entre EDR e antivírus
- 2.9.3. O futuro dos sistemas EDR

2.10. Controlo sobre a instalação de software
- 2.10.1. Repositórios e lojas de software
- 2.10.2. Listas de softwares permitidos ou proibidos
- 2.10.3. Critérios de atualizações
- 2.10.4. Privilégios para instalar software

Módulo 3. Segurança da Rede (Perimetral)

3.1. Sistemas de deteção e prevenção de ameaças
- 3.1.1. Quadro geral dos incidentes de segurança
- 3.1.2. Sistemas de defesa atuais: defesa em profundidade e SOC
- 3.1.3. Arquiteturas de rede atuais
- 3.1.4. Tipos de ferramentas para a deteção e prevenção de incidentes
  - 3.1.4.1. Sistemas baseados na Internet
  - 3.1.4.2. Sistemas baseados em *Host*
  - 3.1.4.3. Sistemas centralizados
- 3.1.5. Comunicação e deteção de instâncias/*hosts*, contentores e *serverless*

3.2. *Firewall*
- 3.2.1. Tipos de *Firewalls*
- 3.2.2. Ataques e mitigação
- 3.2.3. *Firewalls* comuns em *Kernel* Linux
  - 3.2.3.1. UFW
  - 3.2.3.2. *Nftables* e *iptables*
  - 3.2.3.3. *Firewalld*
- 3.2.4. Sistemas de deteção baseados nos registos do sistema
  - 3.2.4.1. TCP *wrappers*
  - 3.2.4.2. *BlockHosts* e *DenyHosts*
  - 3.2.4.3. Fail2Ban

3.3. Sistemas de deteção e prevenção de intrusões (IDS/IPS)
- 3.3.1. Ataques sobre IDS/IPS
- 3.3.2. Sistemas de IDS/IPS
  - 3.3.2.1. *Snort*
  - 3.3.2.2. Suricata

3.4. *Firewalls* da próxima geração (NGFW)
- 3.4.1. Diferenças entre NGFW e *firewalls* tradicionais
- 3.4.2. Principais capacidades
- 3.4.3. Soluções comerciais
- 3.4.4. *Firewalls* para serviços de *Cloud*
  - 3.4.4.1. Arquitetura *Cloud* VPC
  - 3.4.4.2. *Cloud* ACLs
  - 3.4.4.3. *Security group*

3.5. *Proxy*
- 3.5.1. Tipos de *Proxy*
- 3.5.2. Utilização de *Proxy*. Vantagens e desvantagens

3.6. Motores de antivírus
- 3.6.1. Contexto geral do *malware* e IOCs
- 3.6.2. Problemas dos motores de antivírus

3.7. Sistemas de proteção de correio
- 3.7.1. Antispam
  - 3.7.1.1. Listas brancas e negras
  - 3.7.1.2. Filtros bayesianos
- 3.7.2. *Mail Gateway* (MGW)

3.8. SIEM
- 3.8.1. Componentes e arquitetura
- 3.8.2. Regras de correlação e casos de utilização
- 3.8.3. Desafios atuais dos sistemas SIEM

3.9. SOAR
- 3.9.1. SOAR e SIEM: inimigos ou aliados
- 3.9.2. O futuro dos sistemas SOAR

3.10. Outros sistemas baseados na Internet
- 3.10.1. WAF
- 3.10.2. NAC
- 3.10.3. *Honeypots* e *Honeynets*
- 3.10.4. CASB

Módulo 4. Segurança de Smartphones

4.1. O mundo do dispositivo móvel
- 4.1.1. Tipos de plataformas móveis
- 4.1.2. Dispositivos iOS
- 4.1.3. Dispositivos Android

4.2. Gestão da segurança móvel
- 4.2.1. Projeto de segurança móvel OWASP
  - 4.2.1.1. Top 10 vulnerabilidades
- 4.2.2. Comunicações, redes e modos de conexão

4.3. O dispositivo móvel no meio empresarial
- 4.3.1. Riscos
- 4.3.3. Monitorização de dispositivos
- 4.3.4. Gestão de Dispositivos Móveis (MDM)

4.4. Privacidade do utilizador e segurança dos dados
- 4.4.1. Estados da informação
- 4.4.3. Armazenamento seguro dos dados
  - 4.4.3.1. Armazenamento seguro em iOS
  - 4.4.3.2. Armazenamento seguro em Android
- 4.4.4. Boas práticas no desenvolvimento de aplicações

4.5. Vulnerabilidades e vetores de ataque
- 4.5.1. Vulnerabilidades
- 4.5.2. Vetores de ataque
  - 4.5.2.1. *Malware*
  - 4.5.2.2. Exfiltração de dados
  - 4.5.2.3. Manipulação de dados

4.6. Principais ameaças
- 4.6.1. Utilizador não formado
- 4.6.2. Malware
  - 4.6.2.1. Tipos de malware
- 4.6.3. Engenharia social
- 4.6.4. Fuga de dados
- 4.6.5. Roubo de informações
- 4.6.6. Redes wifi não seguras
- 4.6.7. Software desatualizado
- 4.6.8. Aplicações maliciosas
- 4.6.9. Palavras-passe pouco seguras
- 4.6.10. Configurações de segurança fracas ou inexistentes
- 4.6.11. Acesso físico
- 4.6.12. Perda ou roubo do dispositivo
- 4.6.13. Suplantação de identidade (integridade)
- 4.6.14. Criptografia fraca ou quebrada
- 4.6.15. Negação de Serviço (DoS)

4.7. Principais ataques
- 4.7.1. Ataques de phishing
- 4.7.2. Ataques relacionados com os modos de comunicação
- 4.7.3. Ataques de *Smishing*
- 4.7.4. Ataques de *Criptojacking*
- 4.7.5. *Man in the Middle*

4.8. *Hacking*
- 4.8.1. *Rooting* e *Jailbreaking*
- 4.8.2. Anatomia de um ataque móvel
  - 4.8.2.1. Propagação da ameaça
  - 4.8.2.2. Instalação de *malware* no dispositivo
  - 4.8.2.3. Persistência
  - 4.8.2.4. Execução do *Payload* e extração da informação
- 4.8.3. *Hacking* em dispositivos iOS: mecanismos e ferramentas
- 4.8.4. *Hacking* em dispositivos Android: mecanismos e ferramentas

4.9. Provas de penetração
- 4.9.1. iOS *pentesting*
- 4.9.2. Android *pentesting*
- 4.9.3. Ferramentas

4.10. Proteção e segurança
- 4.10.1. Definições de segurança
  - 4.10.1.1. Em dispositivos iOS
  - 4.10.1.2. Em dispositivos Android
- 4.10.2. Medidas de segurança
- 4.10.3. Ferramentas de proteção

Módulo 5. Segurança da IoT

5.1. Dispositivos
- 5.1.1. Tipos de dispositivos
- 5.1.2. Arquiteturas padronizadas
  - 5.1.2.1. OneM2M
  - 5.1.2.2. IoTWF
- 5.1.3. Protocolos de aplicação
- 5.1.4. Tecnologias de conetividade

5.2. Dispositivos IoT. Áreas de aplicação
- 5.2.1. SmartHome
- 5.2.2. SmartCity
- 5.2.3. Transportes
- 5.2.4. *Wearables*
- 5.2.5. Setor Saúde
- 5.2.6. IIoT

5.3. Protocolos de comunicação
- 5.3.1. MQTT
- 5.3.2. LWM2M
- 5.3.3. OMA-DM
- 5.3.4. TR-069

5.4. SmartHome
- 5.4.1. Domótica
- 5.4.2. Redes
- 5.4.3. Eletrodomésticos
- 5.4.4. Vigilância e segurança

5.5. SmartCity
- 5.5.1. Iluminação
- 5.5.2. Meteorologia
- 5.5.3. Segurança

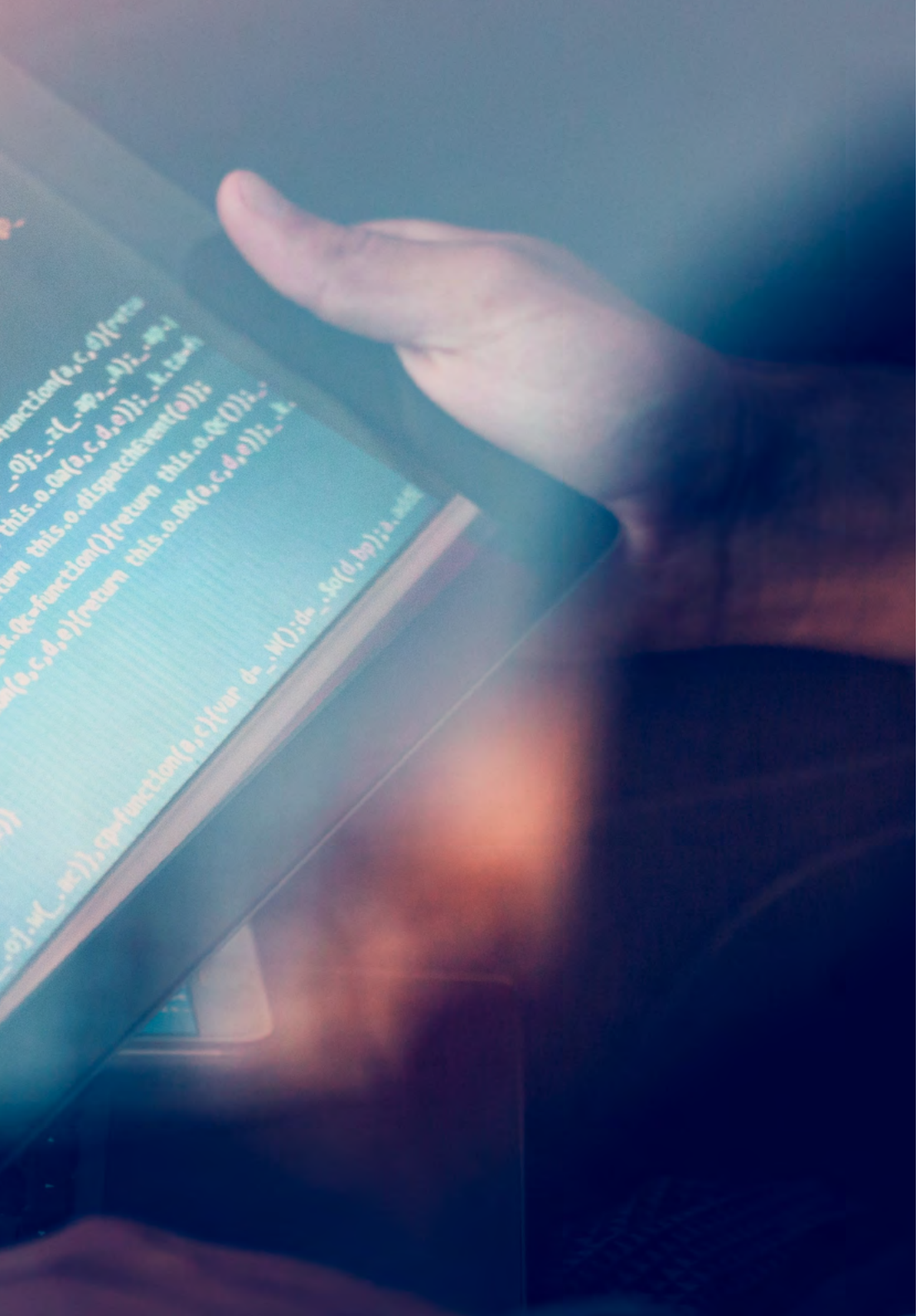
5.6. Transportes
- 5.6.1. Localização
- 5.6.2. Realização de pagamentos e obtenção de serviços
- 5.6.3. Conectividade

5.7. *Wearables*
- 5.7.1. Vestuário inteligente
- 5.7.2. Joias inteligentes
- 5.7.3. Relógios inteligentes

5.8. Setor Saúde
- 5.8.1. Monitorização de exercício/ritmo cardíaco
- 5.8.2. Monitorização de pacientes e idosos
- 5.8.3. Implantáveis
- 5.8.4. Robôs cirúrgicos

5.9. Conectividade
- 5.9.1. Wifi
- 5.9.2. Bluetooth
- 5.9.3. Conectividade incorporada

5.10. Segurança
- 5.10.1. Redes dedicadas
- 5.10.2. Gestor de palavras-passe
- 5.10.3. Utilização de protocolos encriptados
- 5.10.4. Conselhos de utilização



Módulo 6. Hacking Ético

6.1. Ambiente de trabalho
- 6.1.1. Distribuições Linux
  - 6.1.1.1. Kali Linux-Offensive Security
  - 6.1.1.2. Parrot OS
  - 6.1.1.3. Ubuntu
- 6.1.2. Sistemas de virtualização
- 6.1.3. Sandbox
- 6.1.4. Implementação de laboratórios

6.2. Metodologias
- 6.2.1. OSSTMM
- 6.2.2. OWASP
- 6.2.3. NIST
- 6.2.4. PTES
- 6.2.5. ISSAF

6.3. Footprinting
- 6.3.1. Inteligência de fontes abertas (OSINT)
- 6.3.2. Pesquisa de violações e vulnerabilidades de dados
- 6.3.3. Utilização de ferramentas passivas

6.4. Análise de redes
- 6.4.1. Ferramentas de análise
  - 6.4.1.1. Nmap
  - 6.4.1.2. Hping3
  - 6.4.1.3. Outras ferramentas de análise
- 6.4.2. Técnicas de análise
- 6.4.3. Técnicas de evasão de *firewall* e IDS
- 6.4.4. Banner *grabbing*
- 6.4.5. Diagramas de rede

6.5. Enumeração
- 6.5.1. Enumeração SMTP
- 6.5.2. Enumeração DNS
- 6.5.3. Enumeração de NetBIOS e Samba
- 6.5.4. Enumeração de LDAP
- 6.5.5. Enumeração de SNMP
- 6.5.6. Outras técnicas de enumeração

6.6. Análise de vulnerabilidade
- 6.6.1. Soluções de análise de vulnerabilidades
  - 6.6.1.1. Qualys
  - 6.6.1.2. Nessus
  - 6.6.1.3. CFI LanGuard
- 6.6.2. Sistemas de avaliação de vulnerabilidades
  - 6.6.2.1. CVSS
  - 6.6.2.2. CVE
  - 6.6.2.3. NVD

6.7. Ataques a redes sem fios
- 6.7.1. Metodologia de *hacking* em redes sem fios
  - 6.7.1.1. Wifi Discovery
  - 6.7.1.2. Análise de tráfego
  - 6.7.1.3. Ataques do *aircrack*
    - 6.7.1.3.1. Ataques WEP
    - 6.7.1.3.2. Ataques WPA/WPA2
  - 6.7.1.4. Ataques de *Evil Twin*
  - 6.7.1.5. Ataques ao WPS
  - 6.7.1.6. *Jamming*
- 6.7.2. Ferramentas para a segurança sem fios

6.8. Hacking de servidores Web
- 6.8.1. *Cross Site Scripting*
- 6.8.2. CSRF
- 6.8.3. *Session Hijacking*
- 6.8.4. *SQL injection*

6.9. Exploração de vulnerabilidades
- 6.9.1. Utilização de *exploits* conhecidos
- 6.9.2. Utilização de *metasploits*
- 6.9.3. Utilização de *malwares*
  - 6.9.3.1. Definição e alcance
  - 6.9.3.2. Geração de *malware*
  - 6.9.3.3. Contornar soluções antivírus

6.10. Persistência
- 6.10.1. Instalação de *Rootkits*
- 6.10.2. Utilização de Ncat
- 6.10.3. Utilização de tarefas programadas para *backdoors*
- 6.10.4. Criação de utilizadores
- 6.10.5. Deteção de HIDS

Módulo 7. Engenharia Inversa

7.1. Compiladores
- 7.1.1. Tipos de códigos
- 7.1.2. Fases de um compilador
- 7.1.3. Tabela de símbolos
- 7.1.4. Gestor de erros
- 7.1.5. Compilador GCC

7.2. Tipos de análise em compiladores
- 7.2.1. Análise lexical
  - 7.2.1.1. Terminologia
  - 7.2.1.2. Componentes léxicos
  - 7.2.1.3. Analisador léxico LEX
- 7.2.2. Análise sintática
  - 7.2.2.1. Gramáticas livres de contexto
  - 7.2.2.2. Tipos de análise sintática
    - 7.2.2.2.1. Análise descendente
    - 7.2.2.2.2. Análise ascendente
  - 7.2.2.3. Árvores sintáticas e derivações
  - 7.2.2.4. Tipos de analisadores sintáticos
    - 7.2.2.4.1. Analisadores LR (*Left To Right*)
    - 7.2.2.4.2. Analisadores LALR
- 7.2.3. Análise semântica
  - 7.2.3.1. Gramáticas de atributos
  - 7.2.3.2. S-atribuídas
  - 7.2.3.3. L-atribuídas

7.3. Estruturas de dados de montagem
- 7.3.1. Variáveis
- 7.3.2. Matrizes
- 7.3.3. Indicadores
- 7.3.4. Estruturas
- 7.3.5. Objetos

7.4. Estruturas de código de montagem
- 7.4.1. Estruturas de seleção
  - 7.4.1.1. If, else if, else
  - 7.4.1.2. *Switch*
- 7.4.2. Estruturas de iteração
  - 7.4.2.1. *For*
  - 7.4.2.2. *While*
  - 7.4.2.3. Utilização do *break*
- 7.4.3. Funções

7.5. Arquitetura hardware x86
- 7.5.1. Arquitetura de processadores x86
- 7.5.2. Estruturas de dados em x86
- 7.5.3. Estruturas de código em x86
- 7.5.4. Estruturas de código em x86

7.6. Arquitetura hardware ARM
- 7.6.1. Arquitetura de processadores ARM
- 7.6.2. Estruturas de dados em ARM
- 7.6.3. Estruturas de código em ARM

7.7. Análise de código estático
- 7.7.1. Desmontadores
- 7.7.2. IDA
- 7.7.3. Reconstrutores de código

7.8. Análise de código dinâmico
- 7.8.1. Análise comportamental
  - 7.8.1.1. Comunicações
  - 7.8.1.2. Monitorização
- 7.8.2. Depuradores de código em Linux
- 7.8.3. Depuradores de código em Windows

7.9. Sandbox
- 7.9.1. Arquitetura de uma Sandbox
- 7.9.2. Evasão de uma Sandbox
- 7.9.3. Técnicas de deteção
- 7.9.4. Técnicas de evasão
- 7.9.5. Contramedidas
- 7.9.6. Sandbox em Linux
- 7.9.7. Sandbox em Windows
- 7.9.8. *Sandbox* em macOS
- 7.9.9. Sandbox em Android

7.10. Análise de *malwares*
- 7.10.1. Métodos de análise de *malware*
- 7.10.2. Técnicas de ofuscação de *malware*
  - 7.10.2.1. Ofuscação de executáveis
  - 7.10.2.2. Restrição de ambientes de execução
- 7.10.3. Ferramentas de análise de *malware*

Módulo 8. Desenvolvimento Seguro

8.1. Desenvolvimento Seguro
- 8.1.1. Qualidade, funcionalidade e segurança
- 8.1.2. Confidencialidade, integridade e disponibilidade
- 8.1.3. Ciclo de vida do desenvolvimento de software

8.2. Fase de requisitos
- 8.2.1. Controlo da autenticação
- 8.2.2. Controlo de funções e privilégios
- 8.2.3. Requisitos orientados para o risco
- 8.2.4. Aprovação de privilégios

8.3. Fases de análise e conceção
- 8.3.1. Acesso a componentes e administração do sistema
- 8.3.2. Pistas de auditoria
- 8.3.3. Gestão de sessões
- 8.3.4. Dados históricos
- 8.3.5. Tratamento adequado de erros
- 8.3.6. Separação de funções

8.4. Fase de implementação e codificação
- 8.4.1. Proteger o ambiente de desenvolvimento
- 8.4.2. Preparação da documentação técnica
- 8.4.3. Codificação segura
- 8.4.4. Segurança das comunicações

8.5. Boas práticas de codificação segura
- 8.5.1. Validação dos dados de entrada
- 8.5.2. Codificação dos dados de saída
- 8.5.3. Estilo de programação
- 8.5.4. Gestão do registo de alterações
- 8.5.5. Práticas criptográficas
- 8.5.6. Gestão de erros e registos
- 8.5.7. Gestão de ficheiros
- 8.5.8. Gestão da memória
- 8.5.9. Padronização e reutilização de funções de segurança

8.6. Preparação do servidor e *hardening*
- 8.6.1. Gestão de utilizadores, grupos e funções no servidor
- 8.6.2. Instalação de software
- 8.6.3. *Hardening* do servidor
- 8.6.4. Configuração robusta do ambiente da aplicação

8.7. Preparação da base de dados e *hardening*
- 8.7.1. Otimização do motor de bases de dados
- 8.7.2. Criação do utilizador próprio para a aplicação
- 8.7.3. Atribuir os privilégios necessários ao utilizador
- 8.7.4. *Hardening* da base de dados

8.8. Fase de teste
- 8.8.1. Controlo de qualidade em controlos de segurança
- 8.8.2. Inspeção faseada do código
- 8.8.3. Verificação da gestão das configurações
- 8.8.4. Testes de caixa negra

8.9. Preparação da transição para a produção
- 8.9.1. Efetuar o controlo das alterações
- 8.9.2. Efetuar o procedimento de transição para a produção
- 8.9.3. Realizar procedimento de *rollback*
- 8.9.4. Testes de pré-produção

8.10. Fase de manutenção
- 8.10.1. Garantia baseada em riscos
- 8.10.2. Testes de manutenção de segurança de caixa branca
- 8.10.3. Testes de manutenção de segurança de caixa negra

Módulo 9. Análise Forense

9.1. Aquisição de dados e duplicação
- 9.1.1. Aquisição de dados voláteis
  - 9.1.1.1. Informação do sistema
  - 9.1.1.2. Informação da rede
  - 9.1.1.3. Ordem de volatilidade
- 9.1.2. Aquisição de dados estáticos
  - 9.1.2.1. Criação de uma imagem duplicada
  - 9.1.2.2. Preparação de um documento para a cadeia de custódia
- 9.1.3. Métodos de validação dos dados adquiridos
  - 9.1.3.1. Métodos para Linux
  - 9.1.3.2. Métodos para Windows

9.2. Avaliação e derrota de técnicas antiforenses
- 9.2.1. Objetivos das técnicas antiforenses
- 9.2.2. Eliminação de dados
  - 9.2.2.1. Eliminação de dados e ficheiros
  - 9.2.2.2. Recuperação de ficheiros
  - 9.2.2.3. Recuperação de partições eliminadas
- 9.2.3. Proteção por palavra-passe
- 9.2.4. Esteganografia
- 9.2.5. Limpeza segura de dispositivos
- 9.2.6. Encriptação

9.3. Análise forense do sistema operativo
- 9.3.1. Análise forense de Windows
- 9.3.2. Análise forense de Linux
- 9.3.3. Análise forense de Mac

9.4. Análise forense da rede
- 9.4.1. Análise dos registos
- 9.4.2. Correlação de dados
- 9.4.3. Investigação da rede
- 9.4.4. Passos a seguir na análise forense da rede

9.5. Análise forense Web
- 9.5.1. Investigação dos ataques Web
- 9.5.2. Deteção de ataques
- 9.5.3. Localização de endereços IP

9.6. Análise forense de bases de dados
- 9.6.1. Análise forense em MSSQL
- 9.6.2. Análise forense em MySQL
- 9.6.3. Análise forense em PostgreSQL
- 9.6.4. Análise forense em MongoDB

9.7. Análise forense na *Cloud*
- 9.7.1. Tipos de crimes na *Cloud*
  - 9.7.1.1. Cloud como sujeito
  - 9.7.1.2. Cloud como objeto
  - 9.7.1.3. Cloud como ferramenta
- 9.7.2. Desafios da análise forense na *Cloud*
- 9.7.3. Investigação dos serviços de armazenamento na *Cloud*
- 9.7.4. Ferramentas de análise forense na *Cloud*

9.8. Investigação de crimes por correio eletrónico
- 9.8.1. Sistemas de correio eletrónico
  - 9.8.1.1. Clientes de correio eletrónico
  - 9.8.1.2. Servidor de correio eletrónico
  - 9.8.1.3. Servidor SMTP
  - 9.8.1.4. Servidor POP3
  - 9.8.1.5. Servidor IMAP4
- 9.8.2. Crimes de correio eletrónico
- 9.8.3. Mensagem de correio eletrónico
  - 9.8.3.1. Cabeçalhos padrão
  - 9.8.3.2. Cabeçalhos estendidos
- 9.8.4. Etapas da investigação destes crimes
- 9.8.5. Ferramentas forenses para correio eletrónico

9.9. Análise forense de dispositivos móveis
- 9.9.1. Redes celulares
  - 9.9.1.1. Tipos de Redes
  - 9.9.1.2. Conteúdo do CR
- 9.9.2. *Subscriber Identity Module* (SIM)
- 9.9.3. Aquisição lógica
- 9.9.4. Aquisição física
- 9.9.5. Aquisição do sistema de ficheiros

9.10. Redação e apresentação de relatórios forenses
- 9.10.1. Aspetos importantes de um relatório forense
- 9.10.2. Classificação e tipos de relatórios
- 9.10.3. Guia para a redação de um relatório
- 9.10.4. Apresentação do relatório
  - 9.10.4.1. Preparação prévia para testemunhar
  - 9.10.4.2. Deposição
  - 9.10.4.3. Lidar com os meios

Módulo 10. Desafios Atuais e Futuros em Matéria de Segurança Informática

10.1. Tecnologia blockchain
- 10.1.1. Âmbitos de aplicação
- 10.1.2. Garantia de confidencialidade
- 10.1.3. Garantia de não repúdio

10.2. Moeda digital
- 10.2.1. Bitcoins
- 10.2.2. Criptomoedas
- 10.2.3. Mineração de criptomoedas
- 10.2.4. Esquemas em pirâmide
- 10.2.5. Outros potenciais crimes e problemas

10.3. Deepfake
- 10.3.1. Impacto nos meios de comunicação
- 10.3.2. Perigos para a sociedade
- 10.3.3. Mecanismos de deteção

10.4. O futuro da inteligência artificial
- 10.4.1. Inteligência artificial e computação cognitiva
- 10.4.2. Utilizações para simplificar o serviço ao cliente

10.5. Privacidade digital
- 10.5.1. Direitos dos dados na Internet
- 10.5.2. Utilização dos dados na Internet
- 10.5.3. Gestão da privacidade e da identidade digital

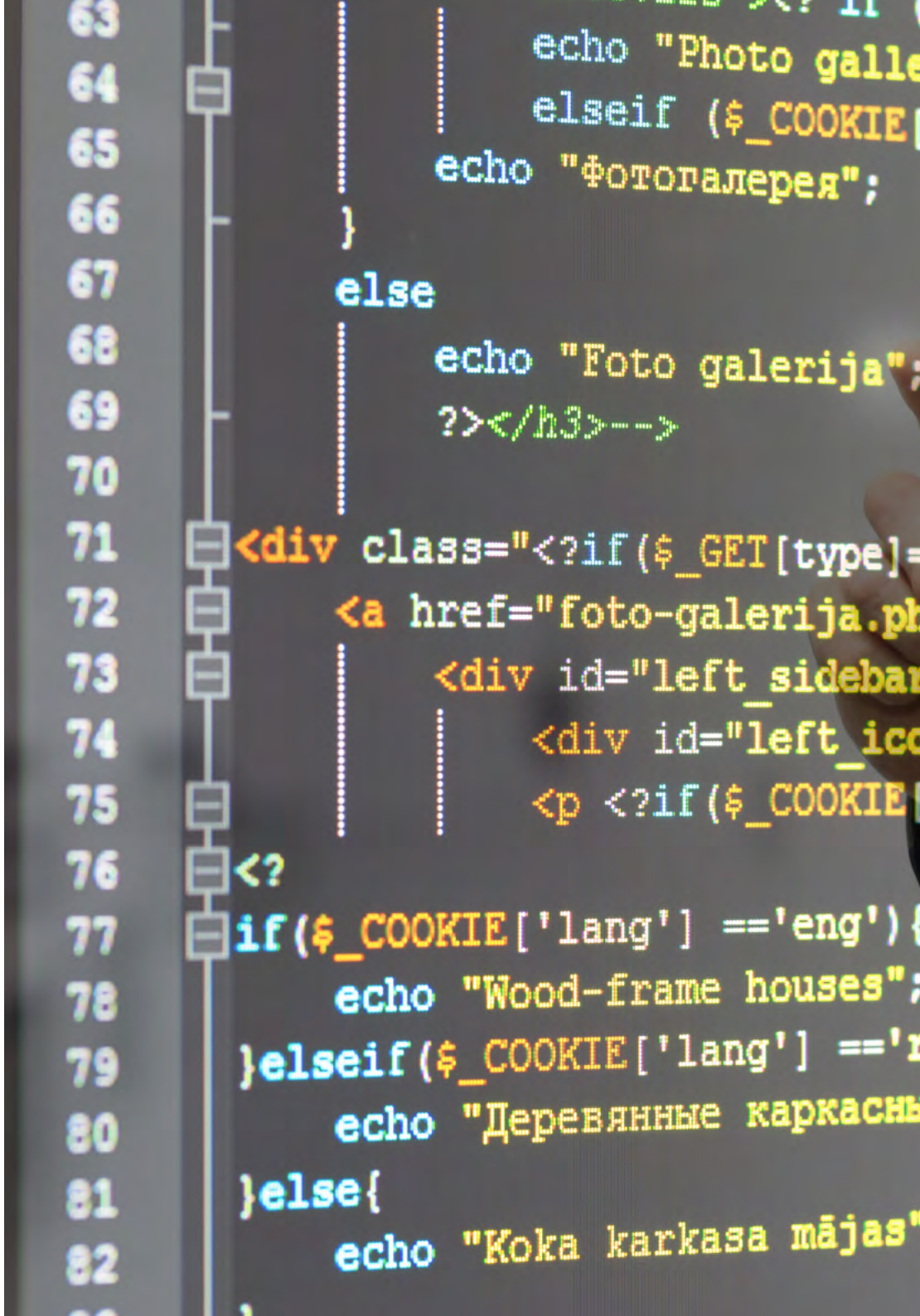
10.6. Ciberconflitos, cibercriminosos e ciberataques
- 10.6.1. O impacto da cibersegurança nos conflitos internacionais
- 10.6.2. Consequências dos ciberataques para a população em geral
- 10.6.3. Tipos de cibercriminosos. Medidas de proteção

10.7. Teletrabalho
- 10.7.1. Revolução do teletrabalho durante e após a COVID-19
- 10.7.2. Obstáculos de acesso
- 10.7.3. Variação da superfície de ataque
- 10.7.4. Necessidades dos colaboradores

10.8. Tecnologias *wireless* emergentes
- 10.8.1. WPA3
- 10.8.2. 5G
- 10.8.3. Ondas milimétricas
- 10.8.4. Tendência do "*Get Smart*" em vez de "*Get More*"

10.9. Endereçamento futuro em redes
- 10.9.1. Problemas atuais com o endereçamento IP
- 10.9.2. IPv6
- 10.9.3. IPv4+
- 10.9.4. Vantagens do IPv4+ em relação ao IPv4
- 10.9.5. Vantagens do IPv6 em relação ao IPv4

10.10. O desafio da sensibilização para a educação precoce e contínua da população
- 10.10.1. Estratégias governamentais atuais
- 10.10.2. Resistência da população à aprendizagem
- 10.10.3. Planos de formação a serem adotados pelas empresas



O seu futuro começa aqui.
Matricule-se hoje e torne-se
no Chief Information Officer de
empresas de grande envergadura"

06

Metodologia

Este programa de capacitação oferece uma forma diferente de aprendizagem. A nossa metodologia é desenvolvida através de um modo de aprendizagem cíclico: ***o Relearning***. Este sistema de ensino é utilizado, por exemplo, nas escolas médicas mais prestigiadas do mundo e tem sido considerado um dos mais eficazes pelas principais publicações, tais como a ***New England Journal of Medicine.***

Descubra o Relearning, um sistema que abandona a aprendizagem linear convencional para o levar através de sistemas de ensino cíclicos: uma forma de aprendizagem que provou ser extremamente eficaz, especialmente em disciplinas que requerem memorização"

Estudo de Caso para contextualizar todo o conteúdo

O nosso programa oferece um método revolucionário de desenvolvimento de competências e conhecimentos. O nosso objetivo é reforçar as competências num contexto de mudança, competitivo e altamente exigente.

Com a TECH pode experimentar uma forma de aprendizagem que abala as fundações das universidades tradicionais de todo o mundo"

Terá acesso a um sistema de aprendizagem baseado na repetição, com ensino natural e progressivo ao longo de todo o programa de estudos.

O estudante aprenderá, através de atividades de colaboração e casos reais, a resolução de situações complexas em ambientes empresariais reais.

Um método de aprendizagem inovador e diferente

Este programa da TECH é um programa de ensino intensivo, criado de raiz, que propõe os desafios e decisões mais exigentes neste campo, tanto a nível nacional como internacional. Graças a esta metodologia, o crescimento pessoal e profissional é impulsionado, dando um passo decisivo para o sucesso. O método do caso, a técnica que constitui a base deste conteúdo, assegura que a realidade económica, social e profissional mais atual é seguida.

> *O nosso programa prepara-o para enfrentar novos desafios em ambientes incertos e alcançar o sucesso na sua carreira"*

O método do caso tem sido o sistema de aprendizagem mais amplamente utilizado nas principais escolas de informática do mundo desde que existem. Desenvolvido em 1912 para que os estudantes de direito não só aprendessem o direito com base no conteúdo teórico, o método do caso consistia em apresentar-lhes situações verdadeiramente complexas, a fim de tomarem decisões informadas e valorizarem juízos sobre a forma de as resolver. Em 1924 foi estabelecido como um método de ensino padrão em Harvard.

Numa dada situação, o que deve fazer um profissional? Esta é a questão que enfrentamos no método do caso, um método de aprendizagem orientado para a ação. Ao longo do programa, os estudantes serão confrontados com múltiplos casos da vida real. Terão de integrar todo o seu conhecimento, investigar, argumentar e defender as suas ideias e decisões.

Relearning Methodology

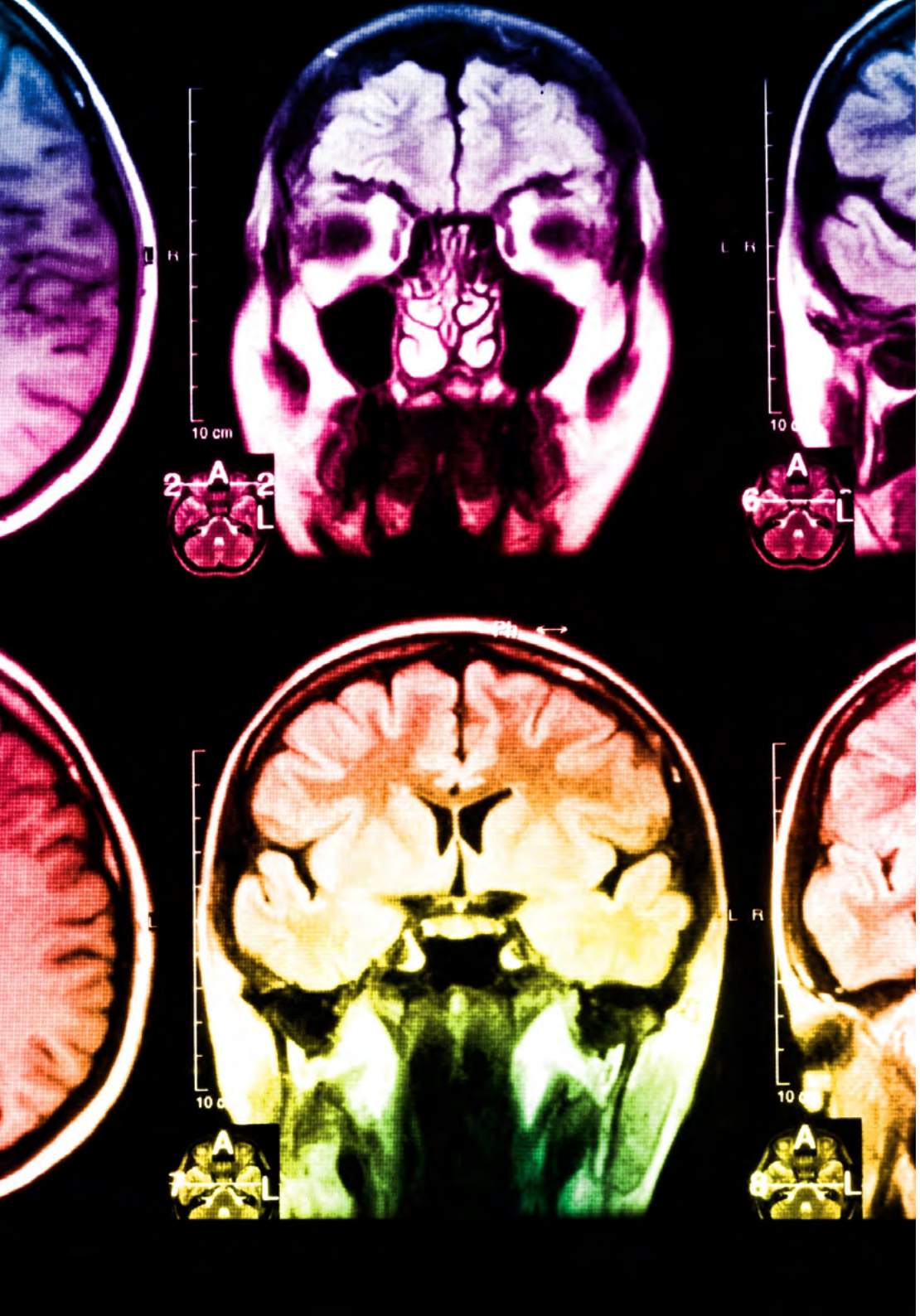
A TECH combina eficazmente a metodologia do Estudo de Caso com um sistema de aprendizagem 100% online baseado na repetição, que combina elementos didáticos diferentes em cada lição.

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

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

Na TECH aprende- com uma metodologia de vanguarda concebida para formar os gestores do futuro. Este método, na vanguarda da pedagogia mundial, chama-se Relearning.

A nossa universidade é a única universidade de língua espanhola licenciada para utilizar este método de sucesso. Em 2019, conseguimos melhorar os níveis globais de satisfação dos nossos estudantes (qualidade de ensino, qualidade dos materiais, estrutura dos cursos, objetivos...) no que diz respeito aos indicadores da melhor universidade online do mundo.



No nosso programa, a aprendizagem não é um processo linear, mas acontece numa espiral (aprender, desaprender, esquecer e reaprender). Portanto, cada um destes elementos é combinado de forma concêntrica. Esta metodologia formou mais de 650.000 licenciados com sucesso sem precedentes em áreas tão diversas como a bioquímica, genética, cirurgia, direito internacional, capacidades de gestão, ciência do desporto, filosofia, direito, engenharia, jornalismo, história, mercados e instrumentos financeiros. Tudo isto num ambiente altamente exigente, com um corpo estudantil universitário com um elevado perfil socioeconómico e uma idade média de 43,5 anos.

O Relearning permitir-lhe-á aprender com menos esforço e mais desempenho, envolvendo-o mais na sua capacitação, desenvolvendo um espírito crítico, defendendo argumentos e opiniões contrastantes: uma equação direta ao sucesso.

A partir das últimas provas científicas no campo da neurociência, não só sabemos como organizar informação, ideias, imagens e memórias, mas sabemos que o lugar e o contexto em que aprendemos algo é fundamental para a nossa capacidade de o recordar e armazenar no hipocampo, para o reter na nossa memória a longo prazo.

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

Este programa oferece o melhor material educativo, cuidadosamente preparado para profissionais:

Material de estudo

Todos os conteúdos didáticos são criados pelos especialistas que irão ensinar o curso, especificamente para o curso, para que o desenvolvimento didático seja realmente específico e concreto.

Estes conteúdos são depois aplicados ao formato audiovisual, para criar o método de trabalho online da TECH. Tudo isto, com as mais recentes técnicas que oferecem peças de alta-qualidade em cada um dos materiais que são colocados à disposição do aluno.

Masterclasses

Existem provas científicas sobre a utilidade da observação por terceiros especializada.

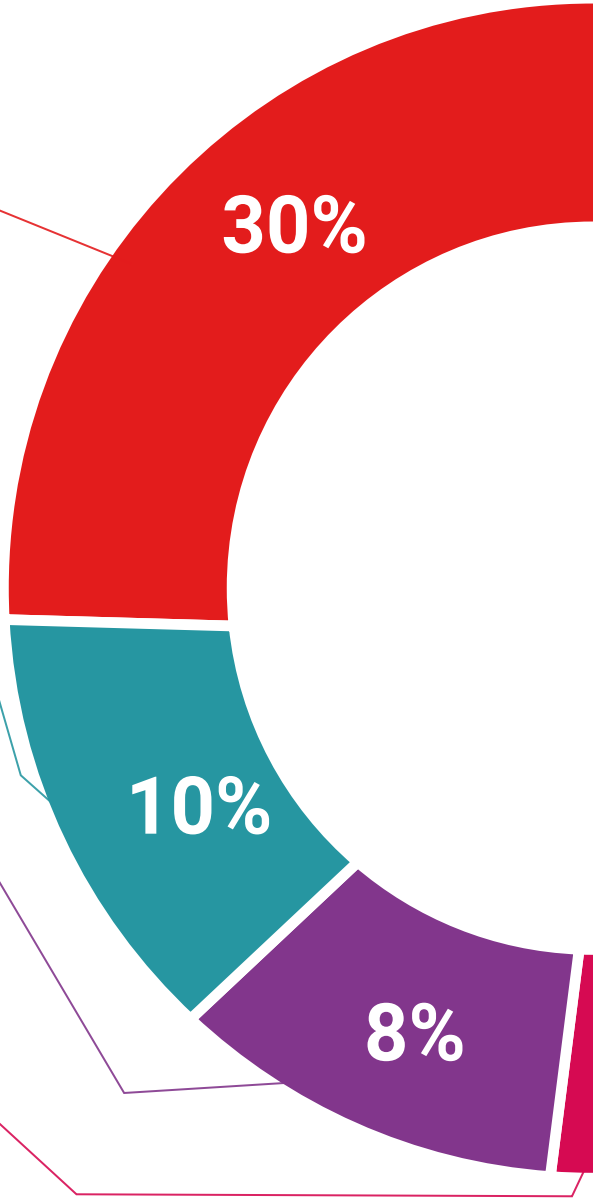
O denominado Learning from an Expert constrói conhecimento e memória, e gera confiança em futuras decisões difíceis.

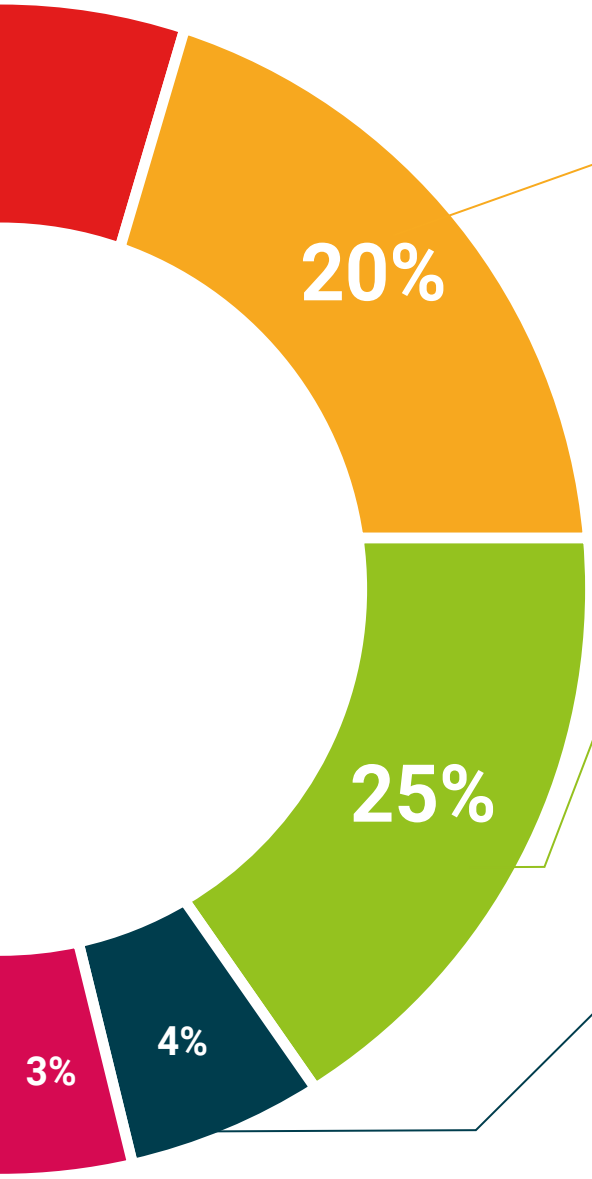
Práticas de aptidões e competências

Realizarão atividades para desenvolver competências e aptidões específicas em cada área temática. Práticas e dinâmicas para adquirir e desenvolver as competências e capacidades que um especialista necessita de desenvolver no quadro da globalização 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 necessita para completar a sua capacitação.





Case studies

Completarão uma seleção dos melhores estudos de casos escolhidos especificamente para esta situação. Casos apresentados, analisados e instruídos pelos melhores especialistas na cena internacional.

Resumos interativos

A equipa da TECH apresenta os conteúdos de uma forma atrativa e dinâmica em comprimidos multimédia que incluem áudios, vídeos, imagens, diagramas e mapas concetuais a fim de reforçar o conhecimento.

Este sistema educativo único para a apresentação de conteúdos multimédia foi premiado pela Microsoft como uma "História de Sucesso Europeu".

Testing & Retesting

Os conhecimentos do aluno são periodicamente avaliados e reavaliados ao longo de todo o programa, através de atividades e exercícios de avaliação e auto-avaliação, para que o aluno possa verificar como está a atingir os seus objetivos.

07

Certificação

O Mestrado Próprio em Gestão de Cibersegurança (CISO, Chief Information Security Officer) garante, para além de um conteúdo mais rigoroso e atualizado, o acesso a um grau de Mestre emitido pela TECH Universidade Tecnológica.

Conclua este plano de estudos com sucesso e receba o seu certificado sem sair de casa e sem burocracias"

Este **Mestrado Próprio em Gestão de Cibersegurança (CISO, Chief Information Security Officer)** conta com o conteúdo educativo mais completo e atualizado do mercado.

Uma vez aprovadas as avaliações, o aluno receberá por correio, com aviso de receção, o certificado* correspondente ao título de **Mestrado Próprio** emitido pela **TECH Universidade Tecnológica.**

O certificado emitido pela **TECH Universidade Tecnológica** expressará a qualificação obtida no Mestrado Próprio, atendendo aos requisitos normalmente exigidos pelas bolsas de emprego, concursos públicos e avaliação de carreiras profissionais.

Certificação: **Mestrado Próprio em Gestão de Cibersegurança (CISO, Chief Information Security Officer)**

Modalidade: **online**

Duração: **12 meses**

tech universidade tecnológica

Concede o presente

CERTIFICADO

a

Sr./Sra. _____, com o documento de identificação nº_____

Por ter concluído e acreditado com sucesso o

MESTRADO PRÓPRIO

em

Gestão de Cibersegurança (CISO, Chief Information Security Officer)

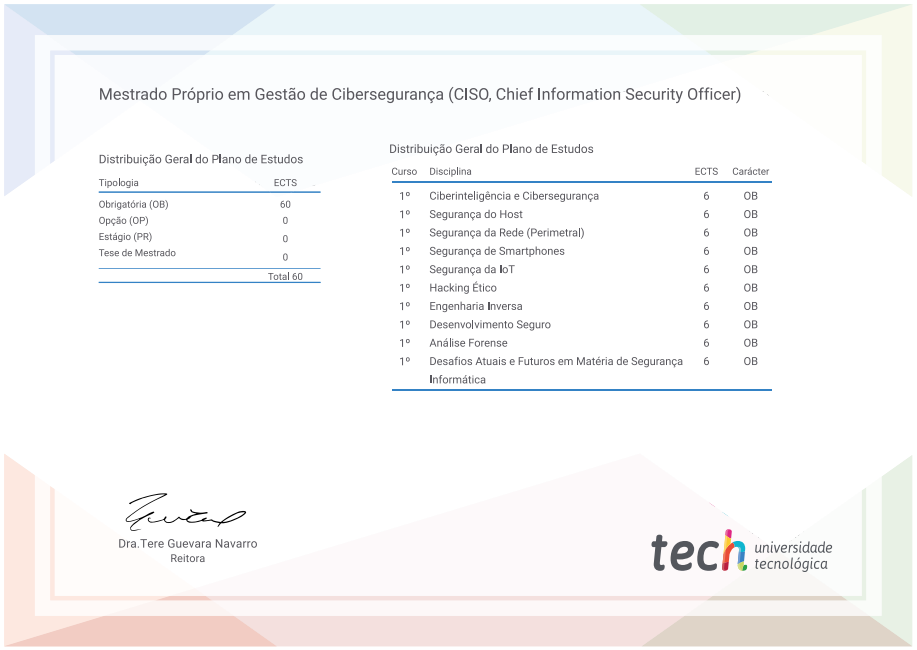
Este é um certificado atribuído por esta Universidade, reconhecido por 60 ECTS e equivalente a 1500 horas, com data de início a dd/mm/aaaaa e data de conclusão a dd/mm/aaaaa.

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

A 17 de junho de 2020

Prof.Tere Guevara Navarro
Reitora

código único TECH: AFWOR23S techtitute.com/titulos



Mestrado Próprio em Gestão de Cibersegurança (CISO, Chief Information Security Officer)

Distribuição Geral do Plano de Estudos

Tipologia	ECTS
Obrigatória (OB)	60
Opção (OP)	0
Estágio (PR)	0
Tese de Mestrado	0
	Total 60

Distribuição Geral do Plano de Estudos

Curso	Disciplina	ECTS	Carácter
1º	Ciberinteligência e Cibersegurança	6	OB
1º	Segurança do Host	6	OB
1º	Segurança da Rede (Perimetral)	6	OB
1º	Segurança de Smartphones	6	OB
1º	Segurança da IoT	6	OB
1º	Hacking Ético	6	OB
1º	Engenharia Inversa	6	OB
1º	Desenvolvimento Seguro	6	OB
1º	Análise Forense	6	OB
1º	Desafios Atuais e Futuros em Matéria de Segurança Informática	6	OB

Dra.Tere Guevara Navarro
Reitora

tech universidade tecnológica

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

tech universidade tecnológica

Mestrado Próprio

Gestão de Cibersegurança (CISO, Chief Information Security Officer)

- Modalidade: **Online**
- Duração: **12 meses**
- Certificação: **TECH Universidade Tecnológica**
- Créditos: **60 ECTS**
- Horário: **Ao seu ritmo**
- Exames: **Online**

Mestrado Próprio

Gestão de Cibersegurança (CISO, Chief Information Security Officer)

tech universidade tecnológica