Mestrado Próprio
Gestão Avançada de Cibersegurança

tech universidade tecnológica

tech universidade tecnológica

Mestrado Próprio
Gestão Avançada de Cibersegurança

- Modalidade: **online**
- Duração: **12 meses**
- Certificação: **TECH Universidade Tecnológica**
- Créditos: **60 ECTS**
- Tempo Dedicado: **16 horas/semana**
- Horário: **ao seu próprio ritmo**
- Exames: **online**

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

Índice

01

Apresentação

O mundo atual está a avançar para uma digitalização completa. Cada vez mais processos, operações e tarefas de todos os tipos são realizados através de um dispositivo eletrónico. Mas este progresso também comporta certos riscos, uma vez que computadores, *smartphones*, *tablets* e todos os tipos de aplicações digitais podem ser suscetíveis de ataques cibernéticos. Por esta razão, muitas empresas procuram especialistas que possam efetivamente liderar e gerir a cibersegurança dos seus serviços. Este novo perfil profissional é muito procurado, pelo que este programa foi concebido para proporcionar os conhecimentos e técnicas mais atualizados ao informático, que estará preparado para ser o diretor da cibersegurança em qualquer empresa que o deseje.

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

Nos últimos anos, o processo de digitalização acelerou, impulsionado pelos avanços contínuos na informática. Assim, não só a tecnologia tem beneficiado de grandes melhorias, como também as próprias ferramentas digitais com as quais muitas tarefas são hoje realizadas. Por exemplo, estes progressos tornaram possível a realização de muitas transações bancárias a partir de uma aplicação móvel. Houve também 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 levaram também a um aumento das vulnerabilidades informáticas. Assim, embora as opções para a realização de várias atividades e tarefas tenham aumentado, os ataques à segurança de dispositivos, aplicações e websites aumentaram proporcionalmente. Por esta razão, cada vez mais companhias procuram profissionais especializados em cibersegurança capazes de lhes proporcionar proteção adequada contra todos os tipos de ataques informáticos.

Assim, o perfil do Diretor de Cibersegurança é um dos mais procurados pelas empresas que operam na Internet ou que têm serviços no ambiente digital. E para responder a esta exigência, a TECH concebeu este Mestrado Próprio em Gestão Avançada de Cibersegurança, que fornecerá ao informático todas as ferramentas necessárias para levar a cabo esta função de forma eficaz e tendo em conta os últimos desenvolvimentos em matéria de proteção e vulnerabilidades neste campo tecnológico.

Neste programa poderá estudar em profundidade aspetos como a segurança no desenvolvimento e conceção de sistemas, e as melhores técnicas criptográficas e a segurança em ambientes *Cloud Computing*. Fá-lo-á através de uma metodologia 100% online com a qual poderá combinar o seu trabalho profissional com os seus estudos, sem horários rígidos ou viagens desconfortáveis a um centro académico. Além disso, com numerosos recursos didáticos multimédia, ministrados pelo pessoal docente mais prestigiado e especializado da cibersegurança.

Este **Mestrado Próprio em Gestão Avançada de Cibersegurança** 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 e cibersegurança
- Os conteúdos gráficos, esquemáticos e eminentemente práticos com que está concebido fornece informações científicas e práticas sobre as disciplinas que são essenciais para a prática profissional
- Exercícios práticos onde o processo de autoavaliação pode ser levado a cabo a fim de melhorar a aprendizagem
- A sua ênfase especial em metodologias inovadoras
- Palestras 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"

Irá beneficiar de inúmeros conteúdos multimédia para acelerar o seu processo de aprendizagem, enquanto recebe o apoio de um corpo docente de grande prestígio no domínio da cibersegurança"

A Metodologia online da TECH permitir-lhe-á escolher a hora e o local para estudar, sem perturbar o seu trabalho profissional.

Poderá tornar-se o Diretor de Segurança Cibernética das melhores empresas da sua área.

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

Graças ao seu conteúdo multimédia, desenvolvido com a mais recente tecnologia educacional, o profissional terá acesso a uma aprendizagem situada e contextual, ou seja, um ambiente de simulação que proporcionará um programa imersivo programado para se formar em situações reais.

A conceção deste programa baseia-se na Aprendizagem Baseada nos Problemas, através da qual o instrutor deve tentar resolver as diferentes situações da atividade profissional que surgem ao longo do curso académico. Para tal, contará com a ajuda de um sistema inovador de vídeo interativo desenvolvido por especialistas reconhecidos.

02

Objetivos

O rápido desenvolvimento das tecnologias informáticas trouxe grandes avanços, prestando muitos serviços à população em geral. Contudo, o número de vulnerabilidades e ciberataques também aumentou, razão pela qual o principal objetivo deste Mestrado Próprio é transformar o informático num verdadeiro especialista na gestão da cibersegurança, garantindo um enorme e imediato progresso profissional. As suas novas competências dar-lhe-ão a oportunidade de ter acesso a grandes empresas digitalmente ativas em vários setores.

O objetivo deste programa é fazer de si um profissional preparado para dirigir 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 esteganoanálise
- 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 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 Próprio, que possui o conhecimento mais avançado 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 atividades 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 maximizemos uma 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, números grandes, 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 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
- Desenvolver 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 Plano de Continuidade do 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 um Plano de Continuidade para o Negócio

03

Competências

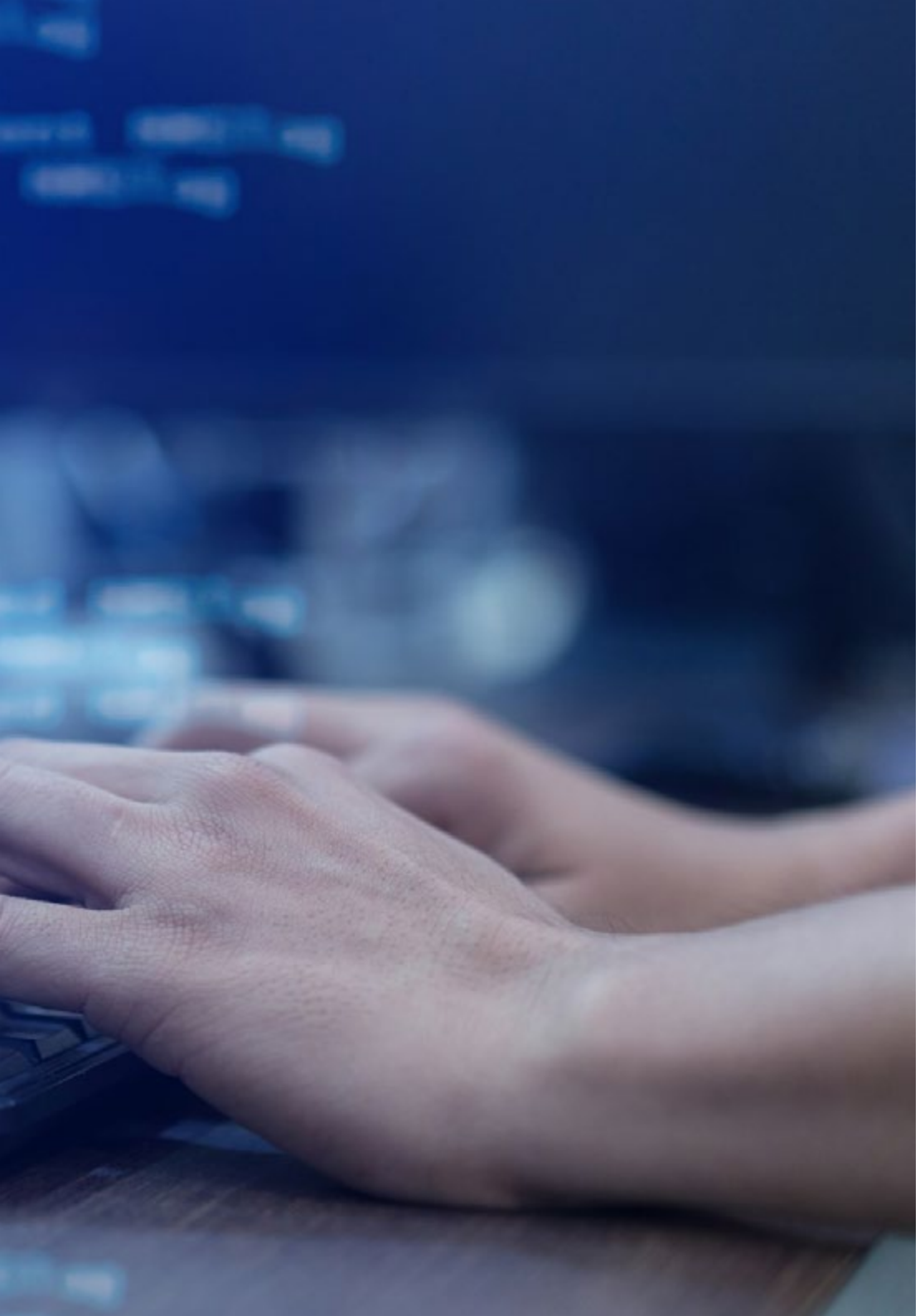
Graças a este Mestrado Próprio, o profissional irá adquirir inúmeras novas competências na área da cibersegurança. O aparecimento nos últimos anos de tecnologias como a *Blockchain*, o *Cloud Computing* ou a inteligência artificial levou ao desenvolvimento de novas áreas de cibersegurança. Por essa razão, este programa foi especialmente concebido para fornecer ao profissional todas as competências necessárias para se adaptar a estas tecnologias em plena expansão.

As competências que este Mestrado Próprio lhe proporcionará permitir-lhe-ão atualizar-se e adaptar-se ao novo ambiente informático, onde tecnologias como a Blockchain ou a 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
- Desenvolver as melhores práticas no desenvolvimento seguro
- Apresentar os riscos para as empresas de não terem um ambiente informático seguro

Não só irá melhorar as suas capacidades de cibersegurança, como também se irá preparar para liderar este departamento em qualquer grande empresa de Internet ou na esfera digital"



Competências específicas

- Desenvolver um Sistema de Gestão de Segurança da Informação (SGSI)
- Identificar os elementos-chave que conformam um SGSI
- Aplicar a metodologia MAGERIT para fazer evoluir o modelo e levá-lo um nível mais avançado
- Conceber novas metodologias de gestão de riscos próprios, com base no conceito *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 contribuição de valor próprio
- 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 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 grande complexidade da cibersegurança atual exige uma aprendizagem abrangente e detalhada. Por esta razão, a TECH encarregou-se de reunir o melhor corpo docente especializado nesta área. Assim, o profissional desfrutará do acompanhamento e supervisão de um corpo docente atualizado com os últimos avanços nesta área, de modo a poder incorporar as melhores técnicas de cibersegurança no seu trabalho diário, ao mesmo tempo que adquire as competências de gestão necessárias nesta área.

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

Direção

Sr. Martín Olalla Bonal

- Client Technical Specialist Blockchain na IBM
- Arquiteto *Blockchain*
- Arquiteto de Infraestrutura na Banca
- Gestão de projetos e implementação de soluções
- Técnico em Eletrónica Digital
- Docente: Formação *Hyperledger Fabric* para empresas
- Docente: Formação *Blockchain* orientado para negócio em empresas

Professores

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 Eletrónica Industrial pela Universidade Pontifícia de Comillas ICAI
- Mestrado em Gestão de Seguros pelo ICEA (Instituto para la Colaboración entre Entidades Aseguradoras)

Dr. Alejandro Entrenas

- Entelgy Innotec
- Innovery España
- Atos Spain
- Licenciatura em Engenharia Técnica em Informática de Sistemas pela Universidade de Córdova
- Mestrado em Gestão da Segurança da Informação na Universidade Politécnica de Madrid

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 Universidade de Tecnologia e Economia de Budapeste (BME)
- Licenciatura em Engenharia de Organização Industrial

Dr. Antonio Gómez Rodríguez

- Engenheiro de soluções Cloud na Oracle
- Diretor de Projetos em Sopra Group
- Diretor de Projetos em Everis
- Chefe de Projetos na Empresa pública de Gestão de Programas Culturais Secretaria de Cultura de Andaluzia
- Analista de Sistemas de Informação. Sopra Group
- Licenciado em Engenharia de Telecomunicações pela Universidade Politécnica da Catalunha
- Pós-graduação em Tecnologias e Sistemas de Informação do Instituto Catalão de Tecnologia
- E-Business Master pela Escola de Negócios La Salle

Dr. Jorge del Valle Arias

- Smart Cities Business Growth Manager Spain em Itron Inc
- Consultor IoT
- Diretor da Divisão IoT na Diode Espanha
- Sales Manager IoT & Celular em Aicox Soluciones
- Fundador e CEO de Sensor Intelligence
- Diretor de Operações em Codium Networks
- Chefe de Área de Eletrónica em Aitemin
- Engenheiro de Telecomunicações pela Universidade Politécnica de Madrid
- Executive MBA pela International Graduate School de La Salle de Madrid

Dr. Juan Luis Gozalo Fernández

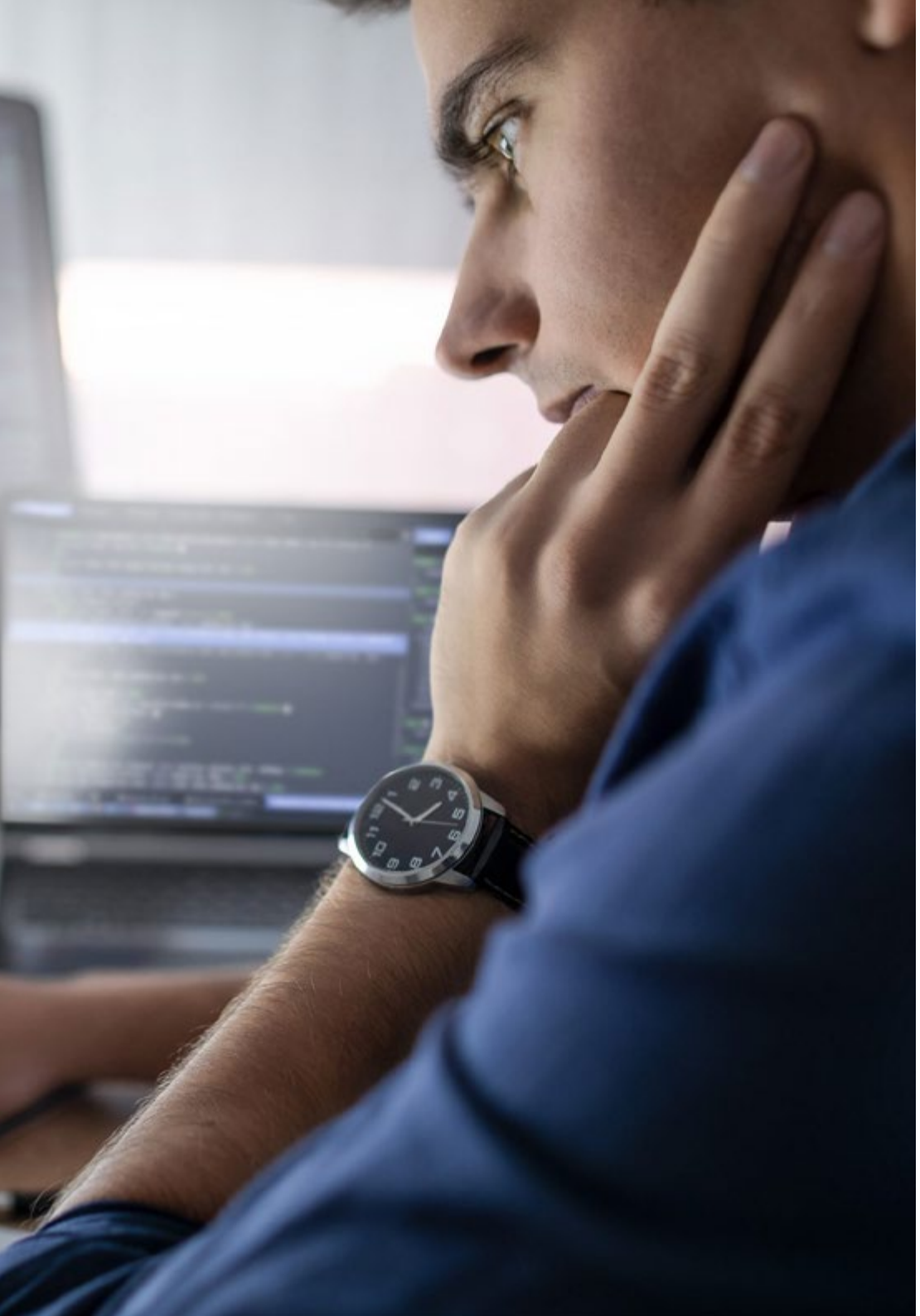
- Engenheiro Informático
- Diretor Blockchain DevOps na Alastria
- Diretor Desenvolvimento Aplicação Móvel Tinkerlink em Cronos Telecom
- Diretor Informático em Banco Santander
- Diretor Tecnologia Gestão de Serviço IT em Barclays Bank Espanha
- Licenciado em Engenharia Superior Informático pela Universidade Nacional de Educação à Distância (UNED)

Dra. Lorena Jurado Jabonero

- Chefe de Segurança da Informação (CISO) no Grupo Pascual
- Licenciada em Engenharia Informática pela Universidade Alfonso X El Sabio
- Engenheira Técnico em Informática de Gestão pela Universidade Politécnica de Madrid
- Conhecimentos: ISO 27001, ISO 27701, ISO 22301, ISO 20000, RGPD/LOPDGDD, NIST CSF, CSA, ITIL, PCI, etc.

Sr. Octavio Ortega

- Programador de Aplicações Informáticas e Desenvolvimento Web.
- Web Design e APPS para clientes, CRDS para Investigações realizadas pelo Instituto de Salud Carlos III, lojas online, aplicações Android, etc
- Docente Segurança Informática
- Licenciado em Psicologia pela Universidade Oberta de Catalunya
- Técnico Superior Universitário em Análise, Design e Soluções de Software
- Técnico Superior Universitário em Programação Avançada



Sr. Mario Embid Ruiz

- Advogado especializado em Direito TIC e proteção de dados
- Responsável Jurídico da Branddocs, SL, empresa tecnológica de soluções de confiança
- Licenciatura em Direito e Administração de Empresas pela Universidade Rey Juan Carlos
- Mestrado em Direito das Novas Tecnologias, Internet e Audiovisual pelo Centro de Estudos Universitários Villanueva e Cremades & Calvo Sotelo

Sr. Juan Manuel Rodrigo Estébanez

- Fundador da ISMET TECH S.L
- Licenciatura em Engenharia pela Universidade de Valladolid
- Mestrado em Sistemas de Gestão Integrada pela CFE-CEU
- ISO 27001 Lead Auditor (IMQ)
- ISO 27001 Lead Auditor (IMQ)
- NATO Standards HPS (OTAN)

05

Estrutura e conteúdo

Este programa está estruturado em 10 módulos especializados que permitirão ao profissional 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 em comunicações e operação software ou o desenvolvimento do plano de continuidade do negócio associado à segurança. Isto permitirá ao informático obter uma compreensão abrangente de todas as questões relevantes da atual cibersegurança.

Não encontrará conteúdo mais completo e inovador do que este para se especializar na gestão avançada de 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 sistema 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 sistema 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 sistema de informação
- 1.8.1 Plano de segurança. Objetivos
- 1.8.2 Plano de segurança. Planificação
- 1.8.3 Plano de riscos Análises
- 1.8.4 Políticas 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 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 de risco
- 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 de *red team*
- 3.8.3 Auditorias de código fonte Desenvolvimento seguro
- 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 Esteganoanálise
- 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. Plano 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)

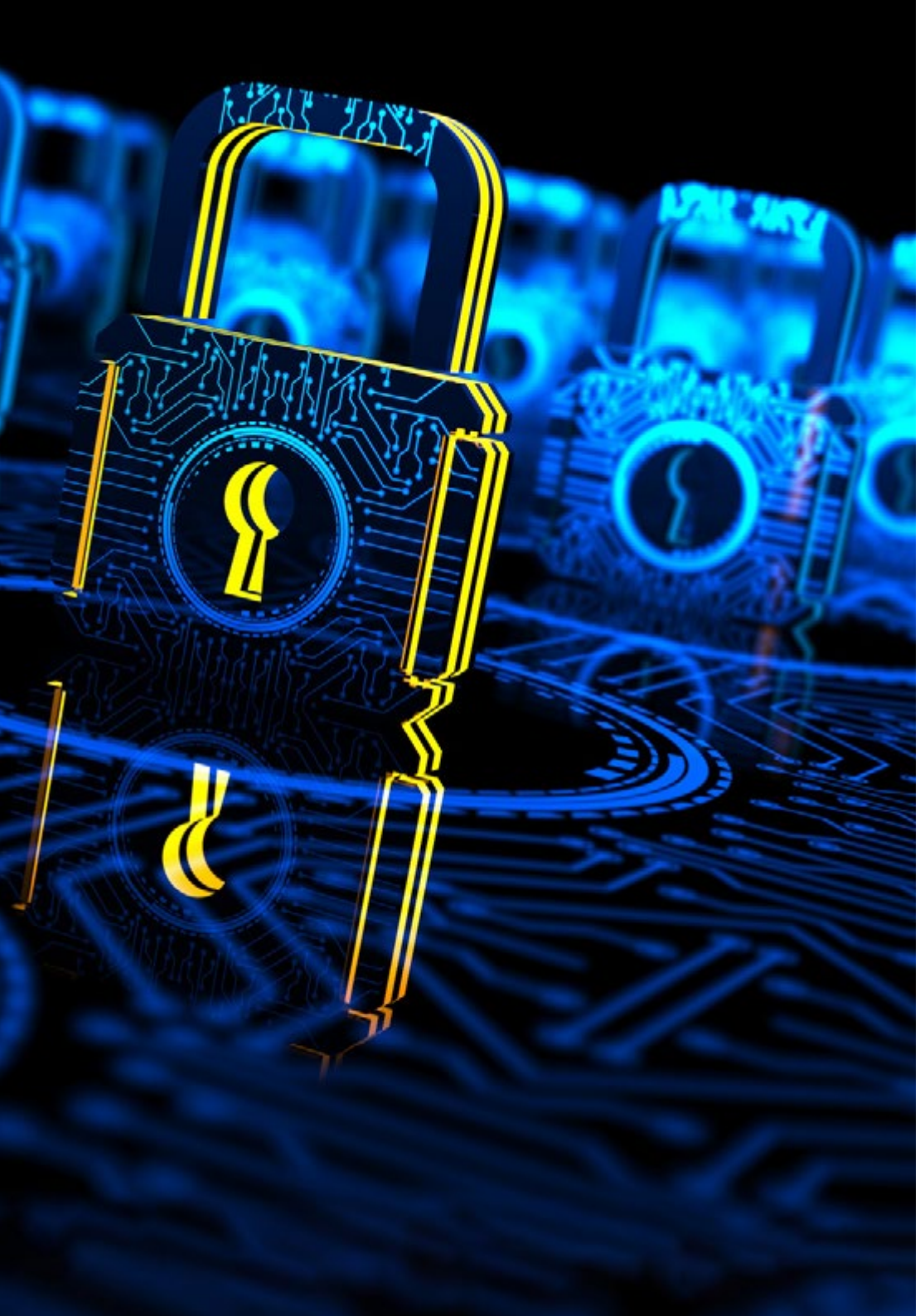
10.4. Gestão de riscos associada ao PCN
- 10.4.1. Análise de impacto no negócio
- 10.4.2. Benefícios da implementação de um PCN
- 10.4.3. Mentalidade baseada em riscos

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. Documentos a entregar

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. Documentos a entregar



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. Documentos a entregar
10.10. Normas ISO associadas aos planos de Continuidade de Negócios (PCN)
  10.10.1. ISO 22301:2019
  10.10.2. ISO 22313:2020
  10.10.3. Outras normas ISO e internacionais relacionadas

O melhor pessoal docente e o sistema inovador de ensino são combinados com o programa mais completo e atualizado: está perante uma grande oportunidade de progredir como informático"

06

Metodologia

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

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

Estudo de Caso para contextualizar todo o conteúdo

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

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

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

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

Um método de aprendizagem inovador e diferente

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

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

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

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

Relearning Methodology

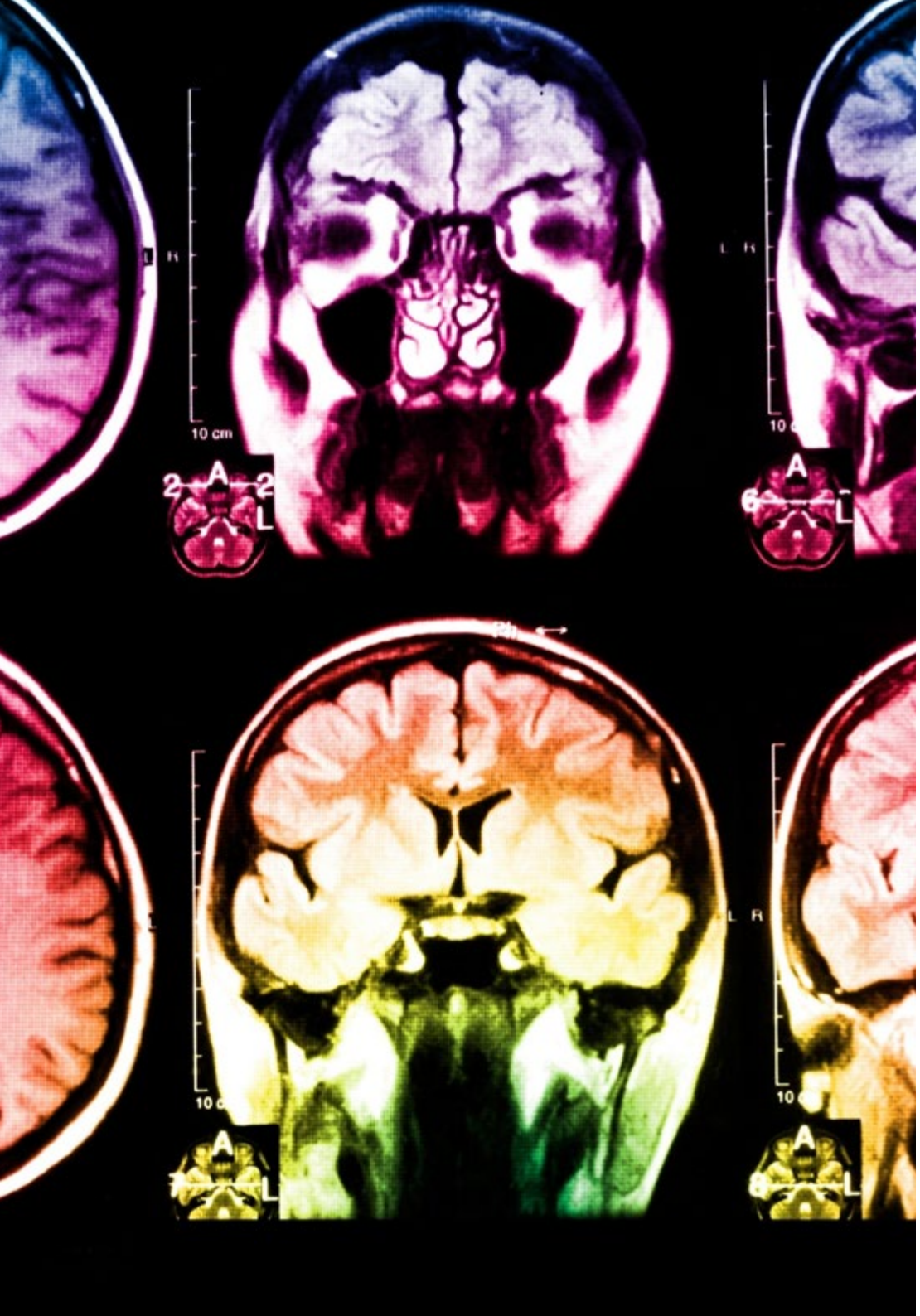
A TECH combina eficazmente a metodologia do Estudo de Caso com um sistema de aprendizagem 100% online baseado na repetição, que combina elementos didáticos diferentes em cada lição.

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

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

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

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



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

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

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

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

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

Material de estudo

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

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

Masterclasses

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

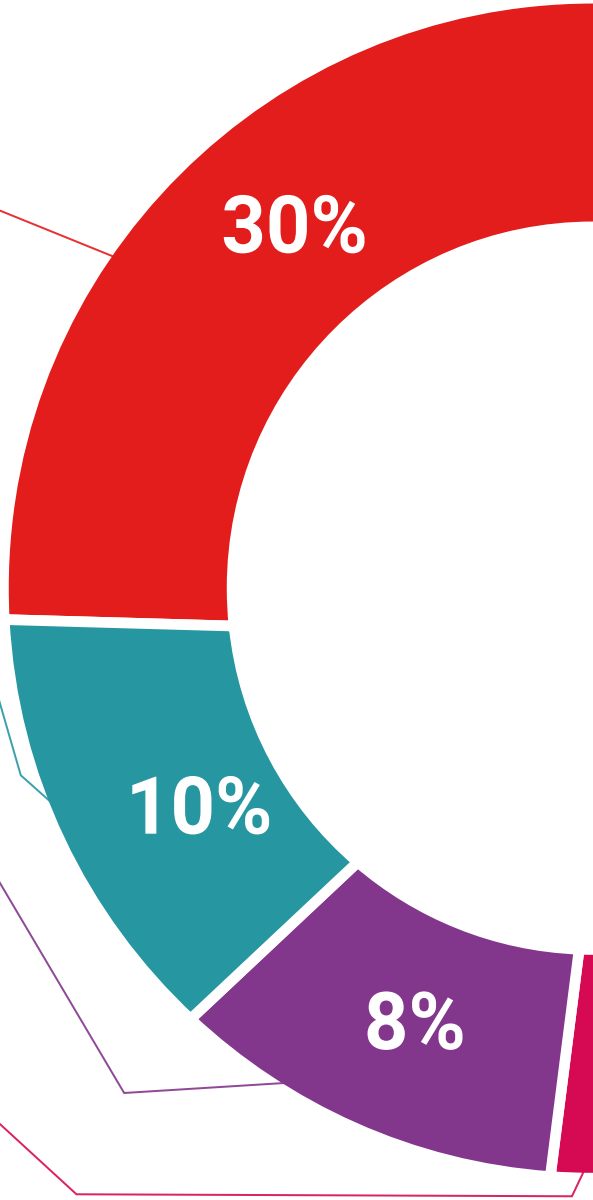
O denominado Learning from an Expert constrói conhecimento e memória, e gera confiança em futuras decisões difíceis.

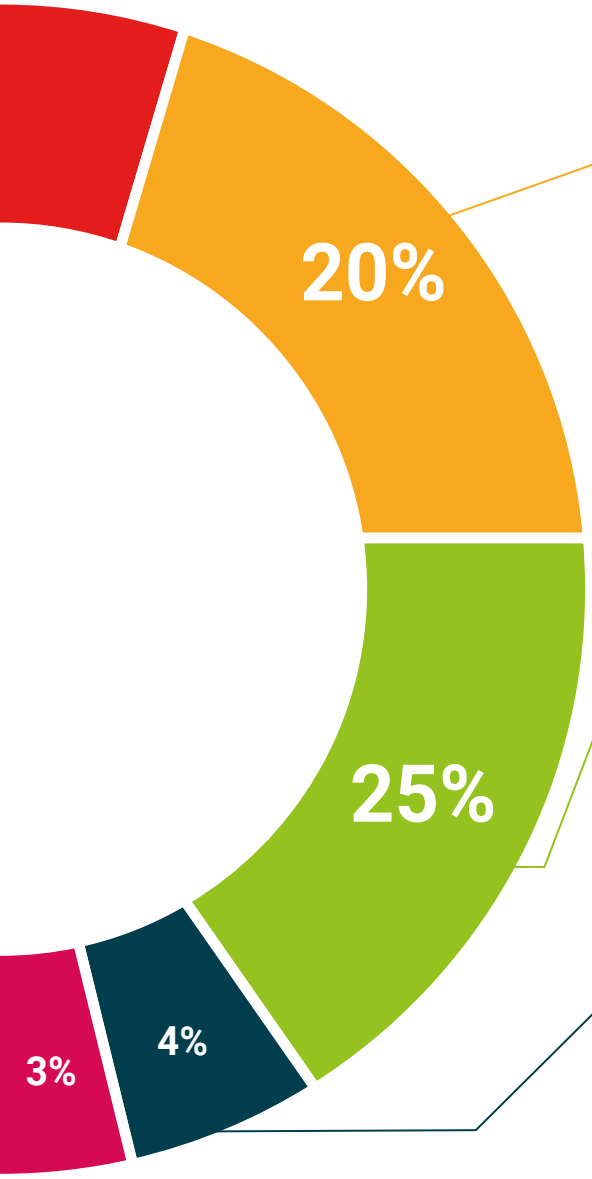
Práticas de aptidões e competências

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

Leituras complementares

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





Case studies

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

Resumos interativos

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

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

Testing & Retesting

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

07

Certificação

O Mestrado Próprio em Gestão Avançada de Cibersegurançade Cibersegurança garante, para além do conteúdo mais rigoroso e atualizado, o acesso a um grau de Mestre emitido pela TECH Universidade Tecnológica.

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

Este **Mestrado Próprio em Gestão Avançada de Cibersegurança** conta com o conteúdo educacional mais completo e atualizado do mercado.

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

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

Certificação: **Mestrado Próprio em Gestão Avançada de Cibersegurança**

ECTS: **60**

Carga horária: **1.500 horas**

tech universidade tecnológica

Concede o presente

CERTIFICADO

a

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

Por ter concluído e acreditado com sucesso o

MESTRADO PRÓPRIO

em

Gestão Avançada de Cibersegurança

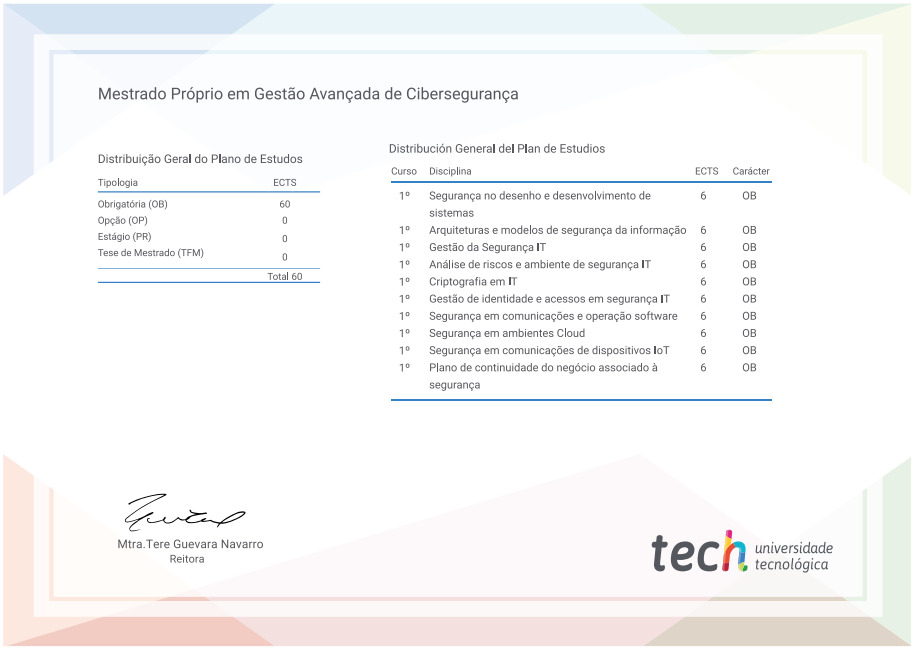
Este é um certificado atribuído por esta Universidade, reconhecido por 60 ECTS e equivalente a 1.500 horas, com data de início a dd/mm/aaaaa e data de conclusão a dd/mm/aaaaa.

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

A 17 de junho de 2020

Prof.Tere Guevara Navarro
Reitora

código único TECH: AFWOR23S techtitute.com/titulos



Mestrado Próprio em Gestão Avançada de Cibersegurança

Distribuição Geral do Plano de Estudos

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

Distribución General del Plan de Estudios

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

Mtra.Tere Guevara Navarro
Reitora

tech universidade tecnológica

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

tech universidade tecnológica

Mestrado Próprio
Gestão Avançada de Cibersegurança

- Modalidade: **online**
- Duração: **12 meses**
- Certificação: **TECH Universidade Tecnológica**
- Créditos: **60 ECTS**
- Tempo Dedicado: **16 horas/semana**
- Horário: **ao seu próprio ritmo**
- Exames: **online**

Mestrado Próprio
Gestão Avançada de Cibersegurança

tech universidade tecnológica