Executive Master

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

MGCCISO

tech universidade tecnológica

tech universidade tecnológica

Executive Master
MBA em Gestão de Cibersegurança (CISO, Chief Information Security Officer)

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

Acesso ao site: **www.techtitute.com/escola-gestao/mestrado-proprio/mestrado-proprio-mba-gestao-ciberseguranca-ciso-chief-information-security-officer**

Índice

01

Boas-vindas

A sociedade atual está hiperconectada. A era da informação permite que os cidadãos estejam a par de todos os dados com um simples clique num botão. Mas isto também significa que as ameaças virtuais estão na ordem do dia, deixando as empresas mais expostas do que nunca ao risco de serem afetadas por um *software* maligno que pode prejudicar a sua produção e segurança, ou mesmo expor dados pessoais de clientes e funcionários, e expor as suas fraquezas informáticas. Embora a proteção nesta área seja da competência dos especialistas em TI, cada vez mais *chief revenue officerse* outros gestores optam por se especializar neste domínio para tentar travar os cibercriminosos e evitar ser alvo dos seus ataques. Por esta razão, a TECH criou este programa, no qual os profissionais de negócios encontrarão as informações mais relevantes do momento, através de um programa didático que será de fácil compreensão para os alunos. Assim, e graças aos conhecimentos adquiridos, o licenciado poderá trabalhar com total sucesso como Chief Information Security Office, uma posição em ascensão e com grandes perspetivas de crescimento.

Executive Master em MBA em Gestão de Cibersegurança (CISO, Chief Information Security Officer).
TECH Universidade Tecnológica

Melhore as suas competências em Gestão da Cibersegurança graças a 10 Masterclasses dadas por um especialista de renome internacional"

02

Porquê estudar na TECH?

A TECH é a maior escola de gestão do mundo, 100% online. Trata-se de uma Escola de Gestão de elite, com um modelo que obedece aos mais elevados padrões académicos. Um centro internacional de ensino de alto desempenho e de competências intensivas de gestão.

A TECH é uma Universidade na vanguarda da tecnologia, que coloca todos os seus recursos à disposição do estudante para o ajudara alcançar o sucesso empresarial"

Na TECH Universidade Tecnológica

Inovação

A universidade oferece um modelo de aprendizagem online, que combina a mais recente tecnologia educacional com o máximo rigor pedagógico. Um método único com o mais alto reconhecimento internacional, que fornecerá os elementos-chave para que o aluno se desenvolva num mundo em constante mudança, onde a inovação deve ser a aposta essencial de cada empresário.

"Caso de Sucesso Microsoft Europa" por incorporar um sistema multivídeo interativo inovador nos programas.

Máxima exigência

O critério de admissão da TECH não é económico. Não é necessário fazer um grande investimento para estudar nesta Universidade. No entanto, para se formar na TECH, serão testados os limites da inteligência e capacidade do estudante. Os padrões académicos desta instituição são muito elevados...

95% | **dos estudantes da TECH concluem os seus estudos com sucesso**

Networking

Profissionais de todo o mundo participam na TECH, pelo que o estudante poderá criar uma vasta rede de contactos que lhe será útil para o seu futuro.

+100 mil

gestores formados todos os anos

+200

nacionalidades diferentes

Empowerment

O estudante vai crescer de mãos dadas com as melhores empresas e profissionais de grande prestígio e influência. A TECH desenvolveu alianças estratégicas e uma valiosa rede de contactos com os principais intervenientes económicos dos 7 continentes.

+500 | **Acordos de colaboração com as melhores empresas**

Talento

Este Curso de Especialização é uma proposta única para fazer sobressair o talento do estudante no meio empresarial. Uma oportunidade para dar a conhecer as suas preocupações e a sua visão de negócio.

A TECH ajuda o estudante a mostrar o seu talento ao mundo no final desta especialização

Contexto Multicultural

Ao estudar na TECH, o aluno pode desfrutar de uma experiência única. Estudará num contexto multicultural. Num programa com uma visão global, graças ao qual poderá aprender sobre a forma de trabalhar em diferentes partes do mundo, compilando a informação mais recente e que melhor se adequa à sua ideia de negócio.

Os estudantes da TECH têm mais de 200 nacionalidades.

Aprenda com os melhores

A equipa docente da TECH explica nas aulas o que os levou ao sucesso nas suas empresas, trabalhando num contexto real, animado e dinâmico. Professores que estão totalmente empenhados em oferecer uma especialização de qualidade que permita ao estudante avançar na sua carreira e destacar-se no mundo dos negócios.

Professores de 20 nacionalidades diferentes.

Na TECH terá acesso aos estudos de casos mais rigorosos e atualizados no meio académico"

A TECH procura a excelência e, para isso, tem uma série de caraterísticas que a tornam uma Universidade única:

Análises

A TECH explora o lado crítico do aluno, a sua capacidade de questionar as coisas, a sua capacidade de resolução de problemas e as suas competências interpessoais.

Excelência académica

A TECH proporciona ao estudante a melhor metodologia de aprendizagem online. A Universidade combina o método *Relearning* (a metodologia de aprendizagem mais reconhecida internacionalmente) com o Estudo de Caso de Tradição e vanguarda num equilíbrio difícil, e no contexto do itinerário académico mais exigente.

Economia de escala

A TECH é a maior universidade online do mundo. Tem uma carteira de mais de 10 mil pós-graduações universitárias. E na nova economia, **volume + tecnologia = preço disruptivo**. Isto assegura que os estudos não são tão caros como noutra universidade.

03

Porquê o nosso programa?

Realizar o curso da TECH significa multiplicar as suas hipóteses de alcançar sucesso profissional da gestão de empresas de topo.

É um desafio que envolve esforço e dedicação, mas que abre a porta a um futuro promissor. O estudante aprenderá com o melhor corpo docente e com a metodologia educativa mais flexível e inovadora.

Contamos com o corpo docente mais prestigiado e o plano de estudos mais completo do mercado, o que nos permite oferecer uma capacitação do mais alto nível académico"

Este programa trará uma multiplicidade de benefícios profissionais e pessoais, entre os quais os seguintes:

01

Dar um impulso definitivo à carreira do aluno

Ao estudar na TECH, o aluno poderá assumir o controlo do seu futuro e desenvolver todo o seu potencial. Com a conclusão deste programa, adquirirá as competências necessárias para fazer uma mudança positiva na sua carreira num curto período de tempo.

70% dos participantes nesta especialização conseguem uma mudança positiva na sua carreira em menos de 2 anos.

02

Desenvolver uma visão estratégica e global da empresa

A TECH oferece uma visão aprofundada da gestão geral para compreender como cada decisão afeta as diferentes áreas funcionais da empresa.

A nossa visão global da empresa irá melhorar a sua visão estratégica.

03

Consolidar o estudante na gestão de empresas de topo

Estudar na TECH significa abrir as portas a um panorama profissional de grande importância para que o estudante se possa posicionar como gestor de alto nível, com uma visão ampla do ambiente internacional.

Trabalhará em mais de 100 casos reais de gestão de topo.

04

Assumir novas responsabilidades

Durante o programa, são apresentadas as últimas tendências, desenvolvimentos e estratégias, para que os estudantes possam realizar o seu trabalho profissional num ambiente em mudança.

45% dos alunos conseguem subir na carreira com promoções internas.

05

Acesso a uma poderosa rede de contactos

A TECH interliga os seus estudantes para maximizar as oportunidades. Estudantes com as mesmas preocupações e desejo de crescer. Assim, será possível partilhar parceiros, clientes ou fornecedores.

Encontrará uma rede de contactos essencial para o seu desenvolvimento profissional.

06

Desenvolver projetos empresariais de uma forma rigorosa

O estudante terá uma visão estratégica profunda que o ajudará a desenvolver o seu próprio projeto, tendo em conta as diferentes áreas da empresa.

20% dos nossos estudantes desenvolvem a sua própria ideia de negócio.

07

Melhorar as *soft skills* e capacidades de gestão

A TECH ajuda os estudantes a aplicar e desenvolver os seus conhecimentos adquiridos e a melhorar as suas capacidades interpessoais para se tornarem líderes que fazem a diferença.

Melhore as suas capacidades de comunicação e liderança e dê um impulso à sua profissão.

08

Ser parte de uma comunidade exclusiva

O estudante fará parte de uma comunidade de gestores de elite, grandes empresas, instituições de renome e professores qualificados das universidades mais prestigiadas do mundo: a comunidade da TECH Universidade Tecnológica.

Damos-lhe a oportunidade de se especializar com uma equipa de professores de renome internacional.

04

Objetivos

Este programa da TECH foi concebido para reforçar as competências profissionais dos gestores de empresas que, para além de serem altamente especializados na sua área de atividade, encontrarão neste programa uma oportunidade única de aperfeiçoamento num sector de grande importância, pois aprenderão a prevenir possíveis ameaças da Internet que podem causar sérios prejuízos às empresas. Desta forma, tornar-se-ão profissionais especializados em diferentes ramos, pelo que poderão controlar todas as áreas da empresa, tornando-se assim Chief Information Security Officer.

Aumente as suas competências e atinja os seus objetivos profissionais graças à formação superior que a TECH lhe oferece com este programa"

A TECH converte os objetivos dos seus alunos nos seus próprios objetivos
Trabalhamos em conjunto para os alcançar

O **Executive Master MBA em Gestão de Cibersegurança (CISO, Chief Information Security Officer)** prepara o aluno para:

01 Analisar o papel do analista de cibersegurança

02 Aprofundar o conhecimento da engenharia social e dos seus métodos

03 Examinar as metodologias OSINT, HUMINT, OWASP, PTEC OSSTM, OWISAM

04 Realizar uma análise de risco e compreender as métricas de risco

05 Determinar a utilização adequada do anonimato e o uso de redes como TOR, I2P e Freenet

06 Compilar os regulamentos vigentes em matéria de cibersegurança

07 Gerar conhecimentos especializados para a realização de uma auditoria de segurança

08 Desenvolver políticas de uso apropriadas

09 Examinar os sistemas de deteção e prevenção das ameaças mais importantes

10 Avaliar os novos sistemas de deteção de ameaças, assim como a sua evolução a partir de soluções mais tradicionais

11 Analisar as principais plataformas móveis atuais, as suas características e utilização

12 Identificar, analisar e avaliar os riscos de segurança das partes do projeto IoT

13 Avaliar a informação obtida e desenvolver mecanismos de prevenção e hacking

14 Aplicar a engenharia inversa ao ambiente da Cibersegurança

15 Especificar os testes a realizar ao software desenvolvido

16 Recolher todas as provas e dados existentes para levar a cabo um relatório forense

17 Apresentar devidamente o relatório forense

18 Analisar o estado atual e futuro da segurança informática

19 Analisar os riscos das novas tecnologias emergentes

20 Compilar as diferentes tecnologias em relação à segurança informática

05

Competências

O MBA em Gestão de Cibersegurança (CISO, Chief Information Security Officer) foi concebido para melhorar a competitividade dos profissionais do sector empresarial. Assim, no final dos seus estudos, os estudantes terão adquirido as competências necessárias para desenvolver uma prática de qualidade e atualizada, baseada na metodologia de ensino mais inovadora. Sem dúvida, um programa que irá melhorar a sua formação e permitirá ser mais competitivo na sua prática diária, unificando todos os aspetos relevantes da segurança informática que os gestores precisam de conhecer e colocar em prática.

Inicie-se no estudo da segurança informática e melhore as suas competências para controlar potenciais ameaças à rede"

01 Conhecer as metodologias utilizadas em matéria de cibersegurança

02 Avaliar cada tipo de ameaça para fornecer uma solução óptima em cada caso

03 Gerar soluções inteligentes completas para automatizar o comportamento em caso de incidentes

04 Avaliar os riscos associados às vulnerabilidades, tanto dentro como fora da empresa

05 Compreender a evolução e o impacto da IoT ao longo do tempo

06 Demonstrar que um sistema é vulnerável, atacando-o preventivamente e resolvendo esses problemas

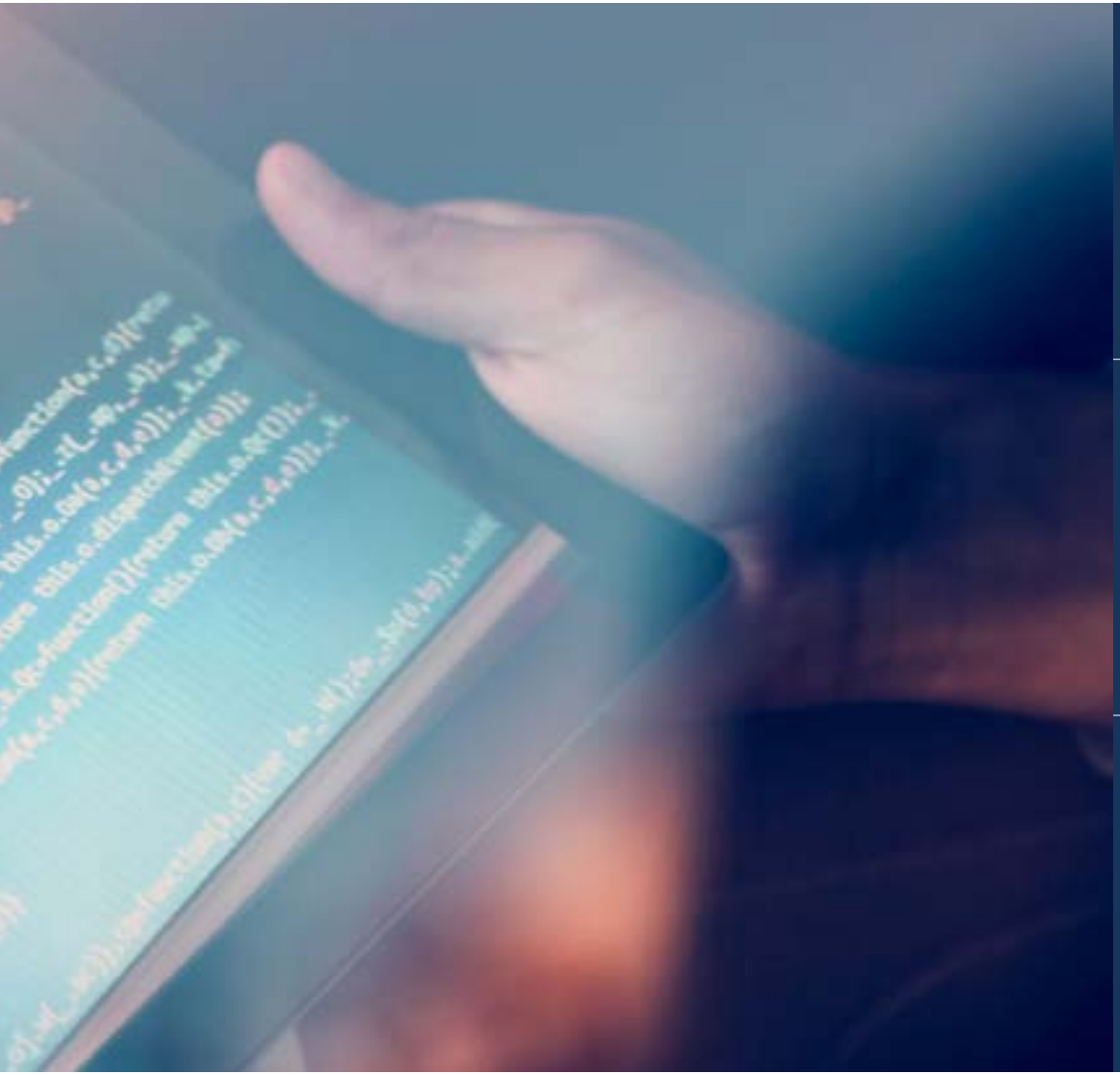
07 Saber aplicar o *sandboxing* em diferentes cenários

08 Conhecer as diretrizes que um bom programador deve seguir para cumprir os requisitos de segurança necessários

09 Realizar operações de segurança defensiva

10 Ter uma perceção profunda e especializada sobre segurança informática

11 Aplicar processos de segurança para smartphones e dispositivos móveis



12 Conhecer os meios para efetuar o chamado *Hacking* ético e proteger uma empresa de um ciberataque

13 Ser capaz de investigar um incidente de cibersegurança

14 Distinguir entre as técnicas de ataque e de defesa existentes

06

Estrutura e conteúdo

Este programa da TECH foi concebido para responder às necessidades de especialização dos profissionais das empresas que desejam alargar os seus conhecimentos em matéria de segurança informática, um domínio fundamental para poder controlar as potenciais ameaças que podem representar um grande risco para a empresa. Desta forma, o MBA permitir-lhes-á adquirir conhecimentos específicos que poderão aplicar na sua prática profissional. Par tal, utilizarão uma metodologia totalmente online que lhes permitirá combinar os seus estudos com o resto das suas obrigações diárias.

Este programa será essencial para detetar possíveis ciberataques na sua empresa"

Plano de estudos

O MBA em Gestão de Cibersegurança (Chief Information Security Officer) da TECH Universidade Tecnológica é um programa intensivo concebido para promover o desenvolvimento de competências de gestão que permitam a tomada de decisões com maior rigor em ambientes incertos.

Ao longo de 1.500 horas de estudo, o estudante adquirirá as competências necessárias para se desenvolver com sucesso na sua prática quotidiana. Trata-se, portanto, de uma verdadeira imersão em situações reais de negócio.

Este programa aborda em profundidade diferentes áreas da empresa e foi concebido para que os gestores compreendam a cibersegurança numa perspetiva estratégica, internacional e inovadora.

Um plano concebido especialmente para os estudantes, centrado no seu aperfeiçoamento profissional e que os prepara para atingir a excelência no domínio da gestão da segurança informática.

Um programa que compreende as suas necessidades e as da sua empresa, através de conteúdos inovadores baseados nas últimas tendências e apoiados na melhor metodologia educativa e um corpo docente excecional.

A tudo isto, juntam-se 10 Masterclasses exclusivas que fazem parte dos materiais didáticos, na vanguarda da tecnologia e da educação. Estas aulas foram concebidas por um especialista de renome internacional em Inteligência, Cibersegurança e Tecnologias Disruptivas. Recursos úteis que ajudarão o profissional executivo a especializar-se em Gestão da Cibersegurança e a gerir eficazmente os departamentos da empresa dedicados a esta importante área.

O programa tem a duração de 12 meses e está dividido em 10 módulos:

Módulo 1	Ciberinteligência e cibersegurança
Módulo 2	Segurança em *Host*
Módulo 3	Segurança em rede (Perimetral)
Módulo 4	Segurança em *Smartphones*
Módulo 5	Segurança em IoT
Módulo 6	*Hacking* ético
Módulo 7	Engenharia inversa
Módulo 8	Desenvolvimento seguro
Módulo 9	Análise forense
Módulo 10	Desafios atuais e futuros em matéria de segurança informática

Onde, quando e como são ministradas?

A TECH oferece a possibilidade de desenvolver este Executive Master em MBA em Gestão de Cibersegurança (CISO, Chief Information Security Officer) completamente online. Durante os 12 meses de duração da especialização, o aluno poderá aceder a todos os conteúdos deste curso em qualquer altura, permitindo-lhe autogerir o seu tempo de estudo.

Uma experiência educativa única, essencial e decisiva para impulsionar o seu desenvolvimento profissional e progredir na sua carreira.

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 enviesamentos do analista de inteligência na atividade avaliativa

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 inteligências
1.3.1. OSINT
1.3.2. SOCMINT
1.3.3. HUMIT
1.3.4. Distribuições de Linux e ferramentas
1.3.5. OWISAM
1.3.6. OWISAP
1.3.7. PTES
1.3.8. OSSTM

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. Apresentação dos resultados da inteligência

1.5. Auditorias e documentação
1.5.1. A auditoria na segurança informática
1.5.2. Documentação e autorizações para a auditoria
1.5.3. Tipos de auditoria
1.5.4. Documentos a entregar
1.5.4.1. Relatório técnico
1.5.4.2. Relatório executivo

1.6. Anonimato na rede
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 nas redes
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
1.8.2. A estratégia nacional de cibersegurança 2019
1.8.3. Família ISO 27000
1.8.4. Quadro de cibersegurança 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. Alcance de 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
1.10.3. INCIBE
1.10.4. OEA
1.10.5. UNASUR-PROSUR

Módulo 2. Segurança em *Host*

2.1. Cópias de segurança
2.1.1. Estratégia 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. StickyPassword
2.5.5. RoboForm

2.6. Detetores de *phishing*
2.6.1. Deteção do *phishing* de forma 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 para proteger o sistema
2.8.2. Ferramentas anti-rastreadores

2.9. *EDR- End Point 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 software permitido ou proibido
2.10.3. Critérios de atualizações
2.10.4. Privilégios para instalar software

Módulo 3. Segurança em 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: *Defense in Depth* 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 em rede
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. Firewalls
3.2.4. Sistemas de deteção baseados em logs do sistema
3.2.4.1. TCP Wrappers
3.2.4.2. BlockHosts e DenyHosts
3.2.4.3. Fai2ban

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 *firewall* tradicional
3.4.2. Capacidades principais
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 eletrónico
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 em rede
3.10.1. WAF
3.10.2. NAC
3.10.3. *HoneyPots* e *HoneyNets*
3.10.4. CASB

Módulo 4. Segurança em *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
4.3.2. Políticas de segurança
4.3.3. Monitorização de dispositivos
4.3.4. Gestão de Dispositivos Móveis (MDM)

4.4. Privacidade do utilizador e segurança de dados
4.4.1. Estados da informação
4.4.2. Proteção e confidencialidade dos dados
4.4.2.1. Autorizações
4.4.2.2. Encriptação
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 dos dados

4.6. Principais ameaças
4.6.1. Utilizador não forçado
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 informação
4.6.6. Redes Wi-Fi não seguras
4.6.7. Software desatualizado
4.6.8. Aplicações maliciosas
4.6.9. Palavras-passe inseguras
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. Roubo de identidade (integridade)
4.6.14. Criptografia fraca ou danificada
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. Configuração de segurança
4.10.1.1. Em dispositivos iOS
4.10.1.2. Dispositivos Android
4.10.2. Medidas de segurança
4.10.3. Ferramentas de proteção

Módulo 5. Segurança em IoT

5.1. Dispositivos
5.1.1. Tipos de dispositivos
5.1.2. Arquiteturas estandardizadas
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. Electrodomésticos
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. Conetividade

5.7. *Wearables*
5.7.1. Roupa 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. Acompanhamento de doentes e pessoas idosas
5.8.3. Implantáveis
5.8.4. Robôs cirúrgicos

5.9. Conetividade
5.9.1. Wi-Fi/Gateway
5.9.2. Bluetooth
5.9.3. Conetividade incorporada

5.10. Securitização
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. OSSTM
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. Procura de brechas e vulnerabilidades de dados
6.3.3. Utilização de ferramentas passivas

6.4. Scanning de redes
6.4.1. Ferramentas de Scanning
6.4.1.1. Nmap
6.4.1.2. Hping3
6.4.1.3. Outras ferramentas de Scanning
6.4.2. Técnicas de Scanning
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 vulnerabilidades
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 pontuação 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. Wi-Fi *Discovery*
6.7.1.2. Análise de tráfico
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 a 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. *SQLinjection*

6.9. Exploração de vulnerabilidades
6.9.1. Utilização de *exploits* conhecidos
6.9.2. Utilização de *metasploit*
6.9.3. Utilização de *malware*
6.9.3.1. Definição e alcance
6.9.3.2. Geração de malware
6.9.3.3. Bypass de 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 léxica
7.2.1.1. Terminologia
7.2.1.2. Componentes léxicos
7.2.1.3. Analisador léxico LEX
7.2.2. Análise sintático
7.2.2.1. Gramáticas livres de contexto
7.2.2.2. Tipos de análise sintáticos
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. Arrays
7.3.3. Apontadores
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

7.6. 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 de comportamento
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 um *sandbox*
7.9.2. Evasão de um *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 *malware*
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 papéis 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. Garantia do ambiente de desenvolvimento
8.4.2. Elaboração da documentação técnica
8.4.3. Codificação segura
8.4.4. Segurança nas comunicações

8.5. Boas práticas de codificação segura
8.5.1. Validação de 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 logs
8.5.7. Gestão de ficheiros
8.5.8. Gestão de memória
8.5.9. Padronização e reutilização das funções de segurança

8.6. Preparação do servidor e *hardening*
8.6.1. Gestão de utilizadores, grupos e papéis 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 BBDD e *hardening*
8.7.1. Otimização do motor de BBDD
8.7.2. Criação do próprio utilizador para a aplicação
8.7.3. Atribuição dos privilégios necessários ao utilizador
8.7.4. *Hardening* da BBDD

8.8. Fase de testes
8.8.1. Controlo de qualidade nos controlos de segurança
8.8.2. Inspeção do código por fases
8.8.3. Comprovação da gestão das configurações
8.8.4. Testes de caixa negra

8.9. Preparação da transição para a produção
8.9.1. Realizar o controlo de alterações
8.9.2. Realizar o procedimento de passagem à produção
8.9.3. Realizar procedimento de *rollback*
8.9.4. Testes em fase de pré-produção

8.10. Fase de manutenção
8.10.1. Garantia baseada no risco
8.10.2. Testes de manutenção de segurança da caixa branca
8.10.3. Testes de manutenção de segurança da 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 de 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 anti-forenses
9.2.1. Objetivos das técnicas anti-forenses
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 apagadas
9.2.3. Proteção com 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 logs
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 de ataques na web
9.5.2. Deteção de ataques
9.5.3. Localização de direções IPs

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 em *Cloud*
9.7.1. Tipos de crimes em *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 em *Cloud*
9.7.3. Investigação dos serviços de armazenamento na *cloud*
9.7.4. Ferramentas de análise forense para *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 standard
9.8.3.2. Cabeçalhos extendidos
9.8.4. Passos na investigação destes crimes
9.8.5. Ferramentas forenses para correio eletrónico

9.9. Análise forense de telemóveis
9.9.1. Redes celulares
9.9.1.1. Tipos de redes
9.9.1.2. Conteúdos do CDR
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 escrever um relatório
9.10.4. Apresentação do Relatório
9.10.4.1. Preparação prévia para o depoimento
9.10.4.2. Deposição
9.10.4.3. Lidar com os meios de comunicação social

Módulo 10. Desafios atuais e futuros em matéria de segurança informática

10.1. Tecnologia *blockchain*
10.1.1. Domínios de aplicação
10.1.2. Garantia de confidencialidade
10.1.3. Garantia de não repúdio

10.2. Dinheiro digital
10.2.1. Bitcoins
10.2.2. Criptomoedas
10.2.3. Exploração de criptomoedas
10.2.4. Esquemas em pirâmide
10.2.5. Outros potenciais delitos e problemas

10.3. *Deepfake*
10.3.1. Impacto nos meios de comunicação social
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. Valor dos dados na rede
10.5.2. Utilização dos dados na rede
10.5.3. Gestão da privacidade e da identidade digital

10.6. Ciberconflitos, cibercrimes 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 Covid19
10.7.2. Obstáculos no acesso
10.7.3. Variação da superfície de ataque
10.7.4. Necessidades dos trabalhadores

10.8. Tecnologias *wireless* emergentes
10.8.1. WPA3
10.8.2. 5G
10.8.3. Ondas milimétricas
10.8.4. Tendência em *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 formação 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

07

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"

A TECH Business School utiliza o 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"

Este programa prepara-o para enfrentar desafios empresariais em ambientes incertos e tornar o seu negócio bem sucedido.

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

Um método de aprendizagem inovador e diferente

Este programa da TECH é um programa de formação intensiva, criado de raiz para oferecer aos gestores desafios e decisões empresariais ao mais alto nível, 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 estudante aprenderá, através de atividades de colaboração e casos reais, a resolução de situações complexas em ambientes empresariais reai"*

O método do caso tem sido o sistema de aprendizagem mais amplamente utilizado pelas melhores faculdades do mundo. 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

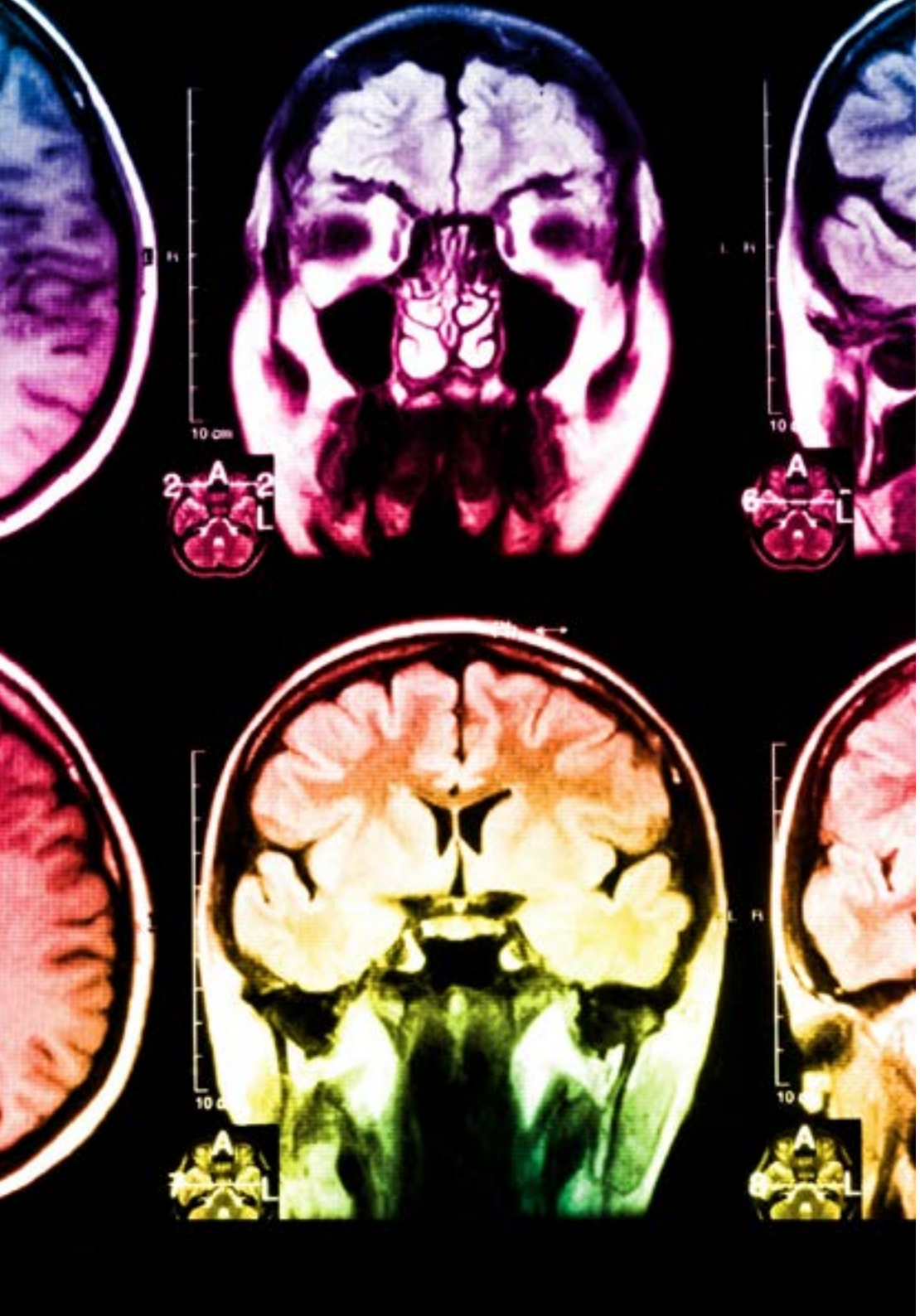
A TECH combina eficazmente a metodologia do Estudo de Caso com um sistema de aprendizagem 100% online baseado na repetição, que combina elementos didáticos diferentes em cada lição.

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

O nosso sistema online permitir-lhe-á organizar o seu tempo e ritmo de aprendizagem, adaptando-o ao seu horário. Poderá aceder ao conteúdo a partir de qualquer dispositivo fixo ou móvel com uma ligação à Internet.

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 escola de gestão é a única escola de língua espanhola licenciada para empregar 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.

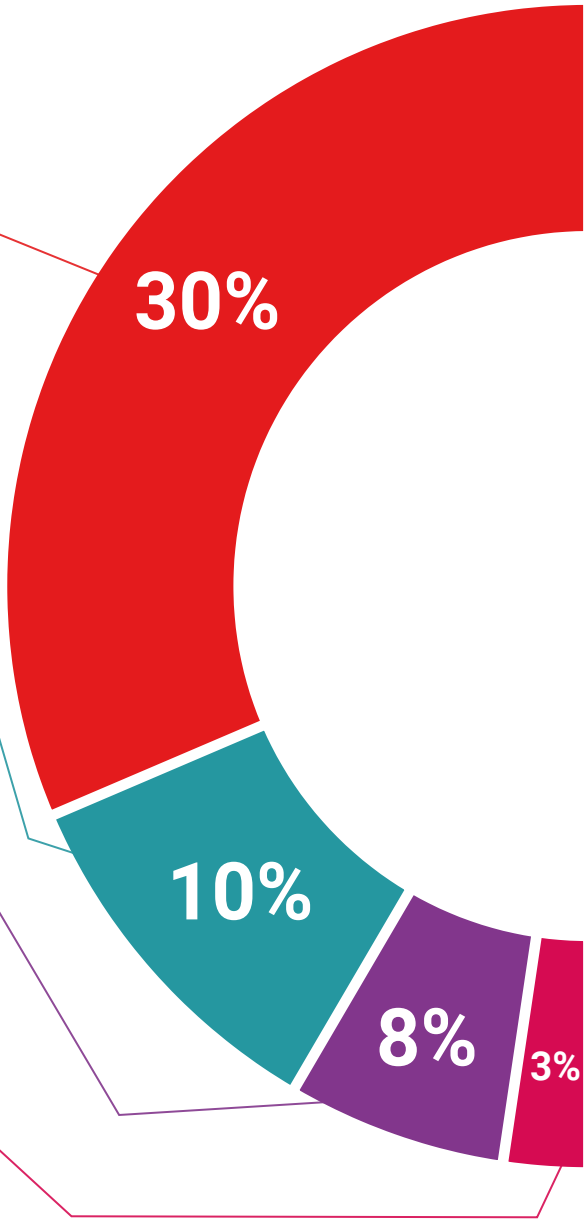
O denominado Learning from an Expert constrói conhecimento e memória, e gera confiança em futuras decisões difíceis.

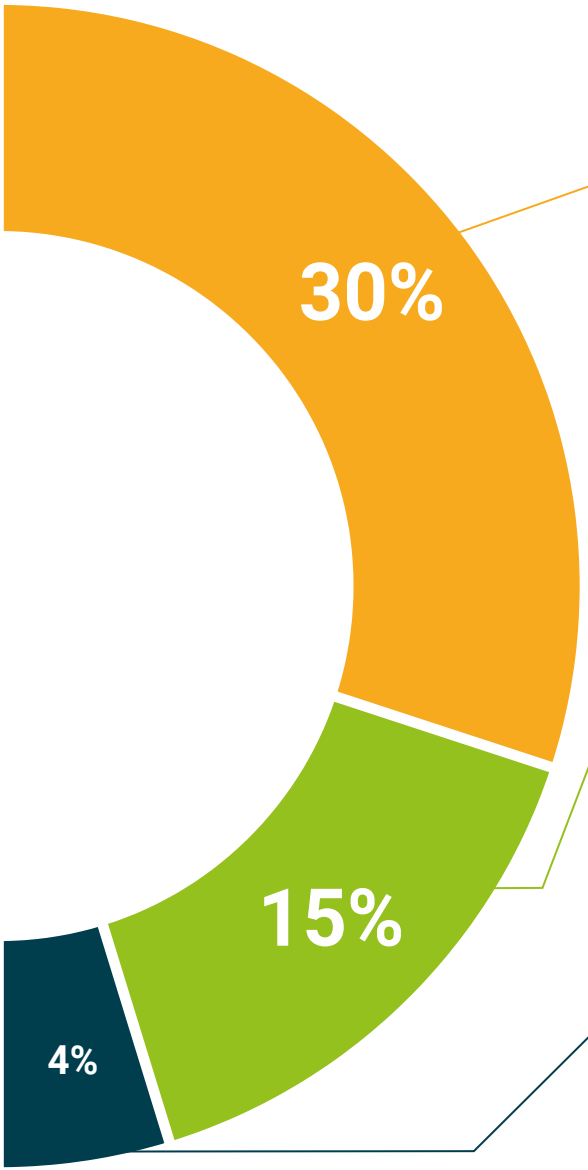
Práticas de aptidões e competências

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 gestor de topo necessita de desenvolver no contexto 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 tutelados pelos melhores especialistas em gestão de topo 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.

08

O perfil dos nossos alunos

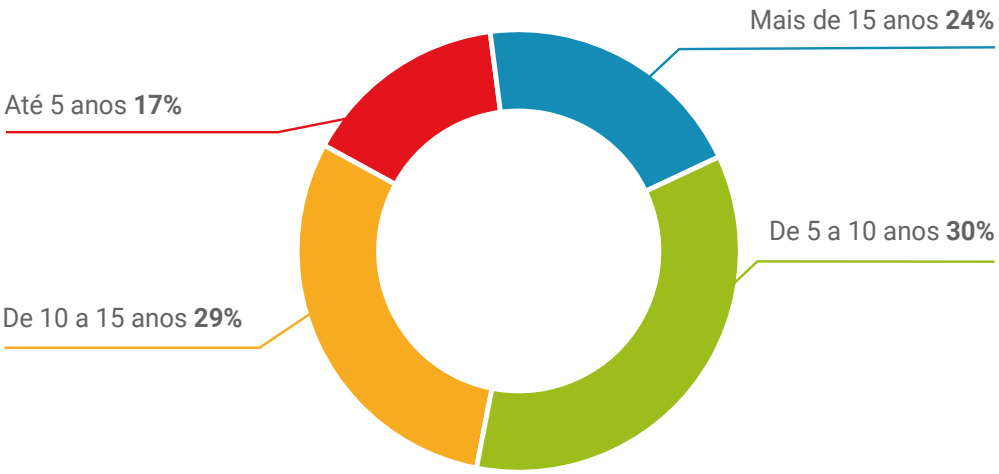
O MBA em Gestão de Cibersegurança (Chief Information Security Officer) é um programa dirigido a profissionais que desejam melhorar as suas competências através de uma educação de qualidade. Estudantes que pretendam alargar os seus conhecimentos noutro ramo ligado à atividade empresarial, como as TI, mas mais especificamente a segurança informática. Um programa destinado a profissionais experientes que acreditam na atualização contínua dos conhecimentos como método de aperfeiçoamento pessoal e profissional.

Os estudantes da TECH são profissionais com uma vasta experiência que procuram um trabalho melhor"

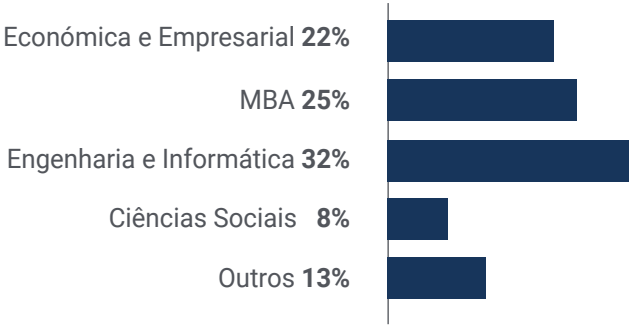
Idade média

Entre **35** e **45** anos

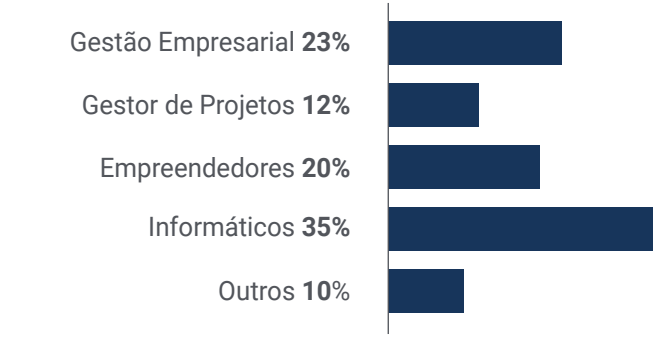
Anos de experiência



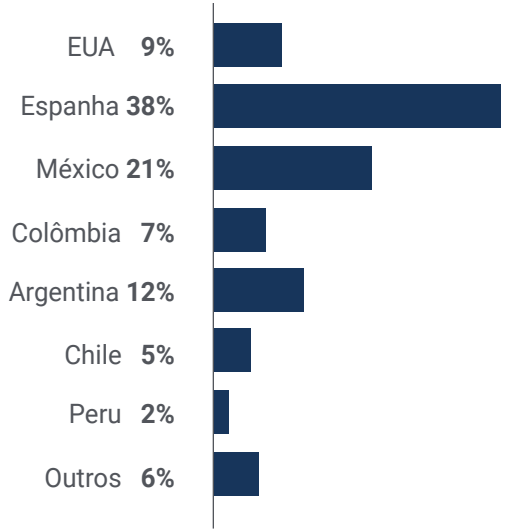
Formação



Perfil académico



Distribuição geográfica



Jaime Díaz

Chief Revenue Officer

"No ambiente empresarial em que trabalho, lidamos com muitas informações confidenciais e dados relevantes que, nas mãos erradas, podem criar um grande problema para a empresa. Por isso, há já algum tempo que pensava em aprofundar os meus conhecimentos em cibersegurança com o objetivo de controlar, eu próprio, todos os processos que podem ser mais sensíveis a uma ameaça informática. "Graças a este curso da TECH, consegui melhorar as minhas qualificações e tornar-me mais eficaz no exercício das minhas funções diárias"

09

Direção do curso

Os professores deste Executive Master MBA em Gestão de Cibersegurança (CISO, Chief Information Security Officer) são profissionais com vasta experiência no setor, tanto a nível profissional como educativo. A sua especialização neste campo permite-lhes ter as qualificações necessárias para oferecer aos estudantes um estudo completo e de alta-qualidade de matérias que serão úteis no seu trabalho diário no mundo dos negócios. São certamente pessoas que acreditam no ensino superior como uma forma de fazer avançar a sua profissão e melhorar a competitividade do seu negócio.

Um pessoal docente experiente para apoiar a sua especialização em cibersegurança"

Diretor Internacional Convidado

O Dr. 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 as suas contribuições relevantes para a investigação e o ensino posicionaram-no como uma figura-chave na **promoção da segurança** e a **compreensão das tecnologias emergentes** atualmente. Durante a sua carreira profissional, concebeu e dirigiu 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 experiência, publicou vários livros de grande relevância, todos eles relacionados com a **inteligência criminal**, o **trabalho policial**, as **ciberameaças** e a **segurança internacional**. Deu também um contributo significativo para o sector da **Cibersegurança** com a publicação de numerosos artigos em revistas académicas, sobre o controlo da criminalidade em caso de catástrofes de grandes proporções, a luta contra o terrorismo, as agências de informação e a cooperação policial. Além disso, foi painelista e orador principal em várias conferências nacionais e internacionais, afirmando-se como uma referência na esfera académica e profissional.

O Dr. Lemieux desempenhou funções editoriais e de avaliação em várias organizações académicas, privadas e governamentais, o que reflete a sua influência e o seu empenho na excelência na sua área de especialização. Desta forma, a sua prestigiada carreira académica levou-o a desempenhar as funções de Professor de Estágios e de Diretor de Faculdade dos programas MPS em **Inteligência Aplicada**, **Gestão de riscos de Cibersegurança**, **Gestão Tecnológica** e **Gestão de Tecnologias da Informação** na **Universidade de Georgetown**.

Doutor Frederic Lemieux

- Diretor do Mestrado em Cybersecurity Risk Management na Universidade de Georgetown nos Estados Unidos
- Diretor do Mestrado em Technology Management na Universidade de Georgetown
- Diretor do Mestrado em Applied Intelligence na Universidade de Georgetown
- Professor de Estágio na Universidade de Georgetown
- Doutoramento em Criminologia pela School of Criminology na Universidade de Montreal
- Licenciado em Sociologia e Minor Degree em Psicologia pela Universidade de Laval
- Membro do New Program Roundtable Committee na Universidade de Georgetown

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

Direção

Sra. Sonia Fernández Sapena

- Formadora em Segurança Informática e Hacking Ético. Centro Nacional de Referência de Getafe em Informática e Telecomunicações. Madrid
- Instrutora certificada E-Council. Madrid
- 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). Universidad de las Islas Baleares
- Engenheira em Informática. Universidad de Alcalá de Henares. Madrid
- Mestrado em DevOps: Docker and Kubernetes. Cas-Training. Madrid
- Microsoft Azure Security Technologies. E-Council. Madrid

Professores

Sr. José Francisco Catalá Barba

- Gestão intermédia no MINISDEF Diferentes funções e responsabilidades no âmbito do GOE III, tais como administração e gestão de incidentes da rede interna, implementação de programas feitos à medida para diferentes áreas, cursos de formação para utilizadores da rede e pessoal do grupo no geral.
- Técnico eletrónico na Fábrica Ford localizada em Almusafes, Valência, programação de robôs, PLCs, reparação e manutenção
- Técnico Eletrónico
- Desenvolvedor de aplicações para dispositivos móveis

Sr. Álvaro Jiménez Ramos

- 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 por Deusto Formación

Sra. Victoria Alicia Marcos Sbarbaro

- Desenvolvedora de Aplicações Móveis Android Nativas na B60 UK
- Analista Programadora para a gestão, coordenação e documentação de ambiente virtualizado de alarme de segurança nas instalações do cliente
- Analista Programadora de aplicações Java para caixas multibanco nas instalações do cliente
- Profissional de Desenvolvimento de Software para aplicação de validação de assinaturas e gestão documental nas instalações do cliente
- Técnico de Sistemas para a migração de equipamentos e para a gestão, manutenção e formação de dispositivos móveis PDAs nas instalações do cliente
- Engenharia Técnica em Sistemas Informáticos Universitat Oberta de Catalunya (UOC)
- Mestrado em Segurança Informática e Hacking Ético Oficial EC- Council e CompTIA pela Escuela Profesional de Nuevas Tecnologías CICE

Sr. Jon Peralta Alonso

- Advogado / DPO Altia Consultores S.A.
- Docente do Mestrado em Proteção de Dados Pessoais, Cibersegurança e Direito das TIC. Universidade Pública do País Basco (UPV-EHU)
- Advogado / Consultor jurídico Arriaga Asociados Asesoramiento Jurídico y Económico, S.L.
- Consultor Jurídico / Estagiário. Gabinete profissional: Oscar Padura
- Licenciatura em Direito. Universidade Pública do País Basco
- Mestrado em Delegado de Proteção de Dados. EIS Innovative School
- Mestrado em Direito. Universidade Pública do País Basco
- Mestrado em Prática de Contencioso Civil. Universidade Internacional Isabel I de Castilla

Jesús Serrano Redondo

- Junior FrontEnd Developer e Junior Cybersecurity Technician
- Desenvolvedor FrontEnd na Telefónica, Madrid
- Desenvolvedor FrontEnd. Best Pro Consulting SL, Madrid
- Instalador de equipamento e serviços de telecomunicações. Grupo Zener, Castilla y León
- Instalador de equipamento e serviços de telecomunicações. Lican Comunicaciones SL, Castilla y León
- Certificado em Segurança Informática. CFTIC Getafe, Madrid
- Técnico Superior: Sistemas Telecomunicações e Informáticos. IES Trinidad Arroyo, Palencia
- Técnico Superior: Instalações Eletrotécnicas de MT e BT. IES Trinidad Arroyo, Palencia
- Formação em engenharia inversa, estenografia, encriptação. Academia Hacker Incibe (Talentos Incibe)

A TECH selecionou cuidadosamente a equipa docente deste programa, para que possa aprender com os melhores especialistas da atualidade"

10

Impacto para a sua carreira

A conclusão deste MBA em Gestão da Cibersegurança (Chief Information Security Officer) acrescentará uma mais-valia qualitativa à qualificação dos profissionais das empresas, oferecendo todos esses conhecimentos que, embora possam parecer totalmente distantes do seu trabalho quotidiano, podem ser muito úteis para controlar os processos informáticos que possam albergar um elemento externo prejudicial que afete toda a organização. Por este motivo, é essencial uma maior especialização neste campo, não só para o desenvolvimento pessoal e profissional dos estudantes, mas também para as empresas em que trabalham.

A TECH coloca todos os seus recursos académicos à disposição dos seus estudantes para que estes adquiram as competências necessárias para os levar ao sucesso"

A conclusão deste MBA permitirá aos estudantes adquirirem a competitividade necessária para fazerem uma mudança radical na sua carreira.

Está pronto para progredir na sua carreira? Espera-o um excelente aperfeiçoamento profissional

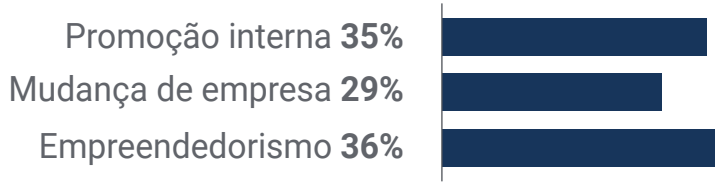
O MBA em Gestão de Cibersegurança (Chief Information Security Officer) da TECH - Universidade Tecnológica é um programa intensivo e de alto valor que visa melhorar as competências profissionais dos estudantes numa área altamente competitiva. Trata-se, sem dúvida, de uma oportunidade única de aperfeiçoamento profissional, mas também pessoal, pois implica esforço e dedicação.

Os estudantes que querem superar-se, fazer uma mudança profissional positiva e interagir com os melhores, encontrarão o seu lugar na TECH.

Um programa com um elevado nível académico para conduzir a sua carreira ao sucesso.

Momento de mudança

Tipo de mudança



Melhoria salarial

A conclusão deste curso significa um aumento salarial de mais de **25,22%**
]para os nossos estudantes**.**

Salário anual anterior	Aumento salarial anual de	Salário anual posterior
57.900 €	**25,22%**	**72.500 €**

11

Benefícios para a sua empresa

O MBA em Gestão de Cibersegurança (Chief Information Security Officer) contribui para elevar o talento da organização a todo o seu potencial através da especialização de líderes de alto nível. Desta forma, os profissionais das empresas poderão trazer uma qualidade acrescida para a sua empresa, ao possuírem as competências necessárias para controlarem eles próprios os processos de cibersegurança. Um programa que se adapta aos estudantes para que estes adquiram as ferramentas necessárias que mais tarde possam aplicar na sua prática diária, obtendo grandes benefícios para a sua empresa.

Um programa indispensável para profissionais de negócios que querem monitorizar e gerir potenciais problemas de Cibersegurança"

Desenvolver e reter o talento nas empresas é o melhor investimento a longo prazo.

01

Crescimento do talento e do capital intelectual

O profissional vai levar para a empresa novos conceitos, estratégias e perspetivas que possam trazer mudanças relevantes na organização.

02

Reter gestores de alto potencial para evitar a perda de talentos

Este programa reforça a ligação entre a empresa e o profissional e abre novos caminhos para o crescimento profissional dentro da empresa.

03

Construção de agentes de mudança

Ser capaz de tomar decisões em tempos de incerteza e crise, ajudando a organização a ultrapassar obstáculos.

04

Maiores possibilidades de expansão internacional

Este programa colocará a empresa em contacto com os principais mercados da economia mundial.

05

Desenvolvimento de projetos próprios
O profissional pode trabalhar num projeto real ou desenvolver novos projetos no domínio de I&D ou Desenvolvimento Comercial da sua empresa.

06

Aumento da competitividade
Este programa dotará os seus profissionais das competências necessárias para enfrentar novos desafios e assim impulsionar a organização.

12

Certificação

O Executive Master MBA em Gestão de Cibersegurança (CISO, Chief Information Security Officer) garante, para além de um conteúdo mais rigoroso e atualizado, o acesso a um Executive Master 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 **Executive Master em MBA Gestão de Cibersegurança (CISO, Chief Information Security Officer)** conta com o conteúdo educacional 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 **Executive Master** emitido pela **TECH Universidade Tecnológica.**

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

Certificação: **Executive Master em MBA Gestão de Cibersegurança (CISO, Chief Information Security Officer)**

Modalidade: **online**

Duração: **12 meses**

ECTS: **60**


tech universidade tecnológica

Concede o presente

CERTIFICADO

a

Sr./Sra. _____ com documento de identificação nº_____

por ter concluído e acreditado com sucesso o programa de

EXECUTIVE MASTER

em

MBA Gestão de Cibersegurança (CISO, Chief Information Security Officer)

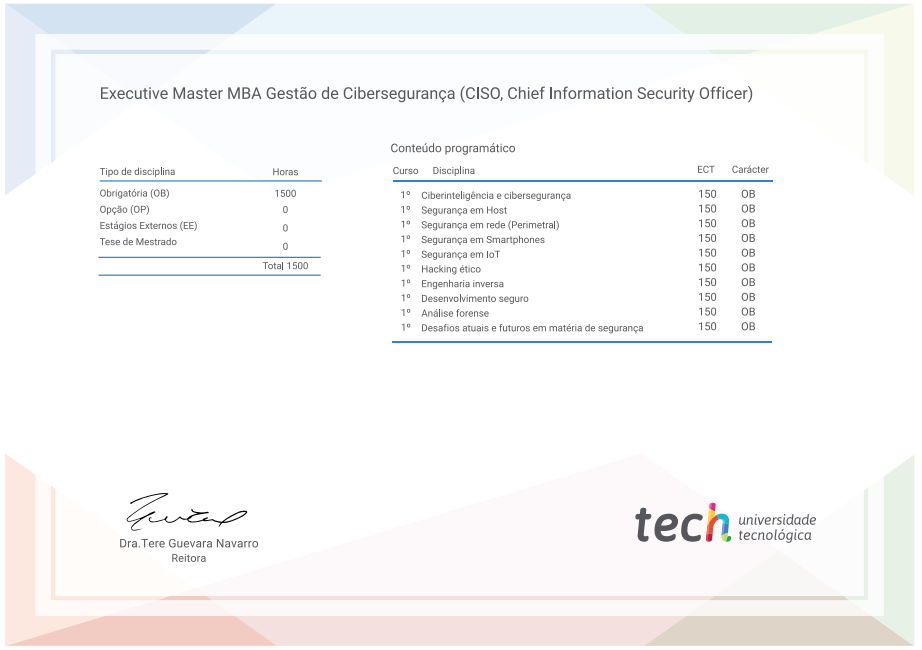
Este é um certificado atribuído por esta Universidade, com a duração de 1500 horas, com data de início a dd/mm/aaaa e data de conclusão a dd/mm/aaaaa.

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

Dra.Tere Guevara Navarro
Reitora

código único TECH: AFWOR23S techtitute.com/titulos


Executive Master MBA Gestão de Cibersegurança (CISO, Chief Information Security Officer)

Tipo de disciplina	Horas
Obrigatória (OB)	1500
Opção (OP)	0
Estágios Externos (EE)	0
Tese de Mestrado	0
	Total 1500

Conteúdo programático

Curso	Disciplina	ECT	Carácter
1º	Ciberinteligência e cibersegurança	150	OB
1º	Segurança em Host	150	OB
1º	Segurança em rede (Perimetral)	150	OB
1º	Segurança em Smartphones	150	OB
1º	Segurança em IoT	150	OB
1º	Hacking ético	150	OB
1º	Engenharia inversa	150	OB
1º	Desenvolvimento seguro	150	OB
1º	Análise forense	150	OB
1º	Desafios atuais e futuros em matéria de segurança	150	OB

Dra.Tere Guevara Navarro
Reitora

tech universidade tecnológica

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

tech universidade tecnológica

Executive Master
MBA em Gestão de Cibersegurança (CISO, Chief Information Security Officer)

- Modalidade: **online**
- Duração: **12 meses**
- Certificação: **TECH Universidade Tecnológica**
- Créditos: **60 ECTS**
- Horário: **ao seu próprio ritmo**
- Exames: **online**

Executive Master

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

tech universidade tecnológica