Advanced Master
Alta Direção de Cibersegurança

tech universidade tecnológica

Advanced Master
Alta Direção de Cibersegurança

- Modalidade: **online**
- Duração: **2 anos**
- Certificação: **TECH Universidade Tecnológica**
- Créditos: **120 ECTS**
- Horário: **Ao seu ritmo**
- Exames: **online**

Acesso ao site: www.techtitute.com/pt/informatica/advanced-master/advanced-master-alta-direcao-ciberseguranca

Índice

01
Apresentação

No mundo atual, a cibersegurança é um elemento fundamental para os indivíduos e as empresas, que se encontram mais expostos do que nunca a ataques. Isto deve-se ao desenvolvimento contínuo de novas tecnologias e ao processo de digitalização, que provocou transformações em todos os tipos de empresas, agilizando muitas atividades, mas também provocando o aparecimento de novas vulnerabilidades. Por este motivo, um dos perfis mais procurados atualmente é o de gestor de cibersegurança, uma figura em crescimento com inúmeras oportunidades de carreira. Este curso investiga mais profundamente esta figura e prepara o informático para enfrentar, de forma eficaz e abrangente, todos os desafios que se colocam atualmente neste domínio, onde também são necessárias competências de gestão e uma perspetiva empresarial. Para além disso, o curso é desenvolvido num formato 100% online, o que o torna perfeito para o conciliar com o trabalho, permitindo ao profissional estudar quando quiser.

Este curso prepará-lo-á para enfrentar todos os desafios do presente e do futuro no domínio da cibersegurança, permitindo-lhe especializar-se na direção desta importante área da informática"

Processos bancários, compras na Internet, comunicações internas em diferentes organizações, procedimentos administrativos... Atualmente, a digitalização transformou a forma como os indivíduos e as empresas trabalham diariamente. Simplificou muitas atividades, tornou desnecessárias certas deslocações, melhorando a qualidade de vida da população e reduzindo os custos para as empresas. No entanto, estas vantagens trouxeram, colateralmente, outras desvantagens em termos de cibersegurança.

Muitas das tecnologias e ferramentas digitais utilizadas atualmente estão em constante desenvolvimento e, por isso, estão sujeitas a ataques. Com o uso generalizado de aplicações e dispositivos digitais, uma falha nestes é grave, pois pode afetar o desenvolvimento da organização, não só em termos de marketing e vendas, mas no seu próprio funcionamento interno, que também depende destas utilidades.

Por este motivo, é importante que as empresas disponham dos melhores especialistas no setor da saúde que possam dar resposta aos diferentes problemas que possam surgir neste domínio. Um dos perfis mais procurados é o de Diretor de Cibersegurança, um cargo que implica uma visão global desta área, e para o qual este Advanced Master oferece uma preparação completa. Assim, este curso é uma grande oportunidade para o informático, uma vez que o aproximará de todos os novos desenvolvimentos neste domínio, preparando-o, ao mesmo tempo, para enfrentar decisões de gestão, que exigem os melhores conhecimentos e capacidades de liderança.

Tudo isto, com base numa metodologia de aprendizagem online que se adapta às circunstâncias profissionais do aluno, sendo acompanhado por um corpo docente de grande prestígio nesta área da informática. Terá também à sua disposição a melhor tecnologia educativa e os mais recentes recursos didáticos: resumos interativos, vídeos, masterclasses, estudos de caso e leituras complementares.

Este **Advanced Master em Alta Direção de Cibersegurança** conta com o conteúdo educativo completo e atualizado do mercado. As suas principais características são:

- O desenvolvimento de casos práticos apresentados por especialistas em informática e cibersegurança
- O conteúdo gráfico, esquemático e eminentemente prático destes reúne informações científicas e práticas sobre as disciplinas essenciais para o exercício profissional
- Exercícios práticos onde o processo de autoavaliação pode ser levado a cabo a fim de melhorar a aprendizagem
- O seu especial foco em metodologias inovadoras na Direção de Cibersegurança
- Palestras teóricas, perguntas ao especialista, fóruns de discussão sobre questões controversas e atividades de reflexão individual
- Possibilidade de aceder ao conteúdo a partir de qualquer dispositivo fixo ou portátil com ligação à internet

Com este Advanced Master, poderá explorar a segurança da IoT, a cloud computing, a blockchain e aprenderá a efetuar auditorias de alto nível a todos os tipos de empresas e organizações".

A direção da cibersegurança é um perfil profissional em crescimento e este curso oferece-lhe a possibilidade, através da metodologia online da TECH, de aceder às melhores oportunidades neste domínio"

Desfrutará do apoio de um corpo docente altamente conceituado, que lhe garantirá a obtenção de todas as informações essenciais no domínio da direção da cibersegurança.

Terá à sua disposição os mais recentes recursos didáticos para garantir um processo de aprendizagem rápido e eficaz.

O seu corpo docente inclui profissionais da área da Cibersegurança que trazem a sua experiência para este programa, assim como especialistas reconhecidos de sociedades líderes e universidades de prestígio.

Graças ao seu conteúdo multimédia, desenvolvido com a mais recente tecnologia educativa, o profissional terá acesso a uma aprendizagem situada e contextual, ou seja, um ambiente de simulação que proporcionará um estudo 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, o profissional contará com a ajuda de um sistema inovador de vídeo interativo desenvolvido por especialistas reconhecidos.

02
Objetivos

O principal objetivo deste Advanced Master é transformar o informático num verdadeiro especialista neste domínio, permitindo-lhe beneficiar das melhores oportunidades profissionais. Não só abrangerá todos os desenvolvimentos mais recentes no domínio da cibersegurança, como também lhe proporcionará as melhores ferramentas para obter uma perspetiva global das necessidades das empresas neste domínio. Desta forma, poderá trabalhar na gestão da segurança das empresas em qualquer altura, conhecendo os melhores métodos para cada caso.

Este Advanced Master ajudá-lo-á a alcançar a evolução profissional que procura, graças ao seu conteúdo completo e atualizado e ao seu prestigiado corpo docente composto por especialistas que trabalham em cibersegurança"

Objetivos gerais

- Analisar o papel do analista de cibersegurança
- Aprofundar o conhecimento da engenharia social e dos seus métodos.
- Examinar as metodologias OSINT, HUMINT, OWASP, PTEC. OSSTM, OWISAM
- Realizar uma análise de risco e compreender as métricas de risco
- Determinar a utilização adequada do anonimato e o uso de redes como TOR, I2P e Freenet.
- Compilar os regulamentos vigentes em matéria de cibersegurança
- Produzir conhecimento especializado para a realização de uma Auditoria de Segurança
- Desenvolver políticas de uso apropriadas
- Examinar os sistemas de deteção e prevenção de ameaças mais importantes
- Avaliar os novos sistemas de deteção de ameaças, assim como a sua evolução a partir de soluções mais tradicionais
- Analisar as principais plataformas móveis atuais, as suas características e utilização.
- Identificar, analisar e avaliar os riscos de segurança das partes do projeto IoT
- Avaliar a informação obtida e desenvolver mecanismos de prevenção e hacking
- Aplicar a Engenharia Inversa ao ambiente da cibersegurança
- Especificar os testes a realizar ao software desenvolvido.
- Recolher todas as provas e dados existentes para levar a cabo um relatório forense
- Apresentar devidamente o relatório forense
- Analisar o estado atual e futuro da segurança informática
- Examinar os riscos das novas tecnologias emergentes
- Compilar as diferentes tecnologias relativas à segurança informática
- 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 adequado à organização
- Identificar os quadros regulamentares aplicáveis e as bases reguladoras dos mesmos
- Analisar a estrutura organizacional e funcional de uma área de segurança da informação (o departamento do CISO)
- Analisar e desenvolver o conceito de risco, incerteza dentro do ambiente em que vivemos
- Examinar o Modelo de Gestão de Riscos com base na norma ISO 31.000
- Examinar a ciência da criptologia e a relação com os seus ramos: criptografia, criptoanálise, esteganografia e estegoanálise
- Analisar os tipos de criptografia de acordo com o tipo de algoritmo e de acordo com a sua utilização
- Examinar os certificados digitais
- Examinar a Infraestrutura de Chave Pública (PKI)
- Desenvolver o conceito de gestão de identidades
- Identificar os métodos de autenticação
- Gerar um conhecimento especializado sobre o ecossistema de segurança Informática
- Avaliar o conhecimento em termos de cibersegurança
- Identificar os âmbitos de segurança em *Cloud*
- Analisar os serviços e ferramentas em cada um dos domínios da segurança
- Desenvolver as especificações de segurança de cada tecnologia LPWAN
- Analisar de forma comparativa a segurança das tecnologias LPWAN

Objetivos específicos

- Desenvolver metodologias utilizadas em matéria de cibersegurança
- Examinar o ciclo de inteligência e estabelecer a sua aplicação na ciberinteligência
- Determinar o papel do analista de inteligência e os obstáculos à atividade de evacuação
- Analisar as metodologias OSINT, OWISAM, OSSTM, PTES, OWASP
- Estabelecer as ferramentas mais comuns para a produção de inteligência.
- Conduzir uma análise de riscos e compreender as métricas utilizadas
- Concretizar as opções de anonimato e a utilização de redes como TOR, I2P, FreeNet
- Detalhar os regulamentos vigentes de cibersegurança
- Concretizar as políticas de *backup* de dados pessoais e profissionais
- Avaliar as diferentes ferramentas para fornecer soluções a problemas específicos de segurança
- Estabelecer mecanismos para ter o sistema atualizado
- Analisar a equipa para detetar intrusos
- Determinar as regras de acesso ao sistema
- Examinar e classificar os correios para evitar fraudes
- Gerar listas de software permitido
- Analisar as arquiteturas de rede atuais para identificar o perímetro que devemos proteger
- Desenvolver as configurações específicas de firewall e Linux para mitigar os ataques mais comuns
- Compilar as soluções mais usadas, tais como Snort e Suricata, assim como a sua configuração
- Examinar as diferentes camadas adicionais fornecidas pelos firewalls de nova geração e as funcionalidades de rede em ambientes *cloud*
- Identificar as ferramentas de proteção da rede e demonstrar porque são fundamentais para uma defesa multicamadas
- Examinar os diferentes vetores de ataque para evitar tornar-se um alvo fácil
- Determinar os principais ataques e tipos de malware a que os utilizadores de dispositivos móveis estão expostos
- Analisar os dispositivos mais recentes para estabelecer uma configuração mais segura
- Especificar os principais passos para realizar um teste de penetração tanto nas plataformas iOS como nas plataformas Android
- Desenvolver conhecimentos especializados sobre as diferentes ferramentas de proteção e segurança
- Definir as melhores práticas de programação para dispositivos móveis
- Analisar as principais arquiteturas IoT
- Examinar as tecnologias de conectividade
- Desenvolver os protocolos de aplicação principais
- Especificar os diferentes tipos de dispositivos existentes
- Avaliar os níveis de risco e vulnerabilidade conhecidas
- Desenvolver políticas de uso seguras
- Estabelecer as condições de utilização apropriadas para estes dispositivos
- Examinar os métodos IOSINT
- Reunir informação disponível nos meios públicos
- Digitalização de Redes para obter informação de modo ativo
- Desenvolver laboratórios de ensaio
- Analisar as ferramentas para o desempenho do *pentesting*

- Catalogar e avaliar as diferentes vulnerabilidades dos sistemas
- Concretizar as diferentes metodologias de hacking
- Analisar as fases de um compilador
- Examinar a arquitetura de processadores x86 e a arquitetura de processadores ARM
- Determinar os diferentes tipos de análise
- Aplicar sandboxing em diferentes ambientes
- Desenvolver as diferentes técnicas de análise de malware
- Estabelecer as ferramentas para análise de malware
- Estabelecer os requisitos necessários para o correto funcionamento de uma aplicação.
- de forma segura
- Examinar ficheiros de registo para compreender mensagens de erro
- Analisar os diferentes eventos e decidir o que mostrar ao utilizador e o que guardar nos registos
- Gerar um Código de qualidade sanitizado, facilmente verificável
- Avaliar a documentação apropriada para cada fase do desenvolvimento
- Concretizar o comportamento do servidor para otimizar o sistema
- Desenvolver código modular, reutilizável e de fácil manutenção.
- Identificar os diferentes elementos que põem em evidência um delito
- Gerar conhecimentos especializados para obter dados de diferentes meios de comunicação antes que estes se percam
- Recuperar dados apagados intencionalmente
- Analisar os registos e os logs dos sistemas
- Determinar como são duplicados os dados de modo a não alterar os originais

- Fundamentar as provas para sejam consistentes
- Gerar um relatório sólido e sem falhas
- Apresentar as conclusões de forma coerente
- Estabelecer como defender o relatório perante a autoridade competente
- Desenvolver estratégias para que o teletrabalho seja seguro
- Conhecer os princípios sintáticos da linguagem gráfica e aplicar as suas regras para descrever objetos e ideias de forma clara e precisa
- Conhecer a origem das letras e a sua importância histórica
- Reconhecer, estudar e aplicar a tipografia aos processos gráficos de forma coerente
- Conhecer e aplicar os fundamentos estéticos da tipografia
- Saber analisar a disposição dos textos no objeto de ***design***
- Ser capaz de realizar trabalhos profissionais baseados na composição tipográfica
- 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
- 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 de funcionários, fornecedores e parceiros
- 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
- Identificar as diferentes estruturas que pode ter uma área de segurança de 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 catividades a serem realizadas após um incidente de segurança
- Configurar um centro de comando de segurança da informação que englobe todos os intervenientes relevantes (autoridades, clientes, fornecedores, etc.)
- 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 nos permitam lidar com os riscos e oportunidades de forma a maximizar a nossa contribuição de valor
- Examinar em profundidade as diferentes técnicas de transferência de riscos, assim como de valor
- Gerar valor a partir da conceção de modelos próprios para a gestão ágil de riscos
- Examinar os resultados para propor melhorias contínuas na gestão de projetos e processos baseados em modelos de gestão promovidos pelo risco ou *risk-driven*
- Inovar e transformar dados gerais em informação relevante para a tomada de decisões baseadas no risco
- Reunir 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
- 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
- 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 de informação
- Fundamentar o funcionamento de um centro de operações de cibersegurança
- Demonstrar a importância das práticas de cibersegurança para as catástrofes organizacionais
- Identificar riscos de uma implantação de infraestrutura em *cloud* pública
- Definir os requisitos de segurança
- Desenvolvimento de um plano de segurança para a implantação em *cloud*
- Identificar os serviços *cloud* a implementar para a execução de um plano de segurança
- Determinar as disposições operacionais necessárias para os mecanismos de prevenção
- Estabelecer as diretrizes para um sistema de *logging* e monitorização
- Propor ações de resposta a incidentes
- 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
- Apresentar os elementos-chave de cada fase e analisar as caraterísticas do Plano de Continuidade de Negócio (PCN)
- Fundamentar a necessidade de um Plano de Continuidade para o Negócio
- Determinar os mapas de sucesso e de risco para cada fase do o Plano de Continuidade de Negócio
- Especificar como é estabelecido um Plano de Ação para a implementação
- Avaliar a integridade de um Plano de Continuidade de Negócio (PCN)
- Desenvolver o Plano para a Implementação com êxito de um Plano de Continuidade para o nosso Negócio

03

Competências

Ao longo deste Advanced Master, o profissional adquirirá uma série de ferramentas e competências que lhe permitirão trabalhar na direção de cibersegurança de uma grande empresa. Por essa razão, este curso não se centra apenas nos aspetos informáticos, mas foca-se também no processo de digitalização, nas tecnologias emergentes e na forma como estes elementos afetaram as atividades comuns e quotidianas das organizações. Desta forma, o aluno poderá adaptar-se ao contexto atual, conhecendo as melhores soluções de segurança para cada empresa.

Melhore as suas competências para se tornar no melhor especialista em cibersegurança do seu meio"

Competências gerais

- Conhecer as metodologias utilizadas em matéria de cibersegurança
- Saber avaliar cada tipo de ameaça para fornecer uma solução adequada a cada caso
- Ser capaz de desenvolver soluções inteligentes completas para automatizar o comportamento em caso de incidentes
- Saber avaliar os riscos associados às vulnerabilidades, tanto dentro como fora da empresa
- Compreender a evolução e o impacto da IdC ao longo do tempo
- Ser capaz de demonstrar que um sistema é vulnerável, atacando-o preventivamente e resolvendo esses problemas
- Saber aplicar *sandboxing* em diferentes ambientes
- Conhecer as diretrizes que um bom programador deve seguir a fim de cumprir os requisitos de segurança necessários
- 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 potenciais riscos da própria conceção
- 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 que as empresas correm por não disporem de um ambiente de segurança informática

Este curso conduzi-lo-á ao futuro da cibersegurança"

Competências específicas

- Saber realizar operações de segurança defensiva
- Ter uma perceção profunda e especializada sobre a segurança informática
- Possuir conhecimentos especializados no domínio da cibersegurança e da ciberinteligência
- Possuir conhecimentos aprofundados sobre aspetos fundamentais como o ciclo de inteligência, fontes de inteligência, engenharia social, metodologia OSINT/HUMINT, anonimização, análise de risco, metodologias existentes (OWASP, OWISAM, OSSTM, PTES) e regulamentos vigentes em matéria de cibersegurança
- Compreender a importância de conceber uma defesa multicamadas, também conhecida como "Defense in Depth", que cubra todos os aspetos de uma rede corporativa onde alguns dos conceitos e sistemas que veremos também podem ser utilizados e aplicados num ambiente doméstico
- Saber como aplicar processos de segurança para smartphones e dispositivos portáteis
- Conhecer os meios para levar a cabo o chamado hacking ético e proteger uma empresa de um ciberataque
- Ser capaz de investigar um incidente de cibersegurança
- Conhecer as diferentes técnicas de ataque e defesa disponíveis
- Analisar o papel do Diretor de Segurança da Informação (Chief Information Security Officer)
- Conhecer o funcionamento da engenharia social e dos seus métodos
- Desenvolver um Sistema de Gestão de Segurança da Informação(SGSI)
- Identificar os elementos chaves que conformam um SGSI
- Aplicar a metodologia MAGERIT para fazer evoluir o modelo e levá-lo um nível mais avançado
- Conceber novas metodologias próprias de gestão de riscos, com base no conceito *agile risk management*
- Identificar, analisar, avaliar e abordar os riscos enfrentados pelo profissional a partir de uma nova perspetiva empresarial baseada num modelo *risk-driven* ou movido pelo risco não só para sobreviver no seu próprio ambiente, mas também para impulsionar a sua própria contribuição de valor
- Examinar o processo de desenho de uma estratégia de segurança ao implantar serviços empresariais em *Cloud*
- Avaliar as diferenças nas implementações concretas de diferentes vendedores de *cloud* pública
- Avaliar as opções de conetividade de IoT para abordar um projeto, com especial ênfase nas tecnologias LPWAN
- Apresentar as especificações básicas das principais tecnologias LPWAN para a IoT

04

Direção do curso

A TECH compilou a informação mais atualizada do modelo no domínio da gestão de sistemas de informação para que os informáticos possam encontrar, num único programa, o suporte didático de que necessitam para melhorar a sua formação e tornar-se um Chief Information Officer de sucesso. Sem dúvida, um Advanced Master que marcará um antes e um depois na sua educação e que lhes dará a oportunidade de aumentar as suas opções de empregabilidade.

Um plano de estudos completo que lhe apresentará os conceitos mais recentes em gestão empresarial e sistemas informáticos para se tornar um Chief Information Officer de sucesso"

Diretor Internacional Convidado

O Dr. Frederic Lemieux é reconhecido internacionalmente como um especialista inovador e líder inspirador nos domínios dos Serviços Secretos, Segurança Nacional, Segurança Interna, Cibersegurança e Tecnologias Disruptivas. A sua dedicação constante e as suas contribuições relevantes para a Investigação e a Educação tornam-no numa figura-chave na promoção da segurança e da compreensão das atuais tecnologias emergentes. Durante a sua carreira profissional, concebeu e dirigiu cursos académicos de vanguarda em várias instituições de renome, incluindo a Universidade de Montreal, a Universidade George Washington e a Universidade de Georgetown.

Ao longo da sua longa trajetória, publicou vários livros importantes, todos relacionados com a inteligência criminal, a polícia, as ciberameaças e a segurança internacional. Também contribuiu significativamente para o domínio da Cibersegurança, publicando numerosos artigos em revistas académicas, que analisam o controlo da criminalidade durante grandes catástrofes, a luta contra o terrorismo, as agências de informação e a cooperação policial. Além disso, foi painelista e orador principal em várias conferências nacionais e internacionais, afirmando-se como uma referência na esfera académica e profissional.

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

Dr. Frederic Lemieux

- Investigador em Inteligência, Cibersegurança e Tecnologias Disruptivas na Universidade de Georgetown
- Diretor do Mestrado em Information Technology Management na Universidade de Georgetown
- Diretor do Mestrado Technology Management na Universidade de Georgetown
- Diretor do Mestrado em Cybersecurity Risk Management na Universidade de Georgetown
- Diretor do Mestrado em Applied Intelligence na Universidade de Georgetown
- Professor de Estágio na Universidade de Georgetown
- Doutoramento em Criminologia pela School of Criminology na Universidade de Montreal
- Licenciatura em Sociologia, Minor Degree em Psicologia, pela Universidade de Laval
- Membro de: New Program Roundtable Committee, pela Universidade de Georgetown

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

Direção

Dra. Sonia Fernández Sapena

- Formador em Segurança Informática e Hacking Ético no Centro de Referência Nacional de Informática e Telecomunicações
- Formador em Segurança Informática e Hacking Ético no Centro de Referência Nacional de Getafe de Informática e Telecomunicações de Madrid
- Instutora certificada E-Council
- Formadora nas seguintes certificações: EXIN Ethical Hacking Foundation e EXIN Cyber & IT Security Foundation. Madrid
- Formador especializado certificado pela CAM para os seguintes certificados de profissionalização: Segurança Informática (IFCT0190), Gestão de Redes de Voz e Dados (IFCM0310), Administração de Redes Departamentais (IFCT0410), Gestão de Alarmes em Redes de Telecomunicações (IFCM0410), Operador de Redes de Voz e Dados (IFCM0110), e Administração de Serviços de Internet (IFCT0509)
- Colaboradora externa CSO/SSA (*Chief Security Officer/Senior Security Architect*) Universidade das Ilh as Baleares
- Engenheira em Informática pela Universidade de Alcalá de Henares de Madrid
- Mestrado em DevOps: Docker and Kubernetes. Cas-Training
- Microsoft Azure Security Techonologies. E-Council

Dr. Martín Olalla Bonal

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

Professores

Dra. Victoria Alicia Marcos Sbarbaro

- Programadora de Aplicações Móveis Android Nativas na B60 UK
- Analista Programadora para a Gestão, Coordenação e Documentação do Ambiente Virtualizado de Alarmes de Segurança
- Analista Programadora de Aplicações Java para caixas de multibanco
- Profissional de Desenvolvimento de *Software* para Aplicação de Validação de Assinaturas e Gestão Documental
- Técnica de Sistemas para a Migração de Equipamentos e para a Gestão, Manutenção e Formação de Dispositivos Móveis PDA
- Engenheira Técnica de Informática de Sistemas pela Universidade Oberta de Cataluña
- Mestrado em Segurança Informática e Hacking Ético Oficial EC- Council e CompTIA pela Escola Profissional de Novas Tecnologias CICE

Dr. Jon Peralta Alonso

- Consultor Sénior de Proteção de Dados e Cibersegurança na Altia
- Advogado / Consultor Jurídico na Arriaga Asociados Asesoramiento Jurídico y Económico S.L.
- Consultor Jurídico / Estagiário num Escritório Profissional: Óscar Padura
- Licenciatura em Direito pela Universidade Pública do País Basco
- Mestrado em Delegado de Proteção de Dados pela EIS Innovative School
- Mestrado Universitário em Advocacia pela Universidade Pública do País Basco
- Mestrado Especializado em Prática de Direito Processual Civil pela Universidade Internacional Isabel I de Castela
- Docente do Mestrado em Proteção de Dados Pessoais, Cibersegurança e Direito das TIC

Dr. Jesús Serrano Redondo

- Programador Web e Técnico de Cibersegurança
- Programador Web na Roams, Palencia
- Programador *FrontEnd* na Telefónica, Madrid
- Programador *FrontEnd* na Best Pro Consulting SL, Madrid
- Instalador de Equipamentos e Serviços de Telecomunicações no Grupo Zener, Castela e Leão
- Instalador de Equipamentos e Serviços de Telecomunicações no Lican Comunicaciones SL, Castela e Leão
- Certificado em Segurança Informática pelo CFTIC Getafe, Madrid
- Técnico Superior em Sistemas de Telecomunicações e Informática pelo IES Trinidad Arroyo, Palencia
- Técnico Superior em Instalações Eletrotécnicas MT e BT pelo IES Trinidad Arroyo, Palencia
- Treinamento em Engenharia Reversa, Estenografia e Criptografia pela Incibe Hacker Academy

Dr. Álvaro Jiménez Ramos

- Analista de Cibersegurança
- Analista de Segurança Sénior na The Workshop
- Analista de Cibersegurança L1 em Axians
- Analista de Cibersegurança L2 em Axians
- Analista de Cibersegurança na SACYR S.A.
- Licenciatura em Engenharia Telemática pela Universidade Politécnica de Madrid
- Mestrado de Cibersegurança e Hacking Ético pelo CICE
- Curso Superior em Cibersegurança por Deusto Formación

Dr. Javier Nogales Ávila

- Enterprise Cloud e Sourcing Senior Consultant na Quint
- Cloud e Technology Consultant na Indra
- Associate Technology Consultant na Accenture
- Licenciado em Engenharia de Organização Industrial pela Universidade de Jaén
- MBA em Administração e Gestão de Empresas pela ThePower Business School

Dr. Antonio Gómez Rodríguez

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

Dr. José Francisco Catalá Barba

- Técnico Eletrónico Especialista em Cibersegurança
- Programador de Aplicações para Dispositivos Móveis
- Técnico eletrónico do Comando Intermédio do Ministério da Defesa de Espanha
- Técnico Eletrónico na Fábrica Ford Sita em Valência

Dr. Félix Gonzalo Alonso

- Diretor de Geral e fundador da Smart REM Solutions
- Responsável pela Engenharia de Risco e Inovação na Dynargy
- Diretor-geral e sócio fundador da empresa de consultoria tecnológica Risknova
- Mestrado em Gestão de Seguros pelo Instituto de Colaboração entre Seguradoras
- Licenciatura em Engenharia Técnica Industrial, especialidade em Eletrónica Industrial pela Universidade Pontifícia de Comillas

Dr. Alejandro Entrenas

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

Dr. Jorge del Valle Arias

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

Dr. Juan Luis Gozalo Fernández

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

Dra. Lorena Jurado Jabonero

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

Dr. Octavio Ortega Esteban

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

Dr. Mario Embid Ruiz

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

Dr. Juan Manuel Rodrigo Estébanez

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

05

Estrutura e conteúdo

Este Advanced Master em Alta Direção de Cibersegurança é composto por 20 módulos e foi cuidadosamente criado para aproximar o profissional dos mais recentes desenvolvimentos neste domínio. Ficará assim a conhecer os últimos desenvolvimentos em questões como a segurança nos *smartphones*, a segurança na internet das coisas, o desenvolvimento seguro, a criptografia e a segurança em ambientes de *cloud computing*. Assim, com este plano de estudos, o informático terá acesso aos conhecimentos mais recentes e completos, preparando-o rapidamente para se tornar um especialista de grande prestígio em cibersegurança.

Não encontrará conteúdo mais completo do que este para se atualizar no domínio da cibersegurança"

Módulo 1. Ciberinteligência e Cibersegurança

1.1. Ciberinteligência
- 1.1.1. Ciberinteligência
  - 1.1.1.1. A Inteligência
    - 1.1.1.1.1. Ciclo de inteligência
  - 1.1.1.2. Ciberinteligência
  - 1.1.1.3. Ciberinteligência e Cibersegurança
- 1.1.2. O Analista de Inteligência
  - 1.1.2.1. O papel do Analista de Inteligência
  - 1.1.2.2. Os enviesamentos do Analista de Inteligência na atividade avaliativa

1.2. Cibersegurança
- 1.2.1. As Camadas de Segurança
- 1.2.2. Identificação das Ciberameças
  - 1.2.2.1. Ameaças Externas
  - 1.2.2.2. Ameaças Internas
- 1.2.3. Ações adversas
  - 1.2.3.1. Engenharia social
  - 1.2.3.2. Métodos habitualmente utilizados

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

1.4. Metodologias de avaliação
- 1.4.1. A Análise de Inteligência
- 1.4.2. Técnicas de organização da informação adquirida
- 1.4.3. Fiabilidade e credibilidade das fontes de informação
- 1.4.4. Metodologias de Análise
- 1.4.5. Apresentação dos Resultados da Inteligência

1.5. Auditorias e documentação
- 1.5.1. Auditoria na Segurança Informática
- 1.5.2. Documentação e autorizações para Auditoria
- 1.5.3. Tipos de Auditorias
- 1.5.4. Documentos a entregar
  - 1.5.4.1. Relatório Técnico
  - 1.5.4.2. Relatório Executivo

1.6. Ameaças na Rede
- 1.6.1. Uso de anonimato
- 1.6.2. Técnicas de anonimato (Proxy, VPN)
- 1.6.3. Redes TOR, Freenet e IP2

1.7. Ameaças e tipos de segurança
- 1.7.1. Tipos de ameaças
- 1.7.2. Segurança física
- 1.7.3. Segurança de redes
- 1.7.4. Segurança lógica
- 1.7.5. Segurança em aplicações web
- 1.7.6. Segurança em dispositivos móveis

1.8. Regulamentos e *Compliance*
- 1.8.1. RGPD
- 1.8.2. A estratégia nacional de cibersegurança 2019
- 1.8.3. Família ISO 27000
- 1.8.4. Quadro de cibersegurança NIST
- 1.8.5. PIC
- 1.8.6. ISO 27032
- 1.8.7. Regulamentos Cloud
- 1.8.8. SOX
- 1.8.9. PCI

1.9. Análise de riscos e métricas
- 1.9.1. Alcance de riscos
- 1.9.2. Os Ativos
- 1.9.3. As ameaças
- 1.9.4. As vulnerabilidades
- 1.9.5. Avaliação do risco
- 1.9.6. Tratamento do risco

1.10. Organismos importantes em matéria de cibersegurança
- 1.10.1. NIST
- 1.10.2. ENISA
- 1.10.3. INCIBE
- 1.10.4. OEA
- 1.10.5. UNASUR-PROSUR

Módulo 2. Segurança em *host*

2.1. Cópias de segurança
- 2.1.1. Estratégia para as cópias de segurança
- 2.1.2. Ferramentas para Windows
- 2.1.3. Ferramentas para Linux
- 2.1.4. Ferramentas para MacOS

2.2. Antivírus de usuário
- 2.2.1. Tipos de antivírus
- 2.2.2. Antivírus para Windows
- 2.2.3. Antivírus para Linux
- 2.2.4. Antivírus para MacOS
- 2.2.5. Antivírus para smartphones

2.3. Detetores de intrusos - HIDS
- 2.3.1. Métodos de deteção de intrusos
- 2.3.2. Sagan
- 2.3.3. Aide
- 2.3.4. Rkhunter

2.4. Firewall local
- 2.4.1. Firewalls para Windows
- 2.4.2. Firewalls para Linux
- 2.4.3. Firewalls para MacOS

2.5. Gestores de palavras-passe
- 2.5.1. Password
- 2.5.2. LastPass
- 2.5.3. KeePass
- 2.5.4. StickyPassword
- 2.5.5. RoboForm

2.6. Detetores de *phishing*
- 2.6.1. Deteção de phishing de forma manual
- 2.6.2. Ferramentas *antiphishing*

2.7. *Spyware*
- 2.7.1. Mecanismos de Prevenção
- 2.7.2. Ferramentas *antispyware*

2.8. Rastreadores
- 2.8.1. Medidas para proteger o sistema
- 2.8.2. Ferramentas anti-rastreadores

2.9. EDR- End Point Detection and Response
- 2.9.1. Comportamento do sistema EDR
- 2.9.2. Diferenças entre EDR e Antivírus
- 2.9.3. O futuro dos sistemas EDR

2.10. Controlo sobre a instalação de software
- 2.10.1. Repositórios e lojas de software
- 2.10.2. Listas de software permitido ou proibido
- 2.10.3. Critérios de atualizações
- 2.10.4. Privilégios para instalar software

Módulo 3. Segurança em rede (Perímetro)

3.1. Sistemas de deteção e prevenção de ameaças
- 3.1.1. Quadro geral dos incidentes de segurança
- 3.1.2. Sistemas de Defesa Atuais: Defense in Depth e SOC
- 3.1.3. Arquiteturas de rede atuais
- 3.1.4. Tipos de ferramentas para a deteção e prevenção de incidentes
  - 3.1.4.1. Sistemas baseados em Rede
  - 3.1.4.2. Sistemas baseados em Host
  - 3.1.4.3. Sistemas centralizados
- 3.1.5. Comunicação e deteção de instâncias/hosts, contentores e *serverless*

3.2. Firewall
- 3.2.1. Tipos de Firewalls
- 3.2.2. Ataques e mitigação

3.2.3. Firewalls comuns em kernel Linux
3.2.3.1. UFW
3.2.3.2. Nftables e iptables
3.2.3.3. Firewalls
3.2.4. Sistemas de deteção baseados em logs do sistema
3.2.4.1. TCP Wrappers
3.2.4.2. BlockHosts e DenyHosts
3.2.4.3. Fai2ban
3.3. Sistemas de Deteção e Prevenção de Intrusões (IDS/IPS)
3.3.1. Ataques sobre IDS/IPS
3.3.2. Sistemas de IDS/IPS
3.3.2.1. Snort
3.3.2.2. Suricata
3.4. Firewalls da Próxima Geração (NGFW)
3.4.1. Diferenças entre NGFW e firewalls tradicionais
3.4.2. Capacidades principais
3.4.3. Soluções comerciais
3.4.4. Firewalls para serviços de Cloud
3.4.4.1. Arquitetura Cloud VPC
3.4.4.2. Cloud ACLs
3.4.4.3. Security Group
3.5. Proxy
3.5.1. Tipos de Proxy
3.5.2. Uso de Proxy. Vantagens e desvantagens
3.6. Motores de Antivírus
3.6.1. Contexto geral do Malware e IOCs
3.6.2. Problemas dos motores de Antivírus
3.7. Sistemas de Proteção de Correio
3.7.1. Anti-spam
3.7.1.1. Listas brancas e negras
3.7.1.2. Filtros bayesianos
3.7.2. Mail Gateway (MGW)
3.8. SIEM
3.8.1. Componentes e Arquitetura
3.8.2. Regras de correlação e casos de utilização
3.8.3. Desafios atuais dos sistemas SIEM
3.9. SOAR
3.9.1. SOAR e SIEM: Inimigos ou aliados
3.9.2. O futuro dos sistemas SOAR
3.10. Outros sistemas baseados em rede
3.10.1. WAF
3.10.2. NAC
3.10.3. HoneyPots y HoneyNets
3.10.4. CASB

Módulo 4. Segurança em *Smartphones*

4.1. O mundo do Dispositivo Móvel
4.1.1. Tipos de plataformas móveis
4.1.2. Dispositivos iOS
4.1.3. Dispositivos Android
4.2. Gestão da Segurança Móvel
4.2.1. Projeto de Segurança Móvel OWASP
4.2.1.1. Top 10 Vulnerabilidades
4.2.2. Comunicações, Redes e Modos de Conexão
4.3. O Dispositivo Móvel no Meio Empresarial
4.3.1. Riscos
4.3.2. Políticas de Segurança
4.3.3. Monitorização de Dispositivos
4.3.4. Gestão de Dispositivos Móveis (MDM)
4.4. Privacidade do Utilizador e Segurança dos Dados
4.4.1. Estados da Informação
4.4.2. Proteção e Confidencialidade dos Dados
4.4.2.1. Autorizações
4.4.2.2. Encriptação

4.4.3. Armazenamento Seguro dos Dados
4.4.3.1. Armazenamento Seguro em iOS
4.4.3.2. Armazenamento Seguro em Android
4.4.4. Boas práticas no Desenvolvimento de Aplicações
4.5. Vulnerabilidades e Vetores de Ataque
4.5.1. Vulnerabilidades
4.5.2. Vetores de ataque
4.5.2.1. Malware
4.5.2.2. Exfiltração de dados
4.5.2.3. Manipulação dos dados
4.6. Principais Ameaças
4.6.1. Utilizador não forçado
4.6.2. Malware
4.6.2.1. Tipos de Malware
4.6.3. Engenharia Social
4.6.4. Fuga de Dados
4.6.5. Roubo de informação
4.6.6. Redes Wi-Fi não seguras
4.6.7. Software desatualizado
4.6.8. Aplicações Maliciosas
4.6.9. Palavras-passe inseguras
4.6.10. Configurações de segurança fracas ou inexistentes
4.6.11. Acesso Físico
4.6.12. Perda ou roubo do dispositivo
4.6.13. Suplantação de identidade (Integridade)
4.6.14. Criptografia fraca ou danificada
4.6.15. Denegação de Serviços (DoS)
4.7. Principais ataques
4.7.1. Ataques de *phishing*
4.7.2. Ataques relacionados com os modos de comunicação
4.7.3. Ataques de *smishing*
4.7.4. Ataques de *criptojacking*
4.7.5. *Man in The Middle*
4.8. Hacking
4.8.1. *Rooting* e *Jailbreaking*
4.8.2. Anatomia de um Ataque Móvel
4.8.2.1. Propagação da ameaça
4.8.2.2. Instalação de Malware no Dispositivo
4.8.2.3. Persistência
4.8.2.4. Execução do *payload* e extração da informação
4.8.3. Hacking em dispositivos iOS: mecanismos e ferramentas
4.8.4. Hacking em dispositivos Android: mecanismos e ferramentas
4.9. Testes de Penetração
4.9.1. iOS PenTesting
4.9.2. Android PenTesting
4.9.3. Ferramentas
4.10. Proteção e Segurança
4.10.1. Configuração de Segurança
4.10.1.1. Em dispositivos iOS
4.10.1.2. Em dispositivos Android
4.10.2. Medidas de Segurança
4.10.3. Ferramentas de proteção

Módulo 5. Segurança em IoT

5.1. Dispositivos
5.1.1. Tipos de Dispositivos
5.1.2. Arquiteturas Padronizadas
5.1.2.1. ONEM2M
5.1.2.2. IoTWF
5.1.3. Protocolos de Aplicação
5.1.4. Tecnologias de conetividade
5.2. Dispositivos IoT. Áreas de aplicação
5.2.1. *SmartHome*
5.2.2. *SmartCity*
5.2.3. Transportes
5.2.4. Wearables
5.2.5. Setor Saúde
5.2.6. IioT

5.3. Protocolos de comunicação
- 5.3.1. MQTT
- 5.3.2. LWM2M
- 5.3.3. OMA-DM
- 5.3.4. TR-069

5.4. *SmartHome*
- 5.4.1. Domótica
- 5.4.2. Redes
- 5.4.3. Eletrodomésticos
- 5.4.4. Vigilância e segurança

5.5. *SmartCity*
- 5.5.1. Iluminação
- 5.5.2. Meteorologia
- 5.5.3. Segurança

5.6. Transportes
- 5.6.1. Localização
- 5.6.2. Realização de pagamentos e obtenção de serviços
- 5.6.3. Conetividade

5.7. *Wearables*
- 5.7.1. Roupa inteligente
- 5.7.2. Joias inteligentes
- 5.7.3. Relógios inteligentes

5.8. Setor Saúde
- 5.8.1. Monitorização de exercício/ritmo cardíaco
- 5.8.2. Acompanhamento de doentes e pessoas idosas
- 5.8.3. Implantáveis
- 5.8.4. Robôs Cirúrgicos

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

5.10. Securitização
- 5.10.1. Redes dedicadas
- 5.10.2. Gestor de Palavras-Passe
- 5.10.3. Utilização de protocolos encriptados
- 5.10.4. Conselhos de utilização

Módulo 6. Hacking Ético

6.1. Ambiente de trabalho
- 6.1.1. Distribuições Linux
  - 6.1.1.1. Kali Linux - Offensive Security
  - 6.1.1.2. Parrot OS
  - 6.1.1.3. Ubuntu
- 6.1.2. Sistemas de Virtualização
- 6.1.3. *Sandbox*
- 6.1.4. Implementação de laboratórios

6.2. Metodologia
- 6.2.1. OSSTM
- 6.2.2. OWASP
- 6.2.3. NIST
- 6.2.4. PTES
- 6.2.5. ISSAF

6.3. *Footprinting*
- 6.3.1. Inteligência de fontes abertas (OSINT)
- 6.3.2. Procura de brechas e vulnerabilidades de dados
- 6.3.3. Uso de ferramentas passivas

6.4. Scanning de Redes
- 6.4.1. Ferramentas de Scanning
  - 6.4.1.1. Nmap
  - 6.4.1.2. Hping3
  - 6.4.1.3. Outras ferramentas de Scanning
- 6.4.2. Técnicas de Scanning
- 6.4.3. Técnicas de Evasão de Firewall e IDS
- 6.4.4. *Banner Grabbing*
- 6.4.5. Diagramas de rede

6.5. Enumeração
- 6.5.1. Enumeração SMTP
- 6.5.2. Enumeração DNS
- 6.5.3. Enumeração de NetBIOS e Samba
- 6.5.4. Enumeração de LDAP
- 6.5.5. Enumeração de SNMP
- 6.5.6. Outras técnicas de Enumeração

6.6. Análise de Vulnerabilidades
- 6.6.1. Soluções de Análise de Vulnerabilidades
  - 6.6.1.1. Qualys
  - 6.6.1.2. Nessus
  - 6.6.1.3. CFI LanGuard
- 6.6.2. Sistemas de pontuação de vulnerabilidades
  - 6.6.2.1. CVSS
  - 6.6.2.2. CVE
  - 6.6.2.3. NVD

6.7. Ataques a Redes Inalámbricas
- 6.7.1. Metodologia de Hacking em Redes Inalámbricas
  - 6.7.1.1. Wi-Fi Discovery
  - 6.7.1.2. Análise de tráfico
  - 6.7.1.3. Ataques do *aircrack*
    - 6.7.1.3.1. Ataques WEP
    - 6.7.1.3.2. Ataques WPA/WPA2
  - 6.7.1.4. Ataques de *Evil Twin*
  - 6.7.1.5. Ataques a WPS
  - 6.7.1.6. *Jamming*
- 6.7.2. Ferramentas para a Segurança Inalámbrica

6.8. Hacking de servidores web
- 6.8.1. *Cross site scripting*
- 6.8.2. CSRF
- 6.8.3. Session Hijacking
- 6.8.4. SQLinjection

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

6.10. Persistência
- 6.10.1. Instalação de *rootkits*
- 6.10.2. Uso de ncat
- 6.10.3. Utilização de tarefas programadas para *backdoors*
- 6.10.4. Criação de utilizadores
- 6.10.5. Deteção de HIDS

Módulo 7. Engenharia Reversa

7.1. Compiladores
- 7.1.1. Tipos de Códigos
- 7.1.2. Fases de um compilador
- 7.1.3. Tabela de símbolos
- 7.1.4. Gestor de erros
- 7.1.5. Compilador GCC

7.2. Tipos de Análise em Compiladores
- 7.2.1. Análise léxica
  - 7.2.1.1. Terminologia
  - 7.2.1.2. Componentes léxicos
  - 7.2.1.3. Analisador léxico LEX
- 7.2.2. Análise sintático
  - 7.2.2.1. Gramáticas livres de contexto
  - 7.2.2.2. Tipos de análise sintáticos
    - 7.2.2.2.1. Análise descendente
    - 7.2.2.2.2. Análise ascendente
  - 7.2.2.3. Árvores sintáticas e derivações
  - 7.2.2.4. Tipos de analisadores sintáticos
    - 7.2.2.4.1. Analisadores LR (*Left To Right*)
    - 7.2.2.4.2. Analisadores LALR

7.2.3. Análise semântica
7.2.3.1. Gramáticas de atributos
7.2.3.2. S-Atribuídas
7.2.3.3. L-Atribuídas

7.3. Estruturas de Dados e Montagem
7.3.1. Variáveis
7.3.2. Arrays
7.3.3. Apontadores
7.3.4. Estruturas
7.3.5. Objetos

7.4. Estruturas de Código de Montagem
7.4.1. Estruturas de seleção
7.4.1.1. *If, else if, Else*
7.4.1.2. Switch
7.4.2. Estruturas de iteração
7.4.2.1. For
7.4.2.2. While
7.4.2.3. Utilização do break
7.4.3. Funções

7.5. Arquitetura Hardware x86
7.5.1. Arquitetura de processadores x86
7.5.2. Estruturas de dados em x86
7.5.3. Estruturas de código em x86
7.5.3. Estruturas de código em x86

7.6. Arquitetura Hardware ARM
7.6.1. Arquitetura de processadores ARM
7.6.2. Estruturas de dados em ARM
7.6.3. Estruturas de código em ARM

7.7. Análise de código estático
7.7.1. Desmontadores
7.7.2. IDA
7.7.3. Reconstrutores de código

7.8. Análise de código dinâmico
7.8.1. Análise de comportamento
7.8.1.1. Comunicações
7.8.1.2. Monitorização
7.8.2. Depuradores de código em Linux
7.8.3. Depuradores de código em Windows

7.9. *Sandbox*
7.9.1. Arquitetura de uma *sandbox*
7.9.2. Evasão de uma *sandbox*
7.9.3. Técnicas de deteção
7.9.4. Técnicas de evasão
7.9.5. Contramedidas
7.9.6. *Sandbox* em Linux
7.9.7. *Sandbox* em Windows
7.9.8. *Sandox* em MacOS
7.9.9. *Sandbox* em Android

7.10. Análise de Malware
7.10.1. Métodos de análise de malware
7.10.2. Técnicas de ofuscação de malware
7.10.2.1. Ofuscação de executáveis
7.10.2.2. Restrição de ambientes de execução
7.10.3. Ferramentas de análise de malware

Módulo 8. Desenvolvimento Seguro

8.1. Desenvolvimento Seguro
8.1.1. Qualidade, funcionalidade e segurança
8.1.2. Confidencialidade, integridade e disponibilidade
8.1.3. Ciclo de vida do desenvolvimento de software

8.2. Fase de Requisitos
8.2.1. Controlo da autenticação
8.2.2. Controlo de papéis e privilégios
8.2.3. Requisitos orientados para o risco
8.2.4. Aprovação de privilégios

8.3. Fases de Análise e Design
  8.3.1. Acesso a componentes e administração do sistema
  8.3.2. Pistas de auditoria
  8.3.3. Gestão de sessões
  8.3.4. Dados históricos
  8.3.5. Tratamento adequado de erros
  8.3.6. Separação de funções
8.4. Fase de Implementação e Codificação
  8.4.1. Garantia do ambiente de desenvolvimento
  8.4.2. Elaboração da documentação técnica
  8.4.3. Codificação segura
  8.4.4. Segurança nas comunicações
8.5. Boas práticas de Codificação Segura
  8.5.1. Validação de dados de entrada
  8.5.2. Codificação dos dados de saída
  8.5.3. Estilo de programação
  8.5.4. Gestão do registo de alterações
  8.5.5. Práticas criptográficas
  8.5.6. Gestão de erros e logs
  8.5.7. Gestão de ficheiros
  8.5.8. Gestão de Memória
  8.5.9. Padronização e reutilização das funções de segurança
8.6. Preparação do servidor e *hardening*
  8.6.1. Gestão de utilizadores, grupos e papéis no servidor
  8.6.2. Instalação de software
  8.6.3. *Hardening* do servidor
  8.6.4. Configuração robusta do ambiente da aplicação
8.7. Preparação da BBDD e *hardening*
  8.7.1. Otimização do motor de BBDD
  8.7.2. Criação do próprio utilizador para a aplicação
  8.7.3. Atribuição dos privilégios necessários ao utilizador
  8.7.4. *Hardening* da BBDD
8.8. Fase de testes
  8.8.1. Controlo de qualidade nos controlos de segurança
  8.8.2. Inspeção do código por fases
  8.8.3. Comprovação da gestão das configurações
  8.8.4. Testes de caixa negra
8.9. Preparação da transição à produção
  8.9.1. Realizar o controlo de alterações
  8.9.2. Realizar o procedimento de passagem à produção
  8.9.3. Realizar procedimento de *rollback*
  8.9.4. Testes em fase de pré-produção
8.10. Fase de manutenção
  8.10.1. Garantia baseada no risco
  8.10.2. Testes de manutenção de segurança da caixa branca
  8.10.3. Testes de manutenção de segurança da caixa negra

Módulo 9. Análise Forense

9.1. Aquisição de dados e duplicação
  9.1.1. Aquisição de dados voláteis
    9.1.1.1. Informação do sistema
    9.1.1.2. informação de rede
    9.1.1.3. Ordem de volatilidade
  9.1.2. Aquisição de dados estáticos
    9.1.2.1. Criação de uma imagem duplicada
    9.1.2.2. Preparação de um documento para a cadeia de custódia
  9.1.3. Métodos de validação dos dados adquiridos
    9.1.3.1. Métodos para Linux
    9.1.3.2. Métodos para Windows
9.2. Avaliação e derrota de técnicas anti-forenses
  9.2.1. Objetivos das técnicas anti-forenses
  9.2.2. Eliminação de dados
    9.2.2.1. Eliminação de dados e ficheiros
    9.2.2.2. Recuperação de ficheiros
    9.2.2.3. Recuperação de partições apagadas

9.2.3. Proteção com palavra-passe
9.2.4. Esteganografia
9.2.5. Limpeza segura de dispositivos
9.2.6. Encriptação

9.3. Análise Forense do sistema operativo
9.3.1. Análise Forense de Windows
9.3.2. Análise Forense de Linux
9.3.3. Análise Forense de Mac

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

9.5. Análise Forense Web
9.5.1. Investigação de ataques na web
9.5.2. Deteção de ataques
9.5.3. Localização de direções IPs

9.6. Análise Forense de Bases de Dados
9.6.1. Análise Forense em MSSQL
9.6.2. Análise Forense em MySQL
9.6.3. Análise Forense em PostgreSQL
9.6.4. Análise Forense em MongoDB

9.7. Análise Forense em Cloud
9.7.1. Tipos de Crimes em Cloud
9.7.1.1. Cloud como Sujeito
9.7.1.2. Cloud como Objeto
9.7.1.3. Cloud como Ferramenta
9.7.2. Desafios da Análise Forense em Cloud
9.7.3. Investigação sobre os serviços de armazenamento na Cloud
9.7.4. Ferramentas de Análise Forense para Cloud

9.8. Investigação de crimes por Correio Eletrónico
9.8.1. Sistemas de Correio Eletrónico
9.8.1.1. Clientes de Correio Eletrónico
9.8.1.2. Servidor de Correio Eletrónico
9.8.1.3. Servidor SMTP
9.8.1.4. Servidor POP3
9.8.1.5. Servidor IMAP4
9.8.2. Crimes de correio
9.8.3. Mensagem de Correio Eletrónico
9.8.3.1. Cabeçalhos Padrão
9.8.3.2. Cabeçalhos Estendidos
9.8.4. Passos na investigação destes crimes
9.8.5. Ferramentas Forenses para Correio Eletrónico

9.9. Análise Forense de Telemóveis
9.9.1. Redes Celulares
9.9.1.1. Tipos de redes
9.9.1.2. Conteúdos do CDR
9.9.2. *Subscriber Identity Module* (SIM)
9.9.3. Aquisição lógica
9.9.4. Aquisição física
9.9.5. Aquisição do sistema de ficheiros

9.10. Redação e apresentação de Relatórios Forenses
9.10.1. Aspetos importantes de um Relatório Forense
9.10.2. Classificação e tipos de relatórios
9.10.3. Guia para escrever um relatório
9.10.4. Apresentação do Relatório
9.10.4.1. Preparação prévia para o depoimento
9.10.4.2. Deposição
9.10.4.3. Lidar com os meios de comunicação social

Módulo 10. Desafios Atuais e Futuros na Segurança Informática

10.1. Tecnologia *Blockchain*
- 10.1.1. Âmbito de aplicação
- 10.1.2. Garantia de confidencialidade
- 10.1.3. Garantia de não repúdio

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

10.3. *Deepfake*
- 10.3.1. Impacto nos meios de comunicação social
- 10.3.2. Perigos para a sociedade
- 10.3.3. Mecanismos de deteção

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

10.5. Privacidade digital
- 10.5.1. Valor dos dados na rede
- 10.5.2. Uso dos dados na rede
- 10.5.3. Gestão da privacidade e da identidade digital

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

10.7. Teletrabalho
- 10.7.1. Revolução do teletrabalho durante e após a Covid19
- 10.7.2. Estrangulamentos no acesso
- 10.7.3. Variação da superfície de ataque
- 10.7.4. Necessidades dos trabalhadores

10.8. Tecnologias *wireless* emergentes
- 10.8.1. WPA3
- 10.8.2. 5G
- 10.8.3. Ondas milimétricas
- 10.8.4. Tendência em "*Get Smart*" em vez de "*Get more*"

10.9. Endereçamento futuro em redes
- 10.9.1. Problemas atuais com o endereçamento IP
- 10.9.2. IPv6
- 10.9.3. IPv4+
- 10.9.4. Vantagens do IPv4+ em relação ao IPv4
- 10.9.5. Vantagens do IPv6 em relação ao IPv4

10.10. O desafio da sensibilização para a educação precoce e contínua da população
- 10.10.1. Estratégias governamentais atuais
- 10.10.2. Resistência da população à aprendizagem
- 10.10.3. Planos de formação a serem adotados pelas empresas

Módulo 11. Segurança no desenho e desenvolvimento de sistemas

11.1. Sistemas de informação
- 11.1.1. O que é um sistema de informação
- 11.1.2. Componentes de um sistema de informação
- 11.1.3. Atividades de um sistema de informação
- 11.1.4. Ciclo de vida de um sistema de informação
- 11.1.5. Recursos de um sistema de Informação

11.2. Sistemas de informação. Tipologia
- 11.2.1. Tipos dos sistemas de informação
  - 11.2.1.1. Empresarial
  - 11.2.1.2. Estratégicos
  - 11.2.1.3. De acordo com o âmbito da aplicação
  - 11.2.1.4. Específicos
- 11.2.2. Sistemas de informação. Exemplos reais
- 11.2.3. Evolução dos sistemas de informação: Etapas
- 11.2.4. Metodologia dos sistemas de informação

11.3. Segurança dos sistemas de informação. Implicações legais
    11.3.1. Acesso a dados
    11.3.2. Ameaças de segurança: Vulnerabilidades
    11.3.3. Implicações legais: Delitos
    11.3.4. Procedimentos de manutenção de um sistema de informação
11.4. Segurança de um sistemas de informação. Protocolos de segurança
    11.4.1. Segurança de um sistema de informação
        11.4.1.1. Integração
        11.4.1.2. Confidencialidade
        11.4.1.3. Disponibilidade
        11.4.1.4. Autenticação
    11.4.2. Serviços de segurança
    11.4.3. Protocolos de segurança da informação. Tipologia
    11.4.4. Sensibilidade de um sistema de informação
11.5. Segurança num sistemas de informação. Medidas e sistemas de controlo de acesso
    11.5.1. Medidas de segurança
    11.5.2. Tipos de medidas de segurança
        11.5.2.1. Prevenção
        11.5.2.2. Deteção
        11.5.2.3. Correção
    11.5.3. Sistema de controlo de acesso. Tipologia
    11.5.4. Criptografia
11.6. Segurança em redes e internet
    11.6.1. Firewalls
    11.6.2. Identificação digital
    11.6.3. Vírus e worms
    11.6.4. Hacking
    11.6.5. Exemplos e casos reais
11.7. Crimes informáticos
    11.7.1. Crime informático
    11.7.2. Crimes informáticos. Tipologia
    11.7.3. Crime informático Ataque Tipologias
    11.7.4. O caso da Realidade Virtual
    11.7.5. Perfis de delinquentes e vítimas Tipificação do crime
    11.7.6. Crimes informáticos. Exemplos e casos reais
11.8. Plano de segurança num sistemas de informação
    11.8.1. Plano de segurança. Objetivos
    11.8.2. Plano de segurança. Planificação
    11.8.3. Plano de riscos Análises
    11.8.4. Políticas de segurança. Implementação na organização
    11.8.5. Plano de segurança. Implementação na organização
    11.8.6. Procedimentos de segurança Tipos
    11.8.7. Planos de segurança. Exemplos
11.9. Plano de contingência
    11.9.1. Plano de contingência. Funções
    11.9.2. Plano de Emergência: Elementos e objetivos
    11.9.3. Plano de contingência na organização. Implementação
    11.9.4. Planos de contingência. Exemplos
11.10. Governação da segurança dos sistemas de informação
    11.10.1. Regulamentos legais
    11.10.2. Padrões
    11.10.3. Certificações
    11.10.4. Tecnologias

Módulo 12. Arquiteturas e modelos de segurança da informação

12.1. Arquitetura de segurança da informação
    12.1.1. SGSI/PDS
    12.1.2. Alienação estratégica
    12.1.3. Gestão do risco
    12.1.4. Medição de desempenho
12.2. Modelos de segurança da informação
    12.2.1. Baseados em políticas de segurança
    12.2.2. Baseados em ferramentas de proteção
    12.2.3. Baseados em equipas de trabalho
12.3. Modelo de segurança Componentes chave
    12.3.1. Identificação de riscos
    12.3.2. Definição de controlos
    12.3.3. Avaliação contínua de níveis de risco
    12.3.4. Plano de sensibilização de funcionários, fornecedores, sócios, etc.

12.4. Processo de gestão de riscos
 12.4.1. Identificação de ativos
 12.4.2. Identificação de ameaças
 12.4.3. Avaliação de risco
 12.4.4. Priorização de controlos
 12.4.5. Reavaliação e risco residual
12.5. Processos de negócio e segurança da informação
 12.5.1. Processos empresariais
 12.5.2. Avaliação de risco com base em parâmetros de negócio
 12.5.3. Análise do impacto no negócio
 12.5.4. As operações de negócio e a segurança da informação
12.6. Processo de melhoria contínua
 12.6.1. O ciclo de Deming
  12.6.1.1. Planificar
  12.6.1.2. Fazer
  12.6.1.3. Verificar
  12.6.1.4. Agir
12.7. Arquiteturas de segurança
 12.7.1. Seleção e homogeneização de tecnologias
 12.7.2. Gestão de identidades. Autenticação
 12.7.3. Gestão de acessos Autorização
 12.7.4. Segurança de infraestrutura de rede
 12.7.5. Tecnologias e soluções de encriptação
 12.7.6. Segurança de equipas terminais (EDR)
12.8. O quadro normativo
 12.8.1. Normativas setoriais
 12.8.2. Certificações
 12.8.3. Legislações
12.9. A Norma ISO 27001
 12.9.1. Implementação
 12.9.2. Certificação
 12.9.3. Auditorias e testes de intrusão
 12.9.4. Gestão contínua do risco
 12.9.5. Classificação da informação
12.10. Legislação sobre privacidade Regulamento Geral de Proteção de Dados - RGPD (GDPR - General Data Protection Regulation)
 12.10.1. Alcance do regulamento geral de proteção de dados (GDPR)
 12.10.2. Dados pessoais
 12.10.3. Papéis no tratamento de dados pessoais
 12.10.4. Direitos ARCO
 12.10.5. O DPO. Funções

Módulo 13. Gestão da Segurança IT

13.1. Gestão da Segurança
 13.1.1. Operações de segurança
 13.1.2. Aspeto legal e regulamentar
 13.1.3. Habilitação do negócio
 13.1.4. Gestão de risco
 13.1.5. Gestão de identidades e acessos
13.2. Estrutura da área de segurança O escritório do CISO
 13.2.1. Estrutura organizativa. Posição do CISO (Chief Information Security Officer) na estrutura
 13.2.2. As linhas de defesa
 13.2.3. Organigrama do escritório do CISO
 13.2.4. Gestão orçamental
13.3. Governo de segurança
 13.3.1. Comité de segurança
 13.3.2. Comité de monitorização de riscos
 13.3.3. Comité de auditoria
 13.3.4. Comité de crise
13.4. Governo de segurança. Funções
 13.4.1. Políticas e normas
 13.4.2. Plano Diretor de segurança
 13.4.3. Painel de instrumentos
 13.4.4. Sensibilização e formação
 13.4.5. Segurança na cadeia de abastecimento
13.5. Operações de segurança
 13.5.1. Gestão de identidades e acessos
 13.5.2. Configuração de regras de segurança de rede. Firewalls

13.5.3. Gestão de plataformas IDS/IPS
13.5.4. Análise de vulnerabilidades

13.6. Quadro de trabalho de Cibersegurança NIST CSF
13.6.1. Metodologia NIST
13.6.1.1. Identificar
13.6.1.2. Proteger
13.6.1.3. Detetar
13.6.1.4. Responder
13.6.1.5. Recuperar

13.7. Centro de operações de segurança (SOC) Funções
13.7.1. Proteção *Red Team, Pentesting, Threat Intelligence*
13.7.2. Deteção SIEM, *User Behavior Analytics, Fraud Prevention*
13.7.3. Resposta

13.8. Auditoria de segurança
13.8.1. Teste de intrusão
13.8.2. Exercícios *red team*
13.8.3. Auditorias de código fonte Desenvolvimento seguro
13.8.4. Segurança de componentes (*Software Supply Chain*)
13.8.5. Análise forense

13.9. Resposta a incidentes
13.9.1. Preparação
13.9.2. Deteção, análise e notificação
13.9.3. Contenção, erradicação e recuperação
13.9.4. Atividades pós-incidente
13.9.4.1. Retenção de evidências
13.9.4.2. Análise forense
13.9.4.3. Gestão de brechas
13.9.5. Guias oficiais de gestão de ciberincidentes

13.10. Gestão de vulnerabilidades
13.10.1. Análise de vulnerabilidades
13.10.2. Avaliação de vulnerabilidade
13.10.3. Base de sistemas
13.10.4. Vulnerabilidade de dia 0. Zero-Day

Módulo 14. Análise de riscos e ambiente de segurança IT

14.1. Análise do ambiente
14.1.1. Análise da situação conjuntural
14.1.1.1. Ambientes VUCA
14.1.1.1.1. Volátil
14.1.1.1.2. Incerto
14.1.1.1.3. Complexo
14.1.1.1.4. Ambíguo
14.1.1.2. Ambientes BANI
14.1.1.2.1. Frágil
14.1.1.2.2. Ansioso
14.1.1.2.3. Não linear
14.1.1.2.4. Incompreensível
14.1.2. Análise do ambiente geral. PESTEL
14.1.2.1. Político
14.1.2.2. Económico
14.1.2.3. Social
14.1.2.4. Tecnológico
14.1.2.5. Ecológico/Ambiental
14.1.2.6. Legal
14.1.3. Análise da situação interna. SWOT
14.1.3.1. Objetivos
14.1.3.2. Ameaças
14.1.3.3. Oportunidades
14.1.3.4. Pontos fortes

14.2. Riscos e incerteza
14.2.1. Risco
14.2.2. Gestão de riscos
14.2.3. Normas de gestão de riscos

14.3. Diretrizes para a gestão de riscos ISO 31.000:2018
14.3.1. Objeto
14.3.2. Princípios
14.3.3. Quadro de referência
14.3.4. Processo

14.4. Metodologia de análise e gestão de riscos dos sistemas de informação (MAGERIT)
   14.4.1. Metodologia MAGERIT
      14.4.1.1. Objetivos
      14.4.1.2. Método
      14.4.1.3. Elementos
      14.4.1.4. Técnicas
      14.4.1.5. Ferramentas disponíveis
14.5. Transferência do risco cibernético
   14.5.1. Transferência de riscos
   14.5.2. Riscos cibernéticos Tipologia
   14.5.3. Seguros de riscos cibernéticos
14.6. Metodologias ágeis para a gestão de riscos
   14.6.1. Metodologias ágeis
   14.6.2. Scrum para a gestão do risco
   14.6.3. *Agile Risk Management*
14.7. Tecnologias para a gestão do risco
   14.7.1. Inteligência artificial aplicada à gestão de riscos
   14.7.2. *Blockchain* e criptografia. Metódos de preservação do valor
   14.7.3. Computação quântica Oportunidade ou ameaça
14.8. Elaboração de mapas de riscos informáticos baseados em metodologias ágeis
   14.8.1. Representação da probabilidade e impacto em ambientes ágeis
   14.8.2. O risco como ameaça do valor
   14.8.3. Re-evolução na gestão de projetos e processos ágeis baseados em KRIs
14.9. *Risk Driven* na gestão de riscos
   14.9.1. *Risk Driven*
   14.9.2. *Risk Driven* na gestão de riscos
   14.9.3. Desenvolvimento de um modelo de gestão empresarial impulsionado pelo risco
14.10. Inovação e transformação digital na gestão de risco informáticos
   14.10.1. A gestão de riscos ágeis como fonte de inovação empresarial
   14.10.2. Transformação de dados em informação útil para a tomada de decisões
   14.10.3. Visão holística da empresa através do risco

Módulo 15. Criptografia em IT

15.1. Criptografia
   15.1.1. Criptografia
   15.1.2. Fundamentos matemáticos
15.2. Criptologia
   15.2.1. Criptologia
   15.2.2. Criptoanálise
   15.2.3. Criptoanálise
15.3. Protocolos criptográficos
   15.3.1. Blocos básicos
   15.3.2. Protocolos básicos
   15.3.3. Protocolos intermédios
   15.3.4. Protocolos avançados
   15.3.5. Protocolos esotéricos
15.4. Técnicas criptográficas
   15.4.1. Longitude de chaves
   15.4.2. Gestão de chaves
   15.4.3. Tipos de algoritmos
   15.4.4. Funções resumo. *Hash*
   15.4.5. Geradores de números pseudoaleatórios
   15.4.6. Uso de algoritmos
15.5. Criptografia simétrica
   15.5.1. Cifras de bloco
   15.5.2. DES (*Data Encryption Standard*)
   15.5.3. Algoritmo RC4
   15.5.4. AES (*Advanced Encryption Standard*)
   15.5.5. Combinação de cifras de bloco
   15.5.6. Derivação de chaves
15.6. Criptografia assimétrica
   15.6.1. Diffie-Hellman
   15.6.2. DSA (*Digital Signature Algorithm*)
   15.6.3. RSA (*Rivest, Shamir e Adleman*)
   15.6.4. Curva elíptica
   15.6.5. Criptografia assimétrica Tipologia

15.7. Certificados digitais
    15.7.1. Assinatura digital
    15.7.2. Certificados X509
    15.7.3. Infraestrutura de chave pública (PKI)
15.8. Implementações
    15.8.1. Kerberos
    15.8.2. IBM CCA
    15.8.3. *Pretty Good Privacy* (PGP)
    15.8.4. ISO *Authentication Framework*
    15.8.5. SSL e TLS
    15.8.6. Cartões inteligentes em meios de pagamento (EMV)
    15.8.7. Protocolos de telefonia móvel
    15.8.8. *Blockchain*
15.9. Esteganografia
    15.9.1. Esteganografia
    15.9.2. Estegoanálise
    15.9.3. Aplicações e usos
15.10. Criptografia quântica
    15.10.1. Algoritmos quânticos
    15.10.2. Proteção de algoritmos frente à computação quântica
    15.10.3. Distribuição de chave quântica

Módulo 16. Gestão de identidade e acessos em segurança IT

16.1. Gestão de identidade e acessos (IAM)
    16.1.1. Identidade digital
    16.1.2. Gestão de identidade
    16.1.3. Federação de identidades
16.2. Controlo de acesso físico
    16.2.1. Sistemas de proteção
    16.2.2. Segurança das áreas
    16.2.3. Instalações de recuperação
16.3. Controlo de acesso lógico
    16.3.1. Autenticação: Tipologia
    16.3.2. Protocolos de autenticação
    16.3.3. Ataques de autenticação
16.4. Controlo de acesso lógico. Autenticação MFA
    16.4.1. Controlo de acesso lógico. Autenticação MFA
    16.4.2. Palavras-passe Importância
    16.4.3. Ataques de autenticação
16.5. Controlo de acesso lógico. Autenticação biométrica
    16.5.1. Controlo de acesso lógico. Autenticação biométrica
        16.5.1.1. Autenticação biométrica Requisitos
    16.5.2. Funcionamento
    16.5.3. Modelo e técnicas
16.6. Sistemas de gestão de autenticação
    16.6.1. *Single Sign On*
    16.6.2. Kerberos
    16.6.3. Sistemas AAA
16.7. Sistemas de gestão de autenticação: Sistemas AAA
    16.7.1. TACACS
    16.7.2. RADIUS
    16.7.3. DIAMETER
16.8. Serviços de controlo de acesso
    16.8.1. FW - Firewall
    16.8.2. VPN - Redes Privadas Virtuais
    16.8.3. IDS - Sistema de Deteção de Intrusões
16.9. Sistema de controlo de acesso à rede
    16.9.1. NAC
    16.9.2. Arquitetura e elementos
    16.9.3. Funcionamento e normalização
16.10. Acesso a redes sem fios
    16.10.1. Tipos de redes sem fios
    16.10.2. Segurança em redes sem fios
    16.10.3. Ataques em redes sem fios

Módulo 17. Segurança em comunicações e operação software

17.1. Segurança informática em comunicações e operação software
- 17.1.1. Segurança Informática
- 17.1.2. Cibersegurança
- 17.1.3. Segurança na nuvem

17.2. Segurança informática em comunicações e operação software. Tipologia
- 17.2.1. Segurança física
- 17.2.2. Segurança lógica

17.3. Segurança em comunicações
- 17.3.1. Principais elementos
- 17.3.2. Segurança de redes
- 17.3.3. Melhores práticas

17.4. Ciberinteligência
- 17.4.1. Engenharia social
- 17.4.2. *Deep Web*
- 17.4.3. *Phishing*
- 17.4.4. *Malware*

17.5. Desenvolvimento seguro em comunicações e operação software
- 17.5.1. Desenvolvimento seguro. Protocolo HTTP
- 17.5.2. Desenvolvimento seguro. Ciclo de vida
- 17.5.3. Desenvolvimento seguro. Segurança PHP
- 17.5.4. Desenvolvimento seguro. Segurança NET
- 17.5.5. Desenvolvimento seguro. Melhores práticas

17.6. Sistemas de gestão de segurança da informação em comunicações e operações software
- 17.6.1. GDPR
- 17.6.2. ISO 27021
- 17.6.3. ISO 27017/ 18

17.7. Tecnologias SIEM
- 17.7.1. Tecnologias SIEM
- 17.7.2. Operativa de SOC
- 17.7.3. SIEM *vendors*

17.8. A função da segurança nas organizações
- 17.8.1. Funções nas organizações
- 17.8.2. Função dos especialistas IoT nas empresas
- 17.8.3. Certificações reconhecidas no mercado

17.9. Análise forense
- 17.9.1. Análise forense
- 17.9.2. Análise forense. Metodologia
- 17.9.3. Análise forense. Ferramentas e implantação

17.10. A cibersegurança na atualidade
- 17.10.1. Principais ataques informáticos
- 17.10.2. Previsões de empregabilidade
- 17.10.3. Desafios

Módulo 18. Segurança em ambientes *cloud*

18.1. Segurança em ambientes *cloud computing*
- 18.1.1. Segurança em ambientes *cloud computing*
- 18.1.2. Segurança em ambientes *cloud computing.* Ameaças e riscos segurança
- 18.1.3. Segurança em ambientes *cloud computing.* Aspetos chave de segurança

18.2. Tipos de infraestrutura *cloud*
- 18.2.1. Público
- 18.2.2. Privado
- 18.2.3. Híbrido

18.3. Modelo de gestão partilhada
- 18.3.1. Elementos de segurança geridos por fornecedor
- 18.3.2. Elementos geridos por cliente
- 18.3.3. Definição da estratégia para a segurança

18.4. Mecanismos de prevenção
- 18.4.1. Sistemas de gestão de autenticação
- 18.4.2. Sistemas de gestão de autorização: Políticas de acesso
- 18.4.3. Sistemas de gestão de chaves

18.5. Securitização de sistemas
- 18.5.1. Securitização dos sistemas de armazenamento
- 18.5.2. Proteção dos sistemas de base de dados
- 18.5.3. Securitização de dados em trânsito

18.6. Proteção de infraestrutura
  18.6.1. Desenho e implementação de rede segura
  18.6.2. Segurança de recursos de computação
  18.6.3. Ferramentas e recursos para proteção de infraestrutura
18.7. Deteção as ameaças e ataques
  18.7.1. Sistemas de auditoria, *logging* e monitorização
  18.7.2. Sistemas de eventos e alarmes
  18.7.3. Sistemas SIEM
18.8. Resposta a incidentes
  18.8.1. Plano de resposta a incidentes
  18.8.2. A continuidade do negócio
  18.8.3. Análise forense e remediação de incidentes da mesma natureza
18.9. Segurança em *clouds* públicas
  18.9.1. AWS (Amazon Web Services)
  18.9.2. Microsoft Azure
  18.9.3. Google GCP
  18.9.4. Oracle Cloud
18.10. Normativa e cumprimento
  18.10.1. Cumprimento de normativas de segurança
  18.10.2. Gestão de risco
  18.10.3. Pessoas e processo nas organizações

Módulo 19. Segurança em comunicações de dispositivos Iot

19.1. Da telemetria à IoT
  19.1.1. Telemetria
  19.1.2. Conetividade M2M
  19.1.3. Democratização da telemetria
19.2. Modelos de referência IoT
  19.2.1. Modelos de referência IoT
  19.2.2. Arquitetura simplificada IoT
19.3. Vulnerabilidade de segurança da IoT
  19.3.1. Dispositivos IoT
  19.3.2. Dispositivos IoT. Estudos de casos de utilização
  19.3.3. Dispositivos IoT. Vulnerabilidades
19.4. Conetividade da IoT
  19.4.1. Redes PAN, LAN, WAN
  19.4.2. Tecnologias sem fios na IoT
  19.4.3. Tecnologias sem fios na LPWAN
19.5. Tecnologias LPWAN
  19.5.1. O triângulo de ferro das LPWAN
  19.5.2. Bandas de frequência livre vs. Bandas licenciadas
  19.5.3. Opções de tecnologias LPWAN
19.6. Tecnologia LoRaWAN
  19.6.1. Tecnologia LoRaWAN
  19.6.2. Casos de utilização LoRaWAN Ecossistema
  19.6.3. Segurança em LoRaWAN
19.7. Tecnologia Sigfox
  19.7.1. Tecnologia Sigfox
  19.7.2. Casos de utilização Sigfox. Ecossistema
  19.7.3. Segurança em Sigfox
19.8. Tecnologia Celular IoT
  19.8.1. Tecnologia Celular IoT (NB-IoT e LTE-M)
  19.8.2. Casos de utilização Celular IoT Ecossistema
  19.8.3. Segurança em Celular IoT
19.9. Tecnologia WiSUN
  19.9.1. Tecnologia WiSUN
  19.9.2. Casos de utilização WiSUN. Ecossistema
  19.9.3. Segurança em WiSUN
19.10. Outras tecnologias IoT
  19.10.1. Outras tecnologias IoT
  19.10.2. Casos de utilização e ecossistema de outras tecnologias IoT
  19.10.3. Segurança em outras tecnologias IoT

Módulo 20. Plano de continuidade do negócio associado à segurança

20.1. Planos de continuidade de negócio
- 20.1.1. Os planos de continuidade de negócio (PCN)
- 20.1.2. Plano de continuidade de negócio (PCN). Questões-chave
- 20.1.3. Plano de continuidade de negócio (PCN) para a avaliação da empresa

20.2. Métricas num plano de continuidade de negócio (PCN)
- 20.2.1. *Recovery Time Objective* (RTO) e *Recovery Point Objective* (RPO)
- 20.2.2. Tempo máximo tolerável (MTD)
- 20.2.3. Níveis mínimos de recuperação (ROL)
- 20.2.4. Ponto de recuperação objetivo (RPO)

20.3. Projetos de continuidade. Tipologia
- 20.3.1. Plano de continuidade de negócio (PCN)
- 20.3.2. Plano de continuidade de TIC (PCTIC)
- 20.3.3. Plano de recuperação em caso de desastres (PRD)

20.4. Gestão de riscos associada ao PCN
- 20.4.1. Análise de impacto no negócio
- 20.4.2. Benefícios da implementação de um PCN
- 20.4.3. Mentalidade baseada em riscos

20.5. Ciclo de vida de um plano de continuidade de negócio
- 20.5.1. Fase 1: análise da organização
- 20.5.2. Fase 2: determinação da estratégia de continuidade
- 20.5.3. Fase 3: resposta à contingência
- 20.5.4. Fase 4: prova, manutenção e revisão

20.6. Fase de análise da organização de um PCN
- 20.6.1. Identificação de processos no âmbito do PCN
- 20.6.2. Identificação de áreas críticas do negócio
- 20.6.3. Identificação de dependências entre áreas e processos
- 20.6.4. Determinação do MTD adequado
- 20.6.5. Documentos a entregar Criação de um plano

20.7. Fase de determinação da estratégia de continuidade num PCN
- 20.7.1. Funções na fase de determinação da estratégia
- 20.7.2. Tarefas da fase de determinação da estratégia
- 20.7.3. Documentos a entregar

20.8. Fase de resposta à contingência num PCN
- 20.8.1. Funções na fase de resposta
- 20.8.2. Tarefas nesta fase
- 20.8.3. Documentos a entregar

20.9. Fase de testes, manutenção e revisão de um PCN
- 20.9.1. Funções na fase de testes, manutenção e revisão
- 20.9.2. Tarefas na fase de testes, manutenção e revisão
- 20.9.3. Documentos a entregar

20.10. Normas ISO associadas aos planos de continuidade de negócios (PCN)
- 20.10.1. ISO 22301:2019
- 20.10.2. ISO 22313:2020
- 20.10.3. Outras normas ISO e internacionais relacionadas

Poderá aprofundar questões como o Plano de Continuidade do Negócio associado à segurança ou à gestão da identidade e do acesso na segurança das TI"

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

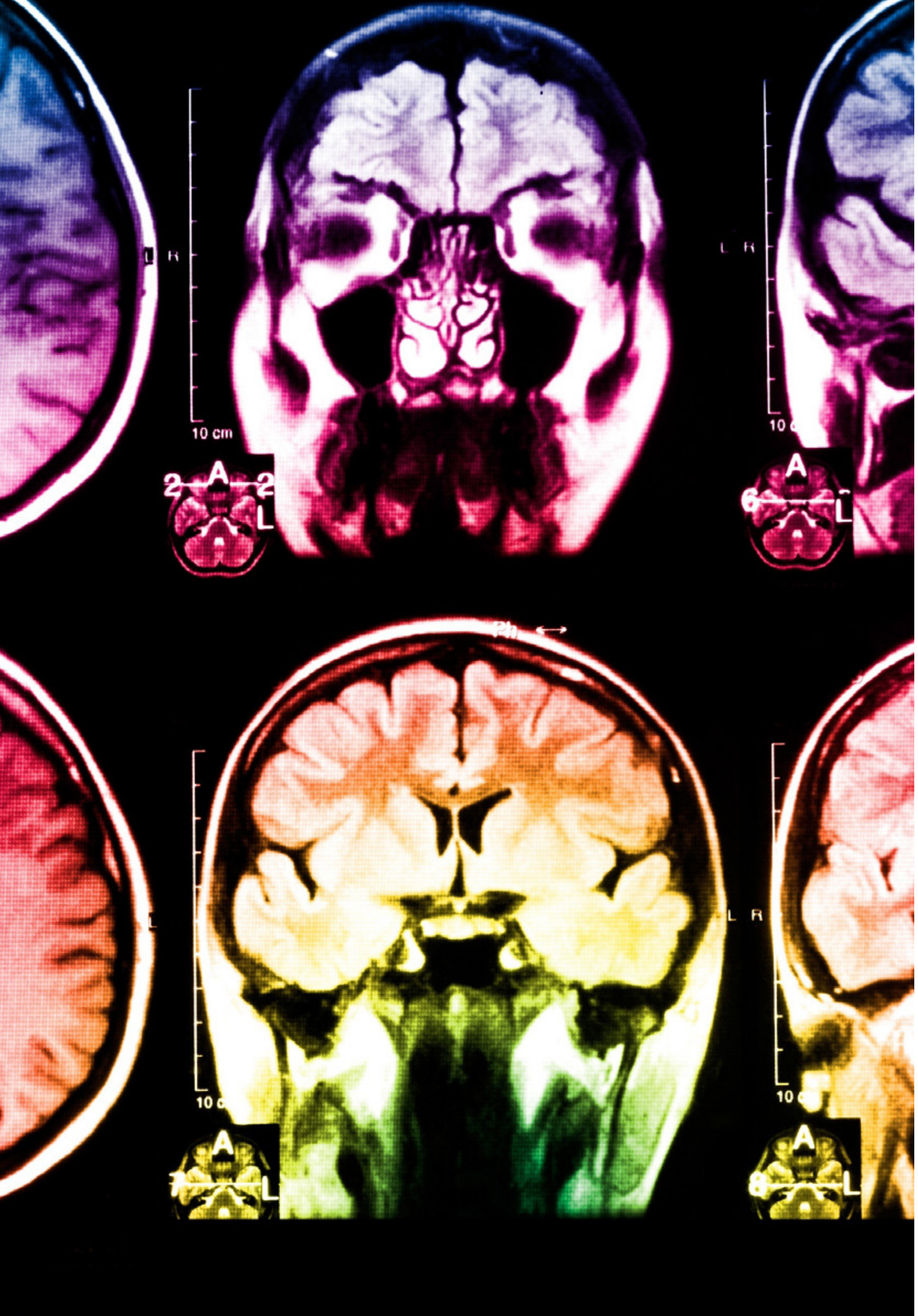
A TECH combina eficazmente a metodologia do Estudo de Caso com um sistema de aprendizagem 100% online baseado na repetição, que combina elementos didáticos diferentes em cada lição.

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.

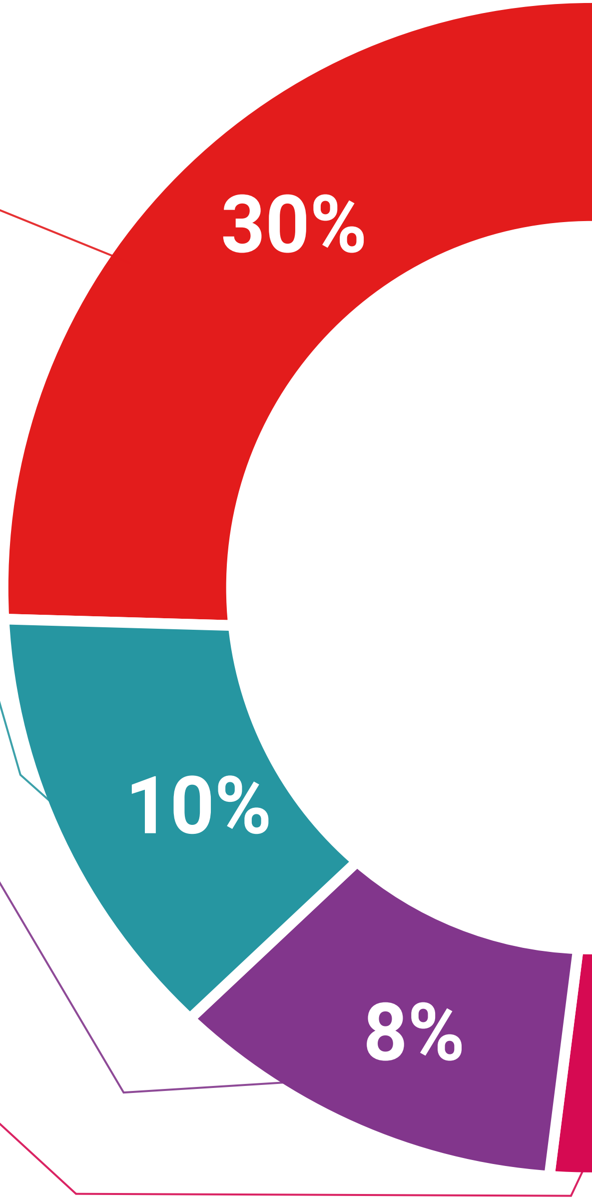
O denominado Learning from an Expert constrói conhecimento e memória, e gera confiança em futuras decisões difíceis.

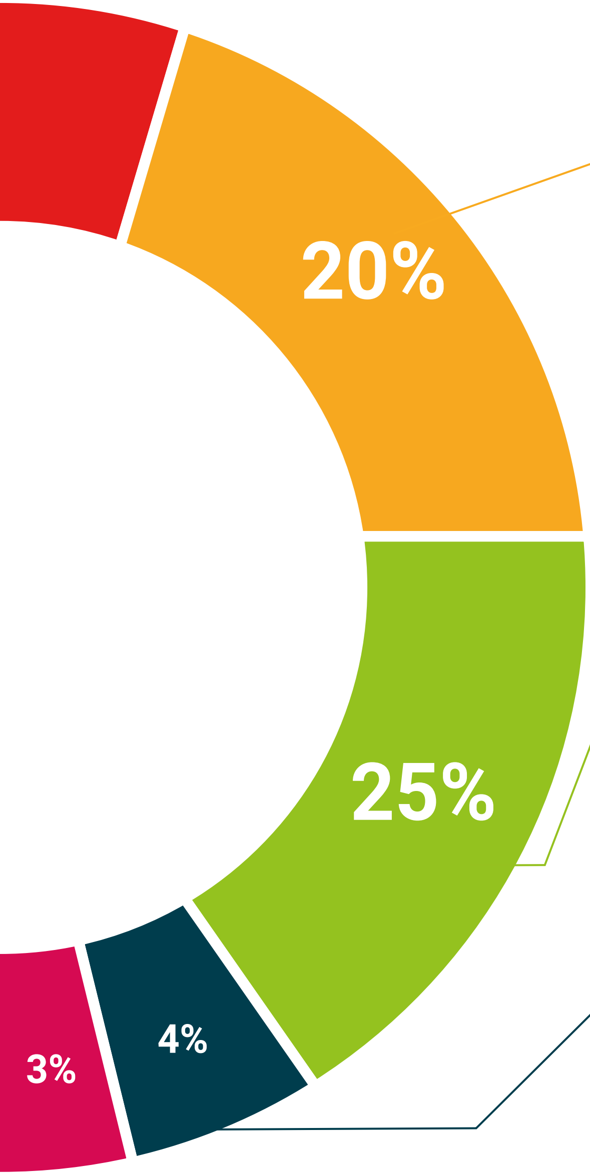
Práticas de aptidões e competências

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 Advanced Master em Alta Direção de Cibersegurança garante, para além de um 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 **Advanced Master em Alta Direção de Cibersegurança** conta com o conteúdo educativo 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 **Advanced Master** emitido pela **TECH Universidade Tecnológica**.

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

Certificação: **Advanced Master em Alta Direção de Cibersegurança**

Modalidade: **online**

Duração: **2 anos**


tech universidade tecnológica

Concede o presente

CERTIFICADO

a

Sr./Sra. _________________, com o documento de identificação nº____________

Por ter concluído e certificado com sucesso o

ADVANCED MASTER

em

Alta Direção de Cibersegurança

Este é um certificado atribuído por esta Universidade, reconhecido por 120 ECTS e equivalente a 3000 horas, com data de início a dd/mm/aaaa e data de conclusão a dd/mm/aaaaa.

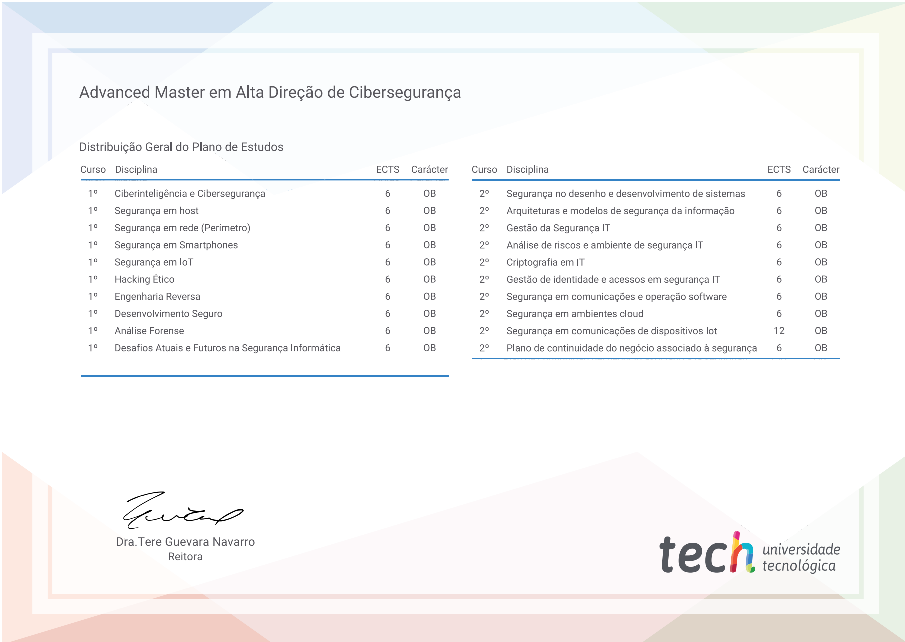
A TECH é uma Instituição Privada de Ensino Superior reconhecida pelo Ministério da Educação Pública a partir de 28 de junho de 2018.

A 17 de junho de 2020

Dra.Tere Guevara Navarro
Reitora

Esta qualificação deve ser sempre acompanhada por um certificado universitário emitido pela autoridade competente para a prática profissional em cada país.

código único TECH: AFWOR23S techtitute.com/titulos


Advanced Master em Alta Direção de Cibersegurança

Distribuição Geral do Plano de Estudos

Curso	Disciplina	ECTS	Carácter
1º	Ciberinteligência e Cibersegurança	6	OB
1º	Segurança em host	6	OB
1º	Segurança em rede (Perímetro)	6	OB
1º	Segurança em Smartphones	6	OB
1º	Segurança em IoT	6	OB
1º	Hacking Ético	6	OB
1º	Engenharia Reversa	6	OB
1º	Desenvolvimento Seguro	6	OB
1º	Análise Forense	6	OB
1º	Desafios Atuais e Futuros na Segurança Informática	6	OB

Curso	Disciplina	ECTS	Carácter
2º	Segurança no desenho e desenvolvimento de sistemas	6	OB
2º	Arquiteturas e modelos de segurança da informação	6	OB
2º	Gestão da Segurança IT	6	OB
2º	Análise de riscos e ambiente de segurança IT	6	OB
2º	Criptografia em IT	6	OB
2º	Gestão de identidade e acessos em segurança IT	6	OB
2º	Segurança em comunicações e operação software	6	OB
2º	Segurança em ambientes cloud	6	OB
2º	Segurança em comunicações de dispositivos Iot	12	OB
2º	Plano de continuidade do negócio associado à segurança	6	OB

Dra.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

Advanced Master
Alta Direção de Cibersegurança

- Modalidade: **online**
- Duração: **2 anos**
- Certificação: **TECH Universidade Tecnológica**
- Créditos: **120 ECTS**
- Horário: **Ao seu ritmo**
- Exames: **online**

Advanced Master
Alta Direção de Cibersegurança