Mestrado Próprio

MBA em Gestão Avançada de Cibersegurança (CISO)

tech universidade tecnológica

tech universidade tecnológica

Mestrado Próprio
MBA em Gestão Avançada de Cibersegurança (CISO)

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

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

Índice

01

Apresentação

O mundo atual avança em direção à completa digitalização. Cada vez mais processos, operações e tarefas básicas de todo tipo são realizados por meio de dispositivos eletrônicos. No entanto, esse progresso também traz certos riscos, já que computadores, *smartphones*, *tablets* e todo tipo de aplicativos digitais podem ser vulneráveis a ataques cibernéticos. Por essa razão, muitas empresas estão em busca de especialistas que possam dirigir e gerenciar de forma eficaz a cibersegurança de seus serviços. Este novo perfil profissional está em grande demanda, portanto, este programa foi projetado para fornecer os conhecimentos e as técnicas mais recentes ao cientista da computação, que estará preparado para ser o diretor de cibersegurança em qualquer empresa que o requeira.

Este programa irá prepará-lo intensamente para se especializar na gestão da cibersegurança, um perfil profissional com a maior procura na área de TI na atualidade"

Nos últimos anos, o processo de digitalização se acelerou, impulsionado pelos contínuos avanços na informática. Desta forma, não apenas a tecnologia passou por grandes melhorias, mas também as próprias ferramentas digitais com as quais muitas tarefas são realizadas atualmente. Por exemplo, esses progressos tornaram possível que muitas operações bancárias sejam realizadas por meio de um aplicativo móvel. Também houve inovações na área da saúde, em sistemas de agendamento prévio ou no acesso a históricos clínicos. Além disso, graças a essas tecnologias, é possível consultar faturas ou solicitar serviços de empresas em setores como o de telefonia.

No entanto, esses avanços também trouxeram um aumento das vulnerabilidades cibernéticas. Embora as opções para realizar diversas atividades e tarefas tenham se ampliado, os ataques à segurança de dispositivos, aplicativos e sites cresceram proporcionalmente. Por esse motivo, cada vez mais empresas buscam profissionais especializados em cibersegurança, capazes de proporcionar a proteção adequada contra todo tipo de ataque cibernético.

Como resultado, o perfil de Diretor de Cibersegurança é um dos mais requisitados pelas empresas que operam na internet ou que prestam serviços no ambiente digital. Para responder a essa demanda, a TECH desenvolveu este MBA em Gestão Avançada de Cibersegurança (CISO), que proporcionará ao profissional de TI todas as ferramentas necessárias para exercer esse cargo de forma eficaz, atendendo às últimas novidades em proteção e vulnerabilidades nesse campo tecnológico.

Neste programa, o aluno poderá se aprofundar em aspectos como segurança no desenvolvimento e design de sistemas, assim como contar com as melhores técnicas criptográficas ou de segurança em ambientes Cloud Computing. E isso será feito por meio de uma metodologia 100% online, com a qual será possível conciliar seu trabalho profissional com os estudos, sem horários rígidos ou deslocamentos desconfortáveis para um centro acadêmico. Além disso, o aluno terá acesso a diversos recursos didáticos multimídia, ministrados pelo corpo docente mais prestigiado e especializado na área de cibersegurança.

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

- O desenvolvimento de casos práticos apresentados por especialistas em Informática e cibersegurança
- O conteúdo gráfico, esquemático e eminentemente prático oferece informações científicas e práticas sobre as disciplinas que são essenciais para a prática profissional
- Contém exercícios práticos em que o processo de autoavaliação é realizado para melhorar o aprendizado
- Destaque especial para as metodologias inovadoras
- Lições teóricas, perguntas aos especialistas, fóruns de discussão sobre temas controversos e trabalhos individuais de reflexão
- Disponibilidade de acesso a todo o conteúdo desde qualquer dispositivo fixo ou portátil com conexão à Internet

Em primeira mão, você conhecerá as melhores técnicas de segurança aplicadas a ambientes Cloud Computing ou à tecnologia Blockchain"

Você desfrutará de vários conteúdos multimídia para acelerar seu processo de aprendizagem, enquanto recebe o apoio de um corpo docente de grande prestígio no campo da cibersegurança"

A metodologia online da TECH permitirá escolher o horário e o local para estudar, sem interromper sua atuação profissional.

Você poderá se tornar o Diretor de Cibersegurança das melhores empresas da sua área.

O corpo docente do curso conta com renomados profissionais da área, que transferem toda a experiência adquirida ao longo de suas carreiras para esta capacitação, além de especialistas reconhecidos em instituições de referência e universidades de prestígio.

O conteúdo multimídia, desenvolvido com a mais recente tecnologia educacional, permitirá ao profissional uma aprendizagem contextualizada, ou seja, realizada através de um ambiente simulado, proporcionando uma capacitação imersiva e programada para praticar diante de situações reais.

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

02

Objetivos

O rápido desenvolvimento das tecnologias da informação trouxe grandes avanços, proporcionando inúmeros serviços à população em geral. No entanto, também aumentou a quantidade de vulnerabilidades e ciberataques, por isso, o objetivo principal deste programa é transformar o profissional de TI em um verdadeiro especialista em direção de cibersegurança, garantindo-lhe um enorme e imediato progresso profissional. Desta forma, seus novos conhecimentos lhe darão a oportunidade de ingressar em grandes empresas que operam digitalmente em diversos setores.

O objetivo deste programa é torná-lo um profissional qualificado para liderar o departamento de cibersegurança de uma grande empresa"

Objetivos gerais

- Obter conhecimento especializado sobre um sistema de informação, tipos e aspectos de segurança a serem levados em conta
- Identificação as vulnerabilidades em um sistema de informação
- Desenvolver a normativa legal e tipificação do crime que ataca um sistema de informação
- Avaliar os diferentes modelos de arquitetura de segurança para estabelecer o modelo mais adequado para a organização
- Identificar os marcos normativos aplicáveis e as bases regulatórias para o crime
- Analisar a estrutura organizacional e funcional de uma área de segurança da informação (o escritório do CISO)
- Analisar e desenvolver o conceito de risco, assim como de incerteza dentro do ambiente em que vivemos
- Examinar o modelo de gestão de riscos baseado na ISO 31.000
- Examinar a ciência da criptologia e a relação com seus ramos: criptografia, criptoanálise, esteganografia e estegoanálise
- Analisar os tipos de criptografia de acordo com o tipo de algoritmo e de acordo com seu uso
- Analisar os certificados digitais
- Analisar a infraestrutura da Chave Pública (PKI)
- Desenvolver o conceito de gestão de identidades
- Identificar os métodos de autenticação
- Gerar conhecimento especializado sobre o ecossistema de segurança de TI
- Avaliar o conhecimento em termos de cibersegurança
- Identificar as áreas de segurança em *Cloud*
- Analisar os serviços e ferramentas em cada um dos domínios de segurança
- Desenvolver especificações de segurança para cada tecnologia LPWAN
- Analisar comparativamente a segurança das tecnologias LPWAN

Seus objetivos profissionais estão ao seu alcance com este Mestrado Próprio, que oferece o conhecimento mais avançado em cibersegurança"

Objetivos específicos

Módulo 1. Segurança no projeto e desenvolvimento de sistemas

- Avaliar a segurança de um sistema de informação em todos os seus componentes e camadas
- Identificar os atuais tipos de ameaças à segurança e suas tendências
- Estabelecer diretrizes de segurança, definindo políticas, planos de segurança e contingência.
- Analisar estratégias e ferramentas para garantir a integridade e a 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
- Contar com um marco legal e tipificação do crime, concluindo a visão com uma tipificação do infrator e de sua vítima

Módulo 2. Arquitetura e modelos de segurança da informação

- Alinhar o Plano Diretor de Segurança com os objetivos estratégicos da organização
- Estabelecer um marco contínuo de gestão de riscos como parte integrante do Plano Diretor de Segurança
- Determinar os indicadores pertinentes para o seguimento da implantação do SGSI
- Estabelecer uma estratégia de segurança baseada em políticas
- Analisar os objetivos e procedimentos associados com o plano de conscientização do funcionário, fornecedor e sócios
- Identificar, dentro do marco regulatório, as normas, certificações e leis aplicáveis a cada organização
- Desenvolver os elementos fundamentais requeridos pela norma ISO 27001:2013
- Estabelecer um modelo de gestão de privacidade em conformidade com o regulamento europeu GDPR/RGPD

Módulo 3. Gestão da Segurança TI

- Identificar as diferentes estruturas de uma área de segurança da informação.
- Desenvolver um modelo de segurança baseado em três linhas de defesa
- Apresentar os diferentes comitês periódicos e extraordinários nos quais a área de cibersegurança está envolvida
- Identificar as ferramentas tecnológicas que respaldam as principais funções da equipe de operações de segurança (SOC)
- Avaliar as medidas de controle de vulnerabilidade adequadas a cada cenário
- Desenvolver a estrutura operacional de segurança com base no NIST CSF
- Especificar o escopo dos diferentes tipos de auditorias (*Red Team*, *Pentesting*, *Bug Bounty*, etc.)
- Propor atividades a serem realizadas após um incidente de segurança
- Estabelecer um centro de comando de segurança da informação que envolva todos os protagonistas pertinentes (autoridades, clientes, fornecedores, etc.)

Módulo 4. Análise de riscos e ambiente de segurança TI

- Analisar, com uma visão holística, o ambiente em que nos movemos.
- Identificar os principais riscos e oportunidades que podem afetar a concretização dos objetivos
- Analisar os riscos com base nas melhores práticas disponíveis em nosso mercado
- Avaliar o possível impacto desses riscos e as oportunidades
- Desenvolver técnicas que nos permitam atuar com riscos e oportunidades, maximizando nosso aporte de valor
- Analisar detalhadamente as diferentes técnicas de transferência de riscos e valor
- Gerar valor a partir do projeto de modelos próprios para uma gestão ágil de riscos
- Examinar os resultados para propor melhorias contínuas na gestão de projetos e processos baseados em modelos de gestão orientados ao *Risk-Driven*
- Inovar e transformar dados gerais em informações relevantes para uma tomada de decisões baseada em riscos

Módulo 5. Criptografia em TI

- Compilar as operações fundamentais (XOR, números grandes, substituição e transposição) e os diversos componentes (funções One-Way, Hash, geradores de números aleatórios)
- Analisar técnicas criptográficas
- Desenvolver os diferentes algoritmos criptográficos
- Demonstrar o uso de assinaturas digitais e sua aplicação em certificados digitais
- Avaliar os sistemas de controle de chaves e a importância dos comprimentos de chaves criptográficas
- Examinar algoritmos de derivação de chaves
- Analisar o ciclo de vida das chaves
- Avaliar os modos de cifrado de bloco e de fluxo
- Determinar geradores de números pseudo-aleatórios
- Desenvolver casos reais de aplicações criptográficas, tais como Kerberos, PGP ou cartões inteligentes
- Examinar associações e órgãos relacionados, tais como ISO, NIST ou NCSC
- Determinar os desafios na criptografia da computação quântica

Módulo 6. Gestão de identidades e acessos em Segurança TI

- Desenvolver o conceito de identidade digital
- Avaliar o controle de acesso físico às informações
- Fundamentar a autenticação biométrica e a autenticação MFA
- Avaliar os ataques relacionados à confidencialidade das informações
- Analisar a federação de identidades
- Estabelecer o controle de acesso à rede

Módulo 7. Segurança nas comunicações e operação de software
- Desenvolver conhecimentos especializados em segurança física e lógica
- Demonstrar conhecimento em comunicações e redes
- Identificar os principais ataques maliciosos
- Estabelecendo uma estrutura de desenvolvimento segura
- Comprovar conhecimento dos principais regulamentos do sistema de gestão de segurança da informação
- Justificar o funcionamento de um centro de operações de cibersegurança
- Demonstrar a importância das práticas de segurança cibernética para as catástrofes organizacionais

Módulo 8. Segurança em ambientes Cloud
- Identificar os riscos de uma implantação de infraestrutura em *cloud* pública
- Definir os requisitos de segurança
- Desenvolver um plano de segurança para a implantação em *cloud*
- Identificar os serviços *cloud* a ser implantados para um plano de segurança
- Determinar as disposições operacionais necessárias para os mecanismos preventivos
- Estabelecer diretrizes para um sistema de *Logging* e monitoramento
- Propor ações de resposta aos incidentes

Módulo 9. Segurança em comunicações de dispositivos IoT
- Apresentar a arquitetura simplificada IoT
- Justificar as diferenças entre as tecnologias de conectividade generalistas e as tecnologias de conectividade para a IoT
- Estabelecer o conceito do triângulo de ferro da conectividade IoT
- Analisar as especificações de segurança da tecnologia LoRaWAN, da tecnologia NB-IoT e da tecnologia WiSUN
- Fundamentar a escolha da tecnologia IoT adequada para cada projeto

Módulo 10. Plano de continuidade de negócio associado à segurança
- Apresentar os elementos-chave de cada fase e analisar as características do plano de continuidade de negócio (PCN)
- Justificar a necessidade de um Plano de Continuidade de Negócio
- Determinar os mapas de sucesso e de risco para cada fase do plano de continuidade do negócio
- Especificar como é estabelecido um plano de ação para uma implantação
- Avaliar a integralidade de um Plano de Continuidade de Negócio (PCN)
- Desenvolver um plano para uma bem sucedida implantação de um plano de continuidade de negócio

Módulo 11. Liderança, Ética e Responsabilidade Social Corporativa
- Analisar o impacto da globalização na governança e no governo corporativo
- Avaliar a importância da liderança eficaz na direção e sucesso das empresas
- Definir as estratégias de gestão intercultural e sua relevância em ambientes empresariais diversos
- Desenvolver habilidades de liderança e entender os desafios atuais que os líderes enfrentam
- Determinar os princípios e práticas da ética empresarial e sua aplicação na tomada de decisões corporativas
- 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 de recursos humanos
- Explorar as competências necessárias para a gestão eficaz de recursos humanos por competências
- Explorar as metodologias para a avaliação de desempenho e a gestão do desempenho
- Integrar as inovações na gestão de talentos e seu impacto na retenção e fidelização de pessoal
- Desenvolver estratégias para a motivação e o desenvolvimento de equipes de alto desempenho
- Propor soluções eficazes para a gestão da mudança e a resolução de conflitos nas organizações

Módulo 13. Gestão Econômico-Financeira

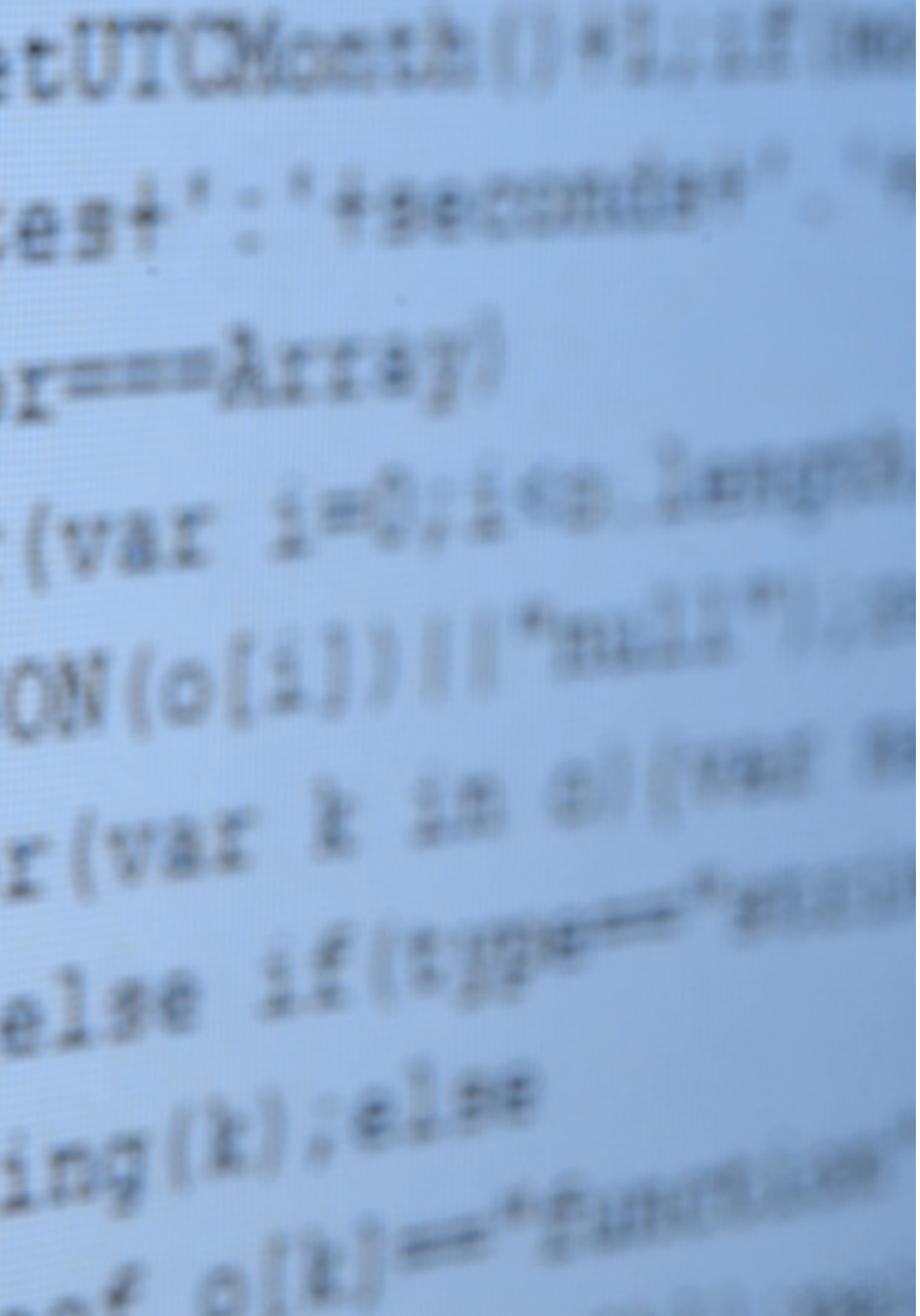
- Analisar o ambiente macroeconômico e sua influência no sistema financeiro nacional e internacional
- Definir os sistemas de informação e Business Intelligence para a tomada de decisões financeiras
- Diferenciar decisões financeiras chave e a gestão de riscos na direção financeira
- Avaliar estratégias para o planejamento financeiro e a obtenção de financiamento empresarial

Módulo 14. Gestão Comercial e Marketing Estratégico

- Estruturar o quadro conceitual e a importância da direção comercial nas empresas
- Explorar os elementos e atividades fundamentais do marketing e seu impacto na organização
- Determinar as etapas do processo de planejamento estratégico de marketing
- Avaliar estratégias para melhorar a comunicação corporativa e a reputação digital da empresa

Módulo 15. *Gestão* Executiva

- Definir o conceito de General Management e sua relevância na direção de empresas
- Avaliar as funções e responsabilidades do executivo na cultura organizacional
- Analisar a importância da gestão de operações e da gestão da qualidade na cadeia de valor
- Desenvolver a comunicação interpessoal e as habilidades de falar em público para a formação de porta-vozes



Seus objetivos profissionais estão ao seu alcance com este Mestrado Próprio, que oferece o conhecimento mais avançado em cibersegurança"

03

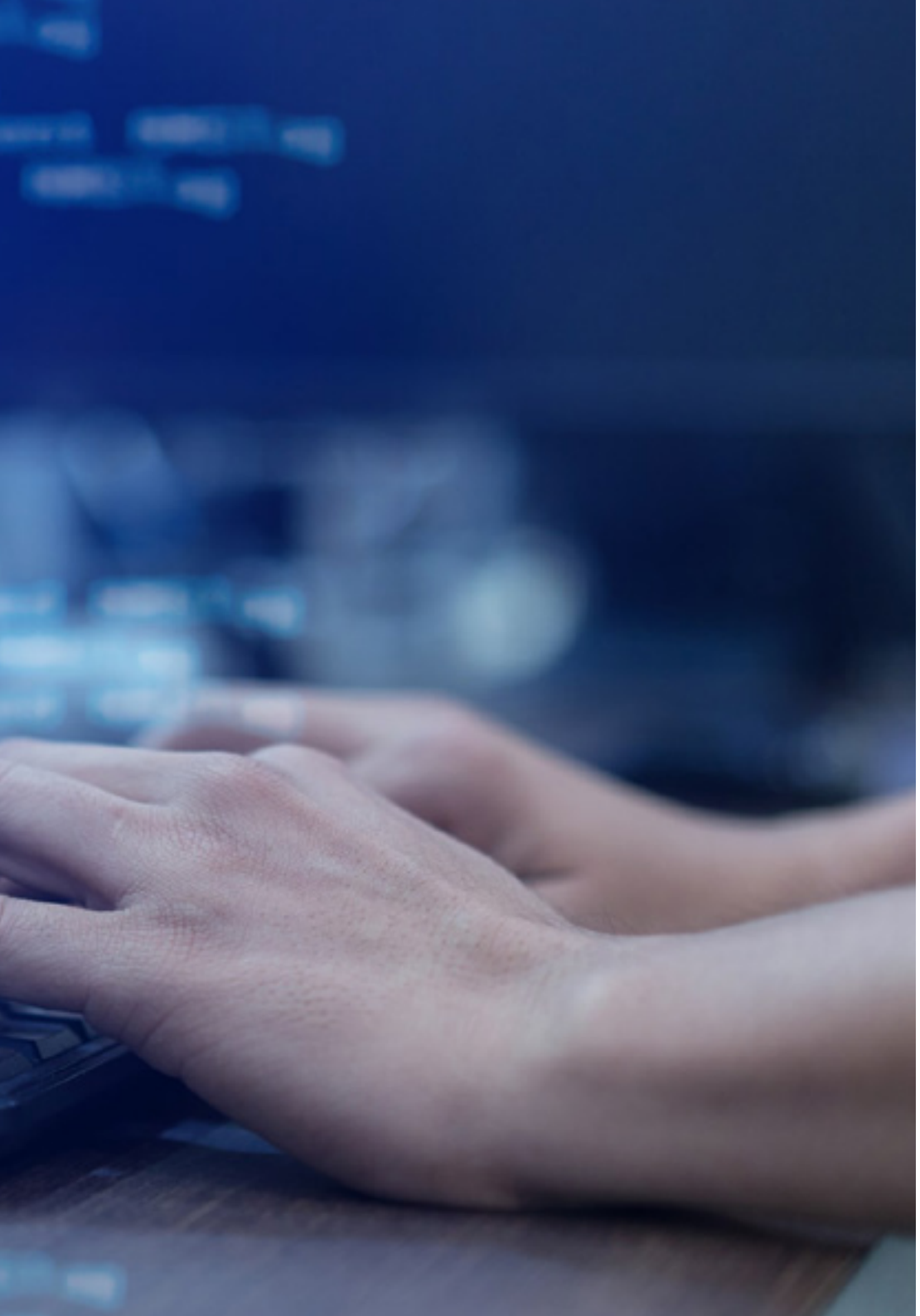
Competências

Com este Mestrado Próprio, o profissional adquirirá inúmeras novas competências na área da cibersegurança. Nos últimos anos, o surgimento de tecnologias como o *Blockchain*, o *Cloud Computing* e a Inteligência Artificial levou ao desenvolvimento de novas áreas de cibersegurança. Por essa razão, este programa foi especialmente desenvolvido para proporcionar ao profissional todas as habilidades necessárias para se adaptar a essas tecnologias em plena ascensão.

As competências que este programa proporcionará irão permitir uma atualização e adaptação ao novo ambiente de TI, onde tecnologias como Blockchain e Inteligência Artificial entraram em cena"

Competências gerais

- Aplicar as medidas de segurança mais adequadas, dependendo das ameaças
- Determinar a política e o plano de segurança do sistema de informação de uma companhia, completando o projeto e a implantação do plano de contingência
- Estabelecer um programa de auditoria que atenda às necessidades de autoavaliação de cibersegurança da organização
- Desenvolver um programa de análise e controle de vulnerabilidade, bem como um plano de resposta a incidentes de cibersegurança
- Maximizar as oportunidades apresentadas e eliminar a exposição a todos os potenciais riscos relacionados ao projeto
- Compilar os sistemas de gestão de chaves
- Avaliar a segurança da informação de uma companhia
- Analisar os sistemas de acesso à informação
- Desenvolver as melhores práticas em desenvolvimento seguro
- Apresentar para as empresas os riscos por não contarem com um ambiente de informática seguro



Competências específicas

- Desenvolver um Sistemas de Gestão de Segurança da Informação(SGSI)
- Identificar os elementos-chave que compõem um SGSI
- Aplicar a metodologia MAGERIT para aperfeiçoar o modelo e levá-lo um passo adiante
- Projetar novas metodologias de gestão de risco, baseadas no conceito *agile Risk Management*
- Identificar, analisar, avaliar e abordar os riscos enfrentados pelo profissional, considerando uma nova perspectiva empresarial baseada em um modelo *Risk-Driven* ou impulsionado pelo risco que permite não só sobreviver em seu próprio ambiente, mas também aportar valor próprio
- Examinar o processo de elaboração de uma estratégia de segurança ao implantar serviços corporativos em *Cloud*
- Avaliar as diferenças nas implementações concretas dos diferentes fornecedores de *Cloud* pública
- Avaliar as opções de conectividade de IoT para abordar um projeto, enfatizando as tecnologias LPWAN
- Apresentar as especificações básicas das principais tecnologias LPWAN para o IoT

04

Direção do curso

A enorme complexidade da cibersegurança atual exige um aprendizado completo e detalhado. Por essa razão, a TECH se encarregou de reunir o melhor corpo docente especializado nesta área. Desta forma, o profissional contará com o acompanhamento e supervisão de um corpo docente que está atualizado com os últimos avanços nessa área, permitindo que ele incorpore ao seu trabalho diário as melhores técnicas de cibersegurança, ao mesmo tempo em que adquire as habilidades necessárias de liderança nesta área.

Você terá à sua disposição autênticos especialistas em cibersegurança. Esta é a oportunidade que você estava procurando"

Diretora Internacional Convidada

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

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

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

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

Sra. Jennifer Dove

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

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

Diretor Internacional Convidado

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

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

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

Sr. Rick Gauthier

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

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

Diretor Internacional Convidado

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

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

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

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

Sr. Romi Arman

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

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

Diretor Internacional Convidado

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

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

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

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

Sr. Manuel Arens

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

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

Diretor Internacional Convidado

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

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

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

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

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

Sr. Andrea La Sala

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

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

Diretor Internacional Convidado

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

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

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

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

Sr. Mick Gram

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

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

Diretor Internacional Convidado

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

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

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

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

Sr. Scott Stevenson

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

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

Diretor Internacional Convidado

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

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

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

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

Sr. Eric Nyquist

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

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

Direção

Sr. Martín Olalla Bonal

- Gerente Sênior de Prática de Blockchain no EY
- Especialista técnico cliente Blockchain para IBM
- Diretor de Arquitetura da Blocknitive
- Coordenador da equipe de banco de dados distribuídos não relacional para a wedoIT (Subsidiária da IBM)
- Arquiteto de infraestruturas na Bankia
- Responsável pelo Departamento de Maquetação da T-Systems
- Coordenador de Departamento para 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
- Formado pela Universidade de Jaén e University of Technology and Economics of Budapest (BME)
- Graduação em Engenharia de Organização Industrial

Sr. Juan Manuel Rodrigo Estébanez

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

Professores

Dr. Antonio Gómez Rodríguez

- Engenheiro principais de soluções Cloud na Oracle
- Co-organizador do Málaga Developer Meetup
- Consultor especializado do Sopra Group e Everis
- Líder de equipe na System Dynamics
- Desenvolvedor de Software na SGO Software
- Mestrado E-Business pela Escola de Negócios La Salle
- Postgraduado em Tecnologias e Sistemas de Informação pelo Instituto Catalão de Tecnologia
- Formado em Engenharia de Telecomunicações pela Universidade Politécnica da Catalunha

Dr. Jorge del Valle Arias

- Smart City Solutions & Software Business Development Manager Espanha. Itron, Inc Consultor IoT
- Diretor de Negócios Interino de IoT. TCOMET
- Responsável pela Unidade de Negócios de IoT e Indústria 4.0. Diode Espanha
- Gerente de Área de Vendas de IoT e Telecomunicações. Aicox Soluções
- Diretor Técnico (CTO) e Gerente de Desenvolvimento de Negócios. Consultoria TELYC
- Fundador e CEO da Sensor Intelligence
- Chefe de Operações e Projetos. Codio
- Diretor de Operações da Codium Networks
- Engenheiro-chefe de design de hardware e firmware. AITEMIN
- Chefe Regional de Planejamento e Otimização de RF - Rede LMDS de 3,5 GHz. Clearwire
- Engenheiro de Telecomunicações da Universidade Politécnica de Madrid
- Executive MBA pela Escola Internacional Graduate School of La Salle, em 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 (Consultoria especializada em tecnologia)
- Formado em Engenharia de Organização Industrial pela Universidade Pontifícia de Comillas ICAI
- Graduado em Engenharia Técnica Industrial especializado em Eletrônica Industrial pela Universidade Pontifícia de Comillas ICAI
- Mestrado em Gestão de Seguros pelo ICEA (Instituto de Colaboração entre Companhias de Seguros)

Dr. Alejandro Entrenas

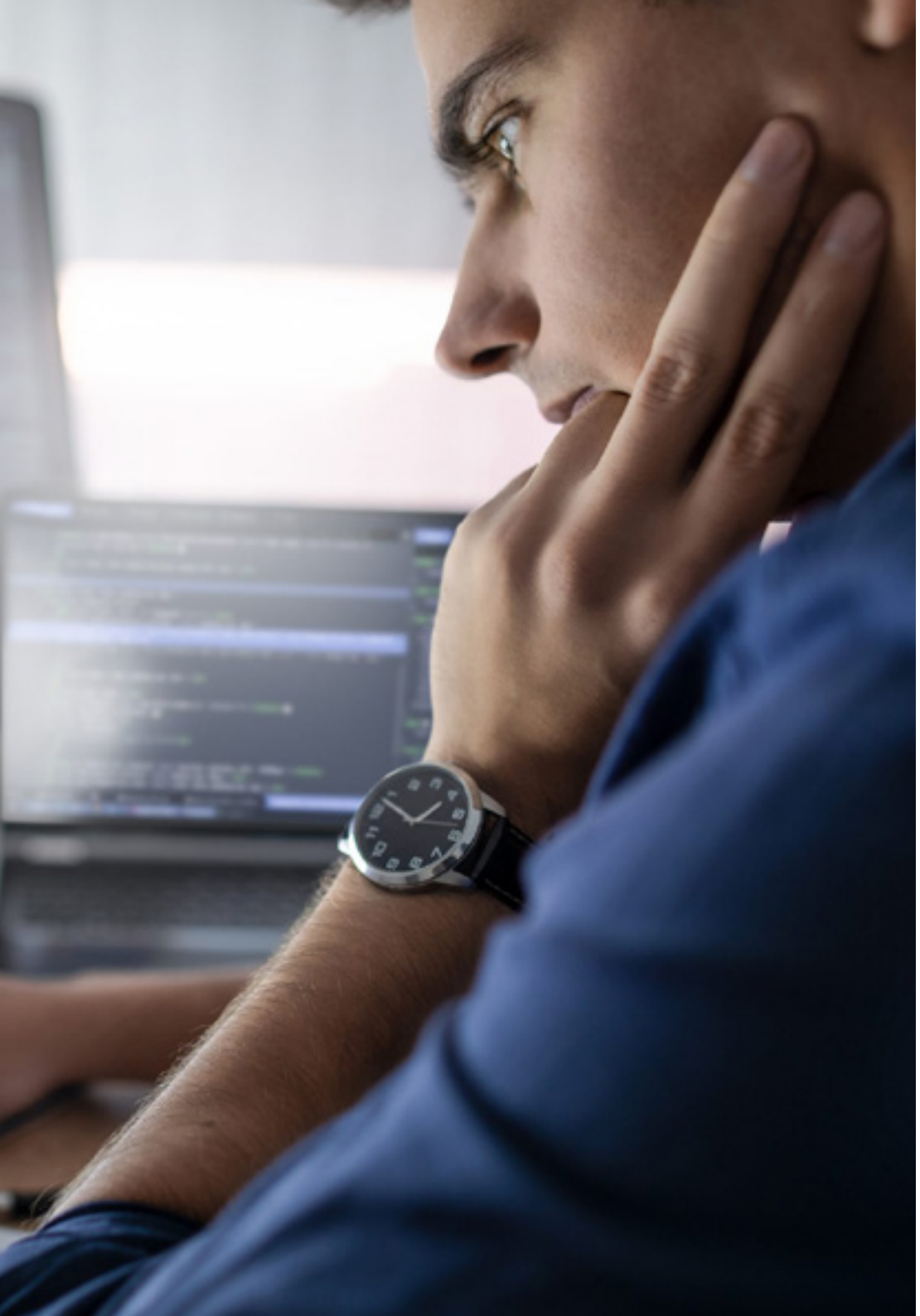
- Gerente de Projetos de Cibersegurança. Entelgy Innotec Security
- Consultor de Cibersegurança. Entelgy
- Analista de Segurança da Informação. Innovery Espanha
- Analista em Segurança da Informação. Atos
- Formado em Engenharia Técnica em Sistemas de Computação pela Universidade de Córdoba
- Mestrado em Gestão de 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

Sr. Octavio Ortega

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

Sr. Mario Embid Ruiz

- Advogado Especialista em TIC e Proteção de Dados na Martínez-Echevarría Advogados
- Responsável Legal na Branddocs SL
- Analista de Risco no Segmento de PME no BBVA
- Docente em estudos de pós-graduação universitária relacionados ao Direito
- Formado em Direito pela Universidade Rey Juan Carlos
- Formado 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

- Gerente de Produtos com base em Blockchain para a Open Canarias
- Diretor Blockchain DevOps na Alastria
- Diretor de Tecnologia Nível de Serviço em Santander Espanha
- Diretor de Desenvolvimento de Aplicações Móveis Tinkerlink na Cronos Telecom
- Diretor de Tecnologia de Gestão de Serviços de TI na Barclays Bank Espanha
- Formado em Engenharia da Computação na UNED
- Especialização em *Deep Learning* na DeepLearning.ai

Dra. Lorena Jurado Jabonero

- Responsável pela Segurança da Informação (CISO) no Grupo Pascual
- Gestor de Cibersegurança na KPMG. Espanha
- Consultor de Processos de TI e Controle e Gestão de Projetos de Infraestrutura no Bankia
- Engenheiro de Ferramentas de Exploração na Dalkia
- Desenvolvedor no Grupo Banco Popular
- Desenvolvedor de Aplicações pela Universidade Politécnica de Madrid
- Graduada em Engenharia Informática pela Universidade Alfonso X el Sabio
- Engenheiro Técnico em Informática de Gestão pela Universidade Politécnica de Madrid
  Certified Data Privacy Solutions Engineer (CDPSE) pela ISACA

05

Estrutura e conteúdo

Este MBA em Gestão Avançada de Cibersegurança (CISO) está estruturado em 10 módulos especializados que permitirão ao profissional se aprofundar em aspectos como a identificação digital, os sistemas de controle de acesso, a arquitetura de segurança da informação, a estrutura da área de segurança, os sistemas de gestão da segurança da informação em comunicações e operação de software, além do desenvolvimento do plano de continuidade de negócios associado à segurança. Com isso, o profissional de TI poderá conhecer de forma completa todas as questões relevantes da cibersegurança atual.

Você não encontrará um conteúdo mais completo e inovador do que este para especializar-se na gestão avançada da cibersegurança"

Módulo 1. Segurança no projeto e desenvolvimento de sistemas

1.1. Sistemas de informação
- 1.1.1. Domínios de 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 de sistemas de informação
  - 1.2.1.1. Empresarial
  - 1.2.1.2. Estratégico
  - 1.2.1.3. De acordo com o escopo de aplicação
  - 1.2.1.4. Específico
- 1.2.2. Sistemas de informação. Exemplos reais
- 1.2.3. Evolução dos sistemas de Informação: etapas
- 1.2.4. Metodologias dos sistemas de Informação

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

1.4. Segurança dos sistemas de Informação Protocolo de segurança
- 1.4.1. Segurança de um sistema de Informação
  - 1.4.1.1. Integridade
  - 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 em sistemas de Informação Medidas e sistemas de controle de acesso
- 1.5.1. Medidas de segurança
- 1.5.2. Tipo de medidas de segurança
  - 1.5.2.1. Prevenção
  - 1.5.2.2. Detecção
  - 1.5.2.3. Correção
- 1.5.3. Sistemas de controle 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. Criminalidade informática
- 1.7.1. Crime Digital
- 1.7.2. Crimes Digitais Tipologia
- 1.7.3. Crime Digital Ataques Tipologia
- 1.7.4. O caso da Realidade Virtual
- 1.7.5. Perfis dos infratores e das vítimas. Tipificação do crime
- 1.7.6. Crimes Digitais Exemplos e casos reais

1.8. Plano de segurança em um sistema de informação
- 1.8.1. Plano de segurança Objetivos
- 1.8.2. Plano de segurança Planejamento
- 1.8.3. Plano de riscos Análise
- 1.8.4. Política de segurança Implementação na organização
- 1.8.5. Plano 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 objetos
- 1.9.3. Plano de contingência na organização Implementação
- 1.9.4. Planos de Contingência Exemplos

1.10. Governança de segurança dos sistemas de informação
- 1.10.1. Regulamentações legais
- 1.10.2. Padrões
- 1.10.3. Certificações
- 1.10.4. Tecnologias

Módulo 2. Arquitetura e modelos de segurança da informação

2.1. Arquitetura de segurança da informação
- 2.1.1. SGSI/PDS
- 2.1.2. Alinhamento estratégico
- 2.1.3. Gestão do risco
- 2.1.4. Avaliação do desempenho

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

2.3. Modelo de segurança Componentes-chave
- 2.3.1. Identificação de riscos
- 2.3.2. Definição de controles
- 2.3.3. Avaliação contínua de níveis de risco
- 2.3.4. Plano de conscientização para funcionários, fornecedores, parceiros, etc.

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

2.5. Processos de negócio e segurança da informação
- 2.5.1. Processos de negócio
- 2.5.2. Avaliação de risco baseada em parâmetros de negócio
- 2.5.3. Análise de impacto nos negócios
- 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. Planejar
  - 2.6.1.2. Realizar
  - 2.6.1.3. Verificar
  - 2.6.1.4. Atuar

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 da infraestrutura de rede
- 2.7.5. Tecnologias e soluções de criptografia
- 2.7.6. Segurança de equipamentos terminais (EDR)

2.8. O marco regulatório
- 2.8.1. Normativas setoriais
- 2.8.2. Certificações
- 2.8.3. Legislações

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

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

Módulo 3. Gestão da Segurança TI

3.1. Gestão da Segurança
- 3.1.1. Operações de segurança
- 3.1.2. Aspecto legal e regulatório
- 3.1.3. Viabilidade do negócio
- 3.1.4. Gestão de riscos
- 3.1.5. Gestão de identidades e acessos

3.2. Estrutura da área de segurança A sede do CISO
- 3.2.1. Estrutura organizacional Posição do CISO na estrutura
- 3.2.2. As linhas de defesa
- 3.2.3. Organograma do escritório do CISO
- 3.2.4. Gestão de orçamento

3.3. Governança de segurança
- 3.3.1. Comitê de Segurança
- 3.3.2. Comitê de Monitoramento de Riscos
- 3.3.3. Comitê de Auditoria
- 3.3.4. Comitê de crises

3.4. Governança de segurança. Funções
- 3.4.1. Políticas e normas
- 3.4.2. Plano diretor de segurança
- 3.4.3. Paineis de controle
- 3.4.4. Conscientização e capacitação
- 3.4.5. Segurança na cadeia de suprimentos

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. Marco de trabalho em cibersegurança NIST CSF
- 3.6.1. Metodologia NIST
  - 3.6.1.1. Identificar
  - 3.6.1.2. Proteger
  - 3.6.1.3. Detectar
  - 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. Detecção. SIEM, *User Behavior Analytics, Fraud Prevention*
- 3.7.3. Resposta

3.8. Auditorias de segurança
- 3.8.1. Teste de intrusão
- 3.8.2. Exercícios de *red team*
- 3.8.3. Auditorias de código fonte. Desenvolvimento seguro
- 3.8.4. Segurança dos componentes (*Software Supply Chain*)
- 3.8.5. Análise Forense

3.9. Resposta a incidentes
- 3.9.1. Preparação
- 3.9.2. Detecção, análise e notificação
- 3.9.3. Contenção, erradicação e recuperação
- 3.9.4. Atividade 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 incidentes cibernéticos

3.10. Gestão de vulnerabilidades
- 3.10.1. Análise de vulnerabilidades
- 3.10.2. Avaliação vulnerabilidade
- 3.10.3. Bastion Host do sistema
- 3.10.4. Vulnerabilidades do 0° dia. *Zero-Day*

Módulo 4. Análise de riscos e ambiente de segurança TI

4.1. Análise do ambiente
- 4.1.1. Análise da situação atual
  - 4.1.1.1. Ambiente 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. Ambiente 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. Econômico
  - 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. Fortalezas

4.2. Risco e incerteza
- 4.2.1. Riscos
- 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. Objetivo
- 4.3.2. Princípios
- 4.3.3. Marco de referência
- 4.3.4. Processo

4.4. Metodologia de análise e gestão dos riscos do sistema 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 (PILAR)

4.5. Transferência de risco cibernético
- 4.5.1. Transferência de riscos
- 4.5.2. Riscos cibernéticos Tipologia
- 4.5.3. Seguro contra riscos cibernéticos

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

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

4.8. Mapeamento de riscos de TI baseados em metodologias ágeis
- 4.8.1. Representação de probabilidade e impacto em ambientes ágeis
- 4.8.2. O risco como uma ameaça ao valor
- 4.8.3. Revolução 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 orientado para o risco

4.10. Inovação e transformação digital na gestão de riscos de TI
- 4.10.1. Inovação e transformação digital na gestão de riscos de TI
- 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 TI

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

5.2. Criptologia
- 5.2.1. Criptologia
- 5.2.2. Criptanálise
- 5.2.3. Esteganografia e estegoanálise

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. Comprimento da chave
- 5.4.2. Gestão da chaves
- 5.4.3. Tipos de algoritmos
- 5.4.4. Funções Hash *Hash*
- 5.4.5. Geradores de números pseudo-aleatórios
- 5.4.6. Uso de algoritmos

5.5. Criptografia simétrica
- 5.5.1. Cifrados 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 cifrados 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 y 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 em relação à computação quântica
- 5.10.3. Distribuição de chaves quânticas

Módulo 6. Gestão de identidades e acessos em Segurança TI

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

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

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

6.4. Controle de acesso lógico Autenticação MFA
- 6.4.1. Controle de acesso lógico Autenticação MFA
- 6.4.2. Senhas Importância
- 6.4.3. Ataques de autenticação

6.5. Controle de acesso lógico Autenticação biométrica
- 6.5.1. Controle de Acesso Lógico. Autenticação biométrica
  - 6.5.1.1. Autenticação biométrica Requisitos
- 6.5.2. Funcionamento
- 6.5.3. Modelos 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 controle de acesso
- 6.8.1. FW-Firewall
- 6.8.2. VPN - Redes Privadas Virtuais
- 6.8.3. IDS - Sistema de Detecção de Intrusão

6.9. Sistemas de controle de acesso a rede
- 6.9.1. NAC
- 6.9.2. Arquitetura e elementos
- 6.9.3. Operação e padronização

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

Módulo 7. Segurança nas comunicações e operação de software

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

7.2. Segurança informática em comunicações e operação de 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 de 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 de 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. Operações SOC
- 7.7.3. SIEM *vendors*

7.8. A função da segurança nas organizações
- 7.8.1. Funções nas organizações
- 7.8.2. Funções dos especialistas em IoT nas companhias
- 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 implementação

7.10. A Cibersegurança atualmente
- 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 na segurança
- 8.1.3. Segurança em ambientes *Cloud Computing.* Aspectos principais 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 compartilhada
- 8.3.1. Elementos de segurança gestionados pelo fornecedor
- 8.3.2. Elementos gestionados pelo cliente
- 8.3.3. Definição da estratégia de 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 de sistemas de banco de dados
- 8.5.3. Securitização de dados em trânsito

8.6. Proteção de infraestrutura
- 8.6.1. Projeto e implementação de rede segura
- 8.6.2. Segurança em recursos computacionais
- 8.6.3. Ferramentas e recursos para a proteção da infraestrutura

8.7. Detecção de ameaças e ataques
- 8.7.1. Sistemas de auditoria, *Logging* e monitoramento
- 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* públicos
- 8.9.1. AWS (Amazon Web Services)
- 8.9.2. Microsoft Azure
- 8.9.3. Google GCP
- 8.9.4. Oracle Cloud

8.10. Regulamentos e conformidade
- 8.10.1. Cumprimento das normas de segurança
- 8.10.2. Gestão de riscos
- 8.10.3. Pessoas e processos nas organizações

Módulo 9. Segurança em comunicações de dispositivos IoT

9.1. Da telemetria ao IoT
- 9.1.1. Telemetria
- 9.1.2. Conectividade 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. Vulnerabilidades de segurança do IoT
- 9.3.1. Dispositivos IoT
- 9.3.2. Dispositivos IoT Casos de uso
- 9.3.3. Dispositivos IoT Vulnerabilidades

9.4. Conectividade IoT
- 9.4.1. Redes PAN, LAN, WAN
- 9.4.2. Tecnologias sem fio não IoT
- 9.4.3. Tecnologias sem fio LPWAN

9.5. Tecnologias LPWAN
- 9.5.1. O triângulo de ferro das redes LPWAN
- 9.5.2. Bandas de frequência livres vs. Bandas licenciadas
- 9.5.3. Opções de tecnologia LPWAN

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

9.7. Tecnologia Sigfox
- 9.7.1. Tecnologia Sigfox
- 9.7.2. Casos de uso 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 uso celular IoT Ecossistema
- 9.8.3. Segurança em celular IoT

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

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

Módulo 10. Plano de continuidade de negócio associado à segurança

10.1. Plano de continuidade de negócio
- 10.1.1. Os planos de continuidade de negócio (PCN)
- 10.1.2. Plano de continuidade de negócio (PCN) Aspectos fundamentais
- 10.1.3. Plano de Continuidade de Negócio (PCN) para a avaliação da empresa

10.2. Métricas em um 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. Objetivo do Ponto de Recuperação (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 desastre(PRD)

10.4. Gestão de riscos associado ao PCN
- 10.4.1. Análise de impacto nos negócios
- 10.4.2. Benefícios da implantação 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 terapia Contingência
- 10.5.4. Fase 4: Testes, manutenção e Revisão

10.6. Fase de 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. Entregáveis Criação de um plano

10.7. Fase de determinação da estratégia de continuidade em um PCN
- 10.7.1. Funções na fase de determinação da estratégia
- 10.7.2. Tarefas na fase de determinação da estratégia
- 10.7.3. Entregáveis

10.8. Fase de resposta a contingências em um PCN
- 10.8.1. Funções na fase resposta
- 10.8.2. Tarefas nesta fase
- 10.8.3. Entregáveis

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

10.10. Normas ISO associadas ao planejamento 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 Corporativa

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

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

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

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

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

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

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

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

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

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

Módulo 12. Gestão de Pessoas e Gestão de Talentos

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

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

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

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

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

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

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

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

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

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

Módulo 13. Gestão Econômico-Financeira

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

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

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

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

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

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

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

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

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

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

Módulo 14. Gestão Comercial e Marketing Estratégico

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

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

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

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

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

14.6. Marketing digital para atrair e reter clientes
- 14.6.1. Estratégias de fidelização e engajamento via internet
- 14.6.2. *Visitor Relationship Management*
- 14.6.3. Hipersegmentação

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

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

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

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

Módulo 15. *Gestão* Executiva

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

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

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

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

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

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

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

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

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

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

A melhor equipe de professores e o sistema didático inovador, combinados em um plano de estudos completo e atualizado: esta é uma grande oportunidade para se tornar um cientista da computação"

06

Metodologia

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

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

Estudo de caso para contextualizar todo o conteúdo

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

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

Você terá acesso a um sistema de aprendizagem baseado na repetição, por meio de um ensino natural e progressivo ao longo de todo o programa.

Através de atividades de colaboração e casos reais, o aluno aprenderá a resolver situações complexas em ambientes reais de negócios.

Um método de aprendizagem inovador e diferente

Este curso da TECH é um programa de ensino intensivo, criado do zero, que propõe os desafios e decisões mais exigentes nesta área, em âmbito nacional ou internacional. Através desta metodologia, o crescimento pessoal e profissional é impulsionado em direção ao sucesso. O método do caso, técnica que constitui a base deste conteúdo, garante que a realidade econômica, social e profissional mais atual seja adotada.

> *Nosso programa prepara você para enfrentar novos desafios em ambientes incertos e alcançar o sucesso na sua carreira"*

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

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

Metodologia Relearning

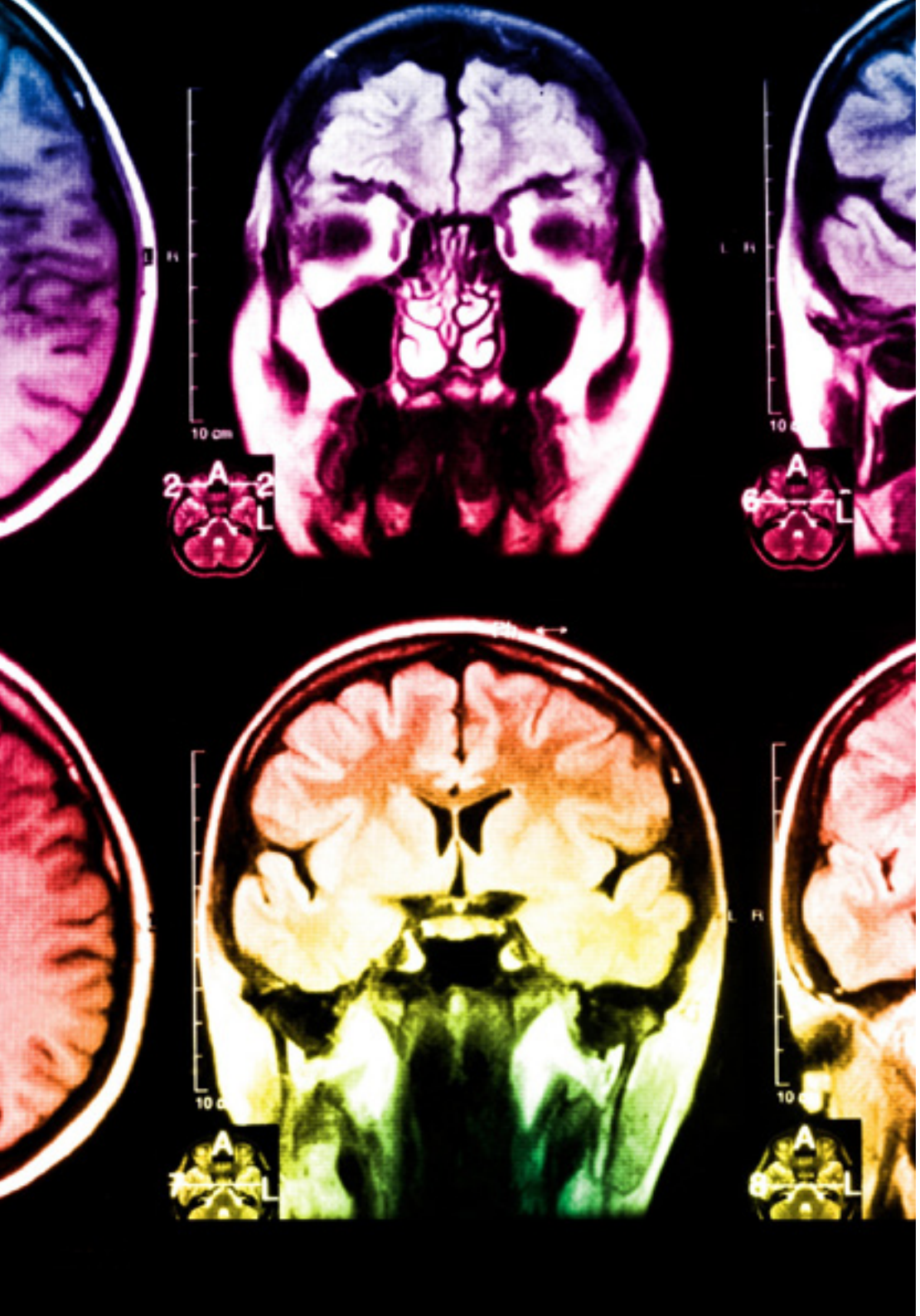
A TECH utiliza de maneira eficaz a metodologia do estudo de caso com um sistema de aprendizagem 100% online, baseado na repetição, combinando elementos didáticos diferentes em cada aula.

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

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

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

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



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

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

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

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

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

Material de estudo

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

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

Masterclasses

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

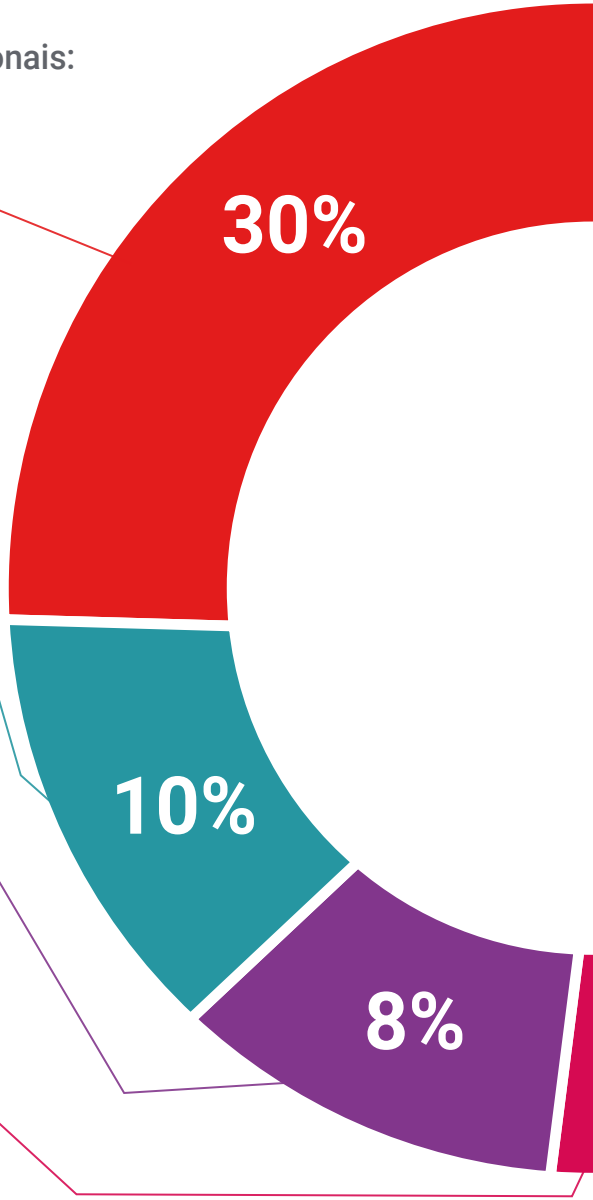
O "Learning from an expert" fortalece o conhecimento e a memória, além de gerar segurança para a tomada de decisões difíceis no futuro.

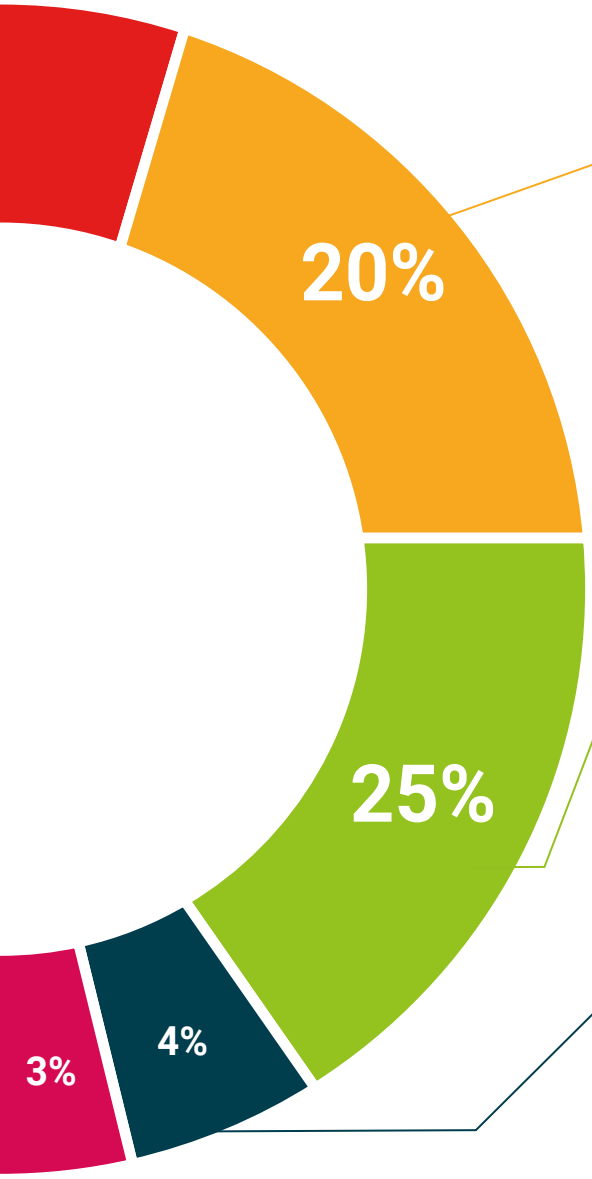
Práticas de habilidades e competências

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

Leituras complementares

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





Estudos de caso

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

Resumos interativos

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

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

Testing & Retesting

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

07

Certificado

O Mestrado Próprio MBA em Gestão Avançada de Cibersegurança (CISO) garante, além da capacitação mais rigorosa e atualizada, o acesso a um título de Mestrado Próprio emitido pela TECH Universidade Tecnológica.

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

Este **Estudio de/em titulo del programa** conta com o conteúdo mais completo e atualizado do mercado.

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

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

Título: **Estudio de/em titulo del programa**

Modalidade: **online**

Duração: **# meses-semanas**


tech universidade tecnológica

Outorga o presente

CERTIFICADO

a

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

por ter concluído e aprovado com sucesso o programa de

MESTRADO PRÓPRIO

em

MBA em Gestão Avançada de Cibersegurança (CISO)

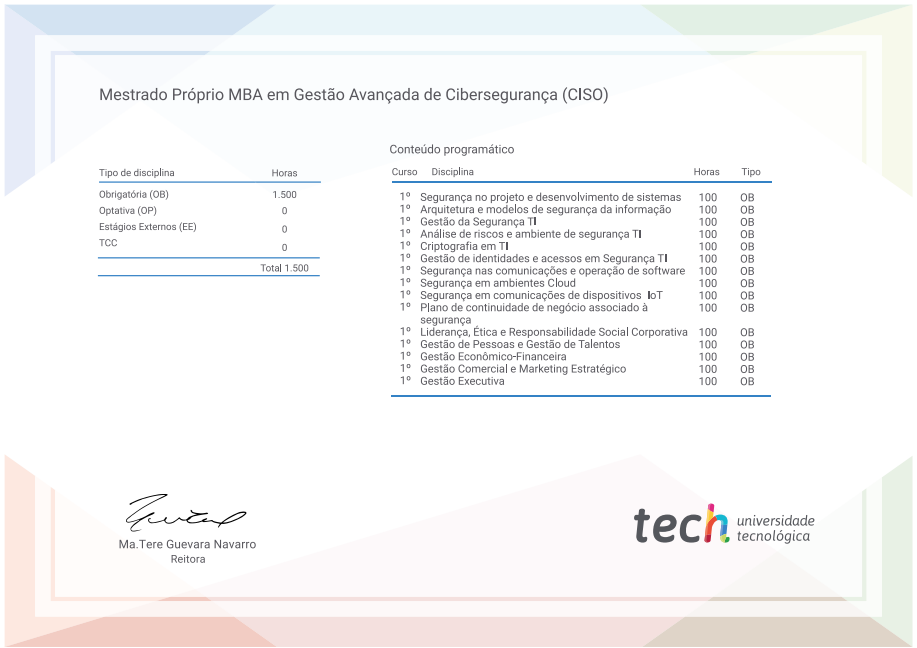
Este é um curso próprio desta Universidade, com duração de 1.500 horas, com data de início dd/mm/aaaa e data final dd/mm/aaaaa.

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

Em 17 de junho de 2020

Ma.Tere Guevara Navarro
Reitora

código único TECH: AFWOR23S techtitute.com/titulos


Mestrado Próprio MBA em Gestão Avançada de Cibersegurança (CISO)

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

Conteúdo programático

Curso	Disciplina	Horas	Tipo
1º	Segurança no projeto e desenvolvimento de sistemas	100	OB
1º	Arquitetura e modelos de segurança da informação	100	OB
1º	Gestão da Segurança TI	100	OB
1º	Análise de riscos e ambiente de segurança TI	100	OB
1º	Criptografia em TI	100	OB
1º	Gestão de identidades e acessos em Segurança TI	100	OB
1º	Segurança nas comunicações e operação de software	100	OB
1º	Segurança em ambientes Cloud	100	OB
1º	Segurança em comunicações de dispositivos IoT	100	OB
1º	Plano de continuidade de negócio associado à segurança	100	OB
1º	Liderança, Ética e Responsabilidade Social Corporativa	100	OB
1º	Gestão de Pessoas e Gestão de Talentos	100	OB
1º	Gestão Econômico-Financeira	100	OB
1º	Gestão Comercial e Marketing Estratégico	100	OB
1º	Gestão Executiva	100	OB

Ma.Tere Guevara Navarro
Reitora

tech universidade tecnológica

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

tech universidade tecnológica

Mestrado Próprio
MBA em Gestão Avançada de Cibersegurança (CISO)

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

Mestrado Próprio

MBA em Gestão Avançada de Cibersegurança (CISO)

tech universidade tecnológica