Executive Master

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

MBA DC CISO

tech universidade tecnológica

tech universidade tecnológica

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

- Modalidade: **online**
- Duração: **12 meses**
- Certificado: **TECH Universidade Tecnológica**
- Horário: **no seu próprio ritmo**
- Provas: **online**

Acesso ao site: **www.techtitute.com/br/escola-de-negocios/executive-master/executive-master-mba-gestao-seguranca-cibernetica-ciso-chief-information-security-officer**

Índice

01

Boas-vindas

A sociedade de hoje está hiperconectada. A era da informação permite que os cidadãos tenham conhecimento de qualquer informação com um simples clique de um botão. Mas isto também significa que as ameaças virtuais estão na ordem do dia, o que coloca mais do que nunca as empresas em risco de receberem um *software* malicioso que pode prejudicar sua produção e segurança, e até mesmo os dados pessoais de clientes e funcionários, expondo suas fraquezas em TI. Embora a proteção nesta área seja o trabalho dos especialistas em TI, cada vez mais os *chief revenue officers*, e outros gerentes, estão escolhendo se especializar neste campo para tentar deter os cibercriminosos e evitar ser alvo de seus ataques. Por esta razão, a TECH desenvolveu este programa, no qual os profissionais das empresas encontrarão as informações mais relevantes do momento, através de um programa de estudos didático que será de fácil compreensão para os alunos. Desta forma, e graças ao conhecimento adquirido, o graduado poderá atuar com total sucesso na posição de Chief Information Security Officer, um cargo em plena ascensão e com grandes perspectivas de crescimento.

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

Aprimore suas habilidades em Gestão de Segurança Cibernética com 10 Masterclasses ministradas por um especialista de prestígio internacional"

02

Por que estudar na TECH?

A TECH é a maior escola de negócios 100% online do mundo. Trata-se de uma Escola de Negócios de elite, com o mais alto nível acadêmico. Um centro internacional de alto desempenho e de capacitação intensiva das habilidades de gestão.

A TECH é uma universidade na vanguarda da tecnologia, que coloca todos os seus recursos à disposição do aluno para ajudá-lo a 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 alto reconhecimento internacional que proporcionará aos alunos o conhecimento necessário para se desenvolverem em um mundo dinâmico, onde a inovação deve ser a principal aposta de todo empresário.

"Caso de Sucesso Microsoft Europa" por incorporar aos cursos um inovador sistema interativo de multivídeo.

Máxima exigência

O critério de admissão da TECH não é econômico. Você não precisa fazer um grande investimento para estudar nesta universidade. No entanto, para concluir os cursos da TECH, os limites de inteligência e capacidade do aluno serão testados. O padrão acadêmico desta instituição é muito alto...

95% | **dos alunos da TECH finalizam seus estudos com sucesso.**

Networking

Os cursos da TECH são realizados por profissionais de todo o mundo, permitindo que os alunos possam criar uma ampla rede de contatos que será útil para seu futuro.

+100.000
gestores capacitados a cada ano

+200
nacionalidades diferentes

Empowerment

O aluno crescerá ao lado das melhores empresas e dos profissionais mais prestigiosos e influentes. A TECH desenvolveu parcerias estratégicas e uma valiosa rede de contatos com os principais agentes econômicos dos 7 continentes.

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

Talento

Este programa é uma proposta única para revelar o talento do aluno no mundo dos negócios. Uma oportunidade para demonstrar suas inquietudes e sua visão de negócio.

Ao concluir este programa, a TECH ajuda o aluno a mostrar ao mundo o seu talento.

Contexto Multicultural

Ao estudar na TECH, o aluno irá desfrutar de uma experiência única. Estudará em um contexto multicultural. Em um curso com visão global, através do qual poderá aprender sobre a forma de trabalhar em diferentes partes do mundo, reunindo as informações mais atuais que melhor se adaptam à sua ideia de negócio.

A TECH conta com alunos de mais de 200 nacionalidades.

Aprenda com os melhores

Em sala de aula, a equipe de professores da TECH explica o que os levou ao sucesso em suas empresas, trabalhando a partir de um contexto real, animado e dinâmico. Professores que se envolvem ao máximo para oferecer uma capacitação de qualidade, permitindo que o aluno cresça profissionalmente e se destaque no mundo dos negócios.

Professores de 20 nacionalidades diferentes.

Na TECH você terá acesso aos estudos de casos mais rigorosos e atuais do mundo acadêmico"

A TECH prima pela excelência e, para isso, conta com uma série de características que a tornam uma universidade única:

Análise

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

Excelência acadêmica

A TECH coloca à disposição do aluno a melhor metodologia de aprendizagem online. A universidade combina o método Relearning (a metodologia de aprendizagem de pós-graduação mais bem avaliada internacionalmente) com o Estudo de Caso. Tradição e vanguarda em um equilíbrio desafiador, com o itinerário acadêmico mais rigoroso.

Economia de escala

A TECH é a maior universidade online do mundo. Conta com um portfólio de mais de 10.000 cursos de pós-graduação. E na nova economia, **volume + tecnologia = preço disruptivo**. Dessa forma, garantimos que estudar não seja tão caro quanto em outra universidade.

03

Por que o nosso programa?

Realizar o programa da TECH significa multiplicar suas chances de alcançar o sucesso profissional na alta gestão empresarial.

É um desafio que exige esforço e dedicação, mas que abre as portas para um futuro promissor. O aluno aprenderá com a melhor equipe de professores e com a mais flexível e inovadora metodologia educacional.

Contamos com o corpo docente mais prestigiado e o plano de estudos mais completo do mercado, o que nos permite oferecer a você uma capacitação do mais alto nível acadêmico”

Este curso irá proporcionar diversas vantagens profissionais e pessoais, entre elas:

01

Dar um impulso definitivo na carreira do aluno

Ao estudar na TECH, o aluno será capaz de assumir o controle do seu futuro e desenvolver todo o seu potencial. Ao concluir este programa, o aluno irá adquirir as habilidades necessárias para promover uma mudança positiva em sua carreira em um curto espaço de tempo.

70% dos participantes desta capacitação alcançam uma mudança profissional positiva em menos de 2 anos.

02

Desenvolver uma visão estratégica e global da empresa

A TECH oferece uma visão aprofundada sobre gestão geral, permitindo que o aluno entenda como cada decisão afeta as diferentes áreas funcionais da empresa.

Nossa visão global da empresa irá melhorar sua visão estratégica.

03

Consolidar o aluno na gestão empresarial

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

Você irá trabalhar mais de 100 casos reais de alta gestão.

04

Você irá assumir novas responsabilidades

Durante o programa de estudos, serão apresentadas as últimas tendências, avanços e estratégias, para que os alunos possam desenvolver seu trabalho profissional em um ambiente que está em constante mudança.

45% dos alunos são promovidos dentro da empresa que trabalham.

05

Acesso a uma poderosa rede de contatos

A TECH conecta seus alunos para maximizar as oportunidades. Alunos com as mesmas inquietudes e desejo de crescer. Assim, será possível compartilhar parceiros, clientes ou fornecedores.

Você irá encontrar uma rede de contatos essencial para o seu desenvolvimento profissional.

06

Desenvolver projetos empresariais de forma rigorosa

O aluno irá adquirir uma visão estratégica aprofundada que irá ajudá-lo a desenvolver seu próprio projeto, levando em conta as diferentes áreas da empresa.

20% dos nossos alunos desenvolvem sua própria ideia de negócio.

07

Melhorar *soft skills* e habilidades de gestão

A TECH ajuda o aluno a aplicar e desenvolver os conhecimentos adquiridos e melhorar suas habilidades interpessoais para se tornar um líder que faz a diferença.

Melhore as suas habilidades de comunicação e liderança e impulsione a sua carreira.

08

Fazer parte de uma comunidade exclusiva

O aluno fará parte de uma comunidade de gestores de elite, grandes empresas, renomadas instituições e profissionais qualificados procedentes das universidades mais prestigiadas do mundo: a comunidade TECH Universidade Tecnológica.

Oferecemos a você a oportunidade de se especializar com uma equipe de professores internacionalmente reconhecida.

04

Objetivos

Este Executive Master da TECH destina-se a reforçar as competências profissionais dos gestores de empresas que, além de estarem altamente especializados na sua área de atuação, encontrarão neste programa de estudos uma oportunidade única de melhoria num setor de grande importância, pois aprenderão a prevenir possíveis ameaças na internet que podem causar sérios danos às empresas. Dessa forma, se tornarão profissionais especialistas em diferentes ramos e poderão controlar todas as áreas da empresa, tornando-se assim Chief Information Security Officer.

Aprimore sua capacitação e alcance seus objetivos profissionais através deste Executive Master oferecido pela TECH"

Seus objetivos são os objetivos da TECH
Trabalhamos juntos para alcançá-losa

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

01 Analisar o papel do analista de cibersegurança

02 Aprofundar a compreensão da engenharia social e seus métodos

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

04 Conduzir uma análise de risco e compreender a métrica de risco

05 Determinar o uso apropriado do anonimato e o uso de redes como TOR, I2P e Freenet

06 Reunir os regulamentos de segurança cibernética existentes

07 Gerar conhecimento especializado para a realização de uma auditoria de segurança

08 Desenvolver políticas de uso apropriadas

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

10 Avaliar novos sistemas de detecção de ameaças, e sua evolução a partir de soluções mais tradicionais

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

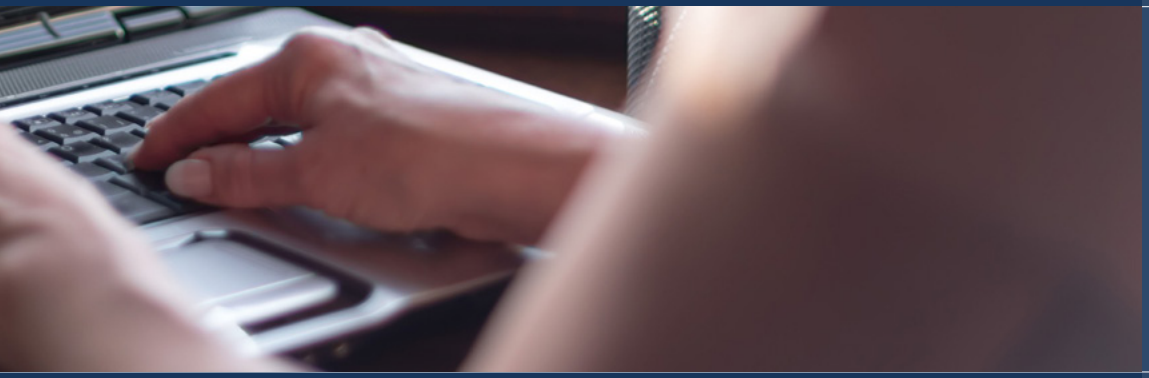
12 Identificar, analisar e avaliar os riscos de segurança dos componentes do projeto IoT

13 Avaliar as informações obtidas e desenvolver mecanismos de prevenção e hacking

14 Aplicar a engenharia reversa ao ambiente de segurança cibernética

15 Especificar os testes a serem realizados no software desenvolvido

16 Coletar todas as provas e dados existentes para realizar um relatório forense



17 Apresentar devidamente o relatório forense

18 Analisar o estado atual e futuro da segurança de TI

19 Examinar os riscos das tecnologias novas e emergentes

20 Compilar as diferentes tecnologias em relação à segurança cibernética

05

Competências

O Executive Master em MBA en Gestão de Segurança Cibernética (CISO, Chief Information Security Officer) foi planejado com o objetivo de melhorar a competitividade dos profissionais do setor empresarial. Por isso, ao finalizar os estudos, o profissional terá adquirido as competências necessárias para desenvolver uma prática atualizada e de qualidade, baseada a metodologia de ensino mais inovadora. Sem dúvida, um programa de estudos que irá melhorar a a qualificação dos alunos e permitir que sejam mais competitivo na sua prática diária, ao unificar todos os aspetos relevantes da segurança cibernética que os gestores devem conhecer e colocar em prática.

Aprofunde-se no estudo da segurança cibernética e melhore suas habilidades para controlar potenciais ameaças da rede"

01 Conhecer as metodologias utilizadas em matéria de segurança cibernética

02 Avaliar qualquer tipo de ameaça para proporcionar uma solução adequada às respectivas situações

03 Gerar soluções inteligentes e completas de automatização do comportamento diante dos incidentes

04 Saber avaliar os riscos associados às vulnerabilidades tanto dentro quanto fora da empresa

05 Entendendo a evolução e o impacto do IoT ao longo do tempo

06 Demonstrar que um sistema é vulnerável, atacando-o de forma preventiva e abordando tais problemas

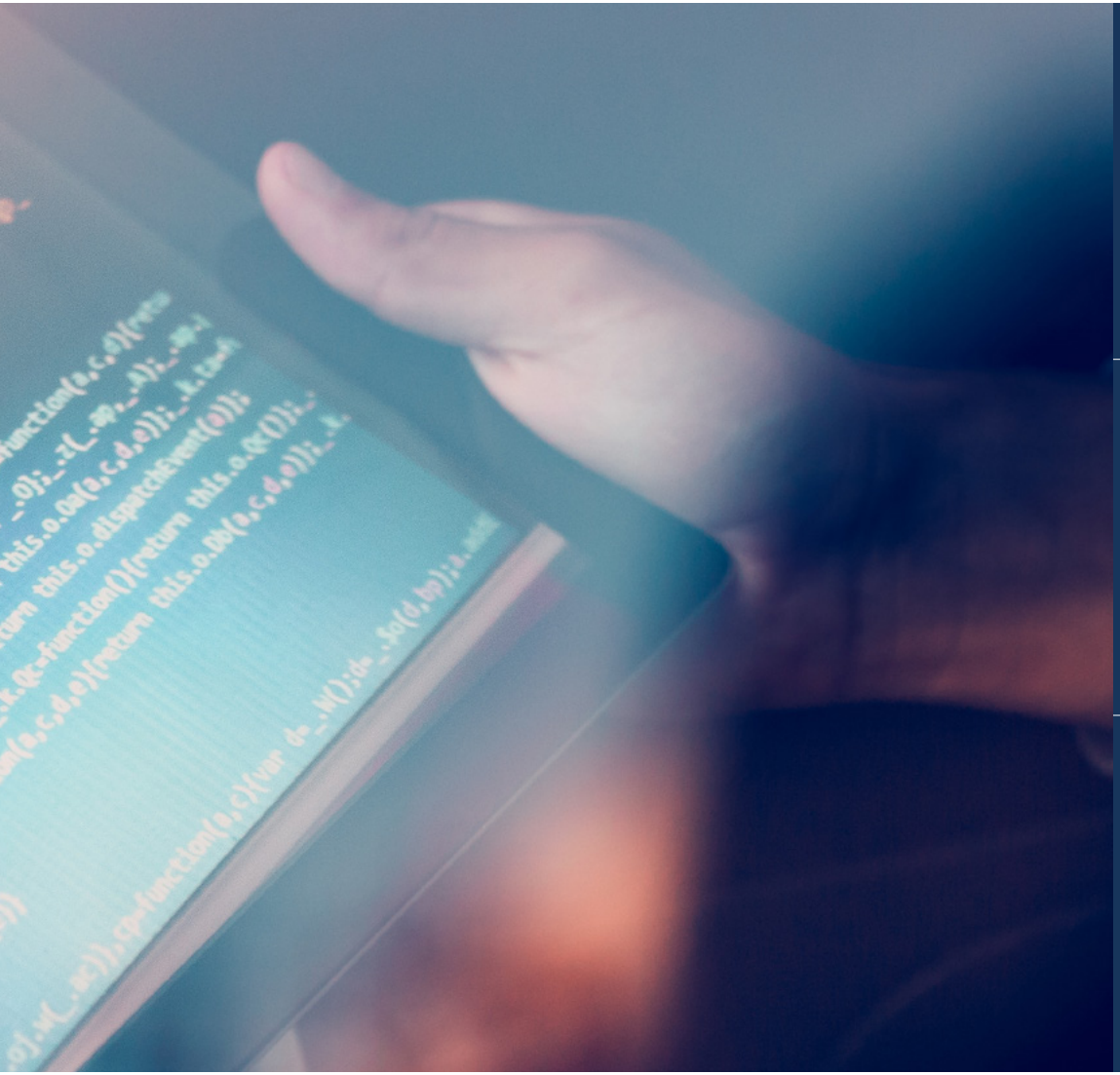
07 Saber como aplicar o *Sandboxing* em diferentes ambientes

08 Conhecer as diretrizes que um bom desenvolvedor deve seguir a fim de cumprir os requisitos de segurança necessários

09 Realizar operações de segurança defensiva

10 Ter uma percepção profunda e especializada da segurança de TI

11 Aplicar processos de segurança para smartphones e dispositivos portáteis



12 Conhecer os meios para realizar o chamado *Hacking* ético e proteger a empresa de um ataque cibernético

13 Ser capaz de investigar um incidente de segurança cibernética

14 Diferenciar entre as técnicas de ataque e defesa disponíveis

06

Estrutura e conteúdo

Este programa de estudos da TECH foi desenvolvido pensando nas necessidades de especialização dos profissionais de negócios que desejam ampliar seus conhecimentos em segurança cibernética, um campo fundamental para poder controlar essas possíveis ameaças que podem representar um grande risco para a empresa. Sendo assim, este curso lhes permitirá adquirir conhecimentos específicos que poderão aplicar à sua prática profissional. E, para isso, eles usarão uma metodologia totalmente online que permitirá combinar seu estudo com o restante de suas obrigações diárias.

Este programa de estudos será essencial para detectar possíveis ciberataques na sua empresa"

Plano de estudos

O conteúdo do MBA em Gestão de Cibersegurança (CISO, Chief Information Security Officer) foi elaborado para fomentar o desenvolvimento de habilidades gerenciais que permitem uma tomada de decisão mais rigorosa em ambientes de maior incerteza.

Ao longo de 2.700 horas de estudo, o aluno adquirirá as habilidades necessárias para se desenvolver com sucesso em sua prática diária. Tratando-se, portanto, de uma verdadeira imersão em situações reais de negócios.

Este programa aborda detalhadamente as diferentes áreas de uma empresa, cuja finalidade é proporcionar aos profissionais uma compreensão da cibersegurança, partindo de uma perspectiva estratégica, internacional e inovadora.

Um plano de estudos desenvolvido especialmente para os alunos, voltado para seu aperfeiçoamento profissional e para prepará-los para alcançar a excelência no campo da direção e gestão da segurança cibernética. Oferecemos um programa que compreende as necessidades de sua empresa por meio de um conteúdo inovador baseado nas últimas tendências e apoiado pela melhor metodologia educacional e por um corpo docente excepcional.

Acrescentamos a tudo isso 10 Masterclasses exclusivas que fazem parte do material didático, representando a vanguarda da tecnologia e da educação. Essas aulas foram elaboradas por um especialista de prestígio internacional nas áreas de inteligência, segurança cibernética e tecnologias disruptivas. São recursos importantes que ajudarão o profissional executivo a se especializar em Gestão de Segurança Cibernética e a gerenciar com eficácia os departamentos da empresa dedicados a essa importante área.

O programa tem uma duração de 12 meses e está dividido em 15 módulos:

Módulo 1	Ciberinteligência e Cibersegurança
Módulo 2	Segurança do *Host*
Módulo 3	Segurança de rede (perímetro)
Módulo 4	Segurança para *Smartphones*
Módulo 5	Segurança de IoT
Módulo 6	*Hacking* ético
Módulo 7	Engenharia inversa
Módulo 8	Desenvolvimento seguro
Módulo 9	Análise Forense
Módulo 10	Desafios atuais e futuros da segurança cibernética
Módulo 11	Liderança, Ética e Responsabilidade Social Corporativa
Módulo 12	*Gestão de Pessoas e Gestão de Talentos*
Módulo 13	*Gestão Econômico-Financeira*
Módulo 14	*Gestão Comercial e Marketing Estratégico*
Módulo 15	*Gestão* Executiva

Onde, quando e como é ensinado?

A TECH oferece a possibilidade a seus alunos de realizar este programa completamente online. Durante os 12 meses de capacitação, você poderá acessar todo o conteúdo deste programa a qualquer momento, o que lhe permitirá gestionar o seu tempo de estudo.

Uma experiência de capacitação única, fundamental e decisiva para impulsionar seu crescimento profissional.

Módulo 1. Ciberinteligência e Cibersegurança

1.1. Ciberinteligência
1.1.1. Ciberinteligência
1.1.1.1. 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. Vias do analista de inteligência em atividade avaliativa

1.2. Segurança Cibernética
1.2.1. Camadas de segurança
1.2.2. Identificação de ameaças cibernéticas
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 comumente utilizados

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

1.4. Metodologias de avaliação
1.4.1. Análise de inteligência
1.4.2. Técnicas para organizar as informações adquiridas
1.4.3. Confiabilidade 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. Auditoria na segurança da informática
1.5.2. Documentação e licenças para auditoria
1.5.3. Tipos de auditoria
1.5.4. Entregáveis
1.5.4.1. Relatório técnico
1.5.4.2. Relatório Executivo

1.6. Anonimato na rede
1.6.1. Uso do anonimato
1.6.2. Técnicas de anonimización (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 de rede
1.7.4. Segurança lógica
1.7.5. Segurança de Aplicações Web
1.7.6. Segurança da dispositivos móveis

1.8. Regulamentos e *compliance*
1.8.1. RGPD
1.8.2. A estratégia nacional de cibersegurança de 2019
1.8.3. Família ISO 27000
1.8.4. Estrutura de Segurança Cibernética da NIST
1.8.5. PIC
1.8.6. ISO 27032
1.8.7. Normativas *cloud*
1.8.8. SOX
1.8.9. PC

1.9. Análise de risco e métricas
1.9.1. Escopo dos riscos
1.9.2. O patrimônio
1.9.3. Ameaças
1.9.4. Vulnerabilidades
1.9.5. Avaliação de risco
1.9.6. Tratamento de risco

1.10. Importantes órgãos de segurança cibernética
1.10.1. NIST
1.10.2. ENISA
1.10.3. INCIBE
1.10.4. OEA
1.10.5. UNASUR - PROSUR

Módulo 2. Segurança do *Host*

2.1. Cópias de segurança
2.1.1. Estratégias para backups
2.1.2. Ferramentas para Windows
2.1.3. Ferramentas para Linux
2.1.4. Ferramentas para MacOS

2.2. Anti-vírus do usuário
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. Detectores de intrusão - HIDS
2.3.1. Métodos de detecção de intrusão
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 senhas
2.5.1. Password
2.5.2. LastPass
2.5.3. KeePass
2.5.4. StickyPassword
2.5.5. RoboForm

2.6. Detectores de *phishing*
2.6.1. Detecção manual de *Phishing*
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-tracking

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. Controle 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 atualização
2.10.4. Privilégios para instalar software

Módulo 3. Segurança de rede (perímetro)

3.1. Sistemas de detecção e prevenção de ameaças
3.1.1. Estrutura geral para incidentes de segurança
3.1.2. Sistemas de defesa atuais: *Defense in Depth* e SOC
3.1.3. Arquiteturas de redes atuais
3.1.4. Tipos de ferramentas de detecção 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 detecção de instâncias/hosts, containers e serverless

3.2. *Firewall*
3.2.1. Tipos de *firewalls*
3.2.2. Ataques e atenuações
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 detecção 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 detecção e prevenção de intrusão (IDS/ IPS)
3.3.1. Ataques ao IDS/IPS
3.3.2. Sistemas IDS/IPS
3.3.2.1. Snort
3.3.2.2. Suricata

3.4. *Firewalls* de próxima geração (NGFWS)
3.4.1. Diferencias entre NGFW e *Firewall* tradicional
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. Uso de *Proxy* Vantagens e Desvantagens

3.6. Motores antivírus
3.6.1. Contexto geral de *Malware* e IOCS
3.6.2. Problemas no motor do antivírus

3.7. Sistemas de proteção de correio
3.7.1. Antispam
3.7.1.1. Listas negras e brancas
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 uso
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 para *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. As 10 principais vulnerabilidades
4.2.2. Comunicações, redes e modos de conexão

4.3. O dispositivo móvel no ambiente empresarial
4.3.1. Riscos
4.3.2. Políticas de segurança
4.3.3. Monitoramento de dispositivos
4.3.4. Gerenciamento de dispositivos móveis (MDM)

4.4. Privacidade do usuário e segurança dos dados
4.4.1. Estados de informação
4.4.2. Proteção e confidencialidade dos dados
4.4.2.1. Permissões
4.4.2.2. Criptografia
4.4.3. Armazenamento seguro de dados
4.4.3.1. Armazenamento seguro no 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. Usuário não forçado
4.6.2. *Malware*
4.6.2.1. Tipos de malware
4.6.3. Engenharia social
4.6.4. Vazamento de dados
4.6.5. Roubo de informações
4.6.6. Redes Wi-Fi inseguras
4.6.7. Software desatualizado
4.6.8. Aplicações maliciosas
4.6.9. Senhas 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. Fraude por personificação (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 aos modos de comunicação
4.7.3. Ataques de *Phishing*
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 de *Payload* e extração de informações
4.8.3. *Hacking* sobre dispositivos iOS: mecanismos e ferramentas
4.8.4. *Hacking* em dispositivos Android: mecanismos e ferramentas

4.9. Testes de penetração
4.9.1. iOS *pentesting*
4.9.2. Android *PenTesting*
4.9.3. Ferramentas

4.10. Segurança e proteção
4.10.1. Configurações de segurança
4.10.1.1. Nos dispositivos iOS
4.10.1.2. Dispositivos Android
4.10.2. Medidas de segurança
4.10.3. Ferramentas de proteção

Módulo 5. Segurança de 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 implementação
5.1.4. Tecnologias de conectividade

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 de 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. Automação doméstica
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. Fazendo pagamentos e obtendo serviços
5.6.3. Conectividade

5.7. *Wearables*
5.7.1. Roupas inteligentes
5.7.2. Joias inteligentes
5.7.3. Relógios Inteligentes

5.8. Setor de saúde
5.8.1. Exercício/monitoramento da frequência cardíaca
5.8.2. Monitoramento de pacientes e pessoas idosas
5.8.3. Implantável
5.8.4. Robôs cirúrgicos

5.9. Conectividade
5.9.1. Wi-Fi/Gateway
5.9.2. Bluetooth
5.9.3. Conectividade embutida

5.10. Securitização
5.10.1. Redes dedicadas
5.10.2. Gerenciador de senhas
5.10.3. Uso de protocolos criptografados
5.10.4. Dicas de uso

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. Implantação 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 código aberto (OSINT)
6.3.2. Busca de violações e vulnerabilidades de dados
6.3.3. Uso de ferramentas passivas

6.4. Escaneamento em rede
6.4.1. Ferramentas de escaneamento
6.4.1.1. Nmap
6.4.1.2. Hping3
6.4.1.3. Outras ferramentas de Escaneamento
6.4.2. Técnicas de digitalização
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 NetBIOS e Samba
6.5.4. Enumeração LDAP
6.5.5. Enumeração 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 Vulnerabilidade
6.6.2.1. CVSS
6.6.2.2. CVE
6.6.2.3. NVD

6.7. Ataques a redes sem fio
6.7.1. Metodologia de *Hacking* em redes wireless
6.7.1.1. Wi-Fi *Discovery*
6.7.1.2. Análise de tráfego
6.7.1.3. Ataques de *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 fio

6.8. Hacking de servidores web
6.8.1. *Cross Site Scripting*
6.8.2. CSRF
6.8.3. *Sessão Hijacking*
6.8.4. *SQLinjection*

6.9. Exploração de vulnerabilidades
6.9.1. Uso de *exploits* conhecidos
6.9.2. Uso de *metasploit*
6.9.3. Uso de *malware*
6.9.3.1. Definição e escopo
6.9.3.2. Geração de malware
6.9.3.3. Bypass de soluções anti-vírus

6.10. Persistência
6.10.1. Instalação de *rootkits*
6.10.2. Uso de ncat
6.10.3. Uso de tarefas programadas para *backdoors*
6.10.4. Criação de usuários
6.10.5. Detecção 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. Tratamento 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 Lexical LEX
7.2.2. Análise sintática
7.2.2.1. Gramáticas sem contexto
7.2.2.2. Tipos de análise sintática
7.2.2.2.1. Análise top-down
7.2.2.2.2. Análise bottom-up
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. Analizadores 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 Códigos 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. Uso do *break*
7.4.3. Funções

7.5. Arquitetura de Hardware x86
7.5.1. Arquitetura de do processador x86
7.5.2. Estruturas de dados de x86
7.5.3. Estruturas de Códigos de x86

7.6. Arquitetura de Hardware ARM
7.6.1. Arquitetura do processador ARM
7.6.2. Estruturas de dados de ARM
7.6.3. Estruturas de Códigos de 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 Dinâmica
7.8.1. Análise comportamental
7.8.1.1. Comunicações
7.8.1.2. Monitoração
7.8.2. Depuradores de código Linux
7.8.3. Depuradores de código no Windows

7.9. *Sandbox*
7.9.1. Arquitetura do *sandbox*
7.9.2. Evasão de *sandbox*
7.9.3. Técnicas de detecção
7.9.4. Técnicas de prevenção
7.9.5. Contra-medidas
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. Análises de *malware*
7.10.1. Métodos de análise de *malware*
7.10.2. Técnicas de ofuscação de *malware*
7.10.2.1. Ofuscação executável
7.10.2.2. Restrição de ambientes de execução
7.10.3. Ferramentas de análise de m*alware*

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. Controle de autenticação
8.2.2. Controle de papéis e privilégios
8.2.3. Requisitos orientados ao risco
8.2.4. Aprovação de privilégios

8.3. Fases de análise e projeto
8.3.1. Acesso aos componentes e administração do sistema
8.3.2. Pistas de auditoria
8.3.3. Gestão da sessão
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. Assegurando 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 seguras
8.5.1. Validação dos dados de entrada
8.5.2. Codificação dos dados de
8.5.3. Estilo de programação
8.5.4. Gerenciamento de registro de mudanças
8.5.5. Práticas criptográficas
8.5.6. Gerenciamento de erros e logs
8.5.7. Gerenciamento de arquivos
8.5.8. Gerenciamento de memória
8.5.9. Padronização e reutilização das funções de segurança

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

8.7. Preparação da BD *hardening*
8.7.1. Otimização do motor da BD
8.7.2. Criação de seu próprio usuário para a aplicação
8.7.3. Atribuição dos privilégios necessários ao usuário
8.7.4. *Hardening* da BD

8.8. Fase de testes
8.8.1. Controle de qualidade nos controles de segurança
8.8.2. Inspeção por fases de código
8.8.3. Verificação da gestão das configurações
8.8.4. Teste da caixa preta

8.9. Preparando a transição para a produção
8.9.1. Realizar o controle de mudanças
8.9.2. Realizar o procedimento de mudança de produção
8.9.3. Realizar o procedimento de *rollback*
8.9.4. Testes de pré-produção

8.10. Fase de manutenção
8.10.1. Garantia baseada em risco
8.10.2. Teste de manutenção de segurança da caixa branca
8.10.3. Teste de manutenção de segurança da caixa preta

Módulo 9. Análise Forense

9.1. Aquisição e replicação de dados
9.1.1. Aquisição volátil de dados
9.1.1.1. Informações do sistema
9.1.1.2. Informação da rede
9.1.1.3. Ordem de volatilidade
9.1.2. Aquisição estática de dados
9.1.2.1. Criação de uma imagem duplicada
9.1.2.2. Preparação de um documento de 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 das técnicas antiforenses
9.2.1. Objetivos das técnicas antiforenses
9.2.2. Eliminação de dados
9.2.2.1. Eliminação de dados e arquivos
9.2.2.2. Recuperação de arquivos
9.2.2.3. Recuperação de partições apagadas
9.2.3. Proteção por senha
9.2.4. Esteganografia
9.2.5. Limpeza segura do dispositivo
9.2.6. Criptografia

9.3. Sistema operacional forense
9.3.1. Windows Forensics
9.3.2. Forense Linux
9.3.3. Mac forensics

9.4. Análise forense de rede
9.4.1. Análise de logs
9.4.2. Correlação dos dados
9.4.3. Pesquisa de rede
9.4.4. Passos a seguir na análise forense da rede

9.5. Análise forense de site
9.5.1. Investigação de ataques na web
9.5.2. Detecção de ataques
9.5.3. Localização de endereços IP

9.6. Base de dados Forense
9.6.1. Forense da MSSQL
9.6.2. Forense da MySQL
9.6.3. Forense da Web
9.6.4. Forense da MSSQL

9.7. Forense da *MySQL*
9.7.1. Tipos de crimes em *Cloud*
9.7.1.1. Cloud como tema
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 em *Cloud*
9.7.4. Ferramentas de análise forense em *Cloud*

9.8. Investigação de crimes por e-mail
9.8.1. Sistemas de e-mail
9.8.1.1. Clientes de e-mail
9.8.1.2. Servidor de e-mail
9.8.1.3. Servidor SMTP
9.8.1.4. Servidor POP3
9.8.1.5. Servidor IMAP4

9.8.2. Crimes por e-mail
9.8.3. Mensagem de e-mail
9.8.3.1. Cabeçalhos padrão
9.8.3.2. Cabeçalhos estendidos
9.8.4. Passos para a investigação destes crimes
9.8.5. Ferramentas forenses por e-mail

9.9. Forense móvel
9.9.1. Redes celulares
9.9.1.1. Tipos de redes
9.9.1.2. Conteúdo 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 arquivo

9.10. Redação e apresentação de relatórios forenses
9.10.1. Aspectos 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. Lidando com a mídia

Módulo 10. Desafios atuais e futuros da segurança cibernética

10.1. Tecnologia *blockchain*
10.1.1. Área de aplicação
10.1.2. Garantia de confidencialidade
10.1.3. Garantia de não repudiação

10.2. Dinheiro digital
10.2.1. Bitcoins
10.2.2. Criptomonedas
10.2.3. Mineração de moedas criptográficas
10.2.4. Esquemas piramidais
10.2.5. Outros crimes e problemas potenciais

10.3. *Deepfake*
10.3.1. Impacto na mídia
10.3.2. Perigos para a sociedade
10.3.3. Mecanismos de detecção

10.4. O futuro da inteligência artificial
10.4.1. Inteligência artificial e computação cognitiva
10.4.2. Usos para simplificar o atendimento ao cliente

10.5. Privacidade digital
10.5.1. Valor dos dados na rede
10.5.2. Uso dos dados na rede
10.5.3. Gerenciamento de privacidade e identidade digital

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

10.7. Trabalho à distância
10.7.1. Revolução do trabalho à distância durante e após a Covid19
10.7.2. Engarrafamentos de acesso
10.7.3. Variação da superfície de ataque
10.7.4. As 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 en *Get Smart* ao invés 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 sobre o IPv4

10.10. O desafio de aumentar a conscientização da educação precoce e contínua da população
10.10.1. Estratégias atuais do governo
10.10.2. Resistência da população ao aprendizado
10.10.3. Planos de capacitação a serem adotados pelas empresas

Módulo 11. Liderança, Ética e Responsabilidade Social Corporativa

11.1. Globalização e Governança
11.1.1. Governança e Governo Corporativo
11.1.2. Fundamentos da Governança Corporativa em empresas
11.1.3. O papel do Conselho de Administração na estrutura da Governança Corporativa

11.2. Liderança
11.2.1. Liderança. Uma abordagem conceitual
11.2.2. Liderança nas Empresas
11.2.3. A importância do líder na direção de empresas

11.3. *Cross Cultural Management*
11.3.1. Conceito de *Cross Cultural Management*
11.3.2. Contribuições para o conhecimento das culturas nacionais
11.3.3. Gestão de Diversidade

11.4. Desenvolvimento de gestão e liderança
11.4.1. Conceito de desenvolvimento gerencial
11.4.2. Conceito de liderança
11.4.3. Teorias de liderança
11.4.4. Estilos de liderança
11.4.5. Inteligência na liderança
11.4.6. Os desafios da liderança atualmente

11.5. Ética empresarial
11.5.1. Ética e moral
11.5.2. Ética empresarial
11.5.3. Liderança e ética nas empresas

11.6. Sustentabilidade
11.6.1. Sustentabilidade e desenvolvimento sustentável
11.6.2. Agenda 2030
11.6.3. Empresas Sustentáveis

11.7. Responsabilidade Social da Empresa
11.7.1. Dimensão Internacional da Responsabilidade Social das Empresas
11.7.2. Implementação da Responsabilidade Social da Empresa
11.7.3. Impacto e Medição da Responsabilidade Social da Empresa

1.8. Sistemas e ferramentas de gerenciamento responsável
10.8.1. RSC: Responsabilidade social corporativa
11.8.2. Aspectos essenciais para implementar uma estratégia de gestão responsável
11.8.3. Passos para a implementação de um sistema de gestão de responsabilidade social corporativa
11.8.4. Ferramentas e padrões de Responsabilidade Social Corporativa (RSC)

11.9. Multinacionais e direitos humanos
11.9.1. Globalização, empresas multinacionais e direitos humanos
11.9.2. Empresas multinacionais perante o direito internacional
11.9.3. Instrumentos jurídicos para multinacionais em matéria de direitos humanos

11.10. Entorno legal e *Corporate Governance*
11.10.1. Regras internacionais de importação e exportação
11.10.2. Propriedade intelectual e industrial
11.10.3. Direito Internacional do Trabalho

Módulo 12. Gestão de Pessoas e Gestão de Talentos

12.1. Gestão estratégica de pessoas
12.1.1. Gestão estratégica e recursos humanos
12.1.2. Gestão estratégica de pessoas

12.2. Gestão de recursos humanos por competências
12.2.1. Análise do potencial
12.2.2. Política de remuneração
12.2.3. Planos de carreira/sucessão

12.3. Avaliação de performance e gestão de desempenho
12.3.1. Gestão de desempenho
12.3.2. Gestão de desempenho: objetivos e processo

12.4. Inovação na gestão de talentos e e as pessoas
12.4.1. Modelos de gestão de talento estratégico
12.4.2. Identificação, capacitação e desenvolvimento de talento
12.4.3. Lealdade e retenção
12.4.4. Proatividade e inovação

12.5. Motivação
12.5.1. A natureza da motivação
12.5.2. Teoria das expectativas
12.5.3. Teorias de necessidades
12.5.4. Motivação e compensação financeira

12.6. Desenvolvimento de equipes de alto desempenho
12.6.1. Os times de alto desempenho: os times autogerenciados
12.6.2. Metodologias de gestão de times autogerenciados de alto desempenho

12.7. Gestão de mudanças
12.7.1. Gestão de mudanças
12.7.2. Tipo de processos na gestão de mudanças
12.7.3. Estágios ou fases na gestão de mudanças

12.8. Negociação e gestão de conflitos
12.8.1. Negociação
12.8.2. Gestão de conflitos
12.8.3. Gestão de crises

12.9. Comunicação gerencial
12.9.1. Comunicação interna e externa no nível empresarial
12.9.2. Departamento de Comunicação
12.9.3. O responsável pelas comunicações da empresa. O perfil do Dircom (Diretor de Comunicação)

12.10. Produtividade, atração, retenção e ativação de talentos
12.10.1. Produtividade
12.10.2. Estratégias de atração e retenção de talentos

Módulo 13. Gestão Econômico-Financeira

13.1. Ambiente Econômico
13.1.1. Ambiente macroeconômico e sistema financeiro nacional
13.1.2. Instituições financeiras
13.1.3. Mercados financeiros
13.1.4. Ativos financeiros
13.1.5. Outras entidades do setor financeiro

13.2. Contabilidade Gerencial
13.2.1. Conceitos básicos
13.2.2. O Ativo da empresa
13.2.3. O Passivo da empresa
13.2.4. O Patrimônio Líquido da empresa
13.2.5. A Demonstração de Resultados

13.3. Sistemas de informação e *Business Intelligence*
13.3.1. Fundamentos e classificação
13.3.2. Fases e métodos de alocação de custos
13.3.3. Escolha do centro de custo e efeito

13.4. Orçamento e Controle de Gestão
13.4.1. O modelo orçamentário
13.4.2. O orçamento de capital
13.4.3. O orçamento operacional
13.4.5. Orçamento de Tesouraria
13.4.6. Controle orçamentário

13.5. Gestão Financeira
13.5.1. As decisões financeiras da empresa
13.5.2. O departamento financeiro
13.5.3. Excedentes de tesouraria
13.5.4. Riscos associados à gestão financeira
13.5.5. Gestão de riscos na direção financeira

13.6. Planejamento Financeiro
13.6.1. Definição do planejamento financeiro
13.6.2. Ações a serem realizadas no planejamento financeiro
13.6.3. Criação e estabelecimento da estratégia empresarial
13.6.4. Demonstrativo de *Cash Flow*
13.6.5. Demonstrativo de Capital Circulante

13.7. Estratégia Financeira Corporativa
13.7.1. Estratégia corporativa e fontes de financiamento
13.7.2. Produtos financeiros para financiamento empresarial

13.8. Financiamento Estratégico
13.8.1. Autofinanciamento
13.8.2. Aumento de fundos próprios
13.8.3. Recursos Híbridos
13.8.4. Financiamento por meio de intermediários

13.9. Análise e planejamento financeiro
13.9.1. Análise de Balanço de Situação
13.9.2. Análise da Conta de Lucros e Perdas
13.9.3. Análise de Rentabilidade

13.10. Análise e resolução de casos/problemas
13.10.1. Informações financeiras da Indústria de Design e Têxtil, S.A. (INDITEX)

Módulo 14. Gestão Comercial e Marketing Estratégico

14.1. Gestão Comercial
14.1.1. Estrutura Conceitual para Gestão Comercial
14.1.2. Estratégia e Planejamento Comercial
14.1.3. O papel dos gerentes comerciais

14.2. Marketing
14.2.1. Conceito de Marketing
14.2.2. Noções básicas de marketing
14.2.3. Atividades de marketing da empresa

14.3. Gestão estratégica de Marketing
14.3.1. Conceito de marketing estratégico
14.3.2. Conceito de planejamento estratégico de marketing
14.3.3. Etapas do processo de planejamento estratégico de marketing

14.4. Marketing digital e e-commerce
14.4.1. Objetivos do Marketing digital e e-Commerce
14.4.2. Marketing Digital e os meios que utiliza
14.4.3. Comércio eletrônico: contexto geral
14.4.4. Categorias do comércio eletrônico
14.4.5. Vantagens e desvantagens do *E-commerce* em relação ao comércio tradicional

14.5. Marketing digital para fortalecer a marca
14.5.1. Estratégias online para melhorar a reputação da sua marca
14.5.2. *Branded Content & Storytelling*

14.6. Marketing Digital para atrair e fidelizar clientes
14.6.1. Estratégias de fidelização e engajamento via internet
14.6.2. Visitor Relationship Management
14.6.3. Hipersegmentação

14.7. Gerenciamento de campanhas digitais
14.7.1. O que é uma campanha de publicidade digital?
14.7.2. Passos para lançar uma campanha de marketing online
14.7.3. Erros comuns em campanhas de publicidade digital

14.8. Estratégia de Vendas
14.8.1. Estratégia de Vendas
14.8.2. Métodos de Vendas

14.9. Comunicação Corporativa
14.9.1. Conceito
14.9.2. Importância da comunicação na organização
14.9.3. Tipo de comunicação na organização
14.9.4. Função da comunicação na organização
14.9.5. Elementos da comunicação
14.9.6. Problemas de comunicação
14.9.7. Cenários da comunicação

14.10. Comunicação e reputação digital
14.10.1. Reputação online
14.10.2. Como medir a reputação digital?
14.10.3. Ferramentas de reputação online
14.10.4. Relatório de reputação online
14.10.5. *Branding* online

Módulo 15. *Gestão* Executiva

15.1. Management
15.1.1. Conceito de Geral Management
15.1.2. A ação do gerente geral
15.1.3. O Gerente Geral e suas funções
15.1.4. Transformando o trabalho de gestão

15.2. Gestores e suas funções A cultura organizacional e suas abordagens
15.2.1. Gestores e suas funções A cultura organizacional e suas abordagens

15.3. Gestão operacional
15.3.1. Importância da gestão
15.3.2. A cadeia de valor
15.3.3. Gestão de Qualidade

15.4. Oratória e capacitação do porta-voz
15.4.1. Comunicação interpessoal
15.4.2. Habilidades de comunicação e influência
15.4.3. Obstáculos à comunicação

15.5. Ferramentas de comunicações pessoais e organizacionais
15.5.1. A comunicação interpessoal
15.5.2. Ferramentas da comunicação interpessoal
15.5.3. A comunicação na organização
15.5.4. Ferramentas na organização

15.6. Comunicação em situações de crise
15.6.1. Crise
15.6.2. Fases da crise
15.6.3. Mensagens: conteúdo e momentos

15.7. Preparando um plano de crise
15.7.1. Análise de problemas potenciais
15.7.2. Planejamento
15.7.3. Adequação de pessoal

15.8. Inteligência emocional
15.8.1. Inteligência emocional e comunicação
15.8.2. Assertividade, Empatia e Escuta Ativa
15.8.3. Autoestima e Comunicação Emocional

15.9. *Branding* personal
15.9.1. Estratégias para o branding pessoal
15.9.2. Leis de branding pessoal
15.9.3. Ferramentas pessoais de construção de marcas

15.10. Liderança e gestão de equipes
15.10.1. Liderança e estilos de liderança
15.10.2. Competências e desafios do líder
15.10.3. Gestão de processos de Mudança
15.10.4. Gestão de Equipes Multiculturais

Este programa abrirá portas para novos caminhos em seu progresso profissional"

07

Metodologia

Este curso oferece uma maneira diferente de aprender. Nossa metodologia é desenvolvida através de um modo de aprendizagem cíclico: ***o Relearning***. Este sistema de ensino é utilizado, por exemplo, nas faculdades de medicina mais prestigiadas do mundo e foi considerado um dos mais eficazes pelas principais publicações científicas, como o ***New England Journal of Medicine.***

Descubra o Relearning, um sistema que abandona a aprendizagem linear convencional para realizá-la através de sistemas de ensino cíclicos: uma forma de aprendizagem que se mostrou extremamente eficaz, especialmente em disciplinas que requerem memorização"

A Escola de Negócios da TECH utiliza o Estudo de Caso para contextualizar todo o conteúdo

Nosso programa oferece um método revolucionário para desenvolver as habilidades e o conhecimento. Nosso objetivo é fortalecer as competências em um contexto de mudança, competitivo e altamente exigente.

Com a TECH você irá experimentar uma forma de aprender que está revolucionando as bases das universidades tradicionais em todo o mundo"

Nosso programa prepara você para enfrentar novos desafios em ambientes incertos e alcançar o sucesso em sua carreira.

Nosso programa prepara você para enfrentar novos desafios em ambientes incertos e alcançar o sucesso em sua carreira.

Um método de aprendizagem inovador e diferente

Este curso da TECH é um programa de ensino intensivo, criado do zero, que propõe ao gerente os desafios e as decisões mais exigentes nesta área, em âmbito nacional ou internacional. Através desta metodologia, o crescimento pessoal e profissional é impulsionado, sendo este um passo decisivo para alcançar o sucesso. O método do caso, técnica que forma a base deste conteúdo, garante que a realidade econômica, social e empresarial mais atual seja seguida.

> *Você aprenderá, através de atividades de colaboração e casos reais, a resolver situações complexas em ambientes reais de negócios"*

O método do caso é o sistema de aprendizagem mais utilizado nas principais escolas de negócios do mundo, desde que elas existem. Desenvolvido em 1912 para que os estudantes de Direito não aprendessem a lei apenas com base no conteúdo teórico, o método do caso consistia em apresentar-lhes situações realmente complexas para que tomassem decisões conscientes e julgassem a melhor forma de resolvê-las. Em 1924 foi estabelecido como o método de ensino padrão em Harvard.

Em uma determinada situação, o que um profissional deveria fazer? Esta é a pergunta que abordamos no método do caso, um método de aprendizagem orientado para a ação. Ao longo do programa, os alunos irão se deparar com diversos casos reais. Terão que integrar todo o seu conhecimento, pesquisar, argumentar e defender suas ideias e decisões.

Metodologia Relearning

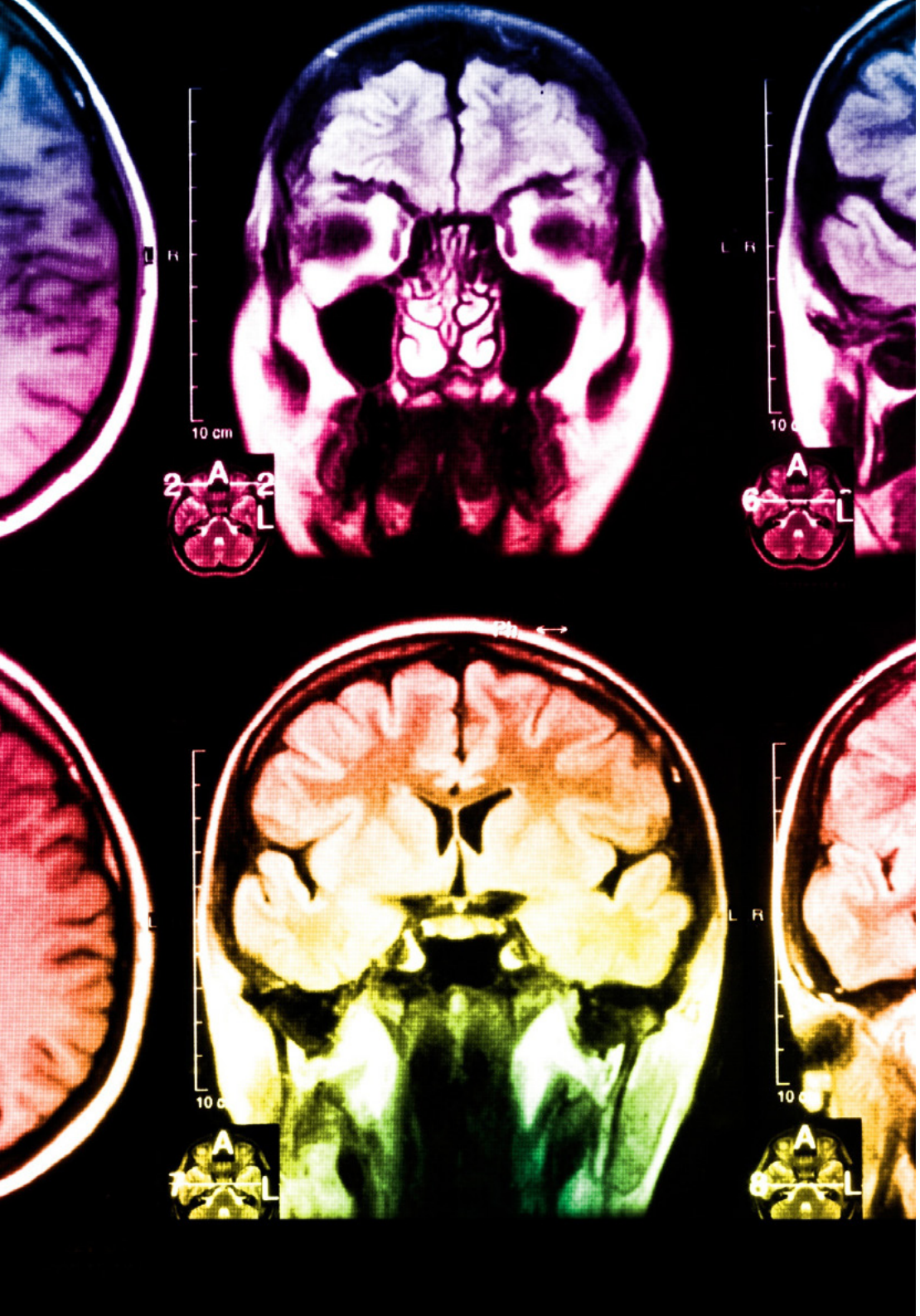
A TECH utiliza de maneira eficaz a metodologia do estudo de caso com um sistema de aprendizagem 100% online, baseado na repetição, combinando elementos didáticos diferentes em cada aula.

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

> *Nosso sistema online lhe permitirá organizar seu tempo e ritmo de aprendizagem, adaptando-os ao seu horário. Você poderá acessar o conteúdo a partir de qualquer dispositivo, fixo ou móvel, com conexão à Internet.*

Na TECH você aprenderá através de uma metodologia de vanguarda, desenvolvida para capacitar os profissionais do futuro. Este método, na vanguarda da pedagogia mundial, se chama Relearning.

Nossa escola de negócios é uma das únicas que possui a licença para usar este método de sucesso. Em 2019 conseguimos melhorar os níveis de satisfação geral de nossos alunos (qualidade de ensino, qualidade dos materiais, estrutura dos cursos, objetivos, entre outros) com relação aos indicadores da melhor universidade online.



No nosso programa, a aprendizagem não é um processo linear, ela acontece em espiral (aprender, desaprender, esquecer e reaprender). Portanto, combinamos cada um desses elementos de forma concêntrica. Esta metodologia já capacitou mais de 650 mil graduados universitários com um sucesso sem precedentes em áreas tão diversas como bioquímica, genética, cirurgia, direito internacional, habilidades gerenciais, ciências do esporte, filosofia, direito, engenharia, jornalismo, história ou mercados e instrumentos financeiros. Tudo isso em um ambiente altamente exigente, com um corpo discente com um perfil socioeconômico médio-alto e uma média de idade de 43,5 anos.

O Relearning permitirá uma aprendizagem com menos esforço e mais desempenho, fazendo com que você se envolva mais em sua especialização, desenvolvendo o espírito crítico e sua capacidade de defender argumentos e contrastar opiniões: uma equação de sucesso.

A partir das últimas evidências científicas no campo da neurociência, sabemos como organizar informações, ideias, imagens, memórias, mas sabemos também que o lugar e o contexto onde aprendemos algo é fundamental para nossa capacidade de lembrá-lo e armazená-lo no hipocampo, para mantê-lo em nossa memória a longo prazo.

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

Neste programa, oferecemos o melhor material educacional, preparado especialmente para os profissionais:

Material de estudo

Todo o conteúdo foi criado especialmente para o curso pelos especialistas que irão ministrá-lo, o que faz com que o desenvolvimento didático seja realmente específico e concreto.

Posteriormente, esse conteúdo é adaptado ao formato audiovisual, para criar o método de trabalho online da TECH. Tudo isso, com as técnicas mais inovadoras que proporcionam alta qualidade em todo o material que é colocado à disposição do aluno.

Masterclasses

Há evidências científicas sobre a utilidade da observação de terceiros especialistas.

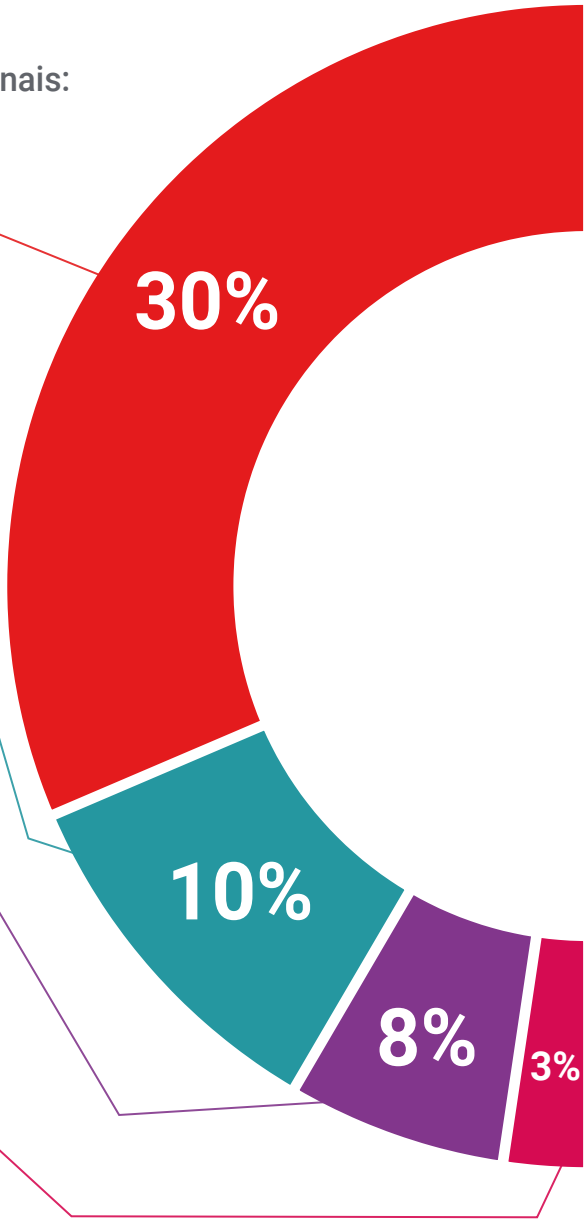
O "Learning from an expert" fortalece o conhecimento e a memória, além de gerar segurança para a tomada de decisões difíceis no futuro

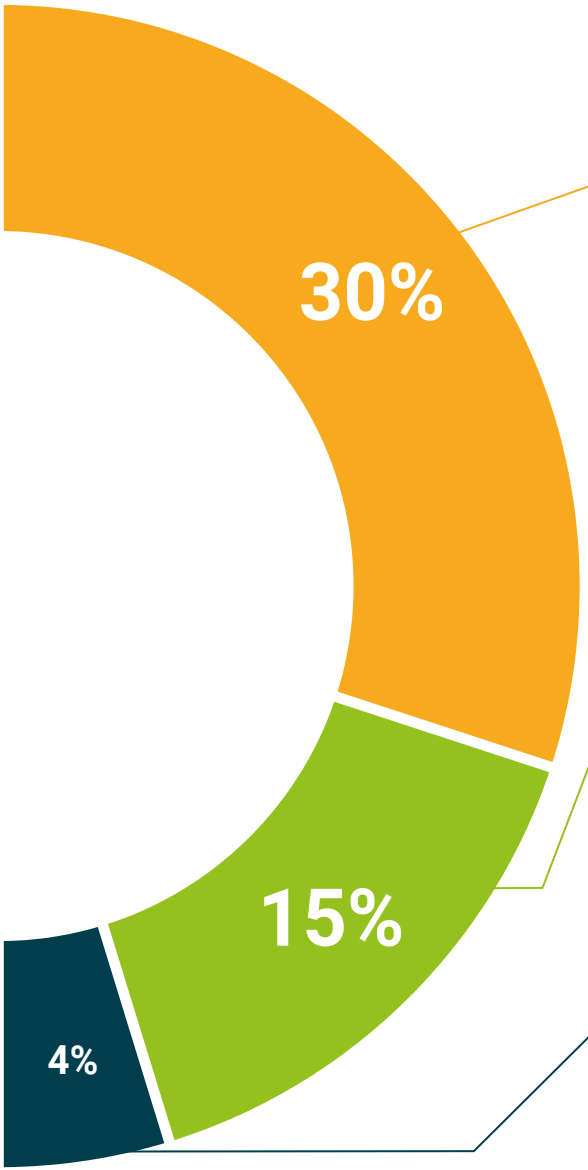
Práticas de habilidades gerenciais

Serão realizadas atividades para desenvolver as competências gerenciais específicas em cada área temática. Práticas e dinâmicas para adquirir e ampliar as competências e habilidades que um gestor precisa desenvolver no contexto globalizado em que vivemos.

Leituras complementares

Artigos recentes, documentos de consenso e diretrizes internacionais, entre outros. Na biblioteca virtual da TECH o aluno terá acesso a tudo o que for necessário para complementar a sua capacitação.





Estudos de caso

Os alunos irão completar uma seleção dos melhores estudos de caso escolhidos especialmente para esta capacitação. Casos apresentados, analisados e orientados pelos melhores especialistas da alta gestão do cenário internacional.

Resumos interativos

A equipe da TECH apresenta o conteúdo de forma atraente e dinâmica através de pílulas multimídia que incluem áudios, vídeos, imagens, gráficos e mapas conceituais para consolidar o conhecimento.

Este sistema exclusivo de capacitação por meio da apresentação de conteúdo multimídia foi premiado pela Microsoft como "Caso de sucesso na Europa"

Testing & Retesting

Avaliamos e reavaliamos periodicamente o conhecimento do aluno ao longo do programa, através de atividades e exercícios de avaliação e autoavaliação, para que possa comprovar que está alcançando seus objetivos.

08

Perfil dos nossos alunos

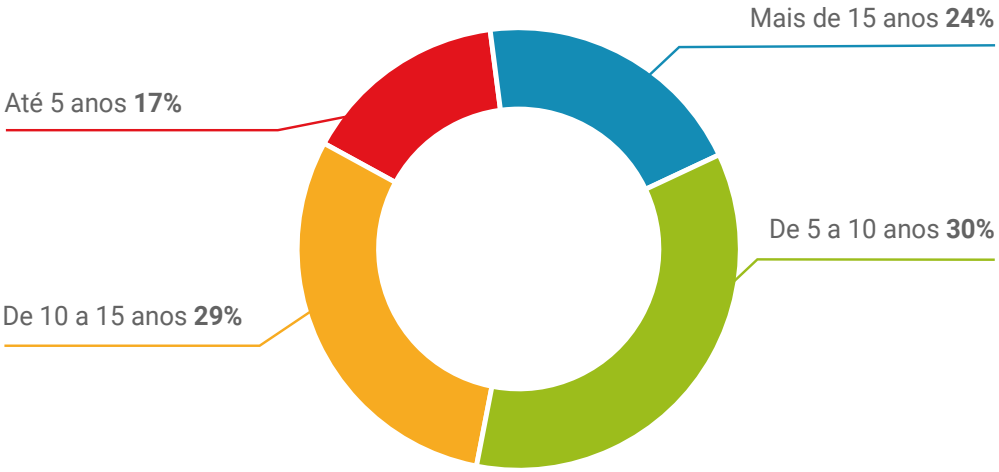
O Executive Master em MBA en Gestão de Segurança Cibernética (CISO, Chief Information Security Officer) é um programa de estudos destinado aos profissionais que visam melhorar suas competências através de um ensino de qualidade. Alunos que desejam ampliar seus conhecimentos em outro ramo relacionado aos negócios, como a Inteligência Artificial ou, mais especificamente, a segurança cibernética. Um programa de estudos voltado para profissionais com experiência, mas que acreditam na especialização superior como método de aprimoramento pessoal e profissional.

Os alunos da TECH são profissionais com ampla experiência visando uma melhor posição”

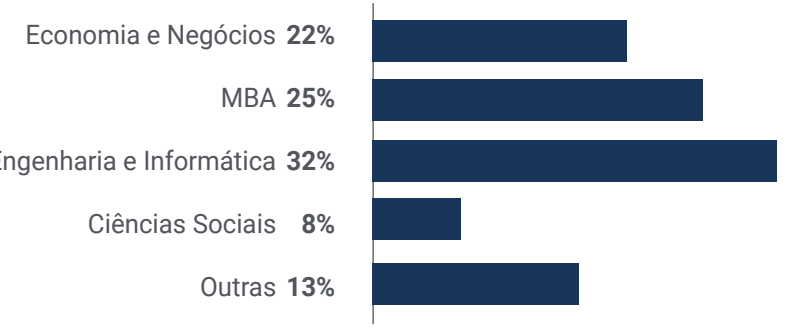
Média de idade

Entre **35** y **45** anos

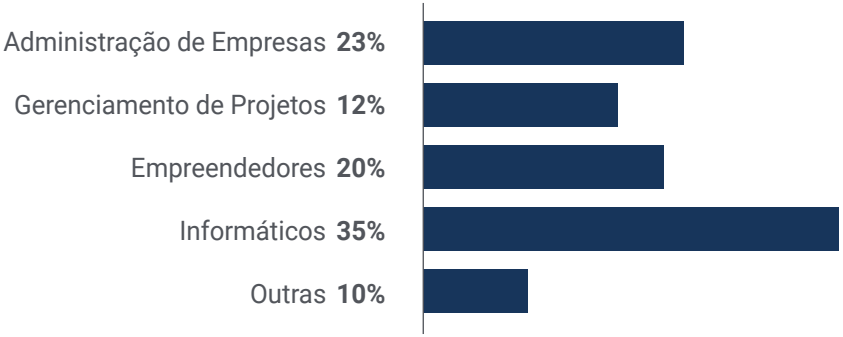
Anos de experiência



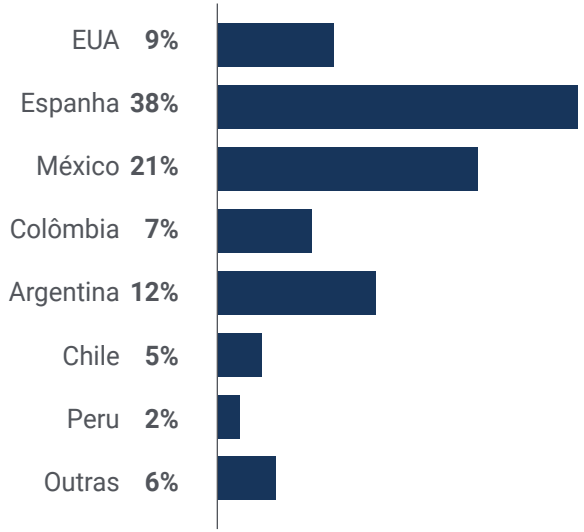
Formação



Perfil acadêmico



Distribuição geográfica



Jaime Díaz

Chief Revenue Officer

" Na área de negócios que trabalho, lidamos com muitas informações confidenciais e dados relevantes que, nas mãos erradas, podem gerar sérios problemas para a empresa. Por isso, há algum tempo eu vinha pensando em ampliar meus conhecimentos sobre segurança cibernética, com o objetivo de controlar, eu mesmo, todos os processos que podem ser mais sensíveis a uma ameaça cibernética. Graças a este curso da TECH, pude melhorar minhas habilidades e me tornar mais confiante em meu trabalho.

09

Direção do curso

Os professores deste Executive Master em MBA en Gestão de Segurança Cibernética (CISO, Chief Information Security Officer) são profissionais com ampla experiência na área, tanto profissional como de ensino. A especialização nesta área lhes confere a qualificação necessária para oferecer aos alunos um estudo completo e de alta qualidade sobre assuntos que serão úteis em seu trabalho diário no mundo empresarial. São pessoas que acreditam no ensino superior como uma forma de progredir na profissão e melhorar a competitividade dos seus negócios.

Um corpo docente com ampla experiência que irá ajudá-lo a se especializar em segurança cibernética"

Diretor Internacional Convidado

O Dr. Frederic Lemieux é reconhecido internacionalmente como um especialista inovador e líder inspirador nos campos de **Inteligência**,**Segurança Nacional**,**Segurança Interna**,**Cibersegurança** e **Tecnologias Disruptivas**. Sua constante dedicação e relevantes contribuições em Pesquisa e Educação o posicionam como uma figura chave na **promoção da segurança** e na **compreensão das tecnologias emergentes** na atualidade. Durante sua trajetória profissional, ele conceituou e dirigiu programas acadêmicos de vanguarda em diversas instituições renomadas, como a **Universidade de Montreal**, a **Universidade George Washington** e **a Universidade de Georgetown.**

Ao longo de sua extensa carreira, publicou múltiplos livros de grande relevância, todos relacionados com a **inteligência criminal**, o **trabalho policial**, as **ameaças cibernéticas** e a **segurança internacional**. Além disso, contribuiu de maneira significativa ao campo da **Cibersegurança** com a publicação de numerosos artigos em revistas acadêmicas, que examinam o controle do crime durante desastres importantes, a luta contra o terrorismo, as agências de inteligência e a cooperação policial. Também foi palestrante e conferencista principal em diversas conferências nacionais e internacionais, consolidando-se como um referencial no âmbito acadêmico e profissional.

O Dr. Lemieux desempenhou papéis editoriais e de avaliação em diferentes organizações acadêmicas, privadas e governamentais, refletindo sua influência e compromisso com a excelência em seu campo de especialização. Desta forma, sua prestigiada carreira acadêmica o levou a atuar como Professor de Práticas e Diretor de Faculdade dos programas MPS em **Inteligência Aplicada**, **Gestão de Riscos em Cibersegurança**, **Gestão Tecnológica** e **Gestão de Tecnologias da Informação** na **Universidade de Georgetown.**

Dr. Frederic Lemieux

- Diretor do Mestrado em Gestão de Riscos em Cibersegurança na Universidade de Georgetown, Washington, Estados Unidos
- Diretor do Mestrado em Gestão de Tecnologia na Universidade de Georgetown
- Diretor do Mestrado em Inteligência Aplicada na Universidade de Georgetown
- Professor de Práticas na Universidade de Georgetown
- Doutor em Criminologia pela Escola de Criminologia na Universidade de Montreal
- Formado em Sociologia com Minor em Psicologia pela Universidade de Laval
- Membro de New Program Roundtable Committee, Universidade de Georgetown

Graças à TECH você será capaz de aprender com os melhores profissionais do mundo"

Diretora Internacional Convidada

Com mais de 20 anos de experiência no design e na direção de equipes globais de **aquisição de talentos**, Jennifer Dove é especialista em **recrutamento** e **estratégia tecnológica**. Ao longo de sua carreira profissional, ocupou cargos de liderança em várias organizações tecnológicas dentro de empresas da lista *Fortune 50*, como **NBC Universal** e **Comcast**. Sua trajetória lhe permitiu se destacar em ambientes competitivos e de alto crescimento.

Como **Vice-presidente de Aquisição de Talentos** na **Mastercard**, ela é responsável por supervisionar a estratégia e a execução da incorporação de talentos, colaborando com líderes empresariais e responsáveis de **Recursos Humanos** para cumprir os objetivos operacionais e estratégicos de contratação. Em especial, seu objetivo é **criar equipes diversas**, **inclusivas** e de **alto desempenho** que impulsionem a inovação e o crescimento dos produtos e serviços da empresa. Além disso, é especialista no uso de ferramentas para atrair e reter os melhores profissionais de todo o mundo. Ela também se encarrega de **amplificar** a **marca empregadora** e a proposta de valor da **Mastercard** através de publicações, eventos e redes sociais.

Jennifer Dove demonstrou seu compromisso com o desenvolvimento profissional contínuo, participando ativamente de redes de profissionais de **Recursos Humanos** e contribuindo para a incorporação de inúmeros trabalhadores em diferentes empresas. Após obter sua graduação em **Comunicação Organizacional** pela Universidade de **Miami**, ocupou cargos de liderança em recrutamento em empresas de diversas áreas.

Por outro lado, foi reconhecida por sua habilidade em liderar transformações organizacionais, **integrar tecnologias** nos **processos de recrutamento** e desenvolver programas de liderança que preparam as instituições para os desafios futuros. Ela também implementou com sucesso programas de **bem-estar laboral** que aumentaram significativamente a satisfação e a retenção de funcionários.

Sra. Jennifer Dove

- Vice-presidente de Aquisição de Talentos na Mastercard, Nova York, Estados Unidos
- Diretora de Aquisição de Talentos na NBCUniversal, Nova York, Estados Unidos
- Responsável pela Seleção de Pessoal na Comcast
- Diretora de Seleção de Pessoal na Rite Hire Advisory
- Vice-presidente Executiva da Divisão de Vendas na Ardor NY Real Estate
- Diretora de Seleção de Pessoal na Valerie August & Associates
- Executiva de Contas na BNC
- Executiva de Contas na Vault
- Graduada em Comunicação Organizacional pela Universidade de Miami

A TECH conta com uma equipe notável e especializada de diretores convidados internacionais, com importantes posições de liderança nas empresas mais avançadas do mercado global"

Diretor Internacional Convidado

Líder tecnológico com décadas de experiência em **grandes multinacionais de tecnologia**, Rick Gauthier se destacou no campo dos **serviços** em **nuvem** e na melhoria de processos de ponta a ponta. Ele foi reconhecido como um líder e gestor de equipes altamente eficiente, mostrando um talento natural para garantir um alto nível de compromisso entre seus colaboradores.

Rick possui habilidades inatas em estratégia e inovação executiva, desenvolvendo novas ideias e apoiando seu sucesso com dados de qualidade. Sua trajetória na **Amazon** lhe permitiu administrar e integrar os serviços de TI da empresa nos Estados Unidos. Na **Microsoft** liderou uma equipe de 104 pessoas responsáveis por fornecer infraestrutura de TI corporativa e apoiar departamentos de engenharia de produtos em toda a companhia.

Essa experiência permitiu que Rick se destacasse como um executivo de alto impacto, com habilidades notáveis para aumentar a eficiência, a produtividade e a satisfação geral dos clientes.

Sr. Rick Gauthier

- Diretor Regional de TI na Amazon, Seattle, Estados Unidos
- Chefe de Programas Sênior na Amazon
- Vice-Presidente da Wimmer Solutions
- Diretor Sênior de Serviços de Engenharia Produtiva na Microsoft
- Graduado em Cibersegurança pela Western Governors University
- Certificado Técnico em *Mergulho Comercial* pelo Divers Institute of Technology
- Graduado em Estudos Ambientais pelo The Evergreen State College

Aproveite a oportunidade para conhecer os últimos avanços nesta área e aplicá-los em sua prática diária"

Diretor Internacional Convidado

Romi Arman é um renomado especialista internacional com mais de duas décadas de experiência em **Transformação Digital**, **Marketing, Estratégia** e **Consultoria**. Ao longo dessa trajetória extensa, assumiu diferentes riscos e é um **defensor permanente** da **inovação** e **mudança** no cenário empresarial. Com essa expertise, colaborou com diretores gerais e organizações corporativas de todo o mundo, incentivando-os a abandonar os modelos tradicionais de negócios. Assim, contribuiu para que empresas como a energética Shell se tornassem **verdadeiros líderes de mercado,** focadas em seus **clientes** e no **mundo digital.**

As estratégias desenvolvidas por Arman têm um impacto duradouro, pois permitiram a várias corporações **melhorar as experiências dos consumidores, funcionários** e **acionistas.** O sucesso desse especialista é quantificável por meio de métricas tangíveis como o **CSAT**, o **engajamento dos funcionários** nas instituições onde atuou e o crescimento do **indicador financeiro EBITDA** em cada uma delas.

Além disso, em sua trajetória profissional, nutriu e **liderou equipes de alto desempenho** que, inclusive, receberam prêmios por seu **potencial transformador**. Com a Shell, especificamente, o executivo sempre se propôs a superar três desafios: satisfazer as complexas **demandas** de **descarbonização** dos clientes, **apoiar** uma "**descarbonização rentável**" e **revisar** um panorama fragmentado de **dados**, **digital y tecnológic**o. Assim, seus esforços evidenciaram que, para alcançar um sucesso sustentável, é fundamental partir das necessidades dos consumidores e estabelecer as bases para a transformação dos processos, dados, tecnologia e cultura.

Por outro lado, o diretor se destaca por seu domínio das **aplicações empresariais** da **Inteligência Artificial,** tema em que possui um pós-graduação da London Business School. Ao mesmo tempo, acumulou experiências em **IoT** e o **Salesforce.**

Sr. Romi Arman

- Diretor de Transformação Digital (CDO) na Shell, Londres, Reino Unido
- Diretor Global de Comércio Eletrônico e Atendimento ao Cliente na Shell
- Gerente Nacional de Contas Chave (fabricantes de equipamentos originais e varejistas de automóveis) para Shell em Kuala Lumpur, Malásia
- Consultor Sênior de Gestão (Setor de Serviços Financeiros) para Accenture em Singapura
- Graduado pela Universidade de Leeds
- Pós-graduação em Aplicações Empresariais de IA para Executivos Seniores pela London Business School
- Certificação Profissional em Experiência do Cliente CCXP
- Curso de Transformação Digital Executiva pelo IMD

Você deseja atualizar seus conhecimentos com a mais alta qualidade educacional? A TECH disponibiliza os conteúdos mais atualizados do mercado acadêmico, elaborados por especialistas de prestígio internacional"

Diretor Internacional Convidado

Manuel Arens é um **profissional experiente** em gerenciamento de dados e líder de uma equipe altamente qualificada. Atualmente, ele ocupa o cargo de **Gerente Global de Compras** na divisão de Infraestrutura Técnica e Centros de Dados da Google, onde construiu a maior parte de sua carreira profissional. Sediada em Mountain View, Califórnia, a empresa forneceu soluções para os desafios operacionais da gigante da tecnologia, como a **integridade de dados mestres,** as **atualizações de dados de fornecedores** e **priorização** desses dados. Ele liderou o planejamento da cadeia de suprimentos do data center e a avaliação de risco do fornecedor, gerando melhorias no processo e no gerenciamento do fluxo de trabalho que resultaram em economias de custo significativas.

Com mais de uma década de experiência fornecendo soluções digitais e liderança para empresas em diversas indústrias, ele possui uma ampla expertise em todos os aspectos da entrega de soluções estratégicas, abrangendo **marketing, análise de mídia, mensuração** e **atribuição.** De fato, ele recebeu vários reconhecimentos por seu trabalho, incluindo o **Prêmio de Liderança BIM**, o **Prêmio de Liderança em Pesquisa**, **o Prêmio de Programa de Geração de Leads de Exportação** e o **Prêmio de Melhor Modelo de Vendas da EMEA (Europa, Oriente Médio e África).**

Além disso, Arens atuou como **Gerente de Vendas** em Dublin, Irlanda. Nesse cargo, ele liderou a formação de uma equipe que cresceu de 4 para 14 membros em três anos, alcançando resultados significativos e promovendo uma colaboração eficaz tanto dentro da equipe de vendas quanto com equipes interfuncionais. Ele também atuou como **Analista Sênior** da Industria, em Hamburgo, Alemanha, criando histórias para mais de 150 clientes usando ferramentas internas e de terceiros para apoiar a análise. Desenvolveu e escreveu relatórios detalhados para demonstrar domínio do assunto, incluindo uma compreensão dos **fatores macroeconômicos e políticos/regulatórios** que afetam a adoção e a difusão da tecnologia.

Também liderou equipes em empresas como **Eaton, Airbus e Siemens**, onde adquiriu valiosa experiência em gestão de contas e cadeia de suprimentos. Destaca-se especialmente seu trabalho para superar continuamente as expectativas através da **construção de relações valiosas com os clientes** e **trabalhando de forma fluida com pessoas em todos os níveis de uma organização**, incluindo stakeholders, gestão, membros da equipe e clientes. Seu enfoque orientado por dados e sua capacidade de desenvolver soluções inovadoras e escaláveis para os desafios da indústria o tornaram um líder proeminente em seu campo.

Sr. Manuel Arens

- Gerente Global de Compras no Google, Mountain View, Estados Unidos
- Responsável Principal de Análise e Tecnologia B2B no Google, Estados Unidos
- Diretor de Vendas no Google, Irlanda
- Analista Industrial Sênior no Google, Alemanha
- Gestor de Contas no Google, Irlanda
- Accounts Payable na Eaton, Reino Unido
- Gestor de Cadeia de Suprimentos na Airbus, Alemanha

Escolha a TECH! Você poderá acessar os melhores materiais didáticos, na vanguarda da tecnologia e da educação, implementados por especialistas de prestígio internacional na área"

Diretor Internacional Convidado

Andrea La Sala é um **experiente executivo** de **Marketing** cujos projetos tiveram um **impacto significativo** no **setor da Moda**. Ao longo de sua bem-sucedida carreira, desenvolveu diversas tarefas relacionadas a **Produtos**, **Merchandising** e **Comunicação**, sempre associado a marcas de prestígio como **Giorgio Armani**, **Dolce&Gabbana**, **Calvin Klein**, entre outras.

Os resultados desse executivo de **alto perfil internacional** estão ligados à sua comprovada capacidade de **sintetizar informações** em estruturas claras e executar **ações concretas** alinhadas com objetivos **empresariais específicos**. Além disso, é reconhecido por sua **proatividade** e **adaptação a ritmos acelerados** de trabalho. Este especialista também possui uma **forte consciência comercial**,
visão de mercado e uma **verdadeira paixão** pelos **produtos**.

Como **Diretor Global de Marca e Merchandising** na **Giorgio Armani**, supervisionou diversas **estratégias de Marketing** para **roupas** e **acessórios**. Suas táticas foram centradas no **varejo** e nas **necessidades** e **comportamentos dos consumidores**. Neste cargo, La Sala também foi responsável pela comercialização de produtos em diferentes mercados, atuando como **chefe de equipe** nos **departamentos de Design**, **Comunicação** e **Vendas**.

Por outro lado, em empresas como **Calvin Klein** e **Gruppo Coin**, empreendeu projetos para impulsionar a **estrutura**, o **desenvolvimento** e a **comercialização** de **diferentes coleções**. Também criou **calendários eficazes** para **campanhas** de compra e venda,
para campanhas gerenciando **termos**, **custos**, **processos** e **prazos de entrega**
de diferentes operações.

Essas experiências tornaram Andrea La Sala um dos principais e mais qualificados **líderes corporativos** no setor da **Moda** e **Luxo**, com uma alta capacidade de implementação eficaz do **posicionamento positivo** de **diferentes marcas** e redefinição de indicadores-chave de desempenho (KPI).

Sr. Andrea La Sala

- Diretor Global de Marca e Merchandising Armani Exchange na Giorgio Armani, Milão, Itália
- Diretor de Merchandising na Calvin Klein
- Responsável de Marca no Gruppo Coin
- Brand Manager na Dolce&Gabbana
- Brand Manager na Sergio Tacchini S.p.A.
- Analista de Mercado na Fastweb
- Graduado em Business and Economics na Università degli Studi del Piemonte Orientale

Os profissionais internacionais mais qualificados e experientes estão esperando por você na TECH para proporcionar um ensino de alto nível, atualizado e baseado nas mais recentes evidências científicas. O que você está esperando para se matricular?"

Diretor Internacional Convidado

Mick Gram é sinônimo de inovação e excelência no campo da **Inteligência Empresarial** em âmbito internacional. Sua carreira de sucesso está associada a cargos de liderança em multinacionais como **Walmart** e **Red Bull.** Além disso, esse especialista se destaca por sua visão para **identificar tecnologias emergentes** que, a longo prazo, têm um impacto duradouro no ambiente corporativo.

O executivo é considerado um **pioneiro** no **uso de técnicas de visualização de dados** que simplificaram conjuntos complexos, tornando-os acessíveis e facilitadores da tomada de decisões. Essa habilidade se tornou o pilar de seu perfil profissional, transformando-o em um ativo desejado por muitas organizações que buscavam **reunir informações** e **gerar ações** concretas a partir delas.

Um de seus projetos mais destacados nos últimos anos foi a **plataforma Walmart Data Cafe**, a maior do tipo no mundo, ancorada na nuvem e destinada à **análise** de ***Big Data***. Além disso, ele atuou como **Diretor** de **Business Intelligence** na **Red Bull,** abrangendo áreas como **Vendas, Distribuição, Marketing e Operações de Cadeia de Suprimento**. Sua equipe foi recentemente reconhecida por sua inovação constante no uso da nova API do Walmart Luminate para insights de Compradores e Canais.

Quanto à sua formação, o executivo possui vários Mestrados e estudos de pós-graduação em instituições renomadas como a **Universidade de Berkeley**, nos Estados Unidos, e a **Universidade de Copenhague**, na Dinamarca. Através dessa capacitação contínua, o especialista alcançou competências de vanguarda. Assim, ele se tornou considerado um **líder nato** da **nova economia mundial**, focada no impulso dos dados e suas possibilidades infinitas.

Sr. Mick Gram

- Diretor de *Business Intelligence* e Análise na Red Bull, Los Angeles, Estados Unidos
- Arquiteto de soluções de *Business Intelligence* para Walmart Data Cafe
- Consultor independente de *Business Intelligence* e *Data Science*
- Diretor de *Business Intelligence* na Capgemini
- Analista Chefe na Nordea
- Consultor Chefe de *Bussiness Intelligence* para a SAS
- Educação Executiva em IA e Machine Learning na UC Berkeley College of Engineering
- MBA Executivo em e-commerce na Universidade de Copenhague
- Graduação e Mestrado em Matemática e Estatística na Universidade de Copenhague

Estude na melhor universidade online do mundo de acordo com a Forbes! Neste MBA, você terá acesso a uma extensa biblioteca de recursos multimídia, desenvolvida por professores de prestígio internacional"

Diretor Internacional Convidado

Scott Stevenson é um distinto especialista no setor de **Marketing Digital** que, por mais de 19 anos, esteve ligado a uma das empresas mais poderosas da indústria do entretenimento, a **Warner Bros. Discovery.** Neste papel, teve uma função fundamental na **supervisão da logística** e dos **fluxos de trabalho criativos** em diversas plataformas digitais, incluindo redes sociais, busca, display e meios lineares.

A liderança deste executivo foi crucial para impulsionar **estratégias de produção** em **meios pagos**, o que resultou em uma notável **melhoria** nas **taxas de conversão** da sua empresa. Ao mesmo tempo, assumiu outros cargos, como Diretor de Serviços de Marketing e Gerente de Tráfego na mesma multinacional durante sua antiga gestão.

Além disso, Stevenson esteve envolvido na distribuição global de videogames e **campanhas de propriedade digital**. Também foi responsável por introduzir estratégias operacionais relacionadas com a formação, finalização e entrega de conteúdo de som e imagem para c**omerciais de televisão** e ***trailers***.

Por outro lado, o especialista possui uma Graduação em Telecomunicações pela Universidade da Flórida e um Mestrado em Escrita Criativa pela Universidade da Califórnia, o que demonstra sua habilidade em **comunicação** e **narrativa**. Além disso, participou da Escola de Desenvolvimento Profissional da Universidade de Harvard em programas de vanguarda sobre o uso da **Inteligência Artificial** nos **negócios**. Assim, seu perfil profissional se destaca como um dos mais relevantes no campo atual do **Marketing** e dos **Meios Digitais.**

Sr. Scott Stevenson

- Diretor de Marketing Digital na Warner Bros. Discovery, Burbank, Estados Unidos
- Gerente de Tráfego na Warner Bros. Entertainment
- Mestrado em Escrita Criativa pela Universidade da Califórnia
- Graduação em Telecomunicações pela Universidade da Flórida

Alcance seus objetivos acadêmicos e profissionais com os especialistas mais qualificados do mundo! Os professores deste MBA irão orientá-lo ao longo de todo o processo de aprendizagem"

Diretor Internacional Convidado

O Dr. Eric Nyquist é um destacado profissional no **no âmbito esportivo internacional**, que construiu uma carreira impressionante, destacando-se por seu **liderança estratégica** e habilidade para impulsionar mudanças e **inovação** em **organizações esportivas** de alto nível.

De fato, ele ocupou cargos de alto escalão, como **Diretor de Comunicações e Impacto** na **NASCAR**, sediada na **Florida, Estados Unidos.** Com muitos anos de experiência nesta organização, o Dr. Nyquist também ocupou várias posições de liderança, incluindo **Vice-Presidente Sênior de Desenvolvimento Estratégico** e **Diretor Geral de Assuntos Comerciais,** gerenciando mais de uma dúzia de disciplinas que vão desde o **desenvolvimento estratégico** até o **Marketing de entretenimento.**

Além disso, Nyquist deixou uma marca significativa nas **principais franquias esportivas** de Chicago. Como **Vice-Presidente Executivo** das franquias dos **Chicago Bulls** e dos **Chicago White Sox** ele demonstrou sua capacidade de impulsionar o **sucesso empresarial** e **estratégico** no mundo do **esporte profissional**.

Por último, é importante destacar que ele iniciou sua carreira no **campo esportivo** enquanto trabalhava em **Nova York** como **principal analista estratégico** para **Roger Goodell** na **National Football League (NFL)** e, anteriormente, como **estagiário jurídico** na **Federação de Futebol dos Estados Unidos.**

Sr. Eric Nyquist

- Diretor de Comunicações e Impacto na NASCAR, Flórida, Estados Unidos
- Vice-Presidente Sênior de Desenvolvimento Estratégico na NASCAR
- Vice-Presidente de Planejamento Estratégico na NASCAR
- Diretor Geral de Assuntos Comerciais na NASCAR
- Vice-Presidente Executivo nas Franquias Chicago White Sox
- Vice-Presidente Executivo nas Franquias Chicago Bulls
- Gerente de Planejamento Empresarial na National Football League (NFL)
- Assuntos Comerciais / Estagiário Jurídico na Federação de Futebol dos Estados Unidos
- Doutor em Direito pela Universidade de Chicago
- Mestrado em Administração de Empresas (MBA) pela Booth School of Business da Universidade de Chicago
- Formado em Economia Internacional pelo Carleton College

Com este curso universitário 100% online, você poderá conciliar seus estudos com suas atividades diárias, contando com o apoio dos principais especialistas internacionais na área do seu interesse. Faça sua matrícula hoje mesmo!"

Direção

Sra. Sonia Fernández Sapena

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

Professores

Sr. José Francisco Barba

- Técnico Eletrônico Especializado em Cibersegurança
- Desenvolvedor de Aplicativos para Dispositivos Móveis
- Técnico Eletrônico em Posição Intermediária no Ministério da Defesa da Espanha
- Técnico Eletrônico na Fábrica Ford Sita em Valência

Sr. Álvaro Jiménez Ramos

- Analista de Cibersegurança
- Analista Sênior de Segurança no The Workshop
- Analista de Cibersegurança L1 na Axians
- Analista de Cibersegurança L2 na Axians
- Analista de Cibersegurança na SACYR S.A.
- Formada em Engenharia Telemática pela Universidade Politécnica de Madri
- Mestrado em Segurança Cibernética e Hacking Ético pela CICE
- Curso Avançado em Segurança Cibernética pela Deusto Formación

Sra. Marcos Sbarbaro, Victoria Alicia

- Desenvolvedora de aplicativos móveis Android nativo na B60. UK
- Analista Programadora para a gestão, coordenação e documentação de um ambiente de alarme de segurança virtualizado nas instalações do cliente
- Analista de Programação de Aplicativos Java para caixas eletrônicos
- Profissional de Desenvolvimento de *Software* para Aplicação de Validação de Assinaturas e Gestão Documental
- Técnico de Sistemas para a Migração de Equipamentos e para a Gestão, Manutenção e Formação de Dispositivos Móveis PDA
- Engenheiro Técnico de Informática de Sistemas pela Universidade Aberta da Catalunha
- Mestrado em Segurança Informática e Hacking Ético Oficial EC- Conselho e CompTIA pela Escola Profissional de Novas Tecnologias CICE

Sr. Jon Peralta Alonso

- Consultor Sênior de Proteção de Dados e Cibersegurança na Altia
- Advogado / Assessor jurídico da Arriaga Associados Assessoria Jurídica e Econômica S.L.
- Assessor Jurídico / Estagiário no Escritório Profissional: Óscar Padura
- Formado em Direito pela Universidade Pública do País Basco
- Mestrado em Delegado de Proteção de Dados pela EIS Innovative School
- Mestrado em Advocacia pela Universidade Pública do País Basco
- Mestrado em Prática Processual Civil pela Universidade Internacional Isabel I de Castilla
- Docente no Mestrado em Proteção de Dados Pessoais, Cibersegurança e Direito das TIC

Sr. Jesús Serrano Redondo

- Desenvolvedor Web e Técnico em Cibersegurança
- Desenvolvedor Web na Roams, Palencia
- Desenvolvedor *FrontEnd* na Telefónica, Madrid
- Desenvolvedor *FrontEnd* na Best Pro Consulting SL, Madrid
- Instalador de Equipamentos e Serviço de Telecomunicações no Grupo Zener, Castilla y León
- Instalador de Equipamentos e Serviços de Telecomunicações na Lican Comunicações SL, Castilla y León
- Certificado em Segurança Informática pelo CFTIC Getafe, Madrid
- Técnico Superior em Sistemas de Telecomunicações e Informática pelo IES Trinidad Arroyo, Palencia
- Técnico Superior em Instalações Eletrotécnicas MT e BT pelo IES Trinidad Arroyo, Palencia
- Formação em Engenharia Reversa, Esteganografia e Criptografia pela Academia Hacker Incibe

A TECH selecionou cuidadosamente toda a equipe de professores deste programa para que você aprenda com os melhores especialistas da atualidade"

10

Impacto para a sua carreira

A conclusão deste Executive Master em MBA en Gestão de Segurança Cibernética (CISO, Chief Information Security Officer) irá agregar mais qualidade à qualificação dos profissionais de negócios, ao oferecer todo o conhecimento que, embora pareça distante do seu trabalho diário, é de grande utilidade para controlar aqueles processos de TI que podem conter um elemento externo prejudicial que afete toda a empresa. Por isso, é essencial uma especialização mais ampla nesta área, não apenas para o desenvolvimento pessoal e profissional dos alunos, mas também para as empresas nas quais eles trabalham.

A TECH coloca todos os seus recursos acadêmicos à disposição dos seus alunos para que adquiram as competências necessárias que os levarão ao sucesso"

Este Executive Master proporcionará ao aluno a qualificação adequada para uma mudança decisiva em sua carreira.

Você está preparado para crescer profissionalmente? Uma excelente melhoria profissional espera por você

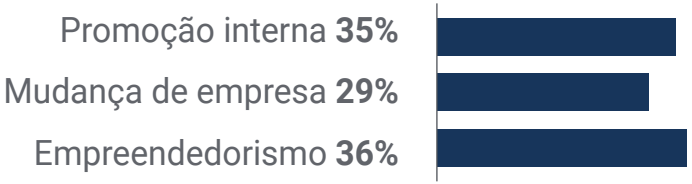
O Executive Master em MBA en Gestão de Segurança Cibernética (CISO, Chief Information Security Officer) da TECH Global University é um programa de estudos intensivo e valioso para a melhoria das habilidades profissionais dos alunos em uma área de ampla competência. É sem dúvida uma oportunidade única para melhorar profissionalmente, mas também pessoalmente, pois envolve esforço e dedicação.

Se você quer se superar, realizar uma mudança profissional positiva e se relacionar com os melhores a TECH é o lugar certo para você.

Um programa com um elevado nível acadêmico que conduzirá sua carreira ao sucesso.

Momento da mudança

Tipo de mudança



Melhoria salarial

A conclusão deste programa significa um aumento salarial anual de mais de **25,22%** para nossos alunos

11

Benefícios para a sua empresa

O Executive Master em MBA en Gestão de Segurança Cibernética (CISO, Chief Information Security Officer) contribui para elevar o talento da organização a seu potencial máximo, especializando líderes de alto nível. Dessa forma, os profissionais de negócios poderão oferecer um plus de qualidade à empresa, através das capacidades necessárias para que eles mesmos possam controlar os processos de cibersegurança. Um programa de estudos que se adapta aos alunos lhe permite adquirir as ferramentas necessárias para aplicá-las em sua prática diária, obtendo grandes benefícios para sua empresa.

Um programa de estudos essencial para profissionais de negócios que desejam monitorar e gerenciar possíveis problemas de Segurança Cibernética"

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

01

Crescimento do talento e do capital intelectual

O profissional irá proporcionar à empresa novos conceitos, estratégias e perspectivas que poderão gerar mudanças relevantes na organização.

02

Retenção de gestores de alto potencial para evitar a evasão de talentos

Esse programa fortalece o vínculo entre empresa e profissional e abre novos caminhos para o crescimento profissional dentro da companhia.

03

Construindo agentes de mudança

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

04

Maiores possibilidades de expansão internacional

Graças a este programa, a empresa entrará em contato com os principais mercados da economia mundial.

05

Desenvolvimento de projetos próprios
O profissional poderá trabalhar em um projeto real ou desenvolver novos projetos na área de P&D ou desenvolvimento de negócio da sua empresa.

06

Aumento da competitividade
Este programa proporcionará aos profissionais as habilidades necessárias para assumir novos desafios e impulsionar a empresa.

12

Certificado

O Executive Master em MBA en Gestão de Segurança Cibernética (CISO, Chief Information Security Officer) garante, além da capacitação mais rigorosa e atualizada, o acesso a um título de Executive Master emitido pela TECH Universidade Tecnológica.

Conclua este programa de estudos com sucesso e receba o seu certificado sem sair de casa e sem burocracias”

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

Uma vez aprovadas as avaliações, o aluno receberá por correio o certificado* correspondente ao título de **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 empregos, concursos públicos e avaliação de carreira profissional.

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

Modalidade: **online**

Duração: **12 meses**


tech universidade tecnológica

Outorga o presente

CERTIFICADO

a

Sr./Sra. _____, com documento de identidade nº_____

por ter concluído e aprovado com sucesso o programa de

EXECUTIVE MASTER

em

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

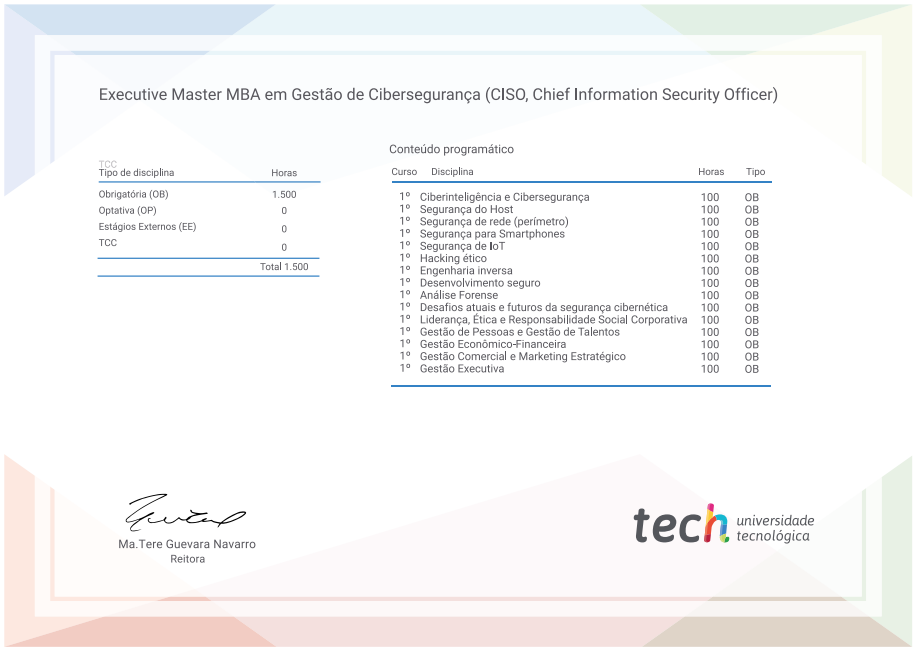
Este é um curso próprio desta Universidade, com duração de 1.500 horas, com data de início dd/mm/aaaa e data final dd/mm/aaaaa.

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

Ma.Tere Guevara Navarro
Reitora

código único TECH: AFWOR23S techtitute.com/titulos


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

TCC

Tipo de disciplina	Horas
Obrigatória (OB)	1.500
Optativa (OP)	0
Estágios Externos (EE)	0
TCC	0
	Total 1.500

Conteúdo programático

Curso	Disciplina	Horas	Tipo
1º	Ciberinteligência e Cibersegurança	100	OB
1º	Segurança do Host	100	OB
1º	Segurança de rede (perímetro)	100	OB
1º	Segurança para Smartphones	100	OB
1º	Segurança de IoT	100	OB
1º	Hacking ético	100	OB
1º	Engenharia inversa	100	OB
1º	Desenvolvimento seguro	100	OB
1º	Análise Forense	100	OB
1º	Desafios atuais e futuros da segurança cibernética	100	OB
1º	Liderança, Ética e Responsabilidade Social Corporativa	100	OB
1º	Gestão de Pessoas e Gestão de Talentos	100	OB
1º	Gestão Econômico-Financeira	100	OB
1º	Gestão Comercial e Marketing Estratégico	100	OB
1º	Gestão Executiva	100	OB

Ma.Tere Guevara Navarro
Reitora

tech universidade tecnológica

*Apostila de Haia: "Caso o aluno solicite que 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**
- Certificado: **TECH Universidade Tecnológica**
- Horário: **no seu próprio ritmo**
- Provas: **online**

Executive Master

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

tech universidade tecnológica