

Mestrado Avançado

Gestão Avançada da Cibersegurança (CISO, Chief Information Security Officer)



Mestrado Avançado Gestão Avançada da Cibersegurança (CISO, Chief Information Security Officer)

- » Modalidade: online
- » Duração: 2 anos
- » Certificação: TECH Global University
- » Acreditação: 120 ECTS
- » Horário: ao seu próprio ritmo
- » Exames: online

Acesso ao site: www.techtitude.com/pt/informatica/mestrado-avancado/mestrado-avancado-gestao-avancada-ciberseguranca-ciso-chief-information-security-officer

Índice

01

Apresentação do programa

pág. 4

02

Porquê estudar na TECH?

pág. 8

03

Plano de estudos

pág. 12

04

Objetivos de ensino

pág. 40

05

Oportunidades de carreira

pág. 46

06

Metodología de estudo

pág. 50

07

Corpo docente

pág. 60

08

Certificação

pág. 70

01

Apresentação do programa

Atualmente, a cibersegurança tornou-se um pilar fundamental para proteger indivíduos e empresas frente ao crescente número de ameaças digitais. Esta disciplina não se foca apenas em salvaguardar os sistemas tecnológicos e a informação crítica das organizações, mas também em liderar o planeamento, implementação e supervisão de estratégias de segurança. Assim, o seu objetivo principal é mitigar riscos e responder de forma eficaz a ciberataques e incidentes. Entre as principais responsabilidades de um Diretor de Cibersegurança destacam-se o desenho de políticas de segurança, a gestão de riscos tecnológicos e a direção de equipas especializadas. Perante os desafios derivados do avanço tecnológico e da digitalização, surge este programa, desenhado especificamente para abordar estas problemáticas. A TECH não se foca somente em garantir a eficiência na proteção da informação, mas também em identificar e gerir novas vulnerabilidades. Isto posiciona o CISO como o elemento mais importante para a resiliência de qualquer organização.





“

Com a TECH, especialize-se e torne-se no líder de uma das direções mais importantes da informática”

A Gestão Avançada da Cibersegurança tem sido fundamental para garantir a estabilidade e continuidade das organizações num mundo digitalizado e altamente interconectado. Através da implementação de estratégias de segurança robustas e da adoção de tecnologias avançadas, têm-se mitigado riscos e prevenido ataques com consequências catastróficas. Em setores críticos como a banca, a saúde e as infraestruturas públicas, a segurança tem sido fortalecida graças à governação e ao cumprimento normativo, impulsionados por líderes especializados nesta área.

Esta disciplina tem permitido às organizações estabelecer ambientes de trabalho digitais mais seguros, fortalecendo assim a confiança de clientes, parceiros e utilizadores. Os resultados bem-sucedidos geraram uma poupança significativa de milhões de dólares em perdas económicas potenciais, ao mesmo tempo que promoveram uma cultura organizacional em que a segurança é uma prioridade partilhada. Além disso, tem-se demonstrado essencial para proteger a inovação, a reputação e a sustentabilidade das organizações num panorama em constante evolução.

O Mestrado Avançado da TECH está desenhado para especializar profissionais na liderança de estratégias de segurança eficazes. Ao longo do programa, o aluno aprenderá ao seu próprio ritmo, focando-se no desenvolvimento de competências diretivas e numa visão empresarial estratégica. Além disso, terá acesso a uma especialização de vanguarda que o prepara para destacar-se numa carreira altamente procurada no mercado global. Graças ao formato 100% online, os participantes poderão conciliar os estudos com as suas responsabilidades profissionais, permitindo-lhes avançar sem comprometer a sua atividade profissional.

Este **Mestrado Avançado em Gestão Avançada da Cibersegurança (CISO, Chief Information Security Officer)** 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
- ♦ Os conteúdos gráficos, esquemáticos e eminentemente práticos, concebidos para oferecer uma informação científica e prática sobre as disciplinas indispensáveis para o exercício profissional
- ♦ Os exercícios práticos onde o processo de autoavaliação pode ser efetuado a fim de melhorar a aprendizagem
- ♦ A sua ênfase especial em metodologias inovadoras em Gestão Avançada da Cibersegurança (CISO, Chief Information Security Officer)
- ♦ As lições teóricas, perguntas aos especialistas, fóruns de discussão sobre temas controversos e trabalhos de reflexão individual
- ♦ A disponibilidade de acesso aos conteúdos a partir de qualquer dispositivo fixo ou portátil com conexão à Internet



Este Mestrado Avançado coloca-o na vanguarda da indústria e abre-lhe inúmeras oportunidades de carreira

“

Desenvolva as competências necessárias para enfrentar os desafios do futuro sem negligenciar as suas atividades atuais”

O seu corpo docente inclui profissionais da área do jornalismo, que trazem a sua experiência profissional para este curso, assim como especialistas reconhecidos de empresas líderes e universidades de prestígio.

O seu conteúdo multimédia, elaborado com a mais recente tecnologia educativa, permitirá ao profissional um aprendizado situado e contextual, ou seja, um ambiente simulado que proporcionará um estudo imersivo programado para treiná-lo em situações reais.

O design deste plano de estudos está centrado na Aprendizagem Baseada em Problemas, através da qual o aluno terá de tentar resolver as diversas situações de prática profissional que lhe serão apresentadas ao longo do curso académico. Para tal, o profissional contará com a ajuda de um sistema inovador de vídeo interativo desenvolvido por especialistas reconhecidos.

Torne-se o protetor das infra-estruturas tecnológicas com o método Relearning que se adapta ao seu ritmo de aprendizagem.

Faça parte da maior universidade digital do mundo e especialize-se a partir de qualquer parte do mundo.



02

Porquê estudar na TECH?

A TECH é a maior universidade digital do mundo. Com um impressionante catálogo de mais de 14.000 programas universitários, disponíveis em 11 línguas, posiciona-se como líder em empregabilidade, com uma taxa de colocação profissional de 99%. Além disso, possui um enorme corpo docente de mais de 6.000 professores de renome internacional.



“

Estuda na maior universidade digital do mundo e garante o teu sucesso profissional. O futuro começa na TECH”

A melhor universidade online do mundo segundo a FORBES

A prestigiada revista Forbes, especializada em negócios e finanças, destacou a TECH como «a melhor universidade online do mundo». Foi o que afirmaram recentemente num artigo da sua edição digital, no qual fazem eco da história de sucesso desta instituição, «graças à oferta académica que proporciona, à seleção do seu corpo docente e a um método de aprendizagem inovador destinado a formar os profissionais do futuro».

Forbes
Mejor universidad
online del mundo

Plan
de estudios
más completo

Os planos de estudos mais completos do panorama universitário

A TECH oferece os planos de estudos mais completos do panorama universitário, com programas que abrangem os conceitos fundamentais e, ao mesmo tempo, os principais avanços científicos nas suas áreas científicas específicas. Além disso, estes programas são continuamente atualizados para garantir aos estudantes a vanguarda académica e as competências profissionais mais procuradas. Desta forma, os cursos da universidade proporcionam aos seus alunos uma vantagem significativa para impulsionar as suas carreiras com sucesso.

O melhor corpo docente top internacional

O corpo docente da TECH é composto por mais de 6.000 professores de renome internacional. Professores, investigadores e quadros superiores de multinacionais, incluindo Isaiah Covington, treinador de desempenho dos Boston Celtics; Magda Romanska, investigadora principal do Harvard MetaLAB; Ignacio Wistumba, presidente do departamento de patologia molecular translacional do MD Anderson Cancer Center; e D.W. Pine, diretor criativo da revista TIME, entre outros.

Profesorado
TOP
Internacional

A maior universidade digital do mundo

A TECH é a maior universidade digital do mundo. Somos a maior instituição educativa, com o melhor e mais extenso catálogo educativo digital, cem por cento online e abrangendo a grande maioria das áreas do conhecimento. Oferecemos o maior número de títulos próprios, pós-graduações e licenciaturas oficiais do mundo. No total, são mais de 14.000 títulos universitários, em onze línguas diferentes, o que nos torna a maior instituição de ensino do mundo.

La metodología
más eficaz

Um método de aprendizagem único

A TECH é a primeira universidade a utilizar o *Relearning* em todos os seus cursos. É a melhor metodologia de aprendizagem online, acreditada com certificações internacionais de qualidade de ensino, fornecidas por agências educacionais de prestígio. Além disso, este modelo académico disruptivo é complementado pelo "Método do Caso", configurando assim uma estratégia única de ensino online. São também implementados recursos didáticos inovadores, incluindo vídeos detalhados, infografias e resumos interativos.

nº1
Mundial
Mayor universidad
online del mundo

A universidade online oficial da NBA

A TECH é a Universidade Online Oficial da NBA. Através de um acordo com a maior liga de basquetebol, oferece aos seus estudantes programas universitários exclusivos, bem como uma grande variedade de recursos educativos centrados no negócio da liga e noutras áreas da indústria desportiva. Cada programa tem um plano de estudos único e conta com oradores convidados excepcionais: profissionais com um passado desportivo distinto que oferecem os seus conhecimentos sobre os temas mais relevantes.

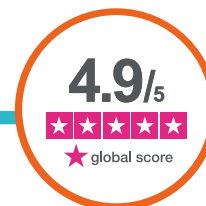
Líderes em empregabilidade

A TECH conseguiu tornar-se a universidade líder em empregabilidade. 99% dos seus estudantes conseguem um emprego na área académica que estudaram, no prazo de um ano após a conclusão de qualquer um dos programas da universidade. Um número semelhante consegue uma melhoria imediata da sua carreira. Tudo isto graças a uma metodologia de estudo que baseia a sua eficácia na aquisição de competências práticas, absolutamente necessárias para o desenvolvimento profissional.



Google Partner Premier

O gigante tecnológico americano atribuiu à TECH o distintivo Google Partner Premier. Este prémio, que só está disponível para 3% das empresas no mundo, destaca a experiência eficaz, flexível e adaptada que esta universidade proporciona aos estudantes. O reconhecimento não só acredita o máximo rigor, desempenho e investimento nas infra-estruturas digitais da TECH, mas também coloca esta universidade como uma das empresas de tecnologia mais avançadas do mundo.



A universidade mais bem classificada pelos seus alunos

Os alunos posicionaram a TECH como a universidade mais bem avaliada do mundo nos principais portais de opinião, destacando a sua classificação máxima de 4,9 em 5, obtida a partir de mais de 1.000 avaliações. Estes resultados consolidam a TECH como uma instituição universitária de referência internacional, refletindo a excelência e o impacto positivo do seu modelo educativo.



03

Plano de estudos

O Mestrado Avançado em Gestão Avançada da Cibersegurança (CISO) está concebido para especializar líderes estratégicos capazes de gerir a segurança da informação em organizações globais. Através de uma abordagem integral e atualizada, o programa abrange áreas chave como a governação da cibersegurança e a gestão de riscos. Desta forma, os alunos desenvolverão competências de liderança para gerir equipas de alto desempenho e implementar políticas de segurança. Além disso, enquanto adquirem conhecimentos sobre as últimas tendências e tecnologias emergentes, os alunos aprenderão a enfrentar os desafios do ambiente digital e a liderar a segurança no futuro.



“

A TECH prepara-o para ser o estratega que previne, deteta e mitiga Ciberameaças em todo o ambiente empresarial global”

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 ciberameaças
 - 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 mais 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. A auditoria na segurança informática
 - 1.5.2. Documentação e autorizações para a auditoria
 - 1.5.3. Tipos de auditoria
 - 1.5.4. Resultados
 - 1.5.4.1. Relatório técnico
 - 1.5.4.2. Relatório executivo
- 1.6. Anonimato na rede
 - 1.6.1. Utilização do 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 nas 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 do utilizador
 - 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 na rede (perimetral)

- 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. Fail2ban
- 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. Utilização 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 eletrónico
 - 3.7.1. Antispam
 - 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 de 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. Roubo de identidade (integridade)
 - 4.6.14. Criptografia fraca ou danificada
 - 4.6.15. Negação de serviço (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. Provas 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. 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 standardizadas
 - 5.1.2.1. ONEM2M
 - 5.1.2.2. IoTWF
 - 5.1.3. Protocolos de aplicação
 - 5.1.4. Tecnologias de conectividade
- 5.2. Dispositivos IoT. Áreas de aplicação
 - 5.2.1. *SmartHome*
 - 5.2.2. *SmartCity*
 - 5.2.3. Transportes
 - 5.2.4. *Wearables*
 - 5.2.5. Setor 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. Conectividade
- 5.7. *Wearables*
 - 5.7.1. Roupas inteligentes
 - 5.7.2. Jóias 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. Conectividade
 - 5.9.1. Wi-Fi/Gateway
 - 5.9.2. Bluetooth
 - 5.9.3. Conectividade 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. Metodologias
 - 6.2.1. OSSTM
 - 6.2.2. OWASP
 - 6.2.3. NIST
 - 6.2.4. PTES
 - 6.2.5. ISSAF
- 6.3. *Footprinting*
 - 6.3.1. Inteligência de fontes abertas (OSINT)
 - 6.3.2. Pesquisa de falhas e vulnerabilidades de dados
 - 6.3.3. Utilização de ferramentas passivas
- 6.4. Verificação de redes
 - 6.4.1. Ferramentas de verificação
 - 6.4.1.1. Nmap
 - 6.4.1.2. Hping3
 - 6.4.1.3. Outras ferramentas de verificação
 - 6.4.2. Técnicas de verificação
 - 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 sem fios
 - 6.7.1. Metodologia de hacking em redes sem fios
 - 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 segurança sem fios
- 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. Utilização de *exploits* conhecidos
 - 6.9.2. Utilização de *metasploit*
 - 6.9.3. Utilização 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. Detecção 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 de montagem
 - 7.3.1. Variáveis
 - 7.3.2. Arrays
 - 7.3.3. Apontadores
 - 7.3.4. Estruturas
 - 7.3.5. Objetos
- 7.4. Estruturas de 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. Reconstructores 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 um *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. Sandbox 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 para a 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. Implementação prática de políticas de segurança de software e hardware

- 9.1. Implementação prática de políticas de segurança de software e hardware
 - 9.1.1. Implementação de identificação e autorização
 - 9.1.2. Implementação de técnicas de identificação
 - 9.1.3. Medidas técnicas de autorização
- 9.2. Tecnologias de identificação e autorização
 - 9.2.1. Identificador e OTP
 - 9.2.2. Token USB ou cartão inteligente PKI
 - 9.2.3. A chave “Confidencial Defesa”
 - 9.2.4. O RFID Ativo
- 9.3. Políticas de segurança no acesso a software e sistemas
 - 9.3.1. Implementação de políticas de controlo de acessos
 - 9.3.2. Implementação de políticas de acesso a comunicações
 - 9.3.3. Tipos de ferramentas de segurança para controlo de acesso
- 9.4. Gestão de acesso a utilizadores
 - 9.4.1. Gestão dos direitos de acesso
 - 9.4.2. Segregação de papéis e funções de acesso
 - 9.4.3. Implementação dos direitos de acesso em sistemas

- 9.5. Controlo de acesso a sistemas e aplicações
 - 9.5.1. Norma do mínimo acesso
 - 9.5.2. Tecnologias seguras de inícios de sessão
 - 9.5.3. Políticas de segurança em palavras-passe
- 9.6. Tecnologias de sistemas de identificação
 - 9.6.1. Diretório ativo
 - 9.6.2. OTP
 - 9.6.3. PAP, CHAP
 - 9.6.4. KERBEROS, DIAMETER, NTLM
- 9.7. Controles CIS para reforço de sistemas
 - 9.7.1. Controles CIS básicos
 - 9.7.2. Controles CIS fundamentais
 - 9.7.3. Controles CIS organizacionais
- 9.8. Segurança na operação
 - 9.8.1. Proteção contra código malicioso
 - 9.8.2. Cópias de segurança
 - 9.8.3. Registo de atividade e monitorização
- 9.9. Gestão das vulnerabilidades técnicas
 - 9.9.1. Vulnerabilidades técnicas
 - 9.9.2. Gestão de vulnerabilidades técnicas
 - 9.9.3. Restrições na instalação de software
- 9.10. Implementação de práticas de políticas de segurança
 - 9.10.1. Vulnerabilidades lógicas
 - 9.10.2. Implementação de políticas de defesa

Módulo 10. Análise forense

- 10.1. Aquisição de dados e duplicação
 - 10.1.1. Aquisição de dados voláteis
 - 10.1.1.1. Informação do sistema
 - 10.1.1.2. Informação da rede
 - 10.1.1.3. Ordem de volatilidade
 - 10.1.2. Aquisição de dados estáticos
 - 10.1.2.1. Criação de uma imagem duplicada
 - 10.1.2.2. Preparação de um documento para a cadeia de custódia



- 10.1.3. Métodos de validação dos dados adquiridos
 - 10.1.3.1. Métodos para Linux
 - 10.1.3.2. Métodos para Windows
- 10.2. Avaliação e derrota de técnicas antiforenses
 - 10.2.1. Objetivos das técnicas antiforenses
 - 10.2.2. Eliminação de dados
 - 10.2.2.1. Eliminação de dados e ficheiros
 - 10.2.2.2. Recuperação de ficheiros
 - 10.2.2.3. Recuperação de partições apagadas
 - 10.2.3. Proteção com palavra-passe
 - 10.2.4. Esteganografia
 - 10.2.5. Limpeza segura de dispositivos
 - 10.2.6. Encriptação
- 10.3. Análise forense do sistema operativo
 - 10.3.1. Análise forense de Windows
 - 10.3.2. Análise forense de Linux
 - 10.3.3. Análise forense de Mac
- 10.4. Análise forense da rede
 - 10.4.1. Análise dos logs
 - 10.4.2. Correlação de dados
 - 10.4.3. Investigação da rede
 - 10.4.4. Passos a seguir na análise forense da rede
- 10.5. Análise forense Web
 - 10.5.1. Investigação de ataques na web
 - 10.5.2. Detecção de ataques
 - 10.5.3. Localização de direções IPs
- 10.6. Análise forense de Bases de Dados
 - 10.6.1. Análise forense em MSSQL
 - 10.6.2. Análise forense em MySQL
 - 10.6.3. Análise forense em PostgreSQL
 - 10.6.4. Análise forense em MongoDB
- 10.7. Análise forense em Cloud
 - 10.7.1. Tipos de crimes em Cloud
 - 10.7.1.1. Cloud como sujeito
 - 10.7.1.2. Cloud como objeto
 - 10.7.1.3. Cloud como ferramenta
 - 10.7.2. Desafios da análise forense em Cloud
 - 10.7.3. Investigação sobre os serviços de armazenamento na Cloud
 - 10.7.4. Ferramentas de análise forense para cloud
- 10.8. Investigação de crimes por correio eletrónico
 - 10.8.1. Sistemas de correio eletrónico
 - 10.8.1.1. Clientes de correio eletrónico
 - 10.8.1.2. Servidor de correio eletrónico
 - 10.8.1.3. Servidor SMTP
 - 10.8.1.4. Servidor POP3
 - 10.8.1.5. Servidor IMAP4
 - 10.8.2. Crimes de correio eletrónico
 - 10.8.3. Mensagem de correio eletrónico
 - 10.8.3.1. Cabeçalhos standard
 - 10.8.3.2. Cabeçalhos extendidos
 - 10.8.4. Passos na investigação destes crimes
 - 10.8.5. Ferramentas forenses para correio eletrónico
- 10.9. Análise forense de telemóveis
 - 10.9.1. Redes celulares
 - 10.9.1.1. Tipos de redes
 - 10.9.1.2. Conteúdos do CDR
 - 10.9.2. *Subscriber Identity Module* (SIM)
 - 10.9.3. Aquisição lógica
 - 10.9.4. Aquisição física
 - 10.9.5. Aquisição do sistema de ficheiros
- 10.10. Redação e apresentação de relatórios forenses
 - 10.10.1. Aspectos importantes de um relatório Forense
 - 10.10.2. Classificação e tipos de relatórios
 - 10.10.3. Guia para escrever um relatório
 - 10.10.4. Apresentação do Relatório
 - 10.10.4.1. Preparação prévia para o depoimento
 - 10.10.4.2. Deposição
 - 10.10.4.3. Lidar com os meios de comunicação social

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. Detecção
 - 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. Planio de segurança. Objetivos
 - 11.8.2. Planio de segurança. Planejamento
 - 11.8.3. Plano de riscos Análise
 - 11.8.4. Políticas de segurança. Implementação na organização
 - 11.8.5. Planio 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. Normativa legal
 - 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 dos riscos
 - 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 RGPD (GDPR)
 - 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. Sistema de gestão da segurança da Informação (SGSI)

- 13.1. Segurança da informação. Aspectos-chave
 - 13.1.1. Segurança da informação
 - 13.1.1.1. Confidencialidade
 - 13.1.1.2. Integração
 - 13.1.1.3. Disponibilidade
 - 13.1.1.4. Medidas de segurança da Informação
- 13.2. Sistemas de gestão da segurança da informação
 - 13.2.1. Modelos de gestão de segurança da informação
 - 13.2.2. Documentos para implementar um SGSI
 - 13.2.3. Níveis e controles de um SGSI
- 13.3. Normas e padrões internacionais
 - 13.3.1. Padrões internacionais na segurança da informação
 - 13.3.2. Origem e evolução do padrão
 - 13.3.3. Padrões internacionais na gestão da segurança da informação
 - 13.3.4. Outras normas de referência
- 13.4. Normas ISO/IEC 27.000
 - 13.4.1. Objeto e âmbito de aplicação
 - 13.4.2. Estrutura da norma
 - 13.4.3. Certificação
 - 13.4.4. Fases de acreditação
 - 13.4.5. Benefícios das normas ISO/IEC 27.000
- 13.5. Projeto e implementação de um sistema geral de segurança da informação
 - 13.5.1. Fases de implementação de um sistema geral de segurança da informação
 - 13.5.2. Planos de continuidade de negócio
- 13.6. Fase I: diagnóstico
 - 13.6.1. Diagnóstico preliminar
 - 13.6.2. Identificação do nível de estratificação
 - 13.6.3. Nível de cumprimento de padrões/normas

- 13.7. Fase II: preparação
 - 13.7.1. Contexto da organização
 - 13.7.2. Análise das normativas de segurança aplicáveis
 - 13.7.3. Escopo do sistema geral de segurança da informação
 - 13.7.4. Política do sistema geral de segurança da informação
 - 13.7.5. Objetivos do sistema geral de segurança da informação
- 13.8. Fase III: planeamento
 - 13.8.1. Classificação de ativos
 - 13.8.2. Avaliação de riscos
 - 13.8.3. Identificação de ameaças e riscos
- 13.9. Fase IV: implementação e acompanhamento
 - 13.9.1. Análise de resultados
 - 13.9.2. Atribuição de responsabilidades
 - 13.9.3. Cronograma do plano de ação
 - 13.9.4. Acompanhamento e auditorias
- 13.10. Políticas de segurança na gestão de incidentes
 - 13.10.1. Fases
 - 13.10.2. Categorização de incidentes
 - 13.10.3. Procedimentos e gestão de incidentes

Módulo 14. Gestão da Segurança IT

- 14.1. Gestão da segurança
 - 14.1.1. Operações de segurança
 - 14.1.2. Aspeto legal e regulamentar
 - 14.1.3. Habilitação do negócio
 - 14.1.4. Gestão de risco
 - 14.1.5. Gestão de identidades e acessos
- 14.2. Estrutura da área de segurança O escritório do CISO
 - 14.2.1. Estrutura organizativa. Posição do CISO na estrutura
 - 14.2.2. As linhas de defesa
 - 14.2.3. Organigrama do escritório do CISO
 - 14.2.4. Gestão orçamental

- 14.3. Governo de segurança
 - 14.3.1. Comité de segurança
 - 14.3.2. Comité de monitorização de riscos
 - 14.3.3. Comité de auditoria
 - 14.3.4. Comité de crise
- 14.4. Governo de segurança. Funções
 - 14.4.1. Políticas e normas
 - 14.4.2. Plano Diretor de segurança
 - 14.4.3. Painel de instrumentos
 - 14.4.4. Sensibilização e formação
 - 14.4.5. Segurança na cadeia de abastecimento
- 14.5. Operações de segurança
 - 14.5.1. Gestão de identidades e acessos
 - 14.5.2. Configuração de regras de segurança de rede. Firewalls
 - 14.5.3. Gestão de plataformas IDS/IPS
 - 14.5.4. Análise de vulnerabilidades
- 14.6. Quadro de trabalho de Cibersegurança NIST CSF
 - 14.6.1. Metodologia NIST
 - 14.6.1.1. Identificar
 - 14.6.1.2. Proteger
 - 14.6.1.3. Detetar
 - 14.6.1.4. Responder
 - 14.6.1.5. Recuperar
- 14.7. Centro de operações de segurança (SOC) Funções
 - 14.7.1. Proteção *Red Team*, *pentesting*, *threat intelligence*
 - 14.7.2. Detecção SIEM, *user behavior analytics*, *fraud prevention*
 - 14.7.3. Resposta
- 14.8. Auditoria de segurança
 - 14.8.1. Teste de intrusão
 - 14.8.2. Exercícios *red team*
 - 14.8.3. Auditorias de código fonte Desenvolvimento seguro
 - 14.8.4. Segurança de componentes (*Software Supply Chain*)
 - 14.8.5. Análise forense

- 14.9. Resposta a incidentes
 - 14.9.1. Preparação
 - 14.9.2. Detecção, análise e notificação
 - 14.9.3. Contenção, erradicação e recuperação
 - 14.9.4. Atividades pós-incidente
 - 14.9.4.1. Retenção de evidências
 - 14.9.4.2. Análise forense
 - 14.9.4.3. Gestão de brechas
 - 14.9.5. Guias oficiais de gestão de ciberincidentes
- 14.10. Gestão de vulnerabilidades
 - 14.10.1. Análise de vulnerabilidades
 - 14.10.2. Avaliação de vulnerabilidade
 - 14.10.3. Base de sistemas
 - 14.10.4. Vulnerabilidade de dia 0. Zero-Day

Módulo 15. Políticas de gestão de incidentes de segurança

- 15.1. Políticas de gestão de incidentes de segurança da informação e melhorias
 - 15.1.1. Gestão de incidentes
 - 15.1.2. Responsabilidades e procedimentos
 - 15.1.3. Notificação de eventos
- 15.2. Sistemas de deteção e prevenção de intrusões (IDS/IPS)
 - 15.2.1. Dados de funcionamento do sistema
 - 15.2.2. Tipos de sistemas de deteção de intrusos
 - 15.2.3. Critérios para a localização dos IDS/IPS
- 15.3. Resposta a incidentes de segurança
 - 15.3.1. Procedimento de recolha de informações
 - 15.3.2. Processo de verificação de intrusão
 - 15.3.3. Organismos CERT
- 15.4. Processo de notificação e gestão de tentativas de intrusão
 - 15.4.1. Responsabilidades no processo de notificação
 - 15.4.2. Classificação dos incidentes
 - 15.4.3. Processo de resolução e recuperação

- 15.5. Análise forense como política de segurança
 - 15.5.1. Evidências voláteis e não voláteis
 - 15.5.2. Análise e recolha de evidências eletrónicas
 - 15.5.2.1. Análise de evidências eletrónicas
 - 15.5.2.2. Recolha de evidências eletrónicas
- 15.6. Ferramentas de Sistemas de deteção e prevenção de intrusões (IDS/IPS)
 - 15.6.1. Snort
 - 15.6.2. Suricata
 - 15.6.3. Solar-Winds
- 15.7. Ferramentas centralizadoras de eventos
 - 15.7.1. SIM
 - 15.7.2. SEM
 - 15.7.3. SIEM
- 15.8. Guia de segurança CCN-STIC 817
 - 15.8.1. Gestão de ciberincidentes
 - 15.8.2. Métricas e Indicadores
- 15.9. NIST SP800-61
 - 15.9.1. Capacidade de resposta a incidentes de segurança informática
 - 15.9.2. Gestão de um incidente
 - 15.9.3. Coordenação e informação partilhada
- 15.10. Normas ISO 27035
 - 15.10.1. Norma ISO 27035. Princípios da gestão de incidentes
 - 15.10.2. Guias para a elaboração de um plano para a gestão de incidentes
 - 15.10.3. Guias de operações na resposta a incidentes

Módulo 16. Análise de riscos e ambiente de segurança IT

- 16.1. Análise do ambiente
 - 16.1.1. Análise da situação conjuntural
 - 16.1.1.1. Ambientes VUCA
 - 16.1.1.1.1. Volátil
 - 16.1.1.1.2. Incerto
 - 16.1.1.1.3. Complexo
 - 16.1.1.1.4. Ambíguo
 - 16.1.1.2. Ambientes BANI
 - 16.1.1.2.1. Frágil
 - 16.1.1.2.2. Ansioso
 - 16.1.1.2.3. Não linear
 - 16.1.1.2.4. Incompreensível
 - 16.1.2. Análise do ambiente geral. PESTEL
 - 16.1.2.1. Político
 - 16.1.2.2. Económico
 - 16.1.2.3. Social
 - 16.1.2.4. Tecnológico
 - 16.1.2.5. Ecológico/Ambiental
 - 16.1.2.6. Legal
 - 16.1.3. Análise da situação interna. SWOT
 - 16.1.3.1. Objetivos
 - 16.1.3.2. Ameaças
 - 16.1.3.3. Oportunidades
 - 16.1.3.4. Pontos fortes
- 16.2. Riscos e incerteza
 - 16.2.1. Risco
 - 16.2.2. Gestão de riscos
 - 16.2.3. Normas de gestão de riscos
- 16.3. Diretrizes para a gestão de riscos ISO 31.000:2018
 - 16.3.1. Objeto
 - 16.3.2. Princípios
 - 16.3.3. Quadro de referência
 - 16.3.4. Processo

- 16.4. Metodologia de análise e gestão de riscos dos sistemas de informação (MAGERIT)
 - 16.4.1. Metodologia MAGERIT
 - 16.4.1.1. Objetivos
 - 16.4.1.2. Método
 - 16.4.1.3. Elementos
 - 16.4.1.4. Técnicas
 - 16.4.1.5. Ferramentas disponíveis
- 16.5. Transferência do risco cibernético
 - 16.5.1. Transferência de riscos
 - 16.5.2. Riscos cibernéticos Tipologia
 - 16.5.3. Seguros de riscos cibernéticos
- 16.6. Metodologias ágeis para a gestão de riscos
 - 16.6.1. Metodologias ágeis
 - 16.6.2. Scrum para a gestão do risco
 - 16.6.3. *Agile Risk Management*
- 16.7. Tecnologias para a gestão do risco
 - 16.7.1. Inteligência artificial aplicada à gestão de riscos
 - 16.7.2. *Blockchain* e criptografia. Métodos de preservação do valor
 - 16.7.3. Computação quântica Oportunidade ou ameaça
- 16.8. Elaboração de mapas de riscos informáticos baseados em metodologias ágeis
 - 16.8.1. Representação da probabilidade e impacto em ambientes ágeis
 - 16.8.2. O risco como ameaça do valor
 - 16.8.3. Re-evolução na gestão de projetos e processos ágeis baseados em KRIs
- 16.9. *Risk Driven* na gestão de riscos
 - 16.9.1. *Risk Driven*
 - 16.9.2. *Risk Driven* na gestão de riscos
 - 16.9.3. Desenvolvimento de um modelo de gestão empresarial impulsionado pelo risco
- 16.10. Inovação e transformação digital na gestão de risco informáticos
 - 16.10.1. A gestão de riscos ágeis como fonte de inovação empresarial
 - 16.10.2. Transformação de dados em informação útil para a tomada de decisões
 - 16.10.3. Visão holística da empresa através do risco

Módulo 17. Políticas de segurança para análise de ameaças em sistemas informáticos

- 17.1. A gestão de ameaças nas políticas de segurança
 - 17.1.1. A gestão do risco
 - 17.1.2. O risco em segurança
 - 17.1.3. Metodologias na gestão de ameaças
 - 17.1.4. Implementação de metodologias
- 17.2. Fases da gestão de ameaças
 - 17.2.1. Identificação
 - 17.2.2. Análise
 - 17.2.3. Localização
 - 17.2.4. Medidas de salvaguarda
- 17.3. Sistemas de auditoria para localização de ameaças
 - 17.3.1. Classificação e fluxo de informação
 - 17.3.2. Análise dos processos vulneráveis
- 17.4. Classificação de riscos
 - 17.4.1. Tipos de risco
 - 17.4.2. Cálculo da probabilidade de ameaça
 - 17.4.3. Risco residual
- 17.5. Tratamento do Risco
 - 17.5.1. Implementação de medidas de salvaguarda
 - 17.5.2. Transferir ou assumir
- 17.6. Controlo de risco
 - 17.6.1. Processo contínuo de gestão de risco
 - 17.6.2. Implementação de métricas de segurança
 - 17.6.3. Modelo estratégico de métricas em segurança da informação
- 17.7. Metodologias práticas para a análise e controlo de ameaças
 - 17.7.1. Catálogo de ameaças
 - 17.7.2. Catálogo de medidas de controlo
 - 17.7.3. Catálogo de salvaguardas

- 17.8. Normas ISO 27005
 - 17.8.1. Identificação do risco
 - 17.8.2. Análise de risco
 - 17.8.3. Avaliação do risco
- 17.9. Matriz de risco, impacto e ameaças
 - 17.9.1. Dados, sistemas e pessoal
 - 17.9.2. Probabilidade de ameaça
 - 17.9.3. Magnitude do dano
- 17.10. Projeto de fases e processos na análise de ameaças
 - 17.10.1. Identificação dos elementos críticos da organização
 - 17.10.2. Determinação de ameaças e impactos
 - 17.10.3. Análise do impacto e risco
 - 17.10.4. Metodologias

Módulo 18. Implementação prática de políticas de segurança perante ataques

- 18.1. *System Hacking*
 - 18.1.1. Riscos e vulnerabilidades
 - 18.1.2. Contramedidas
- 18.2. DoS em serviços
 - 18.2.1. Riscos e vulnerabilidades
 - 18.2.2. Contramedidas
- 18.3. *Session Hijacking*
 - 18.3.1. O processo de *Hijacking*
 - 18.3.2. Contramedidas ao *Hijacking*
- 18.4. Evasão de IDS, *Firewalls* and *Honeypots*
 - 18.4.1. Técnicas de evasão
 - 18.4.2. Implementação de contramedidas
- 18.5. *Hacking Web Servers*
 - 18.5.1. Ataques a servidores web
 - 18.5.2. Implementação de medidas de defesa

- 18.6. *Hacking Web Applications*
 - 18.6.1. Ataques a aplicações web
 - 18.6.2. Implementação de medidas de defesa
- 18.7. *Hacking Wireless Networks*
 - 18.7.1. Vulnerabilidades em redes Wi-Fi
 - 18.7.2. Implementação de medidas de defesa
- 18.8. *Hacking Mobile Platforms*
 - 18.8.1. Vulnerabilidades de plataformas móveis
 - 18.8.2. Implementação de contramedidas
- 18.9. *Ransomware*
 - 18.9.1. Vulnerabilidades causadoras do Ransomware
 - 18.9.2. Implementação de contramedidas
- 18.10. Engenharia social
 - 18.10.1. Tipos de engenharia social
 - 18.10.2. Contramedidas para a engenharia social

Módulo 19. Criptografia em IT

- 19.1. Criptografia
 - 19.1.1. Criptografia
 - 19.1.2. Fundamentos matemáticos
- 19.2. Criptologia
 - 19.2.1. Criptologia
 - 19.2.2. Criptoanálise
 - 19.2.3. Criptoanálise
- 19.3. Protocolos criptográficos
 - 19.3.1. Blocos básicos
 - 19.3.2. Protocolos básicos
 - 19.3.3. Protocolos intermédios
 - 19.3.4. Protocolos avançados
 - 19.3.5. Protocolos esotéricos

- 19.4. Técnicas criptográficas
 - 19.4.1. Longitude de chaves
 - 19.4.2. Gestão de chaves
 - 19.4.3. Tipos de algoritmos
 - 19.4.4. Funções resumo. *Hash*
 - 19.4.5. Geradores de números pseudoaleatórios
 - 19.4.6. Uso de algoritmos
- 19.5. Criptografia simétrica
 - 19.5.1. Cifras de bloco
 - 19.5.2. DES (*Data Encryption Standard*)
 - 19.5.3. Algoritmo RC4
 - 19.5.4. AES (*Advanced Encryption Standard*)
 - 19.5.5. Combinação de cifras de bloco
 - 19.5.6. Derivação de chaves
- 19.6. Criptografia assimétrica
 - 19.6.1. Diffie-Hellman
 - 19.6.2. DSA (*Digital Signature Algorithm*)
 - 19.6.3. RSA (Rivest, Shamir e Adleman)
 - 19.6.4. Curva elíptica
 - 19.6.5. Criptografia assimétrica Tipologia
- 19.7. Certificados digitais
 - 19.7.1. Assinatura digital
 - 19.7.2. Certificados X509
 - 19.7.3. Infraestrutura de chave pública (PKI)
- 19.8. Implementações
 - 19.8.1. Kerberos
 - 19.8.2. IBM CCA
 - 19.8.3. *Pretty Good Privacy* (PGP)
 - 19.8.4. *ISO Authentication Framework*
 - 19.8.5. SSL e TLS
 - 19.8.6. Cartões inteligentes em meios de pagamento (EMV)
 - 19.8.7. Protocolos de telefonia móvel
 - 19.8.8. *Blockchain*

- 19.9. Esteganografia
 - 19.9.1. Esteganografia
 - 19.9.2. Estegoanálise
 - 19.9.3. Aplicações e usos
- 19.10. Criptografia quântica
 - 19.10.1. Algoritmos quânticos
 - 19.10.2. Proteção de algoritmos frente à computação quântica
 - 19.10.3. Distribuição de chave quântica

Módulo 20. Gestão de identidade e acessos em segurança IT

- 20.1. Gestão de identidade e acessos (IAM)
 - 20.1.1. Identidade digital
 - 20.1.2. Gestão de identidade
 - 20.1.3. Federação de identidades
- 20.2. Controlo de acesso físico
 - 20.2.1. Sistemas de proteção
 - 20.2.2. Segurança das áreas
 - 20.2.3. Instalações de recuperação
- 20.3. Controlo de acesso lógico
 - 20.3.1. Autenticação: Tipologia
 - 20.3.2. Protocolos de autenticação
 - 20.3.3. Ataques de autenticação
- 20.4. Controlo de acesso lógico. Autenticação MFA
 - 20.4.1. Controlo de acesso lógico. Autenticação MFA
 - 20.4.2. Palavras-passe Importância
 - 20.4.3. Ataques de autenticação
- 20.5. Controlo de acesso lógico. Autenticação biométrica
 - 20.5.1. Controlo de acesso lógico. Autenticação biométrica
 - 20.5.1.1. Autenticação biométrica Requisitos
 - 20.5.2. Funcionamento
 - 20.5.3. Modelo e técnicas
- 20.6. Sistemas de gestão de autenticação
 - 20.6.1. *Single Sign On*
 - 20.6.2. Kerberos
 - 20.6.3. Sistemas AAA

20.7. Sistemas de gestão de autenticação: Sistemas AAA

20.7.1. TACACS

20.7.2. RADIUS

20.7.3. DIAMETER

20.8. Serviços de controlo de acesso

20.8.1. FW - Firewall

20.8.2. VPN - Redes Privadas Virtuais

20.8.3. IDS - Sistema de Detecção de Intrusões

20.9. Sistema de controlo de acesso à rede

20.9.1. NAC

20.9.2. Arquitetura e elementos

20.9.3. Funcionamento e normalização

20.10. Acesso a redes sem fios

20.10.1. Tipos de redes sem fios

20.10.2. Segurança em redes sem fios

20.10.3. Ataques em redes sem fios

Módulo 21. Segurança em comunicações e operação software

21.1. Segurança informática em comunicações e operação software

21.1.1. Segurança Informática

21.1.2. Cibersegurança

21.1.3. Segurança na nuvem

21.2. Segurança informática em comunicações e operação software. Tipologia

21.2.1. Segurança física

21.2.2. Segurança lógica

21.3. Segurança em comunicações

21.3.1. Principais elementos

21.3.2. Segurança de redes

21.3.3. Melhores práticas

21.4. Ciberinteligência

21.4.1. Engenharia social

21.4.2. Deep Web

21.4.3. Phishing

21.4.4. Malware

21.5. Desenvolvimento seguro em comunicações e operação software

21.5.1. Desenvolvimento seguro. Protocolo HTTP

21.5.2. Desenvolvimento seguro. Ciclo de vida

21.5.3. Desenvolvimento seguro. Segurança PHP

21.5.4. Desenvolvimento seguro. Segurança NET

21.5.5. Desenvolvimento seguro. Melhores práticas

21.6. Sistemas de gestão de segurança da informação em comunicações e operação software

21.6.1. GDPR

21.6.2. ISO 27021

21.6.3. ISO 27017/ 18

21.7. Tecnologias SIEM

21.7.1. Tecnologias SIEM

21.7.2. Operativa de SOC

21.7.3. SIEM vendors

21.8. A função da segurança nas organizações

21.8.1. Funções nas organizações

21.8.2. Função dos especialistas IoT nas empresas

21.8.3. Certificações reconhecidas no mercado

21.9. Análise forense

21.9.1. Análise forense

21.9.2. Análise forense. Metodologia

21.9.3. Análise forense. Ferramentas e implantação

21.10. A cibersegurança na atualidade

21.10.1. Principais ataques informáticos

21.10.2. Previsões de empregabilidade

21.10.3. Desafios

Módulo 22. Segurança em ambientes *cloud*

- 22.1. Segurança em ambientes *cloud computing*
 - 22.1.1. Segurança em ambientes *cloud computing*
 - 22.1.2. Segurança em ambientes *cloud computing*. Ameaças e riscos segurança
 - 22.1.3. Segurança em ambientes *cloud computing*. Aspectos chave de segurança
- 22.2. Tipos de infraestrutura *cloud*
 - 22.2.1. Público
 - 22.2.2. Privado
 - 22.2.3. Híbrido
- 22.3. Modelo de gestão partilhada
 - 22.3.1. Elementos de segurança geridos por fornecedor
 - 22.3.2. Elementos geridos por cliente
 - 22.3.3. Definição da estratégia para a segurança
- 22.4. Mecanismos de prevenção
 - 22.4.1. Sistemas de gestão de autenticação
 - 22.4.2. Sistemas de gestão de autorização: Políticas de acesso
 - 22.4.3. Sistemas de gestão de chaves
- 22.5. Securitização de sistemas
 - 22.5.1. Securitização dos sistemas de armazenamento
 - 22.5.2. Proteção dos sistemas de base de dados
 - 22.5.3. Securitização de dados em trânsito
- 22.6. Proteção de infraestrutura
 - 22.6.1. Desenho e implementação de rede segura
 - 22.6.2. Segurança de recursos de computação
 - 22.6.3. Ferramentas e recursos para proteção de infraestrutura
- 22.7. Detecção as ameaças e ataques
 - 22.7.1. Sistemas de auditoria, *logging* e monitorização
 - 22.7.2. Sistemas de eventos e alarmes
 - 22.7.3. Sistemas SIEM

- 22.8. Resposta a incidentes
 - 22.8.1. Plano de resposta a incidentes
 - 22.8.2. A continuidade do negócio
 - 22.8.3. Análise forense e remediação de incidentes da mesma natureza
- 22.9. Segurança em *clouds* públicas
 - 22.9.1. AWS (Amazon Web Services)
 - 22.9.2. Microsoft Azure
 - 22.9.3. Google GCP
 - 22.9.4. Oracle Cloud
- 22.10. Normativa e cumprimento
 - 22.10.1. Cumprimento de normativas de segurança
 - 22.10.2. Gestão de risco
 - 22.10.3. Pessoas e processo nas organizações

Módulo 23. Ferramentas de Monitorização em Políticas de Segurança dos sistemas de informação

- 23.1. Políticas de monitorização de sistemas de informação
 - 23.1.1. Monitorização de Sistemas
 - 23.1.2. Métricas
 - 23.1.3. Tipos de métricas
- 23.2. Auditoria e registo em Sistemas
 - 23.2.1. Auditoria e registo em Windows
 - 23.2.2. Auditoria e registo em Linux
- 23.3. Protocolo SNMP. *Simple Network Management Protocol*
 - 23.3.1. Protocolo SNMP
 - 23.3.2. Funcionamento de SNMP
 - 23.3.3. Ferramentas SNMP
- 23.4. Monitorização de redes
 - 23.4.1. A monitorização de rede em sistemas de controlo
 - 23.4.2. Ferramentas de monitorização para sistemas de controlo

23.5. Nagios. Sistema de monitorização de redes

23.5.1. Nagios

23.5.2. Funcionamento de Nagios

23.5.3. Instalação de Nagios

23.6. Zabbix. Sistema de monitorização de redes

23.6.1. Zabbix

23.6.2. Funcionamento de Zabbix

23.6.3. Instalação de Zabbix

23.7. Cacti. Sistema de monitorização de redes

23.7.1. Cacti

23.7.2. Funcionamento de Cacti

23.7.3. Instalação de Cacti

23.8. Pandora. Sistema de monitorização de redes

23.8.1. Pandora

23.8.2. Funcionamento de Pandora

23.8.3. Instalação de Pandora

23.9. SolarWinds. Sistema de monitorização de redes

23.9.1. SolarWinds

23.9.2. Funcionamento de SolarWinds

23.9.3. Instalação de SolarWinds

23.10. Normativa sobre monitorização

23.10.1. Controlo CIS sobre auditoria e registo

23.10.2. NIST 800-123 (EUA)

Módulo 24. Segurança em comunicações de dispositivos IoT

24.1. Da telemetria à IoT

24.1.1. Telemetria

24.1.2. Conetividade M2M

24.1.3. Democratização da telemetria

24.2. Modelos de referência IoT

24.2.1. Modelos de referência IoT

24.2.2. Arquitetura simplificada IoT

24.3. Vulnerabilidade de segurança da IoT

24.3.1. Dispositivos IoT

24.3.2. Dispositivos IoT. Estudos de casos de utilização

24.3.3. Dispositivos IoT. Vulnerabilidades

24.4. Conetividade da IoT

24.4.1. Redes PAN, LAN, WAN

24.4.2. Tecnologias sem fios na IoT

24.4.3. Tecnologias sem fios na LPWAN

24.5. Tecnologias LPWAN

24.5.1. O triângulo de ferro das LPWAN

24.5.2. Bandas de frequência livre vs. Bandas licenciadas

24.5.3. Opções de tecnologias LPWAN

24.6. Tecnologia LoRaWAN

24.6.1. Tecnologia LoRaWAN

24.6.2. Casos de utilização LoRaWAN Ecosystema

24.6.3. Segurança em LoRaWAN

24.7. Tecnologia Sigfox

24.7.1. Tecnologia Sigfox

24.7.2. Casos de utilização Sigfox. Ecosystema

24.7.3. Segurança em Sigfox

24.8. Tecnologia Celular IoT

24.8.1. Tecnologia Celular IoT (NB-IoT e LTE-M)

24.8.2. Casos de utilização Celular IoT Ecosystema

24.8.3. Segurança em Celular IoT

24.9. Tecnologia WiSUN

24.9.1. Tecnologia WiSUN

24.9.2. Casos de utilização WiSUN. Ecosystema

24.9.3. Segurança em WiSUN

24.10. Outras tecnologias IoT

24.10.1. Outras tecnologias IoT

24.10.2. Casos de utilização e ecosystema de outras tecnologias IoT

24.10.3. Segurança em outras tecnologias IoT

Módulo 25. Plano de continuidade do negócio associado à segurança

- 25.1. Planos de continuidade de negócio
 - 25.1.1. Os planos de continuidade de negócio (BCPs)
 - 25.1.2. Plano de continuidade de negócio (PCN). Aspectos-chave
 - 25.1.3. Plano de continuidade de negócio (PCN) para a avaliação da empresa
- 25.2. Métricas num plano de continuidade de negócio (PCN)
 - 25.2.1. *Recovery time objective* (RTO) e *recovery point objective* (RPO)
 - 25.2.2. Tempo máximo tolerável (MTD)
 - 25.2.3. Níveis mínimos de recuperação (ROL)
 - 25.2.4. Ponto de recuperação objetivo (RPO)
- 25.3. Projetos de continuidade. Tipologia
 - 25.3.1. Plano de continuidade de negócio (PCN)
 - 25.3.2. Plano de continuidade de TIC (PCTIC)
 - 25.3.3. Plano de recuperação em caso de desastres (PRD)
- 25.4. Gestão de riscos associada ao PCN
 - 25.4.1. Análise de impacto no negócio
 - 25.4.2. Benefícios da implementação de um PCN
 - 25.4.3. Mentalidade baseada em riscos
- 25.5. Ciclo de vida de um plano de continuidade de negócio
 - 25.5.1. Fase 1: Análise da Organização
 - 25.5.2. Fase 2: Determinação da estratégia de continuidade
 - 25.5.3. Fase 3: Resposta à contingência
 - 25.5.4. Fase 4: Prova, manutenção e revisão
- 25.6. Fase de análise da organização de um PCN
 - 25.6.1. Identificação de processos no âmbito do PCN
 - 25.6.2. Identificação de áreas críticas do negócio
 - 25.6.3. Identificação de dependências entre áreas e processos
 - 25.6.4. Determinação do MTD adequado
 - 25.6.5. Documentos a entregar Criação de um plano
- 25.7. Fase de determinação da estratégia de continuidade num PCN
 - 25.7.1. Funções na fase de determinação da estratégia
 - 25.7.2. Tarefas da fase de determinação da estratégia
 - 25.7.3. Resultados

- 25.8. Fase de resposta à contingência num PCN
 - 25.8.1. Funções na fase de resposta
 - 25.8.2. Tarefas nesta fase
 - 25.8.3. Resultados
- 25.9. Fase de testes, manutenção e revisão de um PCN
 - 25.9.1. Funções na fase de testes, manutenção e revisão
 - 25.9.2. Tarefas na fase de testes, manutenção e revisão
 - 25.9.3. Resultados
- 25.10. Normas ISO associadas aos planos de continuidade de negócios (PCN)
 - 25.10.1. ISO 22301:2019
 - 25.10.2. ISO 22313:2020
 - 25.10.3. Outras normas ISO e internacionais relacionadas

Módulo 26. Política de Recuperação Prática de Desastres de Segurança

- 26.1. DRP. Plano de Recuperação de Desastres
 - 26.1.1. Objetivo de um DRP
 - 26.1.2. Benefícios de um DRP
 - 26.1.3. Consequências da ausência de um DRP e não atualizado
- 26.2. Guia para definir um DRP (Plano de Recuperação de Desastres)
 - 26.2.1. Escopo e objetivos
 - 26.2.2. Desenho da estratégia de recuperação
 - 26.2.3. Atribuição de papéis e responsabilidades
 - 26.2.4. Realização de um Inventário de hardware, software e serviços
 - 26.2.5. Tolerância para tempo de inatividade e perda de dados
 - 26.2.6. Estabelecimento dos tipos específicos de DRPs que são necessários
 - 26.2.7. Realização de um Plano de formação, sensibilização e comunicação
- 26.3. Escopo e objetivos de um DRP (Plano de Recuperação de Desastres)
 - 26.3.1. Garantia de resposta
 - 26.3.2. Componentes tecnológicos
 - 26.3.3. Escopo da política de continuidade

- 26.4. Desenho da Estratégia de um DRP (Recuperação de Desastre)
 - 26.4.1. Estratégia de Recuperação de Desastre
 - 26.4.2. Orçamento
 - 26.4.3. Recursos Humanos e Físicos
 - 26.4.4. Posições gerenciais em risco
 - 26.4.5. Tecnologia
 - 26.4.6. Dados
- 26.5. Continuidade dos processos de informação
 - 26.5.1. Planejamento da continuidade
 - 26.5.2. Implementação da continuidade
 - 26.5.3. Verificação e avaliação da continuidade
- 26.6. Escopo de um BCP (Plano de Continuidade Empresarial)
 - 26.6.1. Determinação dos processos de maior criticidade
 - 26.6.2. Enfoque por ativo
 - 26.6.3. Enfoque por processo
- 26.7. Implementação dos processos garantidos de negócio
 - 26.7.1. Atividades Prioritárias (AP)
 - 26.7.2. Tempos de recuperação ideais (TRI)
 - 26.7.3. Estratégias de sobrevivência
- 26.8. Análise da organização
 - 26.8.1. Obtenção de informações
 - 26.8.2. Análise de impacto sobre o negócio (BIA)
 - 26.8.3. Análise de riscos na organização
- 26.9. Resposta à contingência
 - 26.9.1. Plano de crise
 - 26.9.2. Planos operacionais de recuperação de ambientes
 - 26.9.3. Procedimentos técnicos de trabalho ou de incidentes
- 26.10. Norma Internacional ISO 27031 BCP
 - 26.10.1. Objetivos
 - 26.10.2. Termos e definições
 - 26.10.3. Funcionamento

Módulo 27. Implementação de políticas de segurança física e ambiental na empresa

- 27.1. Áreas seguras
 - 27.1.1. Perímetro de segurança física
 - 27.1.2. Trabalho em áreas seguras
 - 27.1.3. Segurança de escritórios, gabinetes e recursos
- 27.2. Controles físicos de entrada
 - 27.2.1. Políticas de controlo de acesso físico
 - 27.2.2. Sistemas de controlo físico de entrada
- 27.3. Vulnerabilidades de acessos físicos
 - 27.3.1. Principais vulnerabilidades físicas
 - 27.3.2. Implementação de medidas de salvaguardas
- 27.4. Sistemas biométricos fisiológicos
 - 27.4.1. Impressão digital
 - 27.4.2. Reconhecimento facial
 - 27.4.3. Reconhecimento de íris e retina
 - 27.4.4. Outros sistemas biométricos fisiológicos
- 27.5. Sistemas biométricos de comportamento
 - 27.5.1. Reconhecimento de assinatura
 - 27.5.2. Reconhecimento de escrita
 - 27.5.3. Reconhecimento de voz
 - 27.5.4. Outros sistemas biométricos de comportamentos
- 27.6. Gestão de riscos em biometria
 - 27.6.1. Implementação de sistemas biométricos
 - 27.6.2. Vulnerabilidades dos sistemas biométricos
- 27.7. Implementação de políticas em hosts
 - 27.7.1. Instalação de fornecimento e segurança de cablagem
 - 27.7.2. Localização dos equipamentos
 - 27.7.3. Saída dos equipamentos fora das dependências
 - 27.7.4. Equipamento informático desatendido e política de posto limpo

- 27.8. Proteção ambiental
 - 27.8.1. Sistemas de proteção contra incêndios
 - 27.8.2. Sistemas de proteção contra sismos
 - 27.8.3. Sistemas de proteção contra terremotos
- 27.9. Segurança em centro de processamento de dados
 - 27.9.1. Portas de segurança
 - 27.9.2. Sistemas de videovigilância (CCTV)
 - 27.9.3. Controlo de segurança
- 27.10. Normativa internacional da segurança física
 - 27.10.1. IEC 62443-2-1 (europeia)
 - 27.10.2. NERC CIP-005-5 (EUA)
 - 27.10.3. NERC CIP-014-2 (EUA)

Módulo 28. Políticas de comunicações seguras na empresa

- 28.1. Gestão da segurança nas redes
 - 28.1.1. Controlo e monitorização de rede
 - 28.1.2. Segregação de redes
 - 28.1.3. Sistemas de segurança em redes
- 28.2. Protocolos seguros de comunicação
 - 28.2.1. Modelo TCP/IP
 - 28.2.2. Protocolo IPSEC
 - 28.2.3. Protocolo TLS
- 28.3. Protocolo TLS 1.3
 - 28.3.1. Fases de um processo TLS1.3
 - 28.3.2. Protocolo *Handshake*
 - 28.3.3. Protocolo de registo
 - 28.3.4. Diferenças com TLS 1.2
- 28.4. Algoritmos criptográficos
 - 28.4.1. Algoritmos criptográficos usados em comunicações
 - 28.4.2. *Cipher-suites*
 - 28.4.3. Algoritmos criptográficos permitidos para TLS 1.3

- 28.5. Funções Digest
 - 28.5.1. MD6
 - 28.5.2. SHA
- 28.6. PKI. Infraestrutura de chave pública
 - 28.6.1. PKI e suas entidades
 - 28.6.2. Certificado digital
 - 28.6.3. Tipos de certificados digitais
- 28.7. Comunicações de túnel e transporte
 - 28.7.1. Comunicações túnel
 - 28.7.2. Comunicações transporte
 - 28.7.3. Implementação túnel cifrado
- 28.8. SSH. *Secure Shell*
 - 28.8.1. SSH. Cápsula segura
 - 28.8.2. Funcionamento de SSH
 - 28.8.3. Ferramentas SSH
- 28.9. Auditoria de sistemas criptográficos
 - 28.9.1. Testes de integridade
 - 28.9.2. Testagem de sistema criptográfico
- 28.10. Sistemas criptográficos
 - 28.10.1. Vulnerabilidades sistemas criptográficos
 - 28.10.2. Salvaguardas em criptografia

Módulo 29. Aspetos organizativos em política de segurança da informação

- 29.1. Organização interna
 - 29.1.1. Atribuição de responsabilidades
 - 29.1.2. Segregação de tarefas
 - 29.1.3. Contactos com autoridades
 - 29.1.4. Segurança da informação na gestão de projetos
- 29.2. Gestão de ativos
 - 29.2.1. Responsabilidade sobre os ativos
 - 29.2.2. Classificação da informação
 - 29.2.3. Manuseamento de suportes de armazenamento

- 29.3. Políticas de segurança nos processos de negócio
 - 29.3.1. Análise dos processos de negócio vulneráveis
 - 29.3.2. Análise de impacto de negócio
 - 29.3.3. Classificação de processos em relação ao impacto de negócio
- 29.4. Políticas de segurança ligada aos Recursos Humanos
 - 29.4.1. Antes de contratação
 - 29.4.2. Durante a contratação
 - 29.4.3. Cesse ou mudança de posto de trabalho
- 29.5. Políticas de segurança na direção
 - 29.5.1. Diretrizes da direção em segurança da informação
 - 29.5.2. BIA- Analisando o impacto
 - 29.5.3. Plano de recuperação como política de segurança
- 29.6. Aquisição e manutenção dos sistemas de informação
 - 29.6.1. Requisitos de segurança dos sistemas de informação
 - 29.6.2. Segurança nos dados de desenvolvimento e suporte
 - 29.6.3. Dados de teste
- 29.7. Segurança com fornecedores
 - 29.7.1. Segurança informática com fornecedores
 - 29.7.2. Gestão da prestação do serviço com garantia
 - 29.7.3. Segurança na cadeia de fornecimento
- 29.8. Segurança operacional
 - 29.8.1. Responsabilidades na operação
 - 29.8.2. Proteção contra código malicioso
 - 29.8.3. Cópias de segurança
 - 29.8.4. Registos de atividade e supervisão
- 29.9. Gestão da segurança e normativas
 - 29.9.1. Cumprimento dos requisitos legais
 - 29.9.2. Revisões na segurança da informação
- 29.10. Segurança na gestão para a continuidade de negócio
 - 29.10.1. Continuidade da segurança da informação
 - 29.10.2. Redundâncias





“

Um plano de estudos completo da TECH aprenderá a ser um líder visionário que garante a proteção a longo prazo da organização”

04

Objetivos de ensino

O Mestrado Avançado em Gestão Avançada da Cibersegurança (CISO) tem como objetivo formar líderes estratégicos capazes de gerir a segurança da informação em qualquer tipo de organização. Ao longo do programa, os participantes desenvolverão competências para identificar, avaliar e mitigar riscos cibernéticos, implementar políticas de segurança eficazes. Além disso, será proporcionado um entendimento profundo das tecnologias emergentes e das melhores práticas em arquitetura de segurança, garantindo a proteção de dados e a continuidade do negócio. O programa também fomenta uma visão empresarial integrada da cibersegurança, alinhando as iniciativas com os objetivos corporativos e garantindo o cumprimento das normativas internacionais. Os alunos estarão preparados para serem agentes de mudança e promover uma cultura organizacional focada na proteção digital.



“

*Nesta especialização 100% online
encontrará o material didático e
as pesquisas mais atualizadas do
panorama universitário”*



Objetivos gerais

- ♦ Desenvolver líderes estratégicos em cibersegurança que possam gerir a proteção dos ativos digitais e das infraestruturas tecnológicas de organizações globais
- ♦ Integrar a cibersegurança dentro da estratégia empresarial, alinhando as iniciativas de proteção digital com os objetivos globais da organização
- ♦ Capacitar na implementação de políticas e marcos normativos de cibersegurança que assegurem o cumprimento regulatório e a proteção da informação em ambientes digitais
- ♦ Fomentar a liderança e a direção de equipas de cibersegurança, melhorando a capacidade de tomar decisões estratégicas em situações de crise e gerir projetos de segurança a nível organizacional



Junte-se à TECH e desenvolva as habilidades necessárias para se tornar um líder que antecipa as ameaças e fortalece as oportunidades”





Objetivos específicos

Módulo 1. Ciberinteligência e cibersegurança

- ♦ Desenvolver as competências necessárias para implementar estratégias de ciberinteligência e Cibersegurança
- ♦ Proteger os sistemas informáticos contra ameaças cibernéticas através da recolha, análise e utilização de inteligência digital

Módulo 2. Segurança em Host

- ♦ Capacitar na Implementação de medidas de segurança em sistemas host
- ♦ Assegurar a proteção de servidores e dispositivos contra vulnerabilidades, *malware* e acessos não autorizados

Módulo 3. Segurança na rede (perimetral)

- ♦ Proporcionar os conhecimentos necessários para proteger as redes informáticas a nível perimetral
- ♦ Gerir técnicas e ferramentas de segurança como firewalls, VPNs e sistemas de deteção de intrusos

Módulo 4. Segurança em *smartphones*

- ♦ Fornecer uma compreensão completa sobre a segurança em dispositivos móveis
- ♦ Aprofundar a proteção contra ameaças como *malware*, perda de dados e ataques através de aplicações móveis

Módulo 5. Segurança em IoT

- ♦ Capacitar na implementação de políticas de segurança para dispositivos IoT
- ♦ Proteger a infraestrutura e os dados gerados por dispositivos conectados através de redes e plataformas IoT

Módulo 6. Hacking ético

- ♦ Desenvolver as competências necessárias para realizar testes de penetração e auditorias de segurança utilizando técnicas de hacking ético
- ♦ Ser capaz de identificar vulnerabilidades e prevenir ataques

Módulo 7. Engenharia reversa

- ♦ Dominar técnicas de engenharia inversa para analisar e compreender o funcionamento de software e *hardware*
- ♦ Identificar possíveis vulnerabilidades e soluções de segurança

Módulo 8. Desenvolvimento seguro

- ♦ Ensinar as melhores práticas de desenvolvimento seguro de software
- ♦ Aplicar princípios de segurança durante todo o ciclo de vida do desenvolvimento para minimizar riscos e vulnerabilidades nas aplicações

Módulo 9. Implementação prática de políticas de segurança em software e *hardware*

- ♦ Proporcionar os conhecimentos necessários para desenhar e implementar políticas de segurança robustas em software e hardware
- ♦ Assegurar a proteção contra ameaças internas e externas

Módulo 10. Análise forense

- ♦ Desenvolver as competências na análise forense digital
- ♦ Analisar a recolha, preservação e análise de provas digitais em casos de incidentes de segurança informática

Módulo 11. Segurança no desenho e desenvolvimento de sistemas

- ♦ Abordar a integração de medidas de segurança desde as fases de design e desenvolvimento de sistemas informáticos
- ♦ Garantir a proteção contra possíveis vulnerabilidades desde o início do projeto

Módulo 12. Arquiteturas e modelos de segurança da informação

- ♦ Proporcionar os conhecimentos necessários sobre as arquiteturas e modelos de segurança da informação
- ♦ Desenhar e implementar sistemas robustos que protejam os dados e recursos da organização

Módulo 13. Sistema de gestão da segurança da Informação (SGSI)

- ♦ Implementar um Sistema de Gestão de Segurança da Informação
- ♦ Proteger a informação empresarial de forma eficaz, assegurando o cumprimento das normas e boas práticas

Módulo 14. Gestão da Segurança IT

- ♦ Proporcionar os conhecimentos necessários para gerir de forma eficaz a segurança nas infraestruturas tecnológicas da empresa
- ♦ Minimizar os riscos e garantir a continuidade operativa

Módulo 15. Políticas de gestão de incidentes de segurança

- ♦ Capacitar na criação e aplicação de políticas eficazes para a gestão de incidentes de segurança
- ♦ Estabelecer protocolos claros para deteção, análise e resposta a brechas de segurança

Módulo 16. Análise de riscos e ambiente de segurança IT

- ♦ Proporcionar os conhecimentos necessários para realizar uma análise de riscos no ambiente de TI, identificando ameaças e vulnerabilidades
- ♦ Aplicar estratégias de mitigação para assegurar a infraestrutura tecnológica

Módulo 17. Políticas de segurança para análise de ameaças em sistemas informáticos

- ♦ Capacitar no desenvolvimento de políticas de segurança para identificar, analisar e mitigar as ameaças nos sistemas informáticos
- ♦ Utilizar ferramentas e métodos adequados para proteger os ativos digitais da organização

Módulo 18. Implementação prática de políticas de segurança perante ataques

- ♦ Implementar políticas de segurança eficazes contra possíveis ataques
- ♦ Assegurar a proteção dos sistemas e da informação crítica na organização

Módulo 19. Criptografia em IT

- ♦ Ensinar os fundamentos e aplicações da criptografia no âmbito da tecnologia da informação
- ♦ Implementar algoritmos de encriptação e segurança na transmissão de dados

Módulo 20. Gestão de identidade e acessos em segurança IT

- ♦ Desenvolver as competências necessárias para gerir a identidade e os acessos em sistemas de TI
- ♦ Estabelecer políticas de autenticação e controlo de acesso para proteger os recursos e dados da organização

Módulo 21. Segurança em comunicações e operação software

- ♦ Capacitar na proteção das comunicações digitais e na implementação de medidas de segurança na operação de software
- ♦ Garantir a confidencialidade, integridade e disponibilidade da informação

Módulo 22. Segurança em ambientes cloud

- ♦ Implementar políticas de segurança em ambientes de computação em nuvem
- ♦ Assegurar que os dados e as aplicações sejam protegidos contra acessos não autorizados e ataques

Módulo 23. Ferramentas de Monitorização em Políticas de Segurança dos sistemas de informação

- ♦ Capacitar no uso de ferramentas de monitorização para avaliar a eficácia das políticas de segurança nos sistemas de informação
- ♦ Aprofundar na deteção precoce de vulnerabilidades e ataques

Módulo 24. Segurança em comunicações de dispositivos IoT

- ♦ Desenvolver competências na implementação de medidas de segurança para proteger as comunicações entre dispositivos IoT
- ♦ Minimizar os riscos associados com o intercâmbio de dados entre dispositivos conectado

Módulo 25. Plano de continuidade de negócios associado à segurança

- ♦ Desenvolver um plano de continuidade de negócios que garanta a proteção e recuperação rápida dos sistemas
- ♦ Estabelecer protocolos para velar pelos dados essenciais em caso de incidentes de segurança

Módulo 26. Política de Recuperação Prática de Desastres de Segurança

- ♦ Criar políticas de recuperação perante desastres
- ♦ Assegurar a rápida restauração dos sistemas e a proteção dos dados em caso de incidentes graves de segurança

Módulo 27. Implementação de políticas de segurança física e ambiental na empresa

- ♦ Capacitar na implementação de políticas de segurança física e ambiental para proteger os recursos físicos da organização
- ♦ Assegurar o ambiente adequado para o funcionamento seguro dos sistemas tecnológicos

Módulo 28. Políticas de comunicações seguras na empresa

- ♦ Proporcionar os conhecimentos para desenvolver políticas de comunicações seguras dentro da organização
- ♦ Proteger as redes e canais de comunicação contra espionagem e filtragem de informação

Módulo 29. Aspectos organizacionais em políticas de segurança da informação

- ♦ Proporcionar as ferramentas necessárias para implementar políticas organizacionais na gestão da segurança da informação
- ♦ Estabelecer papéis, responsabilidades e processos adequados para proteger os ativos de informação

05

Oportunidades de carreira

Ao finalizar o Mestrado Avançado em Gestão Avançada da Cibersegurança (CISO, Chief Information Security Officer), os alunos estarão plenamente capacitados para assumir funções chave na proteção e gestão da segurança da informação em diversas organizações. Além disso, poderão liderar estratégias de segurança em empresas multinacionais, gerindo e mitigando riscos cibernéticos. Da mesma forma, estarão preparados para ocupar cargos que exigem habilidades para liderar iniciativas de cibersegurança e garantir a proteção dos ativos digitais em qualquer setor.



“

*Com este Mestrado Avançado, irá
especializar-se como um Diretor
capaz de antecipar os riscos e
proteger a informação crítica”*

Perfil dos nossos alunos

O aluno do Mestrado Avançado em Gestão Avançada da Cibersegurança (CISO, Chief Information Security Officer) será um líder estratégico com uma compreensão profunda da segurança da informação no contexto de organizações globais. Estará capacitado para desenhar e implementar políticas de segurança avançadas e liderar equipas multidisciplinares. Ademais, terá sólidas competências de gestão e governança, permitindo-lhe enfrentar os desafios da cibersegurança em diversos setores, garantindo a proteção dos ativos digitais. Esta oportunidade proporcionará as ferramentas necessárias para estar atualizado com as últimas tendências tecnológicas e adaptar-se às rápidas mudanças no panorama digital.

Prepare-se para ser um dos melhores profissionais, minimizando o impacto dos ciberataques e recuperando a normalidade rapidamente.

- ♦ **Liderança estratégica e adaptabilidade:** Capacidade para liderar equipas multidisciplinares e gerir políticas de segurança, adaptando-se às rápidas mudanças tecnológicas e emergentes em cibersegurança
- ♦ **Gestão de riscos e tomada de decisões informadas:** Habilidade para identificar, avaliar e mitigar riscos cibernéticos, tomando decisões baseadas em dados e análises detalhadas
- ♦ **Análise crítica e gestão de incidentes:** Capacidade para identificar vulnerabilidades, gerir incidentes de segurança e coordenar a resposta a crises, garantindo a continuidade do negócio
- ♦ **Comunicação eficaz e pensamento estratégico:** Habilidade para comunicar riscos e soluções de forma clara a diferentes stakeholders, adotando uma abordagem global e estratégica para a proteção dos ativos digitais



Após realizar o Mestrado Avançado, poderá desempenhar os seus conhecimentos e competências nos seguintes cargos:

- 1. Chief Information Security Officer (CISO):** Líder estratégico responsável pela proteção da informação e da cibersegurança em toda a organização, desenvolvendo políticas e supervisionando a infraestrutura de segurança digital
- 2. Diretor de Cibersegurança:** Responsável pela gestão e supervisão das equipas de segurança informática, desenvolvendo e implementando estratégias para proteger a infraestrutura tecnológica da empresa.
- 3. Gestor de Segurança Informática:** Responsável por gerir e coordenar as políticas de segurança digital, supervisionando a proteção de dados e sistemas informáticos contra possíveis ameaças.
- 4. Consultor de Cibersegurança:** Especialista em aconselhar empresas sobre a melhor maneira de implementar e gerir políticas de cibersegurança, ajudando a mitigar riscos e a cumprir com as normativas internacionais
- 5. Gerente de Gestão de Riscos Informáticos:** Responsável por identificar, avaliar e mitigar os riscos cibernéticos que possam afetar a segurança da informação e os sistemas tecnológicos da organização
- 6. Chefe de Segurança da Informação:** Líder responsável por supervisionar e coordenar todas as iniciativas relacionadas com a proteção dos dados e sistemas informáticos dentro da organização



Está a um passo de melhorar a sua vida profissional com este Mestrado Avançado que só oferece-lhe a TECH”

06

Metodologia de estudo

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

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



“

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

O aluno: a prioridade de todos os programas da TECH

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

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

“

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



Os programas de ensino mais abrangentes do mundo

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

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

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

“

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

Case studies ou Método de caso

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

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

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



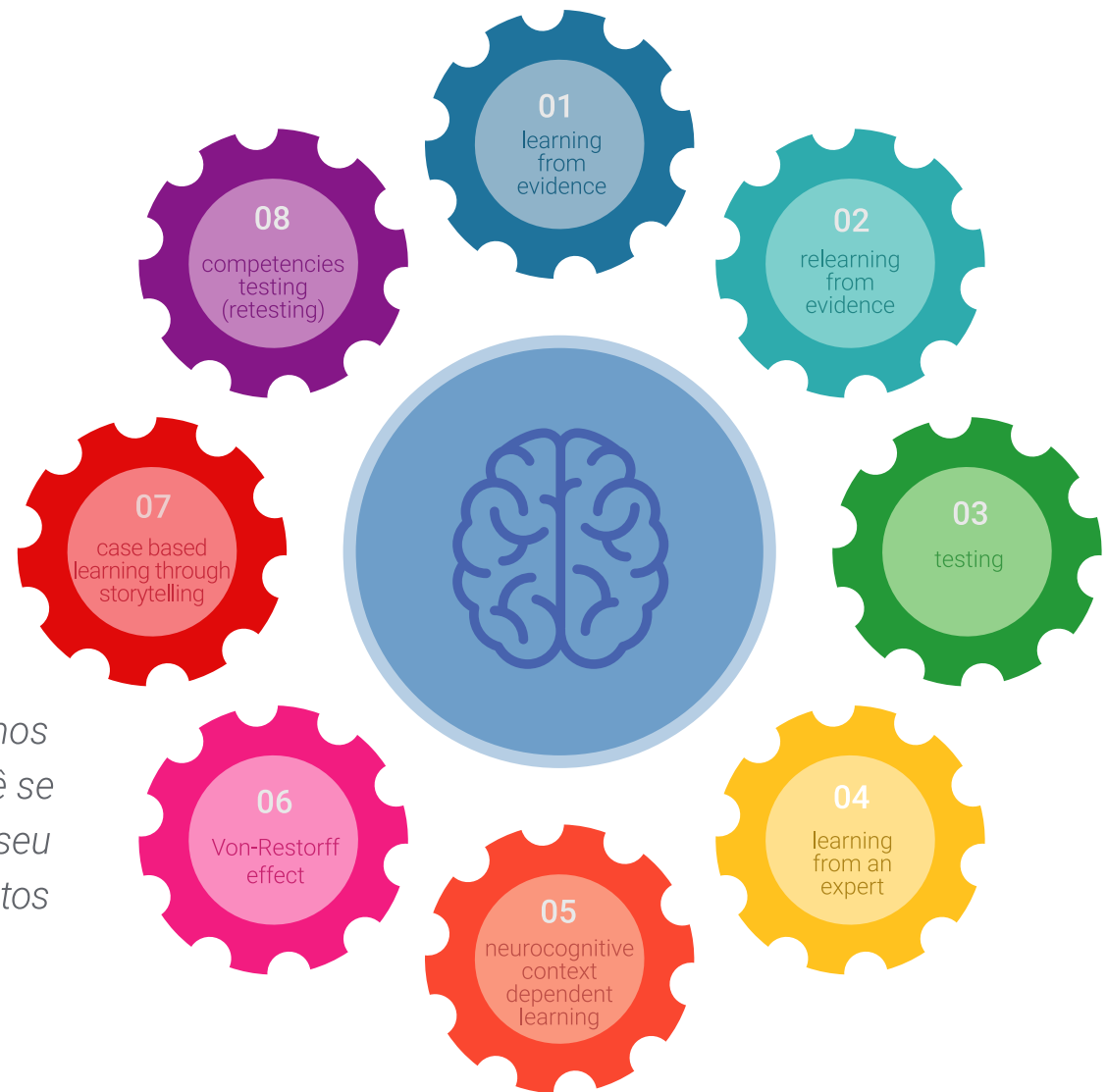
Método Relearning

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

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

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

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



Um Campus Virtual 100% online com os melhores recursos didáticos

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

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

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

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



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

A eficácia do método é justificada por quatro conquistas fundamentais:

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

A metodologia universitária mais bem avaliada por seus alunos

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

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

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

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



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



Material de estudo

O conteúdo didático foi elaborado especialmente para este curso pelos especialistas que irão ministrá-lo, o que permite que o desenvolvimento didático seja realmente específico e concreto.

Posteriormente, esse conteúdo é adaptado ao formato audiovisual, para criar o método de trabalho online, com as técnicas mais recentes que nos permitem lhe oferecer a melhor qualidade em cada uma das peças que colocaremos a seu serviço.



Práticas de aptidões e competências

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



Resumos interativos

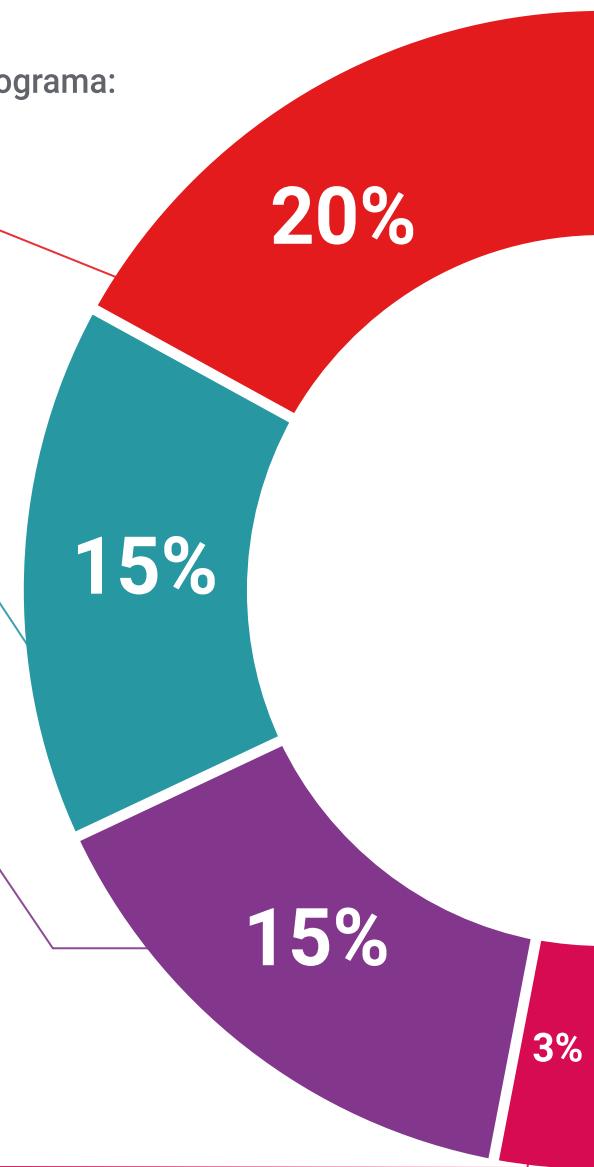
Apresentamos os conteúdos de forma atraente e dinâmica em pílulas multimídia que incluem áudio, vídeos, imagens, diagramas e mapas conceituais com o objetivo de reforçar o conhecimento.

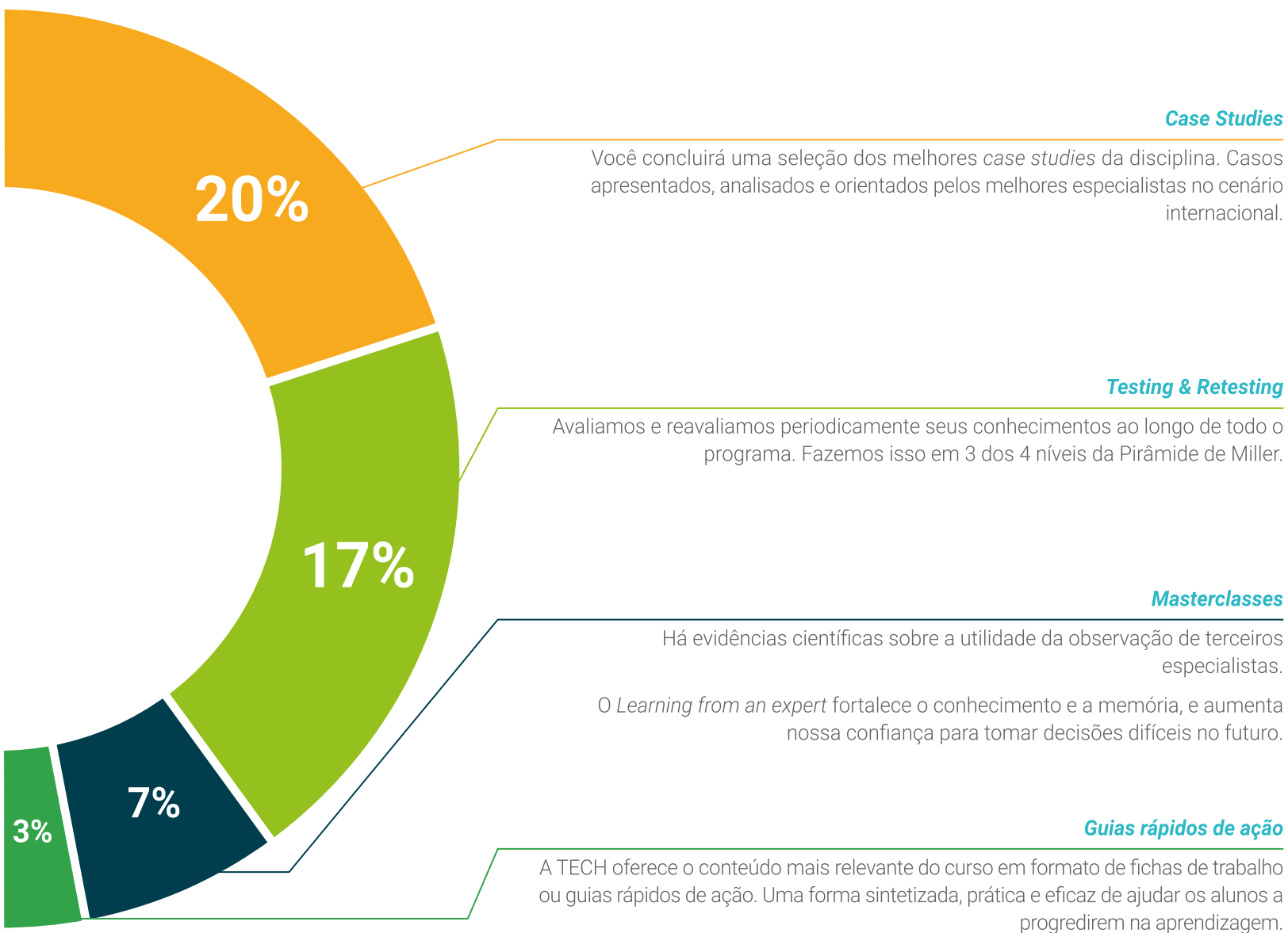
Este sistema exclusivo de capacitação por meio da apresentação de conteúdo multimídia foi premiado pela Microsoft como "Caso de sucesso na Europa"



Leituras complementares

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





07

Corpo docente

Este Mestrado Avançado em Gestão Avançada da Cibersegurança (CISO, Chief Information Security Officer) conta com um corpo docente composto por profissionais em ativo que conhecem na perfeição o estado atual desta área, e que, por isso, irão transmitir todas as chaves da cibersegurança atual ao aluno. Deste modo, garante-se que o estudante deste programa obtenha os últimos avanços neste campo, ao poder aceder a eles graças ao prestigiado corpo docente selecionado pela TECH.



“

A TECH oferece-lhe os Diretores e Docentes mais especializados para que o seu enfoque e aprendizagem sejam os melhores”

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 o ensino posicionam-no como uma figura-chave na promoção da segurança e da compreensão das tecnologias emergentes atuais. 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 painelistas 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**.



Sr. Lemieux, Frederic

- Diretor do Mestrado em Cybersecurity Risk Management na Universidade de Georgetown nos Estados Unidos
- Diretor do Mestrado em Technology Management na Universidade de Georgetown
- Diretor do Mestrado em Applied Intelligence na Universidade de Georgetown
- Professor de Estágio na Universidade de Georgetown
- Doutorado em Criminologia pela School of Criminology na Universidade de Montreal
- Licenciatura em Sociologia e Minor Degree em Psicologia pela Universidade de Laval
- Membro de: New Program Roundtable Committee na Universidad de Georgetown

“

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

Direção



Sra. Fernández Sapena, Sonia

- Formadora 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
- Formadora especializada certificada 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*) na Universidade das Ilhas Baleares
- Engenheira em Informática pela Universidade de Alcalá de Henares de Madrid
- Mestrado em DevOps: Docker and Kubernetes. Cas-Training
- Microsoft Azure Security Technologies. E-Council



Sr. Olalla Bonal, Martín

- Gestor Sênior 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

Sra. Marcos Sbarbaro, Victoria Alicia

- ♦ 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 Catalunya
- ♦ Mestrado em Segurança Informática e Hacking Ético Oficial EC- Council e CompTIA pela Escola Profissional de Novas Tecnologias CICE

Sr. Entrenas, Alejandro

- ♦ 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 Córdoba
- ♦ 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

Sr. Catalá Barba, José Francisco

- ♦ Técnico Eletrónico com Especialização 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

Sr. Peralta Alonso, Jon

- ♦ 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 Proteção de Dados Delegado pela EIS Innovative School
- ♦ Mestrado em Advocacia pela Universidade Pública do País Basco
- ♦ Mestrado Especialista em Contencioso Civil pela Universidade Internacional Isabel I de Castilla
- ♦ Docente do Mestrado em Proteção de Dados Pessoais, Cibersegurança e Direito das TIC

Sr. Gonzalo Alonso, Félix

- ♦ 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 Companhias de Seguros
- ♦ Licenciatura em Engenharia Técnica Industrial, especialidade em Eletrónica Industrial pela Universidade Pontifícia de Comillas

Sr. Jiménez Ramos, Álvaro

- ♦ 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

Sr. Redondo, Jesús Serrano

- ♦ Programador Web e Técnico de Cibersegurança
- ♦ Programador Web na Roams, Palencia
- ♦ Desenvolvedor FrontEnd na Telefónica, Madrid
- ♦ Programador FrontEnd na Best Pro Consulting SL, Madrid
- ♦ Instalador de Equipamentos e Serviços de Telecomunicações no Grupo Zener, Castilla y León
- ♦ 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

Sr. Nogales Ávila, Javier

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

Sr. Gómez Rodríguez, Antonio

- ♦ 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
- ♦ Licenciatura em Engenharia de Telecomunicações pela Universidade Politécnica da Catalunha

Sr. Rodrigo Estébanez, Juan Manuel

- ♦ 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
- ♦ Licenciatura em Engenharia pela Universidade de Valladolid
- ♦ Mestrado em Sistemas de Gestão Integrados pela Universidade CEU San Pablo

Sr. Del Valle Arias, Jorge

- ♦ 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

Sr. Gozalo Fernández, Juan Luis

- ♦ 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



Sra. Jurado Jabonero, Lorena

- ♦ 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
- ♦ Licenciatura em Engenharia Informática pela Universidade Alfonso X El Sabio
- ♦ Engenheiro Técnico em Informática de Gestão pela Universidade Politécnica de Madrid
- ♦ Certified Data Privacy Solutions Engineer (CDPSE) pelo ISACA

Sr. Ortega Esteban, Octavio

- ♦ 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
- ♦ Licenciatura em Psicologia pela Universidade Aberta da Catalunha
- ♦ Técnico Superior Universitário em Análise, Design e Soluções de *Software*
- ♦ Técnico Superior Universitário em Programação Avançada

Sr. Embid Ruiz, Mario

- ♦ 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
- ♦ Licenciatura em Direito pela Universidade Rey Juan Carlos
- ♦ Licenciatura 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



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

08

Certificação

O Mestrado Avançado em Gestão Avançada da Cibersegurança (CISO, Chief Information Security Officer) garante, além da formação mais rigorosa e atualizada, o acesso a um certificado de Mestrado Avançado emitido pela TECH Global University.



“

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

Este programa permitirá a obtenção do certificado próprio de **Mestrado Avançado em Gestão Avançada da Cibersegurança (CISO, Chief Information Security Officer)** reconhecido pela TECH Global University, a maior universidade digital do mundo.

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

Título: **Mestrado Avançado em Gestão Avançada da Cibersegurança (CISO, Chief Information Security Officer)**

Modalidade: **online**

Duração: **2 anos**

Acreditação: **120 ECTS**



futuro
saúde confiança pessoas
informação orientadores
educação certificação ensino
garantia aprendizagem
instituições tecnologia
comunidade compromisso
atenção personalizada
conhecimento inovação
presente qualidade
desenvolvimento site



Mestrado Avançado
Gestão Avançada da
Cibersegurança (CISO,
Chief Information
Security Officer)

- » Modalidade: online
- » Duração: 2 anos
- » Certificação: TECH Global University
- » Acreditação: 120 ECTS
- » Horário: ao seu próprio ritmo
- » Exames: online

Mestrado Avançado

Gestão Avançada da
Cibersegurança (CISO, Chief
Information Security Officer)