Mestrado

MBA em Gestão de Cibersegurança Avançada (CISO)

tech global university

tech global university

Mestrado
MBA em Gestão de Cibersegurança Avançada (CISO)

- Modalidade: **Online**
- Duração: **12 meses**
- Certificação: **TECH Global University**
- Acreditação: **90 ECTS**
- Horário: **Ao seu próprio ritmo**
- Exames: **Online**

Acesso ao site: www.techtitute.com/pt/informatica/mestrado/mestrado-mba-gestao-ciberseguranca-avancada-ciso

Índice

01

Apresentação

O mundo atual está a caminhar para a digitalização total. Cada vez mais processos, operações e tarefas de todos os tipos são realizados através de um dispositivo eletrónico. Mas este progresso tem também alguns riscos, como é o caso dos computadores, *smartphones*, *tablets* e todos os tipos de aplicações digitais podem ser susceptíveis de ciberataques. Por esta razão, muitas empresas estão à procura de especialistas que possam liderar e gerir eficazmente a cibersegurança dos seus serviços. Este novo perfil profissional é muito procurado, pelo que este programa foi concebido para fornecer os mais recentes conhecimentos e técnicas ao informático, que estará preparado para ser o diretor de cibersegurança em qualquer empresa que o requeira.

Este programa irá prepará-lo intensivamente para se especializar na gestão da cibersegurança, o perfil profissional mais procurado atualmente no domínio das TI"

Nos últimos anos, o processo de digitalização acelerou, impulsionado pelos avanços contínuos nas tecnologias da informação. Assim, não foi apenas a tecnologia que registou grandes melhorias, mas também as próprias ferramentas digitais com as quais muitas tarefas são realizadas atualmente. Por exemplo, estes desenvolvimentos tornaram possível que muitas transacções bancárias sejam efetuadas a partir de uma aplicação móvel. Houve também novos desenvolvimentos no setor da saúde, nos sistemas de marcação de consultas e no acesso aos registos médicos. Além disso, graças a estas tecnologias,é possível consultar faturas ou solicitar serviços a empresas em áreas como a telefonia.

Mas estes avanços também conduziram a um aumento das vulnerabilidades informáticas. Assim, enquanto as opções para realizar várias atividades e tarefas se expandiram, os ataques à segurança dos dispositivos, aplicações e sítios Web aumentaram proporcionalmente. Consequentemente, cada vez mais empresas procuram profissionais de cibersegurança capazes de lhes proporcionar uma proteção adequada contra todos os tipos de ciberataques.

Assim, o perfil de Gestor de Cibersegurança é um dos mais procurados pelas empresas que operam na Internet ou têm serviços no ambiente digital. E para responder a esta procura, a TECH concebeu este MBA em Gestão de Cibersegurança Avançada (CISO), que fornecerá ao especialista em informática todas as ferramentas necessárias para desempenhar este cargo de forma eficaz e de acordo com os últimos desenvolvimentos em matéria de proteção e vulnerabilidades neste domínio tecnológico.

Neste programa poderá estudar em profundidade aspectos como a segurança no desenvolvimento e conceção de sistemas, as melhores técnicas criptográficas e a segurança em ambientes de computação em nuvem. E fá-lo-á através de uma metodologia 100% online com a qual poderá conciliar o seu trabalho profissional com os seus estudos, sem horários rígidos nem deslocações incómodas a um centro académico. Beneficiará também de numerosos recursos pedagógicos multimédia, ministrados pelos docentes mais prestigiados e especializados na área da cibersegurança.

Este **Mestrado em MBA Gestão de Cibersegurança Avançada (CISO)** conta com o conteúdo educacional mais completo e atualizado do mercado. As suas principais características são:

- O desenvolvimento de casos práticos apresentados por especialistas em Informática Cibersegurança
- Os conteúdos gráficos, esquemáticos e predominantemente práticos com que está concebido fornecem informações científicas e práticas sobre as disciplinas que são essenciais para a prática profissional
- Os exercícios práticos onde o processo de autoavaliação pode ser efetuado a fim de melhorar a aprendizagem
- O seu foco especial em metodologias inovadoras
- Aulas teóricas, perguntas ao especialista, fóruns de discussão sobre questões controversas e atividades de reflexão individual
- A disponibilidade de acesso ao conteúdo a partir de qualquer dispositivo fixo ou portátil com ligação à Internet

Conheça em primeira mão as melhores técnicas de segurança aplicadas a ambientes de Cloud Computing ou tecnologia Blockchain"

Desfrutará de uma vasta oferta de conteúdos multimédia para acelerar o seu processo de aprendizagem, ao mesmo tempo que recebe um corpo docente de grande prestígio no domínio da cibersegurança"

A metodologia online da TECH permitir-lhe-á escolher a hora e o local de estudo, sem prejudicar o seu trabalho profissional.

Poderá tornar-se o Gestor de Cibersegurança das melhores empresas da sua área.

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

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

O design deste programa foca-se na Aprendizagem Baseada em Problemas, através da qual o profissional deverá tentar resolver as diferentes situações da atividade profissional que surgem ao longo do curso. Para tal, contará com a ajuda de um sistema inovador de vídeo interativo desenvolvido por especialistas reconhecidos.

02

Objetivos

O rápido desenvolvimento das tecnologias da informação trouxe grandes avanços, proporcionando numerosos serviços à população em geral. No entanto, o número de vulnerabilidades e de ciberataques também aumentou, pelo que o principal objetivo deste programa é transformar o informático num verdadeiro especialista em gestão da cibersegurança, garantindo-lhe uma enorme e imediata progressão profissional. As suas novas competências dar-lhe-ão a oportunidade de aceder a grandes empresas digitalmente activas em vários sectores.

O objetivo deste programa é fazer de si um profissional preparado para liderar o departamento de cibersegurança de uma grande empresa"

Objetivos gerais

- Gerar conhecimentos especializados sobre um sistema de informação, tipos e aspetos de segurança a ter em conta
- Identificar as vulnerabilidades de um sistema de informação
- Desenvolver a regulamentação legal e a tipificação do delito no ataque a um sistema de informação
- Avaliar os diferentes modelos de arquitetura de segurança para estabelecer o modelo mais apropriado para a organização
- Identificar os quadros regulamentares aplicáveis e as bases reguladoras dos mesmos
- Analisar a estrutura organizacional e funcional de uma área de segurança da informação (o departamento do CISO)
- Analisar e desenvolver o conceito de risco, incerteza dentro do ambiente em que vivemos
- Examinar o Modelo de Gestão de Riscos com base na norma ISO 31.000
- Examinar a ciência da criptologia e a relação com os seus ramos: criptografia, criptoanálise, esteganografia e estegoanálise
- Analisar os tipos de criptografia de acordo com o tipo de algoritmo e de acordo com a sua utilização
- Examinar os certificados digitais
- Examinar a Infraestrutura de Chave Pública (PKI)
- Desenvolver o conceito de gestão de identidades
- Identificar os métodos de autenticação
- Gerar um conhecimento especializado sobre o ecossistema de segurança Informática
- Avaliar o conhecimento em termos de cibersegurança
- Identificar os âmbitos de segurança em *Cloud*
- Analisar os serviços e ferramentas em cada um dos domínios da segurança
- Desenvolver as especificações de segurança de cada tecnologia LPWAN
- Analisar de forma comparativa a segurança das tecnologias LPWAN

Os seus objetivos profissionais estarão agora ao seu alcance graças a este Mestrado, que proporciona os conhecimentos mais avançados em cibersegurança"

Objetivos específicos

Módulo 1. Segurança no desenho e desenvolvimento de sistemas

- Avaliar a segurança de um sistema de informação em todos os seus componentes e camadas
- Identificar os tipos de ameaças à segurança atuais e as suas tendências
- Estabelecer orientações de segurança definindo políticas e planos de segurança e contingência
- Analisar estratégias e ferramentas para garantir a integridade e segurança dos sistemas de informação
- Aplicar as técnicas e ferramentas específicas para cada tipo de ataque ou vulnerabilidade de segurança
- Proteger a informação sensível armazenada no sistema de informação
- Dispor do enquadramento legal e tipificação do crime, completando a visão com a tipificação do infrator e da sua vítima

Módulo 2. Arquiteturas e modelos de segurança da informação

- Alinhar o Plano Diretor de Segurança com os objetivos estratégicos da organização
- Estabelecer um quadro contínuo de gestão de riscos como parte integrante do Plano Diretor de Segurança
- Determinar os indicadores apropriados para monitorizar a implementação do SGSI
- Estabelecer uma estratégia de segurança baseada em políticas
- Analisar os objetivos e procedimentos associados ao plano de sensibilização dos empregados, fornecedores e sócios
- Identificar, dentro do quadro regulamentar, os regulamentos, certificações e leis aplicáveis a cada organização
- Desenvolver os elementos fundamentais exigidos pela norma ISO 27001:2013
- Implementar um modelo de gestão da privacidade em conformidade com o regulamento europeu GDPR/RGPD

Módulo 3. Gestão da Segurança IT

- Identificar as diferentes estruturas que pode ter uma área de segurança da informação
- Desenvolver um modelo de segurança baseado em três linhas de defesa
- Apresentar os diferentes comités periódicos e extraordinários em que está envolvida a área de cibersegurança
- Identificar as ferramentas tecnológicas que apoiam as principais funções da equipa de operações de segurança (SOC)
- Avaliar as medidas de controlo da vulnerabilidade adequadas a cada cenário
- Desenvolver o quadro de operações de segurança com base em NIST CSF
- Especificar o âmbito dos diferentes tipos de auditorias (*Red Team*, *Pentesting*, *Bug Bounty*, etc.)
- Propor as actividades a serem realizadas após um incidente de segurança
- Configurar um centro de comando de segurança da informação que englobe todos os atores relevantes (autoridades, clientes, fornecedores, etc.)

Módulo 4. Análise de riscos e ambiente de segurança IT

- Examinar, com uma visão holística, o ambiente em que nos movemos
- Identificar os principais riscos e oportunidades que podem afetar a realização dos nossos objetivos
- Analisar os riscos com base nas melhores práticas à nossa disposição
- Avaliar o impacto potencial de tais riscos e oportunidades
- Desenvolver técnicas que permitam lidar com os riscos e oportunidades de uma forma que maximize a nossa contribuição de valor
- Examinar em profundidade as diferentes técnicas de transferência de riscos, assim como de valor
- Gerar valor a partir da conceção de modelos próprios para a gestão ágil de riscos
- Examinar os resultados para propor melhorias contínuas na gestão de projetos e processos com base em modelos de gestão orientados para o risco o *Risk-Driven*
- Inovar e transformar dados gerais em informação relevante para a tomada de decisões com base no risco

Módulo 5. Criptografia em IT

- Compilar as operações fundamentais (XOR, grandes números, substituição e transposição) e os vários componentes (funções One-Way, Hash, geradores de números aleatórios)
- Analisar as técnicas criptográficas
- Desenvolver os diferentes algoritmos criptográficos
- Demonstrar a utilização de assinaturas digitais e a sua aplicação nos certificados digitais
- Avaliar os sistemas de gestão de chaves e a importância da longitude das chaves criptográficas
- Examinar algoritmos de derivação de chaves
- Analisar o ciclo de vida das chaves
- Avaliação dos modos de cifragem de blocos e cifragem de fluxo
- Determinar os geradores de números pseudoaleatórios
- Desenvolver casos reais de aplicações criptográficas, tais como Kerberos, PGP ou cartões inteligentes
- Examinar associações e organismos relacionados, tais como ISO, NIST ou NCSC
- Determinar os desafios na criptografia da computação quântica

Módulo 6. Gestão de identidade e acessos em segurança IT

- Desenvolver o conceito de identidade digital
- Avaliar o controlo de acesso físico à informação
- A lógica da autenticação biométrica e da autenticação MFA
- Avaliar ataques relacionados com a confidencialidade da informação
- Analisar a federação de identidades
- Estabelecer o controlo de acesso à rede

Módulo 7. Segurança em comunicações e operação software

- Desenvolver conhecimento especializado em matéria de segurança física e lógica
- Demonstrar o conhecimento em comunicações e redes
- Identificar os principais ataques ataques maliciosos
- Estabelecer um quadro de desenvolvimento seguro
- Demonstrar conhecer os principais regulamentos dos sistemas de gestão da segurança da informação
- Fundamentar o funcionamento de um centro de operações de cibersegurança
- Demonstrar a importância das práticas de cibersegurança para as catástrofes organizacionais

Módulo 8. Segurança em ambientes Cloud

- Identificar riscos de uma implantação de infraestrutura em *Cloud* pública
- Definir os requisitos de segurança
- Desenvolvimento de um plano de segurança para a implantação em *Cloud*
- Identificar os serviços *Cloud* a implementar para a execução de um plano de segurança
- Determinar as disposições operacionais necessárias para os mecanismos de prevenção
- Estabelecer as diretrizes para um sistema de *Logging* e monitorização
- Propor ações de resposta a incidentes

Módulo 9. Segurança em comunicações de dispositivos Iot

- Apresentar a arquitetura simplificada do IoT
- Fundamentar as diferenças entre tecnologias de conetividade generalistas e tecnologias de conectividade para a IoT
- Estabelecendo o conceito do triângulo de ferro da conectividade da IoT
- Analisar as especificações de segurança da tecnologia LoRaWAN, da tecnologia NB-IoT e da tecnologia WiSUN
- Fundamentar a eleição da tecnologia IoT adequada para cada projeto

Módulo 10. Plano de continuidade do negócio associado à segurança

- Apresentar os elementos-chave de cada fase e analisar as caraterísticas do Plano de Continuidade de Negócio (PCN)
- Fundamentar a necessidade de um Plano de Continuidade para o Negócio
- Determinar os mapas de sucesso e de risco para cada fase do o Plano de Continuidade de Negócio
- Especificar como é estabelecido um Plano de Ação para a implementação
- Avaliar a integridade de um Plano de Continuidade de Negócios (PCN)
- Desenvolver um plano para a implementação bem sucedida de umo Plano de Continuidade de Negócio

Módulo 11. Liderança Ética e Responsabilidade Social das Empresa

- Analisar o impacto da globalização na governação e no governo das sociedades
- Avaliar a importância de uma liderança eficaz na gestão e no sucesso das empresas
- Definir estratégias de gestão transculturais e a sua relevância em ambientes empresariais diversificados
- Desenvolver competências de liderança e compreender os desafios atuais que os líderes enfrentam
- Identificar os princípios e práticas da ética empresarial e a sua aplicação na tomada de decisões empresariais
- Estruturar estratégias para a implementação e melhoria da sustentabilidade e responsabilidade social nas empresas

Módulo 12. Gestão de Pessoas e Gestão de Talentos

- Determinar a relação entre a direção estratégica e a gestão dos recursos humanos
- Aprofundar as competências necessárias para uma gestão eficaz dos recursos humanos por competências
- Aprofundar as metodologias de avaliação e gestão do desempenho
- Integrar as inovações na gestão de talentos e o seu impacto na retenção e conservação da equipe
- Desenvolver estratégias de motivação e desenvolvimento de equipas de elevado desempenho
- Propor soluções eficazes para a gestão da mudança e a resolução de conflitos nas organizações

Módulo 13. Gestão Económica-financeira

- Analisar o ambiente macroeconómico e a sua influência no sistema financeiro nacional e internacional
- Definir os sistemas de informação e o Business Intelligence para a tomada de decisões financeiras
- Distinguir entre decisões financeiras fundamentais e gestão do risco na gestão financeira
- Avaliar estratégias de planeamento financeiro e de obtenção de financiamento para as empresas

Módulo 14. Gestão comercial e marketing estratégico

- Estruturar o quadro concetual e a importância da gestão empresarial nas empresas
- Aprofundar os principais elementos e atividades do marketing e o seu impacto na organização
- Determinar as fases do processo de planeamento estratégico de marketing
- Avaliar estratégias para melhorar a comunicação empresarial e a reputação digital da empresa

Módulo 15. *Management* Executivo

- Definir o conceito de Gestão Geral e a sua relevância para a gestão empresarial
- Avaliar as funções e responsabilidades do gestor na cultura organizacional
- Analisar a importância da gestão das operações e da gestão da qualidade na cadeia de valor
- Desenvolver as capacidades de comunicação interpessoal e de falar em público para a formação de porta-vozes

Os seus objetivos profissionais estarão agora ao seu alcance graças a este Mestrado, que proporciona os conhecimentos mais avançados em cibersegurança”

03

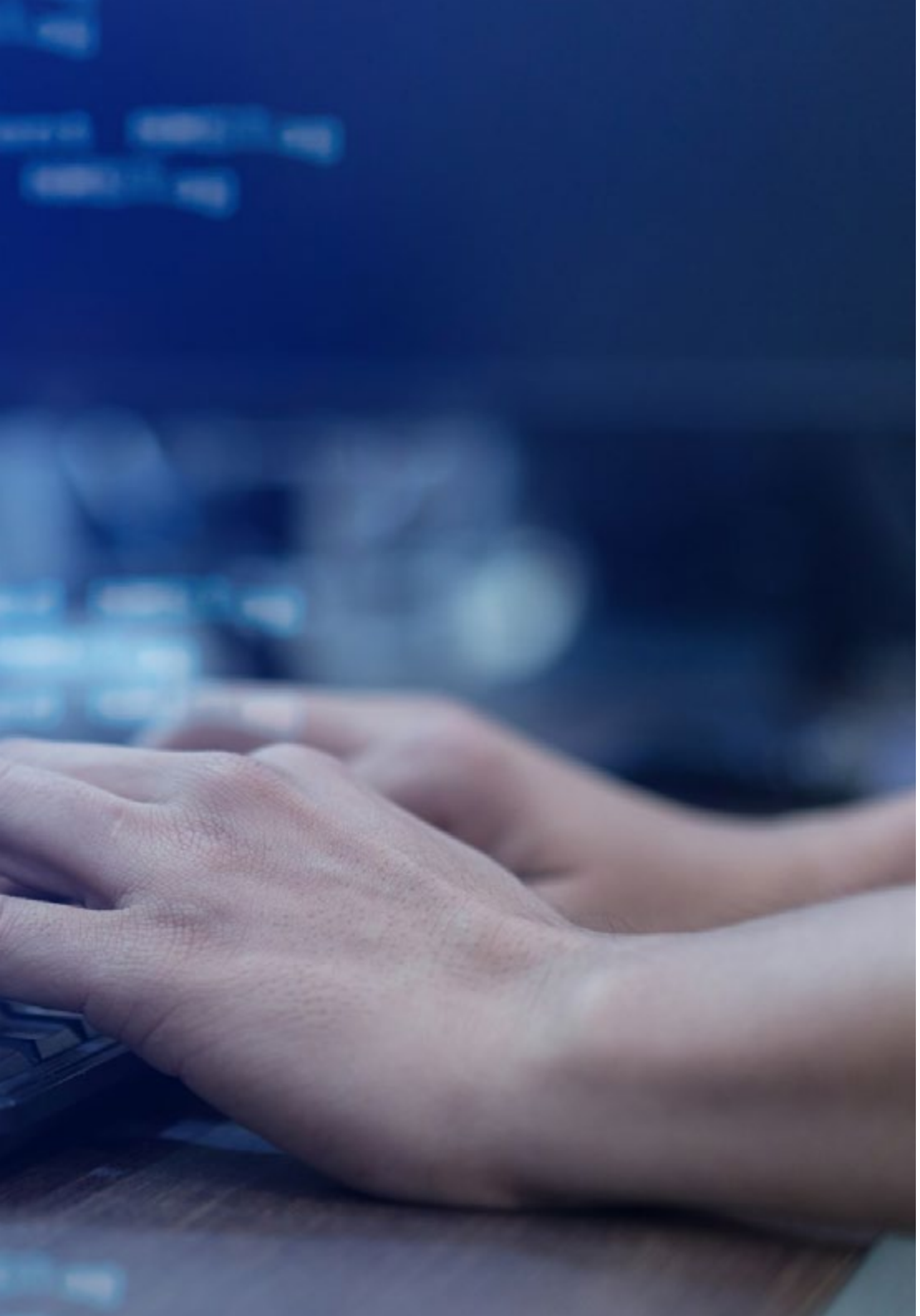
Competências

Graças a este Mestrado, o profissional adquirirá inúmeras novas competências no domínio da cibersegurança. A irrupção, nos últimos anos, de tecnologias como o *Blockchain*, o *Cloud Computing* ou a inteligência artificial conduziu ao desenvolvimento de novos domínios da cibersegurança. Por esta razão, este programa foi especialmente concebido para dotar o profissional de todas as competências necessárias para se adaptar a estas tecnologias em crescimento.

As competências que este programa lhe proporcionará permitir-lhe-á atualizar-se e adaptar-se ao novo ambiente informático, onde tecnologias como Blockchain e inteligência artificial entraram em cena"

Competências gerais

- Aplicar as medidas de segurança mais adequadas em função das ameaças
- Determinar a política e o plano de segurança do sistema de informação de uma empresa, completando a conceção e implementação do plano de contingência
- Estabelecer um programa de auditoria que satisfaça as necessidades de autoavaliação da organização em matéria de cibersegurança
- Desenvolver um programa de análise e controlo de vulnerabilidades e um plano de resposta a incidentes de cibersegurança
- Maximizar as oportunidades apresentadas e eliminar a exposição a todos os riscos potenciais a partir do próprio desenho
- Compilar Sistemas de gestão de chaves
- Avaliar a segurança da informação de uma empresa
- Analisar os sistemas de acesso à informação
- Desnvolver as melhores práticas no desenvolvimento seguro
- Apresentar os riscos para as empresas de não terem um ambiente informático seguro



Competências específicas

- Desenvolver um Sistema de Gestão de Segurança da Informação(SGSI)
- Identificar os elementos chaves que conformam um SGSI
- Aplicar a metodologia MAGERIT para fazer evoluir o modelo e levá-lo um nível mais avançado
- Conceber novas metodologias próprias de gestão de riscos, com base no conceito de *agile Risk Management*
- Identificar, analisar, avaliar e abordar os riscos enfrentados pelo profissional a partir de uma nova perspetiva empresarial baseada num modelo *risk-driven* ou movido pelo risco não só para sobreviver no seu próprio ambiente, mas também para impulsionar a sua própria contribuição de valor
- Examinar o processo de desenho de uma estratégia de segurança ao implantar serviços empresariais em *Cloud*
- Avaliar as diferenças nas implementações concretas de diferentes fornecedores de *Cloud* pública
- Avaliar as opções de conetividade de IoT para abordar um projeto, com especial ênfase nas tecnologias LPWAN
- Apresentar as especificações básicas das principais tecnologias LPWAN para a IoT

04

Direção do curso

A enorme complexidade da cibersegurança atual exige um processo de aprendizagem minucioso e detalhado. Por este motivo, a TECH decidiu reunir o melhor pessoal docente especializado neste domínio. Desta forma, o profissional beneficiará do acompanhamento e supervisão de um corpo docente atualizado com os últimos avanços nesta área, para adquirir as competências necessárias para técnicas de cibersegurança no seu trabalho quotidiano, ao mesmo tempo que obtêm as competências de gestão necessárias neste domínio.

Terá verdadeiros especialistas em cibersegurança à sua disposição. Esta é a oportunidade que estava à procura"

Diretor Internacional Convidado

Com mais de 20 anos de experiência na conceção e gestão de equipas globais de **aquisição de talentos**, Jennifer Dove é especialista em **recrutamento** e **estratégia tecnológica**. Ao longo da sua experiência profissional, ocupou cargos de direção em várias organizações tecnológicas de empresas cotadas na bolsa ***Fortune 50***, como **NBCUniversal** e **Comcast**. O seu historial permitiu-lhe destacar-se em ambientes competitivos e de elevado crescimento.

Como **Vice-presidente de Aquisição de Talentos** na **Mastercard**, é responsável pela supervisão da estratégia e execução da integração de talentos, trabalhando com os líderes empresariais e de **Recursos Humanos** para atingir os objetivos operacionais e estratégicos de recrutamento. Em particular, tem por objetivo **criar equipas diversificadas**, **inclusivas** e **de alto rendimento** que promovem a inovação e o crescimento dos produtos e serviços da empresa. É também uma especialista na utilização de ferramentas para atrair e reter os melhores profissionais de todo o mundo. É também responsável por **amplificar** a **marca do empregador** e a proposta de valor de **Mastercard** através de publicações, eventos e redes sociais.

Jennifer Dove tem demonstrado o seu empenho no desenvolvimento profissional contínuo, participando ativamente em redes de profissionais de **Recursos Humanos** e contribuindo para a incorporação de numerosos trabalhadores em diferentes empresas. Depois de obter a sua licenciatura em **Comunicação Organizacional** pela Universidade de **Miami**, ocupou cargos superiores de recrutamento em empresas de vários setores.

Por outro lado, foi reconhecida pela sua capacidade de liderar transformações organizacionais, **integrar tecnologias** nos **processos de recrutamento** e desenvolver programas de liderança que preparem as instituições para os desafios futuros. Também implementou com êxito programas de **bem-estar profissional** que aumentaram significativamente a satisfação e a retenção dos trabalhadores.

Sra. Jennifer Dove

- Vice-Presidente, Aquisição de Talentos, Mastercard, Nova Iorque, EUA
- Diretora de Aquisição de Talentos na NBCUniversal Media, Nova Iorque, EUA
- Diretora de Recrutamento da Comcast
- Responsável pelo recrutamento na Rite Hire Advisory
- Vice-Presidente Executiva, Divisão de Vendas na Ardor NY Real Estate
- Diretora de Recrutamento na Valerie August & Associates
- Executiva de contas na BNC
- Executivo de contas na Vault
- Formada em Comunicação Organizacional pela Universidade de Miami

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

Diretor Internacional Convidado

Líder tecnológico com décadas de experiência nas multinacionais líderes no sector da tecnologia **, Rick Gauthier desenvolveu-se de forma notável no domínio dos** serviços **na** nuvem e melhoria de processos de ponta a ponta. Foi reconhecido como um líder e gestor de equipas altamente eficiente, demonstrando um talento natural para assegurar um elevado nível de empenho entre os seus empregados.

Tem um dom inato para a estratégia e a inovação executiva, desenvolvendo novas ideias e apoiando o seu sucesso com dados de qualidade. **A sua carreira na** Amazon permitiu-lhe gerir e integrar os serviços informáticos da empresa nos Estados Unidos. **Na** Microsoft liderou uma equipa de 104 pessoas, responsável pelo fornecimento de infraestruturas de TI a toda a empresa e pelo apoio aos departamentos de engenharia de produtos em toda a empresa.

Esta experiência permitiu-lhe destacar-se como um gestor de alto impacto com capacidades notáveis para aumentar a eficiência, a produtividade e a satisfação geral dos clientes.

Dr. Rick Gauthier

- Gestor regional de TI na Amazon, Seattle, EUA
- Gestor de programas sénior na Amazon
- Vice-presidente da Wimmer Solutions
- Diretor Sénior de Serviços de Engenharia de Produtividade na Microsoft
- Licenciado em Cibersegurança pela Western Governors University
- Certificado técnico em *Commercial Diving* por Divers Institute of Technology
- Licenciado em Estudos Ambientais pelo The Evergreen State College

Aproveite a oportunidade para conhecer os últimos desenvolvimentos neste domínio e aplicá-los à sua prática quotidiana"

Diretor Internacional Convidado

Romi Arman é uma especialista de renome internacional com mais de duas décadas de experiência em **Transformação Digital**, **Marketing, Estratégia** e **Consultoria**. Ao longo da sua longa carreira, assumiu diferentes riscos e é um permanente **defensor** da **inovação** e a **mudança** no ambiente empresarial. Com essa experiência, tem trabalhado com diretores executivos e organizações empresariais em todo o mundo, levando-os a afastarem-se dos modelos de negócio tradicionais. Assim, ajudou empresas como a energética Shell a tornarem-se **verdadeiros líderes de mercado,** centradas em seus **clientes** e o **mundo digital.**

As estratégias concebidas por Arman têm um impacto latente, uma vez que permitiram a várias empresas **melhorar as experiências dos consumidores, a equipe** e **os acionistas** por igual. O sucesso deste especialista é quantificável através de métricas tangíveis como o **CSAT**, o **envolvimento dos colaboradores** nas instituições onde trabalhou e o crescimento do **indicador financeiro EBITDA** em cada uma delas.

Além disso, na sua carreira profissional, cultivou e **liderou equipas com elevado desempenho** que até receberam prémios pelo seu trabalho no **potencial transformador**. No caso da Shell, em particular, o executivo sempre se propôs a superar três desafios: dar resposta à complexa **demandas** de **descarbonização** de clientes, **apoiar** uma "**descarbonização rentável**" e **revisar** uma imagem fragmentada de **dados, digital e tecnológic**o. Assim, os seus esforços demonstraram que, para alcançar um sucesso sustentável, é essencial partir das necessidades dos consumidores e lançar as bases para a transformação dos processos, dos dados, da tecnologia e da cultura.

Por outro lado, o diretor distingue-se pelo seu domínio das **aplicações empresariais** da **Inteligencia Artificial,** em que possui um diploma de pós-graduação da London Business School. Ao mesmo tempo, acumulou experiência em **IoT** e o **Salesforce.**

Sr. Romi Arman

- Diretor de Transformação Digital (CDO) na Corporação Energética Shell, Londres, Reino Unido
- Chefe Global de E-Commerce e Atendimento ao Cliente na Corporação Energética Shell
- Gestor de Conta Nacional (fabricantes de equipes originais e minoristas de automação) para a Shell em Kuala Lumpur, Malásia
- Consultor de gestão sénior (sector dos serviços financeiros) para a Accenture de Singapura
- Licenciado pela Universidade de Leeds
- Diploma de Pós-Graduação em Aplicações Empresariais de IA para Executivos Seniores
  Escola de Negócios de Londres
- Certificação CCXP para profissionais de experiência do cliente
- Curso Executivo de Transformação Digital do IMD

Pretende atualizar os seus conhecimentos com a mais elevada qualidade educativa? A TECH oferece-lhe o conteúdo mais atualizado do mercado académico, concebido por especialistas de renome internacional"

Diretor Internacional Convidado

Manuel Arens é um **profissional experiente** em gestão de dados e líder de uma equipa altamente qualificada. De fato, Arens ocupa o cargo de **gestor global de compras** na divisão de Infra-estruturas Técnicas e Centros de Dados da Google, onde passou a maior parte da sua carreira. Com sede em Mountain View, Califórnia, forneceu soluções para os desafios operacionais do gigante tecnológico, tais como **integridade dos dados principais,** as **actualizações dos dados dos fornecedores** e a **priorização** dos mesmos. Liderou o planeamento da cadeia de fornecimento de centros de dados e a avaliação de riscos de fornecedores, conduzindo a melhorias de processos e à gestão do fluxo de trabalho que resultaram em poupanças de custos significativas.

Com mais de uma década de trabalho no fornecimento de soluções digitais e liderança para empresas em diversos sectores, tem uma vasta experiência em todos os aspectos do fornecimento de soluções estratégicas, incluindo **Marketing, análise dos media, medição** e **atribuição.** De facto, recebeu vários prémios pelo seu trabalho, incluindo o **Prémio de Liderança BIM**, o **Prémio de Liderança de Pesquisa**, **Prémio do Programa de Geração de Chumbo para Exportação** e o **Prémio para o melhor modelo de vendas da EMEA.**

Arens foi também **Gerente de Ventas** em Dublin, Irlanda. Nesta função, criou uma equipa de 4 para 14 membros em três anos e levou a equipa de vendas a alcançar resultados e a colaborar bem entre si e com equipas multifuncionais. Também trabalhou como **Analista Sénior** de Indústria, em Hamburgo, Alemanha, criando histórias para mais de 150 clientes, utilizando ferramentas internas e de terceiros para apoiar a análise. Desenvolveram e redigiram relatórios aprofundados para demonstrar o seu domínio do assunto, incluindo a compreensão dos **factores macroeconómicos e políticos/regulamentares** que afetam a adoção e difusão de tecnologias.

Também liderou equipas em empresas como **Eaton, Airbus e Siemens**, onde adquiriu uma experiência valiosa na gestão de contas e da cadeia de abastecimento. É particularmente conhecido pelo seu trabalho para exceder continuamente as expectativas, **construindo relações valiosas com os clientes** e **trabalhando sem problemas com pessoas a todos os níveis de uma organização,** incluindo partes interessadas, gestão, membros da equipa e clientes. A sua abordagem orientada para os dados e a sua capacidade para desenvolver soluções inovadoras e expansíveis para os desafios do sector tornaram-no um líder proeminente no seu domínio.

Sr. Manuel Arens

- Diretor global de aquisições na Google, Mountain View, EUA
- Diretor Sénior, Análise e Tecnologia B2B, Google, EUA
- Diretor de vendas na Google, Irlanda
- Analista industrial sénior na Google, Alemanha
- Gestor de contas Google, Irlanda
- Contas a Pagar em Eaton, Reino Unido
- Gestor da cadeia de abastecimento na Airbus, Alemanha

Aposte na TECH! Terá acesso aos melhores materiais didácticos, na vanguarda da tecnologia e da educação, implementados por especialistas de renome internacional na área"

Diretor Internacional Convidado

Andrea La Sala é umexecutivo de Marketing experiente cujos projetos tiveram um impacto significativo no ambiente da Moda. Ao longo da sua carreira de sucesso, desenvolveu uma variedade de tarefas relacionadas com Produtos, o Merchandising e a Comunicação.. **Tudo isto ligado a marcas de prestígio como** Giorgio Armani, Dolce&Gabbana, Calvin Klein**, entre outras.**

Os resultados deste gestor internacional dealto nível internacional **estão ligados à sua capacidade comprovada de** sintetizar a informação **em quadros claros e executar** ações concretas **alinhadas a objetivos** comerciais específicos. **Além disso, é reconhecido pela sua**proatividade e capacidade de adaptação a um ritmo acelerado. **de trabalho. A tudo isto, este especialista acrescenta uma** uma forte consciência comercial, visão de mercado e uma verdadeira paixão pelos produtos.s.

Como Diretor Global de Marca e Merchandising na Giorgio Armani**, supervisionou várias** estrategias de marketing **para** ropa e acessórios. **Além disso, as suas tácticas têm-se centrado nasnecessidades** e no comportamento dos retalhistas e dos consumidores.. **Neste cargo, La Sala foi também responsável pela conceção da comercialização de produtos em diferentes mercados, actuando como** chefe de equipa **nos**departamentos de Design, Comunicação e Vendas.

Por outro lado, em empresas como Calvin Klein o o Gruppo Coin**, realizou projetos para impulsionar** a estrutura, o desenvolvimento e a comercialização de diferentes coleções.. **Ao mesmo tempo, foi encarregado de criar** calendários eficazes para as campanhas **de compra e venta. Foi também responsável pelas** condições, custos, processos e prazos de entrega de várias operações.

Estas experiências fizeram de Andrea La Sala um dos principais e mais qualificados líderes empresariais no sector da Moda e do Luxo. Uma elevada capacidade de gestão que lhe permitiu implementar eficazmente o posicionamento positivo de diferentes marcas **redefinir os seus os seus indicadores-chave de desempenho (KPI).**

Sra. Andrea La Sala

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

Os profissionais internacionais mais qualificados e experientes esperam por si na TECH para lhe oferecer um ensino de primeira classe, atualizado e baseado nas últimas evidências científicas. Do que está à espera para se inscrever?"

Diretor Internacional Convidado

Mick Gram é sinónimo de inovação e excelência no domínio do Business Intelligence a nível internacional. A sua carreira de sucesso está ligada a posições de liderança em multinacionais como a Walmart e a Red Bull. É também conhecido pela sua visão na identificação de tecnologias emergentes que, a longo prazo, têm um impacto duradouro no ambiente empresarial.

Por outro lado, o executivo é considerado pioneiro na utilização de técnicas de visualização de dados que simplificaram conjuntos complexos, tornando-os acessíveis e facilitando a tomada de decisões. Esta competência tornou-se o pilar do seu perfil profissional, transformando-o numa mais-valia desejada por muitas organizações empenhadas em recolher informações e em gerar acções concretas com base nelas.

Um dos seus projectos mais proeminentes nos últimos anos tem sido a plataforma Walmart Data Cafe, a maior do seu género no mundo, ancorada na nuvem para análise de Big Data. Ocupou também o cargo de Diretor de Business Intelligence na Red Bull, abrangendo áreas como Vendas, Distribuição, Marketing e Operações da Cadeia de Abastecimento. A sua equipa foi recentemente reconhecida pela sua constante inovação na utilização da nova API do Walmart Luminate para obter informações sobre compradores e canais.

Quanto à sua formação, o executivo tem vários mestrados e pós-graduações em centros de prestígio como a Universidade de Berkeley, nos Estados Unidos, e a Universidade de Copenhaga, na Dinamarca. Através desta atualização contínua, o perito adquiriu as competências mais avançadas. Como tal, passou a ser visto como um líder nato da nova economia global, centrada na procura de dados e nas suas infinitas possibilidades.

Sr. Mich Gram

- Diretor de Business Intelligence e Analytics na Red Bull, Los Angeles, Estados Unidos
- Arquiteto de soluções de Business Intelligence para o Walmart Data Cafe
- Consultor independente de Business Intelligence e Ciência de Dados
- Diretor de Business Intelligence na Capgemini
- Analista sénior na Nordea
- Consultor Sénior de Business Intelligence para SAS
- Educação executiva em IA e aprendizagem automática na Faculdade de UC Berkeley de Engenharia
- MBA executivo em comércio eletrónico na Universidade de Copenhaga
- Licenciatura e Mestrado em Matemática e Estatística na Universidade de Copenhaga

Estuda na melhor universidade online do mundo segundo a Forbes! Neste MBA, terá acesso a uma extensa biblioteca de recursos multimédia, desenvolvida por professores de renome internacional"

Diretor Internacional Convidado

Scott Stevenson é um distinto especialista no sector do Marketing Digital que, há mais de 19 anos, está ligado a uma das empresas mais poderosas da indústria do entretenimento, a Warner Bros. **Discovery.** Nesta função, desempenhou um papel fundamental na supervisão da logística e do fluxo de trabalho do trabalho criativo em várias plataformas digitais, incluindo as redes sociais, pesquisa, display e meios lineares.

A liderança deste executivo tem sido crucial na condução de estratégias de produção de media pagos, resultando numa melhoria acentuada das taxas de conversão. Simultaneamente, assumiu outras funções, tais como Diretor de Serviços de Marketing e Gestor de Tráfego na mesma multinacional durante a sua anterior gestão.

Stevenson também esteve envolvido na distribuição global de jogos de vídeo e campanhas de propriedade digital. Foi também responsável pela introdução de estratégias operacionais relacionadas com a conceção, finalização e entrega de conteúdos de som e imagem para anúncios televisivos e trailers.

Além disso, o especialista possui um bacharelato em Telecomunicações pela Universidade da Florida e um mestrado em Escrita Criativa pela Universidade da Califórnia, o que demonstra as suas competências em comunicação e narração de histórias. Além disso, participou na Escola de Desenvolvimento Profissional da Universidade de Harvard em programas de vanguarda sobre a utilização da Inteligência Artificial nas empresas. Assim, o seu perfil profissional é um dos mais relevantes na área atual do Marketing e dos Media Digitais.

Sr. Scott Stevenson

- Diretor de Marketing Digital na Warner Bros. Discovery, Burbank, Estados Unidos
- Gestor de tráfego na Warner Bros. Entertainment
- Mestrado em Escrita Criativa pela Universidade da Califórnia
- Bacharelato em Telecomunicações pela Universidade da Florida

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

Diretor Internacional Convidado

Vencedora dos prémios "International Content Marketing Awards" pela criatividade, liderança e qualidade dos conteúdos noticiosos Wendy Thole-Muir é uma reputada Diretora de Comunicação altamente especializada no domínio da gestão da reputação.

Neste sentido, desenvolveu uma sólida carreira profissional de mais de duas décadas neste domínio, que o levou a fazer parte de prestigiadas entidades de referência internacional como a Coca-Cola. Esta função implica a supervisão e a gestão da comunicação empresarial, bem como o controlo da imagem da organização. As suas principais contribuições incluem a liderança da implementação da plataforma de interação interna Yammer. Como resultado, os empregados aumentaram o seu envolvimento com a marca e criaram uma comunidade que melhorou significativamente a transmissão de informações.

Além disso, tem sido responsável pela gestão da comunicação dos investimentos estratégicos das empresas em diferentes países africanos. Geriu diálogos em torno de investimentos significativos no Quénia, demonstrando o empenho das entidades no desenvolvimento económico e social do país. Por sua vez, recebeu numerosos prémios pela sua capacidade de gerir a perceção das empresas em todos os mercados em que opera. Desta forma, assegurou que as empresas mantivessem um perfil elevado e que os consumidores as associassem a uma elevada qualidade.

Além disso, no seu firme compromisso com a excelência, tem participado ativamente em conferências e simpósios mundiais de renome com o objetivo de ajudar os profissionais da informação a manterem-se na vanguarda das técnicas mais sofisticadas para o desenvolvimento de planos de comunicação estratégica bem sucedidos. Ajudou assim numerosos peritos a antecipar situações de crise institucional e a gerir eficazmente os acontecimentos adversos.

Sra. Wendy Thole-Muir

- Diretora de Comunicação Estratégica e Reputação Corporativa na Coca-Cola, África do Sul
- Diretor de Reputação Corporativa e Comunicações da ABI na SABMiller de Lovania, Bélgica
- Consultora de comunicação na ABI, Bélgica
- Consultora de Reputação e Comunicação da Third Door em Gauteng, África do Sul
- Mestrado em Estudos de Comportamento Social pela Universidade da África do Sul
- Mestrado em Sociologia e Psicologia pela Universidade da África do Sul
- Bacharelato em Ciências Políticas e Sociologia Industrial pela Universidade de KwaZulu-Natal
- Licenciatura em Psicologia pela Universidade da África do Sul

Graças a este curso universitário 100% online, poderá conciliar os seus estudos com as suas tarefas quotidianas, com a ajuda dos maiores especialistas internacionais no domínio do seu interesse. Inscreva-se já!

Direção

Dr. Martín Olalla Bonal

- Gestor Sénior de Práticas de Blockchain, EY
- Especialista Técnico de Cliente Blockchain, IBM
- Diretor de Arquitetura para Blocknitive
- Coordenador de Equipa em Bases de Dados Distribuídas Não-Relacionais para a WedoIT, uma subsidiária da IBM
- Arquiteto de Infraestruturas na Bankia
- Responsável do Departamento de Layout na T-Systems
- Coordenador de Departamento para a Bing Data España SL

Professores

Dr. Javier Nogales Ávila

- Enterprise Cloud and sourcing senior consultant. Quint
- Cloud and Technology Consultant. Indra
- Associate Technology Consultant. Accenture
- Licenciado pela Universidade de Jaén e University of Technology and Economics of Budapest (BME)
- Licenciatura em Engenharia de Organização Industrial

Dr. Juan Manuel Rodrigo Estébanez

- Cofundador da Ismet Tech
- Gestor de Segurança da Informação no Ecix Group
- *Operational Security Officer* na Atos IT Solutions and Services A/S
- Docente de Gestão da Cibersegurança em estudos universitários
- Licenciado em Engenharia pela Universidade de Valladolid
- Mestrado em Sistemas de Gestão Integrados pela Universidade CEU San Pablo

Professores

Dr. Antonio Gómez Rodríguez

- Engenheiro Principal de Soluções Cloud na Oracle
- Coorganizador do Málaga Developer Meetup
- Consultor Especialista para o Sopra Group e Everis
- Líder de equipas na System Dynamics
- Programador de Softwares na SGO Software
- Mestrado em E-Business pela Escola de Negócios de La Salle
- Pós-graduação em Tecnologias e Sistemas de Informação do Instituto Catalão de Tecnologia
- Licenciado em Engenharia Superior de Telecomunicações pela Universidade Politécnica da Catalunha

Dr. Jorge del Valle Arias

- Smart City Solutions & Software Business Development Manager España. Itron, Inc Consultor IoT
- Diretor de Negócios Interino de IoT. TCOMET
- Responsável pela Unidade de Negócios IoT, Indústria 4.0. Diode España
- Gestor da Área de Vendas da IoT e Telecomunicações. Aicox Soluciones
- Diretor Técnico (CTO) e Gestor de Desenvolvimento de Negócios. Consultoria TELYC
- Fundador e CEO de Sensor Intelligence
- Chefe de Operações e Projetos. Codio
- Diretor de Operações em Codium Networks
- Engenheiro-chefe de design de hardware e firmware. AITEMIN
- Chefe Regional de Planeamento e Otimização RF - Rede LMDS 3,5 GHz. Clearwire
- Engenheiro de Telecomunicações pela Universidade Politécnica de Madrid
- Executive MBA pela International Graduate School de La Salle de Madrid
- Mestrado em Energias Renováveis CEPYME

Sr. Félix Gonzalo Alonso

- Diretor-Geral e fundador da Smart REM Solutions
- Sócio Fundador e Responsável pela Engenharia de Riscos e Inovação. Dynargy
- Gerente e Sócio Fundador Risknova (Gabinete Pericial Especializado em Tecnologia)
- Licenciado em Engenharia de Organização Industrial pela Universidade Pontifícia de Comillas ICAI.
- Licenciado em Engenharia Técnica Industrial especializado em Electrónica Industrial pela Universidade Pontifícia de Comillas ICAI
- Mestrado em Gestão de Seguros pelo ICEA (Instituto para la Colaboración entre Entidades Aseguradoras)

Dr. Alejandro Entrenas

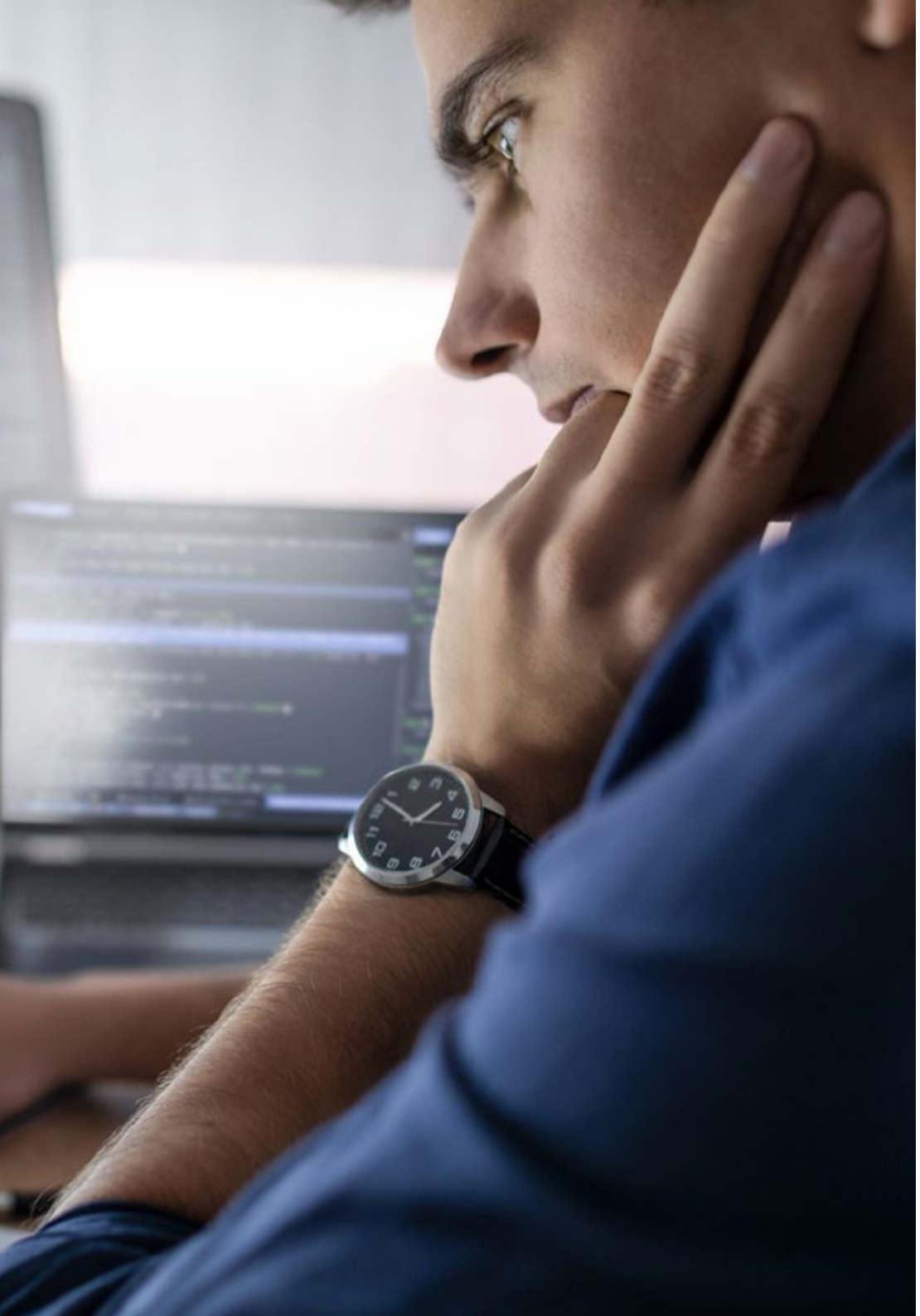
- Gestor de Projetos de Cibersegurança Entelgy Innotec Security
- Consultor de Cibersegurança Entelgy
- Analista de Segurança da Informação Innovery España
- Analista em Segurança da Informação Atos
- Licenciatura em Engenharia Técnica em Informática de Sistemas pela Universidade de Córdova
- Mestrado em Gestão da Segurança da Informação na Universidade Politécnica de Madrid
- ITIL v4 Foundation Certificate in IT Service Management. ITIL Certified
- IBM Security QRadar SIEM 7.1 Advanced. Avnet
- IBM Security QRadar SIEM 7.1 Foundations. Avnet

Dr. Octavio Ortega

- Especialista em Marketing e Desenvolvimento Web
- Programador de Aplicações Informáticas e Desenvolvimento Web *Freelance*
- *Chief Operating Officer* na Smallsquid SL
- Administrador e-commerce de Ortega y Serrano
- Docente em cursos de Certificado de Profissionalismo em Informática e Comunicações
- Docente de cursos de Segurança Informática
- Licenciado em Psicologia pela Universidade Aberta da Catalunha
- Técnico Superior Universitário em Análise, Design e Soluções de *Software*
- Técnico Superior Universitário em Programação Avançada

Dr. Mario Embid Ruiz

- Advogado Especialista em TIC e Proteção de Dados em Martínez-Echevarría Abogados
- Responsável legal da Branddocs SL
- Analista de Risco do Segmento PME do BBVA
- Docente em pós-graduações universitárias relacionados com Direito
- Licenciado em Direito pela Universidade Rey Juan Carlos
- Licenciado em Administração e Direção de Empresas pela Universidade Rey Juan Carlos
- Mestrado em Direito das Novas Tecnologias, Internet e Audiovisual pelo Centro de Estudos Universitários Villanueva



Dr. Juan Luis Gozalo Fernández

- Gestor de Produtos baseados em Blockchain para a Open Canarias
- Diretor Blockchain DevOps em Alastria
- Diretor de Tecnologia de Nível de Serviço no Santander Espanha
- Diretor Desenvolvimento Aplicação Móvel Tinkerlink em Cronos Telecom
- Diretor Tecnologia Gestão de Serviço IT em Barclays Bank Espanha
- Licenciatura em Engenharia Superior de Informática pela UNED
- Especialização em *Deep Learning* em DeepLearning.ai

Dra. Lorena Jurado Jabonero

- Responsável da Segurança da Informação (CISO) no Grupo Pascual
- Cybersecurity Manager na KPMG. Espanha
- Consultora de Processos TI e Controlo e Gestão de Projetos de Infraestrutura na Bankia
- Engenheira de Ferramentas Operacionais na Dalkia
- Programadora no Grupo Banco Popular
- Programadora de Aplicações pela Universidade Politécnica de Madrid
- Licenciada em Engenharia Informática pela Universidade Alfonso X El Sabio
- Engenheiro Técnico em Gestão Informática pela Universidade Politécnica de Madrid. Certified Data Privacy Solutions Engineer (CDPSE) pela ISACA

05

Estrutura e conteúdo

Este Advanced Master reúne uma série de módulos especializados que permitirão ao Profissionais aprofundar aspetos como a identificação digital, sistemas de controlo de acesso, arquitetura da segurança da informação, a estrutura da área de segurança, sistemas de gestão da segurança da informação na operação das comunicações e software ou o desenvolvimento do plano de continuidade de negócios associado à segurança. Isto dará ao cientista informático uma compreensão abrangente de todas as questões relevantes na cibersegurança atual.

Não encontrará conteúdo mais completo e inovador do que este para se especializar em gestão avançada da cibersegurança"

Módulo 1. Segurança no desenho e desenvolvimento de sistemas

1.1. Sistemas de informação
- 1.1.1. O que é um sistema de informação
- 1.1.2. Componentes de um sistema de informação
- 1.1.3. Atividades de um sistema de informação
- 1.1.4. Ciclo de vida de um sistema de informação
- 1.1.5. Recursos de um sistema de Informação

1.2. Sistemas de informação. Tipologia
- 1.2.1. Tipos dos sistemas de informação
  - 1.2.1.1. Empresarial
  - 1.2.1.2. Estratégicos
  - 1.2.1.3. De acordo com o âmbito da aplicação
  - 1.2.1.4. Específicos
- 1.2.2. Sistemas de informação. Exemplos reais
- 1.2.3. Evolução dos sistemas de informação: etapas
- 1.2.4. Metodologia dos sistemas de informação

1.3. Segurança dos sistemas de informação. Implicações legais
- 1.3.1. Acesso a dados
- 1.3.2. Ameaças de segurança: vulnerabilidades
- 1.3.3. Implicações legais: delitos
- 1.3.4. Procedimentos de manutenção de um sistema de informação

1.4. Segurança de um sistemas de informação. Protocolos de segurança
- 1.4.1. Segurança de um sistema de informação
  - 1.4.1.1. Integração
  - 1.4.1.2. Confidencialidade
  - 1.4.1.3. Disponibilidade
  - 1.4.1.4. Autenticação
- 1.4.2. Serviços de segurança
- 1.4.3. Protocolos de segurança da informação. Tipologia
- 1.4.4. Sensibilidade de um sistema de informação

1.5. Segurança num sistemas de informação. Medidas e sistemas de controlo de acesso
- 1.5.1. Medidas de segurança
- 1.5.2. Tipos de medidas de segurança
  - 1.5.2.1. Prevenção
  - 1.5.2.2. Deteção
  - 1.5.2.3. Correção
- 1.5.3. Sistema de controlo de acesso. Tipologia
- 1.5.4. Criptografia

1.6. Segurança em redes e internet
- 1.6.1. Firewalls
- 1.6.2. Identificação digital
- 1.6.3. Vírus e worms
- 1.6.4. *Hacking*
- 1.6.5. Exemplos e casos reais

1.7. Crimes informáticos
- 1.7.1. Crime informático
- 1.7.2. Crimes informáticos. Tipologia
- 1.7.3. Crime informático Ataque Tipologias
- 1.7.4. O caso da Realidade Virtual
- 1.7.5. Perfis de delinquentes e vítimas Tipificação do crime
- 1.7.6. Crimes informáticos. Exemplos e casos reais

1.8. Plano de segurança num sistemas de informação
- 1.8.1. Planio de segurança. Objetivos
- 1.8.2. Planio de segurança. Planeamento
- 1.8.3. Plano de riscos Análise
- 1.8.4. Políticas de segurança. Implementação na organização
- 1.8.5. Planio de segurança. Implementação na organização
- 1.8.6. Procedimentos de segurança Tipos
- 1.8.7. Planos de segurança. Exemplos

1.9. Plano de contingência
- 1.9.1. Plano de contingência. Funções
- 1.9.2. Plano de Emergência: Elementos e objetivos
- 1.9.3. Plano de contingência na organização. Implementação
- 1.9.4. Planos de contingência. Exemplos

1.10. Governação da segurança dos sistemas de informação
- 1.10.1. Normativa legal
- 1.10.2. Padrões
- 1.10.3. Certificações
- 1.10.4. Tecnologias

Módulo 2. Arquiteturas e modelos de segurança da informação

2.1. Arquitetura de segurança da informação
- 2.1.1. SGSI/PDS
- 2.1.2. Alienação estratégica
- 2.1.3. Gestão do risco
- 2.1.4. Medição de desempenho

2.2. Modelos de segurança da informação
- 2.2.1. Baseados em políticas de segurança
- 2.2.2. Baseados em ferramentas de proteção
- 2.2.3. Baseados em equipas de trabalho

2.3. Modelo de segurança Componentes chave
- 2.3.1. Identificação de riscos
- 2.3.2. Definição de controlos
- 2.3.3. Avaliação contínua de níveis de risco
- 2.3.4. Plano de sensibilização de funcionários, fornecedores, sócios, etc.

2.4. Processo de gestão de riscos
- 2.4.1. Identificação de ativos
- 2.4.2. Identificação de ameaças
- 2.4.3. Avaliação dos riscos
- 2.4.4. Priorização de controlos
- 2.4.5. Reavaliação e risco residual

2.5. Processos de negócio e segurança da informação
- 2.5.1. Processos empresariais
- 2.5.2. Avaliação de risco com base em parâmetros de negócio
- 2.5.3. Análise do impacto no negócio
- 2.5.4. As operações de negócio e a segurança da informação

2.6. Processo de melhoria contínua
- 2.6.1. O ciclo de Deming
  - 2.6.1.1. Planificar
  - 2.6.1.2. Fazer
  - 2.6.1.3. Verificar
  - 2.6.1.4. Agir

2.7. Arquiteturas de segurança
- 2.7.1. Seleção e homogeneização de tecnologias
- 2.7.2. Gestão de identidades. Autenticação
- 2.7.3. Gestão de acessos Autorização
- 2.7.4. Segurança de infraestrutura de rede
- 2.7.5. Tecnologias e soluções de encriptação
- 2.7.6. Segurança de Equipas Terminais (EDR)

2.8. O quadro normativo
- 2.8.1. Normativas setoriais
- 2.8.2. Certificações
- 2.8.3. Legislações

2.9. A Norma ISO 27001
- 2.9.1. Implementação
- 2.9.2. Certificação
- 2.9.3. Auditorias e testes de intrusão
- 2.9.4. Gestão contínua do risco
- 2.9.5. Classificação da informação

2.10. Legislação sobre privacidade RGPD (GDPR)
- 2.10.1. Alcance do Regulamento Geral de Proteção de Dados (RGPD)
- 2.10.2. Dados pessoais
- 2.10.3. Papéis no tratamento de dados pessoais
- 2.10.4. Direitos ARCO
- 2.10.5. O DPO. Funções

Módulo 3. Gestão da Segurança IT

3.1. Gestão da segurança
- 3.1.1. Operações de segurança
- 3.1.2. Aspeto legal e regulamentar
- 3.1.3. Habilitação do negócio
- 3.1.4. Gestão de risco
- 3.1.5. Gestão de identidades e acessos

3.2. Estrutura da área de segurança O escritório do CISO
- 3.2.1. Estrutura organizativa. Posição do CISO na estrutura
- 3.2.2. As linhas de defesa
- 3.2.3. Organigrama do escritório do CISO
- 3.2.4. Gestão orçamental

3.3. Governo de segurança
- 3.3.1. Comité de segurança
- 3.3.2. Comité de monitorização de riscos
- 3.3.3. Comité de auditoria
- 3.3.4. Comité de crise

3.4. Governo de segurança. Funções
- 3.4.1. Políticas e normas
- 3.4.2. Plano Diretor de segurança
- 3.4.3. Painel de instrumentos
- 3.4.4. Sensibilização e formação
- 3.4.5. Segurança na cadeia de abastecimento

3.5. Operações de segurança
- 3.5.1. Gestão de identidades e acessos
- 3.5.2. Configuração de regras de segurança de rede. *Firewalls*
- 3.5.3. Gestão de plataformas IDS/IPS
- 3.5.4. Análise de vulnerabilidades

3.6. Quadro de trabalho de Cibersegurança NIST CSF
- 3.6.1. Metodologia NIST
  - 3.6.1.1. Identificar
  - 3.6.1.2. Proteger
  - 3.6.1.3. Detetar
  - 3.6.1.4. Responder
  - 3.6.1.5. Recuperar

3.7. Centro de Operações de Segurança (SOC) Funções
- 3.7.1. Proteção *Red Team, Pentesting, Threat Intelligence*
- 3.7.2. Deteção SIEM, *User Behavior Analytics, Fraud Prevention*
- 3.7.3. Resposta

3.8. Auditoria de segurança
- 3.8.1. Teste de intrusão
- 3.8.2. Exercícios *red team*
- 3.8.3. Auditorias de código fonte Programação segura
- 3.8.4. Segurança de componentes (*Software Supply Chain*)
- 3.8.5. Análise forense

3.9. Resposta a incidentes
- 3.9.1. Preparação
- 3.9.2. Deteção, análise e notificação
- 3.9.3. Contenção, erradicação e recuperação
- 3.9.4. Atividades pós-incidente
  - 3.9.4.1. Retenção de evidências
  - 3.9.4.2. Análise forense
  - 3.9.4.3. Gestão de brechas
- 3.9.5. Guias oficiais de gestão de ciberincidentes

3.10. Gestão de vulnerabilidades
- 3.10.1. Análise de vulnerabilidades
- 3.10.2. Avaliação de vulnerabilidade
- 3.10.3. Base de sistemas
- 3.10.4. Vulnerabilidade de dia 0. *Zero-Day*

Módulo 4. Análise de riscos e ambiente de segurança IT

4.1. Análise do ambiente
- 4.1.1. Análise da situação conjuntural
  - 4.1.1.1. Ambientes VUCA
    - 4.1.1.1.1. Volátil
    - 4.1.1.1.2. Incerto
    - 4.1.1.1.3. Complexo
    - 4.1.1.1.4. Ambíguo
  - 4.1.1.2. Ambientes BANI
    - 4.1.1.2.1. Frágil
    - 4.1.1.2.2. Ansioso
    - 4.1.1.2.3. Não linear
    - 4.1.1.2.4. Incompreensível
- 4.1.2. Análise do ambiente geral. PESTEL
  - 4.1.2.1. Político
  - 4.1.2.2. Económico
  - 4.1.2.3. Social
  - 4.1.2.4. Tecnológico
  - 4.1.2.5. Ecológico/Ambiental
  - 4.1.2.6. Legal
- 4.1.3. Análise da situação interna. SWOT
  - 4.1.3.1. Objetivos
  - 4.1.3.2. Ameaças
  - 4.1.3.3. Oportunidades
  - 4.1.3.4. Pontos fortes

4.2. Riscos e incerteza
- 4.2.1. Risco
- 4.2.2. Gestão de riscos
- 4.2.3. Normas de gestão de riscos

4.3. Diretrizes para a gestão de riscos ISO 31.000:2018
- 4.3.1. Objeto
- 4.3.2. Princípios
- 4.3.3. Quadro de referência
- 4.3.4. Processo

4.4. Metodologia de Análise e Gestão de Riscos dos Sistemas de Informação (MAGERIT)
- 4.4.1. Metodologia MAGERIT
  - 4.4.1.1. Objetivos
  - 4.4.1.2. Método
  - 4.4.1.3. Elementos
  - 4.4.1.4. Técnicas
  - 4.4.1.5. Ferramentas disponíveis

4.5. Transferência do risco cibernético
- 4.5.1. Transferência de riscos
- 4.5.2. Riscos cibernéticos Tipologia
- 4.5.3. Seguros de riscos cibernéticos

4.6. Metodologias ágeis para a gestão de riscos
- 4.6.1. Metodologias ágeis
- 4.6.2. Scrum para a gestão do risco
- 4.6.3. *Agile Risk Management*

4.7. Tecnologias para a gestão do risco
- 4.7.1. Inteligência artificial aplicada à gestão de riscos
- 4.7.2. *Blockchain* e criptografia. Metódos de preservação do valor
- 4.7.3. Computação quântica Oportunidade ou ameaça

4.8. Elaboração de mapas de riscos informáticos baseados em metodologias ágeis
- 4.8.1. Representação da probabilidade e impacto em ambientes ágeis
- 4.8.2. O risco como ameaça do valor
- 4.8.3. Re-evolução na gestão de projetos e processos ágeis baseados em KRIs

4.9. *Risk Driven* na gestão de riscos
- 4.9.1. *Risk Driven*
- 4.9.2. *Risk Driven* na gestão de riscos
- 4.9.3. Desenvolvimento de um modelo de gestão empresarial impulsionado pelo risco

4.10. Inovação e transformação digital na gestão de risco informáticos
- 4.10.1. A gestão de riscos ágeis como fonte de inovação empresarial
- 4.10.2. Transformação de dados em informação útil para a tomada de decisões
- 4.10.3. Visão holística da empresa através do risco

Módulo 5. Criptografia em IT

5.1. Criptografia
- 5.1.1. Criptografia
- 5.1.2. Fundamentos matemáticos

5.2. Criptologia
- 5.2.1. Criptologia
- 5.2.2. Criptoanálise
- 5.2.3. Criptoanálise

5.3. Protocolos criptográficos
- 5.3.1. Blocos básicos
- 5.3.2. Protocolos básicos
- 5.3.3. Protocolos intermédios
- 5.3.4. Protocolos avançados
- 5.3.5. Protocolos esotéricos

5.4. Técnicas criptográficas
- 5.4.1. Longitude de chaves
- 5.4.2. Gestão de chaves
- 5.4.3. Tipos de algoritmos
- 5.4.4. Funções resumo. *Hash*
- 5.4.5. Geradores de números pseudoaleatórios
- 5.4.6. Uso de algoritmos

5.5. Criptografia simétrica
- 5.5.1. Cifras de bloco
- 5.5.2. DES (*Data Encryption Standard*)
- 5.5.3. Algoritmo RC4
- 5.5.4. AES (*Advanced Encryption Standard*)
- 5.5.5. Combinação de cifras de bloco
- 5.5.6. Derivação de chaves

5.6. Criptografia assimétrica
- 5.6.1. Diffie-Hellman
- 5.6.2. DSA (*Digital Signature Algorithm*)
- 5.6.3. RSA (Rivest, Shamir e Adleman)
- 5.6.4. Curva elíptica
- 5.6.5. Criptografia assimétrica Tipologia

5.7. Certificados digitais
- 5.7.1. Assinatura digital
- 5.7.2. Certificados X509
- 5.7.3. Infraestrutura de chave pública (PKI)

5.8. Implementações
- 5.8.1. Kerberos
- 5.8.2. IBM CCA
- 5.8.3. *Pretty Good Privacy* (PGP)
- 5.8.4. ISO *Authentication Framework*
- 5.8.5. SSL e TLS
- 5.8.6. Cartões inteligentes em meios de pagamento (EMV)
- 5.8.7. Protocolos de telefonia móvel
- 5.8.8. *Blockchain*

5.9. Esteganografia
- 5.9.1. Esteganografia
- 5.9.2. Estegoanálise
- 5.9.3. Aplicações e usos

5.10. Criptografia quântica
- 5.10.1. Algoritmos quânticos
- 5.10.2. Proteção de algoritmos frente à computação quântica
- 5.10.3. Distribuição de chave quântica

Módulo 6. Gestão de identidade e acessos em segurança IT

6.1. Gestão de identidade e acessos (IAM)
- 6.1.1. Identidade digital
- 6.1.2. Gestão de identidade
- 6.1.3. Federação de identidades

6.2. Controlo de acesso físico
- 6.2.1. Sistemas de proteção
- 6.2.2. Segurança das áreas
- 6.2.3. Instalações de recuperação

6.3. Controlo de acesso lógico
- 6.3.1. Autenticação: tipologia
- 6.3.2. Protocolos de autenticação
- 6.3.3. Ataques de autenticação

6.4. Controlo de acesso lógico. Autenticação MFA
- 6.4.1. Controlo de acesso lógico. Autenticação MFA
- 6.4.2. Palavras-passe Importância
- 6.4.3. Ataques de autenticação

6.5. Controlo de acesso lógico. Autenticação biométrica
- 6.5.1. Controlo de acesso lógico. Autenticação biométrica
  - 6.5.1.1. Autenticação biométrica Requisitos
- 6.5.2. Funcionamento
- 6.5.3. Modelo e técnicas

6.6. Sistemas de gestão de autenticação
- 6.6.1. *Single Sign On*
- 6.6.2. Kerberos
- 6.6.3. Sistemas AAA

6.7. Sistemas de gestão de autenticação: Sistemas AAA
- 6.7.1. TACACS
- 6.7.2. RADIUS
- 6.7.3. DIAMETER

6.8. Serviços de controlo de acesso
- 6.8.1. FW - Firewall
- 6.8.2. VPN - Redes Privadas Virtuais
- 6.8.3. IDS - Sistema de Deteção de Intrusões

6.9. Sistema de controlo de acesso à rede
- 6.9.1. NAC
- 6.9.2. Arquitetura e elementos
- 6.9.3. Funcionamento e normalização

6.10. Acesso a redes sem fios
- 6.10.1. Tipos de redes sem fios
- 6.10.2. Segurança em redes sem fios
- 6.10.3. Ataques em redes sem fios

Módulo 7. Segurança em comunicações e operação software

7.1. Segurança informática em comunicações e operação software
- 7.1.1. Segurança Informática
- 7.1.2. Cibersegurança
- 7.1.3. Segurança na nuvem

7.2. Segurança informática em comunicações e operação software. Tipologia
- 7.2.1. Segurança física
- 7.2.2. Segurança lógica

7.3. Segurança em comunicações
- 7.3.1. Principais elementos
- 7.3.2. Segurança de redes
- 7.3.3. Melhores práticas

7.4. Ciberinteligência
- 7.4.1. Engenharia social
- 7.4.2. *Deep Web*
- 7.4.3. *Phishing*
- 7.4.4. *Malware*

7.5. Desenvolvimento seguro em comunicações e operação software
- 7.5.1. Desenvolvimento seguro. Protocolo HTTP
- 7.5.2. Desenvolvimento seguro. Ciclo de vida
- 7.5.3. Desenvolvimento seguro. Segurança PHP
- 7.5.4. Desenvolvimento seguro. Segurança NET
- 7.5.5. Desenvolvimento seguro. Melhores práticas

7.6. Sistemas de gestão de segurança da informação em comunicações e operação software
- 7.6.1. GDPR
- 7.6.2. ISO 27021
- 7.6.3. ISO 27017/ 18

7.7. Tecnologias SIEM
- 7.7.1. Tecnologias SIEM
- 7.7.2. Operativa de SOC
- 7.7.3. SIEM *Vendors*

7.8. A função da segurança nas organizações
- 7.8.1. Funções nas organizações
- 7.8.2. Função dos especialistas IoT nas empresas
- 7.8.3. Certificações reconhecidas no mercado

7.9. Análise forense
- 7.9.1. Análise forense
- 7.9.2. Análise forense. Metodologia
- 7.9.3. Análise forense. Ferramentas e implantação

7.10. A cibersegurança na atualidade
- 7.10.1. Principais ataques informáticos
- 7.10.2. Previsões de empregabilidade
- 7.10.3. Desafios

Módulo 8. Segurança em ambientes Cloud

8.1. Segurança em ambientes *Cloud Computing*
- 8.1.1. Segurança em ambientes *Cloud Computing*
- 8.1.2. Segurança em ambientes *Cloud Computing* Ameaças e riscos segurança
- 8.1.3. Segurança em ambientes *Cloud Computing* Aspetos chave de segurança

8.2. Tipos de infraestrutura *Cloud*
- 8.2.1. Público
- 8.2.2. Privado
- 8.2.3. Híbrido

8.3. Modelo de gestão partilhada
- 8.3.1. Elementos de segurança geridos por fornecedor
- 8.3.2. Elementos geridos por cliente
- 8.3.3. Definição da estratégia para a segurança

8.4. Mecanismos de prevenção
- 8.4.1. Sistemas de gestão de autenticação
- 8.4.2. Sistema de gestão de autorização: políticas de acesso
- 8.4.3. Sistemas de gestão de chaves

8.5. Securitização de sistemas
- 8.5.1. Securitização dos sistemas de armazenamento
- 8.5.2. Proteção dos sistemas de base de dados
- 8.5.3. Securitização de dados em trânsito

8.6. Proteção de infraestrutura
- 8.6.1. Desenho e implementação de rede segura
- 8.6.2. Segurança de recursos de computação
- 8.6.3. Ferramentas e recursos para proteção de infraestrutura

8.7. Deteção as ameaças e ataques
- 8.7.1. Sistemas de auditoria, *Logging* e monitorização
- 8.7.2. Sistemas de eventos e alarmes
- 8.7.3. Sistemas SIEM

8.8. Resposta a incidentes
- 8.8.1. Plano de resposta a incidentes
- 8.8.2. A continuidade do negócio
- 8.8.3. Análise forense e remediação de incidentes da mesma natureza

8.9. Segurança em *Clouds* públicas
- 8.9.1. AWS (Amazon Web Services)
- 8.9.2. Microsoft Azure
- 8.9.3. Google GCP
- 8.9.4. Oracle Cloud

8.10. Normativa e cumprimento
- 8.10.1. Cumprimento de normativas de segurança
- 8.10.2. Gestão de risco
- 8.10.3. Pessoas e processo nas organizações

Módulo 9. Segurança em comunicações de dispositivos Iot

9.1. Da telemetria à IoT
- 9.1.1. Telemetria
- 9.1.2. Conetividade M2M
- 9.1.3. Democratização da telemetria

9.2. Modelos de referência IoT
- 9.2.1. Modelos de referência IoT
- 9.2.2. Arquitetura simplificada IoT

9.3. Vulnerabilidade de segurança da IoT
- 9.3.1. Dispositivos IoT
- 9.3.2. Dispositivos IoT. Estudos de casos de utilização
- 9.3.3. Dispositivos IoT. Vulnerabilidades

9.4. Conetividade da IoT
- 9.4.1. Redes PAN, LAN, WAN
- 9.4.2. Tecnologias sem fios na IoT
- 9.4.3. Tecnologias sem fios na LPWAN

9.5. Tecnologias LPWAN
- 9.5.1. O triângulo de ferro das LPWAN
- 9.5.2. Bandas de frequência livre vs. Bandas licenciadas
- 9.5.3. Opções de tecnologias LPWAN

9.6. Tecnologia LoRaWAN
- 9.6.1. Tecnologia LoRaWAN
- 9.6.2. Casos de utilização LoRaWAN Ecossistema
- 9.6.3. Segurança em LoRaWAN

9.7. Tecnologia Sigfox
- 9.7.1. Tecnologia Sigfox
- 9.7.2. Casos de utilização Sigfox. Ecossistema
- 9.7.3. Segurança em Sigfox

9.8. Tecnologia Celular IoT
- 9.8.1. Tecnologia Celular IoT (NB-IoT e LTE-M)
- 9.8.2. Casos de utilização Celular IoT Ecossistema
- 9.8.3. Segurança em Celular IoT

9.9. Tecnologia WiSUN
- 9.9.1. Tecnologia WiSUN
- 9.9.2. Casos de utilização WiSUN. Ecossistema
- 9.9.3. Segurança em WiSUN

9.10. Outras tecnologias IoT
- 9.10.1. Outras tecnologias IoT
- 9.10.2. Casos de utilização e ecossistema de outras tecnologias IoT
- 9.10.3. Segurança em outras tecnologias IoT

Módulo 10. Plano de continuidade do negócio associado à segurança

10.1. Planos de Continuidade de Negócio
- 10.1.1. Os Planos de Continuidade de Negócio (PCN)
- 10.1.2. Plano de Continuidade de Negócio (PCN). Questões-chave
- 10.1.3. Plano de Continuidade de Negócio (PCN) para a avaliação da empresa

10.2. Métricas num Plano de Continuidade de Negócio (PCN)
- 10.2.1. *Recovery Time Objective* (RTO) e *Recovery Point Objective* (RPO)
- 10.2.2. Tempo Máximo Tolerável (MTD)
- 10.2.3. Níveis Mínimos de Recuperação (ROL)
- 10.2.4. Ponto de Recuperação Objetivo (RPO)

10.3. Projetos de continuidade. Tipologia
- 10.3.1. Plano de Continuidade de Negócio (PCN)
- 10.3.2. Plano de continuidade de TIC (PCTIC)
- 10.3.3. Plano de recuperação em caso de desastres (PRD)

10.4. Gestão de riscos associada ao PCN
- 10.4.1. Análise de impacto no negócio
- 10.4.2. Benefícios da implementação de um PCN
- 10.4.3. Mentalidade baseada em riscos

10.5. Ciclo de vida de um plano de continuidade de negócio
- 10.5.1. Fase 1: Análise da Organização
- 10.5.2. Fase 2: Determinação da estratégia de continuidade
- 10.5.3. Fase 3: Resposta à contingência
- 10.5.4. Fase 4: Prova, manutenção e revisão

10.6. Fase de análise análise da organização de um PCN
- 10.6.1. Identificação de processos no âmbito do PCN
- 10.6.2. Identificação de áreas críticas do negócio
- 10.6.3. Identificação de dependências entre áreas e processos
- 10.6.4. Determinação do MTD adequado
- 10.6.5. Documentos a entregar Criação de um plano

10.7. Fase de determinação da estratégia de continuidade num PCN
- 10.7.1. Funções na fase de determinação da estratégia
- 10.7.2. Tarefas da fase de determinação da estratégia
- 10.7.3. Resultados

10.8. Fase de resposta à contingência num PCN
- 10.8.1. Funções na fase de resposta
- 10.8.2. Tarefas nesta fase
- 10.8.3. Resultados

10.9. Fase de testes, manutenção e revisão de um PCN
- 10.9.1. Funções na fase de testes, manutenção e revisão
- 10.9.2. Tarefas na fase de testes, manutenção e revisão
- 10.9.3. Resultados

10.10. Normas ISO associadas aos Planos de Continuidade de Negócio (PCN)
- 10.10.1. ISO 22301:2019
- 10.10.2. ISO 22313:2020
- 10.10.3. Outras normas ISO e internacionais relacionadas

Módulo 11. Liderança Ética e Responsabilidade Social das Empresa

11.1. Globalização e Governança
- 11.1.1. Governança e Governo Corporativo
- 11.1.2. Fundamentos do Governo Corporativo nas empresas
- 11.1.3. O Papel do Conselho de Administração no painel do Governo Corporativo

11.2. Liderança
- 11.2.1. Liderança Uma abordagem conceptual
- 11.2.2. Liderança nas empresas
- 11.2.3. A importância do Líder na gestão de empresas

11.3. *Cross Cultural Management*
- 11.3.1. Concceito de *Cross Cultural Management*.
- 11.3.2. Contribuições para o Conhecimento das Culturas Nacionais
- 11.3.3. Gestão da Diversidade

11.4. Desenvolvimento executivo e liderança
- 11.4.1. Conceito de Desenvolvimento Executivo
- 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 nos dias de hoje

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 das Empresas

11.8. Sistemas e ferramentas de Gestão responsável
- 11.8.1. RSE: Responsabilidade social empresarial
- 11.8.2. Aspetos essenciais para a aplicação de uma estratégia de gestão responsável
- 11.8.3. Passos para a implementação de um sistema de gestão da responsabilidade social das empresas
- 11.8.4. Ferramentas e Padrões da RSE

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 as multinacionais no domínio dos direitos humanos

11.10. Meio legal e *Corporate Governance*
- 11.10.1. Normas 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. Direção Estratégica de pessoas
- 12.1.1. Direção Estratégica e recursos humanos
- 12.1.2. Gestão estratégica de pessoas

12.2. Gestão de recursos humanos baseada na competência
- 12.2.1. Análise do potencial
- 12.2.2. Política de remuneração
- 12.2.3. Planeamento de carreira/sucessão

12.3. Avaliação da produtividade e gestão do desempenho
- 12.3.1. Gestão de desempenho
- 12.3.2. Gestão do desempenho: objetivos e processo

12.4. Inovação na gestão de talentos e pessoas
- 12.4.1. Modelos estratégicos de gestão de talentos
- 12.4.2. Identificação, formação e desenvolvimento de talentos
- 12.4.3. Fidelização e retenção
- 12.4.4. Proatividade e inovação

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

12.6. Desenvolvimento de equipas de alto desempenho
- 12.6.1. Equipas de elevado desempenho: equipas autogeridas
- 12.6.2. Metodologias para a gestão de equipas autogeridas de alto desempenho

12.7. Gestão da mudança
- 12.7.1. Gestão da mudança
- 12.7.2. Desenvolvimento de sistemas de gestão de mudança
- 12.7.3. Etapas ou fases da gestão da mudança

12.8. Negociação e gestão de conflitos
- 12.8.1 Negociação
- 12.8.2 Gestão de conflitos
- 12.8.2 Gestão de Crise

12.9. Comunicação executiva
- 12.9.1. Comunicação interna e externa no ambiente empresarial
- 12.9.2. Departamentos de Comunicação
- 12.9.3. A pessoa responsável pela comunicação da empresa. O perfil do DirCom

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

Módulo 13. Gestão Económica-financeira

13.1. Enquadramento Económico
- 13.1.1. Enquadramento macroeconómico 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 Diretiva
- 13.2.1. Conceitos básicos
- 13.2.2. O Ativo da empresa
- 13.2.3. O Passivo da empresa
- 13.2.4. O Património Liquido da empresa
- 13.2.5. A Declaração de Rendimentos

13.3. Sistemas de Informação e ***Business Intelligence***
- 13.3.1. Fundamentos e classificação
- 13.3.2. Fases e métodos de repartição de custos
- 13.3.3. Escolha do centro de custos e efeito

13.4. Orçamento e Controlo de Gestão
- 13.4.1. O modelo orçamental
- 13.4.2. O Orçamento de Capital
- 13.4.3. O Orçamento Operacional
- 13.4.5. Orçamento de Tesouraria
- 13.4.6. Controlo orçamental

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 da gestão financeira

13.6. Planeamento Financeiro
- 13.6.1. Definição de planeamento financeiro
- 13.6.2. Ações a realizar no planeamento financeiro
- 13.6.3. Criação e estabelecimento da estratégia empresarial
- 13.6.4. O quadro *Cash Flow*
- 13.6.5. O quadro do ativo circulante

13.7. Estratégia Financeira Empresarial
- 13.7.1. Estratégia empresarial e fontes de financiamento
- 13.7.2. Produtos financeiros para empresas

13.8. Financiamento Estratégico
- 13.8.1. Autofinanciamento
- 13.8.2. Aumento dos fundos próprios
- 13.8.3. Recursos híbridos
- 13.8.4. Financiamento através de intermediários

13.9. Análise e planeamento financeiro
- 13.9.1. Análise de Balanços
- 13.9.2. Análise da Conta de Resultados
- 13.9.3. Análise da Rentabilidade

13.10. Análise e resolução de casos/problemas
- 13.10.1. Informações financeiras sobre a Industria de Design y Textil, S.A. (INDITEX)

Módulo 14. Gestão comercial e marketing estratégico

14.1. Gestão comercial
- 14.1.1. Quadro conceitual da Gestão comercial
- 14.1.2. Estratégia e planeamento empresarial
- 14.1.3. O papel dos diretores comerciais

14.2. Marketing
- 14.2.1. Conceito de Marketing
- 14.2.2. Elementos básicos do marketing
- 14.2.3. Atividades de marketing na empresa

14.3. Gestão Estratégica de Marketing
- 14.3.1. Conceito de Marketing Estratégico
- 14.3.2. Conceito de Planeamento Estratégico de Marketing
- 14.3.3. Etapas do processo de Planeamento Estratégico de Marketing

14.4. Marketing digital e comércio eletrónico
- 14.4.1. Objetivos do Marketing digital e comércio eletrónico
- 14.4.2. Marketing digital e meios utilizados
- 14.4.3. Comércio eletrónico. Contexto geral
- 14.4.4. Categorias do comércio eletrónico
- 14.4.5. Vantagens e desvantagens do *Ecommerce* versus o comércio tradicional

14.5. Marketing Digital para reforçar 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 envolvimento através da Internet
- 14.6.2. *Visitor Relationship Management*
- 14.6.3. Hipersegmentação

14.7. Gestão 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 nas campanhas de publicidade digital

14.8. Estratégia de vendas
- 14.8.1. Estratégia de vendas
- 14.8.2. Métodos de vendas

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

14.10. Comunicação e reputação digital
- 14.10.1. A 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. *Management* Executivo

15.1. General Management
- 15.1.1. Conceito de General Management
- 15.1.2. A ação do Diretor Geral
- 15.1.3. O Diretor Geral e as suas funções
- 15.1.4. Transformação do trabalho da Direção

15.2. O gestor e as suas funções A cultura organizacional e as suas abordagens
- 15.2.1. O gestor e as suas funções A cultura organizacional e as suas abordagens

15.3. Gestão de operações
- 15.3.1. Importância da direção
- 15.3.2. A cadeia de valor
- 15.3.3. Gestão de qualidade

15.4. Oratória e capacitação de porta-voz
- 15.4.1. Comunicação interpessoal
- 15.4.2. Capacidade de comunicação e influência
- 15.4.3. Barreiras na comunicação

15.5. Ferramentas de comunicação pessoais e organizacionais
- 15.5.1. A comunicação interpessoal
- 15.5.2. Ferramentas da comunicação interpessoal
- 15.5.3. A comunicação nas organizações
- 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: conteúdos e momentos

15.7. Preparação de um plano de crise
- 15.7.1. Análise de potenciais problemas
- 15.7.2. Planeamento
- 15.7.3. Adequação do 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* Pessoal
- 15.9.1. Estratégias para desenvolver a marca pessoal
- 15.9.2. Leis do branding pessoal
- 15.9.3. Ferramentas da construção de marcas pessoais

15.10. Liderança e gestão de equipas
- 15.10.1. Liderança e estilos de liderança
- 15.10.2. Capacidades e desafios do Líder
- 15.10.3. Gestão de Processos de Mudança
- 15.10.4. Gestão de Equipas Multiculturais

O melhor corpo docente e o sistema de ensino inovador combinam-se com o programa de estudos mais completo e atualizado: tem uma grande oportunidade de progredir como informático"

06

Metodologia de estudo

A TECH é a primeira universidade do mundo a unir a metodologia dos ***case studies*** com o ***Relearning***, um sistema de aprendizado 100% online baseado na repetição guiada.

Essa estratégia de ensino inovadora foi projetada para oferecer aos profissionais a oportunidade de atualizar conhecimentos e desenvolver habilidades de forma intensiva e rigorosa. Um modelo de aprendizagem que coloca o aluno no centro do processo acadêmico e lhe dá o papel principal, adaptando-se às suas necessidades e deixando de lado as metodologias mais convencionais.

A TECH prepara você para enfrentar novos desafios em ambientes incertos e alcançar o sucesso em sua carreira"

O aluno: a prioridade de todos os programas da TECH

Na metodologia de estudo da TECH, o aluno é o protagonista absoluto. As ferramentas pedagógicas de cada programa foram selecionadas levando-se em conta as demandas de tempo, disponibilidade e rigor acadêmico que, atualmente, os alunos, bem como os empregos mais competitivos do mercado, exigem.

Com o modelo educacional assíncrono da TECH, é o aluno quem escolhe quanto tempo passa estudando, como decide estabelecer suas rotinas e tudo isso no conforto do dispositivo eletrônico de sua escolha. O aluno não precisa assistir às aulas presenciais, que muitas vezes não poderá comparecer. As atividades de aprendizado serão realizadas de acordo com sua conveniência. O aluno sempre poderá decidir quando e de onde estudar.

> *Na TECH, o aluno NÃO terá aulas ao vivo (das quais poderá nunca participar)".*

Os programas de ensino mais abrangentes do mundo

A TECH se caracteriza por oferecer os programas acadêmicos mais completos no ambiente universitário. Essa abrangência é obtida por meio da criação de programas de estudo que cobrem não apenas o conhecimento essencial, mas também as últimas inovações em cada área.

Por serem constantemente atualizados, esses programas permitem que os alunos acompanhem as mudanças do mercado e adquiram as habilidades mais valorizadas pelos empregadores. Dessa forma, os alunos da TECH recebem uma preparação abrangente que lhes dá uma vantagem competitiva significativa para avançar em suas carreiras.

Além disso, eles podem fazer isso de qualquer dispositivo, PC, tablet ou smartphone.

> *O modelo da TECH é assíncrono, portanto, você poderá estudar com seu PC, tablet ou smartphone onde quiser, quando quiser e pelo tempo que quiser"*

Case studies ou Método de caso

O método de casos tem sido o sistema de aprendizado mais amplamente utilizado pelas melhores escolas de negócios do mundo. Desenvolvido em 1912 para que os estudantes de direito não aprendessem a lei apenas com base no conteúdo teórico, sua função também era apresentar a eles situações complexas da vida real. Assim, eles poderiam tomar decisões informadas e fazer julgamentos de valor sobre como resolvê-los. Em 1924 foi estabelecido como o método de ensino padrão em Harvard.

Com esse modelo de ensino, é o próprio aluno que desenvolve sua competência profissional por meio de estratégias como o *Learning by doing* ou o *Design Thinking*, usados por outras instituições renomadas, como Yale ou Stanford.

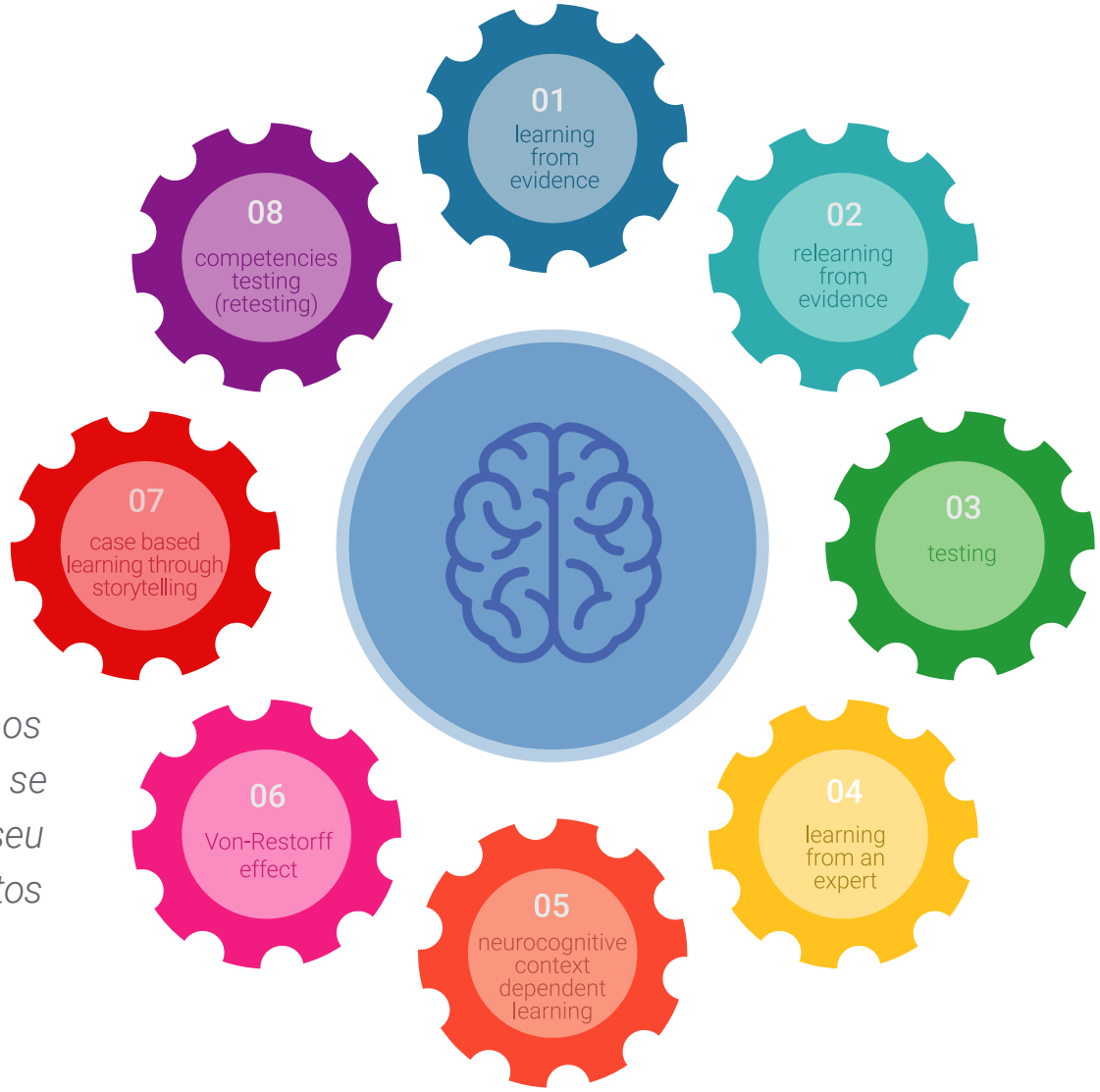
Esse método orientado para a ação será aplicado em toda a trajetória acadêmica do aluno com a TECH. Dessa forma, o aluno será confrontado com várias situações da vida real e terá de integrar conhecimentos, pesquisar, argumentar e defender suas ideias e decisões. A premissa era responder à pergunta sobre como eles agiriam diante de eventos específicos de complexidade em seu trabalho diário.

Método *Relearning*

Na TECH os *case studies* são alimentados pelo melhor método de ensino 100% online: o *Relearning*.

Esse método rompe com as técnicas tradicionais de ensino para colocar o aluno no centro da equação, fornecendo o melhor conteúdo em diferentes formatos. Dessa forma, consegue revisar e reiterar os principais conceitos de cada matéria e aprender a aplicá-los em um ambiente real.

Na mesma linha, e de acordo com várias pesquisas científicas, a repetição é a melhor maneira de aprender. Portanto, a TECH oferece entre 8 e 16 repetições de cada conceito-chave dentro da mesma lição, apresentadas de uma forma diferente, a fim de garantir que o conhecimento seja totalmente incorporado durante o processo de estudo.



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

Um Campus Virtual 100% online com os melhores recursos didáticos

Para aplicar sua metodologia de forma eficaz, a TECH se concentra em fornecer aos alunos materiais didáticos em diferentes formatos: textos, vídeos interativos, ilustrações e mapas de conhecimento, entre outros. Todos eles são projetados por professores qualificados que concentram seu trabalho na combinação de casos reais com a resolução de situações complexas por meio de simulação, o estudo de contextos aplicados a cada carreira profissional e o aprendizado baseado na repetição, por meio de áudios, apresentações, animações, imagens etc.

As evidências científicas mais recentes no campo da neurociência apontam para importância de levar em conta o local e o contexto em que o conteúdo é acessado antes de iniciar um novo processo de aprendizagem. A capacidade de ajustar essas variáveis de forma personalizada ajuda as pessoas a lembrar e armazenar o conhecimento no hipocampo para retenção a longo prazo. Trata-se de um modelo chamado *Neurocognitive context-dependent e-learning* que é aplicado conscientemente nesse curso universitário.

Por outro lado, também para favorecer ao máximo o contato entre mentor e mentorado, é oferecida uma ampla variedade de possibilidades de comunicação, tanto em tempo real quanto em diferido (mensagens internas, fóruns de discussão, serviço telefônico, contato por e-mail com a secretaria técnica, bate-papo, videoconferência etc.).

Da mesma forma, esse Campus Virtual muito completo permitirá que os alunos da TECH organizem seus horários de estudo de acordo com sua disponibilidade pessoal ou obrigações de trabalho. Dessa forma, eles terão um controle global dos conteúdos acadêmicos e de suas ferramentas didáticas, em função de sua atualização profissional acelerada.

> *O modo de estudo online deste programa permitirá que você organize seu tempo e ritmo de aprendizado, adaptando-o à sua agenda"*

A eficácia do método é justificada por quatro conquistas fundamentais:

1. Os alunos que seguem este método não só assimilam os conceitos, mas também desenvolvem a capacidade intelectual através de exercícios de avaliação de situações reais e de aplicação de conhecimentos.
2. A aprendizagem se consolida nas habilidades práticas, permitindo ao aluno integrar melhor o conhecimento à prática clínica.
3. A assimilação de ideias e conceitos se torna mais fácil e eficiente, graças à abordagem de situações decorrentes da realidade.
4. A sensação de eficiência do esforço investido se torna um estímulo muito importante para os alunos, o que se traduz em um maior interesse pela aprendizagem e um aumento no tempo dedicado ao curso.

A metodologia universitária mais bem avaliada por seus alunos

Os resultados desse modelo acadêmico inovador podem ser vistos nos níveis gerais de satisfação dos alunos da TECH.

A avaliação dos alunos sobre a qualidade do ensino, a qualidade dos materiais, a estrutura e os objetivos do curso é excelente. Não é de surpreender que a instituição tenha se tornado a universidade mais bem avaliada por seus alunos na plataforma de avaliação Trustpilot, com uma pontuação de 4,9 de 5.

Acesse o conteúdo do estudo de qualquer dispositivo com conexão à Internet (computador, tablet, smartphone) graças ao fato da TECH estar na vanguarda da tecnologia e do ensino.

Você poderá aprender com as vantagens do acesso a ambientes de aprendizagem simulados e com a abordagem de aprendizagem por observação, ou seja, aprender com um especialista.

Assim, os melhores materiais educacionais, cuidadosamente preparados, estarão disponíveis neste programa:

Material de estudo

O conteúdo didático foi elaborado especialmente para este curso pelos especialistas que irão ministrá-lo, o que permite que o desenvolvimento didático seja realmente específico e concreto.
Posteriormente, esse conteúdo é adaptado ao formato audiovisual, para criar o método de trabalho online, com as técnicas mais recentes que nos permitem lhe oferecer a melhor qualidade em cada uma das peças que colocaremos a seu serviço.

Práticas de aptidões e competências

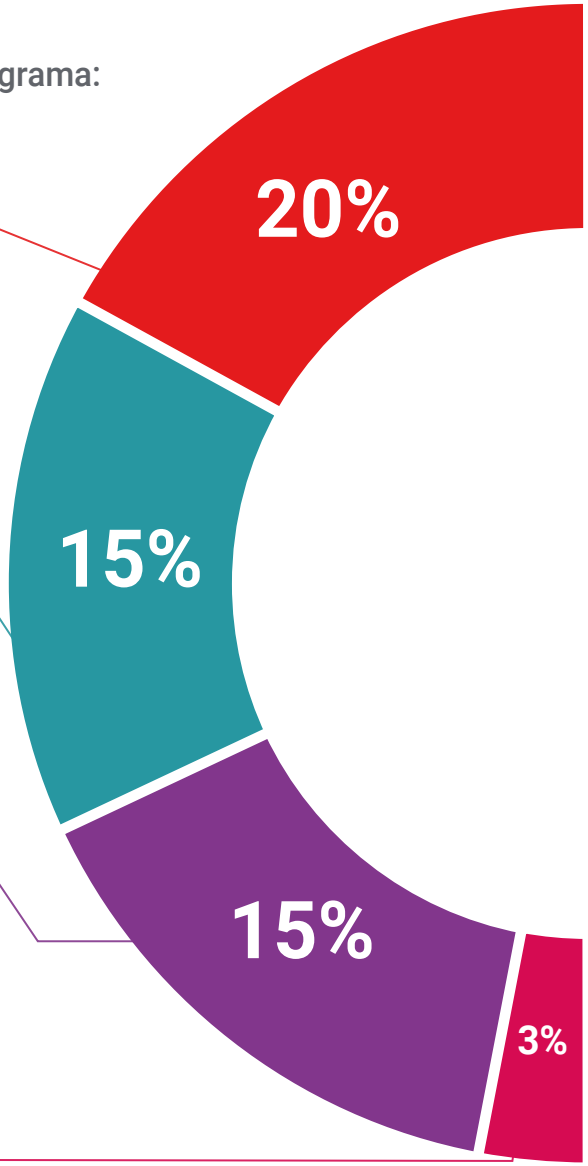
Serão realizadas atividades para desenvolver as habilidades e competências específicas em cada área temática. Práticas e dinâmicas para adquirir e desenvolver as competências e habilidades que um especialista precisa desenvolver no âmbito da globalização.

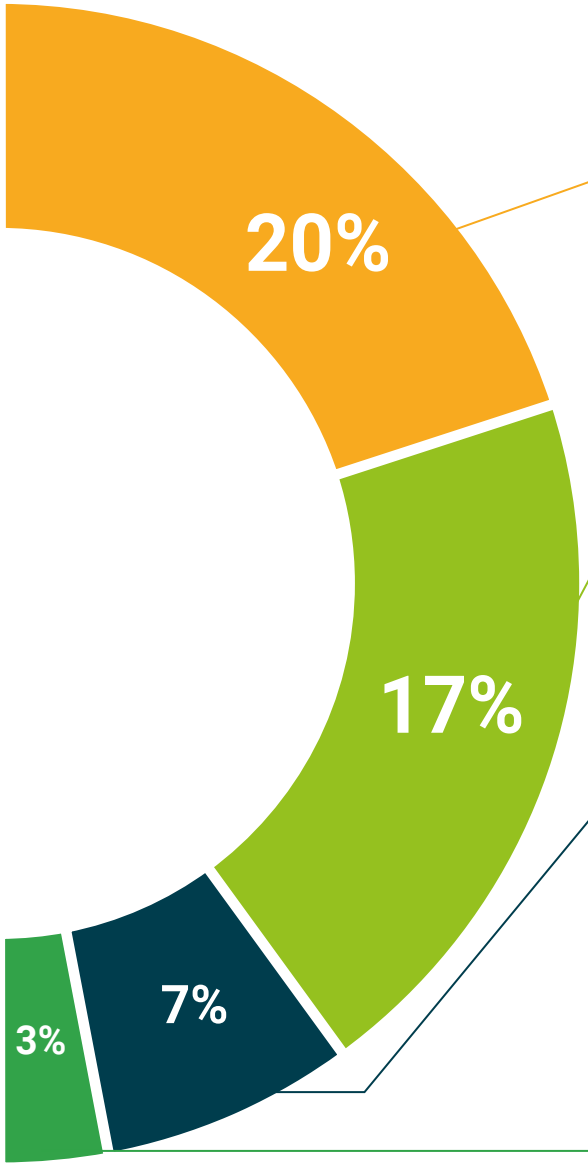
Resumos interativos

Apresentamos os conteúdos de forma atraente e dinâmica em pílulas multimídia que incluem áudio, vídeos, imagens, diagramas e mapas conceituais com o objetivo de reforçar o conhecimento.
Este sistema exclusivo de capacitação por meio da apresentação de conteúdo multimídia foi premiado pela Microsoft como "Caso de sucesso na Europa"

Leituras complementares

Artigos recentes, documentos científicos, guias internacionais, entre outros. Na biblioteca virtual do estudante você terá acesso a tudo o que for necessário para completar sua capacitação.





Case Studies

Você concluirá uma seleção dos melhores *case studies* da disciplina. Casos apresentados, analisados e orientados pelos melhores especialistas no cenário internacional.

Testing & Retesting

Avaliamos e reavaliamos periodicamente seus conhecimentos ao longo de todo o programa. Fazemos isso em 3 dos 4 níveis da Pirâmide de Miller.

Masterclasses

Há evidências científicas sobre a utilidade da observação de terceiros especialistas.
O *Learning from an expert* fortalece o conhecimento e a memória, e aumenta nossa confiança para tomar decisões difíceis no futuro.

Guias rápidos de ação

A TECH oferece o conteúdo mais relevante do curso em formato de fichas de trabalho ou guias rápidos de ação. Uma forma sintetizada, prática e eficaz de ajudar os alunos a progredirem na aprendizagem.

07

Certificação

O MBA em Gestão de Cibersegurança Avançada (CISO), além da formação mais rigorosa e atualizada, o acesso a um certificado de mestrado emitido pela TECH Global University.

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

Este programa permitirá a obtenção do certificado próprio de **Mestrado em MBA Gestão de Cibersegurança Avançada (CISO)** reconhecido pela TECH Global University, a maior universidade digital do mundo

A **TECH Global University,** é uma Universidade Europeia Oficial reconhecida publicamente pelo Governo de Andorra ***(bollettino ufficiale)***. Andorra faz parte do Espaço Europeu de Educação Superior (EEES) desde 2003. O EEES é uma iniciativa promovida pela União Europeia com o objetivo de organizar o modelo de formação internacional e harmonizar os sistemas de ensino superior dos países membros desse espaço. O projeto promove valores comuns, a implementação de ferramentas conjuntas e o fortalecimento dos seus mecanismos de garantia de qualidade para fomentar a colaboração e a mobilidade entre alunos, investigadores e académicos.

Esse título próprio da **TECH Global University**, é um programa europeu de formação contínua e atualização profissional que garante a aquisição de competências na sua área de conhecimento, conferindo um alto valor curricular ao aluno que conclui o programa.

Título: **Mestrado em MBA Gestão de Cibersegurança Avançada (CISO)**

Modalidade: **online**

Duração: **12 meses**

Acreditação: **90 ECTS**

tech global university

Sr./Sra. _____, com o documento de identidade nº _____, foi aprovado satisfatoriamente e obteve o certificado de:

Mestrado em MBA Gestão de Cibersegurança Avançada (CISO)

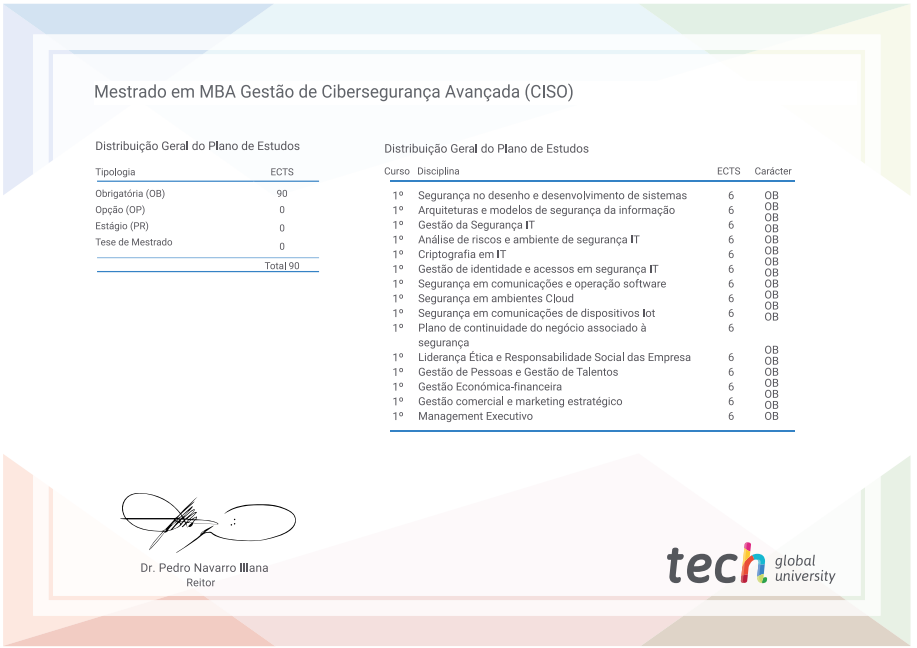
Trata-se de um título próprio com duração de 2700 horas, o equivalente a 90 ECTS, com data de início dd/mm/aaaa e data final dd/mm/aaaa.

A TECH Global University é uma universidade oficialmente reconhecida pelo Governo de Andorra em 31 de janeiro de 2024, que pertence ao Espaço Europeu de Educação Superior (EEES).

Andorra la Vella, 28 de fevereiro de 2024

Dr. Pedro Navarro Illana
Reitor

código único TECH: BBADCEADBECB990 techtitute.com/titulos



Mestrado em MBA Gestão de Cibersegurança Avançada (CISO)

Distribuição Geral do Plano de Estudos

Tipologia	ECTS
Obrigatória (OB)	90
Opção (OP)	0
Estágio (PR)	0
Tese de Mestrado	0
	Total 90

Distribuição Geral do Plano de Estudos

Curso	Disciplina	ECTS	Carácter
1º	Segurança no desenho e desenvolvimento de sistemas	6	OB
1º	Arquiteturas e modelos de segurança da informação	6	OB
1º	Gestão da Segurança IT	6	OB
1º	Análise de riscos e ambiente de segurança IT	6	OB
1º	Criptografia em IT	6	OB
1º	Gestão de identidade e acessos em segurança IT	6	OB
1º	Segurança em comunicações e operação software	6	OB
1º	Segurança em ambientes Cloud	6	OB
1º	Segurança em comunicações de dispositivos Iot	6	OB
1º	Plano de continuidade do negócio associado à segurança	6	OB
1º	Liderança Ética e Responsabilidade Social das Empresa	6	OB
1º	Gestão de Pessoas e Gestão de Talentos	6	OB
1º	Gestão Económica-financeira	6	OB
1º	Gestão comercial e marketing estratégico	6	OB
1º	Management Executivo	6	OB

Dr. Pedro Navarro Illana
Reitor

tech global university

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

tech global university

Mestrado
MBA em Gestão de Cibersegurança Avançada (CISO)

- Modalidade: **Online**
- Duração: **12 meses**
- Certificação: **TECH Global University**
- Acreditação: **90 ECTS**
- Horário: **Ao seu próprio ritmo**
- Exames: **Online**

Mestrado

MBA em Gestão de Cibersegurança Avançada (CISO)

tech global university